



GENERAL SUBSCRIPTION TERMS FOR SaaS SERVICES
("Agreement" herein)

Witnesseth:

Whereas, Syntax is a company dedicated to the production, creation, design and development of technology applied to information services; to the development, manufacture, import, export, distribution and maintenance of electronic equipment and other computer-related products, especially software development; to the provision of services related to teaching, advice and consultancy on such products and services; as well as the provision of artificial intelligence tools that autonomously creates content, such as text or data ("AI Outputs"), by inferring from prompts, queries, or other input they receive (hereinafter "Syntax GenAI Services").

Whereas, the Parties acknowledge that Syntax and Subscriber wish to execute this Agreement to set out the terms on which Syntax will make available to Subscriber a license to use the Syntax SaaS Services.

Now, Therefore, in consideration of the mutual covenants and undertakings contained herein, and intending to be legally bound hereby, the Parties hereto agree as follows:

1. Definitions.

"Affiliate(s)" means any business entity from time to time controlling, controlled by, or under common control with either party. As used in this definition, "Control" means the right to control more than fifty percent (50%) of the voting interests of the entity.

"Order Schedule" means a signed ordering document for Services, which specifies the Services and applicable fees, as amended from time to time.

"Syntax SaaS Services" means the list of SaaS Services specified in Customer's Order Schedule(s).

2. Subject Matter.

(a) Subject to Subscriber's and its Users' compliance with the terms and conditions of this Agreement (including any Order Schedule(s) thereof), Syntax hereby grants Subscriber: (A) a limited, non-exclusive, fully revocable and non-transferable right to access and use the Syntax SaaS Services solely for the specific usage purpose which shall be described and set forth in an Order Schedule(s), during the term of this Agreement and within the geographical location (the "Territory") specified in an Order Schedule(s); (B) a limited, revocable, non-exclusive, non-sublicensable (except to Subscriber's Affiliates and for permitted use by permitted Users), non-transferable license during the applicable Term (defined in the Order Schedule) to: (i) access and use the Syntax API for the purpose of facilitating the transfer of information from Subscriber to the Syntax SaaS Services for the Subscriber's business purposes; and (C) revocable, non-exclusive, non-sublicensable (except for permitted use by permitted Users), non-transferable, limited license during the applicable Term to use Syntax materials, documentation and reports solely for the purpose of use and receipt of the Syntax SaaS Services.

(b) Under no circumstances shall the Syntax SaaS Services be used for the purpose of creating any derivative works whatsoever, except, as may be the case, to the extent expressly set forth in an applicable Order Schedule(s). The Syntax SaaS Services may be accessed, viewed, and used only by Subscriber's users as specified in an applicable Order Schedule(s). Subscriber shall not permit any other individuals, whether or not Subscriber employees or agents, to access, view, or use the Syntax SaaS Services. The Syntax SaaS Services and any component thereof may not be sold, distributed, or made available by Subscriber to others as part of any commercial product or any product for use by any Party.

3. Order Schedules. Syntax shall permit Subscriber to access and/or use the Syntax SaaS Services described in each Order Schedule in accordance with the terms and conditions of this Agreement and the applicable Order Schedule(s). Use of



the Syntax SaaS Services is subject to any restrictions set forth in the Order Schedule. For purposes of this Agreement, an Order Schedule is defined to include all attachments and/or exhibits attached thereto. Subscriber may add additional Syntax services if Syntax and Subscriber each execute additional Order Schedules to this Agreement. In the event of any conflict between the terms of this Agreement and the terms of any Order Schedule, the terms of the Order Schedule shall govern.

4. Responsibilities and Exclusions.

- (a) Subscriber shall acquire, install, operate and maintain at Subscriber's expense all communications lines, equipment, services and related technology necessary to use the Syntax SaaS Services. In the event the Subscriber requests that hardware or software other than the Syntax SaaS Services be acquired on its behalf by Syntax, the same, including additional fees, will be itemized in an additional Order Schedule. Subscriber is responsible for maintaining in place, at its expense, any hardware and software maintenance or support agreements with such third-party vendor/licensor, and for all user fees, license fees, and other licensor fees related to such hardware and software. Notwithstanding anything to the contrary in this Agreement, Syntax will have no liability to the Subscriber for any failure of the Syntax SaaS Services to perform as expected which results directly or indirectly from the Subscriber's failure to comply with its obligations under this Agreement
- (b) Subscriber will provide any remote connectivity and credentials for the relevant Syntax personnel to provide the Syntax SaaS Services or related support services.
- (c) Independently of the actual user composition defined in the applicable Order Schedule from time to time (i.e., Subscriber's employees, agents, consultants, or otherwise), Subscriber shall assume full responsibility for any action or omission by the users in using Syntax SaaS Services. Specifically, Subscriber shall ensure that each user will comply with the Syntax SaaS Services usage restrictions, confidentiality, and data protection obligations depicted under this Agreement.
- (d) Syntax takes no responsibility for the nature, accuracy, completeness or type of information and content stored by the Subscriber.
- (e) Syntax is excluded from any liability for damages of any kind that may arise out of access to and/or use of the service by the Subscriber in breach of this Agreement.

5. Fees.

- (a) Syntax SaaS Services rendered by Syntax will be invoiced in accordance with the fees structure the Parties have agreed upon in the applicable Order Schedule from time to time. If the fee for a Syntax SaaS Service is not stated in the relevant Order Schedule, Syntax's official rates valid at the time of commissioning shall apply to the Syntax SaaS Service provided by Syntax.
- (b) Shipping, travel costs, and travel time as well as overnight and catering costs incurred by Syntax in connection with the provision of Syntax SaaS Services shall be reimbursed to Syntax by the Subscriber at the rates agreed in the applicable Order Schedule from time to time.
- (c) Subscriber is solely responsible for payment of any sales and use taxes, excluding those based on the income of Syntax, arising out of and imposed because of the Services provided under this Master Subscription Agreement. All fees and expenses are quoted exclusive of sales and use taxes. In addition, Subscriber agrees to hold Syntax harmless from all claims and liability arising from Subscriber's failure to report or pay such taxes.
- (d) Payments shall be due and payable in full within fourteen (14) calendar days after the date of Syntax's invoice (the "Standard Payment Term") without deduction. If, upon completion of the Standard Payment Term, Subscriber fails to pay the due Fee within a further period of at least fourteen (14) calendar days set by Syntax, Syntax reserves the right to suspend the performance of the affected Order Schedule. Claims for damages remain unaffected.

- (e) **Adjustment.** The Parties expressly acknowledge and agree that Syntax may adjust the prices or fees for Services with effect from the beginning of each calendar year (the “Annual Adjustment”). Syntax shall communicate such Annual Adjustment by means of a written declaration to Subscriber at its discretion in compliance with the following principles:
- i. Syntax may adjust the prices and fees based on the changes in the general Consumer Price Index (the “CPI”) in the previous twelve (12) months, which is published by the bodies listed below or whatever body may supersede it.
 1. For the **United States**, published by the US Department of Labor, as located at <https://www.bls.gov/cpi/>
 2. For **Germany**, published by German Federal Statistical Office (“Statistisches Bundesamt”) - Genesis Online Index No. 62361-0016, code WZ08-62, as located at <https://www-genesis.destatis.de/datenbank/online/url/f7e59aec>
 3. For **Canada**, published by Statistics Canada, as located at https://www.statcan.gc.ca/en/subjects-start/prices_and_price_indexes/consumer_price_indexes
 4. For **Spain**, published by the Instituto Nacional de Estadística, as located at <https://www.ine.es/dyngs/IPC/es/index.htm?cid=1425>
 - ii. The Annual Adjustment will be effective as from the beginning of every calendar year. If the CPI is published with delay, then the Parties expressly acknowledge and agree that the prices or fees for Services will be adjusted retroactively once the CPI has been published. For the avoidance of doubt, any delay in notifying the Annual Adjustment, will not be understood as a waiver or loss of the right of Syntax to adjust the prices and fees in accordance with this clause.
 - iii. The Parties expressly agree that: (i) successive Annual Adjustments will be cumulative and (ii) the Annual Adjustment will only be applied in case the CPI is positive and therefore, no negative adjustment will be applicable regardless of the CPI being negative.
 - iv. In the event that the CPI is no longer published, the index published by the bodies listed above or any superseding body which most closely reflects the development of average price index shall form the basis for the determination of the changed framework.

