<div align="center">DATA PROCESSING ADDENDUM</div>

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1 (with Annex 1), Schedule 2 and Schedule 3.

2. This DPA has been pre-signed on behalf of Syncron. The Standard Contractual Clauses in Schedule 1 have been pre-signed by Syncron as the data importer.

3. To complete this DPA, Customer must:

(i) Complete the information in the signature box and sign on Page 7.

(ii) Complete the information in the signature box and sign on Pages 16.

(iii) Send the completed and signed DPA to Syncron by email, indicating the full legal entity name (as set out on the applicable underlying Master Subscription Agreement/Order Form), to privacy@syncron.com.

WHEREAS

This Data Processing Addendum ("**DPA**") is hereby incorporated to and forms part of the Master Subscription Agreement or other written or electronic agreement between Syncron and Customer for the subscription of cloud Services (including associated offline or mobile components) from Syncron (the "**Agreement**"), identified either as Services or otherwise in the applicable agreement, ("**Services**"). This DPA is intended to reflect the parties' agreement regarding the processing of personal data that Customer or its Users may, from time to time, transfer to Syncron.

The Customer entity that is a party to the Agreement should be a party to this DPA. The Syncron entity that is a party to the Agreement should be a party to this DPA.

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, Syncron may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

This DPA shall not replace any comparable or additional rights relating to Processing of Customer Data contained in the Agreement.

1.   **DEFINITIONS**

"**Affiliate**" means an entity that is: (a) controlled, directly or indirectly, by a party to this DPA; (b) controls, directly or indirectly, a party to this DPA; or (c) is under common control with a party to this DPA, whereby "control" means the possession by virtue of ownership, directly or indirectly, of more than fifty percent (50%) of the shares of voting rights.

"**Authorized Affiliate**" means any of Customer's Affiliate(s) that (a) is permitted to use the Services pursuant to the Agreement between Customer and Syncron, but has not signed its own Agreement or purchase order with Syncron and is not a "Customer" as defined under the Agreement.

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

"**Controller**" means the entity that determines the purposes and means of the Processing of Personal Data.

"**Customer**" as defined in the Agreement.

"**Customer Data**" means what is defined in the Agreement as "Customer Data", which may include Personal Data.

"**Data Protection Laws and Regulations**" means GDPR, CCPA, and any other applicable data protection or privacy laws of any state or country, in each case as amended, consolidated, re-enacted or replaced from time to time, and to the extent applicable to the processing of Personal Data under the Agreement.

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

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,

and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Services**" as defined in the Agreement.

"**Standard Contractual Clauses**" means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council; or any document that replaces these clauses; the Standard Contractual Clauses are deemed to be amended from time to time to reflect any change made in accordance with Data Protection Laws and Regulations as applicable by (i) the EU Commission to or of the equivalent contractual clauses approved by the EU Commission under the GDPR (in the case of the Data Protection Laws and Regulations of the European Union or a member state); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another jurisdiction.

"**Personal Data**" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations); categories of Customer's Personal Data, which may be processed by Syncron, are specified in sec. 3.1. below.

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

"**Processor**" means the entity that Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA, or any related role under applicable Data Protection Laws and Regulations.

"**Syncron**" means the Syncron entity that is a party to this DPA, being Syncron AB, a company registered in Sweden, Syncron UK Ltd, a company registered in England and Wales, Syncron Germany GmbH, a company registered in Germany, Syncron Software India Private Limited, a company registered in Karnataka, India; Syncron Italy s. a r.l., a company registered in Italy, Syncron Poland sp. z o.o. and Syncron Poland Services sp. z o.o., companies registered in Poland, Syncron Japan Corp., a company incorporated in Japan, Syncron Inc., a company incorporated in Illinois, Syncron France SAS, a company registered in France, Mize Inc., a company incorporated in Delaware, or Mize Software Solutions Private Limited, a company registered in Telangana, India, as applicable.

"**Third-Party Sub-processor**" means a third-party subcontractor, other than a Syncron Affiliate, engaged by Syncron that, as part of the subcontractor's role of delivering the Services, may Process Personal Data of the Customer.

"**Supervisory Authority**" means an independent public authority that is established by an EU Member State pursuant to the GDPR, or an equivalent body established under applicable Data Protection Laws and Regulations.

2. CONTROLLER AND PROCESSOR OF PERSONAL DATA AND PURPOSE OF THE PERSONAL DATA PROCESSING

2.1 Customer will at all times remain the Controller for the purposes of provision of Services by Syncron. Customer is responsible for compliance with its obligations as a Controller under Data Protection Laws and Regulations, in particular for justification of any transmission of Personal Data to Syncron (including the basis of the processing, providing any required notices and obtaining any required consents and authorizations), and for its decisions and actions concerning the Processing and use of the Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations and Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data so far as applicable under the CCPA or other applicable Data Protection Laws and Regulations. Customer represents and warrants to Syncron, that Personal Data does not and will not contain any sensitive data, health information, any biometric information, or any payment card information subject to the Payment Card Industry Data Security Standard (other than any Customer payment card information used to pay for the Services, if applicable).

2.2 Customer may provide instructions in writing to Syncron with regard to Processing of Personal Data. Syncron will comply with all such instructions without additional charge to the extent necessary for Syncron to comply

with its obligations as a Processor in the performance of the Services. Customer, on behalf of itself and of any Authorized Affiliate, instructs Syncron (and authorizes Syncron to instruct each Third-Party Sub-processor) to process Personal Data and transfer Personal Data to any country or territory as reasonably necessary for the provision of the Services set forth in the Agreement and warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instruction set out above on behalf of each Authorized Affiliate. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations.

