Dated 2 March 2022

INTESA SANPAOLO SPA

and

KAIZEN REPORTING LIMITED

MASTER SERVICES AGREEMENT

THIS MASTER SERVICES AGREEMENT is made on the 2 March 2022

BETWEEN:

(1) **INTESA SANPAOLO SPA**, a company registered in Italy with registration number 00799960158 and LEI Code 2W8N8UU78PMDQKZENC08 and whose registered office is situated at Piazza San Carlo 156, 10121, Torino (the "**Client**"); and

(2) **KAIZEN REPORTING LIMITED**, a company registered in England and Wales with registration number 08362415 and LEI Code 254900RYLWYAV1Y93K81 and whose registered office is situated at 12 Groveland Court, London EC4M 9EH (the "**Supplier**"),

each a **"party"** to this Agreement and together the "**parties**".

WHEREAS:

A. The Supplier provides testing services in respect of regulatory reporting.

B. The Client wishes to receive from the Supplier and the Supplier has agreed to provide to the Client certain testing services in respect of regulatory reporting as described in the applicable Statement of Work subject to the Terms of this Master Services Agreement.

IT IS HEREBY AGREED as follows:

1. Definitions and Interpretation

1.1. The definitions and rules of interpretation in this clause apply in these Terms.

Definition	Description
Additional Consultancy Services	the additional consultancy services as agreed by the parties.
Additional Terms	the terms and conditions (if any) set out in Exhibit A.
Affiliate	any entity controlled, directly or indirectly by the Client, any entity that controls, directly or indirectly, the Client, or any entity directly or indirectly under common control with the Client. For the purposes of this definition "control" shall be as defined in section 1124 of the Corporation Tax Act 2010.
Authorised Users	those employees of the Client who are authorised by the Client to use the Services and the Documentation.
Business Day	any day which is not a Saturday, Sunday or public holiday in the UK.

Client Data	the data provided by the Client to the Supplier for the purpose of performing the Services.
Confidential Information	all information in respect of a party (or in respect of the Client's or its Affiliates' customers) including, without prejudice to the generality of the foregoing, any ideas; business methods; finance; prices; business, financial, marketing, development or manpower plans; customer lists or details; computer systems or software; products or services and information concerning a party's relationship with clients or potential clients, including, in the case of the Client (or in respect of the Client's or its Affiliates' customers), Documentation and the Client Data identified as Confidential Information in clause 16.
Controller	has the meaning given in applicable Data Protection Legislation from time to time;
Data Protection Legislation	means all applicable statutes, laws and regulations pertaining to privacy and data protection, including the General Data Protection Regulation (Regulation (EU) 2016/679), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and the Data Protection Act 2018 as may be amended from time to time.
Data Protection Supervisory Authorities	means the Information Commissioner in the UK or other competent data privacy authority with jurisdiction over the Client and its Affiliates as specified in the Statement of Work, and any successor body.
Authorities	means any authority that, pursuant to current legislation, is empowered to conduct controls on behalf of the Client (included but not limited to Data Protection Supervisory Authorities, Regulator, the social security institutions, the tax authorities and the Resolution Authority.
Documentation	the documentation provided to the Client by the Supplier in relation to the provision of the Services including but not limited to the Project Results.
Data Subject	has the meaning given in applicable Data Protection Legislation from time to time.
Effective Date	the date of this Master Services Agreement.
Fees	the fees in respect of the Services as specified in each Statement of Work.
GDPR	means the General Data Protection Regulation (EU) 2016/679 and any successor regulation or legislation.
Helpdesk	the helpdesk made available by Supplier during Normal Business Hours.
Intellectual Property Rights	all patents, rights to inventions, copyright and related rights, trade marks, trade names and domain names, rights in goodwill or to sue for passing off, rights in designs, rights in computer software, database rights, rights in confidential information (including know-how and trade secrets) and any other intellectual property rights, in each case whether registered or unregistered and including all applications (and rights to apply) for, and renewals or extensions of, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist, now or in the future, in any part of the world.

