SP CE

Version 1.0
May 17, 2021

TERMS OF SERVICE

This agreement is linked to all use of the platform SP_CE and is to be agreed, upon signing up for any subscription tier (Freemium, Premium, Enterprise) and the date for sign up will be considered the effective date for this agreement.

PARTIES

1. Meeting Maker Global AB (SP_CE), a company incorporated in Sweden (registration number 559258-5417) having its registered office at Kvarnbäcksvägen 5, 302 91 Halmstad (the "**Provider**"); and

2. the party who subscribe to any of the provider offered subscription models, "**Customer**").

AGREEMENT

1. Definitions

1.1 In this Agreement except to the extent expressly provided otherwise:

"**Access Credentials**" means the usernames, passwords and other credentials enabling access to the Hosted Services, including both access credentials for the User Interface and access credentials for the API;

"**Agreement**" means this agreement including any Schedules, and any amendments to this Agreement from time to time;

"**API**" means the application programming interface for the Hosted Services defined by the Provider and made available by the Provider to the Customer;

"**Charges**" means the following amounts:

(a) the amounts specified in Section 2 of Schedule 1 (Hosted Services particulars);

(b) such amounts as may be agreed in writing by the parties from time to time; and

"**Customer Confidential Information**" means:

(a) any information disclosed by or on behalf of the Customer to the Provider during the Term OR at any time before the termination of this Agreement (whether disclosed in writing, orally or otherwise) that at the time of disclosure:

(i) was marked or described as "confidential"; or

(ii) should have been reasonably understood by the Provider to be confidential; and

(b) the Customer Data;

"**Customer Data**" means all data, works and materials: uploaded to, recorded or stored on the Platform by the Customer; transmitted by the Platform at the instigation of the Customer; supplied by the Customer to the Provider for uploading to, transmission by or storage on the Platform; or generated by the Platform as a result of the use of the Hosted Services by the Customer (but excluding analytics data relating to the use of the Platform and server log files);

"**Customer Personal Data**" means any Personal Data that is processed by the Provider on behalf of the Customer in relation to this Agreement;

"**Data Protection Laws**" means the EU GDPR and the UK GDPR and all other applicable laws relating to the processing of Personal Data;

"**Documentation**" means the documentation for the Hosted Services produced by the Provider and delivered or made available by the Provider to the Customer;

"**Effective Date**" means the date of execution of this Agreement;

"**EU GDPR**" means the General Data Protection Regulation (Regulation (EU) 2016/679) and all other EU laws regulating the processing of Personal Data, as such laws may be updated, amended and superseded from time to time;

"**Force Majeure Event**" means [an event, or a series of related events, that is outside the reasonable control of the party affected (including failures of the internet or any public telecommunications network, hacker attacks, denial of service attacks, virus or other malicious software attacks or infections, power failures, industrial disputes affecting any third party, changes to the law, disasters, epidemics, pandemics, explosions, fires, floods, riots, terrorist attacks and wars)];

"**Hosted Services**" means *SP_CE*, as specified [in the Hosted Services Specification],] which will be made available by the Provider to the Customer as a service via the internet in accordance with this Agreement;

"**Hosted Services Defect**" means a defect, error or bug in the Platform having an adverse effect OR a material adverse effect on the appearance, operation, functionality or performance of the Hosted Services, but excluding any defect, error or bug caused by or arising as a result of:

(a) any act or omission of the Customer or any person authorised by the Customer to use the Platform or Hosted Services;

(b) any use of the Platform or Hosted Services contrary to the Documentation, whether by the Customer or by any person authorised by the Customer;

(c) a failure of the Customer to perform or observe any of its obligations in this Agreement; and/or

(d) an incompatibility between the Platform or Hosted Services and any other system, network, application, program, hardware or software.

"**Hosted Services Specification**" means the specification for the Platform and Hosted Services set out in Section 1 of Schedule 1 (Hosted Services particulars) and in the Documentation;

"**Intellectual Property Rights**" means all intellectual property rights wherever in the world, whether registrable or unregistrable, registered or unregistered, including any application or right of application for such rights (and these "intellectual property rights" include copyright and related rights, database rights, confidential information, trade secrets, know-how, business names, trade names, trade marks, service marks, passing off rights, unfair competition rights, patents, petty patents, utility models, semi-conductor topography rights and rights in designs);

“Licensed users” means all users holding a valid subscription to the platform;

"**Mobile App**" means any eventual mobile application that is made available by the Provider through the *Google Play Store* and the *Apple App Store*;

“Invited Participants” means people invited to the platform by a licensed user;

"**Personal Data**" means personal data under any of the Data Protection Laws;

"**Platform**" means the platform managed by the Provider and used by the Provider to provide the Hosted Services, including the application and database software for the Hosted Services, the system and server software used to provide the Hosted Services, and the computer hardware on which that application, database, system and server software is installed;

"**Schedule**" means any schedule attached to the main body of this Agreement;

"**Services**" means any services that the Provider provides to the Customer, or has an obligation to provide to the Customer, under this Agreement;

"**Support Services**" means support in relation to the use of, and the identification and resolution of errors in, the Hosted Services, but shall not include the provision of training services;

"**Supported Web Browser**" means the current release from time to time of Google Chrome or Microsoft Edge, or any other web browser that the Provider agrees in writing shall be supported;

"**Term**" means [the term of this Agreement, commencing in accordance with Clause 3.1 and ending in accordance with Clause 3.2];

"**UK GDPR**" means the EU GDPR as transposed into UK law (including by the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019) and all other UK laws regulating the processing of Personal Data, as such laws may be updated, amended and superseded from time to time; and

"**User Interface**" means the interface for the Hosted Services designed to allow individual human users to access and use the Hosted Services.

2. Credit

2.1 This document was created using a template from Docular (https://docular.net).

3. Term

3.1 Terms of service can be changed at any time by the Provider, by informing all users electronically. Usage after such date will mean consent to new terms and conditions.

