Master Services Agreement

This Master Services Agreement is entered into by and between the relevant Provider entity and the Customer entity, each as set out in an applicable Order Form ("**Provider**" and "**Customer**", each also referred to as a "**Party**" and collectively as the "**Parties**") as of the Effective Date. This Services Agreement, its applicable Schedules, an applicable Order Form, including any Document incorporated therein and any applicable amendment (collectively the "**Agreement**") constitute the entire agreement between the Parties with respect to the Customer's purchase and use of the Services.

When incorporated by reference, this Agreement shall govern the provision of the Services by Provider to Customer.

Now therefore, the Parties agree as follows:

1. Definitions

Any capitalized terms not otherwise defined in the Agreement have the meanings set out below. Any reference to the singular includes a reference to the plural and vice versa, unless expressly otherwise provided in this Agreement, and any reference to the masculine includes a reference to the feminine and vice versa, and (unless the context clearly indicates the contrary) the words "including" and "in particular" shall be deemed to be followed by the words "without limitation".

Affiliate	As used in relation to any Persons means any other Person that, directly or indirectly, controls, is controlled by, or is under common control with, such first Person; provided in any event that the holding of more than 50% of the capital or voting rights in another Person or the power to, directly or indirectly and by whichever means, direct, or cause the direction of, the management of another Person shall irrefutably be deemed to confer 'control' over such Person, provided, that, any direct or indirect shareholders of the Parties and their Affiliates (that are not subsidiaries of the Parties) and any fund directly or indirectly holding an interest in the one of the Parties or otherwise affiliated with the a Party or with an aforementioned fund, or operating/portfolio entities in which any such fund directly or indirectly holds an interest, shall not be deemed to be an Affiliate of the relevant Party
Confidential Information	Information of a party concerning its business and/or affairs, including without limitation to information relating to a party's operations, technical or commercial know-how, specifications, inventions, processes or initiatives, plans, product information, pricing information, know-how, designs, trade secrets, software, documents, data and information which, when provided by a party to the other: a) are clearly identified as "Confidential" or "Proprietary" or are marked with a similar legend; b) are disclosed orally or visually, identified as Confidential Information at the time of disclosure and confirmed as Confidential Information in writing within 10 days; or c) a reasonable person would understand to be confidential or proprietary at the time of disclosure. Details of the Provider Software, Documentation, Services, Provider Data, the Pricing and other Customer-specific commercial terms subject to the applicable Order Form,

	feedback on the Services and the results of any performance tests of the Services, constitute Provider's Confidential Information
Effective Date	The date this Agreement takes effect, which is the date of the last signature of the Parties to the applicable Order Form incorporating this Agreement by reference
Force Majeure Event	Acts, events, omissions or accidents beyond a party's reasonable control, including, without limitation, strikes, lock-outs or other industrial disputes, failure of a utility service or transport or telecommunications network, act of God, war, riot, civil commotion, malicious damage, fire, flood or storm; Notwithstanding the foregoing, as the Services are provided virtually, a government mandated office location or other work closure shall not constitute Force Majeure unless such Force Majeure also involves significant interruption of telecommunications or internet service
Initial Subscription Term	The period for which a Subscription is purchased initially, as set out in an applicable Order Form.
Order Form	An order document document or statement of work that is signed by the Parties, incorporating this Agreement by reference and setting out the commercial specifications of the Agreement, in particularly regarding Provider, the purchased Services and the Scope.
Professional Services	The in-person Services provided by Provider to assist Customer in its use of the Solutions, as set in an applicable Order Form.
Renewal Term	Such period for which a Subscription auto-renews, as set out in section 6.2 of the Master Services Agreement.
Schedule	Any document incorporated by reference or otherwise included in the Agreement that the Parties agree to further specify the rights and obligations agreed under the Agreement that may or may not be signed by the Parties and may or may not be titled schedule
Scope	the scope of Customer's use of the Services as set out in applicable Order Form and this Agreement;

Scoping Document	A document used by the Parties to assess and specify Customer's technical needs and requirements and for the Provider to generate the offer and Order Form. A Scoping Document is typically used only to assess the technical background needed to prepare the offer, whereas the contractual, commercial specifications will be detailed exclusively in an applicable Order Form based on standardized Subscriptions and/or Service Packages. If a Customer requires the provision of non-standard Professional Services, this must be agreed and the Scoping Document shall be attached to the relevant Order Form.
Services	The enterprise product to consumer cloud software Solutions and certain additional Professional Services, such as, but not limited to, implementation, onboarding, data migration, managed services and support services, in each case as further defined in this Agreement, its applicable Schedules and an applicable Order Form
Subscription	Services purchased for a fixed period, as set out in an applicable Order Form
Term	Collectively means the Initial Subscription Term and the Renewal Term, as set out in section 6.2 of the Master Services Agreement.

2. Services

2.1 This Agreement governs the provision of certain enterprise product to consumer cloud software Solutions and certain additional Professional Services, such as, but not limited to, implementation, onboarding, data migration, managed services and support services, in each case as further defined in this Agreement, its applicable Schedules and an applicable Order Form (collectively the "**Services**"), from Provider to Customer.

2.2 The Services set out under this Agreement are services provided by or on behalf of the Productsup Group ("**Productsup**") to its customers and/or authorized partners, in each case as further defined in this Agreement. They may be provided to Customer by any Affiliate of Productsup or by an authorized Partner. The relevant Provider entity will be set out in an applicable Order Form.

2.3 Solutions

Solutions shall be provided in accordance with the applicable Solutions Schedule.

2.4 Professional Services

Productsup Professional Services shall be provided in accordance with the Professional Services Schedule.

3. Purchase and Scope, Provision of Services

Customer and Provider shall enter into an Order Form specifying (i) the Customer; (ii) the Provider of each of the Services; (iii) the relevant terms and conditions that shall form the Agreement and govern the provision of the Services; (iv) the Scope of the Customer's purchase of the Services from the Provider and (v) such other relevant terms and conditions of the purchase, as further set out in this Agreement. An applicable Order Form may reference different Providers regarding the provision of certain Services. The Provider shall provide the Services, as set out in the applicable Order Form and in this Agreement. The provision of the Services will commence on the relevant date set out in the applicable Order Form. Order Forms shall be created on the basis of a Scoping Document filled out by Customer, which Provider shall use to assess the required Sevrices and Scope.

4. Warranty

4.1 Provider warrants that, throughout the Term, the Services will be provided and will function substantially in accordance with the specifications and service levels set out in any applicable Schedule, including the applicable Documentation, in the Scope set forth in an applicable Order Form and any applicable Schedule, and that the Services will be delivered with reasonable skill and care.

4.2 The warranties provided in this section shall not apply to the extent of any non-conformance which is caused by:

4.2.1 Customer's use of the Services contrary to Provider's instructions, the applicable Documentation or otherwise in breach of the Agreement; or

4.2.2 modification or alteration of the Services by any party other than Provider or on behalf of Provider by Provider's duly authorized contractors or agents.

4.3 If the Services do not conform with the warranty provided in this section, Provider will, at its expense, (i) use commercially reasonable efforts to correct any such non-conformance within a reasonable period of time; or (ii) provide the Customer with an alternative means of accomplishing the desired performance.

4.4 Notwithstanding the foregoing, Provider:

4.4.1 does not warrant that Customer's use of the Services will be uninterrupted or error-free, or that the Services, applicable Documentation or the information obtained by Customer through the Services will meet Customer's requirements; and

4.4.2 is not responsible for any Virus which was not detected by Provider using reasonable current commercial methods of detection or transmitted through any third-party services other than third party-services provided by Provider's duly authorized contractors or agents.

4.5 EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS SECTION 4, PROVIDER (AND ITS AFFILIATES) TO THE EXTENT PERMITTED BY APPLICABLE LAW, DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, ACCURACY, CORRESPONDENCE WITH DESCRIPTION, FITNESS FOR A PARTICULAR PURPOSE OR USE, AND SATISFACTORY QUALITY, AND NON-INFRINGEMENT.

4.6 This Agreement shall not prevent Provider from entering into similar agreements with third parties, or from independently developing, using, selling or licensing documentation, products and/or services which are similar to those provided under the Agreement.

5. Fees and Payment Terms

5.1 Invoicing and Payment

5.1.1 Provider will invoice Customer for the fees as specified in an applicable Order Form. The invoices of Provider are due for payment (i) within the time frame, (ii) in the currency and (iii) in the method agreed upon in an applicable Order Form. If Customer is in default repeatedly, Provider reserves the right to, in its sole discretion, accept payments from Customer via credit card or direct debit only. Customer acknowledges and agrees that it is obliged to transition its payment mode in this case.

5.1.2 All fees are exclusive of all taxes and may not be reduced to account for any taxes, including sales, value-added, use, excise, or withholding taxes imposed by any governmental entity in connection with the Services (excluding taxes based solely on Provider's income). Customer shall be solely responsible to pay all applicable Taxes relating to the Fees. In the event Provider invoices Customer for any such taxes, Customer shall pay all taxes invoiced by Provider.

5.1.3 If Provider has not received payment for any invoices which are not the subject of a bona fide dispute by the due dates and without prejudice to any other rights and remedies of Provider, Provider may (i) by giving fourteen (14) days prior written notice to Customer, may suspend the provision of or the access to any Services and shall be under no obligation to provide any or all of the Services while the applicable invoice(s) remain unpaid; and (ii) charge interest which shall accrue on past due amounts at the standard statutory interest rate under applicable law.

5.2 Increase of Fees

5.2.1 For each Renewal Term, all fees due under this Agreement or any applicable Order Form shall automatically increase at an annual rate of 5% or the consumer price index (overall average) as published by the German Federal Statistical Office (*Statistisches Bundesamt*) (CPI) (whichever is higher).

5.2.2 In the case of a sudden, unforeseen and significant increase of the costs required to provide the Services, Provider is entitled to increase the fees such Services by a written notice with a notice period of ninety (90) days to the end of a month, provided that: (i) Provider cannot otherwise provide the Services in an economically reasonable manner (even in consideration of any eventual profits); (ii) the increase in costs is arising from a sphere out of Provider's reasonable control; and (iii) the fees are increased only insofar as it is necessary to provide the Services without incurring significant losses.

6. Term and Termination

6.1 This Agreement shall commence on the Effective Date and shall continue to be in effect until the expiration of the Term of any applicable Order Form (or until all Services have been provided, if later) unless otherwise terminated as provided in this section.

6.2 Each Subscription purchased under an Order Form shall commence on the date specified in the Order Form and shall continue for the Initial Subscription Term set out in the Order Form. Thereafter, unless stated otherwise in the applicable Order Form, the Subscription shall automatically renew for successive periods of twelve (12) months (or such other period as specified in the applicable Order Form) (each a "**Renewal Term**" and collectively the "**Term**"), unless either Party terminates with not less than three (3) months' written notice prior to the end of the Initial Subscription Term or relevant Renewal Term or otherwise terminates in accordance with the provisions of this section. At the end of the Term, Customer's access and use of the Services shall automatically terminate.

6.3 Without prejudice to any other rights or remedies to which the Parties may be entitled, either Party may terminate this Agreement or an applicable Order Form without liability to the other at any time with immediate effect upon written notice if the other Party:

6.3.1 is in material breach of any of its obligations under the Agreement and, in the case of a breach which is capable of remedy, fails to remedy such breach within thirty (30) days following notice of the breach; or

6.3.2 files, or has filed against it, a petition of bankruptcy or insolvency, and the petition is not vacated within sixty (60) days being filed; or shall have a receiver or administrative receiver appointed over it or any of its assets; or shall pass a resolution for winding-up or dissolution of the business affairs of an entity; or if the other Party shall become subject to an administration order or shall enter into any voluntary arrangement with its creditors or shall cease or threaten to cease to carry on business; or is subject to any analogous event or proceeding in any applicable jurisdiction.

6.4 On termination or expiration of this Agreement or an applicable Order Form for any reason, (i) Customer's rights of use granted under this Agreement (or under the applicable Order Form in the case of termination of an individual Order Form only) shall immediately terminate and Customer shall immediately cease the use of the Services; (ii) Customer shall pay all fees due or to become due through the effective date of termination in respect of the Services that are subject to termination; and (iii) Provider shall refund on a pro-rata basis any fees paid by Customer in advance for the Services that are subject to termination for any period following the effective date of termination.

7. Confidentiality

7.1 Each Party may be given access to Confidential Information from the other Party in order to perform its obligations under the Agreement. A Party's Confidential Information shall not be deemed to include information that:

7.1.1 is or becomes publicly known other than through any act or omission of the receiving party;

7.1.2 was in the receiving party's lawful possession before the disclosure;

7.1.3 is lawfully disclosed to the receiving party by a third party without restriction on disclosure;

7.1.4 is independently developed by the receiving party, which independent development can be shown by written evidence; or

7.1.5 is required to be disclosed by law, by any court of competent jurisdiction or by any regulatory or administrative body.

7.2 Each Party shall hold the other's Confidential Information in confidence and, unless required by law, not make the other's Confidential Information available to any third party except its employees, contractors, third-party service providers and advisors who have a need to know and are bound by confidentiality obligations no less restrictive than this section, or use the other Party's Confidential Information for any purpose other than the implementation of the Agreement.

7.3 Except where a Party is expressly required by law to retain a copy, on termination of the Agreement and when requested to do so in writing by the disclosing party, the receiving party shall promptly: (i) deliver to the disclosing party any documents and other materials in its possession or control that contain any of the Confidential Information; (ii) permanently delete, destroy and/or erase all electronic copies of the Confidential Information from any computer or data storage system into which the Confidential Information was entered; and (iii) make no further use of the Confidential Information.

7.4 The receiving party, if requested by the disclosing party, shall confirm in writing that the provisions of section have been complied with. The obligations of confidentiality under this section shall survive any expiration or termination of the Agreement.

8. Limitation of Liability

8.1 EXCEPT WITH RESPECT TO AMOUNTS OWED BY CLIENT TO PROVIDER HEREUNDER, THE AGGREGATE LIABILITY OF EACH PARTY FOR OR IN RESPECT OF ANY LOSS OR DAMAGE SUFFERED BY THE OTHER PARTY (WHETHER DUE TO BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE) UNDER OR IN CONNECTION WITH THE AGREEMENT IN ANY CLAIM YEAR SHALL BE LIMITED TO THE TOTAL AMOUNT OF FEES PAID BY CLIENT DURING SUCH CLAIM YEAR.

8.2 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR SPECIAL, CONSEQUENTIAL, INCIDENTAL OR OTHER INDIRECT DAMAGES, OR FOR LOSS OF PROFITS, ANTICIPATED SAVINGS, BUSINESS OPPORTUNITY, GOODWILL, OR LOSS OF REVENUE, LOSS OF USE OR LOSS OF DATA (INCLUDING CORRUPTION OF DATA), OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES ARISING OF THE AGREEMENT, HOWSOEVER CAUSED AND UNDER ANY THEORY OF LIABILITY (INCLUDING CONTRACT, TORT, NEGLIGENCE OR OTHERWISE) EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE PARTIES ACKNOWLEDGE THAT THE AMOUNTS PAYABLE HEREUNDER ARE BASED IN PART ON THESE LIMITATIONS AND FURTHER AGREE THAT THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. PRODUCTSUP ACCEPTS NO LIABILITY FOR FAILURE TO MAINTAIN ANY LEVEL OF AVAILABILITY OF THE SERVICES OTHER THAN WHERE IT IS IN BREACH OF ITS OBLIGATIONS UNDER THE AGREEMENT.

8.3 IN ADDITION TO THE OTHER EXCLUSIONS SET OUT IN THIS SECTION 8, PROVIDER HAS NO LIABILITY:

8.3.1 FOR ANY OTHER THIRD PARTY PRODUCTS OR SERVICES ACCESSED AND/OR USED BY CLIENT THROUGH THE SERVICES;

8.3.2 WHERE ANY FAILURE TO PROVIDE THE SERVICES IS CAUSED BY A NETWORK, HARDWARE OR SOFTWARE FAULT IN EQUIPMENT WHICH IS NOT UNDER THE CONTROL OF PROVIDER;

8.3.3 ANY ACT OR OMISSION OF CLIENT;

8.3.4 USE OF THE SERVICES IN BREACH OF THE AGREEMENT;

8.3.5 ANY UNAUTHORIZED ACCESS TO THE SERVICES INCLUDING A MALICIOUS SECURITY BREACH; OR

8.3.6 LOSS OR DAMAGE CAUSED BY CLIENT'S DELAY OR FAILURE TO TIMELY PROVIDE ANY REQUIRED INFORMATION OR TO FULFIL ITS OBLIGATIONS UNDER THE AGREEMENT.

8.4 IN THE EVENT OF ANY LOSS OR DAMAGE TO CLIENT DATA, CLIENT'S SOLE AND EXCLUSIVE REMEDY SHALL BE AS SET OUT THE PRODUCTSUP SOLUTIONS SCHEDULE AVAILABLE AT https://www.productsup.com/legal/.

8.5 CLIENT ASSUMES SOLE RESPONSIBILITY FOR RESULTS OBTAINED FROM THE USE OF THE SERVICES AND THE DOCUMENTATION BY CLIENT, AND FOR CONCLUSIONS DRAWN FROM SUCH USE. PROVIDER SHALL HAVE NO LIABILITY FOR ANY DAMAGE CAUSED BY ERRORS OR OMISSIONS IN ANY INFORMATION, DATA OR INSTRUCTIONS PROVIDED TO PROVIDER BY CLIENT IN CONNECTION WITH THE SERVICES OR ANY ACTIONS TAKEN BY PROVIDER AT CLIENT'S DIRECTION.

8.6 PROVIDER DOES NOT AND CANNOT CONTROL THE FLOW OF DATA TO OR FROM THE NETWORK WHERE THE SERVICES RESIDE AND OTHER PORTIONS OF THE INTERNET INCLUDING DENIAL OF SERVICE ATTACKS (AN ATTACK WHICH SEND A FLOOD OF INCOMING MESSAGES TO THE TARGET SYSTEM FORCING THE SYSTEM TO SHUT DOWN, THEREBY DENYING SERVICE TO LEGITIMATE USERS). SUCH FLOW DEPENDS IN LARGE PART ON THE PERFORMANCE OF INTERNET SERVICES PROVIDED OR CONTROLLED BY THIRD PARTIES. AT TIMES, ACTIONS OR INACTIONS OF SUCH THIRD PARTIES CAN IMPAIR OR DISRUPT CLIENT'S CONNECTIONS TO THE INTERNET (OR PORTIONS THEREOF). PROVIDER CANNOT GUARANTEE THAT SUCH EVENTS WILL NOT OCCUR. ACCORDINGLY, PROVIDER, ITS SUPPLIERS AND SUBCONTRACTORS, IF ANY, DISCLAIM ANY AND ALL LIABILITY RESULTING FROM OR RELATED TO SUCH EVENTS AND CLIENT SHALL HAVE NO CLAIM IN RESPECT THEREOF.

8.7 PROVIDER SHALL HAVE NO LIABILITY TO CLIENT UNDER THE AGREEMENT IF IT IS PREVENTED FROM OR DELAYED IN PERFORMING ITS OBLIGATIONS UNDER THE AGREEMENT DUE TO A FORCE MAJEURE EVENT. PRODUCTSUP SHALL PROVIDE CLIENT WITH NOTICE OF A FORCE MAJEURE EVENT AND ITS EXPECTED DURATION.

8.8 EACH PARTY RECOGNIZES AND AGREES THAT THE WARRANTY DISCLAIMERS AND LIABILITY AND REMEDY LIMITATIONS IN THE AGREEMENT ARE MATERIAL, BARGAINED FOR BASES OF THE AGREEMENT, AND THAT THEY HAVE BEEN TAKEN INTO ACCOUNT AND REFLECTED IN DETERMINING THE CONSIDERATION TO BE GIVEN BY EACH PARTY UNDER THE AGREEMENT AND IN THE DECISION BY EACH PARTY TO ENTER INTO THE AGREEMENT.

9. Marketing

9.1 Customer Logo Usage by Provider

Unless explicitly excluded from the scope of the Agreement in an applicable Order Form, Customer agrees that Provider and its Affiliates may publish Customer's name and logo in its Customer lists, and promotional, marketing and investment materials, in any media and grants Provider a non-exclusive, revocable, unlimited license for the described purpose. Any use of Customer's name and logo shall be in accordance with the applicable brand guidelines as notified by Customer from time to time.

9.2 Further Marketing Cooperation

If explicitly agreed and further specified in an applicable Order Form, Customer will co-operate with Provider in producing any press releases, case studies or other marketing materials regarding the supply of the Services to Customer.

10. General

10.1 **Force Majeure.** Neither Party shall be liable for any delay in performing or failure to perform its obligations under this Agreement to the extent that and for so long as the delay or failure results from a Force Majeure Event provided that the relevant affected Party shall (i) promptly upon becoming aware of the occurrence of the Force Majeure Event inform the other Party with detail of the circumstances giving rise to the Force Majeure Event and its anticipated duration and effects on the obligations; and (ii) take all reasonable steps to comply with the terms of this Agreement as fully and promptly as possible.