2.3 For the purposes of provision of the Services set forth in the Agreement, Syncron is a Processor, and Syncron or Syncron Affiliates may engage Third-Party Sub-processors in accordance with this DPA. Syncron will Process Personal Data as necessary for the provision of the Services set forth in the Agreement, and will not otherwise (i) Process Personal Data for purposes other than those set forth in the Agreement or as instructed by Customer in good faith pursuant to this DPA, or (ii) disclose such Personal Data to third parties other than Syncron Affiliates or Third-Party Sub-processors for the aforementioned purposes or as required by Data Protection Laws and Regulations.

2.4 Syncron shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the DPA and the Agreement to fulfil Syncron's obligations arising therefrom, in particular to ensure secure access to and usage of the Services by authorized Users and to provide support; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.5 Syncron will comply with applicable Data Protection Laws and Regulations to the extent that such laws by their terms impose obligations directly upon Syncron as a Processor in connection with the Services provided to the Customer.

2.6 Syncron Processes Personal Data under Data Protection Laws and Regulations' requirements directly applicable to Syncron's provision of its Services. Upon Customer's request, Syncron shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligations and tasks under applicable Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Syncron.

2.7 The parties acknowledge and agree that, by executing the Agreement, the Customer enters into the DPA on behalf of itself and, as applicable and to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Syncron and each such Authorized Affiliate subject to the provisions of the Agreement and this DPA. Customer warrants that Customer's entry into this DPA as an agent for each Authorized Affiliate will have been duly authorized by each Authorized Affiliate and that each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and will be only deemed as a party to the DPA. All access to and use of the Services and its content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

3. CATEGORIES OF PERSONAL DATA AND DATA SUBJECTS

3.1 In order to execute the Agreement, and in particular to perform the Services, Customer authorizes and requests that Syncron Processes the following:

Categories of Personal Data: Personal Data may include, among other information, personal contact information such as name, company address, telephone or mobile number, fax number, email address; employment details including employer's name, job title, identification numbers; user ID, location data; connection data; device specific information, IP addresses, and online behavior data (as applicable).

Categories of Data Subjects: Data subjects may include administrators and users of Services, such as employees, contractors of Customer and its Authorized Affiliates; collaborators, partners, dealers, suppliers and their respective employees and contractors, and other users of the Customer (as applicable). Data subjects may also include Customer's contact persons, its authorized signatories and, if applicable, contact details to Customer's business partners, dealers, suppliers or other people designated by Customer.

3.2 Syncron will Process Personal Data for the duration of the Agreement, unless otherwise agreed between the

syncron

Parties.

4.   RIGHTS OF DATA SUBJECTS

As further set out in Chapter III of the GDPR and as otherwise set out by applicable Data Protection Laws and Regulations, a Data Subject has certain rights (e.g. information and access to personal data, rectification and erasure, restriction of processing, data portability, right to object to processing). The Controller is obliged to facilitate the exercise of these data subject rights under applicable Data Protection Laws and Regulations. The Processor shall assist the Controller by appropriate technical and organizational measures, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights. In consequence, Syncron shall, to the extent legally permitted, notify Customer if Syncron or any Third-Party Sub-processor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, etc. ("Request"). Taking into account the nature of the Processing, Syncron shall assist Customer, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Request under Data Protection Laws and Regulations. Syncron shall not respond to such request except on the documented instructions of the Customer or as required by Data Protection Laws and Regulations (Syncron shall to the extent permitted by Data Protection Laws and Regulations inform Customer of that legal requirement before responding to the request).

5.   PERSONNEL

5.1   Syncron shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed confidentiality undertakings. Syncron shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

5.2   Syncron shall take commercially reasonable steps to ensure the reliability of any Syncron personnel engaged in the Processing of Personal Data.

5.3   Syncron shall ensure that Syncron's access to Personal Data is limited to those personnel performing services in accordance with the Agreement.

5.4   Syncron and its Affiliates have appointed a data protection officer. The appointed person may be reached at privacy@syncron.com.

6.   SYNCRON AFFILIATES AND THIRD-PARTY SUB-PROCESSORS

6.1   Some or all of Syncron's obligations under the Agreement may be performed by Syncron's Affiliates and Third-Party Sub-processors. Syncron maintains a list of Syncron's Affiliates and Third-Party Sub-processors that may Process Personal Data, which is part of Syncron Privacy Policy available here and reiterated below in Schedule 3 of this DPA. Customer agrees to the processing of Personal Data by sub-processors presented therein as of the date of entering into the Agreement.

6.2   Customer acknowledges and authorizes Syncron to (a) retain Syncron's Affiliates as sub-processors; and to (b) appoint (and permit each Syncron Affiliate and any Third-Party Sub-processor to appoint) Third-Party Sub-processors in connection with the provision of the Services (in accordance with this DPA).

6.3   The Syncron Affiliates and Third-Party Sub-processors are required to abide by substantially the same obligations as Syncron under this DPA as applicable to their Processing of Personal Data. Syncron or a Syncron Affiliate shall enter into a written agreement with each Third-Party Sub-processor containing data protection obligations, which offer at least the same level of protection for Personal Data as those set out in this DPA and meet the requirements of article 28(3) of the GDPR or other applicable Data Protection Laws and Regulations to the extent applicable to the nature of the Services provided by such Third-Party Sub-processor.

6.4   Syncron shall notify the Customer about appointment of any new Third-Party Sub-processor, including about the purpose of the Processing to be undertaken by the Third-Party Sub-processor, by sending a notification to Customer's primary contact or, on Customer request, to a dedicated e-mail address submitted to privacy@syncron.com. Customer may object to Syncron's use of a given Third-Party Sub-processor by sending the objection in writing within 14 days' from receiving the notification from Syncron. Objection shall be provided to Syncron to privacy@syncron.com and shall include reasonable grounds for objection. In the event Customer objects to a Third-Party Sub-processor, the parties will come together in good faith to discuss a resolution. Syncron will use reasonable efforts to recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to Third-Party Sub-processor without unreasonably burdening Customer.