3.2 This Agreement shall come into force upon the Effective Date.

3.3 This Agreement shall continue in force until the date when the subscription shall terminate automatically OR until the end date of the agreement has passed without renewal OR until the agreement has been terminated by any parties and the period of the subscription has passed OR until it is terminatez automatically OR in subject to termination in accordance with Clause 18 or any other provision of this Agreement.

4. Hosted Services

4.1 The Provider shall provide, or shall ensure that the Platform will provide, to the Customer upon the end of the subscription period, the Access Credentials necessary to enable the Customer to access and use the Hosted Services.

4.2 The Provider hereby grants to the Customer a worldwide, non-exclusive licence to use the Hosted Services by means of the User Interface and services that the chosen subscription, at the time, makes available.

4.3 The licence granted by the Provider to the Customer under Clause 4.2 is subject to the following limitations:

(a) the User Interface may only be used through a Supported Web Browser.

(b) the User Interface may only be used by the Licensed Users or Invited Participants.

(c) the User Interface must not be used at any point in time by more than one physical individual per Licensed User (i e every Licensed User account is not to be used by any other than that named user) and

(d) the API may only be used by an application or applications approved by the Provider in writing and controlled by the Customer.

4.4 Except to the extent expressly permitted in this Agreement or required by law on a non-excludable basis, the licence granted by the Provider to the Customer under Clause 4.2 is subject to the following prohibitions:

(a) the Customer must not sub-license its right to access and use the Hosted Services;

(b) the Customer must not permit any unauthorised person or application to access or use the Hosted Services;

(c) the Customer must not use the Hosted Services to provide services to third parties;

(d) the Customer must not republish or redistribute any content or material from the Hosted Services;

(e) the Customer must not make any alteration to the Platform, except as permitted by the Documentation; and

(f) the Customer must not conduct or request that any other person conduct any load testing or penetration testing on the Platform or Hosted Services without the prior written consent of the Provider.

4.5 The Customer shall implement and maintain reasonable security measures relating to the Access Credentials to ensure that no unauthorised person or application may gain access to the Hosted Services by means of the Access Credentials.

4.6 The Provider shall use all reasonable endeavors to maintain the availability of the Hosted Services to the Customer at the gateway between the public internet and the network of the hosting services provider for the Hosted Services, but does not guarantee 100% availability.

4.7 For the avoidance of doubt, downtime caused directly or indirectly by any of the following shall not be considered a breach of this Agreement:

(a) a Force Majeure Event;

(b) a fault or failure of the internet or any public telecommunications network;

(c) a fault or failure of the Customer's computer systems or networks;

(d) any breach by the Customer of this Agreement; or

(e) scheduled maintenance carried out in accordance with this Agreement.

4.8 The Customer must comply with Schedule 2 (Acceptable Use Policy), and must ensure that all persons using the Hosted Services with the authority of the Customer or by means of the Access Credentials comply with Schedule 2 (Acceptable Use Policy).

4.9 The Customer must not use the Hosted Services in any way that causes, or may cause, damage to the Hosted Services or Platform or impairment of the availability or accessibility of the Hosted Services.

4.10 The Customer must not use the Hosted Services in any way that uses excessive Platform resources and as a result is liable to cause a material degradation in the services provided by the Provider to its other customers using the Platform; and the Customer acknowledges that the Provider may use reasonable technical measures to limit the use of Platform resources by the Customer for the purpose of assuring services to its customers generally.

4.11 The Customer must not use the Hosted Services:

(a) in any way that is unlawful, illegal, fraudulent or harmful; or

(b) in connection with any unlawful, illegal, fraudulent or harmful purpose or activity.

4.12 For the avoidance of doubt, the Customer has no right to access the software code (including object code, intermediate code and source code) of the Platform, either during or after the Term.

4.13 The Provider may suspend the provision of the Hosted Services if any amount due to be paid by the Customer to the Provider under this Agreement is overdue, and the Provider has given to the Customer at least 30 days' written notice, following the amount becoming overdue, of its intention to suspend the Hosted Services on this basis.

5. Scheduled maintenance

5.1 The Provider may from time to time suspend the Hosted Services for the purposes of scheduled maintenance to the Platform, providing that such scheduled maintenance must be carried out in accordance with this Clause 5.

5.2 The Provider shallwhere practicable give to the Customer at least 5 Business Days' prior written notice of scheduled maintenance that will, or is likely to, affect the availability of the Hosted Services or have a material negative impact upon the Hosted Services.

5.3 The Provider shall strive for all scheduled maintenance to be carried out outside Business Hours.

5.4 The Provider shall ensure that, during each calendar month, the aggregate period during which the Hosted Services are unavailable as a result of scheduled maintenance, or negatively affected by scheduled maintenance to a material degree, does not exceed 4 hours.

6. Support Services

6.1 The Provider shall provide the Support Services to the Customer during the Term.

6.2 The Provider shall make available to the Customer a FAQ helpdesk.

6.3 The Provider shall provide the Support Services according to the paid subscription

6.4 The Customer may use the helpdesk for the purposes of requesting and, where applicable, receiving the Support Services; and the Customer must not use the helpdesk for any other purpose.

6.5 The Provider shall respond promptly to all requests for Support Services made by the Customer through the helpdesk.

6.6 The Provider may suspend the provision of the Support Services if any amount due to be paid by the Customer to the Provider under this Agreement is overdue, and the Provider has given to the Customer at least 30 days' written notice, following the amount becoming overdue, of its intention to suspend the Support Services on this basis.

7. Customer Data

7.1 The Customer hereby grants to the Provider a non-exclusive licence to copy, reproduce, store, distribute, publish, export, adapt, edit and translate] the Customer Data to the extent reasonably required for the performance of the Provider's obligations and the exercise of the Provider's rights under this Agreement. The Customer also grants to the Provider the right to sub-license these rights to its hosting, connectivity and telecommunications service providers, subject to any express restrictions elsewhere in this Agreement.

7.2 The Customer warrants to the Provider that the Customer Data OR the Customer Data when used by the Provider in accordance with this Agreement will not infringe the Intellectual Property Rights or other legal rights of any person, and will not breach the provisions of any law, statute or regulation, in any jurisdiction and under any applicable law.

