



## DATA PROCESSING ADDENDUM

### HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1 (with Appendix 1), Schedule 2 and Schedule 3.
2. This DPA has been pre-signed on behalf of Synchron. The Standard Contractual Clauses in Schedule 1 have been pre-signed by Synchron 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 as the data exporter on Page 9.
  - (iii) Complete the information in the signature box and sign on Pages 14, 15.
  - (iv) Send the completed and signed DPA to Synchron by email, indicating the full legal entity name (as set out on the applicable underlying Master Subscription Agreement/Order Form), to [privacy@synchron.com](mailto:privacy@synchron.com).

### WHEREAS

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

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

This DPA is hereby incorporated to the Master Subscription Agreement and constitutes its integral part.

In relation to signing of the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Synchron processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates.

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, Synchron 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 contracting party's (i.e., either Synchron or Customer) affiliated company that is: (a) controlled, directly or indirectly, by contracting party; (b) controls, directly or indirectly, the contracting party; or (c) is under common control with the contracting party, 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 Synchron, but has not signed its own Agreement or purchase order with Synchron and is not a "Customer" as defined under the Agreement, and (b) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states and/or the United Kingdom.

**"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 the Directive, as transposed into domestic legislation of each member state of the European Union and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR and, to the extent applicable, the data protection or privacy laws of any other country including laws and regulations of the European Economic Area and their member states and the United Kingdom, applicable to the Processing of Personal Data under the Agreement.

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

**“Directive”** means Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, as amended, on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such data.

**“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 ([processors](#)) annexed to EU Commission Decision 2010/87/EU of February 5, 2010 for the transfer of personal data to processors established in third countries under the Directive; 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 EU Directive 95/46/EC or 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 Synchron, 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.

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

**“Third-Party Sub-processor”** means a third-party subcontractor, other than a Synchron Affiliate, engaged by Synchron 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.



## **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 Synchron. 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 Synchron (including 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. Customer may provide instructions in writing to Synchron with regard to Processing of Personal Data. Synchron will comply with all such instructions without additional charge to the extent necessary for Synchron to comply with its obligations as a Processor in the performance of the Services. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer, on behalf of itself and of any Authorized Affiliate, instructs Synchron (and authorizes Synchron 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 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. 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 Data Protection Laws and Regulations.
- 2.2 For the purposes of provision of the Services set forth in the Agreement, Synchron is a Processor, and Synchron or Synchron Affiliates may engage Third-Party Sub-processors in accordance with this DPA. Synchron will Process Personal Data as necessary for the provision of the Services set forth in the Agreement, and will not otherwise (i) Process or use Personal Data for purposes other than those set forth in the Agreement or as instructed by Customer in good faith, or (ii) disclose such Personal Data to third parties other than Synchron Affiliates or Third- Party Sub-processors for the aforementioned purposes or as required as required by Data Protection Laws and Regulations.
- 2.3 Synchron 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 Synchron'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.
- 2.4 Synchron will comply with applicable Data Protection Laws and Regulations to the extent that such laws by their terms impose obligations directly upon Synchron as a Processor in connection with the Services provided to the Customer.
- 2.5 Synchron Processes Personal Data in accordance with the GDPR requirements directly applicable to Synchron's provision of its Services. Upon Customer's request, Synchron shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligations and tasks under the GDPR 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 Synchron.
- 2.6 The parties acknowledge and agree that, by executing the Agreement, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Synchron 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 Synchron 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).

- 3.2 Synchron will Process Personal Data for the duration of the Agreement, unless otherwise agreed between the Parties.

### 4. RIGHTS OF DATASUBJECTS

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 and automated individual decision-making). The Controller is obliged to facilitate the exercise of these data subject rights under articles 15 to 22 of the GDPR. 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 laid down in Chapter III of the GDPR. In consequence, Synchron shall, to the extent legally permitted, notify Customer if Synchron 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, Synchron 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. Synchron shall not respond to such request except on the documented instructions of the Customer or as required by Data Protection Laws and Regulations (Synchron 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 Synchron 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. Synchron shall ensure that such confidentiality obligations survive the termination of the personnel engagement.
- 5.2 Synchron shall take commercially reasonable steps to ensure the reliability of any Synchron personnel engaged in the Processing of Personal Data.
- 5.3 Synchron shall ensure that Synchron's access to Personal Data is limited to those personnel performing services in accordance with the Agreement.
- 5.4 Synchron and its Affiliates have appointed a data protection officer. The appointed person may be reached at [privacy@synchron.com](mailto:privacy@synchron.com).

