SMB Solutions Cloud Services

Cloud Service Schedule (insert customer) Effective ("Effective Date")

This SMB Solutions Cloud Service Schedule ("**Cloud EULA Acceptance Form**") is between SMB Solutions Cloud Services and [Insert Customer Name] of [Insert Customer Address] referred to as "**Parties**".

RECITAL

WHEREAS, Customer has purchased or will purchase the right to use SMB Solutions Cloud Hosting Services for a certain period of time. WHEREAS, SMB Solutions Cloud Services wants to grant Customer the right to use SMB Solutions Cloud Hosting Service.

NOW THEREFORE, the Parties agree as follows:

1. Any terms not defined in this Cloud EULA Acceptance Form will have the meaning ascribed to them in the Master Terms for SMB Solutions Cloud Services.
2. Customer agrees to use the SMB Solutions Cloud Services in accordance with the terms and conditions of the following documents in effect as of the effective date which are incorporated and made a part hereof by reference. All documents are listed in order of precedence and collectively referred to as the "**Agreement**".

The Customer has had the opportunity to review the General Terms and Conditions for SMB Cloud Services and the incorporated documents prior to executing this Cloud EULA Acceptance Form.

SMB Solutions Cloud Services recommends that Customer prints copies of these documents for Customer's records.

All defined terms in the Cloud EULA used in this Cloud EULA Acceptance Form have the meaning stated in the Cloud EULA. All references in the Supplements to "Service" mean "Cloud Service", and to "Named Users" mean "Authorised Users."

1. Under this Agreement, Customer only receives the right to use services as set out in the order and the other non- recurring services (if any); the fees for the cloud services set out in the order and the other non-recurring services (if any) themselves are not

contemplated under this Agreement. SMBSCS does not accept any liability for the provision of services by the Partner.

2. Customer's contact details for sending system notices are:

Name	
Email	
Direct Contact Number	

The system provisioning notification recipient name and e-mail address are necessary for system notices.

IN WITNESS WHEREOF, the Parties hereto have caused this **Cloud EULA Acceptance Form** to be executed by their respective authorised representatives.

Accepted BY

[Insert Customer Name] who holds the authorised company position of [Insert Position Title]

_____

Signature

Date _____

Master Terms

(With effect from 1st December 2019)

Background

A SMB Solutions Cloud Services provides a range of information technology services, including:

- managed services; outsourcing; (incl Ultimate Care product);
- cloud services; (incl Infrastructure as a Service (IaaS) and Backup and Recovery as a Service (BRS) products);
- infrastructure services; systems integration; project services; (incl Service Pack)
- hardware and software procurement
- intranet solutions; application management; application development;
- telephony and unified communications

B These Master Terms set out the terms and conditions under which SMB Solutions Cloud Services supplies these services.

Agreement

1. Parties

The parties are:

1.1. the Company named in a SMB Solutions Cloud Services Order Form ('SMB', 'us', 'we' or 'our'); and

1.2. the Client named in a SMB Solutions Cloud Services Order Form ('you' or 'your').

2. Master Terms

These Master Terms apply to all IT services provided by us to you to the exclusion of any purchase order or other document submitted by you to us. For clarity any Voice or Data service that we supply to you are covered by a separate Standard Form of Agreement (SFOA).

3. Product Terms

3.1. The services that we are able to provide are described in the Product Terms.

3.2. Each of the Product Terms sets out:

3.2.1. the scope of the service;

3.2.2. the fees for the service; and

3.2.3. any special conditions that apply to the service.

4. Order Form

4.1. You may request a service by submitting a SMB Solutions Cloud Services Order Form to us.

4.2. Each SMB Solutions Cloud Services Order Form:

4.2.1. must be in our standard form, as current at the time;

4.2.2. must clearly identify the service requested by reference to Product Terms;

4.2.3. must set out the required commencement date and term of the service;

4.2.4. must be completed by you accurately, with all required information; and

4.2.5. is a request for service and not a contract unless and until accepted by us.

5. Service Contracts

5.1. If we accept a SMB Solutions Cloud Services Order Form in writing, a binding contract is created ('Service Contract') comprising:

5.1.1. the Product Terms, including any special conditions;

5.1.2. the SMB Solutions Cloud Services Order Form; and

5.1.3. these Master Terms.

5.2. Each Service Contract is an independent contract.

5.3. If there is any inconsistency between the parts of a Service Contract, the order of priority, from highest to lowest, is:

5.3.1. any special conditions in the Product Terms;

5.3.2. the remainder of the Product Terms;

5.3.3. the SMB Solutions Cloud Services Order Form; and

5.3.4. these Master Terms.

6. Services

6.1. For each Service Contract, we will provide you with the service specified in the relevant Product Terms ('the service').

7. Fees

7.1. The fees for a service are:

7.1.1. the fees specified in Order Form;

7.1.2. if none are specified, our then current published fees for that service; or

7.1.3. if there are no current published fees, at our time and materials rates for similar services.

7.2. Except where we have agreed fixed fees for services, we may adjust our fees at any time.

7.3. If we perform any work that is not covered by the Product Terms, we may charge for that work:

7.3.1. at our current published rates for that type of work; or

7.3.2. if there are no current published rates, at our time and materials rates for similar work.

7.4. Unless we say otherwise in writing, when we use the term Monthly Base Fee this means the standard price contained in the Order Form, excluding variations, usage, consumption, Excluded Item fees or set up fees.

8. Pre-paid fees

8.1. If Product Terms require fees to be pre-paid:

8.1.1. services will not be provided until you pay the pre-paid fees;

8.1.2. we may suspend providing a service if the balance of the pre-paid fees will not cover our fees for the service required; and

8.1.3. we may apply amounts you owe us against the balance of your pre-paid fees in any manner we decide.

8.2. Pre-paid fees are non-refundable.

9. Expenses

9.1. You must reimburse our out of pocket expenses provided:

9.1.1. the expenses have been approved in writing; and

9.1.2. we supply reasonable evidence substantiating the expense.

10. Invoicing and payment

10.1. We will invoice you:

10.1.1. in accordance with any payment schedule specified in the Product Terms;

10.1.2. otherwise:

10.1.2.1. monthly in advance for pre-paid fees

10.2. You must pay each invoice in full:

10.2.1. by the due date specified in the invoice; or

10.2.2. if no due date is specified, within 14 days of the invoice date.

10.3. Late invoicing does not affect our right to payment or your obligation to pay.

10.4. If a payment is overdue, in addition to our other rights:

10.4.1. we may charge interest on the overdue amount at the Default Rate, calculated daily;

10.4.2. we may withhold providing services under any Service Contract; and

10.4.3. you must indemnify us against all costs and expenses (including legal expenses on a solicitor / client basis) incurred by us in attempting to recover the overdue amount. 'Default Rate' means the overdraft reference rate quoted by our principal banker on the first day of the applicable month plus 2%.