7.3 The Provider shall create a back-up copy of the service as well as Customer Data at least daily, shall ensure that each such copy is sufficient to enable the Provider to restore the Hosted Services to the state they were in at the time the back-up was taken, and shall retain and securely store each such copy for a minimum period of 30 days.

7.4 Within the period of 1 Business Day following receipt of a written request from the Customer, the Provider shall use all reasonable endeavours to restore to the Platform the Customer Data stored in any back-up copy created and stored by the Provider in accordance with Clause 7.3. The Customer acknowledges that this process will overwrite the Customer Data stored on the Platform prior to the restoration.

8. Mobile App

8.1 The parties acknowledge and agree that the use of any Mobile App provided by the provider, the parties' respective rights and obligations in relation to the Mobile App and any liabilities of either party arising out of the use of the Mobile App shall be subject to separate terms and conditions, and accordingly this Agreement shall not govern any such use, rights, obligations or liabilities.

9. No assignment of Intellectual Property Rights

9.1 Nothing in this Agreement shall operate to assign or transfer any Intellectual Property Rights from the Provider to the Customer, or from the Customer to the Provider.

10. Charges

10.1 The Customer shall pay the Charges to the Provider in accordance with the subscription chosen, the number of subscribed users and this Agreement.

10.2 In case of any extra services is ordered the Charges are based in whole or part upon the time spent by the Provider performing the Services, the Provider must obtain the Customer's written consent before performing Services that result in any estimate of time-based Charges given to the Customer being exceeded or any budget for time-based Charges agreed by the parties being exceeded; and unless the Customer agrees otherwise in writing, the Customer shall not be liable to pay to the Provider any Charges in respect of Services performed in breach of this Clause 10.2.

10.3 All amounts stated in or in relation to this Agreement are, unless the context requires otherwise, exclusive of any applicable value added taxes, which will be added to those amounts and payable by the Customer to the Provider.

10.4 The Provider may elect to vary any element of the Charges by giving to the Customer not less than 30 days' written notice of the variation, providing that no such variation shall constitute a percentage increase in the relevant element of the Charges] that exceeds 2% over the percentage increase, since the date of the most recent variation of the subscription fee.

11. Payments

11.1 The Provider shall issue invoices for the Charges to the Customer in advance of the period to which they relate OR

11.2 The Customer must pay the Charges to the Provider direct upon subscription via Credit Card or, in case of invoicing, within the period of 30 days following the issue of an invoice in accordance with this Clause 11.

11.3 The Customer must pay the Charges using such payment details as are notified by the Provider to the Customer from time to time.

11.4 If the Customer does not pay any amount properly due to the Provider under this Agreement, the Provider may:

(a) charge the Customer interest on the overdue amount at the rate of [8% per annum above the base rate from time to time in the country origin of the provider] (which interest will accrue daily until the date of actual payment and be compounded at the end of each calendar month); or

(b) claim interest and statutory compensation from the Customer pursuant to the Late Payment of Commercial Debts (Interest) Act 1998.

12. Provider's confidentiality obligations

12.1 The Provider must:

(a) keep the Customer Confidential Information strictly confidential;

(b) not disclose the Customer Confidential Information to any person without the Customer's prior written consent, and then only under conditions of confidentiality approved in writing by the Customer OR no less onerous than those contained in this Agreement;

(c) use the same degree of care to protect the confidentiality of the Customer Confidential Information as the Provider uses to protect the Provider's own confidential information of a similar nature, being at least a reasonable degree of care;

(d) act in good faith at all times in relation to the Customer Confidential Information; and

(e) not use any of the Customer Confidential Information for any purpose other than over all generic data processing and analytics.

12.2 Notwithstanding Clause 12.1, the Provider may disclose the Customer Confidential Information to the Provider's officers, employees, professional advisers, insurers, agents and subcontractors who have a need to access the Customer Confidential Information for the performance of their work with respect to this Agreement and who are bound by a written agreement or professional obligation to protect the confidentiality of the Customer Confidential Information.

12.3 This Clause 12 imposes no obligations upon the Provider with respect to Customer Confidential Information that:

(a) is known to the Provider before disclosure under this Agreement and is not subject to any other obligation of confidentiality;

(b) is or becomes publicly known through no act or default of the Provider; or

(c) is obtained by the Provider from a third party in circumstances where the Provider has no reason to believe that there has been a breach of an obligation of confidentiality.

12.4 The restrictions in this Clause 12 do not apply to the extent that any Customer Confidential Information is required to be disclosed by any law or regulation, by any judicial or governmental order or request, or pursuant to disclosure requirements relating to the listing of the stock of the Provider on any recognised stock exchange.

12.5 The provisions of this Clause 12 shall continue in force indefinitely following the termination of this Agreement.

13. Data protection

13.1 Each party shall comply with the Data Protection Laws with respect to the processing of the Customer Personal Data.

13.2 The Customer warrants to the Provider that it has the legal right to disclose all Personal Data that it does in fact disclose to the Provider under or in connection with this Agreement.

13.3 The Customer shall only supply to the Provider, and the Provider shall only process, in each case under or in relation to this Agreement:

(a) the Personal Data of data subjects falling within the categories specified in Section 1 of Schedule 3 (Data processing information); and

(b) Personal Data of the types specified in Section 2 of Schedule 3 (Data processing information.

13.4 The Provider shall only process the Customer Personal Data for the purposes specified in Schedule 3 (Data processing information).

13.5 The Provider shall only process the Customer Personal Data during the Term and for not more than 30 days following the end of the Term, subject to the other provisions of this Clause 13.

13.6 The Provider shall only process the Customer Personal Data on the documented instructions of the Customer (including with regard to transfers of the Customer Personal Data to a third country under the Data Protection Laws), as set out in this Agreement or any other document agreed by the parties in writing.

13.7 The Customer hereby authorises the Provider to make the following transfers of Customer Personal Data:

(a) the Provider may transfer the Customer Personal Data internally to its own employees, offices and facilities, providing that such transfers must be protected by appropriate safeguards.