### 6. SYNCRON AFFILIATES AND THIRD-PARTY SUB-PROCESSORS

- 6.1 Some or all of Synchron's obligations under the Agreement may be performed by Synchron's Affiliates and Third- Party Sub-processors. Synchron maintains a list of Synchron's Affiliates and Third-Party Sub-processors that may Process Personal Data, which is part of Synchron 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 underlying master subscription agreement.
- 6.2 Customer acknowledges and authorizes Synchron to (a) retain Synchron's Affiliates as sub-processors; and to (b) appoint (and permit each Synchron 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 Synchron Affiliates and Third-Party Sub-processors are required to abide by substantially the same obligations as Synchron under this DPA as applicable to their Processing of Personal Data. Synchron or a Synchron Affiliate should 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 to the extent applicable to the nature of the Services provided by such Third-Party Sub-processor.
- 6.4 Synchron 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@synchron.com](mailto:privacy@synchron.com). Customer may object to Synchron's use of a given Third-Party Sub-processor by sending the objection in writing within 14 days' from receiving the notification from Synchron. Objection shall be provided to Synchron to [privacy@synchron.com](mailto:privacy@synchron.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. Synchron 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 Synchron remains responsible at all times for compliance with the terms of this DPA by Synchron's Affiliates and Third-Party Sub-processors to the same extent Synchron 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 Synchron treats all Personal Data in a manner consistent with the requirements of the Agreement and this DPA in all locations globally. Synchron'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 Synchron'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 Synchron and/or Synchron Affiliates is made subject to this DPA and (i) Standard Contractual Clauses with Customer acting as the "data exporter" and Synchron and/or Synchron Affiliate(s) acting as the "data importers", incorporated here by reference; or (ii) other appropriate transfer mechanisms that provide an adequate level of protection in compliance with the GDPR, 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 Synchron to Synchron Affiliates located in third countries, Synchron represents that such transfers are subject to (i) the terms of Synchron Intracompany Data Processing Agreement (with Intracompany Confidentiality Undertaking) entered into between Synchron AB and its Affiliates, which requires all transfers of Personal Data to be made in compliance with Standard Contractual Clauses and all applicable Synchron security and data privacy policies and standards (without prejudice to sec. 7.3 below in relation to Synchron Inc.), or (ii) other appropriate transfer mechanisms that provide an adequate level of protection in compliance with the GDPR.
  - 7.2.3 For transfer from Synchron and/or Synchron Affiliates to Third-Party Sub-processors, in addition to the agreement referred to in sec. 6.3 above, Synchron or Synchron Affiliate has entered or will enter into the unchanged version of the Standard Contractual Clauses 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 Synchron and the Third-Party Sub-processors located outside of the EEA or Switzerland.
- 7.3 Synchron is committed to Process Personal Data in accordance with the GDPR requirements for international data transfers.

## 8. SECURITY

Synchron 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 2 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 (as defined in GDPR) 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 (a) return a complete copy of all Customer Personal Data to Customer; and (b) delete and procure the deletion of all other copies of Personal Data Processed by Syncron, any Syncron Affiliate or any Third-Party Sub-processor. Syncron and each Syncron Affiliate shall comply with any such written request within 60 days of the Cessation Date.
- 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, Synchron and each Synchron 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 in relation to the Processing of the Personal Data by Synchron, any Synchron 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 Synchron or the relevant Synchron Affiliate a reasonable notice (at least 30 days) of any audit or inspection to be conducted under section 12.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing any damage, injury or disruption to Synchron, any Synchron Affiliate or any Third-Party Sub-processor' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. Synchron, any Synchron 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 Synchron, any Synchron 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 Synchron's or the relevant Synchron 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.

**13. GENERAL TERMS, GOVERNING LAW AND DISPUTE RESOLUTION**

- 13.1 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 Appendices.
- 13.2 This DPA shall come into effect upon its signing by both Parties. Without prejudice to Section 11, this DPA shall automatically expire upon any termination or expiration of the Agreement.
- 13.3 Synchron 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. Synchron will notify the Customer about any such amendments by sending a notification to Customer's primary contact or, on Customer request, to a dedicated e-mail address submitted to [privacy@synchron.com](mailto:privacy@synchron.com). Customer may object to a given amendment by sending the objection in writing within 14 days' from receiving the notification from Synchron. Objection shall be provided to Synchron to [privacy@synchron.com](mailto:privacy@synchron.com) and shall include reasonable grounds for objection. The parties will come together in good faith to discuss a resolution.
- 13.4 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.

\_\_\_\_\_

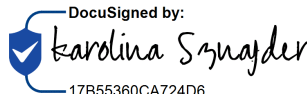
This DPA has been executed in two originals of which the parties have taken one each.

Date: \_\_\_\_\_

Date: 26 August 2020

On behalf of CUSTOMER (Controller)

On behalf of SYNCRON (Processor)

DocuSigned by:  
  
17B55360CA724D6...