10.2 **Entire Agreement**. The Agreement sets out the entire agreement and understanding between the Parties and supersedes any previous agreement between the Parties relating to its subject matter. Unless otherwise expressly agreed in writing, the Agreement applies in place of and prevails over any terms or conditions contained in or referred to in (i) any Customer purchase order or general terms and conditions; (ii) any correspondence; or (iii) elsewhere or implied by trade custom or course of dealing. In entering into the Agreement each Party acknowledges and agrees that it has not relied on any representations made by the other. Any such representations are excluded. Nothing in this section shall limit liability for any representations made fraudulently.

10.3 **Warranty of Authority**. Each Party represents and warrants to the other that it is duly organized, validly existing and in good standing under the laws of the jurisdiction of its organization, and has the requisite power and authority to execute, deliver and perform its obligations under the Agreement. Each Party represents and warrants to the other that the Agreement has been duly authorized, executed and delivered by such Party and constitutes a valid and binding obligations of such Party enforceable against such party according to its terms.

10.4 **Governing Law and Jurisdiction**. The Agreement and any disputes or claims arising out of or in connection with it, its subject matter or formation (including non-contractual disputes or claims) shall be governed by the laws of New South Wales without reference to conflicts of laws principles. The Parties agree that any disputes under the Agreement shall be subject to the exclusive jurisdiction of the courts in Sydney.

10.5 **Third Party Rights**. A person who is not a party to the Agreement has no rights to enforce, or to enjoy the benefit of, any term of the Agreement.

10.6 **Subcontracting and Assignment**. Provider may at any time involve any of its Affiliates, successors or assigns as subcontractors under the Agreement. Provider may, at any time by notice in writing to the Customer, assign or otherwise transfer its rights and obligations under the Agreement to any of its Affiliates, successors or assigns. Provider shall have the right to subcontract any of its obligations under the Agreement to a third party, provided that Provider shall continue to remain responsible for the performance of the Services. Customer may by notice in writing to Provider assign, or otherwise transfer its rights and obligations under the Agreement in full (but not in part) to an Affiliate provided that such Affiliate is at least of the same financial standing as Customer. Any attempted assignment, sub-contracting or other transfer in violation of the Agreement shall be null and void.

10.7 **Notices**. All notices to be given under the Agreement shall be given in English or German in writing via email or in writing by courier, by fax, or by certified or registered mail, to the contact set forth in an applicable Order Form with copy to the legal department at the address stated in the applicable Order Form, or to such other address as shall be given by either Party to the other in writing. All notices shall be deemed to have been given and received upon the date of actual receipt.

10.8 **Variations**. Save as otherwise expressly stated in this Agreement, this Agreement, its Schedules, an Order Form or a Scoping Document may only be modified or varied in writing executed by duly authorized representatives of both Parties through an amendment to this Agreement or an applicable Order Form. This also applies to any modifications of this section 16.7.

10.9 **Changes to the Agreement**. Notwithstanding anything in section 16.8, Provider may change the Agreement, provided that the change does not have any material impact on the contractual rights and obligations between the Parties, upon four weeks' notice to Customer and such change shall be deemed effective, if Customer does not expressly objects to such change withing the four weeks' notice period. Provider will draw attention to this consequence in the notice. The notice may be sent by email to Customer's general contact person specified in the Order Form.

10.10 **Independent Contractor**. The Parties to the Agreement are independent contractors. Customer bears all risk and cost of operating its own business, including risk of loss. Nothing in the Agreement is intended to, or shall be deemed to, constitute a partnership or joint venture of any kind or employment relationship between the Parties, not constitute any party an employee or agent of another party for any purpose. No party shall have authority to act as employee or agent for, or to bind, the other party in any way.

10.11 **Severability**. Should parts of the Agreement be or become invalid, this shall not affect the validity of the remaining provisions of the Agreement, which shall remain unaffected. The invalid provision shall be replaced by the Parties with such term which comes as close as possible, in a legally permitted manner, to the commercial terms intended by the invalid provision.

10.12 **Waiver**. The waiver of one breach or default or any delay in exercising any rights shall not constitute a waiver of any subsequent breach or default.

10.13 **Survival**. Those provisions which by their nature are intended to survive any termination of the Agreement shall survive such termination or expiration of the Agreement.

List of Applicable Schedules

The applicable Schedules listed below, in each case in their then current form, are incorporated in this Agreement and form an integral part of the Agreement.

Schedule	Location
Solutions Schedule	Available at https://www.productsup.com/legal/
Acceptable Use Policy	Available at https://www.productsup.com/legal/
Productsup Platform Description	Available at https://www.productsup.com/legal/
WoC Software Description	Available at https://www.productsup.com/legal/
System Availability Service Level Agreement	Available at https://www.productsup.com/legal/
Product and Account Support Service Level Agreement	Available at https://www.productsup.com/legal/
Professional Services Schedule	Available at https://www.productsup.com/legal/
Productsup Professional Services Description	Available at https://www.productsup.com/legal/
WoC Professional Services Description	Available at https://www.productsup.com/legal/
Agreement for order processing according to Art. 28 EU General Data Protection Regulation (DPA)	Available at https://www.productsup.com/legal/

Productsup Information Security Policy	Available at https://www.productsup.com/legal/
World of Content Information Security Policy	Available at https://www.productsup.com/legal/

Solutions Schedule

When incorporated by reference, the terms set forth in this Solutions Schedule shall specify and govern the provision of the Solutions from the Provider entity to the Customer entity, each as set out in an applicable Order Form ("**Provider**" and "**Customer**", each also referred to as a "**Party**" and collectively as the "**Parties**") as of the Effective Date and form an integral part of the terms agreed between Provider and Customer (the "**Agreement**")

Now therefore, the Parties agree as follows:

1. Definitions

Any capitalized terms not otherwise defined in the Agreement have the meanings set out below. Any reference to the singular includes a reference to the plural and vice versa, unless expressly otherwise provided in this Agreement, and any reference to the masculine includes a reference to the feminine and vice versa, and (unless the context clearly indicates the contrary) the words "including" and "in particular" shall be deemed to be followed by the words "without limitation". Unless defined otherwise by the Parties in any part of the Agreement that takes precedence over this Schedule, any defined term shall have the given meaning for the purposes of the Agreement.

Account	Means the Customer's instance within the Productsup Platform, that Customer and its Authorized Users may use to access, manage and administer their use of the Productsup Platform.
Applicable Data Protection Laws	Means all applicable state and federal statutory and regulatory requirements regarding privacy and the protection of "personal data" or "personally identifiable information" (as defined by such laws) as amended from time to time or any other applicable similar laws relating to the protection of personal data in other jurisdictions, including, as applicable, the General Data Protection Regulation (EU) 2016/679 (and as implemented under applicable national law) and any other applicable data protection laws and regulations
Authorized Users	Those employees, agents and independent contractors of Customer who are authorized by Customer to access and use the Services under Customer's Account
Customer Data	The (i) data and information provided by Customer to Provider and/or imported, inputted, uploaded and/or shared by Customer, Authorized Users or Provider on Customer's behalf, for the purpose of using the Solutions or facilitating Customer's use of the Solutions; or (ii) data collected and processed by or for Customer through Customer's use of the Solutions, but excluding Provider Data. For the avoidance of doubt, any data processed and exported using the Solutions shall be considered Customer Data.
Documentation	Has the meaning given in section 2.7 of this Solutions Schedule.

Intellectual Property Rights	Intellectual property rights including without limitation rights in patents, trademarks, service marks, trade names, other trade-identifying symbols and inventions, copyrights, design rights, database rights, rights in know-how, trade secrets and any other intellectual property rights arising anywhere in the world, whether registered or unregistered, and including applications for the grant of any such rights
Productsup Platform	Has the meaning given in section 2.3 of this Solutions Schedule.
Product and Account Support	Has the meaning given in section 2.4 of this Solutions Schedule.
Provider Data	Any information or data provided by Provider to Customer as part of the Services, for the avoidance of doubt excluding any Customer Data processed by Provider and/or exported from the Productsup Platform
Solutions	Has the meaning given in section 2.2 of this Solutions Schedule.
WoC Software	Has the meaning given in section 2.5 of this Solutions Schedule.

2. Solutions

2.1 The Solutions set out under this Agreement are the software services provided by or on behalf of the Productsup Group ("**Productsup**") to its customers and/or authorized partners, in each case as further defined in this Agreement. They may be provided to Customer by any Affiliate of Productsup or by an authorized partner. The relevant Provider entity will be set out in an applicable Order Form.

2.2 **Solutions**: collectively means the (i) Productsup Platform and relevant Documentation, (ii) Productsup Product and Account Support ((i) and (ii) collectively the "**Productsup Platform Solutions**"), (iii) WoC Software and relevant Documentation, (iv) WoC Software Support ((iii) and (iv) collectively the "**WoC Solutions**"), each as further set out in the Agreement.

2.3 **Productsup Platform**: means the Productsup web-environment upon which the Productsup cloud software solutions are made available to Customer via the Customer's Account and may be accessed, controlled and managed by the Customer or its Authorized Users to process Customer Data in the contractually agreed Scope. The scope and functionalities of the Productsup Platform and its relevant licensing modules are further described in the Productsup Platform Description, available via https://www.productsup.com/legal/.

2.4 **Product and Account Support**: means the support services provided by Productsup to Customer for the Productsup Platform (i) in the event of malfunctions of the Productsup Platform and (ii) regarding Customer's functional issues or questions about the Productsup Platform; and means the support services provided to Customer for the WoC Software (i) in the event of malfunctions of the WoC Software and (ii) regarding Customer's functional issues or questions. Unless expressly agreed by the parties in writing, Product and Account Support is provided exclusively subject to the further specifications and the service levels set out for the provision of Product and Account Support in the Product and Account Support Schedule, available via https://www.productsup.com/legal/.

2.5 **WoC Software:** Means the cloud software solutions provided under the "World of Content" brand, which are separate from the Productsup Platform. The WoC Software is made available to Customer via the Customer's Account and may be accessed, controlled and managed by the Customer or its

Authorized Users to process Customer Data in the contractually agreed Scope. The scope and functionalities of the World of Content Software and its relevant licensing modules are further described in the World of Content Software Description, available via https://www.productsup.com/legal/.

2.6 **Documentation:** the then current document(s) and other relevant information, made available to Customer by Provider or on Provider's behalf, which set out a description of the relevant Solutions and the user instructions for the relevant Solutions, as updated from time to time.

3. Service Levels

3.1 Productsup Platform and WoC Software

The Productsup Platform and the WoC Software shall be available to Customer in accordance with the System Availability Service Level Agreement.

3.2 Product and Account Support

The Productsup Platform and the WoC Product and Account Support shall be provided in accordance with the Product and Account Support Service Level Agreement, available via https://www.productsup.com/legal/.

4. Information Security and Data Hosting

4.1 The Solutions are hosted on third party server infrastructure located in Germany and other member states of the EEA. A list of such third-party hosting providers in respect of the relevant Solution shall be provided upon Customer's request.

4.2 Productsup Platform Solutions

4.2.1 To safeguard the integrity of and the Customer Data processed via the Productsup Platform Solutions, Productsup maintains commercially reasonable technical and organizational measures in compliance with the internationally accepted ISO 27001:2013 information security standard framework, designed: (a) to secure its systems from unauthorized disclosure, access or alteration, and (b) to protect against unlawful destruction or accidental loss, as further described in the Information Security Policy available under https://www.productsup.com/legal/ in its then current form, as amended from time to time.

4.2.2 Except for the login credentials of Customer's Authorized Users, the Productsup Platform Solutions can be operated without processing any personal data. Should certain Productsup Platform Solutions, by exception, process any personal data and such personal data pertain to citizens of the European Union, Customer and Provider shall enter into a separate data processing agreement subject to Art. 28 of the General Data Protection Regulation (GDPR).

4.3 WoC Software Solutions

4.3.1 To safeguard the integrity of and the Data processed via the WoC Software Solutions, WoC maintains commercially reasonable technical and organizational Information Security Measures

as described in the Information Security Policy available under https://www.productsup.com/legal/.

4.3.2 The WoC Software Solutions process certain personal data on Customer's behalf. If Customer purchases any WoC Software Solutions from Provider and where such personal data processed on Customer's behalf pertain to citizens of the European Union, Customer and Provider shall enter into a separate data processing agreement ("DPA") subject to Art. 28 of the General Data Protection Regulation (GDPR). Provider's standard DPA is available under https://www.productsup.com/legal/.

5. Use of the Solutions

The use of Solutions is subject to Provider's Acceptable Use Policy which is incorporated into this Agreement.

6. Overage Use Fees

6.1 For the Productsup Platform

In any month during the applicable Subscription Term that the Services used by Customer exceed the agreed quantities as set out in the applicable Order Form, Customer shall pay additional Fees for the excess use as indicated in the applicable Order Form and the Productsup Platform Description incorporated into this Agreement. These Fees will be charged as incidental charges on a monthly base.

6.2 For the WoC Software

For any use outside the Scope, as well as any exceeding of the agreed limit of use of the Services, the Customer is deemed to have entered into a new, separate Agreement with Provider, for which the associated costs will be charged separately on the basis of subsequent calculation, subject to notification to Client. Provider has the right to charge the aforementioned costs directly to the Customer; earlier than and separately from any recurring invoice.

7. Intellectual Property Rights and License Grant, Use Rights

7.1 Customer acknowledges that Provider and its licensors and suppliers shall own all Intellectual Property Rights in the Solutions, all related source code, Provider Data, Documentation and any enhancements or feedback thereto. Except as expressly stated herein, the Agreement does not grant Customer any applicable Intellectual Property Rights or any other rights or licenses.

7.2 Subject to Provider's payment of the agreed fees and compliance with the and conditions of the Agreement, Provider grants Customer, throughout the term of any applicable Order Form, a limited, non-exclusive, non-transferable, non-assignable and non-sublicensable license, solely for Customer's internal business operations, to access and use the Solutions via its Account in accordance with the Scope throughout the agreed subscription term.

7.3 Provider reserves its right to change the Solutions through Updates in order to adapt them to the state of the art for similar services, or to optimize them. For the avoidance of doubt, Provider is not obliged

to provide any Updates except as part of Provider's obligation to provide Product and Account Support.

7.4 Customer shall own all right, title and interest in and to all of the Customer Data. For the avoidance of doubt, insofar as the Solutions are used by Customer to process, transform and/or create derivative works of Customer Data, Customer shall own all right, title and interest in and to all such Customer Data. Nothing in this Agreement shall be construed to grant Provider any rights in any Customer Data, except for the limited rights set out set out in this section.

7.5 Customer grants Provider a limited, non-exclusive, royalty-free, worldwide, license to use Customer Data (i) in connection with the provision of the Solutions as required to perform its obligations under the Agreement and in the agreed Scope; and (ii) for the purposes of improving and/or developing the Services.

7.6 Customer further acknowledges and agrees that Provider may obtain, generate and use anonymized and aggregated data in connection with Customer's use of the Solutions and that Provider may use such data at any time to develop, analyze, improve, support, operate and provide the Solutions or other services.

7.7 Provider shall follow industry standard archiving and back-up procedures for Customer Data, as set out in Provider's Data Backup Policy, which is incorporated into this Agreement and forms an integral part thereof.

8. Use of External Services

Customer, at its sole discretion, may choose to authorize Provider to use certain data from YouTube, Google, Facebook, Instagram, Twitter, and other platforms, strictly for the purpose of powering certain Provider features for the benefit of Customer and exclusively subject to Customers authorization. Customer can request its authorized data be deleted from Provider by contacting Provider's support team. Customer can learn more about each respective Social Platform's terms of service and privacy policies via the links below:

1. Social Platforms Terms of Service:

Google: https://www.google.com/intl/en/policies/terms/
YouTube: https://www.youtube.com/t/terms
YouTube API Customer:
https://developers.google.com/youtube/terms/api-services-terms-of-service
Facebook: https://www.facebook.com/legal/terms
Instagram: https://help.instagram.com/478745558852511
Twitter: https://twitter.com/en/tos

2. Social Platforms Privacy Policies:

Google & YouTube: http://www.google.com/policies/privacy
Facebook: https://www.facebook.com/privacy/explanation
Instagram: https://help.instagram.com/155833707900388
Twitter: https://twitter.com/en/privacy

3. Customer can revoke Provider's access to its data from YouTube, Google, Facebook, Instagram, and Twitter at any time via each relevant platform's app and security

settings via the links below. Revoking such authorizations may limit or eliminate certain functionalities in the Productsup Platform.

4. Revoke Access:

YouTube & Google: https://security.google.com/settings/security/permissions
Facebook: https://www.facebook.com/settings?tab=applications
Instagram: https://www.instagram.com/accounts/manage_access/
Twitter: https://twitter.com/settings/applications

9. Marketing

9.1 Customer Logo Usage by Provider

Unless explicitly excluded from the scope of the Agreement in an applicable Order Form, Customer agrees that Provider and its Affiliates may publish Customer's name and logo in its Customer lists, and promotional, marketing and investment materials, in any media and grants Provider a non-exclusive, revocable, unlimited license for the described purpose. Any use of Customer's name and logo shall be in accordance with the applicable brand guidelines as notified by Customer from time to time.

9.2 Further Marketing Cooperation

If explicitly agreed and further specified in an applicable Order Form, Customer will co-operate with Provider in producing any press releases, case studies or other marketing materials regarding the supply of the Services to Customer.

List of Applicable Schedules

The Schedules listed below, in each case in their then current form, are incorporated in this Agreement and form an integral part of the Agreement.

Schedule	Location
Acceptable Use Policy	Available at https://www.productsup.com/legal/
Productsup Platform Description	Available at https://www.productsup.com/legal/
Product and Account Support Service Level Agreement	Available at https://www.productsup.com/legal/
WoC Software Description	Available at https://www.productsup.com/legal/
System Availability Service Level Agreement	Available at https://www.productsup.com/legal/
Agreement for order processing according to Art. 28 EU General Data Protection Regulation (DPA)	Available at https://www.productsup.com/legal/
Productsup Information Security Policy	Available at https://www.productsup.com/legal/
WoC Information Security Policy	Available at https://www.productsup.com/legal/

Acceptable Use Policy

When incorporated by reference, the terms set forth in this Acceptable Use Policy shall specify and govern the provision of the Solutions from the Provider entity to the Customer entity, each as set out in an applicable Order Form ("**Provider**" and "**Customer**", each also referred to as a "**Party**" and collectively as the "**Parties**") as of the Effective Date and form an integral part of the terms agreed between Provider and Customer (the "**Agreement**").

Now therefore, the Parties agree as follows:

1. Customer's Use of the Solutions

1.1 Customer shall ensure that each Authorized User uses a secure and confidential password to access the Solutions.

1.2 Customer shall:

1.2.1 procure that its Authorized Users shall: (i) use the Solutions in accordance with the terms and conditions of the Agreement; (ii) each use a secure and confidential password to access the Account (iii) comply with all applicable laws and regulations with respect to its activities under the Agreement; (iv) only use the Solutions for lawful purposes. Customer shall be liable for any breach of the Agreement by its Authorized Users;

1.2.2 use commercially reasonable efforts to prevent any unauthorized access to, or use of, the Solutions, and, in the event of any unauthorized access or use, promptly notify Provider;

1.2.3 except where expressly agreed otherwise by the Parties in writing and subject to a separate agreement pertaining to such services, be solely responsible for the accuracy, completeness, design, appropriateness, creation, maintenance, and updating of all Customer Data in the use of the Solutions. Provider shall not be liable for any errors or inaccuracies in (i) any information provided by Customer; (ii) any Customer Data, or (iii) any changes or modifications to any Customer Data by Provider upon Customer's written instructions, beyond its responsibility to accurately reproduce such Customer Data upon Customer's instruction;

1.2.4 be solely responsible for using a supported browser that is needed to access the Productsup Platform; a list of supported browsers for the use of the Productsup Platform can be found under https://help.productsup.com/en/29407-29410-supported-browsers.html; and

1.2.5 be responsible for obtaining all necessary licenses and consents required to use Customer Data in the agreed Scope, if any, including without limitation those from the owners or licensees of any third-party information, and Customer warrants and represents that such licenses and consents have been obtained.

1.3 Customer acknowledges and agrees that the Productsup Platform serves the purpose of distributing and syndicating Customer Data, but does not serve as a storage solution for Customer Data and shall not be used in this way.