6. Term and Termination.

- (a) This Agreement shall commence as of the Effective Date and shall continue in effect thereafter for as long as any Order Schedule entered into pursuant to this Agreement remains in effect. The term of each Order Schedule will commence on the commencement date stated therein (the “Commencement Date”) and shall continue for the duration of the initial term as specified therein (the “Initial Term”). Unless otherwise set forth in the Order Schedule, following the Initial Term, each Order Schedule shall automatically renew for successive one (1) year terms (each a “Renewal Term”) unless either Party notifies the other of its decision not to extend the term of the applicable Order Schedule at least sixty (60) days prior to the expiration of the term then in effect.
- (b) This Agreement may be terminated as follows: (a) if Subscriber commits a breach of any provision of this Agreement or any Order Schedule(s) and fails to remedy such breach within thirty (30) business days of receiving written notice thereof by Syntax (“Notice of Breach”), Syntax may then deliver a second written notice to Subscriber terminating this Agreement and any or all Order Schedules, in which event this Agreement and any or all Order Schedules, and the licenses granted hereunder, will terminate on the date specified in such second notice; or (b) if a receiver is appointed over any assets of either Party or if either Party makes any arrangement with its creditors or becomes subject to an administration order or goes into liquidation or anything equivalent to the foregoing under any jurisdiction or ceases to carry on business, the other may terminate by giving written notice with immediate effect.

- (c) Upon any expiration or termination of this Agreement and the Order Schedules, Subscriber will (i) immediately terminate all access to the Syntax SaaS Service, and/or (ii) where applicable, immediately delete any code lines and/or in general any Syntax IP (as defined under section 12 hereunder), then in its possession or stored on any device within Subscriber's control; except if: (i) required to be retained by applicable law, rule or regulation or for audit purposes; or (ii) it has been created pursuant to automatic archiving or back-up procedures and which cannot be reasonably deleted; provided that Subscriber shall not disclose, access or use any such computer records or files following the date on which Subscriber would have otherwise destroyed them. Sections 1, 5, 6(c), 10, 11, 12, 13 (for a period of three years), and section 14 (for a period of five years) shall survive any termination or expiration of this Agreement and the Order Schedules.

7. Usage Restrictions. Prohibited usage activities include, without limitation, any use of the Syntax SaaS Services in a manner that, in Syntax's reasonable judgment, involves, facilitates, or attempts any of the following:

- i. Copying, in whole or in part, modifying, adapting, tampering with, translating or creating derivative works from Syntax SaaS Service.
- ii. Except as expressly set forth in the applicable Order Schedule, reverse engineering, selling, redistributing internally, licensing to any third parties the Syntax SaaS Service, or any part thereof, including the same or any part thereof in any commercial product or service of the Subscriber, publishing performance or benchmark tests or analysis relating to the Syntax SaaS Services.
- iii. Creating an internal or external product or service similar to or which may in any way compete in capabilities with and or function as a substitute of the Syntax SaaS Services.
- iv. Using the Syntax SaaS Service as a component in any other software system unless specifically authorized by Syntax. Subscriber agrees to indemnify and reimburse Syntax for any damage to the operations of Syntax that may be caused by violation of this provision.
- v. Violating any law of any applicable jurisdiction.
- vi. Except with Syntax's prior written permission, publishing performance or benchmark tests or analyses relating to the Syntax SaaS Services.
- vii. Sending of unsolicited or unauthorized advertising, promotional materials, junk e-mails, chain letters or spam to individuals or lists of individuals who have not requested or consented thereto.
- viii. Modifying any material originating from or belonging to Syntax.
- ix. Using the Syntax SaaS Services or Syntax SaaS Services' content in any way to create or send misleading or false information.
- x. Remove or obscure any proprietary notices or labels on the Syntax SaaS Service.

Any other uses of the Syntax SaaS Service outside those expressly granted under this Agreement and the applicable Order Schedule require the prior written consent of Syntax. In the event that the Subscriber performs, threatens to perform or attempts to perform any of the actions described in points i) to x) above, Syntax may temporarily block the provision of the affected Syntax SaaS Services to Subscriber.

Moreover, as between Syntax and Subscriber, Subscriber acknowledges that the Syntax SaaS Services and all components thereof are Syntax's property and are subject to modification by Syntax. Where possible, Syntax shall provide to the Subscriber reasonable advance notice of any change including changing the functionality of Syntax SaaS Services. Syntax may, at its sole discretion from time-to-time issue new versions of the Syntax SaaS Services. Subscriber agrees to, as directed by Syntax and the applicable release documentation, accept such updates and perform required update procedures.

9. Audits and Inspections. No more than once per year, for the purpose of verifying compliance with this Agreement, Syntax (and Syntax authorized representatives) shall have the right, during normal business hours upon reasonable advance notice and without material disruption to Subscriber's business and subject to Subscriber's security and other policies



pertinent to audits, to audit and inspect Subscriber's offices, books and records relevant to this Agreement and to observe the use made of the Syntax SaaS Services and the manner in which the Syntax SaaS Services are accessed. For the avoidance of doubts, Syntax audits rights shall include, but not be limited to confirmation of Subscriber's deletion of any Syntax code lines and/or in general any Syntax IP in its possession or stored on any device within Subscriber's control, in line with section 6 (c) above. Moreover, the Subscriber acknowledges and agrees that the Syntax SaaS Services may contain internal controls to verify the proper use of the same in compliance with this Agreement, and which may prevent the Syntax SaaS Services from working properly if the granted usage limitation is exceeded.

10. Limitation of Liability and Indemnification.

- I. **WAIVER.** NEITHER PARTY NOR ITS REPRESENTATIVES SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, CONSEQUENTIAL, RELIANCE OR PUNITIVE DAMAGES (IN TORT, CONTRACT OR OTHERWISE), INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS OR LOST REVENUES, REPLACEMENT GOODS, LOSS OF TECHNOLOGY, RIGHTS OR SERVICES, LOSS OF DATA, LOSS RELATED TO OR ARISING FROM ANY THIRD-PARTY HARDWARE OR SOFTWARE, WHICH MAY BE INCLUDED IN THE SERVICES, OR INTERRUPTION OR LOSS OF USE OF SERVICE OR EQUIPMENT, REGARDLESS OF WHETHER SUCH PARTY HAS BEEN ADVISED OF THE LIKELIHOOD OF SUCH DAMAGES.
- II. **LIMITATION OF LIABILITY.** THE COLLECTIVE AGGREGATE LIABILITY OF SYNTAX SHALL BE LIMITED TO AND SHALL NOT EXCEED THE TOTAL AMOUNT OF FEES ACTUALLY PAID BY THE SUBSCRIBER TO SYNTAX UNDER THE CORRESPONDING ORDER SCHEDULE IN THE TWELVE (12) MONTHS PRECEDING A CLAIM. THE LIMITATIONS SET FORTH UNDER THIS SUBSECTION II SHALL NOT APPLY WITH RESPECT TO LIABILITIES FOR DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE (LIFE, BODY, OR HEALTH) OR TO THE EXTENT THAT DAMAGES ARE CAUSED BY SYNTAX'S FRAUDULENT ACTS, GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.
- III. **SYNTAX INDEMNITY.** SYNTAX WILL INDEMNIFY AND DEFEND SUBSCRIBER AND ITS REPRESENTATIVES FROM AND AGAINST ANY AND ALL THIRD-PARTY CLAIMS, DEMANDS, ACTIONS, CAUSES OF ACTIONS, LAWSUITS, ADMINISTRATIVE PROCEEDINGS OR SIMILAR ACTIONS, AND ALL LOSSES, DAMAGES, COSTS, EXPENSES AND OTHER LIABILITIES RELATED THERETO TO THE EXTENT RESULTING FROM OR ARISING OUT OF SYNTAX'S VIOLATION, INFRINGEMENT, MISAPPROPRIATION OR WRONGFUL USE OF ANY INTELLECTUAL PROPERTY OR OTHER PROPRIETARY RIGHTS BY ANY SERVICES, AS DEFINED, EXCLUDING ANY THIRD-PARTY HARDWARE, SOFTWARE OR SERVICES INCLUDED IN THE SERVICES PROVIDED BY SYNTAX TO SUBSCRIBER HEREUNDER (EACH AN "INFRINGEMENT CLAIM"). THE PRECEDING SENTENCE NOTWITHSTANDING, SYNTAX SHALL HAVE NO OBLIGATION TO DEFEND AND INDEMNIFY SYNTAX AGAINST ANY INFRINGEMENT CLAIM CAUSED BY: (I) SUBSCRIBER USE OF THE SERVICES IN ANY MANNER THAT DOES NOT COMPLY IN ALL MATERIAL RESPECTS WITH THE AGREEMENT OR APPLICABLE LAWS OR REGULATIONS, (II) AN UNAUTHORIZED MODIFICATION TO THE SERVICES BY ANYONE OTHER THAN SYNTAX OR ITS REPRESENTATIVES, (III) SUBSCRIBER USE OF THE SERVICES IN COMBINATION WITH SYSTEMS, SOFTWARE (INCLUDING OPEN SOURCE SOFTWARE OR HARDWARE), OR OTHER ITEMS NOT SUPPLIED BY SYNTAX, PROVIDED THAT THE INFRINGEMENT WOULD NOT HAVE OCCURRED BUT FOR THE COMBINATION, (IV) SUBSCRIBER USE OF THE SERVICES AFTER SYNTAX NOTIFIES SUBSCRIBER TO DISCONTINUE USE BECAUSE OF ACTUAL OR POSSIBLE INFRINGEMENT, (V) SUBSCRIBER USE OF A SUPERSEDED RELEASE OF ANY SOFTWARE THAT IS INCLUDED AS PART OF THE SERVICES, IF THE INFRINGEMENT WOULD HAVE BEEN AVOIDED BY A CURRENT RELEASE OF SUCH SOFTWARE MADE AVAILABLE TO SUBSCRIBER BY SYNTAX, OR (VI) SUBSCRIBER CONFIDENTIAL INFORMATION, SUBSCRIBER IP, OR MATERIAL PROVIDED BY SUBSCRIBER (SECTION (I) THROUGH (VI), COLLECTIVELY, "SUBSCRIBER ACTS"). FOR ANY INFRINGEMENT CLAIM COVERED BY THIS SECTION, SYNTAX WILL, AT ITS ELECTION, EITHER: (I) PROCURE THE RIGHTS TO USE THAT PORTION OF THE SERVICES ALLEGED TO BE INFRINGING; (II) REPLACE THE ALLEGED INFRINGING PORTION OF THE SERVICES WITH A NON-INFRINGING ALTERNATIVE; (III) MODIFY THE ALLEGED INFRINGING PORTION OF THE SERVICES TO MAKE IT NON-INFRINGING; OR (IV) TERMINATE THE ALLEGEDLY INFRINGING PORTION OF THE SERVICES OR THE APPLICABLE ORDER SCHEDULE. FOR CLARIFICATION PURPOSES, IT IS EXPRESSLY AGREED THAT SYNTAX SHALL NOT BE LIABLE TO THE SUBSCRIBER FOR COSTS OR DAMAGES, IN THE EVENT OF SECURITY BREACHES OF THE SUBSCRIBER'S NETWORK OR DATA.
- IV. **SUBSCRIBER INDEMNITY.** SUBSCRIBER WILL INDEMNIFY AND DEFEND SYNTAX AND ITS REPRESENTATIVES FROM AND AGAINST ANY AND ALL THIRD-PARTY CLAIMS, DEMANDS, ACTIONS, CAUSES OF ACTIONS, LAWSUITS, ADMINISTRATIVE PROCEEDINGS OR SIMILAR ACTIONS, AND ALL LOSSES, DAMAGES, COSTS, EXPENSES AND OTHER LIABILITIES RELATED THERETO TO THE EXTENT RESULTING FROM OR ARISING OUT OF SUBSCRIBER ACTS. SUBSCRIBER'S OBLIGATIONS UNDER THIS SECTION INCLUDE CLAIMS ARISING OUT OF THE ACTS OR OMISSIONS OF SUBSCRIBER'S EMPLOYEES OR AGENTS, ANY OTHER PERSON TO WHOM SUBSCRIBER HAS GIVEN ACCESS TO THE SERVICES, AND ANY PERSON WHO GAINS ACCESS TO THE SERVICES AS A RESULT OF SUBSCRIBER'S FAILURE TO USE REASONABLE SECURITY PRECAUTIONS, EVEN IF THE ACTS OR OMISSIONS OF SUCH PERSONS WERE NOT AUTHORIZED BY SUBSCRIBER.