(b) the Provider may transfer the Customer Personal Data to its third party processors in the jurisdictions identified in Section 5 of Schedule 3 (Data processing information) and may permit its third party processors to make such transfers, providing that such transfers must be protected by any appropriate safeguards identified therein]; and

(c) the Provider may transfer the Customer Personal Data to a country, a territory or sector to the extent that the competent data protection authorities have decided that the country, territory or sector ensures an adequate level of protection for Personal Data.

13.8 The Provider shall promptly inform the Customer if, in the opinion of the Provider, an instruction of the Customer relating to the processing of the Customer Personal Data infringes the Data Protection Laws.

13.9 Notwithstanding any other provision of this Agreement, the Provider may process the Customer Personal Data if and to the extent that the Provider is required to do so by applicable law. In such a case, the Provider shall inform the Customer of the legal

requirement before processing, unless that law prohibits such information on important grounds of public interest.

13.10 The Provider shall ensure that persons authorised to process the Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

13.11 The Provider and the Customer shall each implement appropriate technical and organisational measures to ensure an appropriate level of security for the Customer Personal Data, including those measures specified in Section 4 of Schedule 3 (Data processing information).

13.12 The Provider must not engage any third party to process the Customer Personal Data without the prior specific or general written authorisation of the Customer. In the case of a general written authorisation, the Provider shall inform the Customer at least 14 days in advance of any intended changes concerning the addition or replacement of any third party processor, and if the Customer objects to any such changes before their implementation, then the Provider must not implement the changes OR the Customer may terminate this Agreement on 7 days' written notice to the Provider, providing that such notice must be given within the period of 7 days following the date that the Provider informed the Customer of the intended changes]. The Provider shall ensure that each third party processor is subject equivalent legal obligations as those imposed on the Provider by this Clause 13.

13.13 As at the Effective Date, the Provider is hereby authorised by the Customer to engage, as sub-processors with respect to Customer Personal Data, the third parties identified in Section 5 of Schedule 3 (Data processing information).

13.14 The Provider shall, insofar as possible and taking into account the nature of the processing, take appropriate technical and organisational measures to assist the Customer with the fulfilment of the Customer's obligation to respond to requests exercising a data subject's rights under the Data Protection Laws.

13.15 The Provider shall assist the Customer in ensuring compliance with the obligations relating to the security of processing of personal data, the notification of personal data breaches to the supervisory authority, the communication of personal data breaches to the data subject, data protection impact assessments and prior consultation in relation to high-risk processing under the Data Protection Laws. The Provider may charge the Customer at its standard time-based charging rates for any work performed by the Provider at the request of the Customer pursuant to this Clause 13.15.

13.16 The Provider must notify the Customer of any Personal Data breach affecting the Customer Personal Data without undue delay and, in any case, not later than 24 hours after the Provider becomes aware of the breach.

13.17 The Provider shall make available to the Customer all information necessary to demonstrate the compliance of the Provider with its obligations under this Clause 13 and the Data Protection Laws. The Provider may charge the Customer at its standard time-based charging rates for any work performed by the Provider at the request of the

Customer pursuant to this Clause 13.17, providing that no such charges shall be levied with respect to the completion by the Provider (at the reasonable request of the Customer, not more than once per calendar year of the standard information security questionnaire of the Customer.

13.18 The Provider shall, at the choice of the Customer, delete or return all of the Customer Personal Data to the Customer after the provision of services relating to the processing, and shall delete existing copies save to the extent that applicable law requires storage of the relevant Personal Data.

13.19 The Provider shall allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer in respect of the compliance of the Provider's processing of Customer Personal Data with the Data Protection Laws and this Clause 13. The Provider may charge the Customer at its standard time-based charging rates for any work performed by the Provider at the request of the Customer pursuant to this Clause 13.19, providing that no such charges shall be levied where the request to perform the work arises out of any breach by the Provider of this Agreement or any security breach affecting the systems of the Provider.

13.20 If any changes or prospective changes to the Data Protection Laws result or will result in one or both parties not complying with the Data Protection Laws in relation to processing of Personal Data carried out under this Agreement, then the parties shall use their best endeavours promptly to agree such variations to this Agreement as may be necessary to remedy such non-compliance.

14. Warranties

14.1 The Provider warrants to the Customer that:

(a) the Provider has the legal right and authority to enter into this Agreement and to perform its obligations under this Agreement;

(b) the Provider will comply with all applicable legal and regulatory requirements applying to the exercise of the Provider's rights and the fulfilment of the Provider's obligations under this Agreement; and

(c) the Provider has or has access to all necessary know-how, expertise and experience to perform its obligations under this Agreement.

14.2 The Provider warrants to the Customer that:

(a) the Platform and Hosted Services will conform in all material respects with the Hosted Services Specification;

(b) the Hosted Services will be free from Hosted Services Defects;

(c) the Platform will be free from viruses, worms, Trojan horses, ransomware, spyware, adware and other malicious software programs; and

(d) the Platform will incorporate security features reflecting the requirements of good industry practice.

14.3 The Provider warrants to the Customer that the Hosted Services, when used by the Customer in accordance with this Agreement, will not breach any laws, statutes or regulations applicable under the laws in the countries it acts.

14.4 The Provider warrants to the Customer that the Hosted Services, when used by the Customer in accordance with this Agreement, will not infringe the Intellectual Property Rights of any person in any jurisdiction and under any applicable law.

14.5 If the Provider reasonably determines, or any third party alleges, that the use of the Hosted Services by the Customer in accordance with this Agreement infringes any person's Intellectual Property Rights, the Provider may at its own cost and expense:

(a) modify the Hosted Services in such a way that they no longer infringe the relevant Intellectual Property Rights; or

(b) procure for the Customer the right to use the Hosted Services in accordance with this Agreement.

14.6 The Customer warrants to the Provider that it has the legal right and authority to enter into this Agreement and to perform its obligations under this Agreement.

14.7 All of the parties' warranties and representations in respect of the subject matter of this Agreement are expressly set out in this Agreement. To the maximum extent permitted by applicable law, no other warranties or representations concerning the subject matter of this Agreement will be implied into this Agreement or any related contract.