1.4 Customer shall not and shall procure that its Authorized Users shall not during the course of its use of the Solutions, upload, input, access, store, distribute or transmit any Viruses, nor any material,

including without limitation Customer Data, which is (i) unlawful (including breach of Intellectual Property Rights of any other party or any other person's rights), harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive; (ii) facilitates illegal activity; (iii) depicts sexually explicit images; (iv) promotes unlawful violence; (v) is discriminatory on the grounds of race, gender, colour, religious belief, sexual orientation, disability or any other illegal activity; or (vi) causes damage or injury to any person or property. Provider reserves the right, without liability or prejudice to its other rights to Customer, to (i) disable Customer's access to any material that breaches the provisions of this section; and to (ii) disable the Solutions in respect of any such content where, in Provider's sole and reasonable discretion, Provider suspects such content to be in violation of this section.

1.5 Customer shall not, and shall cause Authorized Users not to, access or use the Solutions, if Customer or any Authorized User is located in a jurisdiction that is that is subject to U.S. or EU economic sanctions, and neither Customer nor any Authorized User shall provide access to the Solutions to any government, entity, or individual located in any such jurisdiction or to any individual identified on any U.S. or EU sanctions lists.

1.6 Provider reserves the right, without liability or prejudice to its other rights to Customer, to (i) disable Customer's access to any material that breaches the provisions of this section; to (ii) disable the Solutions with regard to any such content which is in violation of this section.

2. Indemnification

Customer agrees to defend, indemnify and hold harmless Provider and its Affiliates from and against any and all claims, losses, damages, expenses and costs, including without limitation reasonable court costs and legal fees, arising out of or in connection with Customer Data (each a "**Claim**"). Provider shall, in this case (i) notify Customer in due time of any Claim; (ii) grant Customer, at Customer's cost, full authority and control of the settlement and defense of the Claim (to the extent possible under applicable law and possible without impairing the effective defense of the Claim; to the extent no full authority and control can be granted, Provider agrees to involve Customer by fully informing Customer of any communication from opposing party, their counsel, and any court, arbitrator, mediator or other similar entity, and by submitting to Customer for prior approval any statement, brief, submission or filing, written or otherwise, to any of the aforementioned); and (iii) reasonably cooperate with Customer in the defense of such Claim, including providing adequate assistance and information.

3. Provider Intellectual Property Rights and License

3.1 Except as may be permitted by applicable law, Customer shall not and shall ensure that its Authorized Users shall not:

3.1.1 make alterations to, or modifications of, the whole or any part of the Solutions or permit the Solutions or any part of it to be combined with, or become incorporated in, any other programs;

3.1.2 disassemble, decompile, reverse-engineer or create derivative works based on the whole or any part of the Solutions or attempt to do any such thing;

3.1.3 copy, frame, or mirror any part of the Solutions;

3.1.4 access all or any part of the Solutions or the Documentation in order to build a product or service which competes with the Solutions or the Documentation;

3.1.5 provide, commercially exploit or otherwise make available the Solutions, in any form to any person;

3.1.6 use the Solutions or the Documentation to provide the Solutions or certain functionalities thereof to third parties, except where expressly agreed otherwise in writing by the duly authorized representatives of Provider.

Service Level Agreement

This Service Level Agreement governs the provision and accessibility of the Productsup Platform or World and Content Software.

1. Definitions

1.1 "**Downtime**" means the total minutes in the calendar month during which Client's designated Login to the Productsup Platform or World of Content Software does not respond to Client's login-request, excluding Excluded Downtime.

1.2 "**Excluded Downtime**" means the total minutes in the calendar month attributable to (i) periods of non-availability due to Internet interruptions Provider is not responsible for or due to other circumstances beyond the responsibility of Provider, in particular those caused by force majeure; (ii) periods of non-availability due to planned maintenance of the Solutions or the content which are carried out on a regular basis ("**Scheduled Maintenance**"); (iii) periods of non-availability due to unscheduled essential maintenance work which is necessary to eliminate malfunctions; (iv) periods of non-availability due to the fact that, temporarily, the necessary technical requirements for the access to the Solutions, which must be created by the Client, are not met, for example in case of disturbances of the Client's hardware.

1.3 "**System Availability SLA**" shall be defined as the minimum System Availability of the Solutions during each calendar month for production versions and calculated in accordance to formula defined under System Availability.

1.4 **"System Availability"** shall be calculated by following formula:

$$System\ Availability\ as\ percentage = \left[\left(\frac{total\ minutes\ in\ the\ calendar\ month - Downtime - Excluded\ Downtime}{total\ minutes\ in\ the\ calendar\ month - Excluded\ Downtime}\right) * 100\right]$$

Example:
An example month has 30 days (= 30*24*60 = 43.200 minutes)
Excluded downtime for this example month was 180 minutes
Downtime for the example month = 30 minutes

$$System\ Availability\ as\ percentage = \left[\left(\frac{43.200 - 30 - 180}{43.200 - 180}\right) * 100\right]$$

System Availability = 99,93%

2. Provider Obligations

2.1 System Availability SLA

The System Availability SLA of the Productsup Platform and World of Content Software shall be at least 99,5%.

2.2 Downtime

In case of Downtime of the Productsup Platform or World of Content Software, Provider will provide Client with regular updates on system status, mitigation efforts and expected timing for Productsup Platform or Wold of Content Software to become available again.

2.3 Notices

All notices with regard to Downtime and System Availability of the Productsup Platform are provided exclusively through Productsup's statuspage status.productsup.io.

All notices with regard to Downtime and System Availability of the World of Content Software are provided exclusively through the World of Content statuspage https://status.worldofcontent.com/.

Product and Account Support Service Level Agreement
Processing times for Client Incidents

This Support SLA governs the provision of Product and Account Support in case of malfunctions of the Productsup Solutions or World of Content Software or for Client's functionality requests.

1. Definitions

1.1 "**Complete System Outage**" shall mean the absolute unavailability of all of the Solutions's components.

1.2 "**Corrective Action**" means either a final resolution to the error or a temporary workaround or an action plan stating the steps that will be taken in order to solve the error within an estimated timeframe.

1.3 "**Incident**" shall mean a support event starting with a failure, a defect or the functional impairment of the Productsup Solutions or World of Content Software as reported to Provider by Client. As soon as the support team is informed about the support event by Client to the dedicated support email address, the support event becomes an Incident.

1.4 "**Initial Response Time**" means the time it takes to acknowledge the reporting of an Incident.

1.5 "**Local Office Hours**" on any Business Day shall mean times from between 9:00 am and 6:00 pm in the following time zone depending on the contracting Provider's Entity. Where any applicable Order Form indicates Productsup to be the Provider, the following time zones shall apply:

Contracting Productsup Entity	Products Up GmbH	Productsup Corp.	Productsup Pty. Ltd.
Applicable time zone	CEST	EST	AEST

Where support is provided by World of Content, the applicable time zone is CEST.

1.6 "**Severity Level**" shall have the meaning set out in section 3 of this Schedule.

1.7 "**Ongoing Response Time**" shall be the time interval in which updates on the recovery process are shared.

2. Provision of Product and Account Support

2.1 Productsup reactively answers Client submitted tickets about a malfunction of the Productsup Platform or any related question on functionality, scope as well as configuration. World of Content support experts reactively answer Client submitted

tickets about a malfunction of the World of Content Software or any related question on functionality, scope as well as configuration. In all cases, the Client is requested to give as many details as possible, such as links, concrete examples, or screenshots.

2.2 Malfunctions of the Productsup Platform should be communicated to the Productsup Support Team via support@productsup.com, while malfunctions of the World of Content Software should be communicated to the World of Content Support Team, via the support@worldofcontent.com address. Productsup is responsible for the Account Support of the Productsup Platform while World of Content is responsible for the Account Support of the World of Content Software.

2.3 When communicating malfunctions of the Productsup Solutions or World of Content Software to Productsup or World of Content, the Client shall reasonably self-diagnose the impact and recommend, in good faith, an appropriate Severity Level designation. Productsup or World of Content support teams shall validate given Severity Level designation or notify Client of a change in the Severity Level designation to a higher or lower level, giving a reason for such change.

2.4 When communicating non-system issues (ascribed as Severity Level 4) to the Productsup or World of Content support teams, these can be questions about platform functionality, scope or best practices in regard to specific setups. The Client will be provided with help articles, step by step explanations or roadmap outlooks in case functionalities are planned, but not available yet. If a desired functionality is not available or in the pipeline, the Client can issue a feature request.

2.5 Productsup and World of Content support teams respond to support issues based on Severity Levels (as defined below) during Local Office Hours.

3. Processing times for Client Incidents

Severity Level of Client Incident	Description	SLA for Initial Response Time (IRT)	SLA for Corrective Action	SLA for Ongoing Response Time (ORT)
1	An Incident is properly ascribed "Severity Level 1" if the Incident has very serious consequences for normal business transactions and urgent, business critical work cannot be performed. The Incident requires immediate processing because the malfunction can cause serious losses. This is generally caused by a Complete System Outage.	6 hours (Local Office Hours)	1 Business Day	Once every 3 hours (Local Office Hours)
2	An Incident is properly ascribed "Severity Level 2" if normal business transactions are seriously affected and essential tasks cannot be performed. This is caused by malfunctions of central functions of the Productsup Software or other incorrect or inoperable functions in the Productsup Software that are required to perform	8 hours (Local Office Hours)	2 Business Days	Once every 6 hours (Local Office Hours)

	essential transactions and/or tasks. The Incident requires immediate processing because the malfunction can seriously disrupt the entire productive business flow.			
3	An Incident is properly ascribed “Severity Level 3” if the Incident has few or no effects on normal business transactions. The problem is caused by incorrect or inoperable functions in the Productsup Platform or World of Content Software that are not required daily or are rarely used.	One Business Day (Local Office Hours)	n/a	Once every 5 Business Days
4	An Issue is properly ascribed “Severity Level 4” if it is not affecting the functionality of the system. These can be product functionality questions, account configuration questions, or other account requests.	One Business Day (Local Office Hours)	n/a	n/a

Productsup Platform Description

This Productsup Platform Description specifies the Services ordered by Client under an applicable Order Form.

A. License Features and Functions

Productsup Platform Solutions

1.	**Subscriptions**

1.1	**Software Subscriptions License**
1.1.1	Productsup Platform License
	Standard 1.0 Productsup Platform License

	General Functionalities
	
	• Number of products manageable depends on chosen Edition
	• Exports/uploads per day depends on chosen Edition
	• Number of user accounts with user right management depends on chosen Edition
	• Standard export channels subject to the specifications and limitations in the then-current, applicable **Export List** available under https://www.productsup.com/legal/, in the 'Data Exports / Imports' section.
	  o The Channels mean all sites described in the then-current, applicable Export Channel Template List available under https://www.productsup.com/legal/.
	  o Every Country/Language Per Channel (listed in the applicable Export Channel Template List) is considered to be an Export In case multiple exports are required for a single channel in a single country due to category specific attributes, the channel only counts once.
	• Creation of FTP accounts depends on chosen Edition
	
	Data Import Functionalities
	
	• Access to various standard data import capabilities (e.g. Productsup API, Feed URL, Google Sheets) subject to the specifications and limitations in the then-current, applicable Import Channel List available under https://www.productsup.com/legal/, in the 'Data Exports / Imports' section.
	• Support of multiple data source formats (e.g. XML, CSV, TXT)
	• Import services to enrich data sources (e.g. ID generation, data transformation)
	• Connection of multiple standard data sources to one feed
	• Import of third-party tracking information
	• Product data API with delta updates possibility
	• Import data from another site
	
	Data Management and Data Processing Functionalities
	
	• Detailed feed scheduling
	• Dataflow to map data from import to export
	• Data-View to preview and analyze the product catalog
	• Access to rule boxes for optimization and manipulation

	• Shared processing capabilities
	• List feature (e.g. category mapping, blacklist, whitelist, normalization lists)
	• Image manipulation (e.g. dataflow manipulation with rule boxes)
	• KPI based ROI strategy feature
	
	Data Export
	
	• Support of multiple feed output formats (e.g. XML, CSV, TXT, etc.)
	• Various data export capabilities (e.g. HTTP, FTP, SFTP, APIs, etc.)
	• Access to various pre-configured standard export templates) subject to the specifications and limitations in the then-current, applicable Data Services List available under https://www.productsup.com/services-documentation/
	• Up to five custom export templates (including delta functionality and XML manipulation) can be enabled in the Productsup Platform
	• Analyze option with best practice recommendations for export templates
	• A/B testing of marketing channels
	
	Administration
	
	• Project- and Site breakdown on account level
	• Error monitoring feature based on feed quality KPIs:
	  o Email notifications
	  o Automated export interruption
	  o Dashboard feature with import and export activity, products count and site status
	  o Error log with details about last runs

1.2	**Add-On-Software Subscriptions**
1.2.1	Feed Management & Marketing Module

	• Included marketing exports • Search Engines, Comparison Shopping, Affiliate & Retargeting, Social Media, Marketing Tech • Google Keyword Planner (not with Starter edition) • Facebook Ad-Insights (only with Grow, Scale and Enterprise editions) • Analytics Connectors (DoubleClick, Webtrekk...) (only with Grow, Scale and Enterprise editions) • Google Ad-Previews (only with Grow, Scale and Enterprise editions) • Tracking • Content Experiments (Content A/B Testing)
1.2.2	Marketplace Module (BETA)
	• Included Marketplace Exports (Amazon, Ebay, etc.) • Order Dashboard • Order Reporting • Number of order syncs (supported marketplaces can be seen in our software specifications) depends on chosen Edition • PII Security
1.2.3	Product Content Syndication Module
	• Syndication to retailers via Item Setup Sheets, Prebuilt Data Pool connections or direct API (only with Grow, Scale and Enterprise editions) • Amazon Vendor and other marketplace/retail hybrids (1P model) (only with Grow, Scale and Enterprise editions)
1.2.4	Industrial Syndication Add-on

	• Classification standards (ETIM, UNSPSC, ECLASS) • Special formats (BMEcat, FAB-DIS...) • Industrial data pools (2ba, ARGE...)
1.2.5	Seller/Vendor Onboarding Module
	• Cloud Services Connectors (e.g. Amazon S3, ...) (only with Grow, Scale and Enterprise editions) • Custom API Enabled (only with Grow, Scale and Enterprise editions) • Number of catalogs (1st party, 3rd party Seller/Vendors) (only with Scale and Enterprise editions) depends on chosen Edition
1.2.6	Content Portal Add-on
	• Self-service portal for internal and external stakeholders to view & download products and assets • Content Portal Add-on comes by default with one Account included, where Account is defined as the Client's dedicated virtual space in the Productsup Content Portal to manage its use of the Productsup Software through its Authorized Users; • Additional Content Portal accounts can be purchased by a Client • Number of user accounts with user right management depends on chosen Edition • Only with Grow, Scale and Enterprise editions
1.2.7	Travel Add-on
	• Included marketing Travel exports (only with Grow, Scale and Enterprise editions) • Travel Channels (Google Hotel Ads, Facebook Hotel Ads, Facebook Flight Ads...) (only with Grow, Scale and Enterprise editions) • Geodata APIs (e.g. Address to Lattitude / Longitude) (only with Grow, Scale and Enterprise editions)

	• Travelportal Ratings Integration (only with Grow, Scale and Enterprise editions) • Weather API (only with Scale and Enterprise editions)
1.2.8	Image Desginer Module
	• Shareable templates (not with Starter Edition) • Clipart Library (not with Starter Edition) • Number of layers depends on Edition (not with Starter Edition)
1.2.9	Dynamic Videos Module
	• Standard Pre-build templates (not with Starter Edition) • Custom Templates (not with Starter Edition)
1.2.10	Crawler Module
	• Data Crawler • Image Properties Crawler
1.3	**Support Services Subscriptions**

1.3.1	Product and Account Support[1]
	Product and Account Support is provided by Productsup subject to the specifications in the applicable MSA and relevant Schedule. Product and Account Support experts reactively answer Client submitted tickets about either a malfunction of the Productsup Software or questions on functionality, scope or configurations of the Productsup Software or Productsup Platform. In both cases, the Client is requested to give as many details as possible, such as links, concrete examples, or screenshots. When communicating malfunctions of the Productsup Software to Productsup, the Client shall reasonably self-diagnose the impact and recommend, in good faith, to Productsup an appropriate Severity Level designation. Productsup shall validate given Severity Level designation or notify Client of a change in the Severity Level designation to a higher or lower level, giving a reason for such change. When communicating non-system issues to Productsup, these can be questions about the functionality of the Productsup Platform, scope or best practices in regard to specific setups. The Client will be provided with help articles, step by step explanations or roadmap outlooks in case certain functionalities are planned, but not available yet. If a desired functionality is not available or in the pipeline, the Client can issue a feature request. Productsup responds to Support Incidents based on Severity Levels (as defined below) during Local Office Hours as specified in the Product and Account Support Service Level Agreement Schedule to the Master Services Agreement.
1.3.2	Access to Help Center and Academy
	Access to the Productsup Help Center with detailed explanations on all available features, as well as examples and use cases. Help articles are constantly updated and kept up-to-date in accordance with new releases of the Productsup Platform.

[1] Subject to the specifications in the applicable Master Services Agreement and the Product and Account Support Service Level Agreement Schedule (Support SLA).

	Access to the Productsup Academy online, where self-paced e-learning courses can be retrieved. The offer will continuously be extended and updated. Costs apply according to prices on the Productsup Academy website. The use of the Productsup Academy is subject to separate terms of service.

1.4	Add-On Purchases

1.5	Add-On Software Products
1.1.1	Video Rendering Template
	• Creating and uploading a custom video design template
1.1.2	On Premise Import Extension
	• SAP Hybris - Productsup Data Export

B. Data Backup's provided by the Productsup Platform

The Productsup Platform performs the following backup actions for Client Data:

- Hourly incremental backups;
- Daily full backups;
- Backups are stored off-site (AWS S3);
- Daily automatic backup-restore tests to assess the reliability of the backup actions.

C. Data Retention

Client Data are removed from the Productsup Platform as set out below

1. Removal of Files on Transport

Files on Transport, older than 12 months will be removed. To prolong the lifetime, the user can export the same file again (update) to set the 12 months' Time To Live ("TTL").

2. Files with Dynamic Filenames

Files with dynamic filenames using a dynamic template fragment ({{ ... }}) have a TTL of 30 days and will be removed if the files have not been updated.