6.5 Syncron remains responsible at all times for compliance with the terms of this DPA by Syncron's Affiliates and Third-Party Sub-processors to the same extent Syncron would be liable if performing the services of each sub-processor directly under the terms of this DPA.

7. INTERNATIONAL DATA TRANSFERS TO THIRD COUNTRIES

7.1 Syncron treats all Personal Data in a manner consistent with the requirements of the Agreement and this DPA in all locations globally. Syncron's information, privacy and security policies, standards and governance practices are managed on a global basis.

7.2 Transfers of Personal Data originating from the EEA or Switzerland to Syncron's Affiliates or Third-Party Sub-processors located in countries outside the EEA or Switzerland that have not received a binding adequacy decision by the European Commission or by a competent national data protection authority (i.e., third countries that does not ensure an adequate level of protection for the rights and freedoms of data subjects), are subject to the following provisions:

7.2.1 Transfer of Personal Data from Customer to Syncron and/or Syncron Affiliates is made subject to this DPA and (i) Standard Contractual Clauses with Customer acting as the "data exporter" and Syncron and/or Syncron Affiliate(s) located in a third country acting as the "data importers", whereas the Standard Contractual Clauses applicable under this DPA constitute Schedule 1,incorporated here by reference; or (ii) other appropriate transfer mechanisms that provide an adequate level of protection in compliance with the Data Protection Laws and Regulations, whereas the terms of this DPA shall be read in conjunction with the Standard Contractual Clauses or other appropriate transfer mechanisms.

7.2.2 For transfers from Syncron to Syncron Affiliates located in third countries, Syncron represents that such transfers are subject to (i) the terms of Syncron Intracompany Data Processing Agreement (with Intracompany Confidentiality Undertaking) entered into between Syncron AB and its Affiliates, which requires all transfers of Personal Data to be made in compliance with Standard Contractual Clauses and all applicable Syncron security and data privacy policies and standards, or (ii) other appropriate transfer mechanisms that provide an adequate level of protection in compliance with the Data Protection Laws and Regulations.

7.2.3 For transfer from Syncron and/or Syncron Affiliates to Third-Party Sub-processors, in addition to the agreement referred to in sec. 6.3 above, Syncron or Syncron Affiliate has entered or will enter into the Standard Contractual Clauses based on the Module 3 thereof, prior to the Third-Party Sub-processor's Processing of Personal Data (unless other lawful transfer mechanism is established). Customer hereby (itself as well as on behalf of each data controller) accedes to the Standard Contractual Clauses between Syncron and the Third-Party Sub-processors located outside of the EEA or Switzerland.

7.3 Syncron is committed to Process Personal Data in accordance with applicable Data Protection Laws and Regulations' requirements for international data transfers.

8. SECURITY

Syncron has, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the assessment of risks to the rights and freedoms of natural persons, implemented and maintains appropriate technical and organizational measures for protection, security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data. Technical and organizational security measures (controls) applied to processing of Customer Data, including Processing of Personal Data, are set forth in Schedule 3 hereto. Syncron regularly monitors compliance with these measures. Syncron will not materially decrease the overall security of the Services during a subscription term. Syncron information security management system achieved the certification with the ISO 27001 standard.

9. CUSTOMER DATA MANAGEMENT AND NOTIFICATION

9.1 Syncron maintains security management policies and procedures in place, including Information security policy and security incident management policy. Syncron shall notify Customer, without undue delay, after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Syncron or its sub-processors. Syncron shall make reasonable efforts to identify the cause of such incident and take those steps as Syncron deems necessary and reasonable in order to remediate the cause of such incident to the extent the remediation is within Syncron's reasonable control. Syncron shall provide Customer with sufficient information to allow Customer to meet any obligations to report or inform data subjects of the personal data breach under applicable Data

Protection Laws and Regulations. Syncron shall co-operate with Customer and take such reasonable commercial steps as directed by Customer to assist in the investigation, mitigation and remediation of each such personal data breach. The obligations herein shall not apply to incidents or breaches that are caused by Customer or Customer's Users.

9.2 Syncron shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with any Supervisory Authority or other competent data privacy authorities, which Customer reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other applicable Data Protection Laws and Regulations, in each case solely in relation to the Processing of Personal Data by, and taking into account the nature of the Processing and information available to Syncron, its Affiliates or any Third-Party Sub-processor.

10. LIMITATION OF LIABILITY

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

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

11. DELETION OR RETURN OF PERSONAL DATA

11.1 Subject to sections 11.2 and 11.3 Syncron and Syncron Affiliates shall promptly and in any event within 30 days of the date of cessation of any Services involving the Processing of Personal Data (the "Cessation Date"), delete all copies of those Personal Data of Customer.

11.2 Subject to section 11.3, Customer may in its absolute discretion by a written notice to Syncron within 30 days of the Cessation Date require Syncron and each Syncron Affiliate to return a complete copy of all Customer Personal Data to Customer by making it available for download.

11.3 Syncron and Syncron Affiliates may retain Personal Data to the extent required by Data Protection Laws and Regulations and only to the extent and for such period as required by Data Protection Laws and Regulations and always provided that Syncron and each Syncron Affiliate shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Data Protection Laws and Regulations requiring its storage and for no other purpose.

11.4 Syncron shall upon request provide written certification to Customer that it and each Syncron Affiliate has fully complied with this section 11 within 60 days of the Cessation Date.

12. AUDIT RIGHTS

12.1 Subject to sections 12.2 to 12.3, Syncron and each Syncron Affiliate shall make available to each Customer on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by Customer or an auditor mandated by Customer (obligated to confidentiality) in relation to the Processing of the Personal Data by Syncron, any Syncron Affiliate or any Third-Party Sub-processor.