Kaizen Wiki	the wiki service made available by Supplier.
Licence	the licence granted in clause 3.1.
Master Services Agreement or Agreement	the agreement comprising the Terms together with the Schedules, Exhibit A and the Statement(s) of Work.
Normal Business Hours	9.00 am to 17.00 pm GMT, each Business Day.
Personal Data	personal data as defined by the General Data Protection Regulation (Regulation (EU) 2016/679) as amended from time to time and any legislation or other regulations made thereunder.
Protected Data	means Personal Data received from or on behalf of the Client, or otherwise obtained in connection with the performance of the Supplier's obligations under this Agreement.
Project Results	all results, records, reports, documents, papers, drawings, designs, transparencies, photos, graphics, logos, typographical arrangements, software, computer programmes or codes, and all other materials in whatever form, including but not limited to hard copy and electronic form, prepared by the Supplier in the course of or for the purposes of provision of the Services.
Reference Charges	the Supplier's standard charges which are set out in Schedule 3.
Regulator	the Financial Conduct Authority in the UK or other competent authority or other financial regulator with jurisdiction over the Client and its Affiliates as specified in the Statement of Work.
Services	the services provided by the Supplier to the Client as more particularly described in Schedule 1. Such Services shall include any Additional Consultancy Services.
Service Period	the time period during which the Services will be delivered pursuant to the applicable Statement of Work.
Software	the proprietary software applications used by the Supplier to deliver the Services.
Statement of Work	an agreement between the parties made pursuant to clause 2, describing the Services to be provided by the Supplier, the timetable for their performance and the related matters listed in the template statement of work set out in Schedule 2.
Supplier Materials	Software and Documentation of the Supplier provided to the Client as part of the Statement of Work or otherwise used in the provision of the Services.
Term	the term of this Agreement as defined in clause 18.1.
Terms	these terms and conditions.

Transaction or Trade reports	records required to be submitted by the Client to the Regulator.
Virus	anything or any device (including any software, code, file or programme) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any programme or data, including the reliability of any programme or data (whether by re-arranging, altering or erasing the programme or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.

1.2. Save as otherwise expressly provided herein, reference to statutory provisions, regulations or notices shall include those provisions, regulations or notices as amended, extended, consolidated, substituted or re-enacted from time to time.

1.3. The headings (other than clause numbers) inserted herein are of no legal effect and are for convenience only and shall not affect the construction of this Agreement.

1.4. References to clauses and schedules are references to clauses of, and schedules to, this Agreement and references to sub-clauses are, unless otherwise stated, references to sub-clauses of the clause in which such reference appears.

1.5. References to the singular shall include the plural and vice versa and references to the masculine gender shall include all other genders and vice versa.

1.6. References to a 'person' shall include any individual, partnership (whether or not some or all of the members thereof or partners therein shall have limited liability), company, body corporate, corporation sole or aggregate, state or agency of a state and any unincorporated association or organisation, in each case whether or not having separate legal personality.

1.7. Words introduced by the word 'other' shall not be given a restrictive meaning because they are preceded by words referring to particular classes of acts, matters or things.

1.8. General words shall not be given a restrictive meaning because they are followed by words which are particular examples of the acts, matters or things covered by the general words and the word 'including' shall be construed without limitation.

2. Structure

2.1. This Master Services Agreement contains the Terms that apply to each Statement of Work for the provision of the Services by the Supplier to the Client.

2.2. The Client or an Affiliate may procure any of the Services by agreeing a Statement of Work with the Supplier.

2.3. Each Statement of Work shall be subject to the Terms contained in this Master Services Agreement. In the event that there is a conflict between a Statement of Work and the Master Services Agreement, the Statement of Work takes precedence.

2.4. In the event an Affiliate enters into a Statement of Work under this Agreement, such Affiliate shall be deemed to be the Client to whom the Supplier provides the Services under this Agreement mutatis mutandis.

2.5. In the event the Agreement is terminated pursuant to clause 18, any Statement of Work which has been agreed between the parties shall remain in force and effect until such Statement of Work terminates or expires.