15. Acknowledgements and warranty limitations

15.1 The Customer acknowledges that complex software is never wholly free from defects, errors and bugs; and subject to the other provisions of this Agreement, the Provider gives no warranty or representation that the Hosted Services will be wholly free from defects, errors and bugs.

15.2 The Customer acknowledges that complex software is never entirely free from security vulnerabilities; and subject to the other provisions of this Agreement, the Provider gives no warranty or representation that the Hosted Services will be entirely secure.

15.3 The Customer acknowledges that the Hosted Services are designed to be compatible only with that software and those systems specified as compatible in the Hosted Services Specification; and the Provider does not warrant or represent that the Hosted Services will be compatible with any other software or systems.

15.4 The Customer acknowledges that the Provider will not provide any legal, financial, accountancy or taxation advice under this Agreement or in relation to the Hosted Services; and, except to the extent expressly provided otherwise in this Agreement, the Provider does not warrant or represent that the Hosted Services or the use of the Hosted Services

by the Customer will not give rise to any legal liability on the part of the Customer or any other person.

16. Limitations and exclusions of liability

16.1 Nothing in this Agreement will:

(a) limit or exclude any liability for fraud or fraudulent misrepresentation;

(b) limit any liabilities in any way that is not permitted under applicable law; or

(c) exclude any liabilities that may not be excluded under applicable law.

16.2 The limitations and exclusions of liability set out in this Clause 16 and elsewhere in this Agreement:

(a) are subject to Clause 16.1; and

(b) govern all liabilities arising under this Agreement or relating to the subject matter of this Agreement, including liabilities arising in contract, in tort (including negligence) and for breach of statutory duty, except to the extent expressly provided otherwise in this Agreement.

16.3 Neither party shall be liable to the other party in respect of any losses arising out of a Force Majeure Event.

16.4 Neither party shall be liable to the other party in respect of any loss of profits or anticipated savings.

16.5 Neither party shall be liable to the other in respect of any loss of revenue or income.

16.6 Neither party shall be liable to the other party in respect of any loss of use or production.

16.7 Neither party shall be liable to the other party in respect of any loss of business, contracts or opportunities.

16.8 Neither party shall be liable to the other party in respect of any loss or corruption of any data, database or software.

16.9 Neither party shall be liable to the other party in respect of any special, indirect or consequential loss or damage.

16.10 The liability of the Provider to the Customer under this Agreement in respect of any event or series of related events shall not exceed the greater of the total amount paid and payable by the Customer to the Provider under this Agreement in the 12 month period preceding the commencement of the event or events.

16.11 The aggregate liability of the Provider to the Customer under this Agreement shall not exceed the greater of the total amount paid and payable by the Customer to the Provider under this Agreement.

17. Force Majeure Event

17.1 If a Force Majeure Event gives rise to a failure or delay in either party performing any obligation under this Agreement (other than any obligation to make a payment), that obligation will be suspended for the duration of the Force Majeure Event.

17.2 A party that becomes aware of a Force Majeure Event which gives rise to, or which is likely to give rise to, any failure or delay in that party performing any obligation under this Agreement, must:

(a) promptly notify the other; and

(b) inform the other of the period for which it is estimated that such failure or delay will continue.

17.3 A party whose performance of its obligations under this Agreement is affected by a Force Majeure Event must take reasonable steps to mitigate the effects of the Force Majeure Event.

18. Termination

18.1 Either party may terminate this Agreement by giving to the other party at least 30 days' written notice of termination, or as client cancellation can be made in the application before any automatic renewal.

18.2 Either party may terminate this Agreement immediately by giving written notice of termination to the other party if the other party commits a material breach of this Agreement.

18.3 Subject to applicable law, either party may terminate this Agreement immediately by giving written notice of termination to the other party if:

(a) the other party:

(i) is dissolved;

(ii) ceases to conduct all (or substantially all) of its business;

(iii) is or becomes unable to pay its debts as they fall due;

(iv) is or becomes insolvent or is declared insolvent; or

(v) convenes a meeting or makes or proposes to make any arrangement or composition with its creditors;

(b) an administrator, administrative receiver, liquidator, receiver, trustee, manager or similar is appointed over any of the assets of the other party;

(c) an order is made for the winding up of the other party, or the other party passes a resolution for its winding up (other than for the purpose of a solvent company

reorganisation where the resulting entity will assume all the obligations of the other party under this Agreement).

19. Effects of termination

19.1 Upon the termination of this Agreement, all of the provisions of this Agreement shall cease to have effect, save that the following provisions of this Agreement shall survive and continue to have effect (in accordance with their express terms or otherwise indefinitely): [Clauses 1, 4.12, 8, 11.2, 11.4, 12, 13, 16, 19, 22 and 23].

19.2 Except to the extent expressly provided otherwise in this Agreement, the termination of this Agreement shall not affect the accrued rights of either party.

20. Notices

20.1 Any notice from one party to the other party under this Agreement must be given by one of the following methods (using the relevant contact details set out in Clause 20.2 and Section 3 of Schedule 1 (Hosted Services particulars)):

(a) sent via email or via physical mail (or by courier), in which case the notice shall be deemed to be received upon delivery; or

(b) delivered as cancellation or other message inside the Platform service itself.

providing that, if the stated time of deemed receipt is not within Business Hours, then the time of deemed receipt shall be when Business Hours next begin after the stated time.

20.2 The Provider's contact details for notices under this Clause 20 are as follows:

Email: hi@spce.com

Address: Meeting Maker Global AB (SP CE), Kvarnbäcksvägen 5, 302 91 Halmstad, Sweden

20.3 The addressee and contact details set out in Clause 20.2 and Section 3 of Schedule 1 (Hosted Services particulars) may be updated from time to time.

21. Subcontracting

21.1 Subject to any express restrictions elsewhere in this Agreement, the Provider may subcontract any of its obligations under this Agreement, providing that the Provider must give to the Customer, promptly following the appointment of a subcontractor, a written notice specifying the subcontracted obligations and identifying the subcontractor in question.