10.5. If:

10.5.1. you fail to pay any amount (whether in whole or part) payable in respect of any hardware and/or Loan Equipment by the time required for payment;

10.5.2. you become insolvent (as that term is defined in the *Corporations Act 2001*); or

10.5.3. the Service Contract between us is terminated, or becomes terminable at our option, we may, without notice to you, enter at any reasonable time any premises where hardware and/or Loan Equipment is located (or believed by us to be located) and take possession of that hardware and/or Loan Equipment not paid for and any other hardware and/or Loan Equipment to the value of the amount owing. Our permission to enter your premises for that purpose is irrevocable. We are not liable to you in contract, tort or otherwise, for any costs, damages, expenses or losses incurred by you as a result of any action taken by us under this clause.

11. Third party charges

11.1. You are responsible for all third-party charges incurred as a result of your use of the service (for example, telecommunications carriage fees) unless we specify otherwise in writing.

11.2. Where we specify that our fees include third party charges, we may increase our fees by written notice to you if there is an increase in third party charges.

12. GST

12.1. Terms in italics in this clause have the same meaning as in the *A New Tax System (Goods and Services Tax) Act 1999*.

12.2. Unless stated otherwise, fees stated under this agreement exclude GST.

12.3. The *consideration* payable by you under this agreement is the *value* of any *taxable supply* for which payment is to be made.

12.4. Subject to us supplying you with a valid *tax invoice*, if we make a *taxable supply* in connection with a Service Contract for a *consideration*, which represents its *value*, then you must pay, at the same time and in the same manner as the *value* is otherwise payable, the amount of any GST payable in respect of the *taxable supply*.

12.5. Subject to us supplying you with a valid tax invoice, if a Service Contract requires you to pay, reimburse or contribute to an amount paid or payable by us in respect of an acquisition of a taxable supply from a third party, the amount required to be paid, reimbursed or contributed by you will be the value of the acquisition by us less any input tax credit to which we are entitled plus, if our recovery from you is a *taxable*

supply, any GST payable under clause 12.4.

13. Service delivery

13.1. We will provide the service:

13.1.1. during Business Hours, unless otherwise specified inwriting;

13.1.2. at the location(s) specified in the Product Terms or, if no location is specified, at the location we determine to be most appropriate; and

13.1.3. with professional skill and care, using appropriately qualified personnel.

'Business Hours' means between 8:00 am and 6:00 pm, Monday to Friday excluding public holidays at the place in which the service is to be provided.

14. Access

14.1. You must provide us with reasonable and timely access to your facilities, premises, information, equipment, personnel, network and data to enable to fulfill our obligations under the Product Terms.

14.2. We will not be responsible for any delay in providing a service where the delay results from your failure to provide timely access in accordance with clause 14.1.

15. Your obligations

15.1. You must:

15.1.1. comply with our reasonable and lawful directions in relation to the service;

15.1.2. provide a safe working environment for our personnel;

15.1.3. comply with all laws, regulations, policies and guidelines (including any acceptable use policy that we inform you of) applicable to the service;

15.1.4. ensure that any incumbent provider who is transitioning the service to us makes available the information, resources and facilities required by us to provide the service; and

15.1.5. maintain regular and complete backups of all of your data.

15.2. We will not be responsible for any failure, default or delay to the extent caused by your failure to perform your obligations under this clause.

16. Hardware supply

16.1. To the extent that the service is for the sale and supply of hardware:

16.1.1. the risk of loss of or damage to the hardware passes to you on delivery. Your obligation to insure hardware commences when risk passes to you. You must insure the hardware for its full value and ensure that our interest is noted on the policy. We may require you to demonstrate compliance with this clause including by producing a copy of the insurance policy;

16.1.2. we remain the legal and beneficial owner of all hardware sold by us to you under these Master Terms until all amounts due in respect of all hardware and any other amounts you owe us, actually or contingently presently or in future, have been paid to us in cleared funds. This applies even if you install the hardware or commingle it with other goods.

16.1.3. you must not sell, dispose of, assign or encumber the hardware unless and until you have paid for it in full;

16.1.4. where the hardware manufacturer's warranty is capable of being assigned to you, it is the only warranty given in relation to the hardware, to the extent permitted by law;

16.1.5. where hardware is subject to export control laws or regulations (including US export laws and regulations), you must not directly or indirectly export, re-export, distribute or otherwise act in violation of such laws and regulations; and

16.1.6. the United Nations Convention on Contracts for the International Sale of Goods does not apply.

17. Loan equipment

17.1. We may install on your premises, loan or otherwise provide you with equipment ("Loan Equipment"). All Loan Equipment:

17.1.1. remains our property;

17.1.2. must only be used by you for the purposes of receiving services from us; and

17.1.3. must be kept secured from loss or damage.

17.2. If Loan Equipment in your possession or control is lost, stolen or damaged:

17.2.1. you must notify us without unreasonably delay; and

17.2.2. you must pay us the replacement cost of the Loan Equipment calculated as the recommended retail price at the date the Loan Equipment was lost, stolen or damaged minus any amount we recover under an insurance policy.

18. Software

18.1. To the extent that a service involves the creation or licensing of software that we own:

18.1.1. we warrant that our software will operate substantially in accordance with its accompanying documentation during the warranty period;

18.1.2. we will use our reasonable efforts to correct any defect provided:

18.1.2.1. you notify us of the defect during the warranty period;

18.1.2.2. you have used the software in accordance with its accompanying documentation and our recommendations;

18.1.2.3. the software has not been used on or in conjunction with equipment or software not approved by us;

18.1.2.4. the software has not been modified by anyone other than us;

18.1.2.5. the defect is not due to a change in your IT or physical environment after delivery of the software; and

18.1.2.6. you are not in breach of this agreement or any Service Contract.

18.2. 'Warranty period' means 90 days from the date of delivery, unless we specify a different period.

18.3. 'Defect' means a reproducible failure of the software to work substantially as described in the documentation that accompanies it.

19. PPS Law

19.1. This clause applies to the extent that the agreement we have with you provides for or contains a 'security interest' for the purposes of the *Personal Property Securities Act 2009* (Cth) ("PPS Law") (or part of it). The security interest granted to us is a 'purchase money security interest' ("PMSI") to the extent that it can be under section 14 of the PPS Law.

19.2. We may register our security interest. You must do anything (such as obtaining consents and signing documents) which we require for the purposes of:

19.2.1. ensuring that our security interest is enforceable, perfected and otherwise effective under the PPS Law;

19.2.2. enabling us to gain first priority (or any other priority agreed to us in writing) for our security interest; and

19.2.3. enabling us to exercise rights in connection with the security interest.