12.2 Information and audit rights of the Customer only arise under section 12.1 to the extent that the Agreement does not otherwise give them information meeting the relevant requirements of Data Protection Laws and Regulations (including, where applicable, article 28(3)(h) of the GDPR).

12.3 Customer undertaking an audit shall give Syncron or the relevant Syncron Affiliate a reasonable notice (at least 30 days) of any audit or inspection to be conducted under section 12.1, which shall be limited to the audit of the architecture, systems and procedures relevant to processing of Personal Data. Before the commencement of any audit, Parties shall mutually agree upon the scope, timing, and duration of the audit, none of which shall adversely affect Syncron, any Syncron Affiliate or any Third-Party Sub-processor', or any how disrupt their business operations. Syncron, any Syncron Affiliate or any Third-Party Sub-processor needs not give access to its premises for the purposes of such an audit or inspection to any individual unless he or she produces a reasonable evidence of identity and authority; outside normal business hours at those premises; or for the

purposes of more than one audit or inspection, in respect of Syncron, any Syncron Affiliate or any Third-Party Sub-processor each, in any calendar year, except for any additional audits or inspections, which: (i) Customer undertaking an audit reasonably considers necessary because of genuine concerns as to Syncron's or the relevant Syncron Affiliate's compliance with this DPA; or (ii) Customer is required or requested to carry out by a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws and Regulations in any country or territory.

12.4   If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request and Syncron has confirmed there are no known material changes in the controls audited, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures. If any controls or measures are not included in the above mentioned audit reports, Customer will provide Syncron with a detailed schedule of such missing controls or measures that Customer wants to audit (at least 30 days prior to an audit).

13.   GENERAL TERMS, GOVERNING LAW AND DISPUTE RESOLUTION

13.1   All notices, permissions and approvals will be provided in accordance with Agreement.

13.2   The governing law and dispute resolution clauses set out in the Agreement shall also be applicable to this DPA. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Schedules and Annexes.

13.3   This DPA shall come into effect upon signing the Agreement by the Parties. Without prejudice to Section 11, this DPA shall automatically expire upon any termination or expiration of the Agreement.

13.4   Syncron reserves the right to amend the terms of this DPA from time to time, so far as necessary to comply with applicable Data Protection Laws and Regulations. Syncron will notify the Customer about any material amendments by sending a notification to Customer's primary contact or, on Customer request, to a dedicated e-mail address submitted to privacy@syncron.com. Customer may object to a given amendment by sending the objection in writing within 14 days' from receiving the notification from Syncron. Objection shall be provided to Syncron to privacy@syncron.com and shall include reasonable grounds for objection. The parties will come together in good faith to discuss a resolution.

13.5   In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail. In the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA shall prevail.
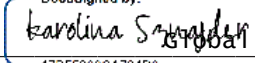
This DPA has been executed in two originals of which the parties have taken one each.

Date: _____   Date: ___24 September 2021___

On behalf of CUSTOMER (Controller)   On behalf of SYNCRON (Processor)

_____   ___Karolina Szmajduk___ Global Legal Counsel

List of Schedules

Schedule 1: Standard Contractual Clauses with Annex 1(Customer-Syncron)

Schedule 2: Technical and organizational security measures

Schedule 3: List of sub-processors

<u>SCHEDULE 1 - Standard Contractual Clauses</u>

[*These Standard Contractual Clauses shall take effect upon signing of the Agreement by Customer. For Customers who have signed the Agreement before September 27, 2021, these new Standard Contractual Clauses shall replace the existing Standard Contractual Clauses previously issued by the European Commission and thus far being part of Customer DPA. New Standard Contractual Clauses shall take effect as from October 27, 2021 and become an integral part of the existing Customer DPA.*

These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Data Transfer which is subject to the Data Protection Laws and Regulations of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement)of these Clauses (or any equivalent thereof) made in accordance with those Data Protection Laws and Regulations by the Commission or an equivalent competent authority.]

<div align="center">SECTION I</div>

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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 or return of data

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

8.6 Security of processing

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

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

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

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

subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

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

8.8 Onward transfers

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

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

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

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

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

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

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. 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 subprocessors at least 14 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

Clauses.

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

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the subprocessor 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) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories

and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

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

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

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

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

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

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

Clause 15

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

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it: (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where: (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension; (ii) the data importer is in substantial or persistent breach of these Clauses; or (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses. In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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

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

Clause 17

Governing law

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

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 EU Member State which law governs the Agreement (or other underlying agreement) between the Parties).

(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):

Customer as described in the Agreement.

Activities relevant to the data transferred under the Clauses: fulfilment of the Agreement

Role (controller/~~processor~~)

Signature (First and Last Name)
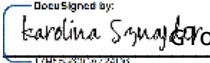
_____

_____

Date

Data importer(s):

Syncron Affiliate(s) located in a third country, as applicable. Syncron Affiliates may take part in provision of Services, which may include support, development, expert services and software maintenance. Syncron is a software-as-a-service provider who offers applications for optimizing its customers after-sales performance, which involves processing personal data provided by users of Services. The data importer will have access to any data provided by the data exporter and will use it exclusively and solely for purposes related to provision of Services.

Activities relevant to the data transferred under the Clauses: fulfilment of the Agreement

Role (~~controller~~/processor)

Signature (First and Last Name)

Karolina Szmajdobal Legal Counsel

24 September 2021

Date

B. DESCRIPTION OF THE TRANSFER

Categories of data subjects whose personal data is transferred: The categories of data subjects whose personal data may be transferred in connection with the Services are determined and controlled by the data exporter in its sole discretion and may include but are not limited to: administrators and users of Services, such as employees, contractors, collaborators, partners, dealers, suppliers and other users of Customer (as applicable), who have access to Services and who may store user account information in the Services. Data subjects may also include Customer's contact persons, its authorized signatories and, if applicable, contact details to Customer's business partners, dealers, suppliers or other people designated by Customer.

