ORIGO LEGAL FRAMEWORK

SERVICES AGREEMENT: PROVIDER – INTERMEDIARY

VERSION 4.0

DRAFT FINAL

31st January 2018

You should carefully read the following terms and conditions. By clicking "Accept" you confirm that you have read and understood the terms and conditions, and that you agree to be bound by them. If you are accepting the terms and conditions on behalf of a firm or corporate entity you warrant that you have the authority to do so.

In these Terms “Aviva”, “Provider”, “we”, “us” or “our” shall mean Aviva Life Services UK Limited.

References in these Terms to “Intermediary”, “you” or “your” shall mean the party to these Terms other than Aviva.

1. DEFINITIONS AND INTERPRETATION

The term "**Agreement**" means this agreement, together with the attached Schedule, as may be amended from time to time in accordance with Clause 20. The meanings of the defined terms in this Agreement are as set out in Schedule 1 (Definitions).

2. TERM

This Agreement will commence on the Commencement Date and remain in force until terminated in accordance with the provisions under this Agreement.

3. APPROVED INTERMEDIARY

3.1 The Intermediary acknowledges that in order to obtain access to the services of an Approved TPSP in respect of the Provider, the Intermediary must have an agreement in place with that Approved TPSP (substantially in the form of the Origo Legal Framework v4.0 Intermediary - Third Party Service Provider Services Agreement) for the provision of the Intermediary Services (the "**Approved TPSP Intermediary Agreement**").

3.2 The Provider will provide the Direct Services to the Intermediary from the Commencement Date or from such other date or dates as set out in the Technical Schedule.

4. THE SYSTEM STANDARDS

4.1 Provider Obligations

4.1.1 The Provider will operate the Provider System in accordance with the relevant part of the Provider Standards.

4.1.2 The Provider will notify the Intermediary immediately on detecting any Defect in the Provider System and will put in place appropriate measures to minimise and to mitigate the effects of any Defect detected in the Provider System and for the correction of such Defect.

4.2 **Intermediary Obligations**

4.2.1 The Intermediary is responsible for ensuring that the Intermediary System is maintained and secured in accordance with the Security Standards.

4.2.2 The Intermediary will operate the Intermediary System in accordance with the Intermediary Standards.

4.2.3 The Intermediary will notify the Provider immediately on detecting any Defect in the Intermediary System and, where reasonably practicable, will put in place appropriate measures to minimise and to mitigate the effects of any Defect detected in the Intermediary System and for the correction of such Defect.

4.3 **General Obligations**

4.3.1 Each Party will notify the other immediately upon becoming aware of, or detecting, any Defect in an Approved TPSP System and shall co-operate with the other Party and will use reasonable endeavours to put in place appropriate measures to minimise and to mitigate the effects of any such Defect detected in the Approved TPSP System.

4.3.2 The Provider will notify the Intermediary, and the Intermediary will notify the Provider, immediately upon becoming aware that an Approved TPSP is in breach of its obligations under, respectively, the Approved TPSP Provider Agreement and the Approved TPSP Intermediary Agreement. Each Party will co-operate with the other Party (to the extent reasonably possible and subject to any obligations of confidentiality) in respect of any investigation into the breach by the Approved TPSP, and will use reasonable endeavours to put in place appropriate measures to minimise and to mitigate the impact of any such breach on the other Party.

5. THE SERVICES

5.1 **General Obligations**

5.1.1 The Intermediary will be responsible for ensuring that it has all the necessary computer hardware, software, modems, connections and other items required for access to, and use of, the Services by the Intermediary and its Users.

5.1.2 The Provider will not be responsible for any delays or failure to perform its obligations under this Agreement if and to the extent that they result from any failure by the Intermediary to provide such assistance as may reasonably be required from the Intermediary by the Provider in order to enable the Provider to carry out its obligations under this Agreement. The Intermediary acknowledges that the Provider will not be liable to the Intermediary for any delay, act or omission of an Approved TPSP.

5.1.3 Where the Provider wishes to provide additional services to the Intermediary within the scope of this Agreement, these will be added to the Services at the Technical Schedule in accordance with Clause 20.

5.1.4 The Provider reserves the right to immediately suspend or terminate the Intermediary's right to use all or part of the Direct Services and to receive Messages from the Provider through any Approved TPSP where:

(a) the Intermediary uses the Direct Services or the Provider System for any purpose not expressly contemplated or permitted by this Agreement; and / or

(b) the Provider deems such suspension necessary to ensure the Provider's compliance with applicable law and regulatory requirements; and/or

(c) the Intermediary persistently fails to ensure that its Users are complying with any User Guidelines.

5.1.5 In addition to Clause 5.1.4, the Provider reserves the right to immediately terminate the Intermediary's right to receive Messages through an Approved TPSP, where the Approved TPSP Provider Agreement with that Approved TPSP is terminated (for whatever reason).

5.1.6 The Intermediary acknowledges and agrees that no Approved TPSP will be liable to the Intermediary or to any User for such suspension or termination by the Provider under Clause 5.1.4 or Clause 5.1.5.

5.1.7 The Intermediary will be responsible for reviewing and complying with the User Guidelines, and will ensure the continued adherence to the User Guidelines by the Users.

5.2 **Direct Services**

5.2.1 The Provider:

(a) will provide the Direct Services to the Intermediary in accordance with this Agreement unless and until this Agreement is terminated or in respect of any individual service forming part of the Direct Services, until that service is withdrawn by the Provider (for whatever reason); and

(b) undertakes to provide the Direct Services in accordance with the Provider Standards.

5.2.2 The Intermediary undertakes to the Provider to access and use, and procure that each User accesses and uses, the Direct Services in accordance with the Intermediary Standards, the User Guidelines and any reasonable instructions given by the Provider from time to time.

6. USER ACCESS

6.1 **General**

6.1.1 A User will only be permitted to gain access to the Services by using the appropriate User Access. The Intermediary will, and will procure that each User will:

(a) only access the Services using the appropriate User Access;

(b) employ the User Access solely for the purpose of accessing the Services in accordance with this Agreement and any User Guidelines, and not attempt to gain unauthorised access to the Provider System;

(c) keep all relevant information and processes in respect of the User Access confidential and not divulge such information and processes to any third party;

(d) store all relevant information concerning the User Access securely; and

(e) notify the Provider immediately on becoming aware of any unauthorised access to the Services or anything amounting to a Security Breach, including compromise of any information concerning the User Access.

6.1.2 Subject to Clause 6.1.3, the Intermediary will implement and maintain a system for recording and / or checking the revocation or suspension of the access rights of Users in

accordance with the Revocation System. The Intermediary will be liable for any and all acts or omissions resulting from the use of the User Access by any of its Users, including Users whose permission to use the Services has been withdrawn or suspended for whatever reason.

6.1.3 The Parties acknowledge that where access to the Intermediary Services is to be controlled by an Approved TPSP (whether alone or in conjunction with the Intermediary), that Approved TPSP will be responsible for recording and/or checking the revocation or suspension of the access rights of Users, but that the Intermediary will remain responsible for ensuring that only permitted individuals access and use the Services.

6.1.4 For the avoidance of doubt, the obligations under Clauses 6.1.1 and 6.1.2 will not affect any administration services or guidelines with which the Intermediary or a User is required to comply under any contract with a third-party provider of the User Access.

6.2 **Direct Services**

6.2.1 Where a User is accessing the Direct Services, the Provider will check that the access rights of the Intermediary to the Direct Services have not been revoked or suspended and will not permit a User to access and use the Direct Services where the Intermediary's access has been revoked or suspended.

7. MESSAGES GENERATED BY THE INTERMEDIARY

7.1 In order for Messages generated by (or on behalf of) the Intermediary to be processed by (or on behalf of) the Provider, they must be created, transmitted and Authenticated in accordance with the Standards.