Karolina Sznajder  
Global Legal Counsel



**List of Schedules**

Schedule 1: Standard Contractual Clauses with Appendix 1

Schedule 2: Technical and organizational security measures

Schedule 3: List of sub-processors



## **SCHEDULE 1**

---

### **Standard Contractual Clauses and Description of Data Processing**

#### **EU STANDARD CONTRACTUAL CLAUSES (Processors)**

*[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 of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the Data Protection Laws 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 Data Protection Law (otherwise).]*

#### **Standard Contractual Clauses (processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization:

Customer name and contact details:

---

(the data **exporter**)

And

Syncron AB and its affiliates

Address: Östra Järnvägsgatan 27, SE-111 20 Stockholm

e-mail: [privacy@syncron.com](mailto:privacy@syncron.com)

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

#### **Background**

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer which are subject to the DPA (*the services*) will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

#### *Clause 1*

#### **Definitions**

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; [*If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words "except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the*

*definition of "personal data" is expanded to include those data" are added.]*

- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

## *Clause 2*

### **Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

## *Clause 3*

### **Third-party beneficiary clause**

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

## *Clause 4*

### **Obligations of the data exporter**

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix (Schedule) 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix (Schedule) 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

#### *Clause 5*

#### ***Obligations of the data importer***

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix (Schedule) 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
  - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  - (ii) any accidental or unauthorised access, and
  - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix (Schedule) 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

*Clause 6*

***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

*Clause 7*

***Mediation and jurisdiction***

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
  - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

*Clause 8*

***Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

*Clause 9*

**Governing Law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

*Clause 10*

**Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

*Clause 11*

**Subprocessing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

*Clause 12*

**Obligation after the termination of personal data processing services**

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

\*\*\*

**On behalf of the data exporter:**

*[Populated with details of, and deemed signed on behalf of, the data exporter:]*

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

**On behalf of the data importer:**


*[Populated with details of, and deemed signed on behalf of, the data exporter:]*

Name (written out in full): Karolina Sznajder

Position: Global Legal Counsel

Address: ul. Twarda 4, 00-105 Warszawa, Poland

Signature.....

Signature.  17B55360CA724D6... ..

**APPENDIX 1 TO THE DPA AND STANDARD CONTRACTUAL CLAUSES**

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

**Data exporter**

The data exporter is the Customer referred in the Agreement and its Authorized Affiliates (if applicable) who subscribed to the Services delivered by Synchron.

**Data importer**

The data importer is: Synchron Affiliate(s) located in a third country, as applicable. Synchron Affiliates may take part in provision of Services, which may include support, development, expert services and software maintenance. Synchron 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.

**Data subjects**

The personal data transferred concern the following categories of data subjects:

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, suppliers and other users of Customer (as applicable), who have access to Services and who may store user account information in the Services.

**Categories of data**

The personal data transferred concern the following categories of data:

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).

**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data:

The special categories of personal data, if any, are determined by the data exporter. Special categories of personal data are not requested by Synchron and are not necessary for provision of Services.

**Processing operations**

The personal data transferred will be subject to the following basic processing activities:

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, and other activities that may be necessary to provide Services in accordance with the Agreement.

On behalf of CUSTOMER (DATA EXPORTER)

Name:.....

Authorised Signature .....

On behalf of SYNCRON (DATA IMPORTER)

Name: Karolina Sznajder

Authorised Signature ..  17B55360CA724D6...

## **SCHEDULE 2: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES**

Technical and organizational security measures described herein define the controls implemented by Synchron for the development, acquisition, maintenance and operation of Synchron cloud solutions supplied in a Software-as-a-service model.

### I. Internal Organization

1. All Synchron employees have an inherent responsibility to protect the company's information assets, confidential data, intellectual capital owned by the company, and any data created within Synchron cloud services by its customers.

To coordinate Information Security at Synchron and to ensure co-operation between different business units, a Security Steering Committee is organized with representatives across the organization. Security Steering Committee's role is to help facilitate integration of information security into the lines of business as information security is an issue for Synchron that reaches across boundaries and departments. The Security Steering Committee is the governing body for all information security and assurance activities in the company.

2. Synchron has appointed the Chief Security Officer to develop, implement and manage Synchron's corporate security vision, strategy and programs and ensure security of information assets, maintain trust of Synchron customers and obtain third party assurance for the Synchron cloud services. The Chief Security Officer is in charge of identifying and developing 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 Security Officer has been also appointed as the Data Protection Officer at Synchron.
3. Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the Synchron assets. No single person should be able to access, modify or use Synchron information assets without authorization or detection.

Synchron security function maintains organizational independence from the operational teams that implement security policies.