3. Licence – Authorised Users

3.1. Subject to the Terms, the Supplier hereby grants to the Client a non-exclusive, non-transferable Licence to permit the Authorised Users to use the Kaizen Wiki and Helpdesk during the Term solely for the Client's and Client's Affiliates internal business operations.

3.2. The Supplier shall issue each Authorised User of the helpdesk service with an individual password or passwords as appropriate (and update the password upon expiry) up to the contracted maximum number of Authorised Users as specified in the Statement of Work or as otherwise agreed in writing.

3.3. In relation to the Authorised Users, the Client shall ensure that:

3.3.1. the Authorised Users keep their assigned passwords confidential and secure and are not used by any other person;

3.3.2. the Documentation is also kept secure and confidential and not shared with any person who is employed, retained or engaged in any capacity by an entity which provides regulatory reporting quality assurance or testing services , without the express written permission of the Supplier such consent not to be unreasonably withheld or delayed;

3.3.3. it shall maintain a written, up to date list of current Authorised Users and provide such list to the Supplier within 5 Business Days of the Supplier's written request at any time or times;

3.3.4. if any password has been provided to any individual who is not an Authorised User, then without prejudice to the Supplier's other rights, the Client shall promptly notify the Supplier in order to disable such passwords and the Supplier shall not issue any new passwords to any such individual.

3.4. The Client and the Supplier shall ensure that it does not access, store, distribute or transmit any Viruses, or any material during the course of its use of the Services that:

3.4.1. is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;

3.4.2. facilitates illegal activity;

3.4.3. depicts sexually explicit images;

3.4.4. would constitute a breach or infringement of the intellectual property rights of a third party;

3.4.5. promotes unlawful violence;

3.4.6. is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability, or any other illegal activity; or

3.4.7. causes damage or injury to any person or property;

and the Supplier reserves the right, without liability to the Client, subject to a prior written notification to the Client of such breach, to disable the Client's access to any specific material that breaches the provisions of this clause.

3.5. The Client shall not:

3.5.1. except to the extent expressly permitted under this Agreement, attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Software, quality control tests and/or Documentation (as applicable) in any form or media or by any means; or

3.5.2. use all or any part of the Services, the quality control tests or Documentation in order to build a product or service which competes with the Services and/or the Documentation; or

3.5.3. use the Services, quality control tests or Documentation to provide services to third parties, unless expressly permitted by the Supplier; or

3.5.4. make the Services available on a network not authorised by the Supplier; or

3.5.5. license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Services, the quality control tests or Documentation available to any third party except the Authorised Users; or attempt to obtain, or assist third parties in obtaining, access to the Services, the quality control tests or Documentation, other than as provided under this clause 3.

3.6. The Client and the Supplier shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Services, the quality control tests and/or the Documentation and, in the event of any such unauthorised access or use, immediately notify the other party.

4. Services

4.1. The Supplier shall, during the Term, provide the Services and make available the Supplier Materials to the Client on and subject to the terms of this Agreement.

4.2. The Services to be provided are set out in the Statement of Work.

4.2.1. The Supplier represents that:

(i) the Services are provided in the UK

(ii) the data centers are located in Ireland.

(iii) cloud computing activities are carried out by AWS for IaaS.

4.3. Where included as a Service under the Statement of Work, the control framework, testing and quality assurance service to be provided by the Supplier has been designed to provide a control environment which the Client will implement to assist it in maintaining and monitoring the overall accuracy, completeness and timeliness of its Transaction or Trade reports submitted to the Regulator. However, neither the testing nor the control framework are held out as guaranteeing or warranting the accuracy, completeness and timeliness of the Client's Transaction or Trade reports.

4.4. Save as expressly set out in a Statement of Work, the Services do not encompass investigation or management of the resolution of any of the issues identified by the provision of the Services by Supplier.

4.5. The Client shall be responsible for the evaluation of the findings and determining whether each finding or combination of findings are material and whether and when to notify the Regulator.