- V. **LIMITATIONS PERIOD.** THE PARTIES EXPRESSLY AGREE THAT ANY CLAIM FOR DAMAGES SHALL BECOME STATUTE-BARRED AFTER ONE YEAR FROM THE DAY IN WHICH THE ACT OR OMISSION CAUSING THE DAMAGE TOOK PLACE AND, IN ANY EVENT, AFTER ONE YEAR FROM THE LAST DAY THE SERVICES WERE RENDERED.

11. **Warranty Disclaimer**

SUBSCRIBER ACKNOWLEDGES AND AGREES THAT THE SYNTAX SAAS SERVICE, ANY COMPONENT THEREOF, THE CONTENTS THEREIN, AND ANY ACCOMPANYING DOCUMENTATION ARE PROVIDED ON AN “AS IS”, “AS AVAILABLE” BASIS AND SYNTAX DOES NOT MAKE ANY AND HEREBY SPECIFICALLY DISCLAIMS ANY REPRESENTATIONS, ENDORSEMENTS, GUARANTEES, OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, OR NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS.

12. Intellectual Property. The Parties acknowledge that, as between Subscriber and Syntax, the Syntax SaaS Services are the valuable intellectual property of Syntax. All rights with respect to the Syntax SaaS Services including, without limitation, names, format, patents and trademarks, whether now existing or which may hereafter come into existence, which are not expressly licensed to the Subscriber herein are reserved by Syntax.

13. Confidentiality. Subscriber and Syntax understand and agree that in the performance of this Agreement and the Order Schedule(s) each Party may have access to private or confidential information of the other Party which either is marked as “confidential” or which the receiving Party should reasonably know under the circumstances that such information is confidential and/or proprietary information of the other Party. Each Party shall hold such information in confidence and not, without the consent of the other, disclose it to a third Party or use it for any purpose other than in performance of this Agreement and any or all Order Schedules. This obligation of confidentiality shall not apply to information that is generally available to the public through no act or omission of the receiving Party or becomes known to the receiving Party through a third party with no obligation of confidentiality, or is required to be disclosed by law, court or by any government or regulatory authority. All confidential information will remain the exclusive property of the owner. No public announcement, press release or communication concerning this Agreement and the Order Schedules shall be made without the prior consent of the other Party.

14. **Data Protection and Data Security.**

- (a) The Parties will comply with all data protection and privacy laws and regulations applicable to the respective party in its role in the Processing of Personal Data under the Agreement. Within the scope of the commissioned activities, the applicable country or region-specific Data Processing Agreement ([Annex 1](#)) shall apply.
- (b) Syntax will take reasonable steps, in accordance with industry standards and best practices, to create a secure environment for the Subscriber's data stored on Syntax systems. All hardware and software supplied or used by Syntax in the provision of Services is designed to be protected from unauthorized control, access and manipulation. However, the Subscriber agrees that Syntax may offer various security options, and it is the Subscriber's responsibility to select the security options that it believes best meet its needs. Syntax will implement the security options as agreed. Syntax advises the Subscriber that security gaps can become present at any time in the internet as an open communication system, and Syntax does not warrant secure operation of the Syntax SaaS Services or that Syntax will be able to prevent third-party attacks or disruptions of the Syntax SaaS Services. Syntax will take defensive measures to the extent necessary after knowledge and verification of security gaps. Nevertheless, in this regard, the Subscriber shall install state-of-the-art security components, software updates and patches on the systems located in its sphere of risk, carry out regular security checks and data backups and, in the event of a particularly high need for security, use further measures to protect against unauthorized access to and/or modification of data.

15. Syntax GenAI Services' Rider. If the performance of Syntax SaaS Services implies the provision of Syntax GenAI Services, the following dedicated terms shall apply and coexist with the relevant terms of this Agreement:

- (a) Limitation of Liability. Syntax makes no guarantees, representations or warranties with respect to the suitability, accuracy, quality, security, legality and reliability of Syntax GenAI Services, including any AI Outputs. Subscriber acknowledges that AI Outputs may contain errors and misstatements and may be incomplete or inaccurate. Before leveraging any AI Outputs, which are provided "AS IS," Subscriber and its users are responsible for making their own determinations that the AI Outputs are suitable, and Subscriber is solely responsible for any reliance on the accuracy, completeness, or usefulness of any AI Outputs. Under no circumstances will Syntax be liable in any way for any AI Outputs or for any loss or damage of any kind incurred as a result of Subscriber's interaction with and/or use of Syntax GenAI Services. Moreover, the control and responsibility for data and its deletion remain with Subscriber. Syntax is not responsible for how the AI model is trained or how third-party vendors utilize Subscriber Confidential Information. The solution is designed to utilize pre-existing LLMs.
- (b) Ownership of Subscriber Data. As between Syntax and Subscriber, Subscriber owns all right, title, and interest, including all Intellectual Property Rights, in and to the Subscriber Data. For the avoidance of doubt, Subscriber Data means all information, data, and other content, in any form or medium, that is submitted, posted, or otherwise transmitted by or on behalf of Subscriber or User through the Syntax GenAI Services, including such information collected from users. Subscriber hereby grants to Syntax a non-exclusive, royalty-free, worldwide license to reproduce, distribute, and otherwise use and display the Subscriber Data and perform all acts with respect to the Subscriber Data as needed for Syntax to provide the Syntax GenAI Services.
- (c) Ownership of Inputs/Prompts and AI Outputs. As between the parties, and to the extent permitted by applicable laws, rules and regulations, if Subscriber provides inputs or prompts to the Syntax GenAI Services, then Subscriber shall maintain its ownership rights over such inputs or prompts (including Subscriber Data) as well as on AI Outputs, including any work product or deliverable created from those AI Outputs. Furthermore, Subscriber shall monitor the input and output where applicable, as Syntax does not assume liability for AI outputs.
- (d) Syntax GenAI Services Representations and Warrants. Where Syntax relies on a third-party's technology or AI Models (hereinafter the "Third Party AI Technology") for the provision of Syntax GenAI Services, Syntax confirms to Subscriber that i) it has the right to use the Third Party AI Technology through a license, ii) it complies with all use restrictions under that license, and iii) it has full power and authority to grant the rights under this Agreement to the Subscriber.
- (e) Syntax GenAI Services Usage Limitation and Regulatory Compliance.
 - i. To the extent applicable, Syntax declares that Syntax GenAI Services and the technologies that comprise them comply with all regulatory compliance requirements that are legally binding under the European Regulation (EU) 2024/1689 ("AI Act"). Likewise, specifically, Syntax GenAI Services comply with the highest quality standards required by law, as well as ethical and social standards in accordance with AI Act and the principles of universal rights that protect and safeguard the fair and peaceful coexistence between people.
 - ii. The scope of application and use of Syntax GenAI Services shall be that stipulated and detailed in the corresponding Order Schedule. Syntax GenAI Services are not designed nor authorized in any way (explicitly or tacitly) for any use outside the scope of application provided for in the Order Schedule agreed between the parties and of which this Agreement forms an inseparable part. Syntax shall not be liable in any way, directly or indirectly, for any use outside this scope.
 - iii. In relation to everything mentioned in the previous clauses, the purpose and scope of use of Syntax GenAI Services shall always be aligned with the uses legally permitted by the Order Schedule, the AI Act and any other applicable regulations. Any other use outside that scope is highly reproached and rejected by Syntax, and therefore, Syntax is not responsible for any malicious misuse that may be made of Syntax GenAI Services and the results that may accrue from it