4. The Chief Security Officer maintains contact with appropriate authorities (including but not limited to the law enforcement authorities, incident response centers and information commissioners) to report identified security incidents (if it is suspected that laws may have been broken) in a timely manner.
5. To improve knowledge about best practices and staying up to date with relevant security information, the company Chief Security Officer maintains contacts with specialist security forums and cloud computing security associations.
6. Chief Security Officer is involved in project management to define security objectives and conduct security risk assessment regardless the type of the project.
7. When hiring external consultants for temporary assignments and projects, information security aspects are considered, and non-disclosure agreements are executed (or confidentiality clauses are included in agreements) between such parties and Synchron prior to granting external parties access to the company information and information processing facilities or sharing sensitive data.

### II. Mobile Devices and Teleworking

1. When using mobile devices, Synchron employees take special care to ensure that customer data or sensitive corporate information is not compromised. The risks of working with mobile devices in unprotected environments are addressed by the measures in the Acceptable Use Terms which is acknowledged by all employees.
2. Teleworking activities are allowed at Synchron per the guidelines and protective measures defined in the Acceptable Use Terms. All users must show great care to protect customer data and Synchron corporate information accessed, processed or stored at teleworking sites.

### III. Human Resources Security

1. All candidates for employment, contractors, and third-party users of Synchron information assets require the successful completion of a background check prior to beginning work at Synchron. Background checks are performed in accordance with the Human Resources Security Procedure and do not violate the relevant jurisdiction or an individual's privacy.



2. All Synchron employees (and contractors) are responsible for protecting Synchron information assets per confidentiality clauses stated in the Employment Agreement.
3. All Synchron employees, contractors and third-party users must be properly briefed on their information security responsibilities prior to being granted access to sensitive information or systems.
4. All Synchron employees and where relevant, contractors and third-party users should attend training to receive information security awareness education per the Synchron Security Awareness Program.
5. Employees, contractors and third-party users who have committed a serious information security breach and failed to comply with this policy through malicious or negligent behavior may be subject to a disciplinary process including the termination of employment / contract.
6. All People Managers (anyone who has at least one person reporting to them) within Synchron are responsible of following the Change of Employment Procedures and associated onboarding and off-boarding processes to ensure that employees, contractors and third-party users exit the organization or change employment in an orderly and timely manner.
7. People Managers must ensure that all employees, contractors and third-party users return all of the organization's assets in their possession upon termination of their employment, contract or agreement.
8. People Managers must inform the Internal IT team to ensure that the access rights of all employees, contractors and third- party users to Synchron information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

#### IV. Asset Management

1. All information assets used for processing, transmitting and storing data relating to our customers and the operation of Synchron product and services are inventoried and controlled per the Asset Management Standard Operating Procedures.
2. All major information assets are accounted for and have a nominated owner to ensure that appropriate protection is maintained.
3. Rules for the acceptable use of information and assets associated with Synchron information processing facilities are defined in the Acceptable Use Terms. All employees, contractors and third-party users should acknowledge these rules prior to the start of employment or contract.
4. All information created and processed by Synchron employees should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.
5. Synchron does not require labeling of all information assets for data classification; however,
  - All customer data is classified as "confidential" by default and is protected accordingly with encryption and access control.
  - All corporate and development data is classified "internal" by default and is restricted accordingly to authorized personnel only.
  - Employees who have been authorized to view information at a particular classification level will only be permitted to access information at that level or at a lower level.
6. No "confidential" data is stored on removable media unless explicitly authorized by the Chief Security Officer. Data on removable media is always be encrypted.
7. When no longer required, storage media containing Synchron data should be disposed of or deleted securely to prevent recovery where the containing media will be re-used.
8. If physical media containing Synchron corporate or customer data to be transferred, appropriate protection measures including encryption and recorded delivery via authorized courier service is employed.

#### V. Access Control

1. Role based access control mechanisms are implemented at all Synchron information processing facilities (all systems and facilities that store, process and transmit company data); employees are only granted access to information and facilities on a need to know and need to use basis per their job requirements.

To prevent unauthorized access to Synchron information systems, each user's access privileges are authorized following a formal access request, according to business need.

The use of non-authenticated (i.e., no password) User-IDs or IDs not associated with a user is prohibited. Shared or group user IDs are never permitted for user-level access.

Every user must have a unique user ID and a personal secret password for access to Synchron computers and computer networks and third-party systems storing corporate data (i.e. cloud applications). Systems and applications must authenticate using a password or token entry.