3. Overview of Scope of Productsup Platform Editions and Modules

Edition					
Platform Features per Edition	**Starter**	**Professional**	**Grow**	**Scale**	**Enterprise**
Push Platform API (import)	-	-	✓	✓	✓
Pull Platform API (export)	-	-	-	-	✓
PIM Connectors	✓	✓	✓	✓	✓
Onlineshop Connectors (e.g Magento, Shopify)	✓	✓	✓	✓	✓
OAuth	✓	✓	✓	✓	✓
Apps (Data Services)	-	-	✓	✓	✓
Users	**3**	**5**	**10**	**25**	**50**

Max SKU/Offer (Max Imported or Exported Lines) (Max lines/sku per import or export)	**1.000**	**5.000**	**50.000**	**250.000**	**500.000**
Included Exports per acccount	**3**	**5**	**15**	**50**	**100**
Syndication Frequency (per Channel)	**Once a day**	**Twice a day**	**Four times a day**	**Once an hour *)**	**> Once an hour *)**
***) Client to deliver deltas. Syndication frequencies cannot exceed processing time per 'run'**					
Setup Fee per Edition & Account	**-**	**Specified in Order Form**	**Specified in Order Form**	**Specified in Order Form**	**Specified in Order Form**

Modules					
Module Features per Module and Edition	**Starter**	**Professional**	**Grow**	**Scale**	**Enterprise**

Channel Modules					
Feed Management & MKT Module					
Included marketing exports	✓	✓	✓	✓	✓
Search Engines, Comparison Shopping, Affiliate & Retargeting, Social Media, Marketing Tech	✓	✓	✓	✓	✓
Google Keyword Planner	-	✓	✓	✓	✓
Facebook Ad-Insights	-	-	✓	✓	✓
Analytics Connectors (DoubleClick, Webtrekk...)	-	-	✓	✓	✓
Google Ad-Previews	-	-	✓	✓	✓
Tracking	✓	✓	✓	✓	✓
Content Experiments (Content A/B Testing)	✓	✓	✓	✓	✓

Local Module (LIA / PoS) Add-on (for Feed Management)					
Locations	-	10	25	50	100
Travel Add-on (for Feed Management)					
Included marketing Travel exports	-	-	✓	✓	✓
Travel Channels (Google Hotel Ads, Facebook Hotel Ads, Facebook Flight Ads...)	-	-	✓	✓	✓
Geodata APIs (e.g. Address to Lattitude / Longitude)	-	-	✓	✓	✓
Travelportal Ratings Integration	-	-	✓	✓	✓
Weather API	-	-	-	✓	✓
Marketplace Module					
Included Marketplace Exports	✓	✓	✓	✓	✓

Amazon, Ebay, etc.	✓	✓	✓	✓	✓
Order Dashboard	✓	✓	✓	✓	✓
Order Reporting	✓	✓	✓	✓	✓
Order sync (supported marketplaces can be seen in our software specifications)	3	5	✓	✓	✓
PII Security	✓	✓	✓	✓	✓
Included revenue per month (exkl. vat)	50.000,-	150.000,-	450.000,-	1.500.000,-	3.000.000,-
Product Content Syndication Module					
Included PCS Exports	-	-	✓	✓	✓
Item-Setup Sheets, Pre-Build APIs, Pre-Build Datapools, Retail Channels	-	-	✓	✓	✓
Exports with Classification (e.g. BMECat)	-	-	-	✓	✓

Content Portal Add-on					
Content Portal	-	-	-	✓	✓
Users	-	-	-	50	100
Seller/Vendor Onboarding Module					
Cloud Services Connectors (e.g. Amazon S3, ...)			✓	✓	✓
Custom API Enabled			✓	✓	✓
Catalogs (1st party, 3rd party Seller/Vendors)			15	50	100
Rich Media Modules					
Image Designer Module					

Shareable templates	-	✓	✓	✓	✓
Clipart Library	-	✓	✓	✓	✓
Unlimited layers	-	20	50	✓	✓
Dynamic Videos Module					
Standard Pre-build templates	-	✓	✓	✓	✓
Custom Templates	-	✓	✓	✓	✓
Setup fee per After Effects template (one off)	-	**Specified in Order Form**	**Specified in Order Form**	**Specified in Order Form**	**Specified in Order Form**
Crawler Module					

Data Crawler	✓	✓	✓	✓	✓
Image Properties Crawler	✓	✓	✓	✓	✓
Website Crawler	✓	✓	✓	✓	✓

4. Applicable Overage Fees

1.	Overage Fees for excess use of the Productsup Platform

1.1	Productsup Platform License Edition Overage Fees						
	Overage Variable	**Overage Event**	**Metrics**	**Overage Fee**			
				EUR	**GBP**	**USD**	**AUD**
1.1.1	Syndication Frequency (per Channel)	Client exceeds the agreed Syndication Frequency (per Channel) for the purchased Productsup Platform License Edition	Measured per Channel and Day for every Account/Edition	250,-	220,-	300,-	389,-
1.1.2	Max SKU/Offer	Client exceeds the agreed amount of SKUs/Offers for the purchased Productsup Platform License Edition	Measured per month and single SKU/Offer line for every Account/Edition	0,10,-	0,09,-	0,12,-	0,15,-
1.1.3	Export Channel	Client exceeds the agreed amount of Export Channels for the purchased Productsup Platform License Edition	Measured per month and Export Channel for every Account/Edition	198,-	175,-	240,-	305,-
1.1.4	Edition User	Client exceeds the agreed number of Users for the purchased Productsup Platform License Edition	Measured per month and User for every Account/Edition	198,-	175,-	240,-	305,-

1.2	Module Overage Fees							
	Module	**Overage Variable**	**Overage Event**	**Frequency**	**Overage Fee**			
1.2.1					**EUR**	**GBP**	**USD**	**AUD**
1.2.2	Content Portal Syndication Module	Content Portal Users	Client exceeds the agreed number of Users for the purchased Content Portal Syndication Module	Measured per month and User for every Module	49,-	45,-	59,-	75,-

1.2.3	Local Module LIA/POS	Locations	Client exceeds the agreed number of Locations for the purchased Local Module LIA/POS	Measured per month and Location for every Module	99,-	85,-	119,-	155,-
1.2.4	Marketplace Module (BETA)	Revenue	Client exceeds the agreed Revenue for the purchased Marketplace Module (BETA)	Measured per month and unit of revenue (depending on currency) for every Module	0,04,-	0,04	0,05,-	0,06
1.2.5	Seller/Vendor Onboarding Module	Onboarding Catalog	Client exceeds the agreed number of Catalogs for the purchased Seller/Vendor Onboarding Module	Measured per month and Catalog for every Module	198,-	175,-	240,-	305,-
1.2.6	Dynamic Videos Module	Dynamic Videos	Client exceeds the agreed number of Dynamic Videos for the purchased Dynamic Video Module	Measured per month and Dynamic Video for every Module	25,-	20,-	30,-	39,-

Professional Services Schedule

When incorporated by reference, the terms set forth in this Professional Services Schedule shall specify and govern the provision of the Professional Services from the Provider entity to the Customer entity, each as set out in an applicable Order Form ("**Provider**" and "**Customer**", each also referred to as a "**Party**" and collectively as the "**Parties**") as of the Effective Date and form an integral part of the terms agreed between Provider and Customer (the "**Agreement**")

Now therefore, the Parties agree as follows:

1. Definitions

Any capitalized terms not otherwise defined in the Agreement have the meanings set out below. Any reference to the singular includes a reference to the plural and vice versa, unless expressly otherwise provided in this Agreement, and any reference to the masculine includes a reference to the feminine and vice versa, and (unless the context clearly indicates the contrary) the words "including" and "in particular" shall be deemed to be followed by the words "without limitation". Unless defined otherwise by the Parties in any part of the Agreement that takes precedence over this Schedule, any defined term shall have the given meaning for the purposes of the Agreement.

2. Professional Services

2.1 The Professional Services set out under this Agreement are the supplementary services provided by or on behalf of the Productsup Group ("**Productsup**") to its customers and/or authorized partners, to assist the Authorized Users of the Productsup Platform and/or the WoC Software in their use and administration of these software solutions, in each case as further defined in this Agreement. They may be provided to Customer by any Affiliate of Productsup or by an authorized partner. The relevant Provider entity will be set out in an applicable Order Form.

2.2 Professional Services collectively refers to the (i) Productsup Professional Services, as further described in the Productsup Professional Services Description and the (ii) WoC Professional Services Description, both available via https://www.productsup.com/legal/.

2.3 **Productsup Platform**: has the meaning given in the relevant agreement or schedule that refers to the provision of Productsup software solutions.

2.4 **WoC Software:** has the meaning given in the relevant agreement or schedule that refers to the provision of Productsup software solutions.

3. Marketing

3.1 Customer Logo Usage by Provider

Unless explicitly excluded from the scope of the Agreement in an applicable Order Form, Customer agrees that Provider and its Affiliates may publish Customer's name and logo in its Customer lists, and promotional, marketing and investment materials, in any media and grants Provider a non-exclusive,

revocable, unlimited license for the described purpose. Any use of Customer's name and logo shall be in accordance with the applicable brand guidelines as notified by Customer from time to time.

3.2 Further Marketing Cooperation

If explicitly agreed and further specified in an applicable Order Form, Customer will cooperate with Provider in producing any press releases, case studies or other marketing materials regarding the supply of the Services to Customer.

List of Applicable Schedules

The Schedules listed below, in each case in their then current form, are incorporated in this Agreement and form an integral part of the Agreement.

Schedule	Location
Productsup Professional Services Description	Available at https://www.productsup.com/legal/
WoC Professional Services Description	Available at https://www.productsup.com/legal/

Productsup Professional Services Description

This Services Documentation specifies the Professional Services ordered by Client under an applicable Order Form.

A. Scope of Professional Services Packages

• **Productsup Professional Services**

1.	• **Subscriptions**

1.1	**Professional Services Subscriptions**[1]
1.1.1	Access to Help Center and Academy
	Access to the Productsup Help Center with detailed explanations on all available features, as well as examples and use cases. Help articles are constantly updated and kept up-to-date in accordance with new releases of the Productsup Platform.

[1] Customer to notice: Professional Services requested by Customer in excess of the Scope of a relevant Professional Services Package may be billed as Overage Fees on a time and materials basis at the hourly rates specified in section B of this Productsup Professional Services Description.

	Access to the Productsup Academy, where self-learning courses and training videos can be retrieved. The offer will continuously be extended and updated. Costs apply according to prices on the Productsup Academy website. The use of the Productsup Academy is subject to separate terms of service.
1.1.2	Managed Services Productsup Platform Package (20 hours/month)
	Managed Services Productsup Platform Package covers initial setup of the Client's user account according to best practices, creation of sites, setup of data sources, and mapping of export channels according to the Client's wishes through a dedicated Productsup solutions expert. Data will be cleansed, optimized and structured according to Client's wishes. Requests may either be sent by email or communicated in bi-weekly calls, as preferred by the Client. Upon request, Productsup will provide documentation for the Client's user account setup and/or insights into it in scheduled calls, as part of the Professional Services hours included in the Managed Services Productsup Platform Package. The Managed Services Productsup Platform Package exclusively covers Services within the Productsup Platform and does not involve Productsup to access or operate any third-party tools or systems. The Managed Services Productsup Platform Package includes the m migration of data sources and/or exports. The Managed Services Productsup Platform Package does not include Productsup being in direct contact with any third-party providers. Such communication needs to be handled exclusively via the Client. The Managed Services Productsup Platform Package does not cover the proactive consulting on best practices outside of the Productsup Platform. Productsup conducts the Managed Services Productsup Platform Package under the assumption that the Client will provide key personnel for the period of its duration. This includes at least one person, but ideally a team, who has knowledge about the injected data and its structure, access to an updating data source and its update schedule, access to export channel specifications and (optionally) upload credentials, and who oversees the completion of the Managed Services Productsup Platform Package as well as the need for and usage of Professional Services hours included in the package. Invalidation of this assumption may alter the scope of services required and may result in additional cost. If the submitted Scoping Document cannot be feasibly achieved with the included Professional Services hours, Productsup will provide an estimate on the total amount of Professional Services hours required per month. All overage hours above the Professional Services hours included in the Managed Services Productsup Platform Package are charged at the overage hourly rates specified in the applicable Master Services Agreement and Order Form. The Managed Services Productsup Platform Package needs to be ordered at least four weeks before the desired start date.

	Managed Services Clients submitting a request to Productsup will be provided with an estimate on delivery time within one Business Day.

2.	• **Add-On Purchases**

2.1	Add-On Professional Services[2]
2.1.1	Guided Platform Onboarding Package (10 Hours)
	The Guided Platform Onboarding Package is conducted via remote video calls by a Productsup solutions expert dedicated to the Client's account. The schedule starts with the planning element. In a discovery call both parties will decide about the participants, call schedule and learning milestones for the Guided Platform Onboarding Package. Once the planning is complete, Productsup will continue with the actual training. Productsup's solutions expert will provide two standard group training sessions aimed at providing the foundational knowledge needed to utilize the Productsup Platform. Two further calls are tailored to the Client's individual needs, as well as best practice setup guidance for the Productsup Platform and deep dives into features especially important to Client's use case. Recommended standard training call schedule: • Discovery Call/Kick-off (30-60 mins); • First Core Training Session (90 mins);

[2] Client to notice: Overage Fees for Add-On Professional Services delivered in excess of the ordered Services may occur subject to the relevant provisions in the applicable Master Services Agreement and Order Form.

	• Second Core Training Session (60 mins). After completing the training calls, the Client can use the remaining package hours for educational purposes in the form of calls. Recordings of all calls are available upon request. Productsup's objective is to make the Client's team independent and confident users of the Productsup Platform, who are capable of its setup, rollout, and ongoing administration. Productsup conducts the Guided Platform Onboarding Package under the assumption that the Client will provide key personnel throughout its duration. This includes at least one person, but ideally a team, who will be trained as an administrator of the platform, has knowledge about the injected data and its structure, access to an updating data source and its update schedule, access to export channel specifications and (optionally) upload credentials, and oversees the completion of the Guided Platform Onboarding Package as well as the need for and usage of Professional Services hours included in this package. Invalidation of this assumption may alter the scope of Services required and may result in additional cost. The Guided Platform Onboarding Package is provided to Client free of charge within 90 days upon execution of the relevant initial Order Form, or, if agreed by the Parties, within 90 days at a later point during the runtime of the applicable Order Form. Upon expiry of this period or the included Professional Services hours, the Services provided as part of the Guided Platform Onboarding Package are provided to Client exclusively at the hourly rates for the provision of Professional Services specified in the applicable Master Services Agreement and Order Form.
2.1.2	Guided Platform Onboarding (Existing Client Accounts)
	The Guided Platform Onboarding for existing Client accounts is conducted via remote video calls by a Productsup solutions expert dedicated to the Client's account. Productsup's solutions expert will provide group training sessions tailored to the Client's individual needs, as well as best practice Productsup Platform setup guidance and deep dives into features that are especially important to the Client's use case. Productsup's objective is to make the Client's team independent and confident users of the Productsup Platform capable of setup, rollout, and ongoing administration of the Productsup Platform. Productsup conducts the Guided Platform Onboarding under the assumption that the Client will provide key personnel for the duration of the Guided Platform Onboarding period. This includes at least one person, but ideally a team, who will be trained as an administrator of the Productsup Platform, has knowledge about the injected data and its structure, access to an updating data source and its update schedule, and oversees the completion of the Guided Platform Onboarding as well as the amount of Professional Service hours required. Invalidation of this assumption may alter the scope of Services required and may result in additional costs. Recommended length: three hours are recommended for five participants. The Guided Platform Onboarding for existing Client accounts is provided at the hourly rates for the provision of Professional Services specified in the applicable Master Services Agreement and Order Form.

2.1.3	Guided Implementation Package (minimum 5 hours)
	The Guided Implementation Package is conducted via remote video/phone calls and/or email by a Productsup solutions expert. The Productsup solutions expert will own the project management of the Client's technical implementation internally. Interactions can be for a range of tasks including (but not limited to): • Project planning and tracking; • Status updates in form or regular meetings and proactive updates; • Technical integration and setup of imports and/or export configurations; • Guidance on API connections; • Proactive best practices/consultation regarding account setup and functionality; • Internal channel coordination and centralized point of contact for channel creation. Productsup conducts this service under the assumption that the Client will provide key personnel for the period of the Guided Implementation Package. This includes at least one person, but ideally a team, who participated in the guided platform onboarding and/or has foundational knowledge about the Productsup Platform, has knowledge about the injected data and its structure, access to an updating data source and its update schedule, access to export channel specifications and (optionally) upload credentials, and oversees the completion of the Guided Implementation Package as well as the need for and usage of Professional Services hours included in the package. Invalidation of this assumption may alter the scope of Services required and may result in additional costs. The period of the Guided Implementation Package will not be extended free of charge to account for delays caused by the Client. If the submitted Scoping Document cannot be feasibly achieved with the ordered Professional Services hours, Productsup will provide an estimate on the total amount of Professional Services hours required. All overage hours required to achieve the agreed Scope in excess of the Professional Services hours included in the Guided Implementation Package are charged at the overage hourly rates specified in the applicable Master Services Agreement and Order Form.
2.1.4	Managed Migration Package (minimum 5 hours)
	Managed import and/or export migration will be conducted by a Productsup solutions expert.

	Managed import migration includes the migration to a new data source, including adjustment of configuration to data source setup, and remapping of attributes in the Productsup Platform, as well as a test run before the launch day of the provided new data source. Within this test run the Productsup solutions expert will point out what exactly changed from the former data source to the new one and create an overview on which attributes need to be remapped/adjusted. According to the time schedule provided by the Client, Productsup will ensure deactivation of export updates during data source switch and activate exports after successful migration. Managed export migration includes the migration to a new export channel destination, such as switching from a feed delivery to an API delivery or vice versa. The Productsup solutions expert conducting the migration will ensure that all attributes are mapped to the channel's requirements, that the provided credentials are leading to a successful upload of data, and the export is completed without errors on Productsup's side. Productsup conducts the Managed Migration Package under the assumption that the Client will provide key personnel for the duration of the period of the Managed Migration Package. This includes at least one person, but ideally a team, who has knowledge about the injected data and its structure, access to credentials for import/export, and oversees the need for and usage of the provided Professional Service hours. Invalidation of this assumption may alter the scope of Services required and may result in additional costs. If the submitted Scoping Document cannot be feasibly achieved with the Professional Service hours included in the Managed Migration Package, Productsup will provide an estimate of Professional Service hours. All overage hours required to achieve the agreed Scope in excess of the Professional Services hours included in the Managed Migration Package are charged at the overage rates specified in the applicable Master Services Agreement and Order Form. The Managed Migration Package needs to be ordered at least two weeks before the desired migration date.
2.1.5	Guided Release Training Package
	Within the Guided Release Training session, the Client will get an overview on features introduced in the last three major Productsup Platform releases. According to Client's preferences and use cases, the Productsup solutions expert conducting the Guided Release Training will focus on certain features. Within the call Productsup's solutions expert will give recommendations on use cases for the new features, ideal setups and be available for Q&A. The Guided Release Training session will take place in a remote video call of 90 minutes. Productsup conducts this Service under the assumption that the Client will provide key personnel for the training. This includes at least one person, but ideally a team, who has foundational knowledge of the Productsup Platform, has knowledge about the injected data and its structure, access to

	an updating data source and its update schedule, and who oversees the Guided Release Training Package completion. Invalidation of this assumption may alter the scope of Services required and may result in additional costs. The Guided Release Training Package needs to be ordered at least four weeks in advance of the call. Client's preferences and use cases need to be provided by the Client at least two weeks in advance of the call to allow for adequate preparation. The Guided Release Training Package needs to be completed within 90 days after Order Date.
2.1.6	Guided Account Health Check Package
	The Productsup Guided Account Health Check is delivered through a Productsup solutions expert. It includes a written analysis of the account structure, setup and performance, as well as a detailed analysis of up to two specific sites, which are selected by the Client. An in-depth explanation of findings, best practice recommendations, and Q&A will take place in a remote video call of 90 minutes. Productsup conducts this service under the assumption that the Client will provide key personnel for the Guided Account Health Check call. This includes at least one person, but ideally a team, who has foundational knowledge of the Productsup Platform, has knowledge about the injected data and its structure, access to an updating data source and its update schedule, and who oversees the Guided Account Health Check Package completion. Invalidation of this assumption may alter the scope of Services required and may result in additional costs. The Guided Account Health Check Package needs to be ordered at least four weeks in advance of the call. Sites for in-depth analysis need to be provided by the Client at least two weeks in advance of the call to allow for adequate preparation. The Guided Account Health Check Package needs to be conducted within 90 days after Order Date.
2.1.7	On-Site Guided Platform Training Package
	Up to eight hours of training on the use and functions of the Productsup Platform conducted by a Productsup solutions expert. Content of training will be tailored according to Client's needs. Travel and accommodation expenses are excluded in the Fee and will be added separately. Productsup conducts this service under the assumption that the Client will provide key personnel for the On-Site Training Day. This includes at least one person, but ideally a team, who will be trained as an administrator of the Productsup Platform, has knowledge about the injected data and its

	structure, access to an updating data source and its update schedule, and who oversees the completion of the On-Site Training Day. Invalidation of this assumption may alter the scope of Services required and may result in additional costs. The On-Site Training Day needs to be ordered at least four weeks in advance of the On-Site Training Day. Training topics need to be provided by the Client at least one week in advance to allow for adequate preparation. The On-Site Training Day needs to be conducted within 90 days after Order Date.
2.1.8	Channel Creation as a Service
	Creation of channel templates in standard file formats (e.g. CSV, standard XML/JSON format, item setup sheet) and, if needed, connectors for import or export in/from the Productsup Platform (e.g. API connections), as well as individual adjustments to Productsup's standard file formats of existing channels. A Channel refers to the company/website that the data will be ultimately received by e.g. Amazon. A Template refers to the specific attributes and format required by such a Channel. e.g. Amazon (DE) Watches or Amazon (US) Bags. Each Channel may require different attributes for different categories, regions and/or languages and therefore, depending on the channel, multiple templates may be required. For accurate scoping, Channel specifications and credentials for creation are mandatory to be provided by the Client alongside a data sample set. If the Client is unable to deliver Channel specifications and credentials, Productsup's solutions experts can be introduced to appropriate contacts on the Channel's side to retrieve the required information from them. The timely effort on this cannot be scoped but will be charged according to the hourly rates specified in the relevant rate card contained in the Productsup Professional Services Description Schedule to the applicable Master Services Agreement. A sandbox environment for development is optional. In case sandbox tests are desired, the sandbox access needs to be provided by the Client. An estimate on delivery time and cost effort will be given before the start of the channel creation. Once timeline and cost are accepted by both Parties, an Order Form will be created and signed by both Parties. This includes the full scope of the project. Changes on the scope during creation will result in a change to the Order Form through a Change Order subject to the applicable Master Services Agreement. The agreed Fee will be billed as set out in the applicable Master Services Agreement and Order Form. Productsup provides this Service under the assumption that the Client will provide key personnel for the duration of the creation. This includes at least one person, but ideally a team, who has knowledge about the desired structure and/or delivery of data and can answer Productsup's questions during the creation of the Channel. Invalidation of this assumption may alter the scope of Services required and may result in additional costs.