7.2 **General**

7.2.1 The Provider will, at the time the Message is received, cross-check that Terms of Business are in force with the Intermediary or, where the Intermediary is an Appointed Representative, with the Authorised Firm.

7.2.2 The Intermediary is responsible for ensuring that all Messages generated by its Users, or generated by the Intermediary System in response to enquiries from its Users, are legitimate and that the Data submitted in the Message is accurate.

7.2.3 The Intermediary undertakes to, and will ensure that each User will:

(a) use all due care and diligence when inputting data; and

(b) check all information carefully before submitting it to the Provider.

7.3 **Intermediary Services**

7.3.1 In respect of the Intermediary Services, the Provider will:

(a) Authenticate the Approved TPSP from which it received the Message; and

(b) identify the Intermediary from the relevant data contained in the Message.

7.4 **Direct Services**

7.4.1 In respect of the Direct Services, the Provider will Authenticate the Intermediary.

8. MESSAGES GENERATED BY THE PROVIDER

8.1 The Provider will create and transmit Messages, or will procure the creation, transmission and Authentication of Messages, in accordance with the Standards.

8.2 The Intermediary acknowledges that a Message may be:

8.2.1 provided to an Intermediary (either directly or via one or more Approved TPSPs) in response to a Message generated by, or on behalf of, the Intermediary; or

8.2.2 automatically generated and provided to the Intermediary at times determined by the Provider or agreed between the Parties.

8.3 **Provider Obligations**

8.3.1 The Provider will provide, or will procure the provision of a Message, to the Intermediary in accordance with the Provider Standards.

8.3.2 The Provider is responsible for ensuring that Data contained in any Message generated by it, or on its behalf, is accurate, subject to any relevant pending transactions not yet fully processed, and that there are no Errors in any Message which it generates.

8.3.3 Where a User is accessing the Services, the Provider will be responsible for cross-checking that the Intermediary is entitled to receive the Data (including the details in respect of a particular Customer policy).

8.4 **Intermediary Obligations**

The Intermediary undertakes to the Provider:

8.4.1 that where any part of a Message generated by, or on behalf of, the Provider is disclosed to a Customer, such disclosure will be made subject to any notes from the Provider which are contained within the Message relating to the presentation or disclosure of that Message;

8.4.2 to ensure that any Message, or Data contained within a Message, received by the Intermediary is not disclosed to any person not authorised to access and / or view it; and

8.4.3 to ensure that a User who receives or is able to access a Message in error will:

(a) not use or disclose the Message for any purpose whatsoever; and

(b) promptly notify the Provider; and

8.4.4 not to use, or permit the use of, the Message for any purposes other than those specified in the Technical Schedule or, if none are specified, not to use, or permit the use of, the Message for any purposes other than as may be required by the Intermediary in order to carry out its legitimate business.

8.5 **Exclusions of Liability**

Subject to the Provider's obligation under Clause 8.3.2, a Message is supplied by the Provider to the User on a "for information only" basis. The Provider will use its reasonable endeavours to ensure the accuracy of any Message but does not warrant to the Intermediary that the Message, the Data contained within the Message or any part of it complies with any legal or regulatory requirements in relation to the presentation and/or the form of that Data, nor that the Data can be used legitimately outside the United Kingdom.

8.6 **Transmissions**

A Message will be deemed to have been received at the time that it enters an information system of the intended recipient provided that no message indicating a failure to deliver has been received by the sender.

9. INTELLECTUAL PROPERTY RIGHTS IN DATA

9.1 The Parties acknowledge and agree that all Intellectual Property Rights in the Data will, at all times, remain with the Party from whom the Data originated (or its licensors), whether the Data is in human or machine-readable form. The Parties agree to comply with their respective obligations in this Clause 9 in respect of the use and protection of Data.

9.2 **Provider Obligations**

9.2.1 The Provider will, at all times, retain control of the keys necessary to decrypt any encrypted Data. Where the encrypted Data cannot be decrypted, the Provider will securely provide the Intermediary with a readable copy of the Data or provide the necessary key for decrypting the encrypted Data, at the request of the Intermediary.

9.2.2 In the event that the Intermediary is required to provide the key necessary to decrypt any encrypted Data to any party who is legally authorised to receive the key, the Provider will securely provide such key immediately on receiving a request from the Intermediary to do so.

9.3 **Collective Obligations**

9.3.1 Each Party undertakes to the other Party not to copy, distribute or use the Data of the other Party, nor reproduce that Data in whole or in part, in any form (whether in hard copy, electronic or other), except as provided by this Agreement or as necessary for the Party to carry out its obligations under this Agreement.

9.3.2 Each Party will bear responsibility for the back-up of its Data and protection against loss of Data.

9.3.3 To the extent permitted by applicable law, neither Party makes any warranties or representations that any Data sent by it is free from computer viruses or other defects. Each Party acknowledges that it is responsible for taking its own precautions to ensure that all Messages, Data, programs and files received from the other Party are free from computer viruses or other defects.

9.3.4 Notwithstanding Clause 9.3.3, each Party:

(a) will take reasonable steps to prevent the introduction by its personnel of computer viruses into any Messages, programs and files sent to the other Party (or to an Approved TPSP); and

(b) warrants, represents and undertakes to the other Party that it will not wilfully introduce any viruses, worms, trojan horses or other contaminants, including any code which will or may be used to access, modify, delete or damage any data, files or other computer programs used by the other Party (or by an Approved TPSP) into any Message or other electronic communication between the Parties (or to or from an Approved TPSP).

9.3.5 Each of the Parties accepts the validity of Messages and agrees to accord Messages the same status as would be applicable to a document or to Data sent or provided otherwise than by electronic means.

10. THIRD PARTY SUPPLIERS

The Parties acknowledge that certain third-party providers of ancillary software or services (including the provider of the User Access and any relevant Approved TPSPs), which may be used by the Provider, the Intermediary and/or the User in relation to the provision of the Services, may require an Intermediary and/or User to agree to additional terms for the use of such software or services by the Intermediary or any User. Such terms will be without prejudice to the obligations and responsibilities of the Parties under this Agreement.

11. CONTACTS

Each of the Parties will designate and give the other Party the details of those key contacts (as may change from time to time) that will oversee the performance of its obligations, and act as its liaison, under this Agreement, and to whom day-to-day communications regarding the Services will be directed.

12. WARRANTIES

12.1 Each of the Parties warrants and represents to the other that:

12.1.1 it has the necessary rights to perform its obligations under this Agreement; and

12.1.2 it has full legal authority to enter into this Agreement.

12.2 The Provider warrants and represents to the Intermediary that:

12.2.1 it will provide the Direct Services and perform all other obligations under this Agreement with reasonable skill and care;

12.2.2 it has full rights to grant the licences referred to in this Agreement free from all liens, claims encumbrances and other restrictions; and

12.2.3 it has all the necessary rights to use the Standards.

12.3 Where the Intermediary is not authorised in its own right under the FSMA, it warrants and represents that it is an Appointed Representative. The Intermediary warrants and represents that it will notify the Provider and the Approved TPSP immediately on ceasing to be the Appointed Representative of the Authorised Firm, in which event the provisions of Clause 16.4 will apply.

13. LIMITATION OF LIABILITY

13.1 Subject to Clause 13.2, the aggregate liability of each Party to the other Party arising out of breach of contract, or breach of any term of this Agreement, whether express or implied or breach of any common law or statutory duty (including any duty in relation to tort (including negligence) for any single event or series of connected events arising out of this Agreement will not exceed fifteen thousand pounds (£15,000) sterling.

13.2 The limitation of liability referred to in Clause 13.1 will not apply to:

13.2.1 the liability of either Party to the other Party pursuant to Clause 15, which liability will not be limited unless a limit on liability is specified in the Technical Schedule as applying (in which case such limit shall apply); and

13.2.2 the liability of any Party for breach of any obligations of confidence, which liability will not be limited.