2. Synchron employees and contractors are only provided with access to the network and network services that they have been specifically authorized to use. No default access is granted.
3. Synchron user registration and deregistration process (new hire and employee termination tickets) is used to enable assignment and removal of access rights.
4. Synchron user access provisioning process and associated forms is followed to assign or revoke access rights for all user types to all systems and services, including cloud services and applications.
5. Privileged access rights (such as administrator accounts) to business-critical applications and customer production environments are allocated upon approval by the Chief Security Officer, the Chief Technology Officer or the approved delegator.
6. All Synchron employees should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment. These responsibilities are documented in the Acceptable Use Terms which must be read and acknowledged by all users prior to being granted access to Synchron systems.
7. Synchron information asset owners shall review users' access rights to Synchron systems at six-month intervals.
8. The access rights of all employees and external party users to information and information processing facilities are removed immediately upon termination of their employment, contract or agreement, or adjusted upon change.
9. All users follow the Synchron password protection practices to keep their passwords and other authentication information confidential and avoid keeping a record unless it can be stored securely using a password vault software approved by the Chief Technology Officer.
10. Access to Synchron systems and applications is controlled by a secure log-on procedure which involves two-step verification (2 factor authentication) for remote access by administrators.  
Remote access to Synchron corporate networks is granted with a legitimate business need and approval from the Chief Technology Officer. Remote access users are reviewed annually by the Chief Security Officer or duly appointed IT staff.
11. All critical Synchron systems are protected with interactive password management systems (Active Directory) and enforce the use of quality passwords.
12. The use of utility programs that can override Synchron system and application controls is restricted to system administrators who are explicitly authorized by the Head of Operations.
13. Access rights to read, write and modify Synchron generic products source code is restricted to Products department members and other employees who are explicitly authorized by the Head of Research & Development. All Customer Success and EazyStock employees are by default granted read-only access to Synchron generic products source code unless decided otherwise by the Head of Customer Success.

## VI. Cryptography

1. All confidential Synchron corporate information, customer data and user credentials shall always be encrypted when transferred over public, open networks (such as the Internet or wireless LANs) or physically moved by mobile or removable media devices.

If deemed to be at risk, cryptography is used to protect 'confidential' classified Synchron corporate information, customer data and user credentials stored in Synchron systems.

2. The Synchron Head of Operations is responsible for ensuring the secure key management; including the generation, protection and revocation of encryption keys and certificates.

All encryption keys are assigned to key holders authorized by the Chief Technology Officer who is responsible to ensure that the use, protection and lifetime of cryptographic keys managed in accordance with industry best practices. Synchron encryption requirements are reviewed annually and upgraded according to current industry best practices by reviewing industry best practices (such as the guidelines from the National Institute of Standards and Technology).

VII. Physical and Environmental Security

1. Perimeters of a building or site containing Synchron information processing facilities are physically sound to prevent break-ins. Physical security measures implemented to protect Synchron offices and data centers follow the Synchron Physical and Environmental Security Standard Operating Procedures.
2. Secure areas used for storing or processing Synchron information assets are protected by appropriate entry controls to ensure that only personnel explicitly authorized by the Head of Operations are allowed access. Access to secure areas is reviewed annually by the Chief Security Officer or duly appointed IT staff.
3. Measures are designed and applied to Synchron offices to ensure physical security and safety of Synchron personnel. Access to Synchron offices are performed via access controlled gates or manned reception areas.  
All visitors to Synchron offices must be reported to the Reception and recorded in the visitor log.
4. If critical information is stored or processed in Synchron owned facilities, physical protection against natural disasters, malicious attack or accidents is designed and applied based on specialist advice obtained on how to avoid damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster.
5. Where third party co-location facilities or Infrastructure-as-a-Service models are used, appropriate certifications and industry accreditations (such as ISO27001, ISO20000 or SAS70) is sought.
6. All Synchron employees must take caution to prevent unauthorized physical access, loss, damage, theft, interference and interruption to Synchron premises and information assets. Contractors or third parties shall always be supervised by personnel when working in secure areas.  
Synchron office alarm codes and associated documentation are confidential and are treated appropriately to prevent unauthorized disclosure.
7. Synchron equipment used for processing, transmitting and storing confidential or operationally critical data is protected from environmental hazards and power failures in accordance with the Synchron Equipment Protection Standard.
8. Except normal usage of end user systems by company employees in accordance with the Acceptable Use Terms, Synchron equipment (except personal computing devices), information or software shall not be taken off-site without prior authorization by the Chief Technology Officer.
9. Synchron employees shall apply physical security measures and consider different risks to protect their devices when working outside the organization's premises. Employee laptops shall not be left unattended or unlocked in publicly accessible places.
10. All printed and electronic media containing confidential Synchron media is disposed of securely using confidential waste bins or secure data disposal methods.
11. Confidential papers and removable storage media shall never be left unattended or unlocked on employee desks.