3.	• **Proof of Concept**

	A Productsup solutions expert will be assigned and made available for the entirety of the booked hours, during Local Office Hours and subject to the specifications in an applicable Proof of Concept Order Form. This expert will be a dedicated, technical, point of contact who owns and executes based on pre-defined success criteria to achieve desired result(s). As a non-binding and non-exhaustive example, activities that may be agreed to be carried out are as follows; ● Setup of the client's platform account; ● Creation of site(s) and project(s); ● Configuration of imports and/or exports (flat files); ● Mapping of export channels, data optimized and structured according to desired outcomes; ● Project planning and tracking; ● Regular meetings and updates. Productsup conducts this service under the assumption that the client will provide key personnel for the period of the Proof of Concept. This includes at least one person who has knowledge of the injected data and its structure. More specifically, access to an updating data source, its update schedule, access to export channel specifications (if required) and (optionally) upload credentials. This person would be our key technical contact and oversee the Proof of Concept. Invalidation of this assumption may alter the scope of Services required and may result in additional costs. The period of the Proof of Concept will not be extended free of charge to account for delays caused by the client. If the originally submitted success criteria cannot be feasibly achieved with the ordered POC hours, Productsup will provide an estimate of additional hours required. All overage hours required to achieve the agreed Scope in excess of the Professional Services hours included in the POC hours are charged at the overage hourly rates specified in the applicable Master Services Agreement and Order Form.

	Unused booked hours are not reimbursed, but will be credited as ‘Guided Implementation’ hours for any further Subscription ordered by the Client within the Assessment Phase specified in an applicable Proof of Concept Order Form.

B. Rate Card for Professional Services and Channel Creation as a Service

Service	Hourly Rate			
	Productsup Corp. (USD)	**Products Up GmbH (EUR)**	**Products Up GmbH (GBP)**	**Productsup Pty. Ltd. (AUD)**
Professional Services	180,-	150,-	130,-	250,-
Channel Creation as a Service	240,-	200,-	175,-	330,-

Productsup Group

Information Security Policy Summary

Version 1.0

Table of Contents

1.0 Common Policy Elements 3
2.0 Information Security 4
3.0 Risk Assessment and Treatment 5
4.0 Organizational Security 6
5.0 Asset Classification and Control 7
6.0 Human Resources Security 8
7.0 Physical and Environmental Security 10
8.0 Asset Management 11
9.0 Access Control 13
10 Cryptographic Controls 15
11.0 Information Security Incident Management 16
12.0 Compliance 17

1.0 Common Policy Elements

1.1 Purpose and Scope

Information is a valuable asset that must be protected from unauthorized disclosure, modification, use or destruction. Prudent steps must be taken to ensure that its confidentiality, integrity and availability are not compromised. This document provides an overview over a uniform set of information security policies for using the Products Up GmbH (hereafter referred to as “Productsup”) technology resources. In addition to defining roles and responsibilities, information security policies increase users’ awareness of the potential risks associated with access to and use of technology resources. Employee awareness through dissemination of these policies helps accelerate the development of new application systems and ensure the consistent implementation of controls for information systems. Productsup’s information security policies are based upon the internationally accepted ISO 27001:2013 information security standard framework. The standards will be considered minimum requirements for providing a secure environment for developing, implementing and supporting information technology and systems.

1.2 Enforcement

These policies must be adhered to by all Productsup departments, divisions and enterprises (hereafter referred to as “departments”) unless specifically granted an exception. Individual departments may develop more detailed procedures to handle department-specific cases, provided they adhere to the policies that they support. This policy will guide annual security reviews by the Information Security Team, as well as audits by a designated third party as requested by Productsup. Violators of these policies may be subject to employee disciplinary procedures as described in the Productsup’s Human Resources Policies. Departments and divisions may impose sanctions upon their employees, within accepted guidelines, for violations of these standards

1.3 Exceptions

Exceptions to information security policies must be approved by the Information Security Team with a review. In each case, the department or vendor must include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the management approval. If approved, exceptions will be documented.

2.0 Information Security

2.1 Policy

2.1.1 Information Security Commitment Statement

2.1.1.1 Information is a valuable Productsup asset and must be protected from unauthorized disclosure, modification, or destruction. Prudent information security policies and procedures must be implemented to ensure that the integrity, confidentiality and availability of Productsup information are not compromised.

2.1.2 Security Responsibility, Review and Evaluation

2.1.2.1 Technology Resources is responsible for establishing and managing the security of all systems. Technology Resources will as needed but at a minimum on an annual basis review the most current best practices regarding the use of technology and will amend and/or issue new policies, procedures, and/or controls to reflect the most appropriate solution for security of Productsup information.

2.1.3 User Responsibility

2.1.3.1 Productsup technology resources are provided to authorized users to facilitate the efficient and effective performance of their duties in a secure electronic environment. The use of such resources imposes certain responsibilities and obligations on users and is subject to all applicable Productsup policies. It is the responsibility of every user to ensure that such resources are not misused and to adhere to all Productsup security policies and procedures, which are located in the Information Security Space on Productsup's Confluence Instance.

3.0 Risk Assessment and Treatment

3.1 Assessing Security Risks

3.1.1 Risk Assessments

3.1.1.1 Risk assessments will be performed annually to address changes in the security requirements and in the risk situation, e.g. in the assets, threats, vulnerabilities, impacts, the risk evaluation, and when significant changes occur.

3.1.1.2 Risk assessments will be undertaken in a methodical manner capable of producing comparable and reproducible results.

3.1.1.3 Risk assessments will have a clearly defined scope in order to be effective.

3.1.1.4 The outcome of a risk assessment will be a report defining and prioritizing risks, based on threats and vulnerabilities and impact to Productsup information.

4.0 Organizational Security

4.1.1 Management Commitment to Information Security

4.1.1.1 Productsup is fully committed to actively supporting security within the organization through clear direction, demonstrated commitment, explicit assignment, acknowledgment of information security responsibilities, and the support of a Information Security Steering Committee developed to provide Governance for all Information Technology policies and procedures.

4.1.1.2 The Information Security Steering Committee will be composed of appointed executive leaders and will meet, at a minimum, on a bi-annual basis. The committee will:

- review and approve information security policy;
- provide clear direction and visible management support for security initiatives;
- approve the resources needed for information security;
- approve assignment of specific roles and responsibilities for information security across Productsup;
- approve plans and programs to maintain information security awareness;
- and ensure that the implementation of information security controls is coordinated across Productsup.

4.1.2 Independent Review

4.1.2.1 Productsup's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) in accordance with the ISO27001 standard will be reviewed on an annual basis.

4.1.2.2 Such a review will be carried out both internally and by individuals independent of the area under review such as a third party organization specializing in such reviews. Individuals carrying out these reviews must have the appropriate skills and experience.

5.0 Asset Classification and Control

5.1 Accountability for Assets

5.1.1 Ownership of Assets

5.1.1.1 All information and assets associated with information processing will be owned by a designated Productsup staff member. The asset owner will be responsible for:

- ensuring that information and assets associated with information processing facilities are appropriately classified;
- and defining, providing, and reviewing access restrictions and classifications, taking into account applicable access control policies.

5.1.2 Acceptable Use of Assets

5.1.2.1 Productsup resources are provided to authorized users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations on users and is subject to Productsup policies. It is the responsibility of each user to understand and abide by Productsup's Acceptable Use Policy and to ensure that such resources are
not misused

5.1.2.3 Productsup reserves the right to retrieve and read any data composed, transmitted or received through inbound/outbound connections and/or stored on Productsup systems.

5.1.3 Information Classification

5.1.3.1 All Productsup information and information entrusted to Productsup from outside agencies fall into one of four sensitivity classifications. Public, Internal, Confidential, Top-Secret.

5.1.3.2. Based on the information sensitivity, specific requirements may apply for labeling, handling, transfer and destruction.

6.0 Human Resources Security

6.1 Prior to Employment

6.1.1 Screening / Terms of Employment

6.1.1.1 Qualification and identity checks will be conducted on all Productsup employees and contractors.

6.1.1.2 The terms of employment specify obligations for secrecy and data privacy.

6.2 During Employment

6.2.1. Responsibilities and Awareness

6.2.1.1 All employees will be required to complete annual training on information security awareness and concepts.

6.2.1.2 All employees will practice security awareness and remain vigilant against fraudulent activities.

6.2.1.3. All employees will immediately report incidents involving any Productsup information to the Information Security Team.

6.2.1.4 All employees will note and report observed or suspected security weaknesses to systems and services directly to the Information Security Team.

6.3 Termination or Change of Employment

6.3.1 Responsibilities for performing employment termination or changes of employment are defined in Productsup's HR procedures.

6.3.2 Human Resources is responsible for the overall termination process and will coordinate with the manager of the person terminating and the Internal IT to manage the access aspects of the relevant procedures.

6.3.3 All employees, contractors, and third party users must return all of the Productsup's assets in their possession upon termination of their employment, contract, or agreement.

6.3.4 The access rights of all employees and third party users to information and information processing facilities must be removed upon termination of their employment, contract, or agreement, or adjusted as necessary upon any change in employment.

7.0 Physical and Environmental Security

7.1 Secure Areas

7.1.1 Physical Security Perimeter

7.1.1.1 A security assessment of all key information processing facilities will be performed annually to assess their physical security.

7.1.2 Physical Entry Controls

7.1.2.1 Access to any Productsup data center, network operations center, telecommunications or other similar information processing facility will be restricted and physically controlled.

7.1.2.2 Access to any office, computer room, or work area that contains confidential information will be physically restricted.

7.2 Equipment Security

7.2.1 Equipment Location and Protection

7.2.1.1 Production systems, including, but not limited to servers, network equipment, and telephony systems will be located within a physically-secured area.

7.2.1.2 Appropriate precautions including removing or encrypting sensitive or confidential data will be taken when sending equipment off site for maintenance.

7.2.2 Secure Disposal or Re-use of Equipment

7.2.2.1 Prior to approved disposal, media containing confidential information must be destroyed to render the information unrecoverable.

7.2.2.2 All hardcopy materials that contain confidential information must be shredded.

8.0 Asset Management

8.1 Media Handling

8.1.1 Management of Removable Media

8.1.1.1 If no longer required and not under public records requirements, the contents of any re-usable media that are to be removed from the organization will be made unrecoverable.

8.1.1.2 Where necessary authorization will be required for media removed from Productsup and a record of such removals will be kept in order to maintain an audit trail.

8.1.1.3 All media will be stored in a safe, secure environment, in accordance with manufacturers' specifications.

8.1.2 Disposal of Media

8.1.2.1 When media is worn, damaged or otherwise no longer required,it will be disposed of in a secure manner. To prevent the compromise of confidential information through careless or inadequate disposal of computer media, formal procedures will be established for secure media disposal.

8.2 Access to Systems

8.2.1 Publicly-Accessible System

8.2.1.1 The dissemination methods for Productsup's information classified as public will have, at a minimum, protection from unauthorized modification and denial of service attacks.

8.2.1.2 Consideration of security controls that will be applied to publicly-available systems will include the following:

- Information to be disseminated is classified in compliance with data protection legislation
- Confidential information must be protected during the collection process and when stored
- Access to the public system does not allow unauthorized access to networks to which it is connected.
- Productsup information classified as other than public will not reside on systems where public information is being served.

8.3 Backup & Recovery

8.3.1 Backup Requirements

8.3.1.1 Backup procedures will be existent for all business critical systems and application to minimize loss of data in case of an incident or outtage.

8.3.1.2 Backup recovery procedures will be regularly tested to ensure backups are operational when required.

8.3.1.3 Backups must be encrypted where confidential data is involved.

9.0 Access Control

9.1 Business Requirement for Access Control

9.1.1 Access Control Policy

9.1.1.1 All confidential information will be protected via access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

9.1.1.2 Access control procedures will control access based on the need to know / least privilege.

9.1.1.3 All information possessed by or used by a particular Productsup unit will have a designated owner who is responsible for determining appropriate sensitivity classifications and criticality ratings, making decisions about who can access the information, and ensuring that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

9.1.1.5 The authority to grant access to Productsup information will be provided in writing, only by the owner of the information or their designate.

9.1.1.6 Default access privileges will be set to “deny-all” prior to any specific permissions being granted.

9.1.1.7 Unless it has specifically been classified as public, all Productsup information will be protected from disclosure. If non-public information is compromised or suspected of being compromised, the information owner and the appropriate security administration will be notified immediately.

9.1.1.8 User access reviews shall be conducted and documented on a quarterly basis to ensure access rights are appropriately assigned to users across all systems and applications.

9.2 User Access Management

9.2.1 Access Authorization

9.2.1.1 User IDs may be granted to specific users only when approved in advance by the user's management.

9.2.1.2 Prior to being granted to users, application system privileges will be approved by the involved application system owner.

9.2.1.3 Without specific formal approval from the user's management, administrators will not grant system privileges to any user.

9.2.2 Clear Desk and Screen Policy

9.2.2.1 Departments that process confidential information will consider adopting a clear desk policy for paper and removal storage media and a clear screen policy, in order to minimize the risks of unauthorized access to and loss of such information, both during and after normal working hours.

9.2.2.2 Computers and mobile devices that access or use confidential data will be protected by password-protected screensavers when unattended.

9.2.2.3 Sensitive or confidential information will be removed from printers and facsimile machines immediately upon printing.

9.2.2.4 The use of power-on passwords will be required where the Computer or any device that contains confidential information.

10 Cryptographic Controls

10.1 Requirements for use of cryptography

10.1.1 Encryption in Transit

10.1.1.1 All data exchanged through the internet will be encrypted in transit using modern encryption algorithms.

10.1.2. Encryption at Rest

10.1.2.1 Servers holding sensitive data will be encrypted at rest where possible.

10.1.2.2 All laptops and or personal computers used by employees for Productsup will be encrypted.

10.1.2.3 Backups will always be encrypted either before transfer or using a technique offered by the provider where the backup is stored (for example Amazon S3 Server-Side-Encryption).

11.0 Information Security Incident Management

11.1 Reporting Information Security Events and Weaknesses

11.1.1 Reporting Security Incidents

11.1.1.1 Any suspected or observed breaches of confidential or restricted information must be reported to the Information Security Team.

11.2 Management of Information Security Incidents and Improvements

11.2.1 Responsibilities and Processes

11.2.1.1 It is the responsibility of all management staff to be familiar with the incident management process.

11.2.2 Collection of Evidence / Learning from Incidents

11.2.2.1 All collection and presentation of evidence will be in compliance with the incident management process.

11.2.2.2 The information gained from the evaluation of information security incidents will be used to identify recurring or high impact incidents.

12.0 Compliance

12.1 Compliance with Legal Requirements

12.1.1 Identification of Compliance Areas

12.1.1.1 Resources has been assigned responsibility for the establishment of Productsup-wide information security policies. However, each department is responsible for developing its own specific procedures necessary to ensure operational compliance with internal provisions and external legal and regulatory requirements.

12.1.1.2 The information processing resources of Productsup are provided for the business purposes of Productsup.

12.1.1.3 Compliance with data protection legislation requires appropriate management control. The owner of such data is responsible for ensuring awareness of the data protection requirements defined in the relevant legislation.

12.2 Compliance with Security Policies and Standards, and Technical Compliance

11.2.1 Identification of Compliance Areas

11.2.1.1 Productsup information systems will submit to regular reviews of technical security audits. These reviews will be performed annually to measure compliance with existing security implementation standards. Technical compliance evaluations are based on performing various types of tests and examining configurations.

11.2.1.2 Compliance testing will identify weaknesses subject to exploitation, and qualify results as to the nature of criticality. Technical evaluations will be done in cooperation with operations personnel to avoid impact on production environments.

11.2.1.3 The handling of results and data obtained in such evaluations will be handled as confidential information.

Agreement

Between

the responsible Customer entity, as set out in an applicable Order Form, hereinafter referred to as customer (CU)

and the processor: the relevant Provider entity as set out in an applicable Order Form , hereinafter referred to as contractor (CO)

the following data processing agreement is made.

Preamble

This agreement is concluded in compliance with the Federal Data Protection Act (BDSG) and the EU General Data Protection Regulation (GDPR) valid from 25.05.2018 as well as with all other relevant data protection regulations. This agreement is governed by the current laws, as amended from time to time.

This agreement concerns the collection, processing and use of personal data in the sense of the BDSG and GDPR by the contractor on behalf of the client ("order processing"). Personal data are individual details about personal or factual circumstances of a specific or identifiable natural person ("data subject"). The agreement deals with the processing of personal data ("order data").

Against this background, the parties agree as follows:

1. Subject and duration of the contract

(1) Subject

The main subject of the contract for the handling of data is the performance of the following tasks by the contractor: Provision of a cloud-based Data-Feed-Management-Platform for maintenance and optimization of contractor’s data.

(2) Duration

The duration of this contract (term) is the duration of the service level agreement.

2. Specification of the content of the order

(1) Nature and purpose of the intended processing of data

The nature and purpose of the processing of personal data by the contractor for the client are specifically described in the service agreement.

The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another Contracting State to the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the client and may only take place if the special requirements of art. 44 et seq. GDPR are met.

(2) Type of data

The subject of the processing of personal data is the following data types/categories (enumeration/description of the data categories)

- ✔ Person master data (contact list of the working group, i.d.R no data subject)
- ✔ Communication data (e.g., telephone, e-mail)
- ✔ Contract master data (contractual relationship, product or contract interest)
- ✔ Billing and payment data

(3) Categories of data subjects

The categories of persons affected by processing include:

- ✔
- ✔ Employees of the client
- ✔ Suppliers and partners of the client

3. Technical-organizational measures

(1) The contractor must document the implementation of the technical and organizational measures set out prior to the award of the contract and prior to processing, in particular with regard to the specific execution of the order, and hand them over to the client for review. If accepted by the client, the documented measures become the basis of the contract. Insofar as the inspection/audit of the client results in a need for adjustment, this must be implemented by mutual agreement.

(2) The contractor has to establish security according to art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with art. 5 para. 1, para. 2 GDPR. Overall, the actions to be taken are data security measures and to ensure a level of protection appropriate to the level of risk with regard to the confidentiality, integrity, availability and resilience of the systems. In this context, the state of the art, the costs of implementation and the nature, scope and purpose of the processing as well as the different probability and severity of the risk for the rights and freedoms of natural persons within the meaning of art. 32 para. 1 GDPR must be taken into account. [See details in attachment 1].

(3) The technical and organizational measures are subject to technical progress and further development. In that regard, the contractor is allowed to implement alternative adequate measures. In doing so, the safety level of the specified measures must not be undershot. Significant changes must be documented.

4. Correction, restriction and deletion of data

(1) The contractor may not correct, delete or restrict the processing of the data processed on behalf of the contract, only on the basis of documented instructions from the client. Insofar as an affected person directly addresses the contractor in this regard, the contractor will immediately forward this request to the client.

(2) Insofar as included in the scope of services, the cancellation concept, the right to be forgotten, rectification, data portability and information according to the client's documented instructions are to be ensured by the contractor directly.

(3) The contractor shall support the customer within the scope of his possibilities, if agreed upon. persons affected by the fulfilment of enquiries and claims pursuant to Chapter III of the GDPR and compliance with the obligations set out in Art. 33 to 36 GDPR.

5. Quality assurance and other obligations of the contractor

In addition to compliance with the provisions of this order, the contractor has statutory obligations according to art. 28 to 33 GDPR; In particular, he ensures compliance with the following requirements:

a) Written appointment of a data protection officer who carries out his activity in accordance with art. 38 and 39 GDPR. As an external data protection officer is:

Nils Möllers, Keyed GmbH, Siemensstraße 12, 48341 Altenberge, n.moellers@keyed.de

appointed to the contractor. A change of the data protection officer has to be told the client immediately.

b) The preservation of confidentiality under art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. The contractor will use only employees who are committed to confidentiality and who have been previously familiarized with the data protection regulations that are relevant to them. The contractor and any person subordinate to the contractor who has access to personal data may process such data only in accordance with the instructions of the client, including the powers granted in this contract, unless they are required by law to process them.

c) The implementation and compliance with all technical and organizational measures required for this contract in accordance with art. 28 para. 3 sentence 2 lit. c, 32 GDPR [details in attachment 1].

d) The client and the contractor cooperate with the supervisory authority on request to fulfill their duties.

e) Immediate information to the client about control actions and measures of the supervisory authority, insofar as they relate to this order. This also applies insofar as a competent authority has determined in the context of an administrative or criminal procedure with regard to the processing of personal data in the processing of orders by the contractor.

f) Insofar as the client himself is subject to inspection by the supervisory authority, an administrative offense or criminal proceeding, the liability claim of a data subject or a third party or any other claim in connection with order processing by the contractor, the contractor shall support him to the best of his ability.

g) The contractor shall regularly review the internal processes as well as the technical and organizational measures to ensure that the processing in its area of responsibility complies with the requirements of applicable data protection law and that the protection of the data subject's rights is ensured.

h) verifiability of the technical and organizational measures taken towards the client within the scope of his control powers according to section 7 of this contract.

i) The contractor shall, in accordance with the instructions of the Client, take reasonable measures to prevent further unlawful disclosure by third parties and/or to avert further impairments by the parties concerned. The Supplier shall take all necessary measures to secure data and minimise damage until any instructions have been given by the Customer.

j) The contractor shall support the Customer in complying with its legal obligations, in particular obligations to ensure the security of personal data, reporting obligations in the event of data breakdowns, information obligations vis-à-vis affected parties and supervisory authorities, data protection impact assessments and prior consultations. The same shall also apply if the client is subject to inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a person concerned or a third party or any other claim in connection with order processing. Upon request, the Contractor shall make available to the Client the list of all processing activities to be carried out by the Contractor in copied form in accordance with the relevant legal provisions.

k) The contractor shall inform the contracting authority without delay if he becomes aware of any infringement of the protection of personal data of the contracting authority. The Contractor shall take the necessary measures to secure the data and to reduce possible negative consequences for the persons concerned and shall consult with the Customer without delay.