Categories of personal data transferred: The categories of personal data are determined by the data exporter in its sole discretion and may include but are not limited to: personal contact information such as name, company address, telephone or

mobile number, fax number, email address; employment details including employer name, job title, identification numbers; user ID, location data; connection data; device specific information, IP addresses, and online behavior data (as applicable).

The frequency of the transfer: the data is transferred on a continuous basis throughout the Subscription Term (term of the underlying agreement)

Nature of the processing: Data will be processed automatically.

Processing activities may include but are not limited to: creation and administration of accounts in the Services, authorization of access to the Services, verification of User's rights, data hosting, provision of support to the Customer, creation of accounts in tools used in provision of expert and support services; back-up, account and contract management, and other activities that may be necessary to provide Services in accordance with the Agreement.

Purpose(s) of the data transfer and further processing: Fulfilment of the Agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: term of the Agreement and up to 30 days after its termination or expiration.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: as specified in the Schedule 3.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13: supervisory authority applicable to the EU member state law indicated in Agreement.

SCHEDULE 2: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Technical and organizational security measures described herein define the controls implemented by Syncron for the development, acquisition, maintenance and operation of Syncron cloud solutions supplied in a Software-as-a-service model. This Schedule 2 also constitutes Annex II under Standard Contractual Clauses.

DATA SECURITY GUIDE
Technical and organizational security measures described herein define the controls implemented by Syncron for the development, acquisition, maintenance, and operation of Syncron cloud solutions supplied in a Software-as-a-Service model

1. SECURITY PROGRAM
Syncron will maintain a written information security program of policies, standard operating procedures, standards, guidelines, and controls governing the processing, storage, transmission, and security of Customer Data (the "Security Program"). The Security Program includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

Syncron has appointed a Chief Information Security Officer, accountable to a Security Steering Committee of executive representatives across the company, to develop, implement and manage Syncron's corporate security, vision, strategy, and programs and ensure security of information assets, maintain trust of Syncron customers and obtain third party assurance for the Service. The Chief Information Security Officer and the Security Steering Committee oversees the identification and development of policies and processes across the organization to reduce risks, respond to incidents and limit exposure to liability in areas of physical security, reputational damage, information security and information technology risk. The Chief Information Security Officer has been also appointed as the Data Protection Officer at Syncron.

Syncron regularly tests, assesses, and evaluates the effectiveness of the Security Program, and its constituent parts, and may periodically review and update the Security Program to address new and evolving security technologies and threats, and changes to industry standard practices, although no such update will materially reduce the commitments, protections or overall level of service provided to Customer as described herein.

2. PHYSICAL, TECHNICAL AND ADMINISTRATIVE SECURITY MEASURES

2.1 PHYSICAL SECURITY MEASURES.

2.1.1 DATA CENTER FACILITIES. (i) Physical access controls, logging, and monitoring that may include a combination of any of the following: multi-zone security, mantraps, CCTV, appropriate perimeter deterrents (e.g., signage, lighting, fencing, berms, guarded gates), on-site guards, multifactor access controls, including biometric access controls, and secure cages; and (ii) fire detection and suppression systems both localized and throughout the data center floor.

2.1.2 EQUIPMENT. (i) Physical protection mechanisms; and (ii) entry controls to limit physical access.

2.1.3 MEDIA. (i) Total use of encrypted storage, facilitating crypto-shredding; (ii) Cloud-Industry standard destruction of sensitive materials before disposition of media; (iii) secure safe for storing damaged hard disks prior to physical destruction; and (iv) physical destruction of all decommissioned hard disks storing Customer Data.

2.1.4 REMOVABLE MEDIA. The use of removable media for customer data is prohibited. The use of removable media for company data is permitted only when encrypted and written approval obtained from Syncron's Security team.

2.2 TECHNICAL SECURITY MEASURES.

2.2.1 ACCESS ADMINISTRATION. Access to all data, including customer data, by Syncron employees and contractors is protected by strong authentication, authorization, and audit mechanisms. User authentication is required to gain access to production and sub-production instances. Access privileges are based on job requirements, and access to customer data is granted on a per-customer, time-limited basis requiring multi-level approvals, and are revoked upon termination of employment or consulting relationships. Production infrastructure includes appropriate user account and password controls e.g.: long complex passwords, multi-factor authentication, multi-level approvals, and dated expiration and user access reviews. All user accounts are unique and uniquely linked to an individual. Shared accounts are not permitted.

2.2.2 SERVICE ACCESS CONTROL. The Syncron products provide user account management, role-based access control, and integration with enterprise identity and access management services (e.g.: SSO). Customers are responsible for configuring such access controls within their instance(s).

2.2.3 LOGGING AND MONITORING. Application logs are stored within the Customer's instance. Production platform logs are centrally collected and are secured in a dedicated AWS Account to prevent tampering and are monitored for anomalies by a trained security team and state-of-the-art analytic tooling.

2.2.4 NETWORK SECURITY. State of the art preventive network security devices are installed at multiple points within the separate Syncron corporate and customer network environments, acting in blocking mode with default traffic denial unless explicitly authorised.

2.2.5 VULNERABILITY MANAGEMENT. Syncron operates a vulnerability management program that regularly evaluates and internal and external systems, and infrastructure for known vulnerabilities and unmanaged configuration changes. Identified issues are remediated in accordance with remediation processes and a risk-based approach. Syncron products and the supporting infrastructure are penetration tested at least annually by an independent third party.

2.2.6 ANTIVIRUS. Syncron uses endpoint threat protection software and updates antivirus, anti-malware, and endpoint threat detection software at regular intervals, using central logging and management tools, and centrally logs events for investigation, which are stored immutably and secured using dedicated security and audit accounts.