19.3. Our rights under our agreement with you are in addition to and not in substitution for our rights under other law (including the PPS Law) and we may choose whether to exercise rights under our agreement and/or under such other law, as we see fit.

19.4. The following provisions of the PPS Law do not apply and, for the purposes of section 115 of the PPS Law are "contracted out" of our agreement with you in respect of goods that are not used predominantly for personal, domestic or household purposes:

19.4.1. sections 95 (notice of removal of accession to the extent it requires us to give a notice to you), 96 (retention of accession), 125 (obligations to dispose of or retain collateral); section 130 (notice of disposal to the extent it requires us to give a notice to you); section 132(3)(d) (contents of statement of account after disposal); section 132(4) (statement of account if no disposal); section 135 (notice of retention); section 142 (redemption of collateral); and section 143 (re-instatement of security agreement).

19.5. The following provisions of the PPS Law:

19.5.1. section 123 (seizing collateral); section 126 (apparent possession); section 128 (secured party may dispose of collateral); section 129 (disposal by purchase); and section 134(1) (retention of collateral), confer rights on us. You agree that in addition to those rights, we shall, if there is default by you, have the right to seize, purchase, take possession or apparent possession, retain, deal with or dispose of any hardware and/or Loan Equipment, not only under those sections but also, as additional and independent rights, under our agreement with you and you agree that we may do so in any manner we see fit including (in respect of dealing and disposal) by private or public sale, lease or licence.

19.6. You waive your rights to receive a verification statement in relation to registration events in respect of commercial property under section 157 of the PPS Law.

19.7. We and you agree not to disclose information of the kind that can be requested under section 275(1) of the PPS Law. You must do everything necessary on your part to ensure that section 275(6)(a) of the PPS Law continues to apply. The agreement in this sub-clause is made solely for the purpose of allowing to us the benefit of section 275(6)(a) and we shall not be liable to pay damages or any other compensation or be subject to injunction if we breach this sub-clause.

19.8. You must not create, purport to create or permit to be created any 'security interest' (as defined in PPS Law) in the hardware and/or Loan Equipment other than with our express written consent.

19.9. You must not lease, hire, bail or give possession of ('sub-hire') the equipment to anyone else unless we (in our absolute discretion) first consent in writing. Any such sub-hire must be in writing in a form acceptable to us and must be expressed to be subject to our rights under our agreement with you.

19.10. You must take all steps including registration under PPS Law as may be required to:

19.10.1. ensure that any security interest arising under or in respect of the sub-hire is enforceable, perfected and otherwise effective under the PPS Law;

19.10.2. enabling us to gain (subject always to our rights) first priority (or any other priority we agree to in writing) for the security interest;and

19.10.3. enabling each of us to exercise our respective rights in connection with the security interest.

19.11. We may recover from you the cost of doing anything under this clause, including registration fees and the costs of notification.

20. Third party materials

20.1. In providing a service we may supply you with materials (including software) licensed by third parties.

20.2. You must comply with the terms of the third-party license and you indemnify us against any loss, damage, claim, liability or demand we incur due to your breach of a third-party license.

21. Delay

21.1. We will use our reasonable efforts to meet any deadlines or milestones that we promise to meet but will not be liable for any delay or failure to meet these.

21.2. To the extent that our provision of a service is impaired by:

21.2.1. you;

21.2.2. a third party;

21.2.3. a failure or defect (not caused by us) in hardware or software (not supplied by us); or

21.2.4. an event beyond our reasonable control – then:

21.2.5. our obligation to provide the service is suspended;

21.2.6. we will not be liable to you in respect of any delay or failure to provide the service.

21.3. Where our personnel are delayed from performing a service due to a delay you cause, we may invoice you those personnel's hourly rate for the duration of the delay subject

only to us making reasonable efforts to reallocate our personnel to other chargeable duties.

22. Confidentiality

22.1. A party must not use or disclose the other party's confidential information without prior written approval.

22.2. Each party must take all reasonable steps to ensure that its employees and agents do not use or disclose the other party's confidential information.

22.3. A party may disclose confidential information where required by law or the rules of a stock exchange.

22.4. This clause survives termination of this agreement.

22.5. 'Confidential information' means all information treated by the owning party ('discloser') as confidential and:

22.5.1. provided to the other party ('recipient'); or

22.5.2. of which the recipient becomes aware –

except information that:

22.5.3. the recipient creates or lawfully obtains independently of the discloser; or

22.5.4. is public knowledge (otherwise than as a result of a breach of confidentiality by the recipient).

23. Intellectual property rights

23.1. Unless otherwise specified in writing, we own exclusively all intellectual property rights in material, including software, that we design, create, modify, supply or license, even if it was created or modified for or suggested by you.

23.2. To the extent necessary for you to receive the benefit of a service, we grant you a non-exclusive, non-transferable, license to use our materials.

23.3. If any of your materials become combined with our materials with your knowledge and without your objection, then we have a perpetual, royalty-free, irrevocable, non-

exclusive license to copy, use, adapt and distribute and sub-license those materials in the course of our ongoing business.

23.4. 'Intellectual property rights' includes all patents, copyright, rights in circuit layouts, registered designs, trademarks, trade, business or company names and the right to have confidential information kept confidential.

24. Limitation of liability

24.1. Our maximum aggregate liability under a Service Contract or Claim, whether for breach of these terms or in negligence or in any other tort or for any other common law or statutory cause of action or otherwise is the amount equal to the fees you have paid to us under the Service Contract.

24.2. We will not be liable to you for data loss under any circumstances.

25. Warranty and Indemnity

25.1. You must indemnify us, our employees and agents against any loss (including reasonable legal costs and expenses) or liability any of us reasonably incurs or suffers arising from any proceedings where such loss or liability was caused by:

25.1.1. your breach of these Master Terms or a Service Contract; or

25.1.2. your wilful, unlawful or negligent act or omission.

26. Termination and Suspension of Service Contracts

26.1. We may terminate or suspend performance of a Service Contract immediately if:

26.1.1. you breach the Service Contract and fail to remedy the breach within 14 days after receiving a notice detailing the breach and requiring that it be cured;

26.1.2. you become insolvent;

26.1.3. you fail to pay money owed to us within 30 days of it being due;

26.1.4. you cease, or threaten to cease, carrying on your business;

26.1.5. you exceed your credit limit or there is an adverse change in our credit assessment of you;

26.1.6. we reasonably believe that you have used a service for unauthorised,

criminal or unlawful activity; or

26.1.7. an administrator or controller (as those terms are defined in the *Corporations Act 2001*) is appointed in respect of any of your assets.

26.2. Your breach of a Service Contract is deemed to be a breach of these Master Terms and all other Service Contracts.

26.3. Termination of a Service Contract does not affect our rights of action based on any breach by you before the termination.