6. Subcontracting

(1) For the purposes of this regulation, subcontracting means such services which directly relate to the provision of the main service. This does not include ancillary services provided by the contractor, e.g. as a telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing facilities. However, the contractor is obliged to take appropriate and legally compliant contractual agreements and control measures in order to ensure data protection and data security of the client's data, even with outsourced ancillary services.

(2) The contractor may only commission subcontractors (other processors) after prior express written consent from the client.

a) ☐ Subcontracting is prohibited.

b) ☒ The client agrees to the assignment of the following subcontractors under the condition of a contractual agreement in accordance with art. 28 para. 2-4 GDPR:

Company subcontractor	Address/Country	Service
Amazon Web Services, Inc.	410 Terry Avenue North Seattle WA 98109 United States	Cloud Services for Server and Data Hosting
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen Deutschland	Web Hosting and Data Center Provider
Google LLC	1600 Amphitheatre Parkway Mountain View, CA 94043 USA	Cloud Services for Server and Data Hosting
World of Content B.V.	Emmaplein 4 D5211VW 's-Hertogenbosch	Affiliate software provider

c) ☒ The outsourcing to subcontractors or / the change of the existing subcontractor are permissible insofar as:

- the contractor indicates such outsourcing to subcontractors at least 2 weeks in advance in writing or in text form, and
- the client does not object to the planned outsourcing in writing or in text form until the date of transfer of the data to the contractor and
- a contractual agreement in accordance with art. 28 para. 2-4 GDPR is used.

(3) The transfer of personal data of the client to the subcontractor and its initial action shall only be permitted upon submission of all conditions for subcontracting.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the contractor shall ensure that the data protection law is admissible by taking appropriate measures. The same applies if service providers within the meaning of para. 1 sentence 2 are to be used.

(5) Further outsourcing by the subcontractor

⬜ is not allowed;

⬜ requires the explicit consent of the main client (at least in text form);

☒ requires the express consent of the main contractor (at least in text form);

All contractual arrangements in the chain of contract must also be imposed on the additional subcontractor.

7. Control rights of the client

(1) The client has the right to carry out inspections in consultation with the contractor or to have them carried out by examiners to be named in individual cases. He has the right to satisfy himself of the compliance of this agreement by the contractor in his business through spot checks, which are usually timely to register.

(2) The contractor shall ensure that the client can satisfy himself of the compliance with the obligations of the contractor in accordance with art. 28 GDPR. The contractor undertakes to provide the client with the necessary information upon request and, in particular, to prove the implementation of the technical and organizational measures.

(3) The proof of such measures, which do not concern only the concrete order, can take place for example by

- the compliance with approved codes of conduct pursuant to art. 40 GDPR;
- the certification according to an approved certification procedure according to art. 42 GDPR;
- up-to-date certificates, reports or statements of independent bodies (e.g. auditors, data protection officers, IT security departments, privacy auditors, quality auditors);
- the appropriate certification through IT security or privacy audit (e.g. according to BSI basic protection).

(4) The contractor may assert a claim for compensation in order to allow controls by the client.

8. Notification in case of violations of the contractor

(1) The contractor supports the client in compliance with art. 32-36 of the GDPR data security obligations, reporting of data breaches, data protection impact assessments and prior consultations. These include

a) ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing and the predicted likelihood and severity of a possible breach of rights through vulnerabilities, and enable the immediate detection of relevant injury events

b) the obligation to report violations of personal data immediately to the client

c) the obligation to assist the contracting entity in providing information to the person concerned, and to provide him with all relevant information without delay in that connection

d) the support of the client for its data protection impact assessment

e) the assistance of the contracting authority in the context of prior consultations with the supervisory authority

(2) For services that are not included in the terms of reference or that are not the result of a wrongdoing by the contractor, the contractor may claim a fee.

(3) For support services which are not included in the service description or are not due to a misconduct of the contractor, the contractor can claim a remuneration if the expenses exceed the number of 2 audits per year.

(4) The contractor shall be liable to the Client for the subcontractor's compliance with the data protection obligations imposed by the Contractor in accordance with this Section of the Contract. Liability is governed by the provisions of Art. 82 GDPR.

(5) The contractor's legal representatives or vicarious agents shall not be liable for slight negligence. However, this exclusion of liability for slight negligence shall not apply in the event of a breach of a material contractual obligation (cardinal obligation). Cardinal obligations or essential contractual obligations are such obligations of the contractor, the fulfilment of which makes the proper execution of

this concrete contract possible in the first place and on the observance of which the customer may regularly rely; i.e. obligations, the breach of which would endanger the achievement of the purpose of the contract.

9. Authorization of the client

The client alone has the authority to decide or issue instructions for order processing. The Contractor shall act solely on behalf of and in the interest of the Client. The responsibility for compliance with the data protection law and the legality of the order processing as well as for the protection of the rights of the parties concerned lies with the client.

The Contractor shall carry out the order processing exclusively within the framework of the agreement and according to written instructions of the Customer, whereby the instructions shall have priority, or if there is a legal obligation to process. Oral instructions shall be confirmed by the client in writing without delay. The contractor is not entitled to make declarations to the parties concerned without the prior written consent of the client. In the event of a statutory obligation, the Contractor shall notify the Customer of this obligation prior to processing.

The Contractor may not correct, delete or restrict the processing of the order data without the Customer's authorization, but only in accordance with the Customer's instructions in writing. The Contractor shall immediately inform the Customer in writing about all inquiries and complaints of the parties concerned and support the Customer in safeguarding the rights of the parties concerned, e.g. by notification, provision of information or correction, blocking and deletion of order data.

The parties shall observe the relevant data protection regulations within the scope of order processing. If the contractor is of the opinion that an agreement or instruction violates data protection regulations, he will inform the client immediately in writing. The contractor is entitled to suspend the execution of the corresponding instruction until it has been confirmed or changed by the client.

(1) Oral instructions shall be confirmed by the Customer without delay (at least in text form).

(2) The contractor shall inform the customer immediately if he is of the opinion that an instruction violates data protection regulations. The contractor is entitled to suspend the execution of the corresponding instruction until it has been confirmed or changed by the client.

10. Deletion and return of personal data

(1) Copies or duplicates of the data are not created without the knowledge of the client. This does not include backup copies, to the extent necessary to ensure proper data processing, and data required for compliance with statutory retention requirements.

(2) After the conclusion of the contractually agreed work or sooner upon request by the client - at the latest upon termination of the service agreement - the contractor shall have all documents, processing results and utilization results as well as data sets which are related to the contract relationship to hand over client or to destroy it after prior consent in accordance with data protection. The same applies to test and scrap material. The log of the deletion must be submitted on request.

(3) Documentation serving as proof of orderly and proper data processing shall be kept by the contractor according to the respective retention periods beyond the end of the contract. He can hand them over to the client for his discharge at the end of the contract.

11. Secrecy

The contractor will keep the information and documents received in the course of the order processing, in particular the order data, strictly confidential ("business and trade secrets"). The confidentiality obligations shall continue to apply indefinitely even after termination of this agreement.

The duty to maintain secrecy shall not apply or shall cease to exist if the information and documents were already known to the public or the contractor upon conclusion of this agreement or became known to the public after conclusion of this agreement, without the contractor being at fault, or if the

contractor is known to a third party, provided the third party does not breach its own confidentiality obligation when handing over the information. The contractor is liable for these facts.

12. Miscellaneous, General

Changes and additions to this agreement and any of its components, including any warranties of the contractor require a written agreement and the explicit reference to the fact that it is a change or supplement of these terms. This also applies to the waiver of this form requirement.

Should the Client's data be endangered by seizure or confiscation by the Contractor, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall immediately inform the Client thereof.

The Contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Customer as the person responsible within the meaning of the Basic Data Protection Regulation.

Amendments and supplements to this Annex and all its components - including any assurances by the Contractor - shall require a written agreement, which may also be made in an electronic format (text form), and an express reference to the fact that these Terms and Conditions have been amended or supplemented. This also applies to the waiver of this formal requirement.

In the event of any contradictions, the provisions of this annex on data protection shall take precedence over the provisions of the contract. Should individual parts of this appendix be invalid, this shall not affect the validity of the remainder of the appendix.

Jurisdiction is Berlin.

Attachment 1 - Technical and organizational activities

If not applicable, please delete. If necessary, please complete further activities.

1. Confidentiality (Article 32 para. 1 lit. b GDPR)

- Physical access control
  No unauthorized access to data processing systems, for example: magnetic or chip cards, keys, electric strikes, security or gatekeepers, alarm systems, video systems;
- System access control
  No unauthorized system usage, such as: (secure) passwords, automatic locking mechanisms, two-factor authentication, disk encryption;
- Data access Control
  No unauthorized reading, copying, modification or removal within the system, for example: authorization concepts and needs-based access rights, logging of accesses;
- Separation Control
  Separate processing of data collected for different purposes, e.g. Multi-client capability, sandboxing;
- Pseudonymisation (Article 32 para. 1 lit. a of the GDPR; article 25 para. 1 of the GDPR)
  The processing of personal data in such a way that the data can no longer be assigned to a specific data subject without the need for additional information, provided that such additional information is kept separate and subject to appropriate technical and organizational measures;

2. Integrity (Article 32 para. 1 lit. b of the GDPR)

- Relay control
  No unauthorized reading, copying, modification or removal during electronic transmission or transport, for example: encryption, Virtual Private Networks (VPN), electronic signature;
- Entry Control
  Determining if and by whom personal data has been entered, altered or removed in data processing systems, e.g. logging, document management;

3. Availability and resilience (Article 32 para. 1 lit. b GDPR)

- Availability Control
  Protection against accidental or willful destruction or loss, such as: on-site/off-site backup strategy, uninterruptible power supply (UPS), antivirus, firewall, reporting and contingency plans;
- Rapid recoverability (Article 32 para. 1 lit. c GDPR);

4. Procedures for regular review and evaluation (Article 32 para. 1 lit. d GDPR), Article 25 para. 1 of the GDPR)

- Privacy Management;
- Incident-Response-Management;
- Privacy-friendly default settings (Article 25 para. 2 GDPR);
- Order control
  No order data processing within the meaning of Art. 28 GDPR without corresponding instructions of the client, for example: Clear contract design, formalized order management, strict selection of the service provider, compulsory pre-compilation, follow-up checks.

WoC Software Description

This World of Content Software Description specifies the Services ordered by Client under an applicable Order Form.

	• **Subscriptions**

1.1	**Software Subscriptions License**
1.1.2	Product Content Syndication - Consumer Goods & Electronics License (by World of Content)
	• Full Content Syndication Platform License to access WoC Solution for Consumer Goods. • All major functionalities of the solution including but not limited to: A+ Content without support, Data management, Syndication. • Usage for one (1) Language (Data) and ten (10) Retail Export Channels.
1.2	**Additional Software Subscriptions**
1.2.1	Data Management Service (DMS) (by World of Content)

	This service automatically captures product data from a digital artwork using OCR. The technique is trained to automatically recognize mandatory data attributes for the purpose of GDSN. Through AI, the data is incorporated within the GDSN data model without manual intervention.
1.2.2	Additional Data Language (by World of Content)
	• Product Content Syndication by World of Content extended by an additional Language (Data). • Incl. Volume: one (1) Language (Data)
1.2.3	Additional Retail Export Channels - Consumer Goods & Electronics (by World of Content)
	• Provides additional Export Channels to the Product Content Syndication by World of Content allowing the export of data to Retail channels such as Tesco, Albert Heijn, etc on a per country basis. • Incl. Volume: one (1) Retail Export Channel
1.2.4	Additional Marketplace Export Channels - Consumer Goods & Electronics (by World of Content)
	• Provides additional Export Channels to the Product Content Syndication by World of Content allowing the export of data to Marketplace channels such as Amazon or Bol.com on a per country basis. • Incl. Volume: one (1) Marketplace Export Channel.

1.2.5	GDSN datapool connection & support Add-on (by World of Content)
	• Provides to Product Content Syndication by World of Content the access and support towards GDSN data pools on a per datapool & per country basis. • Incl. Volume: one (1) Datapool for one (1) country
1.2.6	Automated Import Connection - API Add-on (by World of Content)
	• Provides to Product Content Syndication by World of Content) an automated import connection on a per datasource basis, to avoid manual importing of data via Excel uploads or manual data entry (typing). This is includes the setup and maintenance of the automated import connection over time. Example of Data Sources could be: PIM, MDM, ERP, etc. • Incl. Volume: 1 Datasource
1.3	**Support Services Subscriptions**
1.3.1	Product and Account Support (by World of Content) [1]
	Product and Account Support is provided by World of Content subject to the specifications in the applicable MSA and relevant Schedule.

[1] Subject to the specifications in the Product and Account Support Service Level Agreement.

	Product and Account Support experts reactively answer Client submitted tickets about either a malfunction of the World of Content Software or questions on functionality, scope or configurations of the World of Content Software. The Client is requested to give as many details as possible, such as links, concrete examples, or screenshots. When communicating malfunctions of the World of Content Software to World of Content, the Client shall reasonably self-diagnose the impact and recommend, in good faith, to World of Content an appropriate Severity Level designation. World of Content shall validate given Severity Level designation or notify Client of a change in the Severity Level designation to a higher or lower level, giving a reason for such change. When communicating non-system issues to World of Content, these can be questions about the functionality of the World of Content Software, scope or best practices in regard to specific setups. The Client will be provided with help articles, step by step explanations or roadmap outlooks in case certain functionalities are planned, but not available yet. If a desired functionality is not available or in the pipeline, the Client can issue a feature request. World of Content responds to Support Incidents based on Severity Levels (as defined below) during Local Office Hours, according to the Central European Time (CET) time zone, as specified in the Product and Account Support Service Level Agreement Schedule of the Master Services Agreement.

World of Content Professional Services Description

This Services Documentation specifies the Professional Services ordered by Client under an applicable Order Form.

- **World of Content Professional Services**

The Scope of these Professional Services is agreed to in a separate Scoping Document. Each Scoping Document will identify the number of Professional Services' hours necessary for the provision of any package below and fulfillment of the identified Scope. Client and Provider will then enter into an Order Form specifying the term and pricing of any Scoping Document.

I.	Managed Services World of Content Software and Dedicated Support Package
	Managed Services World of Content Software and Dedicated Support Package covers initial setup of the Client's user account according to best practices, setup of account and initiation of Client's desired activities through a dedicated World of Content solutions expert. The account and workings on the software will be optimized and structured according to Client's wishes. The Scoping Document may specify any other specific service included in this Package. Requests may either be sent by email or communicated in any requested call, as preferred by the Client. Upon request, World of Content will provide documentation for the Client's user account setup and/or insights into it in scheduled calls, as part of the Professional Services hours included in the Managed Services World of Content Software and Dedicated Support Package. The Managed Services World of Content Software and Dedicated Support Package exclusively covers Services within the World of Content Software and does not involve World of Content to access or operate any third-party tools or systems. The Managed Services World of Content Software and Dedicated Support Package includes the migration of data and initial set-up.

	The Managed Services World of Content Software and Dedicated Support Package does not include World of Content being in direct contact with any third-party providers. Such communication needs to be handled exclusively via the Client. The Managed Services World of Content Software and Dedicated Support Package does not cover the proactive consulting on best practices outside of the World of Content Software. World of Content conducts the Managed Services World of Content Software and Dedicated Support Package under the assumption that the Client will provide key personnel for the period of its duration. This includes at least one person, but ideally a team, who has knowledge about the injected data and its structure, access to an updating data source, strategy with the software and credentials of any external service relied upon, and who oversees the completion of the Managed Services as well as the need for and usage of Professional Services hours included in the package. Invalidation of this assumption may alter the scope of services required and may result in additional cost. The Managed Services World of Content Software and Dedicated Support Package may be ordered at least four weeks before the desired start date. Upon receipt of the request and within three Business Days from receipt, World of Content will provide a Scoping Document where the specific Managed Services applicable to the use case and necessary Dedicated Support Professional Services hours will be indicated. If the submitted Scoping Document cannot be feasibly achieved with the included Professional Services hours, World of Content will provide an estimate on the total amount of Professional Services hours required per month and a new contract will need to be concluded.
II.	Guided Software Training and Onboarding Package
	The Guided Platform Training Package is conducted via remote video calls by a World of Content Software Trainer. The Scoping Document will indicate the total hours of training purchased with the Order and what topics will be addressed in the training, which can be chosen freely by the Client. World of Content's objective is to make the Client's team independent and confident users of the World of Content Software, who are capable of its setup, rollout, and ongoing administration. World of Content's conducts the Guided Software Training and Onboarding Package under the assumption that the Client will provide key personnel throughout its duration. This includes at least one person, but ideally a team, who will be trained as an administrator of the software and oversees the completion of the Guided Software Training and Onboarding Package as well as the

	need for and usage of Professional Services hours included in this package. Invalidation of this assumption may alter the scope of Services required and may result in additional cost. The Guided Software Training and Onboarding Package is provided to Client within 90 days upon execution of the relevant initial Order Form, or, if agreed by the Parties, within 90 days at a later point during the runtime of the applicable Order Form. Upon expiry of this period or the included Professional Services hours, the Services provided as part of the Guided Software Training and Onboarding Package are provided to Client exclusively at the hourly rates for the provision of Professional Services specified in any separate Order Form that Client and Provider may enter into.
II.	Guided Implementation Consulting
	Guided Implementation Consulting is conducted via remote video/phone calls and/or email by a World of Content solutions' expert. The World of Content solutions expert will own the project management of the Client's technical World of Content software implementation. The objective of the implementation is to guide the Client through the setup of their individual World of Content software instance, as detailed in the Scoping Document. The scope of the guided implementation is agreed upon in the Scoping Document and may only cover a portion of the full scope. Consulting is limited to features within the World of Content software and does not include involvement in third-party tools. After successful completion of the Guided Implementation Consulting, the Client will have expert knowledge about the individual account setup and be able to maintain it independently. Interactions can be for a range of tasks connected to the agreed scope, including (but not limited to): ● Project planning and tracking; ● Status updates in form or regular meetings and proactive updates; ● Hands-on support in the setup of various configurations;

	• Guidance on setting up API connections; • Proactive best practices/consultation regarding account setup and functionality to ensure highest possible processing speed and meet user management requirements; World of Content conducts this service under the assumption that the Client will provide key personnel for the period of the Guided Implementation Consulting. This includes at least one person, but ideally a team, who participated in a platform training and/or has foundational knowledge about the World of Content software, has knowledge about the data and its structure, access to how the client wishes to work with World of Content software and desired outcome, has access to any necessary credential, and oversees the completion of the Guided Implementation Consulting as well as the need for and usage of Professional Services hours included in the package. Invalidation of this assumption may alter the scope of Services required and may result in additional costs. The period of the Guided Implementation Consulting will not be extended free of charge to account for delays caused by the Client. If the submitted Scoping Document cannot be feasibly achieved with the ordered Professional Services hours, World of Content will provide an estimate on the total amount of Professional Services hours required. All overage hours required to achieve the agreed Scope in excess of the Professional Services hours included in the Guided Implementation Consulting are charged separately and subject to a separate agreement with Client.
V.	Managed Migration Package
	Managed import and/or export migration will be conducted by a World of Content solutions expert. Managed import migration includes the migration to a new data source, including adjustment of configuration to data source setup, and remapping of attributes in the World of Content software, as well as a test run before the launch day of the provided new data source. Within this test run the World of Content solutions expert will point out what exactly changed from the former data source to the new one and create an overview on which attributes need to be remapped/adjusted. According to the time schedule provided by the Client, World of Content will ensure deactivation of export updates during data source switch and activate exports after successful migration.

	Managed export migration includes the migration to a new export channel destination, such as switching from a feed delivery to an API delivery or vice versa. The World of Content solutions expert conducting the migration will ensure that all attributes are mapped to the channel's requirements, that the provided credentials are leading to a successful upload of data, and the export is completed without errors on World of Content's side. World of Content's conducts the Managed Migration Package under the assumption that the Client will provide key personnel for the duration of the period of the Managed Migration Package. This includes at least one person, but ideally a team, who has knowledge about the injected data and its structure, access to credentials, and oversees the need for and usage of the provided Professional Service hours. Invalidation of this assumption may alter the scope of Services required and may result in additional costs. If the submitted Scoping Document cannot be feasibly achieved with the Professional Service hours included in the Managed Migration Package, World of Content's will provide an estimate of Professional Service hours. All overage hours required to achieve the agreed Scope in excess of the Professional Services hours included in the Managed Migration Package are charged separately and subject to a separate agreement with Client. The Managed Migration Package needs to be ordered at least two weeks before the desired migration date.