Syntax GenAI Services may include AI models, technologies or features licensed from third parties ("Third Party Components") that require Syntax to pass through additional terms. Specific terms applicable to Third Party

Components will be available here: <https://www.syntax.com/third-party-policies/> (collectively, the “Third-Party Terms”). For the avoidance of doubt:

- i. If new Third Party Components are added from time to time or if any of the applicable Third-Party Terms are modified, such new or updated terms will be accessible via the above-mentioned link.
- ii. Insofar as Subscriber has agreed to terms and conditions directly with the provider of such Third-Party Components, such agreed terms shall take precedence over the Third-Party Terms in their area of application.
- iii. Syntax reserves the right to add, remove, or exchange Third Party Components at any time, in its sole and absolute discretion.
- iv. If Third Party Components become unavailable, cease to function or are suspended for any reason (the “Affected AI”), Syntax will make commercially reasonable efforts to replace such Affected AI with another of similar specifications in due course. If no replacement is possible, Syntax may either reduce the scope of use or remove the Affected AI altogether.
- v. Subscriber acknowledges and agrees that the Third-Party Components, and any accompanying documentation, are provided on an “as is”, “as available” basis at Subscriber’s own risk. Syntax does not make any and hereby explicitly disclaims all representations, endorsements, guarantees, conditions, undertakings, or warranties, express or implied, including, without limitation, any of merchantability, fitness for a particular purpose, title, or non-infringement of IP rights or any warranties concerning the Third-Party Components being error free or that they will operate without interruption.
- vi. Under no circumstances shall Syntax be liable to Subscriber for any indirect, consequential, special, incidental, punitive or exemplary damages, including, without limitation, lost profits, lost data, lost savings and lost revenues, whether or not characterized in negligence, contract, or other theory of liability, arising from the access or use by Subscriber of any Third Party Components.

16. Non-solicitation Clause. During the period in which Syntax provides Syntax SaaS Services to Subscriber under an Order Schedule and for a period of one (1) year thereafter, neither party shall, without the prior written consent of the other, directly or indirectly, through an existing corporation, unincorporated business, affiliated party, successor employer, or otherwise, solicit or hire from the other party, for the purpose of employment and/or on a part-time, consulting, advising, or any other basis, any such officers, directors, employees, agents or freelancers who have been involved in the provision of the Syntax SaaS Services and whose employment with the other party ended less than six (6) months prior to the date of such solicitation. In the event of failure to comply with these covenants, the non-breaching Party will be entitled to claim compensation from the breaching Party for any damages caused by such a breach.

16. 1. If Customer’s above-referenced principal place of business is located in Canada, then the terms set forth below shall apply instead of section 16 above.

During the period in which Syntax provides Syntax SaaS Services to Subscriber under an Order Schedule and for a period of one (1) year thereafter, Subscriber shall not employ or solicit for employment (or in any way assist another in recruiting, soliciting, or inducing to terminate their relationship with Syntax), directly or indirectly, any employee, independent contractor, or consultant of Syntax involved in the performance of the Services (a “Restricted IT Employee”) and whose employment with the other party ended less than six (6) months prior to the date of such solicitation, unless Syntax has granted express written consent otherwise. If any Restricted IT Employee of Syntax is hired by Subscriber, either directly or indirectly, during the non-solicitation period specified above and in violation of this Section 16.1, Non-Solicitation Clause, Syntax will be entitled to claim compensation from Subscriber for any damages caused by such a breach.

17. Notices. All notices with respect to this Agreement shall be in writing, and delivered by certified mail, return receipt requested, overnight or express courier service, or by electronic email with confirmation by the above described mailing methods to the respective address(es) of the Parties first set forth above, or to a different address which a Party may give written notice of pursuant to this Section from time to time. Notice will be deemed delivered and received on the date it is actually received.

18. Governing Law & Venue / Principles of Cooperation, Escalation.

- (a) This Agreement and the Order Schedule(s), as well as any and all contract, tort, or other claims arising from this Agreement and the Order Schedule(s) will be governed by and construed in accordance with the laws of the State of New Jersey except for application of its conflict of laws principles and any state or federal provision interpreting the Agreement more strongly against the drafter. The sole jurisdiction and venue for any litigation arising out of the Agreement or an Order Schedule will be an appropriate federal or state court in New Jersey. Syntax hereby reserves its right to sue the Subscriber at the court which is competent for the country or federal state or court district in which Syntax is domiciled.
- (b) The Parties commit themselves to loyal cooperation. If there is an obstacle to the project or if there is a disagreement about the rights and obligations of both Parties and/or about the performance of the Syntax SaaS Services, the Parties shall endeavor in good faith to reach an appropriate solution by way of negotiations. As a first step, the contact persons responsible for the Order Schedule in question will discuss the problem and, if possible, resolve it by mutual agreement as far as their decision-making authority is sufficient. If the responsible contact persons are unable to resolve the conflict within a reasonable period of time or if a solution lies outside their decision-making authority, the Parties will attempt to resolve the conflict at management level within two weeks of addressing the conflict to the other party, at the latest, as a second step. If the management is unable to resolve the conflict within a reasonable period of time but within 4 weeks at the latest, both Parties are free to undertake arbitration or another attempt at agreement with a jointly determined expert.

19. Miscellaneous.

- (a) Assignment: Subscriber may not assign its rights and obligations under the Agreement without the prior written consent of Syntax, which Syntax will not unreasonably withhold.
- (b) Place of performance, service transfer point: The place of performance at which Syntax is to perform the service activities is the applicable registered office of Syntax unless otherwise agreed in this SaaS Agreement. This SaaS Agreement may indicate service transfer points. At such transfer points the responsibility of Syntax for the provision of the Services ends and the performance risk passes to the Subscriber. Unless otherwise agreed in this SaaS Agreement, the service transfer points shall be the network interface or the entry point of Syntax's computer center into the Internet.
- (c) Suspension: Syntax may temporarily suspend the Services and/or Subscriber's access thereto as provided in an applicable SOW or if such suspension is (i) required by law, (ii) for a Force Majeure Event, (iii) for maintenance, inspection and repair necessitated by emergency circumstances, including a Security Threat, as defined in a SOW, as reasonably determined in good faith by Syntax, or (iv) subject to Section 5(d), for failure to make timely payment of Recurring Services fees or undisputed Consulting Services fees. If Services are suspended, Syntax shall, unless the circumstances make it impracticable, provide a reasonable prior notice to Subscriber of any such suspension that is scheduled in advance. In the event Syntax suspends the Services as set forth in Section 5(d), Syntax will (1) endeavor to provide Subscriber with reasonable notice considering the facts and circumstances related to the subject emergency, and (2) use commercially reasonable efforts to minimize any interruption to the Services. Notwithstanding the foregoing, Syntax does not guarantee that the Services will be uninterrupted.
- (d) Waiver, Continuance: A waiver of a provision or the non-enforcement of a provision in the event of a breach of the Agreement shall not be deemed a waiver of a breach or a waiver of the right to enforce the provision. All terms of the Agreement which by their nature extend beyond the termination or expiration of the Agreement shall remain in full force and effect until they have been performed.
- (e) Force majeure and other obstacles to performance: Except for the payment obligations under this Agreement, neither party shall be liable to the other for any failure to perform or delay in performing their obligations pursuant to this Agreement and/or the applicable Order Schedule(s) from time to time caused by force majeure or any other event unforeseeable at the time of entering into the Agreement.