26.4. On termination we may:

26.4.1. repossess any of our property in your possession, custody or control;

26.4.2. retain all moneys paid to us under the Service Contract;

26.4.3. provide you with an invoice for all unpaid fees and expenses and any costs incurred by us as a result of termination; and

26.4.4. pursue any additional or alternative remedies provided by law.

26.5. If you terminate a Service Contract prior to its expiry, then you must pay us within 14 days of invoice, the equivalent of the Monthly Service Fee multiplied by the number of months remaining in the Service Contract[1].

26.6. The termination fee in clause 26.5:

26.6.1. is a reasonable pre-estimate of our loss and damage arising from an early termination of a Service Contract; and

26.6.2. is without prejudice to any other rights we may have to recover other sums from you.

[1] e.g. if the Monthly Service Fee is $200 (inc GST), and there are 3 months remaining in the Service Contract, you must pay us $600.

26.7. Should the Service Contract expire and not be expressly terminated by you it will continue indefinitely on a quarter by quarter basis and you must provide us with 90 days notice to cancel the service.

26.8. Upon expiry or termination of a Service Contract each party must return any property belonging to the other party within 7 days.

26.8.1. Where you have a right to terminate a Service Contract, or any individual service, under these terms, you may only do so by providing us with written notice through our cancellation form available at from us on request.

26.9. Should the Service Contract expire and not be expressly terminated by you it will continue indefinitely on a quarter by quarter basis and you must provide us with 90 days' notice to cancel the service.

26.10. Any discount provided to you in relation to the Service Contracts Fixed Term (Generally 25%) shall be revoked and your pricing will revert to the Uncontracted Price.

27. Termination for Non-Performance

27.1. You may terminate the Service Contract immediately if we breach a Service Level Agreement and fail to remedy the breach within 14 days after receiving a notice detailing the breach and requiring that it be cured;

27.2. Termination of a Service Contract does not affect our rights of action based on any breach by you before the termination and is without prejudice to any other rights we may have to recover other sums from you.

27.3. On termination we may retain all moneys paid to us under the Service Contract;

27.4. If you terminate a Service Contract prior to its expiry as per clause 30.1, then no termination fee will be payable.

28. Notices

28.1. All notices must be:

28.1.1. in writing;

28.1.2. signed by the party giving it (or its authorised representative); and

28.1.3. sent to a party's service address.

28.2. A party's service address is any of:

28.2.1. in the case of a corporation, its current registered office;

28.2.2. the parties' business addresses set out in an SMB Solutions Cloud Services Order Form; or

28.2.3. any other address a party nominates, by written notice to the other party, as a service address.

29. Restraints

29.1. Neither party may approach the Employees, Agents or Contractors of the other party to this Agreement, with an offer of employment during the term of this Agreement or for each of the following periods, 2 months, 3 months, 6 months and 12 months after its expiry or termination.

29.2. For the avoidance of doubt, nothing in this clause 32 prevents either party from employing an employee of the other party as a result of the employee responding to a public notice, in the absence of any solicitation however if this occurs then the employing party will pay a replacement recruitment fee to the other party of $15,000 ex GST.

30. General matters

30.1. We are an independent contractor and have no authority to bind you by contract or otherwise.

30.2. We may sub-contract the performance of this agreement if we obtain your prior written consent (which you must not unreasonably withhold).

30.3. We may assign or novate our rights and obligations under this Agreement at any time without your consent.

30.4. You may not assign your rights and obligations under this agreement without our prior written consent (which we will not unreasonably withhold).

30.5. If a party overlooks a breach of a Service Contract by the other party on one or more occasions, it is not taken to have agreed to any future breach.

30.6. These Master Terms, the Product Terms and the Order Form are the entire agreement between the parties with respect to the services specified in the Product Terms and all prior agreements regarding those services are superseded. No

amendment or modification of a Service Contract is binding unless in writing and executed by the parties.

30.7. Anything that is unenforceable must be read down, to the point of severance if necessary.

30.8. Anything a party can do, it may do through an appropriately authorised representative.

30.9. Any matter in our discretion is in our absolute and unfettered discretion.

31. Applicable law and disputes

31.1. This agreement is subject to the laws that apply in Queensland, Australia.

31.2. Any dispute or difference arising in connection with this agreement will be submitted to arbitration in accordance with and subject to the Institute of Arbitrators and Mediators Australia Expedited Commercial Arbitration Rules.

31.3. Otherwise, legal proceedings relating to this agreement or any dispute about it must be brought in the courts of Queensland, Australia.

32. Interpretation

32.1. Headings are for navigational assistance only and do not affect the meaning of this agreement.

32.2. Where a term is said to 'include' one or more things, the list is not exhaustive and does not limit the natural meaning of the term in anyway.

32.3. A schedule or attachment to a document (including a schedule or attachment to this agreement) is part of that document, as is any document incorporated by reference.

32.4. A reference to the singular includes the plural and vice versa.

32.5. There is no significance in the use of gender-specific language.

32.6. A 'person' includes any entity which can sue and be sued and any legal successor to or representative of that person.

32.7. A reference to 'hardware' or 'Loan Equipment' includes all IT and communication products and equipment including hardware, software and related parts, accessories and other goods.

32.8. A reference to a law includes any amendment or replacement of that law.

32.9. A provision must not be construed to the disadvantage of a party because that party prepared or required it.

SERVICE LEVEL AGREEMENT FOR SMB SOLUTIONS CLOUD SERVICES

This Service Level Agreement for SMB Solutions Cloud Services sets forth the System Availability Service Level Agreement ("**SLA**") for the productive version of the applicable Cloud Services to which customer has subscribed ("**Cloud Services**") in an Order Form with SMB Solutions Cloud Services.

Please note that we have utilised the standard Service Level Agreement for SAP Cloud Services as the model for our Service Level Agreement.

This Service Level Agreement for Cloud Services shall not apply to any Cloud Service for which a System Availability SLA is explicitly set forth in the applicable Supplemental Terms and Conditions for such Cloud Service or for which the applicability of the System Availability SLA is explicitly excluded in theAgreement.

Definitions

"**Downtime**" means the Total Minutes in the Month during which the productive version of the applicable SMB Cloud Service is not available, except for Excluded Downtimes.
"**Month**" means a calendar month.
"**Monthly Subscription Fees**" means the monthly (or 1/12 of the annual fee) subscription fees paid for the Cloud Service which did not meet the System Availability SLA.
"**Total Minutes in the Month"** are measured 24 hours at 7 days a week during a Month. "**UTC**" means Coordinated Universal Time standard.

1. System Availability SLA and Credits

1.1 Claim process, Reports

Customer may claim a credit in the amount described in the table of Section 3.2 below in case of SMBSCS's failure to meet the System Availability SLA, which credit Customer may apply to a future invoice relating to the SMB Cloud Service that did not meet the System Availability SLA.