World of Content

Security & Privacy Policies

S. Lit

202106-v1.1

Introduction

World of Content has created a series of policies to help us with data security and privacy. These policies are distributed to every workforce member and are regularly updated and expanded to reflect changes in the organization.

Some of these policies are adapted from the Datica HIPA Compliance Policies, which open sourced well documented and audited policies under a Creative Commons License.

Any questions regarding the following material can be directed towards the Security Officer:

Simon Lit
simon@worldofcontent.com

Note: The following document is an exported copy of our security and privacy policies and not the official version as distributed to the World of Content workforce.

Commonly Used Terms

- "Production Systems", systems that create, receive, store, or transmit user generated data.
- "Production Data", any data that resides on production systems.
- "Personal Data", any information that relates to an identified or identifiable living individual.
- "Third Party Companies", any party that is not registered as World of Content B.V. in The Netherlands, and include any associated (international) businesses like joint ventures, partner companies and contracted clients.
- "GDPR", General Data Protection Regulation.
- "Workforce Member", any individual that performs work for World of Content including but not limited to, employees, freelancers, and interns.
- "Security Officer", the highest authority on privacy and security.
- "Quality Management System", a system used for tracking and resolving issues. In our case this is Gitlab.
- "Customer", a representative of the contractually defined legal entity customer of one the World of Content created systems.
- "Partner", a representative of a legal entity sharing resources with World of Content. 1

Index

Introduction 1 Commonly Used Terms 1 Index 2

1. Data Classification Policy 4 1.1 Data Classification 4 1.2 Risk Assessment 4

2. Access Control Policy 5 2.1 Access Establishment 5 2.2 Person or Entity Authentication 6 2.3 Employee Workstation Use 7 2.4 Employee Termination Procedures 7 2.5 Password Management 7

3. Personal Data Processing Policy 9 3.1 Data Protection 9 3.2 Data Storage 9 3.3 Data Access 9 3.4 Data Transfers 10

3.4.1 Non Restricted Transfers 10 3.4.2 Restricted Transfers 10 3.5 Data Retention 11

4. Data Integrity Policy 12 4.1 Monitoring 12 4.2 Patch Management 12 4.3 System Security 12 4.4 Production Data Security 12 4.5 Vulnerability Scanning 13 4.6 Backup Policy and Procedures 14

5. Auditing Policy 15 5.1 Auditing Policies 15 5.2 Audit Requests 17 5.3 Review and Reporting of Audit Findings 17 5.4 Audit Log Security Controls and Backup 18 5.5 Workforce Training, Education, Awareness and Responsibilities 18 5.6 External Audits of Information Access and Activity 18

6. Approved Tools Policy 19 6.1 Approved Tools 19

6.2 Tool Approval 19

7. Configuration and Change Management Policy 21 7.1 Configuration Management Policies 21 7.2 Provisioning Production Systems 21 7.3 Changing Existing Systems 22 7.4 Software Development Procedures 22 7.5 Software Builds 23

8. Incident Response Policy 24 8.1 Incident Management Policies 24 8.2.1 Identification Phase 25 8.2.2 Containment Phase (Technical) 26 8.2.3 Eradication Phase (Technical) 27 8.2.4 Recovery Phase (Technical) 28 8.2.5 Follow-up Phase (Technical and Non-Technical) 29 8.2.6 Periodic Evaluation 29

1. Data Classification Policy

1.1 Data Classification

1. Any system and its data is classified and documented in one of the following categories:
    - Secret: Reserved for sensitive data like personal information, user generated data, secrets, and access to critical systems. Access to secret data can only be granted by the highest security authority, the Security Officer in our case.
    - Confidential: Any company information that is not meant to be shared publicly, including, but limited to, source codes and usage statistics. Access to this data is contractually managed.
    - Public: Any information that is meant for the public domain, for example a blog article.

1.2 Risk Assessment

1. The Security Officer is responsible for granting access to Secret Data as explained in the Access Control Policy.
2. For every workforce member a risk assessment is created based on which information and systems the user has access to. This is managed and maintained by the Security Officer.
    - When assessing the risk someone poses of leaking, deleting or otherwise misusing secret or confidential information the Security Officer should create a distinction between read-only and update rights to this information.
    - Permanent deletion of secret and confidential information should not be possible without explicit permission of the Security Officer.

2. Access Control Policy

Access to World of Content systems and applications is limited for all users, including but not limited to employees, consultants, interns, and contracted partners. Access by any entity is always granted on a minimum necessary basis. These guidelines have been established to limit unauthorized access to any of the organization's systems.

2.1 Access Establishment

1. Requests for access to World of Content systems and applications are made formally using the following process:
2. A World of Content workforce member initiates the access request by creating an Issue in the World of Content Quality Management System.
    - User identities must be verified prior to granting access to new accounts.

    - ○ Identity verification must be done in person where possible; for remote employees, identities must be verified over the phone.
    - ○ For new accounts, the method used to verify the user's identity must be recorded on the Issue.
3. The Security Officer will grant access to systems as dictated by the employee's job title. If additional access is required outside of the minimum necessary to perform job functions, the requester must include a description of why the additional access is required as part of the access request.
4. Once the review is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation. 5. If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required. The Security Officer then grants requested access. ○ New accounts will be created with a temporary secure password that meets all requirements from Password Management in §2.5, which must be changed on the initial login.
    - ○ All password exchanges must occur over an authenticated channel. ○ All password exchanges must either be secured by end-to-end encryption or the password must be split and exchanged using at least two different channels.
    - ○ Access grants are accomplished by leveraging the access control mechanisms built into the systems. Account management for non-production systems may be delegated to a workforce member at the discretion of the Security Officer.
6. Access is not granted until receipt, review, and approval by the Security Officer.
7. The request for access is retained for future reference.
8. All access to World of Content systems and services is reviewed and updated on a bi-annual basis to ensure proper authorizations are in place commensurate with job functions.

9. Access to production systems is controlled using centralized user management and authentication.
10. Temporary accounts are not used unless absolutely necessary for business purposes.
    - ○ Accounts are reviewed every 90 days to ensure temporary accounts are not left unnecessarily.
    - ○ Accounts that are inactive for over 90 days are removed.
11. All application to application communication using service accounts is restricted and not permitted unless absolutely needed. Automated tools are used to limit account access across applications and systems.
12. Access is granted through encrypted, VPN tunnels that utilize two-factor authentication.
    - ○ Two-factor authentication is accomplished using a Time-based One-Time Password (TOTP) as the second factor.

    - VPN connections use 256-bit AES 256 encryption, or equivalent.
    - VPN sessions are automatically disconnected after 30 minutes of inactivity.

13. In cases of increased risk or known attempted unauthorized access, immediate steps are taken by the Security Officer to limit access and reduce risk of unauthorized access.
14. Direct system to system, system to application, and application to application authentication and authorization are limited and controlled to restrict access.

2.2 Person or Entity Authentication

1. Role based access categories for each World of Content system and application are pre-approved by the Security Officer, or an authorized delegate of the Security Officer.
2. World of Content utilizes hardware and software firewalls to segment data, prevent unauthorized access, and monitor traffic for denial of service attacks.
3. Each workforce member has and uses a unique user ID and password that identifies him/her as the user of the information system.
4. Generic or shared accounts are not allowed on any of the World of Content systems.
5. Each Customer and Partner has and uses a unique user ID and password that identifies him/her as the user of the information system.
6. All Customer support desk interactions must be verified before support personnel will satisfy any request having information security implications.
7. Passwords requirements mandate strong password controls (see below) and are not displayed or transmitted in plain text at any time.

2.3 Employee Workstation Use

All workstations at World of Content are company owned:

1. Workstations may not be used to engage in any activity that is illegal or is in violation of organization's policies.
2. Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization's best interests.
3. Solicitation of non-company business, or any use of organization's information systems/applications for personal gain is prohibited.

2.4 Employee Termination Procedures

1. The Human Resources Department (or other designated department), users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitating completion of the "Termination Checklist".
2. The Human Resources Department, users, and supervisors are required to notify the Security Officer to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report): ○ The user has been using their access rights inappropriately;
    ○ A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);
    ○ An unauthorized individual is utilizing a user's User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).
3. The Security Officer will terminate users' access rights immediately upon notification, and will coordinate with the appropriate workforce member to terminate access to any non-production systems managed by those employees.
4. The Security Officer audits and may terminate access of users that have not logged into the organization's information systems/applications for an extended period of time.

2.5 Password Management

1. User IDs and passwords are used to control access to World of Content systems and may not be disclosed to anyone for any reason.
2. Users may not allow anyone, for any reason, to have access to any information system using another user's unique user ID and password.
3. On all production systems and applications in the World of Content environment, and where supported, password configurations are set to require:
    ○ a minimum length of 8 characters;

    ○ a mix of uppercase characters, lower case characters, and numbers or special characters;
    ○ a 90-day password expiration, or 60-day password expiration for administrative accounts;
    ○ prevention of password reuse using a history of the last 6 passwords; ○ where supported, modifying at least 4 characters when changing passwords; 4. 2 Factor Authentication (2FA) must be enabled where possible. The authentication factors could be:
    ○ Passwords;
    ○ Security tokens;
    ○ USB sticks with a secret token;

- Biometrics;

5. All system and application passwords must be stored and transmitted securely.
   - Where possible, passwords should be stored in a hashed format using a salted cryptographic hash function (SHA-256 or equivalent).
6. Passwords are inactivated immediately upon an employee's termination (refer to the Employee Termination Procedures in §2.4).
7. All default system and application passwords are changed before deployment to production.
8. Upon initial login, users must change any passwords that were automatically generated for them.
9. Password change methods must use a confirmation method to correct for user input errors.
10. All passwords used in configuration scripts must be environment based, and securely stored.
11. If a user believes their user ID has been compromised, they are required to immediately report the incident to the Security Officer.

3. Personal Data Processing Policy

3.1 Data Protection

● Personal Data is classified as "Confidential". See Data Classification Policy §1. ● World of Content must comply with the European data protection law and principles outlined in the General Data Protection Regulation(“GDPR”), which means that personal data is:

- Collected only for valid and documented purposes and not used in any way

that is incompatible with those purposes;
    - Accurate and kept up to date;
    - Stored only for as long as necessary;
    - Kept securely and protected against unauthorized access;
    - Protected against loss or destruction using appropriate technical and organizational measures;
- The organization ensures that any associate or employee having to access personal information:
    - Have received appropriate training on their responsibilities;
    - Have all their actions logged and available for auditing;

3.2 Data Storage

- Installation of Personal Data on systems not owned by World of Content must be approved by the Customer or Partner and the Security Officer.
- If not done prior to transmittal, Personal Data should be scrubbed immediately upon storage, to eliminate storage of data not related to the originally purpose of processing.
- Personal Data must be stored in a manner that ensures it is sufficiently segregated from other data, to ensure proper access controls.
- Hard disks containing Personal Data must use disk level encryption consistent with current industry best practices.
- All systems housing Personal Data must have active anti-virus protection. ● Members of the World of Content workforce must not store Personal Data on their company workstation or mobile device.

3.3 Data Access

Requesting and granting access to any of the World of Content systems is outlined in the Access Control Policy.

3.4 Data Transfers

When personal data has to be processed by third party companies, for Error Tracking or Usage Statistics for example, we have to send that data to the servers of that third party company. These cases are outlined below:

3.4.1 Non Restricted Transfers

Transferring personal data to Third Party Companies within the EEA, including but not

limited to user ids, emails, and names, is regulated under the GDPR. For these transfers the following rules apply:

- Active members of the EEA are listed here.
- Data transfers to a company within the EEA is only allowed in the following circumstances:
    - Incidental data transfers are allowed only if approved by the Security Officer.
    - Regular data transfers are only allowed to one the approved tools as described in Approved Tools Policy §6.1.
- The Security Officer is responsible for receiving permission from the user for the data transfer, whether contractually or explicitly by receiving written consent. ● Data transfers are only allowed when a Data Processing Addendum is in place. More information about DPA's can be found here.
- Data transfers for both incidental and regular data transfers are documented on:
    - Company details including name and country;
    - Date (or date range if regular);
    - General description of the data;
    - Reason for transferring data;
- Data transfers contain only the minimum required data to adequately perform the intended action by the third party.

3.4.2 Restricted Transfers

A transfer of personal data outside the protection of the GDPR (which we refer to as a 'restricted transfer'), most often involves a transfer from inside the EEA to a country outside the EEA. For these transfers we maintain the following guidelines:

- On top of the policy outlines as described in §3.4.1 of this document, data can only be transferred if approved by the following process:
    - Do we need to make a restricted transfer of personal data in order to meet our purposes? If no, the transfer without any personal data is approved. ○ Has the EU made a positive 'adequacy decision' in relation to the country or territory where the receiver is located or a sector which covers the receiver? If yes, the transfer is approved.
    - Have we put in place one of the 'appropriate safeguards' referred to in the GDPR? If yes, the transfer is approved.

    - Does an exception provided for in the GDPR apply? If yes, the transfer is approved.
    - If none of the questions found a provision which permits the restricted transfer, then that restricted transfer is not approved in accordance with the GDPR.

Note: since the US-EU Privacy Shield is no longer valid as of July 2020, the USA is

not deemed adequate.

3.5 Data Retention

All personal data and user generated data is retained for the duration of the contract, which is usually a year over year recurring contract. After the contract has expired data will be deleted within one month but might remain in our backups for a maximum of one year. We collect the following data with the following reasons:

- Functional data, like products, exports, account data from my.worldofcontent.com; ○ This is the data the users stores in our database to use our primary services. ○ Data will remain in backups for one year after deletion.
- System logs, every time the user triggers an action like export, image resize, etc. a log is created with detailed information about the request;
  - ○ We use these logs for finding bugs and performance issues. We don't store any information about the user, but filenames might reference user generated data.
  - ○ These logs automatically expire after 1 month
- System errors, every time an exception occurs we log detailed information about that and previous requests;
  - ○ We use these logs for finding and resolving bugs. We don't store any information that is relatable to a specific user, but we might reference a model id that is created by a user. For example if the client created a product and something went wrong, we might reference the id or name of that product in one of our logs.
  - ○ The bugs are auto resolved after one year.

4. Data Integrity Policy

World of Content takes data integrity seriously. We strive to assure data is protected from unauthorized access and that it is available when needed. The following policies drive many of our procedures and technical settings in support of the World of Content mission of data protection.

4.1 Monitoring

1. All access to Production Systems are logged. This is done following the Auditing Policy.
2. All alterations to Production Data, whether this is done directly in the database or by users of any of the World of Content systems, are also logged according to the Auditing Policy.

4.2 Patch Management

1. Software patches and updates will be applied to all systems in a timely manner. In the case of routine updates, they will be applied after thorough testing. In the case of updates to correct known vulnerabilities, priority will be given to testing to speed the time to production. Critical security patches are applied within 30 days from testing and all security patches are applied within 90 days after testing.

4.3 System Security

1. All Production Systems must disable services that are not required to achieve the business purpose or function of the system.
2. Production systems are monitored using IDS systems. Suspicious activity is logged and alerts are generated.
3. Vulnerability scanning of Production Systems must occur on a predetermined, regular basis, no less than annually. Currently this is done during every production and development build (at least once per day). Scans are reviewed by the Security Officer, and retained for future reference.
4. System, network, and server security is managed and maintained by the Security Officer in conjunction with the Dev Ops team.
5. Up-to-date system lists and architecture diagrams are kept for all production environments.

4.4 Production Data Security

1. Appropriate safeguards are in place to reduce the risk of compromise of production data, this includes but is not limited to:

    - Review controls designed to protect Production Data from improper alteration or destruction;
    - Access logs are available for Production Data and automated monitoring is in place for potential security incidents;
    - Personal data is segmented and only accessible to workforce members

authorized to access data;

2. All Production Data is stored on encrypted disks, backups are also encrypted before transmission.

4.5 Vulnerability Scanning

World of Content is proactive about information security and understands that vulnerabilities need to be monitored on an ongoing basis. World of Content has multiple systems in place to pro-actively find and resolve security vulnerabilities.

1. We use the following tools for automatically finding security vulnerabilities during production and development builds:
    - Gitleaks. Gitleaks is a SAST tool for detecting hardcoded secrets like passwords, api keys, and tokens in git repos. Gitleaks aims to be the easy-to-use, all-in-one solution for finding secrets, past or present, in your code.
    - ESLint Security. This project will help identify potential security hotspots, but finds a lot of false positives which need triage by a human.
    - PHPCS Security Audit. phpcs-security-audit is a set of PHP_CodeSniffer rules that finds vulnerabilities and weaknesses related to security in PHP code.
    - Amazon ECR image scanning. Amazon ECR image scanning helps in identifying software vulnerabilities in your container images. Amazon ECR uses the Common Vulnerabilities and Exposures (CVEs) database from the open source Clair project and provides you with a list of scan findings.
2. If new vulnerabilities are found during review, the process outlined below is used to test those vulnerabilities. Once those steps are completed, the Issue is then reviewed again.
3. Once the review is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review.
4. If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
5. In the case of new vulnerabilities, the following steps are taken:
    - All new vulnerabilities are verified manually to assure they are repeatable. Those not found to be repeatable are manually tested after the next vulnerability scan, regardless of if the specific vulnerability is discovered again.

- Vulnerabilities that are repeatable manually are documented and reviewed by the Security Officer to see if they pose a serious risk. Based on the risk assessment the security vulnerability is mitigated in a timely manner.

6. Penetration testing is performed regularly as part of the World of Content vulnerability

management policy.
○ External penetration testing is performed annually by a third party. ○ Internal penetration testing is performed quarterly. Below is the process used to conduct internal penetration tests.
■ The Security Officer initiates the penetration test by creating an Issue in the World of Content Quality Management System.
■ The Security Officer, or a Security Engineer assigned by the Security Officer, is assigned to conduct the penetration test.
■ Gaps and vulnerabilities identified during penetration testing are reviewed, with plans for correction and/or mitigation, by the Security Officer before the Issue can move to be approved.
■ Once the testing is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further testing and review.
■ If the Issue is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
7. This vulnerability policy is reviewed on a quarterly basis by the Security Officer.

4.6 Backup Policy and Procedures

1. All data in World of Content production systems are backed up daily. 2. The World of Content Dev Ops Team is designated to be in charge of backups. 3. Dev Ops Team members are trained and assigned to complete backups and manage the backup media.
4. Backups are securely encrypted and stored in a manner that protects them from loss or environmental damage.
5. Backups are annually tested to make sure that files can be successfully restored. 14

5. Auditing Policy

World of Content safeguards the confidentiality, integrity, and availability of data, applications, systems, and networks in order to ensure business continuity and client trust. Therefore it will audit access and activity to detect, report, and guard against:

- Network vulnerabilities and intrusions;
- Breaches in confidentiality and security;
- Performance problems and flaws in applications;
- Improper alteration or destruction of user generated data;
- Out of date software and/or software known to have vulnerabilities.

5.1 Auditing Policies

1. Responsibility for auditing information system access and activity is assigned to the World of Content Security Officer. The Security Officer shall:

    - Assign the task of generating reports for audit activities to the workforce member responsible for the application, system, or network;
    - Assign the task of reviewing the audit reports to the workforce member responsible for the application, system, or network, to the Security Officer, or any other individual determined to be appropriate for the task;
    - Organize and provide oversight to a team structure charged with audit compliance activities (e.g., parameters, frequency, sample sizes, report formats, evaluation, follow-up, etc.).

2. World of Content auditing processes shall address access and activity at the following levels listed below. Auditing processes may address date and time of each log-on attempt, date and time of each log-off attempt, devices used, functions performed, etc.

    - User: User level audit trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and data and services accessed.
    - Application: Application level audit trails generally monitor and log all user activities, including data accessed and modified and specific actions. ○ System: System level audit trails generally monitor and log user activities, applications accessed, and other system defined specific actions.
    - Network: Network level audit trails generally monitor information on what is operating, penetrations, and vulnerabilities.

3. World of Content shall log all incoming and outgoing traffic to into and out of its environment. This includes all successful and failed attempts at data access and editing. Data associated with this data will include origin, destination, time, and

other relevant details that are available to World of Content.

4. World of Content's Security Officer is authorized to select and use auditing tools that are designed to detect network vulnerabilities and intrusions. Such tools are

explicitly prohibited by others, including other workforce members, without the explicit authorization of the Security Officer. These tools may include, but are not limited to:

- ○ Scanning tools and devices;
- ○ Password cracking utilities;
- ○ Network "sniffers".
- ○ Passive and active intrusion detection systems.