2.2.7 CHANGE CONTROL. Syncron ensures that changes to applications and infrastructure are managed, evaluated with respect to risk, and conducted using standard operating procedures.

2.2.8 CONFIGURATION CONTROL. Syncron operates an entirely software-defined infrastructure. All infrastructure is engineered with secure defaults, and monitored for configuration integrity, and changes.

2.2.9 DATA SEPARATION. Customer Data is stored within separate dedicated databases and accessed via separate dedicated application servers on an underlying multi-tenant cloud infrastructure that is logically and physically separate from Syncron's corporate infrastructure. There are no automatic trusts between customer environments and corporate environments. Data from multiple customers is never stored on the same database and there is no commingling of customer data.

2.3 ADMINISTRATIVE SECURITY MEASURES.

2.3.1 DATA CENTER INSPECTIONS. Syncron routinely monitors supplier data centers to ensure that they continue to maintain effective security controls, compatible with the needs of our customers and our Security Program. This is achieved through a review of vendor-supplied 3rd party audit reports.

2.3.2 PERSONNEL SECURITY. Syncron performs personnel security screening on all employees and all contractors who have access to Customer Data in accordance with the then current applicable standard operating procedure, and subject to applicable laws.

2.3.3 SECURITY AWARENESS AND TRAINING. Syncron maintains a security awareness program that includes appropriate training of Syncron personnel on the Security Program and required behavior around common risks. Training is conducted at time of hire and periodically throughout employment or engagement by Syncron.

2.3.4 VENDOR RISK MANAGEMENT. Syncron maintains a vendor risk management program that assesses all vendors that may access, store, process or transmit Customer Data, for appropriate security controls

3. SERVICE CONTINUITY

3.1 DATA MANAGEMENT; DATA BACKUP. Syncron host Customers in multiple availability zones within their chosen datacenter region. All datacenters have attained SSAE 18 Type 2 attestations, ISO 27001 certifications, or equivalent. Each datacenter includes full redundancy (N+1) and fault tolerant infrastructure for electrical, cooling and network systems. Production database servers are replicated in near real time to multiple availability zones.

3.2 PERSONNEL. Syncron support, operations, and engineering teams are geographically distributed to ensure business continuity for support operations, and tools and services are architected similarly to the customer cloud product, operating across multiple availability zones.

3.3 CORPORATE IT. Syncron's own IT services are architecturally distinct from and separate to the Syncron Service, but managed within the same governance framework, and using the same architectural best practices, for the provision of a resilient corporate IT service.

4. CERTIFICATIONS AND AUDITS

4.1 CERTIFICATIONS AND ATTESTATIONS. Syncron operates an Information Security Management System with sufficient controls to meet the objectives stated in ISO 27001, and SSAE18 SOC 2 Type). At least once per calendar year, such as to provide an unbroken period of observation, Syncron shall obtain an assessment against these standards by an independent third-party auditor.

4.2 CUSTOMER MONITORING RIGHTS.

4.2.1 REMOTE SELF ASSESSMENTS. Syncron shall make available upon request documentation supporting Syncron's audit process.

4.2.2 AUDIT. No more than once per year and only upon written request by Customer, Customer shall have the right directly or through its representative(s) (provided however, that such representative(s) shall enter into written obligations of confidentiality and non-disclosure directly with Syncron), to access all reasonable and industry recognized documentation evidencing Syncron's policies and procedures governing the security of Customer Data ("Audit"). Syncron reserves the right to refuse to provide Customer (or its representatives) with any information which would pose a security risk to Syncron or its customers, or which Syncron is prohibited to provide or disclose under applicable law or contractual obligation.

4.2.3 OUTPUT. Upon completion of the Audit, Syncron and Customer may schedule a mutually convenient time to discuss the output of the Audit. Syncron may in its sole discretion, consistent with industry and Syncron's standards and practices, make commercially reasonable efforts to implement Customer's suggested improvements noted in the Audit to improve Syncron's Security Program. The Audit and the results derived therefrom are Confidential Information of Syncron.

4.2.4 CUSTOMER EXPENSES. Any expenses incurred by Customer in connection with the Audit shall be borne exclusively by Customer.

5. MONITORING AND INCIDENT MANAGEMENT

5.1 MONITORING, MANAGEMENT AND NOTIFICATION.

5.1.1 INCIDENT MONITORING AND MANAGEMENT. Syncron will monitor, analyze and respond to security incidents in accordance with Syncron's standard operating procedure for incident management. Syncron's Incident Response Team, and Syncron's security group will escalate and engage specialist response teams and authorities as may be necessary to address an incident.

5.1.2 BREACH NOTIFICATION. Syncron will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data (a "Breach") without undue delay following determination by Syncron that a Breach has occurred.

5.1.3 CUSTOMER OBLIGATIONS. Customer will cooperate with Syncron in maintaining accurate and usable contact information and by making available any reasonably requested information, with respect to any security incident in order to identify its root cause(s) and prevent a recurrence. Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.

5.2 COOKIES. Syncron uses cookies to operate the Service including for the purposes of: (i) tracking session state; (ii) routing browser requests via load balancers; and (iii) identifying users. Customer shall be responsible for providing notice to, and collecting any necessary consents from, its authorized users of Services for Syncron's use of cookies.

6. PENETRATION TESTS

6.1 BY A THIRD-PARTY. Syncron contracts with third-party vendors to perform a penetration test on the Syncron applications to identify risks and remediation opportunities to improve security.

6.2 BY CUSTOMER. No more than once per calendar year Customer may request to perform, at its own expense, an application penetration test of a sub-production instance of their Syncron product(s). Customer shall notify Syncron in advance of any test by submitting a request to schedule an application penetration test via their account team. Syncron and Customer must agree on a mutually acceptable time, duration, method, and scope, for the test. All results of testing must remain confidential to Customer, Syncron, and to the agreed third-party testers, and shall be shared with Syncron in full without undue delay. Customer shall not perform a penetration test without Syncron's express written authorization. Tests must be conducted in accordance only with the agreed as part of the conditional approval to test.