Claims under this Service Level Agreement for SMB Cloud Services must be made in good faith and by submitting a support case within thirty (30) business days after the end of the relevant Month in which SMBSCS did not meet the System Availability SLA.

SMBSCS will provide to customers a monthly report describing the System Availability percentage for the applicable SMB Cloud Service either (i) by email following a customer's request to its assigned SMBSCS account manager, (ii) through the SMB Cloud Service or (iii) through an online portal made available to customers, if and when such online portal becomes available.

1.2 System Availability

System Availability percentage is calculated as follows:

$$\textit{System Availability Percentage} = \frac{\text{(Total Minutes per Month – Excluded Downtime – Downtime * 100)}}{\text{Total Minutes per Month – Excluded Downtime}} =$$

System Availability SLA	99.5% System Availability percentage during each Month for productive versions
Credit	2% of Monthly Subscription Fees for each 1% below System Availability SLA, not to exceed 100% of Monthly Subscription Fees
Excluded Downtime	Total Minutes in the Month attributable to: (i) a Scheduled Downtime for which a Regular Maintenance Window is described in Section 4 below, or (ii) any Major Upgrade Window described in Section 5 for which the customer has been notified at least five (5) business days prior to such Major Upgrade Window or (iii) unavailability caused by factors outside of SMB's reasonable control, such as unpredictable and unforeseeable events that could not have been avoided even if reasonable care had been exercised.
Scheduled Downtime	Scheduled Downtime for the applicable SMB Cloud Services to whichcustomer has subscribed is set forth in Section 2 below entitled "Maintenance Windows for SMB Solutions Cloud Services".

2. Maintenance Windows for SMB Solutions Cloud Services

SMB can use the following maintenance windows for Scheduled Downtimes as listed below. Time sones refer to the location of the primary data centre where the Cloud Service is hosted. SMBSCS will provide Customer reasonable notice without undue delay of any major upgrades or emergency maintenance to the SMB Solutions Cloud Services.

2.1 Weekly Maintenance Windows for SMB Solutions Cloud Services – Standard Windows

SMB weekly standard maintenance windows are scheduled as listed below for the Cloud Services in this section:

Start Time for all Regions Sunday 3 a.m.

The documented maintenance windows define the maximum scheduled downtime from which certain cloud services consume only partially.

2.2 Weekly Maintenance Windows for SMB Solutions Cloud Services Cloud Services – Individual Windows

Due to specific business reasons, the below listed SMB Cloud Services use individual maintenance windows

Cloud Services with individual maintenance window durations		
Cloud Service	**Maintenance Window**	**Duration**
SMB	3 a.m. – 7 a.m. Sunday	4 hours

23 Major Upgrade Windows for SMB Solutions Cloud Services

For more extensive changes to the SMB Cloud Services such as changing product versions, SMB uses the following Major Upgrade Windows for SMB Cloud Services

SMB Solutions Business One Cloud	**Up to 4 times per year:** Sunday 3 am – 3 pm

PERSONAL DATA PROCESSING AGREEMENT
FOR SMB SOLUTIONS CLOUD SERVICES CUSTOMERS (EU Region)

1. BACKGROUND

1.1 **Purpose and Application.** This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between B and Customer. This DPA applies to Personal Data processed by SMBSCS and its Subprocessors in connection with its provision of the Cloud Service. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by SMBSCS, and Customer shall not store Personal Data in such environments.

1.2 **Structure.** Appendices 1 and 2 are incorporated into and form part of this DPA. They set out the agreed subject-matter, the nature and purpose of the processing, the type of Personal Data, categories of data subjects and the applicable technical and organisational measures.

1.3 **GDPR.** SMBSCS and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("**GDPR**"), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA. For illustration purposes, Appendix 3 lists the relevant GDPR requirements and the corresponding sections in this DPA.

1.4 **Governance.** SMBSCS acts as a Processor and Customer (and those entities that it permits to use the Cloud Service) act as Controllers under this DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorisations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use SMBSCS as a Processor. Where authorisations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer, but also on behalf of any other such other Controller/s as the Customer has permitted to use the Cloud Service. Where SMBSCS informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service and it is Customer's responsibility to forward such information and notices to the relevant Controllers.

1.5 **The Act With Respect to the Use of Numbers to Identify a Specific Individual in Administrative Procedures (the "Act").** Without limiting Customer's obligations to SMBSCS under section 1.4 above, Customer and those entities that Customer permits to use the Cloud Service as Controllers under this DPA have complied with the obligations including, without limitation, obtaining the consent of all relevant Persons (as defined in the Act) with respect to the provision of Specific Personal Information (as defined in the Act) as may be required or directed under the Act, including, without limitation, Article 19.

2. SECURITY OF PROCESSING

2.1 **Appropriate Technical and Organisational Measures.** SMBSCS has implemented and will apply the technical and organisational measures set forth in Appendix 2. Customer has reviewed such measures and agrees that as to the Cloud Service selected by Customer in the Order Form the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

2.2 **Changes.** SMBSCS applies the technical and organisational measures set forth in Appendix 2 to SMBSCS's entire customer base hosted out of the same Data Center and receiving the same Cloud Service. SMBSCS may change the measures set out in Appendix 2 at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

3. SMBSCS OBLIGATIONS

3.1 **Instructions from Customer.** SMBSCS will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Cloud Service then constitutes further instructions. SMBSCS will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or SMBSCS otherwise cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, SMBSCS will immediately notify Customer (email permitted).

3.2 **Processing on Legal Requirement.** SMBSCS may also process Personal Data where required to do so by applicable law. In such a case, SMBSCS shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

3.3 **Personnel.** To process Personal Data, SMBSCS and its Subprocessors shall only grant access to authorised personnel who have committed themselves to confidentiality. SMBSCS and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures

3.4 **Cooperation.** At Customer's request, SMBSCS will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding SMBSCS's processing of Personal Data or any Personal Data Breach. SMBSCS shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. SMBSCS shall provide functionality that supports Customer's ability to correct or remove Personal Data from the Cloud Service or restrict its processing in line with Data Protection Law. Where such functionality is not provided, SMBSCS will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

3.5 **Personal Data Breach Notification.** SMBSCS will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. SMBSCS may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by SMBSCS.

3.6 **Data Protection Impact Assessment.** If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, SMBSCS will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.

4. DATA EXPORT AND DELETION

4.1 **Export and Retrieval by Customer.** During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case SMBSCS and Customer will find a reasonable method to allow Customer access to Personal Data.

4.2 **Deletion.** Before the Subscription Term expires, Customer may use SMBSCS's self-service export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs SMBSCS to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed six months) unless applicable law requires retention.