Force majeure is any event beyond the control of the respective Party that prevents the Party from fulfilling its obligations in whole or in part, including (but not limited to) fire and storm damage, natural disasters (such as floods, earthquakes, avalanches), computer or Internet or telecommunications breakdowns and, in general,

breakdowns of any kind, denial of service attacks, cyber Attacks, difficulties in procuring materials or energy, transport delays, strikes, lawful lockouts, difficulties in obtaining necessary governmental permits, governmental measures or failure to receive supplies or supplies from suppliers in a timely or incorrect manner as well as operational disruptions or official decrees for which the Party is not responsible, and in particular epidemics and/or pandemics, insofar as these are identified by the World Health Organization or the Robert Koch Institute and the performance of a Party is directly or indirectly impaired or limited by these to a not insignificant extent. Supply difficulties and other service disruptions on the part of Syntax's suppliers and/or subcontractors are only considered to be force majeure if the supplier and/or subcontractor is itself prevented from providing the service incumbent upon it by an event in accordance with this paragraph. The party affected by the impediment to performance shall immediately notify the other party of the occurrence and removal of the impediment to performance and shall use its best endeavors to remedy it and limit its effects as far as possible.

Insofar as such events make Syntax's delivery or Syntax SaaS Services substantially more difficult or impossible and the hindrance is not only of a temporary nature, each Party shall be entitled to terminate the affected Order Schedule in accordance with Clause 6.

- (f) “Rebus sic stantibus” doctrine: In the event that a force majeure situation substantially and unforeseeably changes the circumstances that were taken into account when the Parties agreed on the terms and conditions of this Agreement and/or the applicable Order Schedule from time to time, and that, as a consequence of said alteration, there is an exorbitant disproportion, that exceeds any calculation, of the expected benefits of the Parties, in such a case the parties undertake to make the necessary changes to the affected terms and conditions, in good faith, in accordance with the “rebus sic stantibus” doctrine. For the avoidance of doubt, according to such doctrine the Parties shall identify the obligations to be modified due to the force majeure event and agree on the modification thereof, in order to be able to comply with them according to the new situation.
- (g) Formal requirements: All amendments and supplements to this Agreement as well as all declarations to be made in accordance with this Agreement, all other declarations of intent relevant to the Agreement and declarations on the assertion of design rights (e.g. termination, reminder, setting of a deadline) must be made in writing or using DocuSign or a comparable technique and refer to the relevant contractual document (Agreement or Order Schedule); qualified electronic signature is not required. The formal requirement also applies to the waiver of this.
- (h) Export and Import Control: The Parties are aware that Syntax SaaS Services may be subject to export and import restrictions. In particular, there may be licensing obligations, or the use of the software and associated technologies abroad may be subject to restrictions. Syntax's performance of this Agreement is subject to the provision that there are no obstacles to such performance due to national and international regulations of export and import law or any other statutory regulations. The Parties will comply with the applicable export and import control regulations of the United States of America as well as all other relevant regulations.
- (i) Anti-corruption: Each Party confirms that it understands the importance of anti-corruption and will comply and procure that its employees comply with all relevant and applicable anti-corruption and anti-bribery laws, rules, and regulations. For the purposes of this Agreement, “bribery” includes, but is not limited to promising or granting to the other Party, or to any of its employees involved in the award or execution of this Agreement, nor to any third party, any kind of bonuses or services, tangible or intangible, to secure a contract or an agreement or gain an important advantage. If either Party becomes aware of any conduct by one of the other Party's employees, subcontractors, independent advisors or consultants or agents that constitutes bribery or corruption in accordance with this Section, or if there is any specific suspicion of such conduct, it shall immediately inform the other Party of such knowledge and information. Each Party confirms that, any act of bribery (as defined above) or any breach of national or other relevant anti-corruption laws, rules and regulations, will be considered as a serious breach of this Agreement, entitling the other Party to terminate the latter and/or claim compensation and/or such other remedies as are available to it.
- (j) Feedback Clause: To the extent that Subscriber or any Permitted User submits ideas, suggestions, documents, or proposals regarding the Syntax Services to Syntax (“Feedback”), Subscriber acknowledges and agrees that:



the Feedback does not contain confidential or proprietary information and Syntax is not under any obligation of confidentiality with respect to the Feedback; and Syntax will be entitled to use, commercialize or disclose (or choose not to use, commercialize or disclose) such Feedback for any purpose, in any way, in any manner and to anyone worldwide without any compensation or reimbursement of any kind to Subscriber for such use.

- (k) Publicity Clause: Notwithstanding any other term of this Agreement, Syntax may refer to Subscriber as a customer of Syntax in announcements, press or marketing releases, publications, presentations, case studies and other public statements and on Syntax's Website and other online channels (collectively, "Publicity"), without notice to or prior written consent of Subscriber. Syntax may use Subscriber's name, logo and trademark in conjunction with any Publicity and disclose the existence of this Agreement, the Services provided to Subscriber and any testimonials received from Subscriber in any such Publicity. Subscriber grants Syntax a limited, perpetual, fully paid-up, irrevocable, non-exclusive, non-transferable, and non-sublicensable license to use its logo and trademarks in connection with any Publicity.
- (l) Severability Clause: If any provision of this Agreement is unlawful, void, or unenforceable, the Parties shall reform it to the extent necessary to correct the unenforceable provision and the remaining provisions shall remain in full force and effect.



Annex 1 – DATA PROCESSING AGREEMENT (“DPA”)

Select a link to quickly access the DPA for each region/country.

North America	Germany and Spain	France
-------------------------------	-----------------------------------	------------------------

For North America Customers

This Annex 1 – Data Processing Agreement (“DPA”) is attached to and forms a part of the General Subscription Terms for SaaS Services between Subscriber and Syntax Systems USA LP (“Processor” or “Syntax”), a Delaware limited partnership, including any subsequent amendments, modifications, extensions, or renewals (the “Agreement”). This DPA applies solely to the extent that Syntax Processes any Personal Data (defined below) in connection with the Services. Subscriber enters into this DPA on behalf of itself and, to the extent required under Applicable Data Protection Law in the name, and on behalf of, its Affiliates.

1. Definitions

“Applicable Data Protection Law” means all data protection and privacy laws and regulations applicable to the respective party in its role in the Processing of Personal Data under the Agreement.

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“Data Privacy Framework” means the EU-U.S. Data Privacy Framework self-certification program operated by the U.S. Department of Commerce (“DOC”); as may be amended, superseded or replaced.

“Data Privacy Framework Principles” means the principles and supplemental principles contained in the relevant Data Privacy Framework; as may be amended, superseded or replaced.

“Individual” shall have the same meaning as the term “Data Subject” or the equivalent term under Applicable Data Protection Law.

“Personal Data” means any information relating to an identified or identifiable individual where (i) such information is contained within Subscriber Data; and (ii) is protected similarly as personal data, personal information, or personally identifiable information under Applicable Data Protection Law.

“Personal Data Breach” means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed pursuant to the Agreement. “Personal Data Breach” will not include unsuccessful attempts or activities that do not compromise the security of Personal Data.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms “Process”, “Processes” and “Processed” will be construed accordingly.

“Processor” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.



“**Regulator**” shall have the same meaning as the term “supervisory authority”, “data protection authority” or the equivalent term under Applicable Data Protection Law.

“**Services**” means the Services directly provided by Syntax in accordance with the Agreement that require the processing by Syntax of Personal Data on Subscriber’s behalf.

“**Sub-Processor**” means a third party, other than a Processor or Processor Affiliate, which Processor subcontracts with and which may Process Personal Data to assist Processor in fulfilling its obligations. “Sub-Processor” shall not include any Syntax employee or consultant.

2. PROCESSING OF PERSONAL DATA

2.1 Scope and Roles. This DPA applies when Personal Data is Processed by Syntax as Processor in its provision of the Services to Subscriber, who will act as either a Controller or Processor, as applicable, of Personal Data. Each party is responsible for compliance with its respective obligations under Applicable Data Protection Law.

2.2 Subscriber Processing. Subscriber agrees that (i) it will comply with its obligations under Applicable Data Protection Law in its Processing of Personal Data and any Processing instructions it issues to Syntax, and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under Applicable Data Protection Law for Syntax to Process Personal Data and provide the Services pursuant to the Agreement (including this DPA).

2.3 Syntax Processing. Syntax agrees that (a) when Syntax Processes Personal Data in its capacity as a Processor on behalf of Subscriber, Syntax will Process the Personal Data as necessary to perform its obligations under the Agreement, and only in accordance with Subscriber’s documented instructions (as set forth in the Agreement, in this DPA, or as directed by the Subscriber through the Services). Syntax is not responsible for determining if Subscriber’s Processing instructions are compliant with applicable law. Notwithstanding the foregoing, If Syntax becomes aware that it cannot Process Personal Data in accordance with Subscriber’s instructions due to a legal requirement under any applicable law, Syntax may, in its discretion, cease all Processing until such time as Subscriber issues new instructions with which Syntax is able to comply. If this provision is invoked, Syntax will not be liable to Subscriber under the Agreement for any failure to perform the Services until such time as Subscriber issues new lawful instructions with regard to the Processing.