7. DATA SECURITY

7.1 TEST DATA. Production data will remain at all times exclusively within the production environments. Customers may request all or a subset of their data be transferred into a test environment, which will be granted only with the appropriate permissions and controls in place.

7.2 CONFIDENTIALITY, ENCRYPTION. All data, including test environments and backups are encrypted at rest and in motion using state-of-the-art encryption, including TLS1.3, and AES-256 encryption

7.3 TRANSFERS. Data remains within its specified environment and region at all times unless expressly requested and authorized by the Customer. Where approved sub-processors are used over and above the use of AWS as the underlying cloud provider, the data still remains within the specified AWS customer data environment is not physically or logically transferred in any way.

7.4 INTEGRITY. All accesses and data activities are logged, and alerts are generated and investigated for anomalous behavior. Syncron undertakes frequent database backups using snapshot technology and is able to rollback to previous states if requested by the customer.

7.5 USE, RETENTION, MINIMIZATION. Data is selected, entered by the Customer and stored and processed by Syncron entirely within the customer data environment, and used solely for the purpose as specified by the Customer. Data is retained for the duration of the contract with the customer and for a period of approximately 30 days after the contract end, during which time the data may be requested by the customer in a common readable format, and after which the data shall be deleted and rendered unrecoverable through the use of crypto-shredding and the removal of the underlying cloud-resources.

<u>SCHEDULE 3 - LIST OF SUB-PROCESSORS AUTHORIZED TO PROCESS PERSONAL DATA OF SYNCRON CUSTOMER</u>

Sub-processors engaged and authorized to process personal data of Customer in the course of provision of the Services by Syncron (Provision of Services may include support, development, expert services, software maintenance, etc.). Sub-processors in bold are specifically used for the provision of Syncron Services and processing of Customer Data (which cover not only personal data of end users, but also all business data). This Schedule 3 also constitutes Annex III under Standard Contractual Clauses.

Subject matter of processing is addressed in column 4 of the table below.

Nature of the processing: data will be processed automatically.

Duration of processing: term of the Agreement and up to 30 days after its termination or expiration.

Name	Address	Purpose of use/Services provided by Subprocessor	Categories of personal data processed by Subprocessor
Third Party Sub-processors (as applicable)			
Amazon Web Services Inc.	**410 Terry Avenue North, Seattle, WA 98109-5210, USA**	**Provision of cloud infrastructure**	**All personal data listed in sec. 3.1. of the DPA:**
Microsoft Corp.	One Microsoft Way Redmond, WA 98052-7329, USA	Provision of support, direct contact with end users, administration/management of customer account (Office 365 tools)	User account information (including name, surname, e-mail, phone number)
Freshworks Inc. (formerly: Natero Inc.)	2950 S.Delaware Street, Suite 201, San Mateo, CA 94403, USA	Customer success/account management during and after Implementation, handling customers' requests	User account information (including e-mail, first and last name, user ID) Customer Data: error-related including name of item, name of warehouse
OpsGenie Inc. (Atlassian affiliate)	450 W Broad St. Suite 421, Falls Church, VA 22046, USA	Error reporting, provision of support	User account information (including user e-mail); Customer Data: error-related including name of item, name of warehouse
T3CH.com LLC (dba Status.io)	19 N. County Line Road Jackson, NJ 08527, USA	Notification about planned maintenance and outages for Services (Optional)	User account information (including user e-mail, first and last name, mobile number) Please note that this is an option opt-in service.
Zoom Video Communications, Inc.	55 Almaden Blvd, 6thFloor San Jose, CA, USA	Conducting online trainings and meetings (teleconferences)	User account information (including name, e-mail)
EPAM Systems (Nordics) AB	Kungsgatan 50, 7 Tr 111 35, Stockholm, Sweden	Support, development, and maintenance of Syncron's SaaS services.	All personal data listed in sec. 3.1. of the DPA

SucceedIT B.V. *Syncron Partner*	Ariane 20 (Kantoor 11) 3824 MB Amersfoort, Netherlands	Provision of support and implementation services, administration/ management of customer account (if applicable for a given Customer)	All personal data listed in sec. 3.1. of the DPA
Exsitec AB *Syncron Partner*	Snickaregatan 40, SE-582 26 Linköpin, Sweden	Provision of support and implementation services, upgrades, administration/ management of customer account (if applicable for a given Customer)	All personal data listed in sec. 3.1. of the DPA
Orango AB *Syncron Partner*	Stortorget 9, 211 22 Malmö, Sweden	Provision of support and implementation services, upgrades, administration/ management of customer account (if applicable for a given Customer)	All personal data listed in sec. 3.1. of the DPA
CBIZ MHM, LLC *Syncron Partner*	225 West Wacker Drive, Suite 2500. Chicago, IL 60606	Provision of support and implementation services, upgrades, administration/ management of customer account (if applicable for a given Customer)	All personal data listed in sec. 3.1. of the DPA
Mkenga Group Limited *Syncron Partner*	main place of business: NSSF Kilimanjaro Commercial Center, Aga Khan Road, Office #20, Moshi, United Republic of Tanzania	Provision of support and implementation services, upgrades, administration/ management of customer account (if applicable for a given Customer)	All personal data listed in sec. 3.1. of the DPA
Ekonomi och Affärssystem Norden AB Syncron Partner	FÄRÖGATAN 33 Kista Science Tower, 164 51 Kista, Sweden	Provision of support and implementation services, upgrades, administration/ management of customer account (if applicable for a given Customer)	All personal data listed in sec. 3.1. of the DPA
Zedcom AB Syncron Partner	Öneslingan 11, 832 51 Frösön, Jämtland, Sweden	Provision of support and implementation services, upgrades, administration/ management of customer account (if applicable for a given Customer)	All personal data listed in sec. 3.1. of the DPA
ProviDo e.U. (promoting its services under the business name "Systempilot") Syncron Partner	Talgasse 4/26, 1150 Vienna, Austria	Provision of support and implementation services, upgrades, administration/ management of customer account (if applicable for a given Customer)	All personal data listed in sec. 3.1. of the DPA