21.2 The Provider shall remain responsible to the Customer for the performance of any subcontracted obligations.

21.3 Notwithstanding the provisions of this Clause 21 but subject to any other provision of this Agreement, the Customer acknowledges and agrees that the Provider may subcontract to any reputable third party hosting business the hosting of the Platform and the provision of services in relation to the support and maintenance of elements of the Platform.

22. General

22.1 No breach of any provision of this Agreement shall be waived except with the express written consent of the party not in breach.

22.2 If any provision of this Agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other provisions of this Agreement will continue in effect. If any unlawful and/or unenforceable provision would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the provision will continue in effect (unless that would contradict the clear intention of the parties, in which case the entirety of the relevant provision will be deemed to be deleted).

22.3 This Agreement may not be varied except by a written document signed by or on behalf of each of the parties.

22.4 Neither party may without the prior written consent of the other party assign, transfer, charge, license or otherwise deal in or dispose of any contractual rights or obligations under this Agreement.

22.5 This Agreement is made for the benefit of the parties, and is not intended to benefit any third party or be enforceable by any third party. The rights of the parties to terminate, rescind, or agree any amendment, waiver, variation or settlement under or relating to this Agreement are not subject to the consent of any third party.

22.6 Subject to Clause 16.1, this Agreement shall constitute the entire agreement between the parties in relation to the subject matter of this Agreement, and shall supersede all previous agreements, arrangements and understandings between the parties in respect of that subject matter.

22.7 This Agreement shall be governed by and construed in accordance with Swedish law.

22.8 The courts of Sweden shall have exclusive jurisdiction to adjudicate any dispute arising under or in connection with this Agreement.

23. Interpretation

23.1 In this Agreement, a reference to a statute or statutory provision includes a reference to:

(a) that statute or statutory provision as modified, consolidated and/or re-enacted from time to time; and

(b) any subordinate legislation made under that statute or statutory provision.

23.2 The Clause headings do not affect the interpretation of this Agreement.

23.3 References in this Agreement to "calendar months" are to the 12 named periods (January, February and so on) into which a year is divided.

23.4 In this Agreement, general words shall not be given a restrictive interpretation by reason of being preceded or followed by words indicating a particular class of acts, matters or things.

SP CE

Version 1.0
May 17, 2021

SCHEDULE 1 (HOSTED SERVICES PARTICULARS)

1. Specification of Hosted Services

SP CE is a software as a service provided by Meeting Maker Global AB (SP CE), with the functionality that from time to other is included in the Customers' chosen subscription tier (described here: https://www.spce.com/pricing/).

2. Financial provisions

Subscription fees are per month according to chosen tier, from the following:

FREEMIUM	$0 per user and month
PREMIUM	$45 per user and month
ENTERPRISE	$45 per user and month

Payment terms are as follows:

FREEMIUM	N/A
PREMIUM	Upfront with Credit Card
ENTERPRISE	Upfront invoice at 30 days net

SP CE

Version 1.0
May 17, 2021

SCHEDULE 2 (ACCEPTABLE USE POLICY)

1. Introduction

1.1 This acceptable use policy (the "**Policy**") sets out the rules governing:

(a) the use of **app.spce.com**, any successor website, and the services available on that website or any successor website (the "**Services**"); and

(b) the transmission, storage and processing of content by you, or by any person on your behalf, under the same subscription, using the Services ("**Content**").

1.2 References in this Policy to "you" are to any user who is granted access through your subscription of the Services and any individual user of the Services (and "your" should be construed accordingly); and references in this Policy to "us" are to Meeting Maker Global AB (SP CE) (and "we" and "our" should be construed accordingly).

1.3 By using the Services, you agree to the rules set out in this Policy.

1.4 We will ask for your express agreement to the terms of this Policy before you upload or submit any Content or otherwise use the Services.

1.5 You must be at least 18 years of age to use the Services; and by using the Services, you warrant and represent to us that you are at least 18 years of age.

1.6 Meeting Maker Global AB (SP CE) take no responsibility for usage or content distributed through the service, why you as subscriber have the full responsibility for compliance in each case in any jurisdiction and under any applicable law.

2. General usage rules

2.1 You must not use the Services in any way that causes, or may cause, damage to the Services or impairment of the availability or accessibility of the Services.

2.2 You must not use the Services:

(a) in any way that is unlawful, illegal, fraudulent, deceptive or harmful; or

(b) in connection with any unlawful, illegal, fraudulent, deceptive or harmful purpose or activity.

2.3 You must ensure that all Content complies with the provisions of this Policy.

3. Unlawful Content

3.1 Content must not be illegal or unlawful, must not infringe any person's legal rights, and must not be capable of giving rise to legal action against any person (in each case in any jurisdiction and under any applicable law).

3.2 Content, and the use of Content by us in any manner licensed or otherwise authorized by you, must not:

(a) be libellous or maliciously false;

(b) be obscene or indecent;

(c) infringe any copyright, moral right, database right, trade mark right, design right, right in passing off, or other intellectual property right;

(d) infringe any right of confidence, right of privacy or right under data protection legislation;

(e) constitute negligent advice or contain any negligent statement;

(f) constitute an incitement to commit a crime, instructions for the commission of a crime or the promotion of criminal activity;

(g) be in contempt of any court, or in breach of any court order;

(h) constitute a breach of racial or religious hatred or discrimination legislation;

(i) be blasphemous;

(j) constitute a breach of official secrets legislation; or

(k) constitute a breach of any contractual obligation owed to any person.

3.3 You must ensure that Content is not and has never been the subject of any threatened or actual legal proceedings or other similar complaint.

4. Graphic material

4.1 Content must be appropriate for all persons who have access to or are likely to access the Content in question, and in particular for children over 12 years of age.

4.2 Content must not depict violence in an explicit, graphic or gratuitous manner.

4.3 Content must not be pornographic or sexually explicit.

5. Etiquette

5.1 Content must be appropriate, civil and tasteful, and accord with generally accepted standards of etiquette and behaviour on the internet.

5.2 Content must not be offensive, deceptive, threatening, abusive, harassing, menacing, hateful, discriminatory or inflammatory.