3. ACCESS

3.1 Personnel. All Syntax and Syntax Affiliates employees, as well as any Sub-Processors that Process Personal Data in accordance with this DPA will be subject to the requirements concerning protection of confidential information described in the Agreement.

4. SUB-PROCESSING AND AFFILIATES

4.1 General Authorization. Subscriber provides general authorization to Syntax’s use of Sub-Processors and Syntax’s Affiliates to Process Personal Data on behalf of Subscriber in accordance with this section.

4.2 Sub-Processor and Affiliate Obligations. To the extent Syntax engages Sub-Processors to Process Personal Data, such entities shall be subject to the same level of data protection and security as Syntax under the terms of the Agreement. Syntax is responsible for the performance of its Affiliates’ and Sub-Processors’ obligations in compliance with the terms of this DPA.

5. ASSISTANCE

5.1 Privacy Inquiries and Requests from Individuals. If Subscriber receives a request or inquiry from an Individual related to Personal Data Processed by Syntax for the provision of Services, Subscriber can either (i) securely access the Personal Data through the Services to address the request, or (ii) to the extent such access is not available to Subscriber, submit a written request with detailed instructions to Syntax on how to assist Subscriber with such request. If Syntax directly receives any such requests or inquiries from Individuals that have identified Subscriber as the Controller, it will promptly pass on such requests to Subscriber without responding to the Individual.

5.2 Legal Requests. Syntax may be required by law to provide access to Personal Data, such as to comply with a subpoena or other legal process, or to respond to government requests, including public and government authorities for national security and/or law enforcement purposes. Syntax will use reasonable efforts to redirect such requests to provide access to Personal Data to Subscriber, unless otherwise required by law. As part of this effort, Syntax may also provide Subscriber's basic contact information to the government body.

6. TRANSFER OF PERSONAL DATA

6.1 Data Transfers. Without prejudice to any applicable regional data center restrictions for Services specified in the Agreement, Syntax may Process Personal Data globally as necessary to perform the Services. Wherever Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Applicable Data Protection Law.

6.2 Data Privacy Framework. To the extent Subscriber's use of the Services requires an onward transfer mechanism to lawfully transfer personal data from a country within the European Economic Area (EEA) to Syntax located outside the EEA, the parties agree that Syntax shall be deemed to provide appropriate safeguards for such Personal Data by virtue of Syntax's compliance with the Data Privacy Framework, evidenced by Syntax's certification to the DOC that it adheres to the Data Privacy Framework Principles.

6.3 Alternative Transfer Mechanisms. If and to the extent that a court of competent jurisdiction or a Regulator with binding authority orders that the measures described in this DPA cannot be relied on to lawfully transfer Personal Data to Syntax, the parties shall reasonably cooperate to agree and take any actions that may be reasonably required to implement any additional measures or alternative transfer mechanism to enable the lawful transfer of such Personal Data.

7. SECURITY

7.1 Security Measures. Syntax will implement the technical and organizational security measures described in the Agreement designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Syntax may modify or update the security measures at its discretion provided that such modification or update does not result in a material degradation in the protection offered by the security measures. Subscriber is responsible for selecting such technical and organizational security measures described in the Agreement as Subscriber considers adequate to maintain appropriate security of Personal Data Processed as a result of Subscriber's use of the Services.

7.2 Security Breach Notification. Syntax will notify Subscriber in writing (including via email), without undue delay, and in no event later than seventy-two (72) hours, of a confirmed Personal Data Breach that impacts the Processing of the Personal Data that is subject to the Agreement. Syntax will also use reasonable efforts to provide timely information regarding the Personal Data Breach as it is collected or otherwise reasonably becomes available to Syntax.



Notwithstanding the foregoing, Subscriber will be responsible for (i) determining the likely consequences of a Personal Data Breach, (ii) determining if there is any resulting notification or other obligation under Applicable Data Protection Law, and (iii) taking necessary action to comply with those obligations.

7.3 Public Statements. Subscriber agrees to coordinate with Syntax on the content of Subscriber's intended public statements or required notices for the affected Individuals and/or notices to the relevant Regulators regarding the Personal Data Breach. Subscriber shall not make reference to or specifically name Syntax in any public statement or notice without prior written approval by Syntax unless such public statement and the inclusion of Syntax's name therein is required by applicable law.

8. RETURN AND DELETION

8.1 Termination. This DPA will continue in full force and effect until the termination of the Agreement. Upon termination of the Agreement and upon Subscriber's written request, Syntax will promptly return or destroy any remaining copies of Personal Data Processed pursuant to this DPA, in accordance with the procedures set out in the Agreement.

8.2 Data Retrieval. For Personal Data held on Subscriber's systems or environments, or for Services for which no data retrieval functionality is provided by Syntax as part of the Services, Subscriber is solely responsible to take appropriate action to back up or otherwise store separately any Personal Data prior to termination of the Agreement.

9. MISCELLANEOUS

9.1 Conflict. In the event of any conflict or inconsistency between any data privacy provisions set out in the Agreement and this DPA, the DPA shall prevail solely with regard to the Processing of Personal Data.

9.2 Liability. Any provisions excluding or limiting either party's liability under the Agreement shall apply to the liability of each party and each party's Affiliates under this DPA.

9.3 Incorporation by Reference. This DPA shall be deemed incorporated by reference and form an integral part of the Agreement as set out herein and shall apply from the date this DPA was executed by both parties.

9.4 Additional Work. Syntax will invoice Subscriber on a time and materials basis for any work provided under this DPA to the extent that such work is (a) outside of the scope of any applicable Agreement, (b) in excess of what is otherwise required of Syntax pursuant to Applicable Data Protection Law, and (c) that results from any security incident that is not solely and directly caused by Syntax.

According to Art. 28 (3) GDPR

Between

CUSTOMER

- Controller-

and

Syntax Systems GmbH & Co. KG

Hoehnerweg 2-4

69469 Weinheim

Germany

OR

Syntax Information Technology S.L.U.

c/Lluçanés 38, 08022 Barcelona Spain

-Processor-

SECTION 1

Clause 1 | Purpose and scope

- (a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- (b) The controllers and processors listed in Appendix 1 have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.
- (c) These Clauses apply to the processing of personal data as specified in Appendix 2.
- (d) Appendices 1 to 4 are an integral part of the Clauses.
- (e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 | Invariability of the Clauses

- (a) The Parties undertake not to modify the Clauses, except for adding information to the Appendices or updating information in them.
- (b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 | Interpretation

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms

shall have the same meaning as in that Regulation.

- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.
- (c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 | Hierarchy

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

Clause 5 | Optional – Docking clause

- (a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Appendices and signing Appendix 1.
- (b) Once the Appendices in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Appendix 1.
- (c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION 2 – OBLIGATIONS OF THE PARTIES

Clause 6 | Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Appendix 2.

Clause 7 | Obligations of the Parties

7.1. Instructions

- (a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
- (b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Appendix 2, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Appendix 2.

7.4. Security of processing

- (a) The processor shall at least implement the technical and organizational measures specified in Appendix 3 to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of

processing and the risks involved for the data subjects.

- (b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

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

7.6. Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- (c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
- (d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

The processor has the controller's general authorization for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 4 (four) weeks in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

The controller may not unreasonably object to any planned sub-processing. If no agreement can be reached between the controller and the processor after an objection has been made, the controller must refrain from sub-processing by issuing instructions or termination of processing. If the contractually agreed service cannot be provided by the processor without sub-processing, or the services cannot be provided in a reasonable manner, the processor shall have the right to terminate the contract for cause. The termination must be made in writing. All other Statements of Work shall remain unaffected by such termination. If no objection is made within the aforementioned period, the change will be considered accepted.

- (a) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (b) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

- (c) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
- (d) Where possible, the processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

- (a) Any transfer of data to a third country or an international organization by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
- (b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 | Assistance to the controller

- (a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorized to do so by the controller.
- (b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions
- (c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
 - the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
 - the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
 - the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
 - the obligations in Article 32 of Regulation (EU) 2016/679/.

The Parties shall set out in Appendix 3 the appropriate technical and organizational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 | Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

- (a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- (b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:
 - the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - the likely consequences of the personal data breach;
 - the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

- (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- (b) the details of a contact point where more information concerning the personal data breach can be obtained;
- (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Appendix 3 all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION 3 – FINAL PROVISIONS

Clause 10 | Non-compliance with the Clauses and termination

- (a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
- (b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
 - the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
 - the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
 - the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding

its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

- (c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
- (d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Clause 11 | Liability

The controller and processor are liable to affected persons in accordance with the regulation laid out under Art. 82 GDPR.

APPENDIX 1

List of Parties

See Subscriber's SaaS Subscription Agreement for details.

APPENDIX 2

Description of the processing

See Subscriber's SaaS Subscription Agreement for details.

APPENDIX 3

Technical and organizational measures including technical and Organizational measures to ensure the security of the data

1. CONFIDENTIALITY (ART. 32 PARA. 1 LIT. B DSGVO)

Access control: No unauthorized access to data processing equipment.