5. CERTIFICATIONS AND AUDITS

5.1 **Customer Audit.** Customer or its independent third-party auditor should be reasonably acceptable to SMBSCS (which shall not include any third-party auditors who are either a competitor of SMBSCS or not suitably qualified or independent) may audit SMBSCS's control environment and security practices relevant to Personal Data processed by SMBSCS only if:

(a) SMBSCS has not provided sufficient evidence of its compliance with the technical and organisational measures

that protect the production systems of the Cloud Service through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 or other SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third-party auditor or SMBSCS;

(b) A Personal Data Breach has occurred;

(c) An audit is formally requested by Customer's data protection authority;

(d) Mandatory Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve-month period unless mandatory Data Protection Law requires more frequent audits.

5.2 **Other Controller Audit.** Any other Controller may audit SMBSCS's control environment andsecurity practices relevant to Personal Data processed by SMBSCS in line with Section 5.1 only if any of the cases set out in Section 5.1 applies to such other Controller. Such audit must be undertaken through and by Customer as set out in Section 5.1 unless the audit must be undertaken by the other Controller itself under Data Protection Law. If several Controllers whose Personal Data is processed by SMBSCS on the basis of the Agreement require an audit, Customer shall use all reasonable means to combine the audits and to avoid multiple audits.

5.3 **Scope of Audit.** Customer shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimise repetitive audits. Customer shall provide the results of any audit to SMBSCS.

5.4 **Cost of Audits.** Customer shall bear the costs of any audit unless such audit reveals a material breach by SMBSCS of this DPA, then SMBSCS shall bear its own expenses of an audit. If an audit determines that SMBSCS has breached its obligations under the DPA, SMBSCS will promptly remedy the breach at its own cost.

6. SUBPROCESSORS

6.1 **Permitted Use.** SMBSCS is granted a general authorisation to subcontract the processing of Personal Data to Subprocessors, provided that:

(a) SMBSCS on its behalf shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. SMBSCS shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;

(b) SMBSCS will evaluate the security, privacy and confidentiality practices of a Subprocessorprior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

(c) SMBSCS's list of Subprocessors in place on the effective date of the Agreement is published by SMBSCS or SMBSCS will make it available to Customer upon request, including the name, address and role of each Subprocessor SMBSCS uses to provide the Cloud Service.

6.2 **New Subprocessors.** SMBSCS's use of Subprocessors is at its discretion, provided that:

(a) SMBSCS will inform Customer in advance (by email or by posting on the support portal available through SMBSCS Support) of any intended additions or replacements to the list of Subprocessors including name, address and role of the new Subprocessor; and

(b) Customer may object to such changes as set out in Section 6.3.

6.3 **Objections to New Subprocessors.**

(a) If Customer has a legitimate reason under Data Protection Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate the Agreement (limited to the Cloud Service for which the new Subprocessor is intended to be used) on written notice to SMBSCS. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of SMBSCS's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this thirty-day period, Customer is deemed to have accepted the new Subprocessor.

(b) Within the thirty-day period from the date of SMBSCS's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties come together in good faith to discuss a resolution to the objection. Such discussions shall not extend the period for termination and do not affect SMBSCS's right to use the

new Subprocessor(s) after the thirty-day period.

(c) Any termination under this Section 6.3 shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

6.4 **Emergency Replacement.** SMBSCS may replace a Subprocessor without advance notice where the reason for the change is outside of SMBSCS's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, SMBSCS will inform Customer of the replacement Subprocessor as soon as possible following its appointment. Section 6.3 applies accordingly.

7. INTERNATIONAL PROCESSING

7.1 **Conditions for International Processing.** SMBSCS shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

7.2 **Relation of the Standard Contractual Clauses to the Agreement.** Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and Subprocessor rules insections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.

7.3 **Governing Law of the Standard Contractual Clauses**. The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.

8. DOCUMENTATION; RECORDS OF PROCESSING

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

8.1 **Exclusions.** The following Personal Data is not subject to 9.2 and 9.3:

(a) Contact details of the sender of a support ticket; and

(b) Any other Personal Data submitted by Customer when filing a support ticket. Customer may choose not to transmit Personal Data when filing a support ticket. If this data is necessary for the incident management process, Customer may choose to anonymise that Personal Data before any transmission of the incident message to SMBSCS.

9. DEFINITIONS Capitalised terms not defined herein will have the meanings given to them in the Agreement.

9.1 **"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to SMBSCS be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

"Data Center" means the location where the production instance of the Cloud Service is hosted for the Customer in its region, as published at: https://www.smbsolutions.com.au/hosting-products/ or notified to Customer or otherwise agreed in an Order Form.

9.2 **"Data Protection Law"** means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by SMBSCS on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).

9.3 **"Data Subject"** means an identified or identifiable natural person as defined by Data Protection Law.

9.4 **"Personal Data"** means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is (i) entered by Customer or its Authorised Users into or derived from their use of the Cloud Service, or (ii) supplied to or accessed by SMBSCS or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).

9.5 **"Personal Data Breach"** means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or unauthorised third-party access to Personal Data or (2) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

9.6 **"Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as Subprocessor of a processor which processes personal data on behalf of the controller.

9.7 **"Standard Contractual Clauses** or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply). The Standard Contractual Clauses *current as of the effective date of the Agreement* are attached hereto as **Appendix 4.**

9.8 **"Subprocessor"** means SMBSCS Affiliates, and third parties engaged by SMBSCS, in connection with the Cloud Service and which process Personal Data in accordance with this DPA.

Appendix 1 to the DPA and, if applicable, the Standard Contractual Clauses

Data Exporter

The Data Exporter is the Customer who subscribed to a Cloud Service that allows Authorised Users to enter, amend, use, delete or otherwise process Personal Data. Where the Customer allows other Controllers to also use the Cloud Service, these other Controllers are also Data Exporters.

Data Importer

SMBSCS supports the Cloud Service data centres remotely from SMBSCS facilities in Australia and includes:

- Monitoring the Cloud Service
- Backup & restoration of Customer Data stored in the Cloud Service
- Release and development of fixes and upgrades to the Cloud Service
- Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database
- Security monitoring, network-based intrusion detection support, penetration testing SMBSCS provide support when a Customer submits a support ticket because the Cloud Service is not available or not working as expected for some or all authorised Users.
- SMBSCS answers phones and performs basic troubleshooting and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service.

Data Subjects

Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service.

Data Categories

The transferred Personal Data concerns the following categories of data:

Customer determines the categories of data per Cloud Service subscribed. Customer can configure the data fields during implementation of the Cloud Service or as otherwise provided by the Cloud Service. The transferred Personal Data typically relates to the following categories of data: name, phone numbers, e- mail address, time zone, address data, system access / usage / authorisation data, company name, contract data, invoice data, plus any application-

specific data that Authorised Users enter into the Cloud Service and may include bank account data, credit or debit card data.