Porl AB Syncron Partner	Kanalgatan 77, 931 34 Skellefteå, Sweden	Provision of support and implementation services, upgrades, administration/ management of customer account (if applicable for a given Customer)	All personal data listed in sec. 3.1. of the DPA
Mize's Third Party Subprocessors			
Amazon Web Services	Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, WA 98109-5210	Mize SaaS application used AWS for cloud services https://aws.amazon.com/compliance/gdpr-center/	All personal data listed in sec. 3.1. of the DPA.
Elastic	Mountain View, CA 800 West El Camino Real Suite 350 Mountain View, California 94040	For Log Aggregation and percolation https://www.elastic.co/	All personal data listed in sec. 3.1. of the DPA.
Google Cloud (Maps)	1600 Amphitheatre Parkway in Mountain View, California, United States.	For Location tracing https://www.google.co.in/maps	Location data, address info like street, city, country, zip to get the location coordinates and also for calculating distance between two locations.
Urbanairship	205 E 42nd Street New YorkNY10017	For Push notifications https://www.airship.com/	Device specific information, (device ID / device key).
Affiliates			
Syncron Germany GmbH	Mies-van-der-Rohe-Straße 4, 80807 München, Germany	Provision of Services; Customer care (account management)	All personal data listed in sec. 3.1. of the DPA.
Syncron Inc.	HQ: One Glenlake Pkwy Suite 1000, Atlanta, GA 30328, USA	Provision of Services, Customer care (account management)	All personal data listed in sec. 3.1. of the DPA.
Syncron UK Ltd	Office: 2nd Floor, 3 Brindleyplace, Birmingham, B1 2JB, UK; Registered address: C/O Begbies 9 Bonhill Street London EC2A 4DJ, UK	Provision of Services, Customer care (account management)	All personal data listed in sec. 3.1. of the DPA.
Syncron AB	Östra Järnvägsgatan 27 111 20 Stockholm, Sweden	Provision of Services, Customer care (account management)	All personal data listed in sec. 3.1. of the DPA.
Syncron Poland sp. z o.o.	ul. Twarda 4 00-105 Warszawa, Poland	Provision of Services, Customer care (account management)	All personal data listed in sec. 3.1. of the DPA.
Syncron Japan Corp.	NCO Kanda Awajicho Building 7F, 2-1-7 Kanda Awajicho, Chiyoda-ku, Tokyo 101-0063 Japan	Provision of Services, Customer care (account management)	All personal data listed in sec. 3.1. of the DPA.
Syncron Software India Private Limited	Municipal No. 206, Mahatma Gandhi Rd, Bengaluru, Karnataka 560001, India	Provision of Services, Customer care (account management)	All personal data listed in sec. 3.1. of the DPA.
Syncron Italy S.r.l.	Via Maurizio Gonzaga 7 CAP 20123, Milano (MI), Italy	Provision of Services, Customer care (account management)	All personal data listed in sec. 3.1. of the DPA.
Syncron France SAS	5 rue du Helder 75009 Paris, France	Provision of Services, Customer care (account management)	All personal data listed in sec. 3.1. of the DPA.
Syncron Services Poland sp. z o.o.	ul. Twarda 4, 00-105 Warszawa, Poland	Provision of Services, Customer care (account management)	All personal data listed in sec. 3.1. of the DPA.

| Mize, Inc. | 12802 Tampa Oaks Blvd Ste 320, Temple Terrace, FL, 33637-1954 United States | Provision of Services, Customer care (account management) | All personal data listed in sec. 3.1. of the DPA. |
| Mize Software Solutions Private Limited | Mjr Magnific, Unit No# 3,Ground Floor Survey 75&76 Nanakramguda X Roads, Raidurga Navkhalsa Hyderabad, Telangana, 500008 India | Provision of Services, Customer care (account management) | All personal data listed in sec. 3.1. of the DPA. |

Change control log

28.11.2019	PM: Updating incomplete information in the Appendix 2 (sec. IV/5; sec. II/1)
22.04.2020	PM: CCPA-related updates in the DPA (sec. 1 and sec. 2 of the DPA); cosmetic changes in sec. 6 (adding reference to Schedule 3), sec. 6 and sec. 7: adding links to the contact form
15.05.2020	PM: Updating the office address of Syncron Services India Private Limited
23.07.2020	PM: Updating the list of subprocessors following the acquisition of Natero by Freshworks, updating legal name of Syncron India
26.08.2020	PM: Updates following Schrems II ruling (updates in sec. 7.2.3, removal of previous sec. 7.3), clarification in sec. 4 (global scope) and sec. 10 (exceptions set out in local laws), addition of new sec. 13.3 regarding communication of amendments to DPA, updating the list of subprocessors (new: Syncron France, additional details: Opsgenie)
22.10.2020	PM: Updating section 13.2 to keep it consistent with the MSA
21.09.2020	PM: Updating subprocessors list (adding Polr AB)
20.09.2021	MZ: Updates following merger with Mize and extending territorial applicability, updating the list of subprocessors (Mize, Inc., Mize Software Solutions Private Limited, Syncron Services Poland sp. z o.o., EPAM Systems (Nordics) AB), updates following adoption of new Standard Contractual Clauses (SCC) by the Commission (EU); harmonization of the wording with Mize DPA; confirming global applicability of the DPA by replacing exclusive references to GDPR with references to applicable data protection laws and regulations, updates of security appendix.