13.3 Except for a breach of Clause 15, neither Party will be liable for any consequential, indirect or special losses, for loss of profits, business revenue, goodwill or anticipated savings suffered or incurred by the other Party as a result of any breach of any warranty contained in this Agreement or any of the provisions of this Agreement, regardless of whether the Party had been informed or had reason to know of the possibility of such loss.

13.4 Each of the Parties acknowledges and agrees that the other will not be liable to it under any circumstances for any consequences arising from Errors, lost Data, or lost or corrupted files as a result of its own failure to implement necessary backup or employ the Standards.

13.5 Nothing contained in this Agreement will exclude or limit either Party's liability for fraud, or for death or personal injury resulting from any act, omission or negligence of that Party or its officers, agents, employees or sub-contractors, or any other liability the exclusion of which is expressly prohibited by statute.

14. INTELLECTUAL PROPERTY

14.1 Except as expressly provided in this Agreement, neither of the Parties will acquire any proprietary rights, title or interest in or to any Intellectual Property Rights of the other Party pursuant to this Agreement.

14.2 The Provider hereby grants, for the duration of the term, a non-exclusive, non-transferable, royalty-free licence to the Intermediary to use the appropriate part of the Provider System as is necessary for the Intermediary to access and use the Direct Services.

15. DATA PROTECTION

15.1 In this Clause "**Controller**", "**Processor**" and "**Data Subject**" will have the meanings set out in the Data Protection Laws, and "**Individual Rights**" means the rights of Data Subjects under the Data Protection Laws.

15.2 Each of the Intermediary and the Provider acknowledges that it acts as a Controller in respect of any Customer Personal Data Processed by that Party (or its Processors on its behalf) irrespective of ownership of the Intellectual Property Rights in Customer Personal Data.

15.3 Each of the Intermediary and the Provider agrees that:

15.3.1 it is separately responsible for compliance with the Data Protection Laws;

15.3.2 it will Process Customer Personal Data in accordance with the Data Protection Laws at all times; and

15.3.3 it will be wholly responsible for its own Processing of Customer Personal Data.

15.4 Each of the Provider and the Intermediary warrants and represents that it has in place all necessary notifications, including notifications to Data Subjects in respect of its Processing of Personal Data, in each case, as required by the Data Protection Laws.

16. TERMINATION

16.1 In addition to the other rights of termination set out in this Agreement, this Agreement may be terminated:

16.1.1 by either Party immediately on giving written notice to the other if the other Party commits any material breach of any provision of this Agreement which is not capable of remedy or, if capable of remedy, fails to remedy the breach within thirty (30) days of receiving notice specifying the breach and requiring it to be remedied; or

16.1.2 by either Party immediately on giving written notice if the other ceases trading, or threatens to cease trading, or becomes apparently insolvent or has a trustee in sequestration appointed, combines with its creditors, or has a liquidator, receiver or administrator appointed over all or any of its assets other than for the purposes of a solvent amalgamation or reconstruction or undergoes any analogous act or proceeding under foreign law; or

16.1.3 by the Provider immediately on giving written notice to the Intermediary if there is a change of control (as defined in Section 574 of the Capital Allowances Act 2001) of the Intermediary to which the Provider reasonably objects; or

16.1.4 by the Provider where either Party to the Terms of Business has served notice to the other to terminate the Terms of Business; or

16.1.5 by either Party on giving the other fourteen (14) days' written notice; or

16.1.6 by the Provider immediately on giving written notice to the Intermediary in the event that the Intermediary uses any Data of the Provider in breach of this Agreement, or carries out any act or conducts itself in a manner which brings the Provider's name into disrepute or is otherwise detrimental to the reputation of, and goodwill in, the Provider's name.

16.2 The Provider will be entitled to withdraw (in whole or in part) any of the services provided under this Agreement (whether provided as part of the Direct Services or provided via an Approved TPSP) at any time without prior notice to the Intermediary.

16.3 For the purposes of this Clause 16, a breach will be capable of remedy if the other Party can comply with the provisions in question in all respects other than as to the time for performance.

16.4 Where the Intermediary is an Appointed Representative, the Provider will be entitled to terminate this Agreement, and require an Approved TPSP to concurrently terminate the Intermediary's right to use the Intermediary Services in respect of the Provider, with immediate effect on being notified that the Intermediary has ceased to be an Appointed Representative of the Authorised Firm.

17. CONSEQUENCES OF TERMINATION

17.1 On termination of this Agreement, for whatever reason, the access rights of the Intermediary (including its Users) to the Direct Services and to the Intermediary Services in respect of the Provider will be withdrawn immediately.

17.2 The Intermediary acknowledges that on termination (for whatever reason) of an Approved TPSP Provider Agreement, the access rights of the Intermediary (including its Users) to the Intermediary Services in respect of the Provider and that Approved TPSP will be withdrawn immediately.

17.3 Any termination of this Agreement, for whatever reason, will be without prejudice to any other rights or remedies of either Party under this Agreement or at law and will not affect any accrued rights or liabilities of a Party at the date of termination, nor will termination affect any rights or obligations of the Parties which are to be observed or performed after such termination including those warranties as set out in this Agreement.

17.4 Within ten (10) Working Days after the date of termination of this Agreement, each Party will delete all copies of all software, materials or information, other than Data, belonging to the other Party, except as otherwise permitted or required by this Agreement or Terms of Business, or to the extent that the Party is required to keep the information for the purposes of complying with any legislation and regulatory requirements.

18. AUDIT AND AUDIT TRAIL

18.1 During the term of this Agreement and for a period of twelve (12) months after the date of termination of this Agreement, the Intermediary will maintain accurate and up-to-date records, documentation and other similar materials, whether financial or otherwise, relating to this Agreement.

18.2 At the request of the Provider, the Intermediary will promptly make available to the Provider, its internal and external auditors, representatives of a Regulator or any third party appointed by the Provider (but no more than twice in any period of twelve (12) months for anyone other than representatives of the Regulator), all information required by the Provider, such auditors or representatives, or any appointed third party relating to the Services at all reasonable times, and will permit the Provider, such auditors or representatives, or any appointed third party, to inspect, review, verify and take copies of any associated records and documentation in the control or possession of the Intermediary.

18.3 The Intermediary agrees to provide such access to the Intermediary's premises and afford all reasonable assistance in good faith, as may reasonably be required for the purposes of the inspection, review and verification under Clause 18.2.

18.4 The Provider will ensure that any inspection or review under this Clause 18 which is undertaken on its instructions be undertaken, as far as reasonably possible, so as to minimise disruption to the Intermediary’s business, both generally and in relation to the provision of the Services.

18.5 Any inspection or review under this Clause 18 is for the sole benefit of the Provider and will not constitute a waiver or exclusion of any obligation of the Intermediary or of the Provider's rights and remedies under this Agreement.

18.6 The Intermediary's costs of any inspection or review under this Clause 18 will be paid by the Intermediary. The Intermediary will additionally bear the reasonable costs of the Provider of any inspection or review under this Clause 18 if the inspection or review finds any material errors or non-compliance on the part of the Intermediary, either with any statutory or regulatory requirements or with the terms of this Agreement. Except as provided in this Clause 18.6, the Provider's costs of any inspection or review will be paid by the Provider.

18.7 Each Party acknowledges that it is advisable to retain its respective part of the Audit Trail for a minimum period of six (6) months from the date of creation of the Audit Trail.

18.8 Each of the Parties may produce and rely on any part of the Audit Trail and any Message in its control to facilitate the resolution of any dispute between the Parties which arises out of, or in connection with, this Agreement. Each of the Parties undertake to keep confidential any disclosed Audit Trail of the other Party and the Intellectual Property Rights in any part of the Audit Trail will remain with the Party from which it originated.