VIII. Operations Security

1. To ensure the correct and secure operation of Synchron information processing facilities, standard operating procedures are documented and approved by the Head of Operations and made available to all users who need them.
2. All changes to Synchron critical information processing facilities and systems must follow the Synchron Change Management, Deployment and Upgrades Standard Operating Procedures to enable tracking, testing and approval. Changes to the Synchron organization, business processes, information processing facilities and systems that affect information security are documented and approved by the Head of Operations or delegated authority.  
The responsible party that will be implementing the change must complete and submit a new item to the Synchron change management system (Jira).  
Major changes are required to be submitted for review by the Chief Technology Officer. Changes that may have an impact on the availability of Synchron products and services are applied during a pre-defined maintenance window.  
After implementation, testing is conducted to determine if a given change was successful, or if rolling implemented changes back is necessary. Change implementers shall notify all parties identified as needing communication of both start and finish times of a change.
3. The Chief Technology Officer shall monitor and tune the use of Synchron information resources and the capacity of Synchron cloud services.

4. Future capacity requirements are projected and planned for by the Chief Technology Officer to ensure the required system performance.
5. Syncron development, test, and production facilities are separated to reduce the risks of unauthorized access or changes to the production systems. The Chief Technology Officer has the ultimate responsibility to maintain separation of these environments while Head of Operations, Head of Customer Success and Head of Research and Development must ensure no customer or confidential data is used in the respective test and development environments utilized by their departments (unless explicitly requested and approved by the customer).
6. Anti-malware solutions are deployed on all Syncron systems commonly affected by malicious software (particularly personal computers and servers). Anti-malware is configured to update virus definitions regularly and scan for malware in real-time.
7. Backup copies of critical Syncron information, software and customer data are taken daily and tested every six months as part of the Business Continuity Plan testing.
8. All customer data held on Syncron cloud products is backed up, encrypted and stored off-site utilizing an appropriate disk- based, online backup and recovery solution.

Under no circumstances shall Syncron customer data be stored on removable physical media, mobile devices or non- corporate personal computers.

9. All event logs recording user activities, exceptions, faults and information security events from critical Syncron infrastructure and applications are produced and the audit trail is retained for at least one year.
10. Logging configuration is only be accessible by the authorized system administrators and log information is protected against tampering and unauthorized access.

Where possible, logs from critical systems are correlated for analysis and review.

11. All administrative access and activities on Syncron systems and products is logged and the audit trail is protected and made available for review.
12. Clocks of all relevant Syncron information processing systems and product components are synchronized to a single reference time source.
13. Installation of software on operational production systems (i.e. customer instances) and the components of Syncron product infrastructure can only be performed by system administrators authorized by the Chief Technology Officer.
14. Syncron Chief Security Officer shall ensure to receive information about technical vulnerabilities of systems being used in a timely fashion. Chief Security Officer is responsible to establish and run a vulnerability management program that evaluates Syncron's exposure to such vulnerabilities.

Syncron's publicly accessible systems and external infrastructure are scanned for vulnerabilities by the Chief Security Officer at least quarterly or after any significant changes. Any identified critical or high severity issues are remediated in a timely manner or the risk is treated in accordance with the risk management processes. Vulnerability scans are repeated until clean results are obtained. Syncron products and the supporting infrastructure are penetration tested at least annually by an independent third party.

#### IX. Communications Security

1. All Syncron networks are managed and controlled by the Head of Operations and the authorized system administrators to protect information systems and applications.  
Anonymous or un-authenticated access to Syncron corporate networks is not allowed.  
Syncron guests and contractors are given access to guest networks which are segregated from office infrastructure.
2. Security mechanisms, service levels and management requirements of all network services are identified by the Head of Operations and reviewed by the Chief Security Officer before included in network services agreements, whether these services are provided in-house or outsourced.
3. Syncron office networks are segregated from Syncron cloud services infrastructure where customer data is stored.
4. Sensitive Syncron corporate information and customer data involved in electronic messaging shall always be protected by means of encryption and/or digital signatures.

5. Prior to sharing sensitive information with third parties, contractors, potential or existing customers, partners or consultants, Syncron employees shall have the third party sign a Non-Disclosure Agreement.

Requirements for confidentiality or non-disclosure agreements reflecting Syncron's needs for the protection of information is identified, regularly reviewed and documented by the Chief Security Officer.

#### X. System Acquisition, Development and Maintenance

1. The information security related requirements defined by the Chief Security Officer are included in the requirements for new information systems or enhancements to existing information systems.

All operating systems, infrastructure, business applications, off-the-shelf products, services, and in-house developed applications used by Syncron must meet the minimum security requirements set forth in Syncron procedures and standards.