4.6. In order to ensure compliance with applicable regulatory rules and having given reasonable prior written notice to the other party, each party reserves the right to:

4.6.1. subject to clause 27, Vary (or ask to vary) the Services from time to time; and

4.6.2. subject to clause 27, make (or ask to make) changes or corrections, alter, suspend or discontinue any aspect of the Services including provision of Documentation.

4.7. The Supplier will, as part of the Services and at no additional cost to the Client, provide the Client with the Helpdesk Services as described in the Statement of Work during Normal Business Hours (except for planned maintenance carried out as notified from time to time by the Supplier to the Client).

5. Additional Consultancy Services

5.1. If agreed by the parties after the Effective Date, the Supplier shall provide Additional Consultancy Services to supplement the Services.

5.2. The Additional Consultancy Services and the timing thereof shall be mutually agreed between the parties in writing.

5.3. The Client will pay fees for the Additional Consultancy Services in accordance with the Reference Charges.

6. Protected Data

6.1 The provision of the Services and the Additional Consultancy Services do not entail the processing of Personal Data. It is understood that if the Supplier processes any Supplier Personal Data, the Supplier will be the Controller of such Supplier Personal Data. Should the Supplier process Client Personal Data, the Parties shall evaluate in good faith the privacy subjective role of the Supplier, according to the requirements set forth in the Data Protection Legislation.

7. Supplier Obligations

7.1. The Supplier warrants that the Services shall be performed with the utmost skill and care by appropriately experienced individuals.

7.2. The Supplier warrants that Services and Supplier Materials will perform in accordance with the Agreement in all material respects. This warranty shall not apply to the extent of any non-conformance which is caused by (i) use of the Services or Supplier Materials contrary to the Supplier's written instructions or this Agreement; or (ii) modification or alteration of the Services or Supplier Materials by any party other than the Supplier.

7.2.1 The Client reserves the right to verify, at any time and also through third parties that are not competitors of the Supplier (i.e. entities which provides regulatory reporting quality assurance or testing services), that the contractual activities are carried out in compliance with all the obligations contractually entered into and in compliance with current regulations.

7.2.2 The Supplier also agrees to allow on 7 Business Days' written notice once every 12 months, at no additional cost to the Client, access to its offices by the Client and the Authorities and agrees to provide to the Client (and/or upon their request, directly to the Authorities) all reasonable data, documents, information and assistance in relation to the Services.

7.2.3 The above is without prejudice to the powers to request information and of investigation of the competent Authorities under Articles 63(1)(a) of Directive 2014/59/EU and 65(3) of Directive 2013/36/EU (and any amendments and additions thereto) which shall be deemed conventionally applicable regardless of the country where the Supplier operates.

7.3. The Supplier:

7.3.1 does not warrant that the Client's use of the Services will be error-free; nor that the Services, Supplier Materials and/or the information provided to the Client will meet all of the Client's requirements; and

7.3.2 is not responsible for any delays, delivery failures, or any other loss or damage resulting from delays in the provision or transfer of data over communications networks and facilities, including the internet subject to proper performance by the Supplier of its obligations in clause 7

of the Agreement, and the Client acknowledges that the Services and Supplier Materials may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

7.4. The Supplier agrees to establish and maintain updated valid business continuity plans and instruments ("Business Continuity Plan" or "BCP"), so as to ensure the provision of it services even upon occurrence of exceptional events. If the Supplier in turn uses third parties for the provision of the Services, the Supplier shall ensure that any such third parties fulfil the same contractual obligations undertaken by the Supplier.

7.4.1. In any event, the Supplier undertakes to specifically submit, on request of the Client, its Business Continuity Plan, as well as to as soon as reasonably practicable inform the Client - as soon as it is aware - of any event or situation that may give rise to one of the aforementioned situations (and, in particular, in the event of a strike, as soon as the strike has been called), or that in any event may obstruct the normal performance of the Services.

7.4.2. If the Client sets up its own BCP and Disaster Recovery Plan, the Supplier undertakes to ensure the same services to support emergency operations at the backup/disaster recovery sites of the Client, in accordance with the solutions adopted.