18.9 The Parties shall co-operate to facilitate the resolution of any dispute between the Provider and an Approved TPSP or the Intermediary and an Approved TPSP in relation to the Intermediary Services and/or Customer Personal Data, and, where reasonably requested by

the other Party, each Party will produce any part of its Audit Trail or any Message which may help the other Party to resolve its dispute with the Approved TPSP.

19. FORCE MAJEURE

19.1 Notwithstanding anything else contained in this Agreement, neither Party will be liable for any delay in or failure to perform its obligations under this Agreement if such delay or failure is caused by an event of Force Majeure, provided that the Party promptly notifies the other Party in writing of the reasons for the delay or failure of the performance of its obligations.

19.2 If any such delay or failure referred to in Clause 19.1 continues for more than eight (8) weeks, either Party may terminate this Agreement immediately on giving notice in writing to the other Party, in which event neither Party will be liable to the other by reason of such termination. Except for delays caused by the acts or omissions of the Party (in which event the rights and liabilities of the Parties will be those conferred and imposed by the other terms of this Agreement and by law) any cost arising from such delay will be borne by the Party incurring the same.

20. AMENDMENT

20.1 The Provider reserves the right to vary the terms and conditions of any part of this Agreement by giving the Intermediary notice in writing. Any variation will take effect on the expiry of thirty (30) days of notice being given to the Intermediary ("**Variation Notice Period**"). If the Intermediary does not agree to the variation, it will be entitled to terminate this Agreement immediately on giving the Provider notice in writing, provided that such termination notice is received by the Provider prior to the expiry of the Variation Notice Period. The Intermediary's continued use of the Services beyond the expiry date will be confirmation of acceptance of this Agreement as varied.

20.2 For the purposes of Clause 20.1, notice may be given to the Intermediary by posting the variation to the Site.

20.3 The Provider may give less than thirty (30) days' notice of a variation where the variation is the result of legislative or regulatory requirements.

21. GENERAL

21.1 **Assignment**

21.1.1 Subject to Clause 21.1.2 below, neither the Provider nor the Intermediary is entitled to assign, transfer, charge, declare a trust for the benefit of, or otherwise deal with any of its rights and obligations arising under this Agreement without the prior written consent of the other, such consent not to be unreasonably withheld or delayed.

21.1.2 The Provider will be entitled to freely assign the entire benefit of this Agreement as a whole to any other Group Company. The Provider may assign its rights under this Agreement (subject to the assumption by the assignee of all of the Provider's obligations) without the prior written consent of the Intermediary to any company or other organisation to which the Provider has transferred all or substantially all of its assets pursuant to its demutualisation under Part VII of FSMA or otherwise.

21.1.3 The Intermediary undertakes to execute such documents as are necessary to effect any assignment referred to in this Clause 21.1.2.

21.2 **Relationship of the Parties**

Nothing in this Agreement will create, or be deemed to create, a partnership or joint venture or relationship of employee and employer or principal and agent between the Parties. Neither Party is agent for the other, and neither Party has any authority to make any contract, whether expressly or by implication, in the name of the other Party, without that Party's prior written consent.

21.3 **Waiver**

Any failure to exercise or any delay in exercising a right or remedy provided by this Agreement or at law will not constitute a waiver of the right or remedy or a waiver of any other rights or remedies. A waiver of a breach of any of the terms of this Agreement will not constitute a waiver of a subsequent breach of that term nor of any other breach and will not affect the other terms of this Agreement.

21.4 **Rights of Third Parties**

Except as provided in this Agreement, a person who is not a party to this Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement but this does not affect any right or remedy of a third party which exists or is available apart from that Act.

21.5 **Severability**

If at any time a provision of this Agreement is held by any court or administrative body of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability will not prejudice the remaining provisions of this Agreement which will remain in full force and effect. If any provision of this Agreement is so found to be invalid or unenforceable but would be valid or enforceable if some part of the provision were deleted, the provision in question will apply with such modification as may be necessary to make it valid.

21.6 **Entire Agreement**

21.6.1 This Agreement (together with the Terms of Business, where relevant) sets out the entire agreement and understanding between the Parties in connection with the provision of the Services, and supersedes all previous agreements, negotiations, representations and undertakings between the Parties relating to the provision of the Services.

21.6.2 Each of the Parties acknowledges and agrees that in entering into this Agreement, it does not rely on, and will have no remedy under, this Agreement in respect of, any statement, representation, warranty or understanding (whether negligently or innocently made) of any person (whether party to this Agreement or not) other than as expressly set out in this Agreement as a warranty. The only remedy available to it under this Agreement for breach of the warranties will be for breach of contract under the terms of this Agreement.

21.6.3 Nothing in this Clause 21.6 will be construed as excluding or intending to exclude the liability of either Party for fraudulent misrepresentation.

21.7 **Notices**

21.7.1 All notices to be given under this Agreement will be in writing and may be given personally or by special delivery post (subject to Clause 20.2). Notices given personally or by post will be delivered to the address of the Party as specified in this Agreement or as may be notified to the other Party from time to time in writing.

21.7.2 Any notice will be deemed to have been received: if delivered personally, at the time of delivery; and if sent by special delivery post, on the expiry of forty-eight (48) hours after posting.

22. LAW AND JURISDICTION

22.1.1 This Agreement is entered into in consideration of the mutual obligations assumed by the Parties under the terms of this Agreement.

22.1.2 This Agreement and any non-contractual obligations arising out of, or in connection with, this Agreement will be governed by, and be construed in all respects in accordance with, English law.

22.1.3 Each of the Parties hereby submits to the non-exclusive jurisdiction of the English courts in relation to all disputes including disputes arising out of, or in connection with, (a) the creation, validity, effect, interpretation, performance or non-performance of, or the legal relationships established by, this Agreement and (b) any non-contractual obligations arising out of, or in connection with, this Agreement.

SCHEDULE 1

DEFINITIONS AND INTERPRETATION

1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement the following words and expressions will have the following meanings unless the context otherwise requires:

"Agreement" has the meaning given in Clause 1;

"Appointed Representative" means a party appointed to act as an agent of an Authorised Firm in the conduct of investment business, in terms of the FSMA, from time to time;

"Approved TPSP" means a third-party service provider from time to time with whom the Provider has entered into an Approved TPSP Provider Agreement, (as such parties are detailed in the Technical Schedule and as may be amended from time to time or otherwise notified by the Provider to the Intermediary);

"Approved TPSP Intermediary Agreement" has the meaning given in Clause 3.1;

"Approved TPSP Provider Agreement" means an agreement between the Provider and an Approved TPSP for the provision of on-line authentication and other services substantially in the form of the Origo Legal Framework v4.0 Provider – Third Party Service Provider Services Agreement;

"Approved TPSP Services" means the Approved TPSP Provider Services and / or the Approved TPSP Intermediary Services, as the case may be;

"Approved TPSP System" means the system and processes operated by an Approved TPSP, including any software and materials owned by, or licensed to, that Approved TPSP which are used by the Approved TPSP to deliver the Approved TPSP Services;

"Audit Trail" means a full and unaltered transactional record of all Messages sent and received by the Parties, and all associated Data;

"Authentication" means:

(a) confirming the identity of the Party in question (or of any Approved TPSP) in accordance with the Standards; and

(b) in the case of an Approved TPSP, confirming that:

(i) the Provider has not terminated or suspended the Approved TPSP Provider Agreement; and

(ii) the Intermediary:

(A) is an Approved Intermediary in relation to that Approved TPSP; and

(B) has not terminated or suspended the Approved TPSP Intermediary Agreement, and "**Authenticate**", "**Authenticated**" or "**Authenticating**" will be construed accordingly;

"Authorised Firm" means a firm, partnership or company which is authorised under the FSMA to carry on investment business and has appointed the Intermediary as its Appointed Representative, and which is either:

(a) the party identified as such in the Technical Schedule; or

(b) each party subsequent to that referred to at (a), where the Intermediary has notified the Provider in accordance with Clause 12.3 and the Provider has chosen not to exercise its right to terminate this Agreement under Clause 16.4;

"Commencement Date" means the date of this Agreement;

"Customer" means an individual, organisation or company, (including an employee of, or individual associated with, such organisation or company) who has appointed the Intermediary as its agent;

"Customer Personal Data" means Personal Data relating to a Customer which is Processed by, or on behalf of, either Party;

"Data" means all information and data transmitted by one Party to the other Party (whether transmitted directly or via an Approved TPSP) or to or from an Approved TPSP, including statistics, policy information and valuations, Personal Data (including Customer Personal Data), information about products and services, commercial information, and whether as images, text or otherwise;

"Data Protection Laws" means the Data Protection Act 1998 or any successor or replacement thereto, and any applicable European Union or Member State law relating to data protection or the privacy of individuals including Regulation (EU) 2016/679 of the European Parliament and the Council (the General Data Protection Regulation);

"Defect" means any and all material errors, omissions or failures in the system of either Party (or, where applicable, in an Approved TPSP System), including errors, omissions or failures by reason of which such a system fails to perform in accordance with the relevant part of the Standards;

"Direct Services" means the services to be provided directly by the Provider to the Intermediary under this Agreement as further detailed in the Technical Schedule;

"Error" means a corruption of the Data contained within a Message, or a failure or omission within the content of the Message or in the structure of the Message;

"Force Majeure" means any event outside the reasonable control of either Party affecting its liability to perform any of its obligations (other than payment) under this Agreement, including Act of God, fire, flood, lightning, war, revolution, act of terrorism, strikes, lock-outs or other industrial action, whether of the affected Party's own employees or others;

"FCA" means the Financial Conduct Authority or any replacement or successor body;

"FSMA" means the Financial Services and Markets Act 2000, and any amending or replacement legislation and all subordinate laws and regulations and Rules which regulate the carrying on of investment or financial business in the United Kingdom;

"Group Company" in relation to any Party means that Party, any subsidiary undertaking, any parent undertaking, and any subsidiary undertaking of that parent undertaking, in each case as the terms "subsidiary undertaking" and "parent undertaking" are defined in Section 1162 of the Companies Act 2006 (except for the purposes of the membership requirement under Sections 1162(2)(b) and 1162(2)(d), an undertaking will be treated as a member of another undertaking

even if its shares in that undertaking are registered (a) in the name of its nominees or (b) in the name of a person (or the nominees of that person) who is holding the shares as security);

"Intellectual Property Rights" means any rights in or to intellectual property including copyright (including rights in computer software and related rights), patents, database rights, designs, trademarks, know-how or confidential information and any other rights in respect of any other industrial or intellectual property, whether registrable or not and wherever existing in the world and including all rights to apply for any of the foregoing rights;

"Intermediary Services" means the services to be provided by an Approved TPSP to the Intermediary in respect of the Provider under the relevant Approved TPSP Intermediary Agreement;

"Intermediary Standards" means the Intermediary's respective part of the Standards;

"Intermediary System" means the system by which the Intermediary connects to, or accesses, the Services;

"Loss" means all or any damages, claims, penalties, fines, costs, liabilities, obligations, encumbrances, losses, reasonable expenses, fees and any interest, charges and / or penalties, including, court costs, reasonable legal fees, disbursements and expenses (in each case to the extent permitted by applicable laws);

"Message" means a transmission of data ultimately between the Provider and the Intermediary, which will be transmitted via an Approved TPSP (and may be transmitted via more than one Approved TPSP) and which could be any of:

(a) a request for data made by the Intermediary; or

(b) a response by the Provider to a request made by the Intermediary; or

(c) a response automatically generated and sent by the Provider at a time determined by the Provider or agreed between the Provider and the Intermediary; or

(d) an electronic message generated by an Approved TPSP on the instructions of the Intermediary and / or the Provider, in each case, where such transmission is made in accordance with the Standards;

"Party or Parties" means a party or the parties to this Agreement;

"Personal Data" will have the meaning set out in the Data Protection Laws;

"PRA" means the Prudential Regulation Authority or any replacement or successor body;

"Processing" has the meaning set out in the Data Protection Laws, and "**Process**" and "**Processed**", when used in relation to Processing of Data, will be construed accordingly;

"Provider Standards" means the Provider's respective part of the Standards defined in the Technical Schedule;

"Provider System" means the system and processes operated by the Provider, including any software and materials owned by or licensed to the Provider which are used by the Provider to deliver the Direct Services;

"Regulator" means any governmental body or regulatory or supervisory authority having responsibility for the regulation or supervision of all or any part of the business of a Party,

including the Information Commissioner's Office (the 'ICO'), the FCA and the PRA (and in each case including any successor or replacement body from time to time);

"Revocation System" means the system, as set out in the Technical Schedule, in accordance with which either:

(a) the Intermediary; or

(b) an Approved TPSP; or

(c) both the Intermediary and the Approved TPSP (as appropriate),

will manage (or in the case of (c), will both be responsible for managing) the revocation and suspension of the access rights of any User to the Direct Services and/or the Intermediary Services;

"Rules" means the Handbooks of Rules and Guidance of the FCA and the PRA, in each case as amended and/or supplemented from time to time;

"Security Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data transmitted, stored or otherwise Processed;

"Security Standards" means the agreed technical security standards, as specified in the Technical Schedule;

"Services" means the Direct Services and / or the Intermediary Services, as the case may be;

"Services Standards" means any agreed standards, as may be set out in the Technical Schedule in accordance with which the Provider will provide the Direct Services;

"Site" means any web site of the Provider through which the Intermediary can access and use the Direct Services;

"Standards" means the System Standards, the Security Standards and the Services Standards;

"System Standards" means the technical system and standards for sending and receiving Messages or accessing, inputting, submitting and displaying Data, as specified in Technical Schedule;

"Technical Schedule" means Schedule 2;

"Terms of Business" means the Provider's terms of business and any other relevant documents upon which the Provider will undertake business from the Intermediary or, if the Intermediary is an Appointed Representative, from the Authorised Firm;

"User" means any individual user who is entitled to access and uses the Services at any time using the User Access, and who may be (a) any individual user of the Intermediary, including a Customer, an employee, agent, consultant or sub-contractor, or (b) an Appointed Representative or any individual user, including a Customer, employee, agent, consultant or sub-contractor, of the Appointed Representative;

"User Access" means the method or process, as specified as part of the Standards, by which a User will access and use the Direct Services and / or the Intermediary Services;

"User Guidelines" means any guidelines in accordance with which a User must use the Direct Services or the Intermediary Services, as may be prescribed in the Technical Schedule;

"Variation Notice Period" has the meaning given in Clause 20.1; and

"Working Day" means any day excluding Saturday and Sunday and public holidays in England;

1.2 Any reference to a Clause is to the relevant clause of this Agreement, unless otherwise stated.

1.3 Headings are used for convenience only and will not affect the construction or interpretation of this Agreement.

1.4 Words importing the singular will include the plural and vice versa. Words importing a gender include every gender and references to persons include an individual, company, corporation, firm or partnership.

1.5 References to any statute, enactment, order, regulation or other similar instrument will be construed as a reference to it as from time to time amended, consolidated or re-enacted and includes all instruments or other subordinate legislation orders made under it.

1.6 The words "**including**" and "**includes**" will be construed as being by way of illustration or emphasis only and will not be construed as, nor will they take effect as, limiting the generality of any preceding words.