2. Information involved in cloud business applications (such as TeamSupport) used by Syncron is protected from fraudulent activity, contract dispute and unauthorized disclosure and modification by using secure authentication methods and authorization processes.

3. Rules for the development of software and systems are defined by the Software Architects and approved by the Head of Research and Development before being established and applied to development of Syncron's cloud solutions. These rules are documented in Syncron Software Development Security Guidelines.

All Syncron product developers are trained on secure coding methods and Syncron's own development guidelines.

4. Changes to Syncron products within the development lifecycle is controlled using formal change control procedures and supporting technical solutions (i.e. Jira) that allow approval, tracking, testing and roll back of changes.

5. When operating platforms are changed, business critical applications and Syncron products are reviewed and tested to ensure there is no adverse impact on organizational operations or the security of Syncron customers' data.

6. As far as possible and practicable, vendor-supplied software packages are used without modification. Necessary changes are performed upon approval by the Head of Operations or the Chief Technology Officer.

7. Syncron software development environments (including people, processes and technology associated with system development) are secured by network segregation, access control and monitoring of changes.

8. All new information systems, business applications and hardware are subject to acceptance testing programs according to the criteria established by the Chief Technology Officer.

Upgrades and new versions of Syncron products are subject to acceptance testing according to the criteria established by the Head of Research and Development before being released to customers.

Any product customizations made by the Customer Success department are subject to acceptance testing to the criteria established by the Head Customer Success before being deployed to production.

9. The use of operational data containing personally identifiable information or any other confidential information for testing purposes are avoided (unless customer requires exception with explicit, written approval).

#### XI. Supplier Relationships

1. When engaging with third parties for infrastructure services or systems which are critical for the operations of Syncron, Service Level Agreements are signed to ensure that the security controls, service definitions and delivery levels are defined in the third-party service delivery agreement and implemented, operated, and maintained by the third parties.

2. Service Level Agreements with Syncron suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

3. The services, reports and records provided by the third parties are regularly monitored and reviewed. Audits should be carried out at least annually for critical service providers and third parties (such as AWS data centers).

4. Any changes to the provision of third party services should be managed and assessed by the Syncron Security Steering Committee taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

XII. Information Security Incident Management

1. The Synchron Incident Response Team ensures that the management responsibilities are allocated, and procedures are documented to ensure a quick, effective and orderly response to information security incidents. Information security incidents affecting Synchron products or customer data shall always be regarded high priority and escalated accordingly.
2. The Synchron Incident Response Team ([incident@synchron.com](mailto:incident@synchron.com)) or the corporate IT are notified immediately of any event in which there is reason to believe there are security implications involving a Synchron computing asset, corporate information or customer data.
3. All employees, contractors and third-party users of Synchron information systems and products are required to note and report any observed or suspected security weaknesses to the Synchron Security Team ([security@synchron.com](mailto:security@synchron.com)).
4. The Synchron Incident Response Team shall assess each information security event and decide whether the event should be classified as an information security incident.
5. Information security incidents are responded to by the Chief Security Officer and the Synchron Incident Response Team in accordance with the documented Incident Response Plan.

The Synchron Chief Security Officer and the Global Legal Counsel are the only people who shall contact authorities and law enforcement agencies in the event that a security incident is believed to have breached laws and regulations.

6. Not more than one week following the incident, members of the Incident Response Team and all affected parties shall meet to determine the effectiveness of the Incident Response Plan. Any areas will be identified in which the plan can be more effective or efficient and the plan/policy will be updated accordingly.

Types, volumes and costs of information security incidents are quantified and monitored by the Chief Security Officer to identify recurring or high impact incidents and is reported to the Security Steering Committee.

7. Synchron shall maintain contact with IT forensics experts to apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence in court in the event of high impact security incidents.

XIII. Information Security Aspects of Business Continuity Management

1. Synchron has determined its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. The continuity of Synchron products' security is captured within the business continuity management process and a business impact analysis is conducted for product security.
2. The Synchron Head of Operations and the IT organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for product security during an adverse situation.

The Business Continuity Plan detailing how Synchron will manage a disruptive event and will maintain the security of its products and customer data to a predetermined level is reviewed and approved by the Chief Technology Officer annually.

3. Organizational, technical, procedural and process changes, whether in an operational or continuity context, can lead to changes in information security continuity requirements. In such cases, the continuity of processes, procedures and controls for Synchron products' security is reviewed by the Chief Security Officer against these changed requirements.
4. All Synchron Information processing facilities and product infrastructure are implemented with redundancy sufficient to meet 99,5% minimum annual uptime requirement.