Special Data Categories (if appropriate)

The transferred Personal Data concerns the following special categories of data: As set out in the Agreement (including the Order Form) if any.

Processing Operations / Purposes

The transferred Personal Data is subject to the following basic processing activities:

- use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)
- provision of Consulting Services;
- communication to Authorised Users
- storage of Personal Data in dedicated Data Centres (multi-tenant architecture)
- upload any fixes or upgrades to the Cloud Service
- back up of Personal Data
- computer processing of Personal Data, including data transmission, data retrieval, data access
- network access to allow Personal Data transfer
- execution of instructions of Customer in accordance with the Agreement.

Appendix 2 to the DPA and, if applicable, the Standard Contractual Clauses – Technical and Organisational Measures

This Appendix 2 comprises two sets of technical and organisational measures ("**TOMs**"):

TOMs SET 1

Last Updated: April 2020

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define SMBSCS's current technical and organisational measures. SMBSCS may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1.1 **Physical Access Control.** Unauthorised persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures: SMBSCS protects its assets and facilities using the appropriate means based on the SMBSCS Security Policy

- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems. Access rights are granted to authorised persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to SMBSCS buildings must register their names at reception and must be accompanied by authorised SMBSCS personnel.
- SMBSCS employees and external personnel must wear their ID cards at all SMBSCS locations.

Additional measures for Data Centres: All Data Centres adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Centre facilities from being compromised. Only authorised representatives have access to systems and infrastructure within the Data Centre facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.

- SMBSCS and all third-party Data Centre providers log the names and times of authorised personnel entering SMBSCS's private areas within the Data Centres.

1.2 **System Access Control.** Data processing systems used to provide the Cloud Service must be prevented from being used without authorisation.

Measures:

- Multiple authorisation levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorisations are managed via defined processes according to the SMBSCS Security Policy
- All personnel access SMBSCS's systems with a unique identifier (user ID).
- SMBSCS has procedures in place to so that requested authorisation changes are implemented only in accordance with the SMBSCS Security Policy (for example, no rights are granted without authorisation). In case personnel leaves the company, their access rights are revoked.
- SMBSCS has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalised user IDs are assigned for authentication. All passwords must fulfil defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver. The company network is protected from the public network by firewalls.
- SMBSCS uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations. Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to SMBSCS's corporate network and critical infrastructure is protected by strong authentication.

1.3 **Data Access Control.** Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorisation in the course of processing, use and storage.

Measures:

- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfil their duty. SMBSCS uses authorisation concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SMBSCS Security Policy.
- All production servers are operated in the Data Centres or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SMBSCS conducts internal and external security checks and penetration tests on its IT systems.
- SMBSCS does not allow the installation of software that has not been approved by SMBSCS. An SMBSCS security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 **Data Transmission Control.** Except as necessary for the provision of the Cloud Services in accordance with the Agreement, Personal Data must not be read, copied, modified or removed without authorisation during transfer. Where data carriers are physically transported, adequate measures are implemented at SMBSCS to provide the agreed-upon service levels (for example, encryption and lead-lined containers).

Measures:

- Personal Data in transfer over SMBSCS internal networks is protected according to SMBSCS Security Policy.
- When data is transferred between SMBSCS and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network-based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of SMBSCS-controlled

systems (e.g. data being transmitted outside the firewall of the SMBSCS Data Centre).

1.5 **Data Input Control.** It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from SMBSCS data processing systems.

Measures:

- SMBSCS only allows authorised personnel to access Personal Data as required in the course of their duty.
- SMBSCS has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SMBSCS or its Subprocessors within the Cloud Service to the extent technically possible.

1.6 **Job Control. Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance** with the Agreement and related instructions of the customer.

Measures:

- SMBSCS uses controls and processes to monitor compliance with contracts between SMBSCS and its customers, Subprocessors or other service providers.
- As part of the SMBSCS Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SMBSCS Information Classification standard.
- All SMBSCS employees and contractual Subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SMBSCS customers and partners.

1.7 **Availability Control.** Personal Data will be protected against accidental or unauthorised destruction or loss.

Measures:

- SMBSCS employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- SMBSCS uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centres.
- SMBSCS has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business-critical services as incorporated into the Order Form for the relevant Cloud Service.
- Emergency processes and systems are regularly tested.

1.8 **Data Separation Control.** Personal Data collected for different purposes can be processed separately.

Measures:

- SMBSCS uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customer (including its Controllers) has access only to its own data.
- If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

1.9 **Data Integrity Control.** Personal Data will remain intact, complete and current during processing activities.

Measures:

SMBSCS has implemented a multi-layered defence strategy as a protection against unauthorised modifications.
In particular, SMBSCS uses the following to implement the control and measure sections described above.

- Firewalls;
- Security Monitoring Centre;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.

TOMs SET 2

Last Updated: May 4 2020

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define SMBSCS's current technical and organisational measures. SMBSCS may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1.1 Physical Access Control.

- SMBSCS protects its assets and facilities using the appropriate means based on the SMBSCS Security Policy
- In general, buildings are secured through access control systems (e.g., smart card access system).
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises may be further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are granted to authorised persons on an individual basis according to the System and Data Access Control measures (see Section 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to SMBSCS buildings must register their names at reception and must be accompanied by authorised SMBSCS personnel.
- SMBSCS employees and external personnel must wear their ID cards at all SMBSCS locations.

Additional measures for Data Centres:

- All Data Centres adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Centre facilities from being compromised. Only authorised representatives have access to systems and infrastructure within the Data Centre facilities. To protect proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
- SMBSCS and all third-party Data Centre providers log the names and times of authorised personnel entering SMBSCS's private areas within the Data Centres.

1.2 System Access Control.

- Multiple authorisation levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorisations are managed via defined processes according to the SMBSCS Security Policy
- All personnel access SMBSCS's systems with a unique identifier (user ID).
- SMBSCS has policies designed to provide that no rights are granted without authorisation and in case personnel leaves the company their access rights are revoked.
- SMBSCS has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalised user IDs are assigned for authentication. All passwords must fulfil defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- SMBSCS uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Security patch management process to deploy relevant security updates on a regular and periodic basis. Full remote access to SMBSCS's corporate network and critical infrastructure is protected by authentication.

1.3 Data Access Control.

- As part of the SMBSCS Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SMBSCS Information Classification standard.
- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfil their duty. SMBSCS uses authorisation concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the SMBSCS Security Policy.
- All production servers are operated in the Data Centres or in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, SMBSCS conducts internal and external security checks and/or penetration tests on its IT systems.
- Processes and policies to detect the installation of unapproved software on production systems.
- An SMBSCS security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control.