5.3 Content must not be liable to cause annoyance, inconvenience or needless anxiety.

5.4 You must not use the Services to send any hostile communication or any communication intended to insult, including such communications directed at a particular person or group of people.

5.5 You must not use the Services for the purpose of deliberately upsetting or offending others.

5.6 You must not unnecessarily flood the Services with material relating to a particular subject or subject area, whether alone or in conjunction with others.

6. Marketing and spam

6.1 You must not without our written permission use the Services for any purpose relating to the marketing, advertising, promotion, sale or supply of any product, service or commercial offering.

6.2 Content must not constitute or contain spam, and you must not use the Services to store or transmit spam - which for these purposes shall include all unlawful marketing communications and unsolicited commercial communications.

6.3 You must not send any spam or other marketing communications to any person using any email address or other contact details made available through the Services or that you find using the Services.

6.4 You must not use the Services to promote, host or operate any chain letters, Ponzi schemes, pyramid schemes, matrix programs, multi-level marketing schemes, "get rich quick" schemes or similar letters, schemes or programs.

6.5 You must not use the Services in any way which is liable to result in the blacklisting of any of our IP addresses.

7. Regulated businesses

7.1 You must not use the Services for any purpose relating to gambling, gaming, betting, lotteries, sweepstakes, prize competitions or any gambling-related activity, unless you have a license permit to do so in the countries of use of the service.

7.2 You must not use the Services for any purpose relating to the offering for sale, sale or distribution of drugs or pharmaceuticals, unless you have a license permit to do so in the countries of use of the service.

7.3 You must not use the Services for any purpose relating to the offering for sale, sale or distribution of knives, guns or other weapons, unless you have a license permit to do so in the countries of use of the service..

8. Monitoring

8.1 You acknowledge that we not actively monitor the Content or the use of the Services.

9. Data mining

9.1 You must not conduct any systematic or automated data scraping, data mining, data extraction or data harvesting, or other systematic or automated data collection activity, by means of or in relation to the Services.

10. Hyperlinks

10.1 You must not link to any material using or by means of the Services that would, if it were made available through the Services, breach the provisions of this Policy.

11. Harmful software

11.1 The Content must not contain or consist of, and you must not promote, distribute or execute by means of the Services, any viruses, worms, spyware, adware or other harmful or malicious software, programs, routines, applications or technologies.

11.2 The Content must not contain or consist of, and you must not promote, distribute or execute by means of the Services, any software, programs, routines, applications or technologies that will or may have a material negative effect upon the performance of a computer or introduce material security risks to a computer.

SP CE

Version 1.0
May 17, 2021

SCHEDULE 3 (DATA PROCESSING INFORMATION)

"**Data Protection Legislation**" means the GDPR, the UK Data Protection Act 2018, Directive 2002/58/EC and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including the General Data Protection Regulation), and all other applicable laws relating to processing of personal data and privacy that may exist in any relevant jurisdiction, including, where applicable, the guidance and codes of practice issued by supervisory authorities;

"**GDPR**" means, in each case to the extent applicable to the processing activities: (i) Regulation (EU) 2016/679; and (ii) Regulation (EU) 2016/679 as amended by any legislation arising out of the withdrawal of the UK from the European Union;

"**Security Breach**" means any accidental, unauthorised or unlawful destruction, loss, alteration, or disclosure of, or access to the personal data that the Supplier processes in the course of providing the Services;

"**controller**", "**processor**", "**data subject**", "**personal data**", "**processing**" and "**appropriate technical and organisational measures**" shall be interpreted in accordance with the GDPR.

1. DATA PROTECTION

1.1 The parties agree the provisions of this clause [1] shall apply to the personal data the Supplier processes in the course of providing the Services. The parties agree that the Customer and the Customer Affiliates are the controller[s] and the Supplier is the processor in relation to the personal data that the Supplier processes in the course of providing the Services.

1.2 The subject-matter of the data processing is the performance of the Services. The obligations and rights of the Customer and Customer Affiliates are as set out in this Agreement. Schedule [1] of this Agreement sets out the nature, duration and purpose of the processing, the types of personal data the Supplier processes and the categories of data subjects whose personal data is processed.

1.3 When the Supplier processes personal data in the course of providing the Services the Supplier will:

- process the personal data only in accordance with documented instructions from the Customer, (which may be specific instructions or instructions of a general nature as set out in this Agreement or as otherwise notified by the Customer to the Supplier from time to time). If the Supplier is required to process the personal data for any other purpose by applicable laws to which the Supplier is subject, the Supplier will inform Customer of this requirement first, unless prohibited by such applicable laws; and

- at all times comply with applicable Data Protection Legislation and notify the Customer immediately if, in the Supplier's reasonable opinion, an instruction for the processing of personal data given by the Customer infringes applicable Data Protection Legislation;

1.4 The Supplier shall ensure that personnel required to access the personal data are subject to a binding duty of confidentiality in respect of such personal data and take reasonable steps to ensure the reliability and competence of the Supplier's personnel who have access to the personal data.

1.5 The Supplier shall ensure that none of the Supplier's personnel publish, disclose or divulge any of the personal data to any third party unless directed in writing to do so by the Customer.

1.6 The Supplier shall assist the Customer [and the Customer Affiliates], always taking into account the nature of the processing at no extra cost:

- by appropriate technical and organisational measures and in so far as is possible, in fulfilling the Customer and the Customer Affiliates obligations to respond to requests from data subjects exercising their rights;

- in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the information available to the Supplier; and

- by making available to the Customer all information which the Customer reasonably requests to allow the Customer to demonstrate that the obligations set out in Article 28 of the General Data Protection Regulation relating to the appointment of processors have been met;

1.7 The Supplier shall implement and maintain appropriate technical and organisational measures to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction, damage or theft of the personal data and having regard to the nature of the personal data which is to be protected.