SCHEDULE 2

TECHNICAL SCHEDULE

1. INTRODUCTION

This Schedule sets out:-

1.1. those commercial provisions which these Terms expressly provide may be set out in this Technical Schedule;

1.2. the technical standards that must be used for sending and receiving Messages, including the minimum system requirements of each Party (the System Standards);

1.3. the technical security measures that must be applied in relation to the creation of Messages and the transmission of Messages between the Parties, (whether directly or through one or more Approved TPSPs), and the method of Authentication (the Security Standards); and

1.4. if applicable, the Direct Services and the standards in accordance with which you will provide the Direct Services (the Services Standards).

1.5 The Information Security, Physical Security Management and Business Continuity Management schedule in Appendix A to this Schedule which the TPSP shall comply with.

2. DEFINITIONS AND INTERPRETATION

2.1. In this Technical Schedule:

2.1.1. “our”, “us” and “we” refers to Aviva; and

2.1.2. “you” and “your” refers to the Intermediary.

3. SERVICES

3.1. Details of the Services supported by these Terms, hours of availability, the products supported, and the third party service providers who are an "Approved TPSP" for the purposes of these Terms can be found on our extranet at www.avivaforadvisers.co.uk or such other address as we may notify you of from time to time (“Extranet”).

4. SYSTEM STANDARDS

4.1. Provider Standards

4.1.1. In relation to the Direct Services the Provider System has the capability to receive your requests.

4.1.2. In relation to the Intermediary Services, the Provider System has the capability to receive your requests from an Approved TPSP on your behalf.

4.1.3. In addition, the Provider System has the capability to:

- validate, assess and process these requests
- enquire on Aviva’s databases
- collate and send electronic responses
- create and send both technical level acknowledgements, and business level error responses, where appropriate

4.2. Intermediary Standards

4.2.1. The Intermediary System must:

- validate, assess and process Intermediary instructions
- collate and forward requests to us
- receive both technical level acknowledgements, and business level error responses, where appropriate
- collate and store information received
- only use back office or Approved TPSPs supported by us. For an up to date list of this software, please visit our Extranet www.avivaforadvisers.co.uk If your back office software is changed or updated in any manner that affects the Direct Services or the Intermediary Services, you must notify us immediately so that we may assess whether or not additional testing or quality assurance of the updated software is required.

5. SECURITY STANDARDS

5.1. Registration

We may require you to register with us. In the event that we require you to do this, we will inform you of this.

5.2. Identification

5.2.1. We will identify you using an Online Account Number (OAN) and password which may be associated with a Unipass Certificate in connection with Direct Services.

5.2.2. The Approved TPSP will identify you to Aviva and we will identify you from the data contained in the request in connection with Intermediary Services.

5.3. Authentication

For each Message exchange, each party must be identified and Authenticated. The mechanism for doing this is as follows:-

5.3.1. Direct Services:

- The electronic communication between Aviva and you must be authenticated in both directions.
- You will be authenticated using an Online Account Number (OAN) and password which may be associated with a Unipass certificate.
- An audit log should be maintained by both parties. The audit log should contain details of all requests and their corresponding responses.

5.3.2. Intermediary Services:

- The responsibility for authentication of the Intermediary lies with the Approved TPSP.
- The Approved TPSP will be authenticated by Aviva using the Approved TPSP's digital certificate, which will have been previously registered with Aviva.

5.4. Revocation System

5.4.1. Direct Services:

Aviva will perform a revocation check if your Unipass certificate. The Unipass Certificate will be revocation checked in line with the following guidelines:

- You must revoke an individual's Unipass certificate as soon as that individual ceases to be authorised by you to use the services.

- We will check your Unipass certificate using the Unipass Certificate Revocation Status Service against the OSIS list of revoked Unipass certificates. If your Unipass certificate is listed on this Service, access will be denied.

- Where we receive confirmation that a revocation check has failed, we will return an error response to you.

5.4.2. Intermediary Services

- We will not perform a revocation check on you as the responsibility for this rests with the Approved TPSP.

- We will perform a revocation check of the Approved TPSP's digital certificate at least once per day.

- We will return an error response to the Approved TPSP if they fail this check.

5.5. Authorisation

5.5.1. We may employ different mechanisms to control access to different systems/data, depending upon the processes involved.

5.5.2. You must have authority to deal with Aviva and vice-versa. There must be an existing business relationship between the two, otherwise no data will be released.

5.5.3. We will check that you have authority to access the Data requested by the following procedure:

- We will check using our own policy and agency records that you identified using the data contained in the request has access to the Data or Services requested.

5.5.4. In addition, if you are accessing Data via an Approved TPSP we will also check that:

- The Approved TPSP must have authority to deal with Aviva and vice-versa. There must be an existing business relationship between the two, otherwise no data will be released.

- The Approved TPSP must have authority to request data on your behalf.

- The Approved TPSP will check that you have has authority to access the policy data requested.

5.6. Data Integrity (Direct Services only)

5.6.1. You and Aviva must ensure that data in a message has not suffered from accidental or malicious tampering.

5.6.2. There should be a mechanism by which tampering can prove to have occurred, both during transmission and after receipt, should messages be stored for any reason.

5.6.3. Aviva will assure the integrity of data transmission by only servicing messages over HTTP/SSL with 128-bit encryption. Connections over standard HTTP protocol will be denied.

5.7. Non-Repudiation

5.7.1. Each party should maintain a mechanism to provide verifiable proof that the content of a message could only have been created and sent by one specific party.

5.7.2. Aviva will maintain an audit trail of messages sent and received. The integrity of the audit trail must be proven. In particular, the audit trail must be secure from tampering.

5.7.3. We will maintain an audit log of each Intermediary authenticated on each occasion.

5.8. Security Breaches

5.8.1. Aviva must be informed immediately when a breach of security is discovered. This breach should be reported via our Helpdesk see 6.2.1). You must take immediate action to suspend your use of the Direct Services and/or Intermediary Services until the security breach has been resolved including informing any Approved TPSP supporting the service.

6. THE SERVICES STANDARDS (DIRECT SERVICES ONLY)

6.1. Change Management

6.1.1. We reserve the right to change the Direct Services at any time.

6.2. Contacts

6.2.1. Our Helpdesk number is 0845 3093999

6.3. Message Volume

6.3.1. To protect the integrity and security of our Services, we reserve the right to monitor the volume of messages transacted with Intermediaries, and to investigate abnormal patterns.

7. USER ACCESS

7.1. We will allow access to our data via our supported software providers. For an up to date list of the software providers we support please visit our Extranet www.avivaforadvisers.co.uk.

7.2. You must ensure that the security of the Approved TPSP or back-office software that you use to access the Intermediary or Direct Services is appropriate.

7.3. The Approved TPSP can generate requests on your behalf as long as this has been contractually agreed between you and the Approved TPSP. This includes the situation where the Approved TPSP is providing a service to your clients on your behalf.

Aviva Life Services Limited. Registered in England (Company No.02403746) and having its registered office at Wellington Row York, North Yorkshire, YO901WR

Appendix A
Information Security, Physical Security Management and Business Continuity Management

GENERAL

The Aviva Group recognises that the confidentiality, integrity and availability of information are fundamental components of its business. The Aviva Group Company is committed to the protection of its information assets and expects the same level of commitment from its TPSPs.

Aviva's decision will be final when any question regarding the interpretation of its security policies and standards is raised and also on what constitutes an acceptable level of security compliance.

Any breach of this Schedule by the TPSP shall entitle Aviva to terminate this Agreement immediately on written notice to the TPSP.

PART A
Security and Access Requirements

The following definitions shall apply to this Appendix A - Information Security, Physical Security Management and Business Continuity Management only:-

Definitions

Aviva Systems means the systems of Provider (or those of any Provider Group Company).

Change Control means the process howsoever described in this Agreement for making changes to this Agreement.

Good Industry Practice means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.

Information Security Controls means controls to protect the confidentiality, integrity or availability of data.