- Personal Data in transfer over SMBSCS internal networks is protected according to SMBSCS Security Policy.
- When data is transferred between SMBSCS and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network-based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of SMBSCS-controlled systems (e.g. data being transmitted outside the firewall of the SMBSCS Data Centre).

1.5 Data Input Control.

- SMBSCS only allows authorised personnel to access Personal Data as required in the course of their duty.
- SMBSCS has implemented a logging system for input, modification and deletion, or blocking of Personal Data by SMBSCS or its sub-processors within the Cloud Service to the extent technically possible.

1.6 Job Control.

- SMBSCS uses controls and processes to monitor compliance with contracts between SMBSCS and its customers, Subprocessors or other service providers.
- As part of the SMBSCS Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the SMBSCS Information Classification standard.
- All SMBSCS employees and contractual Subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of SMBSCS customers and partners.

1.7 Availability Control.

- SMBSCS employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- SMBSCS uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centres.
- SMBSCS has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business-critical Services as further set out in the Order Form for the relevant Cloud Service.
- Emergency processes and systems are regularly tested.

1.8 Data Separation Control.

- SMBSCS uses the technical capabilities of the deployed software (for example: multi- tenancy, or separate system landscapes) to achieve data separation among Personal Data originating from multiple customers.
- Customer (including its Controllers) has access only to its own data.
- If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

1.9 Data Integrity Control.

SMBSCS has implemented a multi-layered defence strategy as a protection against unauthorised modifications. In particular, SMBSCS uses the following to implement the control and measure sections described above.

- Firewalls;
- Security Monitoring Centre;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing and/or regular external audits to prove security measures.

Appendix 3 to the DPA and, if applicable, the Standard Contractual Clauses

The following table sets out the relevant Articles of GDPR and corresponding terms of the DPA for illustration purposes only.

Article of GDPF	**Section of DPA**	
28(1)	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organisational Measures
28(2), 28(3) (d) and 28 (4)	6	Subprocessors
28 (3) sentence 1	1.1 and Appendix 1, 1.2	Purpose and Application Structure
28(3) (a) and 29	3.1 and 3.2	Instructions from Customer. Processing on Legal Requirement.
28(3) (b)	3.3	Personnel
28(3) (c) and 32	2 and Appendix 2	Security of Processing and Appendix 2, Technical and Organisational Measures
28(3) (e)	3.4	Cooperation
28(3) (f) and 32-36	2 and Appendix 2, 3.5, 3.6	Security of Processing and Appendix 2, Technical and Organisational Measures. Personal Data Breach Notification. Data Protection Impact Assessment.
28(3) (g)	4	Data export and Deletion.
28(3) (h)	5	Certifications and Audits
28 (4)	6	Subprocessor
30	8	Documentation; Records of processing.
46(2) (c)	7.2	Standard Contractual Clauses.

Appendix 4

[The Standard Contractual Clauses set out in this Appendix 4 are current as at 31 March 2018, and the Japanese translation is provided as a matter of convenience only. These Standard Contractual Clauses are automatically subject to updates by the European Commission and as subsequently published by the European Commission, Customer should always access the URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087 for updated versions of the Standard Contractual Clauses.

Customer's local language may not be supported at the European Commission, or at URL, and it will be Customer's responsibility to ensure that it is aware of the current version/s of the Standard Contractual Clauses and manages any necessary translations of any updates of those Standard Contractual Clauses]

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)[1]

For the purposes of Article 26(2) of Directive 95/46/EC (or, after 25 May 2018, Article 44 et seq. of Regulation 2016/79) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Customer also on behalf of the other Controllers (in the Clauses hereinafter referred to as the '**data exporter'**) SMBSCS (in the Clauses hereinafter referred to as the 'data importer') each a 'party'; together 'the parties',

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

[1] Pursuant to Commission Decision of 5 February 2010 (2010/87/EU)

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 1

Details of the transfer

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

Clause 2

Third-party beneficiary

1. The data subject can enforce against the data exporter this Clause, Clause 3(b) to (i), Clause 4(a) to (e), and (g) to (j), Clause 5(1) and (2), Clause 6, Clause 7(2), and Clauses 8 to 11 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 4(a) to (e) and (g), Clause 5, Clause 6,Clause 7(2), and Clauses 8 to 11, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 4(a) to (e) and (g), Clause 5, Clause 6, Clause 7(2), and Clauses 8 to 11, in cases where both the data exporter and the data

importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 3

Obligations of the data exporter

The data exporter agrees and warrants:

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

Clause 4

Obligations of the data importer

The data importer agrees and warrants:

1. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
2. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
3. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
4. that it will promptly notify the data exporter about:
    a. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
    b. any accidental or unauthorised access; and
    c. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
5. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
6. at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
7. to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
8. that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
9. that the processing services by the sub-processor will be carried out in accordance with Clause 11;
10. to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 5

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub- processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually

disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

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

Clause 6

Mediation and jurisdiction

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

Clause 7

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 4(2).

Clause 8

Governing law

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

Clause 9

Variation of the contract

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

Clause 10

Sub-processing

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

Clause 11

Obligation after the termination of personal data-processing services

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

SMB Solutions Cloud Services Order Form

Customer Information

Click or tap to enter a date.
Date Required

Business Name

Reseller / Partner

Street address, City, State, Post Code

Primary Contact Name and Phone number | Other phone number

Email address

SAP Business One Solution:

☐ SQL Server ☐ HANA ☐ Version 10 ☐ Version 9.3

Do you have an existing customer/database to migrate?

☐ Yes ☐ No

Financial Year Posting Periods

☐ Yearly ☐ Quarterly ☐ Monthly

Financial Year Start Date: 01/07/2019 (please adjust accordingly)

Billing Schedule:

☐ Yearly ☐ Quarterly ☐ Monthly

User Details

Please list the names and emails of all new users

Name Email

Name Email

Name Email

Name Email

Name	Email
Name	Email
Name	Email
Name	Email
Name	Email
Name	Email
Name	Email
Name	Email
Name	Email

Please use a duplicate of this page for any additional users.

Extra Functionality Request Form

SAP Business One Solution:

☐ Crystal Reports ☐ Data Transfer Workbench ☐ Excel Report Tools

SAP Extensions / Addons:

☐ Payment Addon ☐ EFM Format Definition ☐ Screen Painter

Other Extensions / Addons:

☐ B1 Usability (Boyum) ☐ Print & Delivery (Boyum) ☐ beAS Manufacturing

☐ Enterpryze ☐ ProcessForce

SAP Business One Mobile Applications:

☐ SAP Business One Mobile Application (SQL & HANA) ☐ SAP Business One Sales App (HANA Only) ☐ SAP Business One Service App (HANA Only)