1.8 In the event of a suspected Security Breach, the Supplier will:

- take action immediately, at the Supplier's own expense, to investigate the suspected Security Breach and to identify, prevent and mitigate the effects of the suspected Security Breach and to remedy the Security Breach;

- notify the Customer immediately and provide the Customer with a detailed description of the Security Breach including:

  - the likely impact of the Security Breach;

  - the categories and approximate number of data subjects affected and their country of residence and the categories and approximate number of records affected;

  - and the risk posed by the Security Breach to individuals; and

  - the measures taken or proposed to be taken by the Supplier to address the Security Breach and to mitigate its adverse effects.

- and provide timely updates to this information and any other information the Customer may reasonably request relating to the Security Breach; and

- not release or publish any filing, communication, notice, press release, or report concerning the Security Breach without the Customer's prior written approval (except where required to do so by law).

1.9 The Supplier shall not give access to or transfer any personal data to any third party (including any affiliates, group companies or sub-contractors) without the prior written consent of the Customer. Where the Customer does consent to the Supplier engaging a sub-contractor to carry out any part of the Services involving the processing of personal data, the Supplier must include in any contract with the third party provisions in favour of the Customer which are the same as or equivalent to those in this clause [1] and as are required by applicable Data Protection Legislation. For the avoidance of doubt, where a third party fails to fulfil its obligations under any sub-processing agreement or any applicable Data Protection Legislation, the Supplier will remain fully liable to the Customer for the fulfilment of the Supplier's obligations under these terms.

1.10 The Supplier shall maintain written records of all categories of personal data processing activities carried out on behalf of the Customer and the Customer Affiliates, including any information prescribed in applicable Data Protection Legislation.

1.11 The Supplier shall allow the Customer and its respective auditors or authorised agents to conduct audits or inspections during the term of the Agreement and for [12] months thereafter which will include providing access to the records held further to clause [1.10], and the premises, resources, and personnel of Supplier and the Supplier's sub-contractors use in connection with the provision of the Services, and provide all reasonable assistance in order to assist the Customer in exercising its audit rights under this clause [1.11]. The purposes of an audit pursuant to this clause include verifying that the Supplier and its subcontractors are processing personal data in accordance with the obligations under this clause [1].

1.12 If the European Commission lays down, or an applicable supervisory authority adopts, standard contractual clauses for the matters referred to in Article 28(3) and Article 28(4) of the General Data Protection Regulation pursuant to Article 28(7) or Article 28(8) of the General Data Protection Regulation (as appropriate) and the Customer notifies the Supplier that it wishes to incorporate any element of any such standard contractual clauses into this Agreement, the Supplier shall agree to the changes as reasonably required by the Customer in order to achieve this.

1.13 The Supplier will not process personal data outside the UK or European Economic Area, or a country in respect of a valid adequacy decision has been issued by the European Commission or adequacy determined in another valid method under applicable Data Protection Legislation, except with the prior written consent of the Customer.

1.14 In the event that the Customer gives its consent to the Supplier transferring personal data outside the European Economic Area and a relevant European Commission decision or other valid adequacy method under applicable Data Protection Legislation on which the Customer has relied in authorising the data transfer is held to be invalid, or that any supervisory authority requires transfers of personal data made pursuant to such decision to be suspended, then the Customer may, at its discretion, require the Supplier to cease processing personal data to which this paragraph applies, or co-operate with it and facilitate use of an alternative transfer mechanism.

1.15 At the end of the Services, upon the Customer's request, the Supplier shall securely destroy or return such personal data to the Customer and/or any affected Customer Affiliates and delete existing copies unless applicable laws require storage of such personal data.

SP CE

Version 1.0
May 17, 2021

SP CE

Version 1.0
May 17, 2021

Schedule 3:1

Data processing information

1. NATURE AND PURPOSE OF PROCESSING OPERATIONS

The personal data transferred are:

Email, first name, last name will, together with chat history, todo-activities and files uploaded by the Customer/user, be stored and processed in the Platform. If approved by the parties and chosen by the Customer/user, meetings can be recorded and transcribed, and therefore processed and stored as a part of the service.

Categories of data subject

The personal data transferred concern the following categories of data:

Prospects and customers email, first name and last name together with eventual chat history and files uploaded by Customer/user.

Categories of data

The personal data transferred concern:

Identifying information such as first name, last name and email address and eventual recordings.

Special categories of data (if appropriate)

N/A

Duration of Processing

The personal data shall be processed for the term of the Agreement or for such longer or shorter period as the Supplier provides data processing services under the Agreement.

2. SECURITY MEASURES

Access control to premises and facilities

Measures are taken to prevent unauthorized physical access to premises and facilities holding personal data. Measures include:

- Verifying cloud provider meets the security requirements.

- The service is hosted in Microsoft Azure cloud service.

For details related to physical access security measurements, please read this documentation:

https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security

Access control to systems

Measures are taken to prevent unauthorized access to IT systems. These include minimum the following technical and organizational measures for user identification and authentication:

- Password protection measurements

- 2FA authentication

- Limiting number of admin accounts

For details related to physical access security measurements, please view this documentation:

https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security

Access control to data

Measures are taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorised input, reading, copying, removal modification or disclosure of data. These measures include:

- Using principle of least privilege

- Regularly go through user access

Disclosure control

Measures are taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures include:

- Encrypt all data in transfer

- Store activity and system event logs

- Create policies and procedures for monitoring signs of unauthorized data access

- Store and renew certificates in a secure way (Azure Managed Certificate)

- Following OWASP guidelines

Input control

Measures are in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained. Measures include:

- Saving audit logs for at least 360 days.

- All maintenance is made by authorized personnel only.

Job control

Measures are in place to ensure that data is processed strictly in compliance with the data importer's instructions. These measures include:

- Regularly conducting data protection impact assessment.

- Security training and education of employees

- Regularly review policies, procedures and safeguards

Availability control

Measures are in place to ensure that data are protected against accidental destruction or loss. These measures include:

- Developing of data breach notification policies and procedures.

- Storing backups that enables restoring of personal data in a timely manner.

Segregation control

Measures are in place to allow data collected for different purposes to be processed separately. These include:

- Role base access control.

- Logical separation of data.

- Physical separation of processing services (micro services)

SP CE

Version 1.0
May 17, 2021