5. The process for review of audit logs, trails, and reports shall include:

   ○ Description of the activity as well as rationale for performing the audit. ○ Identification of which World of Content workforce members will be responsible for review (workforce members shall not review audit logs that pertain to their own system activity).
   ○ Frequency of the auditing process.
   ○ Determination of significant events requiring further review and follow-up. ○ Identification of appropriate reporting channels for audit results and required follow-up.

6. Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), whether publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.

   ○ Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services - separation of duties).
   ○ Testing shall be done on a routine basis, currently monthly.

7. Software patches and updates will be applied to all systems in a timely manner as described in Data Integrity §4.2.

5.2 Audit Requests

1. A request may be made for an audit for a specific cause. The request may come

from a variety of sources including, but not limited to the Security Officer, as workforce member or an application user.

2. A request for an audit for specific cause must include time frame, frequency, and nature of the request. The request must be reviewed and approved by World of Content's Security Officer.

5.3 Review and Reporting of Audit Findings

1. Audit information that is routinely gathered must be reviewed in a timely manner by the responsible workforce member(s).
2. The Security Officer initiates the log review by creating an Issue in the World of Content Quality Management System.
3. The Security Officer, or a member of World of Content DevOps team assigned by the Security Officer, is assigned to review the logs.
4. Relevant audit log findings are added to the Issue; these findings are investigated in a later step. Once those steps are completed, the Issue is then reviewed again. 5. Once the review is completed, the Security Officer approves or rejects the Issue. Relevant findings are reviewed at this stage. If the Issue is rejected, it goes back for further review and documentation. The communications protocol around specific findings are outlined below.
6. If the Issue is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.
7. The reporting process shall allow for meaningful communication of the audit findings to those workforce members, Customers, or Partners requesting the audit. ○ Significant findings shall be reported immediately in a written format. World of Content's security incident response form may be utilized to report a single event.
    ○ Routine findings shall be reported to the sponsoring leadership structure in a written report format.
8. Reports of audit results shall be limited to internal use on a minimum necessary/need-to-know basis. Audit results shall not be disclosed externally without administrative and/or legal counsel approval.
9. Security audits constitute an internal, confidential monitoring practice that may be included in World of Content's performance improvement activities and reporting. Care shall be taken to ensure that the results of the audits are disclosed to administrative level oversight structures only and that information which may further expose organizational risk is shared with extreme caution.
10. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible workforce members.

5.4 Audit Log Security Controls and Backup

1. Audit logs shall be protected from unauthorized access or modification, so the

information they contain will be made available only if needed to evaluate a security incident or for routine audit activities as outlined in this policy.
2. All audit logs are protected in transit and encrypted at rest to control access to the content of the logs.

5.5 Workforce Training, Education, Awareness and Responsibilities

1. World of Content workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and Personal Data. World of Content's commitment to auditing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies. World of Content workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the auditing process detect a workforce member's failure to comply with organizational policies.

5.6 External Audits of Information Access and Activity

1. Prior to contracting with an external audit firm, World of Content shall:
    - ○ Outline the audit responsibility, authority, and accountability;
    - ○ Choose an audit firm that is independent of other organizational operations;
    - ○ Ensure technical competence of the audit firm staff;
    - ○ Require the audit firm's adherence to applicable codes of professional ethics;
    - ○ Assign organizational responsibility for supervision of the external audit firm.

6. Approved Tools Policy

World of Content uses a set of tools used by members of the workforce. These software tools are either self-hosted, with security managed by World of Content, or they are hosted by a Subcontractor with appropriate business associate agreements in place to preserve data integrity. These tools and the approval of new tools are outlined below.

6.1 Approved Tools

- **Gitlab**. GitLab is an open source tool built on top of Git and is hosted and secured by World of Content. It is utilized for storage of configuration scripts and other infrastructure automation tools, as well as for source and version control of application code.
- **Google Suite**. Google Suite is used for email exchange, file storage, calendars, and document collaboration.
- **Sentry**. Sentry is a service for tracking exceptions in production environments. ● **Mailgun**. Mailgun is a service for sending and receiving emails from code. This is used to automatically notify users of World of Content built services when certain actions are performed.
- **Google Analytics**. Google Analytics is used to track usage statistics of World of content services.
- **MailChimp**. MailChimp is used for communicating in bulk with all World of Content associates, employees, and users.
- **Amazon Web Services**. Amazon Web Services is used for hosting the infrastructure of all World of Content created systems demanding high availability.
- **Hetzner**. Hetzner is used for hosting the infrastructure of systems used by World of Content.
- **Slack**. Slack is used as the main business communication channel. ● **UptimeRobot**. UptimeRobot is used to detect if all internet facing apps are responding.
- **Jira**. Jira is used for technical support, e.g. for reporting a bug.

6.2 Tool Approval

1. When using a new tool to process confidential or secret data, the tool must be approved by the Security Officer. Tools are only approved when:
    - The tool is deemed required or critical for business continuity;
    - When a Data Processing Addendum is in place;
    - When the data is only processed in the EEA. If this is not the case the transfer of data automatically falls into the "Restricted Transfer" category. Data can only be transferred if it is compliant with Personal Data Processing §3.4.2;

2. All tools are reviewed before and during use to detect, report, and guard against any form of misuse as described in Auditing Policy §5.1 (Hereafter: "flaw") according to the following interval:
    - ○ After the finding of a flaw;
    - ○ On a quarterly basis;
3. Reviewing tools as well as further investigation into discovered flaws is the responsibility of the Security Officer. Tools are investigated regularly for the following flaws:
    - ○ User accounts compliance according to Access Control Policy; ○ Personal data processing compliance according to Personal Data Processing Policy;
    - ○ Data integrity compliance according to Data Integrity Policy;
4. Approved tools are added to the list above and to the "System Access Control Overview" document by the Security Officer or approved delicate.

7. Configuration and Change Management Policy

World of Content standardizes and automates configuration and deployments using different tools for security scanning, change log creations, infrastructure upgrades, and scalability settings. These are described in the policy below:

7.1 Configuration Management Policies

1. All World of Content production infrastructure is hosted using Amazon Web Services (AWS).
2. No systems are deployed into AWS environments without approval of the Head of Development and the Security Officer.
3. All changes to production systems, network devices, and firewalls are approved by the Security Officer before they are implemented to assure they comply with security requirements.
4. The configuration of systems deployed to AWS are managed by CloudFormation:
    - CloudFormation templates are stored in a central repository;
    - All procedures as described in Software Development Procedures §7.4 apply;
5. All changes to production systems are tested before they are implemented in production.
6. Implementation of approved changes are only performed by members of the World of Content workforce.
7. All frontend functionality (developer dashboards and portals) is separated from backend (database and app servers) systems by being deployed on separate servers or containers.
8. All software and systems are tested using appropriate testing techniques, which include unit tests, end to end tests, and integration tests.
9. World of Content utilizes development and staging environments that mirror production to assure proper function.
10. All committed code is reviewed using merge requests to assure software code quality and proactively detect potential security issues in development.

7.2 Provisioning Production Systems

1. Before provisioning any systems, Dev Ops team members must file a request in the World of Content Quality Management System.
2. The Head of Development, or an authorized delegate, must approve the provisioning request before any new system can be provisioned, an exception to this is the provisioning of new instances of an existing system for scalability.
3. Once provisioning has been approved, the Dev Ops team member can configure the new system.

4. Once the system has been provisioned, the ops team member must contact the Security Officer to inspect the new system. The Security Officer or a delegate will verify that baseline security measures have been applied including, but not limited to, verifying the following items:
    - Removal of default users used during provisioning.
    - Network configuration for system.
    - Data volume encryption settings.
    - Intrusion detection and virus scanning software installed.
5. The new system may be rotated into production once the Head of Development and Security Officer verify all the provisioning steps listed above have been correctly followed and has marked the Issue with the "Approved" state.

7.3 Changing Existing Systems

1. Subsequent changes to already-provisioned systems are handled by updating CloudFormation templates, and can only be performed by members of the Dev Ops team.
2. Configuration changes must be initiated by creating a Merge Request in GitLab.
3. In all cases, before rolling out the change to production, the change must be checked by the Security Officer or an approved delegate.
4. Once the request has been approved by the Security Officer or an approved delegate, the Dev Ops team member may roll out the change into production environments.

7.4 Software Development Procedures

1. All development uses feature and hotfix branches based on the main development branch for the current release. Any changes required for a new feature or defect fix are committed to that branch.
    - These changes must be covered under 1) a unit test where possible, or 2) integration tests.
    - Integration tests are required if unit tests cannot reliably exercise all facets of the change.
2. Developers are strongly encouraged to follow the commit message conventions suggested by GitHub.
    - Commit messages should be wrapped to 72 characters.
    - Commit messages should be written in the present tense. This convention matches up with commit messages generated by commands like git merge and git revert.
3. Once the feature and corresponding tests are complete, a merge request will be created using the GitLab web interface. The merge request should indicate which

feature or defect is being addressed and should provide a high-level description of the changes made. Before merging, merge request must:
    - Not have any unresolved issues or comments;
    - Be approved by at least one other team member when deploying to Development;
    - Be approved by the Security Officer or an approved delegate, and a Senior Developer when deploying to Staging or Production;
4. Merge request must always link one or multiple Issues which it tends to resolve, each issue must have labels indicating the nature of the issue.
5. Code reviews are performed as part of the merge request procedure. Once a change is ready for review, the author(s) will notify other engineers using an appropriate mechanism, typically via an "@channel" message in Slack.
    - Other members of the development team will review the changes, using the guidelines above.
    - Members of the development team should note all potential issues with the code; it is the responsibility of the author(s) to address those issues or explain why they are not applicable.

7.5 Software Builds

- All environment specific builds of World of Content systems containing application code must be stored for at least 6 months and contain at least:
    - The environment target;
    - An increasing and unique version or build number;
    - A change log;
    - Any artifacts containing information about security vulnerabilities;

8. Incident Response Policy

World of Content implements an information security incident response process to consistently detect, respond to, and report incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.
The incident response process addresses:

- Continuous monitoring of threats through intrusion detection systems (IDS) and other monitoring applications;
- Establishment of an information security incident response team;
- Establishment of procedures to respond to media inquiries;
- Establishment of clear procedures for identifying, responding, assessing, analyzing, and follow-up of information security incidents;
- Workforce training, education, and awareness on information security incidents and required responses; and
- Facilitation of clear communication of information security incidents with internal, as well as external, stakeholders.

8.1 Incident Management Policies

The World of Content incident response process follows the process recommended by SANS, an industry leader in security. Process flows are a direct representation of the SANS process which can be found below.

1. **Events** - Any observable computer security-related occurrence in a system or network with a negative consequence. Examples:

- Hardware component failing causing service outages.
- Software error causing service outages.
- General network or system instability.

2. **Precursors** - A sign that an incident may occur in the future. Examples:
    - Monitoring system showing unusual behavior.
    - Audit log alerts indicated several failed login attempts.
    - Suspicious emails targeting specific World of Content staff members with administrative access to production systems.
3. **Indications** - A sign that an incident may have occurred or may be occurring at the present time. Examples:
    - Antivirus alerts for infected files.
    - Excessive network traffic directed at unexpected geographic locations.
4. **Incidents** - A violation of computer security policies or acceptable use policies, often resulting in data breaches. Examples:
    - Unauthorized disclosure of Personal Information.
    - Unauthorized change or destruction of Personal Information.
    - A data breach accomplished by an internal or external entity.

    - A Denial-of-Service (DoS) attack causing a critical service to become unreachable.

World of Content workforce members must report any unauthorized or suspicious activity seen on production systems or associated with related communication systems (such as email or Slack). In practice this means keeping an eye out for security events, and letting the Security Officer know about any observed precursors or indications as soon as they are discovered.

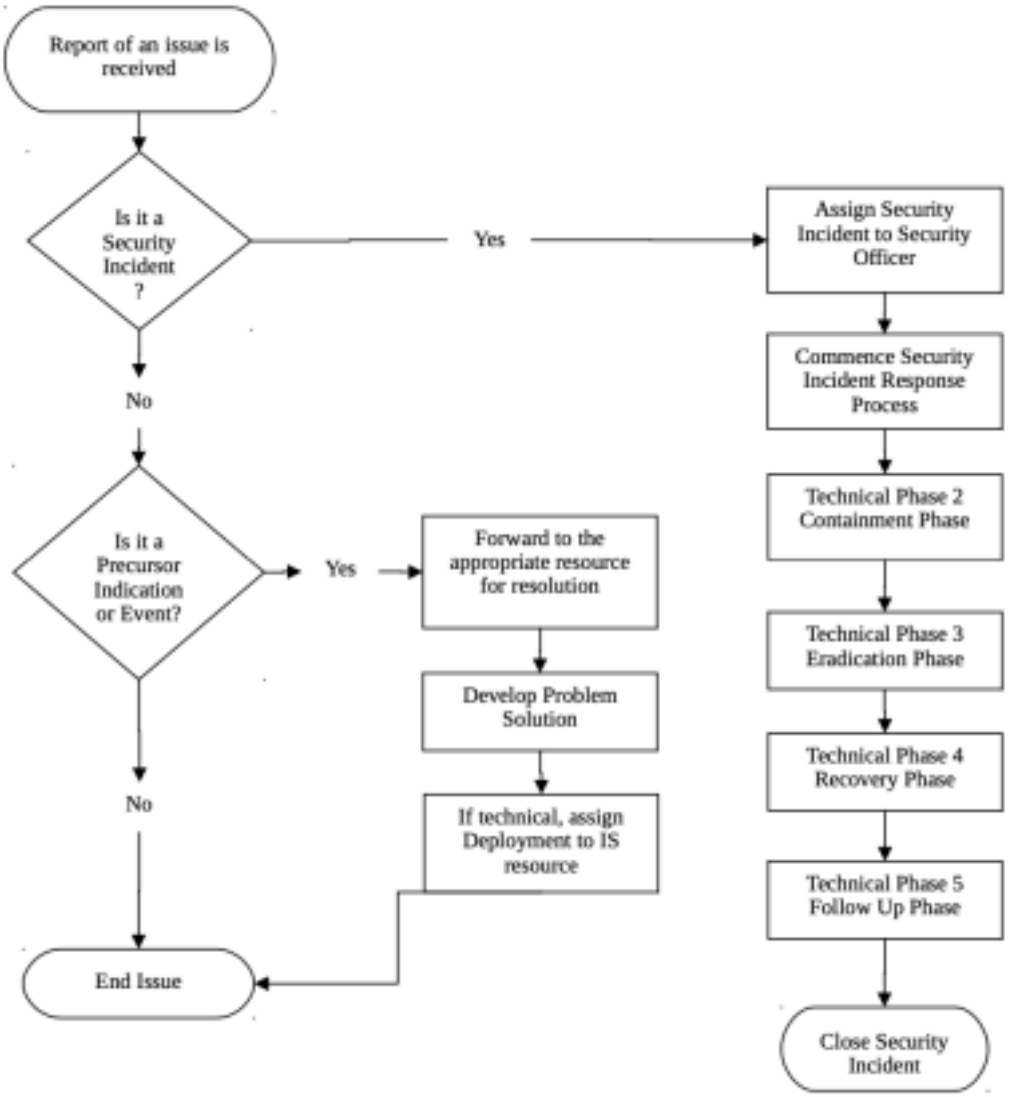

Figure 1: A representation of the SANS process.

8.2.1 Identification Phase

1. Immediately upon observation World of Content members report suspected and known Events, Precursors, Indications, and Incidents in one of the following ways: 1. Direct report to management, the Security Officer, or other;

2. Email;
3. Phone call;
4. Slack;
5. Anonymously through workforce member's desired channels;

2. The Security Officer determines if the issue is an Event, Precursor, Indication, or Incident.

1. If the issue is an event, indication, or precursor the Security Officer forwards it to the appropriate resource for resolution.
2. If the issue is a security incident the Security Officer activates the Security Incident Response Team (SIRT) and notifies the Head of Development. 1. If a non-technical security incident is discovered the SIRT completes the investigation, implements preventative measures, and resolves the security incident.
2. Once the investigation is completed, progress to Phase V, Follow-up.
3. If the issue is a technical security incident, commence to Phase II: Containment.
4. The Containment, Eradication, and Recovery Phases are highly technical. It is important to have them completed by a highly qualified technical security resource with oversight by the SIRT team.
5. Each individual on the SIRT and the technical security resource document all measures taken during each phase, including the start and end times of all efforts.
6. The lead member of the SIRT team facilitates initiation of a SIR Form supplied by the Security Officer. The intent of the SIR form is to provide a summary of all events, efforts, and conclusions of each Phase of this policy and procedures.

3. The Security Officer notifies any affected Customers and Partners. If no Customers and Partners are affected, notification is at the discretion of the Security Officer. 4. In the case of a threat identified, the Security Officer is to form a team to investigate and involve necessary resources, both internal and potentially external.

8.2.2 Containment Phase (Technical)

In this Phase, World of Content's IT department attempts to contain the security incident. It is extremely important to take detailed notes during the security incident response process. This provides that the evidence gathered during the security incident can be used successfully during prosecution, if appropriate.

1. The SIRT reviews any information that has been collected by the Security Officer or any other individual investigating the security incident.
2. The SIRT secures the network perimeter.
3. The IT department performs the following:
    1. Securely connect to the affected system over a trusted connection. 26
    2. Retrieve any volatile data from the affected system.
    3. Determine the relative integrity and the appropriateness of backing the system up.
    4. If appropriate, back up the system.
    5. Change the password(s) to the affected system(s).
    6. Determine whether it is safe to continue operations with the affected

system(s).

7. If it is safe, allow the system to continue to function;
    1. Complete any documentation relative to the security incident on the SIR Form.
    2. Move to Phase V, Follow-up.
8. If it is NOT safe to allow the system to continue operations, discontinue the system(s) operation and move to Phase III, Eradication.
9. The individual completing this phase provides written communication to the SIRT.

4. Continuously apprise the Head of Development of progress.
5. Continue to notify affected Customers and Partners with relevant updates as needed

8.2.3 Eradication Phase (Technical)

The Eradication Phase represents the SIRT's effort to remove the cause, and the resulting security exposures, that are now on the affected system(s).

1. Determine symptoms and cause related to the affected system(s). 2. Strengthen the defenses surrounding the affected system(s), where possible (a risk assessment may be needed and can be determined by the Security Officer). This may include the following:
    1. An increase in network perimeter defenses.
    2. An increase in system monitoring defenses.
    3. Remediation ("fixing") any security issues within the affected system, such as removing unused services/general host hardening techniques.
3. Conduct a detailed vulnerability assessment to verify all the holes/gaps that can be exploited have been addressed.
    1. If additional issues or symptoms are identified, take appropriate preventative measures to eliminate or minimize potential future compromises.
4. Update the documentation with the information learned from the vulnerability assessment, including the cause, symptoms, and the method used to fix the problem with the affected system(s).
5. Apprise the Head of Development of the progress.
6. Continue to notify affected Customers and Partners with relevant updates as needed.
7. Move to Phase IV, Recovery.

8.2.4 Recovery Phase (Technical)

The Recovery Phase represents the SIRT's effort to restore the affected system(s) back to operation after the resulting security exposures, if any, have been corrected. 1. The technical team determines if the affected system(s) have been changed in any way.

1. If they have, the technical team restores the system to its proper, intended

functioning ("last known good").

2. Once restored, the team validates that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit that owns the affected system(s).
3. If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline or dropped from the network while triaged), restart the restored and validated system(s) and monitor for behavior.
4. If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.
5. Update the documentation with the detail that was determined during this phase.
6. Apprise the Head of Development of progress.
7. Continue to notify affected Customers and Partners with relevant updates as needed.
8. Move to Phase V, Follow-up.

8.2.5 Follow-up Phase (Technical and Non-Technical)

The Follow-up Phase represents the review of the security incident to look for "lessons learned" and to determine whether the process that was taken could have been improved in any way. It is recommended all security incidents be reviewed shortly after resolution to determine where response could be improved. Timeframes may extend to one to two weeks

post-incident.

1. Responders to the security incident (SIRT Team and technical security resource) meet to review the documentation collected during the security incident. 2. Create a "lessons learned" document and attach it to the completed SIR Form. 1. Evaluate the cost and impact of the security incident to World of Content using the documents provided by the SIRT and the technical security resource.
    2. Determine what could be improved.
    3. Communicate these findings to the Head of Development for approval and for implementation of any recommendations made post-review of the security incident.
    4. Carry out recommendations approved by the Head of Development; sufficient budget, time and resources should be committed to this activity. 5. Close the security incident.

8.2.6 Periodic Evaluation

It is important to note that the processes surrounding security incident response should be periodically reviewed and evaluated for effectiveness. This also involves appropriate training of resources expected to respond to security incidents, as well as the training of the workforce regarding the organizations expectation for them, relative to security responsibilities. The incident response plan is tested annually.