Public Cloud Services means any data hosting, processing or storage service which is provided to the TPSP by a third party, where the service is provided on infrastructure owned and located at the third party's premises, and the service is made available over the internet using infrastructure shared amongst customers.

SMEs means subject matter experts.

TPSP Company means a member of the group of companies of which the TPSP is a member from time to time.

TPSP Personnel means any employee, officer, agent or other person whatsoever acting for the TPSP or otherwise under the control and direction of the TPSP (or of a TPSP Company) or of any of the TPSP's (or, as the case may be, of a TPSP Company's) sub-contractors.

TPSP's Key Information Security Contact means the TPSP contact with responsibility for security of the Services.

1. INFORMATION SECURITY REQUIREMENTS

The TPSP shall maintain and implement appropriate security systems, controls, policies and procedures that are at least as effective at minimising the risk of an information security breach as required by Good Industry Practice.

The TPSP will appoint an appropriate individual to act as the TPSP's Key Information Security Contact who will: (i) have authority to approve any technical or procedural changes required to maintain the security of the Services or have access to appropriate escalation routes within the TPSP's organisation to obtain prompt approval; and (ii) ensure that a direct on-site or remote assessment by Aviva information security SMEs under Aviva's general rights of audit in this Agreement is facilitated.

The output of any direct on-site or remote assessment by Aviva must enable Aviva to compare the adequacy of the TPSP's Information Security Controls against the standards of security required in the Agreement.

Where the TPSP's Information Security Controls (as assessed either by Aviva or by an independent audit) are

deemed to be inadequate: (i) Aviva and the TPSP shall agree on a remedial plan and a timetable for achievement of improvements; and (ii) the TPSP will allow Aviva to conduct a further assessment.

2. INCIDENT MANAGEMENT

The TPSP will ensure that the TPSP's Key Information Security Contact is the first point of contact for Aviva for all information security related questions, issues and incidents.

The TPSP will implement a process for the management and reporting of security related incidents or suspected security incidents which includes: (i) communication to all persons accessing the Services in order to promote prompt reporting and control of any suspected, attempted or actual security breaches; and (ii) notification to Aviva with details of the incident and its potential impact. The TPSP will promptly make Aviva aware of the remediation being instigated by the TPSP in order to resolve the incident to all parties' satisfaction.

3. INFORMATION ASSET MANAGEMENT

The TPSP shall implement and maintain a register of all Aviva information assets stored or otherwise managed by it. The register will: (i) include a TPSP owner for each information store, together with a meaningful description of both the information and the information store (including its location and the location of any backup copies of the data); and (ii) be updated whenever there are changes to either the data stored or the storage location.

4. CHANGE REQUIREMENTS

Aviva recognises that Information Security Controls will periodically be subject to change as a result of developments in, by way of example only, external threats to information security, technologies, regulation, international security standards and Aviva Group policies. Aviva therefore reserves the right to amend this Schedule to ensure it remains suitable for the purpose of protecting Aviva, the Aviva Companies and their respective customers. Any such change will be subject to Change Control.

5. ACCESS MANAGEMENT

The TPSP shall maintain and implement appropriate security systems, controls, policies and procedures to ensure the secure use of (and protected access to) all applications, databases and devices used to service the Aviva Companies' businesses.

The TPSP shall ensure that access is: (i) only granted to those TPSP Personnel who reasonably need it for the purposes of delivering the Services; and (ii) restricted in accordance with the role or function of the individual. The TPSP shall also ensure that adequate procedures are in place so that TPSP Personnel access is: (i) added, modified and deleted in a timely manner; and (ii) routinely reviewed for recertification and revalidation purposes.

6. REMOTE ACCESS SECURITY

The TPSP shall ensure that controls are in place to prevent unauthorised remote access, including (but not limited to): (i) using strong authentication (e.g. two-factor authentication) to authenticate the TPSP's users; (ii) encryption from the end-point (e.g. laptop) to the network for all data travelling across a remote access mechanism; and (iii) logging of all remote access attempts and reviewing of any suspicious activity.

7. PORTABLE STORAGE DEVICE SECURITY

The TPSP shall not store Aviva Data on unencrypted portable storage devices (such as external hard drives, USB sticks, laptops or portable backup media) unless explicit approval is provided by Aviva in writing. Where portable devices do hold Aviva Data, the TPSP shall ensure that: (i) they are locked securely away when not in use; (ii) use in public areas is avoided; (iii) the data stored within the device is no more than the minimum required; and (iv) all devices are adequately encrypted and password protected.

8. DATA TRANSFER SECURITY

The TPSP shall ensure that all Aviva Data sent over the internet either by e-mail or via other internet protocols (e.g. FTP) is: (i) encrypted using at least a 128 bit encryption mechanism; and (ii) only transferred via pre-configured communications with electronic acknowledgement. The TPSP shall also ensure that no unapproved transfer technologies are used to communicate Aviva Data.

9. **DOCUMENT STORAGE SECURITY**

The TPSP shall ensure that all information is: (i) secured under lock and key if left unattended by TPSP Personnel; and (ii) accessible only to those TPSP Personnel allowed to have access.

10. **DATA DISPOSAL**

The TPSP shall ensure that any hardcopy Aviva Data is shredded (using a cross-cut shredder or incineration) and securely disposed of via an internal disposal mechanism or by using a third party.

For IT assets, the TPSP must ensure that any IT assets and electronic media that are being used to store Aviva Data but which are no longer required are destroyed by incineration, damaged beyond repair or that the Aviva Data is erased using data erasure technology such that Aviva Data is erased and is not recoverable (and certify to Aviva in writing that the foregoing has been done).

11. **PASSWORD MANAGEMENT**

The TPSP will ensure that:

(i) in respect of any passwords used for access to its systems, standard password configuration includes (without limitation): minimum length, complexity, expiry, history, and account lockout following consecutive failed logon attempts;

(ii) the above configuration is implemented at system level and documented within a password management strategy or policy document;

(iii) all non-personal IDs are documented (including the purpose of the access);

(iv) all staff are provided with a level of access that is limited to only what is required to perform their roles, and that this access is regularly reviewed to ensure that each member of staff's access level is accurate;

all staff are made aware of the importance of keeping their passwords confidential.

12. **NETWORK SECURITY**

The TPSP shall agree to conducting (or engaging a third party to perform) annual penetration testing on all externally-facing services. Where Aviva is an affected party: (i) the results of such testing will be made available to Aviva for scrutiny; and (ii) all reasonable steps for remediation shall be undertaken and demonstrated for audit purposes.

The TPSP shall perform regular anti-virus and perimeter scanning activities on its IT estate which include firewall and email scanning services. The results of such scanning shall be provided to Aviva upon request with clear evidence of vulnerability remediation being undertaken.

The TPSP shall perform regular patch management activity which includes the execution of a patch management implementation schedule and follows a standard patch methodology of phased testing and deployment activity.

13. CONTRACT EXPIRY

Without prejudice to any other provisions of the Agreement regarding the consequences of termination and/or exit (and in addition to those provisions), upon the expiry or termination of the Agreement, the TPSP shall:

13.1 assist Aviva in:

13.1.1 performing a termination review of any remaining information security risks;

13.1.2 the return, transfer and/or destruction of all Aviva Data from all sources, networks and devices used by:

(a) the TPSP; or
(b) any TPSP Company; or
(c) any of the TPSP's (or, as the case may be, of a TPSP Company's) sub-contractors

in the provision of the Services; and

13.2 ensure that all:

13.2.1 physical or logical assets, intellectual property and licences are returned;

13.2.2 physical and logical system access to Aviva Data or Aviva Systems is revoked; and

within timescales agreed with Aviva.