XIV. Compliance

1. All Synchron employees shall use best endeavors to ensure data protection and privacy of individuals per applicable laws and regulations.
2. For each Synchron product offering and the organization itself, the Global Legal Counsel shall explicitly identify, document and keep up to date all relevant legislative, statutory, regulatory and contractual requirements and the organization's approach to meet these requirements.
3. All Synchron employees must adhere to intellectual property rights when using proprietary software products. Software products are installed in accordance with the Synchron Acceptable Use Terms.
4. Synchron's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed annually as part of the internal audit process.

5. All Synchron employees shall ensure that the Synchron security procedures within their area of responsibility are carried out correctly to achieve compliance with the information security policy.
6. The Chief Security Officer has the overall responsibility and the right to perform technical compliance checks on all Synchron information systems and products to ensure compliance with this document.

### **SCHEDULE 3 - LIST OF SUB-PROCESSORS AUTHORIZED TO PROCESS PERSONAL DATA OF SYNCRON CUSTOMER**

Sub-processors engaged and authorized to process personal data of Customer in the course of provision of the Services by Synchron (Provision of Services may include support, development, expert services, software maintenance, etc.).

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	User account information (including name, surname, corporate e-mail, company name)
Team Support Inc.	8330 Lyndon B Johnson Fwy, Suite 1025, Dallas, TX 75243, USA	Provision of a support tool used by Synchron support team	User account information (including name, surname, corporate e-mail, company name)
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 and account management during and after implementation	User account information (including e-mail, first and last name, user ID)
LogMeIn, Inc.	320 Summer Street, Boston, Massachusetts 02210; USA	Conducting online training for end users; user experience analysis, enhancement of Services and development of new services/ activities (teleconferences via GotoMeeting/ GoToWebinar)	User account information (including name, e-mail)
Callidus Software Inc. (aka Litmos, an SAP America, Inc. company)	2700 Camino Ramon Suite 400 San Ramon, CA 94583	Provision of e-learning (Optional)	User account information (including name, surname and user e-mail) Please note that this is an option opt-in service.
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)
Carlisle & Company, Inc.  <i>Synchron's Partner</i>	30 Monument Square, Suite 22S, Concord, MA 01742, USA	Provision of support and/or implementation services, upgrades, administration/ management of customer account  (if applicable for a Customer)	All personal data listed in sec. 3.1. of the DPA: user's 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).
CGI Technologies and Solutions Inc.  <i>Synchron's Partner</i>	11325 Random Hills Road, Fairfax, Virginia 22030, USA	Provision of support and/or implementation services, upgrades, administration/management of customer account  (if applicable for a Customer)	All personal data listed in sec. 3.1. of the DPA: user's 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).
Integration and Solution Technology Inc.  <i>Synchron's Partner</i>	Matsukaze Building 3rd Floor, 4-1-1 Kitachinagawa Shinagawa-ku, Tokyo 140-0001 Japan	Provision of support and/or implementation services, upgrades, administration/management of customer account  (if applicable for a Customer)	All personal data listed in sec. 3.1. of the DPA: user's 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).
<b>Synchron Affiliates (as applicable)</b>			
Synchron Germany GmbH	Mies-van-der-Rohe-Straße 4, 80807 München, Germany	Provision of Services; Customer care (account administration)	User account information (name, surname, corporate e-mail, company name)
Synchron Inc.	HQ: One Glenlake Pkwy Suite 1000, Atlanta, GA 30328, USA	Provision of Services, Customer care (account management)	User account information (name, surname, corporate e-mail, company name)
Synchron 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)	User account information (name, surname, corporate e-mail, company name)
Synchron AB	Östra Järnvägsgatan 27 111 20 Stockholm, Sweden	Provision of Services, Customer care (account management)	User account information (name, surname, corporate e-mail, company name)



Syncron Poland sp. z o.o.	ul. Twarda 4 00-105 Warszawa, Poland	Provision of Services, Customer care (account management)	User account information (name, surname, corporate e-mail, company name)
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)	User account information (name, surname, corporate e-mail, company name)
Syncron Software India Private Limited	Municipal No. 206, Mahatma Gandhi Rd, Bengaluru, Karnataka 560001, India	Provision of Services, Customer care (account management)	User account information (name, surname, corporate e-mail, company name)
Syncron Italy S.r.l.	Via Maurizio Gonzaga 7 CAP 20123, Milano (MI), Italy	Provision of Services, Customer care (account management)	(contact details of customer's contact person/signatory: name, surname, e-mail, phone number)
Syncron France SAS	5 rue du Helder  75009 Paris, France	Provision of Services, Customer care (account management)	(contact details of customer's contact person/signatory: name, surname, e-mail, phone number)

#### 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
30.06.2020	PM: Updating the list of subprocessors following the acquisition of Natero by Freshworks
24.07.2020	PM: 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, Litmos)