7.4.3. Verifications in relation to the above may be made directly by the Audit Function of the Client, also by access to the office of the Supplier for the execution of the Services on 7 Business Days written notice once every 12 months.

7.5 This Agreement shall not prevent the Supplier from entering into similar agreements with third parties, or from independently developing, using, selling or licensing documentation or services which are similar to those provided under this Agreement.

7.6 The Supplier warrants that it has full power and authority to enter into this Agreement.

7.7. The Supplier warrants that it has and will maintain during the Term, all necessary licences, consents, and permissions necessary for the performance of its obligations under this Agreement.

7.8. The Supplier acknowledges that credit institutions and investment firms are subject to the provisions set out in Directive 2014/59/EU, as implemented in Italy by Legislative Decree no. 180 and no. 181 of 16 November 2015 and Regulation (EU) no. 806/2014, as amended.

7.9 The Supplier shall comply with all applicable laws and regulations with respect to its activities under this Agreement.

8. Insurance

8.1. During the Term of this agreement, the Supplier shall maintain in force, with a reputable insurance company, professional indemnity insurance in an amount not less than £6,000,000 and shall, on the Client's request, produce both the insurance certificate giving details of cover and the receipt for the current year's premium.

9. Client's Obligations

9.1. The Client shall:

9.1.1. provide the Supplier with:

a. all necessary co-operation in relation to this Agreement; and

b. all necessary access to such information as may be required by the Supplier in a digital format that can readily be ingested into a structured file format in order to render the Services,

including but not limited to Client Data, (including transactional data from trading systems, the Client's selected ARM, Trade Repository or APA, third party data, underlying Clients data, instrument static, broker contracts, clearing agreements, lists of exchange and central counterparty memberships, relevant instrument static data, details of the Client's systems architecture).

9.1.2. provide any requested data, including but not limited to Client Data, in a format that is compatible with the Supplier's systems;

9.1.3. provide any requested data, including but not limited to Client Data, supporting documentation or general queries within the timescales agreed by the parties;

9.1.4. ensure that any data, including but not limited to Client Data, supporting documentation, information or other materials provided to the Supplier in connection with the Services is accurate and complete;

9.1.5. comply with all applicable laws and regulations with respect to its activities under this Agreement; and

9.1.6. carry out all other applicable responsibilities set out in this Agreement in a timely and efficient manner.

9.2 In the event of any failure by the Client to comply with the timeframes set out in a Statement of Work or this clause 9, including but not limited to, a delay in the provision of Client Data to the Supplier, the Supplier may adjust any agreed timetable or delivery schedule as reasonably necessary.

9.3 The Client for itself and on behalf of its Affiliates consents to the use of the Client Data for reconciliation purposes against data obtained from third party sources.

10. Expenses

10.1. The Supplier will be reimbursed for expenses reasonably incurred in the performance of the Services provided that the expenses were approved in advance by the Client.

10.2. Expenses are to be invoiced separately by the Supplier, supported by a claim sheet and VAT invoice if appropriate.

11. Fees

11.1. The Client shall pay the Fees set out in the Statement of Work to the Supplier in accordance with this clause 11.

11.2. The Supplier shall send an invoice to the Client in accordance with the Statement of Work and such invoice will be payable within 30 days from receipt of invoice.

11.3. Save as otherwise expressly provided for in a Statement of Work, the Supplier shall be entitled to submit an invoice to the Client for 50% of the Fees on or after the SOW Date (as defined in the relevant Statement of Work). Invoices for the balance of the Fees in respect of such Statement of Work shall be submitted in advance on or after the first day of each subsequent quarter during the Service Period of the applicable Statement of Work in equal instalments.

11.4. The Supplier shall invoice the Client for any Additional Consultancy fees incurred during the previous month as agreed with the Client in relation to Additional Consultancy Services provided to the Client from time to time and, unless otherwise agreed in the Statement of Work, such invoice

will be payable within 30 days from receipt of invoice.