14. PUBLIC CLOUD SERVICES

The TPSP will:

14.1 not store, host, or process any Aviva Data or Confidential information in any Public Cloud Service without the prior written consent of Aviva;

14.2 (subject to paragraph 14.1) provide adequate assurance of the Public Cloud Services provider's security controls by allowing Aviva access to any or all of the following:

14.2.1 documentation relating to the TPSP's due diligence activity in respect of the Public Cloud Services provider;

14.2.2 ISAE 3000, ISAE 3402, SSAE16 or any similar independent SOC II audit of the Public Cloud Services provider;

14.2.3 where applicable, details of the scope and certification status of ISO/IEC 27001:2013;

14.3 where requested by Aviva) ensure that access to any Public Cloud Services which are used for the purposes of Aviva Group business are configured to accept requests only from Aviva Group networks;

14.4 (where requested by Aviva) provide Aviva with the functionality of federated accounts to provide Authorised Users with single sign-on access to any Public Cloud Services.

PART B
Physical Security Management

Definitions:

Aviva Assets means Aviva personnel, Aviva Data or Relevant Infrastructure.

Aviva Data has the meaning given in Part A of this Schedule.

Aviva Infrastructure means the infrastructure of Aviva or any Aviva Company to which the TPSP or a TPSP Company or any of the TPSP's (or, as the case may be, a TPSP Company's) sub-contractors has access in the course of the provision of the Services.

Delay means adequate physical barriers and resistance to attack time, and "to Delay" shall be construed accordingly.

Denial means a comprehensive series of integrated barriers supported by security systems to provide an enhanced resistance to attack time, to deny success to an opportunist, and "to Deny" shall be construed accordingly.

Detection means a comprehensive, monitored and consistent application of electronic intruder detection systems supported by CCTV, and "to Detect" shall be construed accordingly.

Deterrence means a delineated perimeter which utilises (inter alia) physical barriers, signage, overt electronic security systems, and "to Deter" shall be construed accordingly.

Physical Security Controls means controls to prevent unauthorised physical access to TPSP or TPSP Company premises.

Physical Security Incident means any event where there is, or potentially could be, unauthorised access to, or use of, or interface with Aviva Assets under the TPSP's or a TPSP Company's or any of the TPSP's (or, as the case may be, a TPSP Company's) sub-contractors' control.

Physical Security Management (or **PSM**) means a structured discipline to ensure the physical security of assets. The Aviva Group's PSM methodology is the development of a protective security profile to Deter, Detect, Delay and Deny any unauthorised intrusion or event and to generate the appropriate response.

Relevant Infrastructure means:

(a) Aviva Infrastructure; and
(b) TPSP Infrastructure.

TPSP Company has the meaning given in Part A of this Schedule.

TPSP Infrastructure means the infrastructure used in the course of the provision of the Services whether the infrastructure of the TPSP or a TPSP Company or any of the TPSP's (or, as the case may be, a TPSP Company's) sub-contractors.

1. The TPSP shall be responsible for all aspects of the security of the provision of the Services and any Aviva Assets whilst they are in the TPSP's or a TPSP Company's or any of the TPSP's (or, as the case may be, a TPSP Company's) sub-contractors' possession, custody or control and shall take action (or procure that action is taken) to safeguard them.

2. The TPSP shall ensure that appropriate Physical Security Controls are put in place at its premises and any other premises from which the Services are supplied or any location at which Aviva Assets are located.

3. The TPSP shall ensure that its Physical Security Controls are aligned with the physical security requirements in international standard ISO/IEC27001:2013 as a minimum.

4. The TPSP will appoint an appropriate person to act as a Physical Security Management contact.

5. The TPSP will implement a standard process for Physical Security Management and the reporting of physical security related incidents.

6. The TPSP shall promptly upon identification, inform Aviva of any Physical Security Incident which could cause an exploitable vulnerability to the physical security profile of Aviva or any other Aviva Company.

7. The TPSP will provide Aviva with such assistance and co-operation as Aviva may reasonably request in relation to the conduct of any investigation into any Physical Security Incidents.

8. Aviva reserves the right to undertake a Physical Security Management review of the TPSP's premises, physical security processes and procedures which relate to the Services. The TPSP shall work with Aviva to address any issues that arise from any such review(s).

PART C

1.1 Business Continuity Management

Definitions:
Business as Usual (or **BAU**) means standard functional operations within an organisation.

Business Continuity Incident means any event as a result of which the Business Continuity Plan is invoked.

Business Continuity Management (or **BCM**) means a structured discipline to ensure the continuance of the provision of the Services to Aviva in the event of a Business Continuity Incident (including Pandemic Planning) including (but not limited to) a proactive process to identify key operations and the recovery requirements thereof from which plans and procedures may be developed to ensure the continuity of those operations, whatever circumstances are encountered, in order to achieve the uninterrupted availability of the Services and not just the recovery from or resumption of business after a Business Continuity Incident.

Business Continuity Plan means the business continuity plan produced by the TPSP invoked upon the occurrence of a Business Continuity Incident.

Incident Management (or **IM**) means the process for managing the lifecycle of any Major Incident.

IT Service Continuity Management (or **ITSCM)** means the lifecycle responsible for managing risks that could seriously impact IT services by ensuring that continuity and recovery plans have been developed in alignment with business continuity plans and business requirements.

Major Incident means an event (natural or otherwise) that poses a serious risk to the continuation of BAU operations within an organisation that requires the implementation of specific arrangements, beyond the routine, to minimise the disruption to service.

Pandemic Planning means a specifically tailored and documented response to deal with any major epidemic or pandemic outbreak.

Recovery Point Objective means the point in time to which work needs to be restored following a Business Continuity Incident.

Recovery Time Objective means the time objective for restoration of Business as Usual in the event of Business Continuity Incident.

1.2 **Revised Operating Level means the minimum level of continued output required of the TPSP to meet its obligations to Aviva.**

TPSP Personnel has the meaning given in Part A of this Schedule.

1. The TPSP shall have documented Business Continuity Management, IT Service Continuity Management and Incident Management processes for the production of appropriate BCM, ITSCM and IM plans enabling it to restore the Services to Business as Usual as per the agreed Recovery Time Objective, Revised Operating Level and Recovery Point Objective (including the meeting of any service levels) in the event of a Major Incident.

2. The TPSP's BCM, ITSCM and IM plans should be reviewed and approved by the TPSP's senior management and Aviva at least annually.

3. The TPSP's BCM, ITSCM and IM processes should reflect all relevant regulations and guidance issued by the regulatory authority and shall be provided to a standard no lower than ISO22301 and whatever standards shall supersede them.

4. The TPSP's BCM, ITSCM and IM plans should be tested at least annually and the results made available to Aviva.

5. The TPSP shall inform Aviva of the date of any planned testing. Dates should be supplied at least 30 days in advance.

6. Any actions raised within testing should be completed within a time period agreed with Aviva.

7. Procedures must exist to ensure that TPSP Personnel are trained in the provision of the Services, understand the BCM processes and, in particular, the conditions under which they are required to invoke and execute the BCM, ITSCM and IM plans. Proper escalation to senior managers must be incorporated and designed to promote active communication, even on issues of relatively minor concern.

8. In the event of a Major Incident, the TPSP shall give full consideration to any input provided by Aviva. The TPSP shall if necessary adjust its BCM, ITSCM and IM plans and processes to take account of Aviva's reasonable requests to ensure, in the event of a Major Incident, that provision of the Services is resumed as soon as reasonably practicable.

9. Aviva reserves the right to undertake annual audits of the TPSP's BCM, ITSCM and IM plans and processes, which relate to the Services. The TPSP shall work with Aviva to address any issues that arise from such audits.

10. The TPSP shall notify Aviva of any invocation of the BCM, ITSCM and IM plans prior to such invocation.

11. Following invocation of a BCM, ITSCM or IM plan or process, the TPSP shall advise Aviva of the expected duration of such invocation.