- SYNTAX buildings in which data processing equipment or data relevant to data protection are stored are secured by magnetic or chip cards or keys or electric door openers, as well as with alarm systems.
- SYNTAX's data centers and housing centers are additionally monitored via plant security or gatekeepers, alarm systems, and video systems. Access is provided via a multi-level security zone model.
- The outside area of the SYNTAX data centers is secured via a singularization gate and two factor authentication (MFA).
- The outdoor area is monitored by means of motion detectors, video surveillance and floodlights.
- The outside area is secured with high fences.
- Access to the data center is secured by means of two-factor authentication (MFA).
- The data center itself is divided into staggered security zones. Access to the computer rooms requires passing through at least three access control points.

- All access control points are strongly secured by means of metal doors.
- Data center access control is independently verified twice a year.

Access control: No unauthorized system use,

- Access to systems is secured via (secure) passwords.
- Access to systems and applications is clearly traceable via the use of individual user IDs in the system or in the PAM.
- In case of multiple incorrect logins, interactive accounts are automatically blocked.
- Administrative access to the operating system, virtualization and network is secured by means of a privileged access management system (PAM), multi-factor authentication (MFA) and personalized accounts.
- Different accounts are used for office IT work and administrative work.
- Access from the Internet is secured via MFA procedures and encrypted connection.
- Each CUSTOMER is protected in its own network area secured by firewall.
- Accesses from the Internet are secured via reverse proxy or WAF (Web Application Firewalls)
- The SYNTAX management infrastructure and back infrastructure is separated from CUSTOMERs and other SYNTAX network structures via firewall.
- Administrative access to systems is separated from SYNTAX IT systems by firewall and terminal server.
- Data carriers of the servers are placed in the strongly secured data centers of SYNTAX.
- Mobile data carriers are encrypted.
- Windows servers in the SYNTAX data centers and managed cloud environments and SYNTAX endpoints are monitored and protected via (EDR) (Endpoint Detection and Response) software. Security-relevant events are processed by a Security Operation Center. (Incident Process)
- The office network only allow an access for authorized devices (IEEE 802.1x)
- Server, network devices are integrated into a central logging system.

Access control - No unauthorized reading, copying, modification or removal within the system,

- Access to systems and applications is clearly traceable via the use of individual user IDs in the system or in the PAM.
- Administrative access to the operating system, virtualization, network and databases is controlled by a granular role concept via a PAM system.
- Access to SAP client 000 is secured by a granular authorization concept.
- SYNTAX operates applications for the CUSTOMER. The authorization concept in the productive applications is the responsibility of the CUSTOMER.
- Administrative access to the operating system, virtualization, network and databases are logged via a PAM system. (Session Logging)
- All data carriers with CUSTOMER data are kept in physically secured data centers or are encrypted.
- All SYNTAX laptops are equipped with a firewall, anti-virus and EDR (Endpoint Detection and Response) software.
- All cloud applications are secured using MFA procedures and encrypted connection.
- The access concepts, as well as the assignment of persons to authorizations, are verified on a regular basis.
- Access logs are collected and analyzed in central SIEM system.
- Data carriers are securely deleted or destroyed after use.
- Files and paper are shredded and destroyed during disposal in accordance with data protection regulations.

Segregation control: Separate processing of data collected for different purposes.

- Operation of application for CUSTOMERs is performed for each CUSTOMER in a separate area.
- The areas are logically separated from each other by means of a firewall.
- Tests of the SYNTAX itself are performed in SYNTAX own environments.
- As part of Managed Service, SYNTAX can provide the CUSTOMER with a multi-level application environment, separated into development, test and productive environments. In this, the CUSTOMER can test their own processing logic in separate environments. (e.g. SAP Prod, SAP QA and SAP Dev environment).

Pseudonymization (Art. 32(1)(a) GDPR; Art. 25(1) GDPR)

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures;

- SYNTAX only operates systems or applications in which the data is processed by the CUSTOMER as part of the managed service. In these applications, the pseudonymization method is not used or must be implemented by the client.
- SYNTAX processes data within the scope of AMS and consulting only on the instruction of the client. In this case, the client must specify the type of pseudonymization.

2. INTEGRITY (ART. 32 PARA. 1 LIT. B DSGVO)

Transfer control: No unauthorized reading, copying, modification or removal during electronic transmission

- Data is transmitted over physically secured lines or encrypted connections.
 - In the case of email, the communication is secured via TLS according to the respective state of the art.
- The transmission of data via the Internet is done using encrypted protocols.
- All transition points between network zones are secured via firewall.
- All transmission paths must be explicitly enabled. (Whitelist Approach)
- Accesses to systems, if this is the responsibility of SYNTAX, are logged.
- If data carriers are shipped, they are transported in secure containers. Dispatch is carried out by reliable service providers. Receipt is documented.
- Old data carriers are disposed of via a data protection system.

Access to services / sites on the Internet is protected via DNS Security Proxy or http Proxy.

Input control Determining whether and by whom personal data have been entered into, modified or removed from data processing systems.

- SYNTAX documents the orders and their execution in the SYNTAX ticket system.
- Administrative access to the operating system, virtualization, network and databases are logged via a PAM system.
- The settings for logging in the CUSTOMER's SAP applications are the responsibility of the CUSTOMER.

3. AVAILABILITY AND RESILIENCE (ART. 32 PARA. 1 LIT. B DSGVO)

Availability control Protection against accidental or deliberate destruction or loss,

Backup

- The CUSTOMER's data is backed up at least daily unless otherwise contractually agreed.
- The execution of the backup is monitored automatically.
- Backups of application in the data centers are stored in a second data center at least 1 km away.
- The recovery is tested exemplary per procedure at least once a year.
- The backup strategy is independently reviewed at least twice a year.

Availability

- Building:
 - SYNTAX has several data centers. Whereby two data centers have a distance of 1km or a distance greater than 20km from each other.
 - The cooling and power supply is designed with at least n+1 redundancy.
 - The data centers have an uninterruptible power supply with battery buffering and emergency generator.
 - The emergency power supply is tested approximately 10 times per year.
 - The UPS system, emergency power system is tested once a year in a black circuit.
 - Performance of proper maintenance is independently verified twice per year.
 - The data centers are equipped with an early fire detection system and an automatic (gas) extinguishing system that enables fires to be extinguished without further damage to other equipment.
 - The building and the rooms among them are designed to be fireproof.
 - The doors between the rooms are designed C90 fireproof.
 - The buildings are designed to be earthquake resistant according to the earthquake risk analysis.
 - The buildings are positioned so that they are not at risk from a flood.
- Components
 - All servers and network components and storage subsystems in the data centers are connected with redundant network, SAN and power supply.
 - All components are monitored centrally and automatically.
 - All data is always backed up via RAID (redundant storage on different disks / SSD).

- SYNTAX offers synchronous or asynchronous mirroring of all data between two data centers, in addition to standard backup mirroring, as an option
- Access to the Internet is redundant via 3 providers and via 3 data centers.
- The network lines between the data centers are redundant.
- Incidents are resolved by means of certified incident (ISO 20000-1)
- The cause of malfunctions is analyzed using the Probenmanagement process (ISO 20000-1) and the cause of the malfunction is eliminated.
- Malfunction and delivery processes are analyzed daily by Operational Management (overall) (Morning Call)
- Windows servers in the SYNTAX data centers and managed cloud environments and SYNTAX endpoints are monitored and protected via (EDR) (Endpoint Detection and Response) software. Security-relevant events are processed by a security operation center.

4. PROCEDURES FOR REGULAR REVIEW, ASSESSMENT AND EVALUATION (ART. 32(1)(D) GDPR; ART. 25(1) GDPR)

Order Control:

Use of subcontractors only after

- Conclusion of the necessary order processing agreement or EU standard contractual clauses.
- Written instructions to the contractor
- Agreement of organizational and technical measures suitable for the service
- Agreement on effective control rights vis-à-vis the contractor
- Obligation of the contractor's employees to maintain confidentiality about the framework agreement.
- Only recordings from suppliers with certified security or with audit reports by independent third parties
- Regulation on the use of further subcontractor
- In case of longer cooperation: Ongoing review of the contractor and its level of protection through verification of certification or new request for audit reports from independent third parties

Privacy Management:

- SYNTAX has appointed a data protection officer who monitors the data protection management system. SYNTAX commits its employees to data secrecy and trains them regularly regarding the requirements of the GDPR.
- SYNTAX has additionally established and had certified its technical organizational measures for the protection of data in accordance with ISO 27001 and TISAX.
- The safety officer reports directly to the SYNTAX management.
- The Security Officer oversees the work of SYNTAX's Security Operation Center.

Incident Response Management:

- SYNTAX has established a process for responding to security incidents. The process is certified in accordance with TISAX, ISO 27001 and ISO 20000-1. In the event of a data breach, SYNTAX's Data Protection Officer coordinates the response.

Data protection-friendly default settings (Art. 25 (2) DS-GVO)

- SYNTAX delivers applications and systems that are configured in such a way that they provide sufficient protection from cyber threats and are focused on data economy.
- As a rule, SYNTAX only operates the application platform.

APPENDIX 4

List of sub-processors

The list of sub-processors published on our website applies, which is located in its current version here: <https://www.syntax.com/de-de/datenschutz/#data-protection>.

This list will be updated accordingly if new sub-processors are engaged to provide services. Syntax will inform you about the use of a new sub-processor in accordance with the provisions of Section [7.7](#) of this Data Processing Agreement.

For France Customers

PREAMBLE

See Subscriber's SaaS Subscription Agreement for details.

§ 1 Scope, duration and specification of contract processing of Data

See Subscriber's SaaS Subscription Agreement for details.

§ 2 Scope of application and responsibilities

- (1) Supplier shall process Data on behalf of Company. Such Contract Processing shall include all activities detailed in the Agreement and its statement of work. Within the scope of this annex, Company shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Supplier and the lawfulness of having Data processed on behalf of Company. Company shall be the «controller» in accordance with Article 4 no. 7 of the GDPR.
- (2) Company's individual instructions on Contract Processing shall, initially, be as detailed in the Agreement. Company shall, subsequently, be entitled to, in writing or in a machine-readable format (in text form*), modifying, amending or replacing such individual instructions by issuing such instructions to the point of contact designated by Supplier. Instructions not foreseen in or covered by the Agreement shall be treated as requests for changes to the statement of work. Company shall, without undue delay, confirm in writing or in text form any instruction issued orally.

§ 3 Supplier's obligations

- (1) Except where expressly permitted by Article 28 (3) (a) of the GDPR, Supplier shall process data subjects' Data only within the scope of the statement of work and the instructions issued by Company. Where Supplier believes that an instruction would be in breach of applicable law, Supplier shall notify Company of such belief without undue delay. Supplier shall be entitled to suspending performance on such instruction until Company confirms or modifies such instruction.
- (2) Supplier shall, within Supplier's scope of responsibility, organise supplier's internal organisation so it satisfies the specific requirements of data protection. Supplier shall implement technical and organisational measures to ensure the adequate protection of Company's Data, which measures shall fulfil the requirements of the GDPR and specifically its Article 32. Supplier shall implement technical and organisational measures and safeguards that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. Company is familiar with these technical and organisational measures, and it shall be Company's responsibility that such measures ensure a level of security appropriate to the risk (s. Anlage).

Supplier reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.
- (3) Supplier shall support Company, insofar as is agreed upon by the parties, and where possible for Supplier, in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 33 to 36 of the GDPR.
- (4) Supplier warrants that all employees involved in Contract Processing of Company's Data and other such persons as may be involved in Contract Processing within Supplier's scope of responsibility shall be prohibited from processing Data outside the scope of the instructions. Furthermore, Supplier warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.
- (5) Supplier shall notify Company, without undue delay, if Supplier becomes aware of breaches of the protection of personal data within Supplier's scope of responsibility. Supplier shall implement the measures necessary for securing Data and for mitigating potential negative consequences for the data subject; the Supplier shall coordinate such efforts with Company without undue delay.
- (6) Supplier shall notify to Company the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR.

- The Company shall be informed of his/her contact details for the purpose of direct contact. The Company shall be informed immediately of any change of Data Protection Officer.
 - His/Her current contact details are always available and easily accessible on the website of the Supplier.
- (7) Supplier warrants that Supplier fulfils its obligations under Article 32 (1)(d) of the GDPR to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- (8) Supplier shall correct or erase Data if so instructed by Company and where covered by the scope of the instructions permissible. Where an erasure, consistent with data protection requirements or a corresponding restriction of processing is impossible, Supplier shall, based on Company's instructions, and unless agreed upon differently in the Agreement, destroy, in compliance with data protection requirements, all carrier media and other material or return the same to Company. In specific cases designated by Company, such Data shall be stored or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Agreement.
- (9) Supplier shall, upon termination of Contract Processing and upon Company's instruction, return all Data, carrier media and other materials to Company or delete the same.
- (10) Where a data subject asserts any claims against Company in accordance with Article 82 of the GDPR, Supplier shall support Company in defending against such claims, where possible.

§ 4 Company's obligations

- (1) Company shall notify Supplier, without undue delay, and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by Company in the results of Supplier's work.
- (2) Section 3 para. 11 above shall apply to claims asserted by data subjects against Supplier in accordance with Article 82 of the GDPR.
- (3) Company shall notify to Supplier the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

§ 5 Enquiries by data subjects

Where a data subject asserts claims for rectification, erasure or access against Supplier, and where Supplier is able to correlate the data subject to Company, based on the information provided by the data subject, Supplier shall refer such data subject to Company. Supplier shall forward the data subject's claim to Company without undue delay. Supplier shall support Company, where possible, and based upon Company's instruction insofar as agreed upon. Supplier shall not be liable in cases where Company fails to respond to the data subject's request in total, correctly, or in a timely manner.

§ 6 Options for documentation

- (1) Supplier shall document and prove to Company Supplier's compliance with the obligations agreed upon in this exhibit by appropriate measures.
- Where specific types of documentation and proof can be identified, with regard to compliance with the obligations agreed upon, Supplier may make available to Company the following information:
- Conducting an own self-audit, or
 - Certifications on data protection and/or information security according to ISO 27001.
- (2) Where, in individual cases, audits and inspections by Company or an auditor appointed by Company are necessary, such audits and inspections will be conducted at Controller's costs and during regular business hours, and without interfering with Supplier's operations, upon prior notice, and observing an appropriate notice period. Supplier may also determine that such audits and inspections are subject to prior notice, the observation of an appropriate notice period, and the execution of a confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and organisational measures and safeguards implemented. Supplier shall be entitled to rejecting auditors, which are competitors of Supplier.
- (3) Where a data protection supervisory authority or another supervisory authority with statutory competence for Company conducts an inspection, para. 2 above shall apply. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

§ 7 Subcontracting

- (1) Supplier shall use subcontractors as further processors on behalf of Company only where approved in advance by Company.

Subcontracting for the purpose of this Agreement is to be understood as meaning services, which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services, tools for supporting internal processes (e.g. ticket-system), examination performances or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Company's data, even in the case of outsourced ancillary services.

Supplier will conduct the performance agreed upon, or the parts of the performance identified in Appendix "Subcontractors", using the subcontractors enumerated in before mentioned Appendix.

Supplier shall obtain Company's consent prior to the use of new or the replacement of existing subcontractors. Company shall be entitled to withholding consent only for material reasons related to statutory data protection regulations.

- (2) Where Supplier commissions subcontractors, Supplier shall be responsible for ensuring that Supplier's obligations on data protection resulting from the Agreement and this exhibit are valid and binding upon subcontractor.

§ 8 Obligations to inform, mandatory written form, choice of law

- (1) Where the Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Supplier's control, Supplier shall notify Company of such action without undue delay. Supplier shall, without undue delay, notify to all pertinent parties in such action, that any data affected thereby is in Company's sole property and area of responsibility, that data is at Company's sole disposition, and that Company is the responsible body in the sense of the GDPR.
- (2) No modification of this annex and/or any of its components – including, but not limited to, Supplier's representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form), and furthermore only if such modification expressly states that such modification applies to the regulations of this annex. The foregoing shall also apply to any waiver or modification of this mandatory written form.
- (3) In case of any conflict, the data protection regulations of this annex shall take precedence over the regulations of the Agreement. Where individual regulations of this annex are invalid or unenforceable, the validity and enforceability of the other regulations of this annex shall not be affected.

Technical and Organisational Measures

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

- **Physical Access Control** - No unauthorised access to Data Processing Facilities, through magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems.
- **Electronic Access Control** - No unauthorised use of the Data Processing and Data Storage Systems, through (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication for network connections, encryption of data carriers/storage media.
- **Internal Access Control** (permissions for user rights of access to and amendment of data) - No unauthorised Reading, Copying, Changes or Deletions of Data within the system, through rights authorisation concept, need-based rights of access, logging of system access events.
- **Isolation Control** - The isolated Processing of Data, which is collected for differing purposes, through multiple client support or sandboxing.
- **Pseudonymisation** (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR) - The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

2. **Integrity (Article 32 Paragraph 1 Point b GDPR)**

- **Data Transfer Control** - No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, through Encryption, Virtual Private Networks (VPN), electronic signature after customer requirement.
- **Data Entry Control** - Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, through Logging, Document Management.

3. **Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)**

- **Availability Control** - Prevention of accidental or wilful destruction or loss, through Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning.
- **Rapid Recovery** (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR)

4. **Procedures for regular testing, assessment and evaluation
(Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)**

- **Data Protection Management**
- **Incident Response Management**
- **Data Protection by Design and Default** (Article 25 Paragraph 2 GDPR)
- **Order or Contract Control** - No third-party data processing as per Article 28 GDPR without corresponding instructions from the Company, through clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.