11.5. All payments shall be made by the Client by bank transfer to the account of the Supplier at a bank to be nominated in writing by the Supplier.

11.6. If the Supplier has not received payment within 30 days after the due date, and without prejudice to any other rights and remedies of the Supplier if following a further 10 days' notice to settle the Client fails to do so:

11.6.1 the Supplier may, subject to submitting written notice of a further 10 days without liability to the Client, disable the Client's passwords, account and access to all or part of the Services and the Supplier shall be under no obligation to provide any or all of the Services while the invoice(s) concerned remain unpaid.

11.7 All amounts and Fees stated or referred to in this Agreement:

11.7.1 shall be payable in Pound Sterling;

11.7.2 are exclusive of value added tax, which shall be added to the Supplier's invoice(s) at the appropriate rate.

11.8 The Client agrees to make all payments under this Agreement without set-off or counterclaim and free and clear of any withholding or deduction (save as required by law) for any present or future taxes, levies, import duties or other charges. If the Client is obliged by law to make any such withholding or deduction, the Client will pay to the Supplier in the same manner and at the same time additional amounts to ensure that the Supplier receives a net amount equal to the full amount which the Supplier would have received if no such deduction or withholding had been required.

11.9 In the event the Client disputes any aspect of the invoice, it shall notify the Supplier within 14 days of receipt otherwise such invoice shall be deemed to be correct and payable.

12 Proprietary Rights

12.1 Nothing in the Agreement will be deemed to transfer any Intellectual Property Rights between the Supplier and the Client or its Affiliates.

12.2 The Client for itself and on behalf of the Affiliates acknowledge and agree that the Supplier and/or its licensors own all Intellectual Property Rights in the Supplier Materials. Except as expressly stated herein, this Agreement does not grant the Client or its Affiliates any rights to, or in, patents, copyrights, database rights, trade secrets, trade names, trade-marks (whether registered or unregistered), or any other rights or licences in respect of the Supplier Materials.

12.3 The Supplier confirms that it has all the rights in relation to the Supplier Materials that are necessary to grant all the rights it purports to grant under, and in accordance with, the terms of this Agreement.

12.4 The Supplier acknowledges and agrees that the Client or its Affiliates as applicable owns all Intellectual Property Rights in the Client Data.

13 Indemnity

13.1 Subject to clause 14.4.3, the Supplier shall indemnify the Client, their officers, directors and employees against any claim that the Services or Supplier Materials infringes any copyright, trade mark, database right or right of confidentiality, and shall indemnify the Client for any amounts awarded against the Client in judgment or settlement of such claims and any reasonable and proper costs and expenses in connection with such claims, provided that;

13.1.1 the Supplier is given prompt notice of any such claim;

13.1.2 the Client provides reasonable co-operation to the Supplier in the defence and settlement of such claim, at the Supplier's expense;

13.1.3 the Supplier is given sole authority to defend or settle the claim; and

13.1.4 the alleged infringement has not arisen from the use of Client's Intellectual Property Rights by the Supplier.

13.2 Without derogating from the Supplier's obligation under Section 13.1, in the defence or settlement of any claim, the Supplier may procure the right for the Client to continue using the Services, replace or modify the Services or Supplier Materials so that they become non-infringing.

13.3 In no event shall the Supplier, its employees, agents and sub-contractors be liable to the Client to the extent that the alleged infringement is based on:

13.3.1 a modification of the Services or Supplier Materials by anyone other than the Supplier; or

13.3.2 the Client's use of the Services or Supplier Materials in a manner contrary to the instructions given to the Client by the Supplier; or

13.3.3 the Client's use of the Services or Supplier Materials after notice of the alleged or actual infringement from the Supplier or any appropriate authority.

14 Limitation of Liability

14.1 Without prejudice for Supplier obligation under Section 13, this clause 14 sets out the entire financial liability of the Supplier (including any liability for the acts or omissions of its employees, agents and sub-contractors) to the Client and its Affiliates in respect of:

14.1.1 any breach of this Agreement;

14.1.2 any use made by the Client of the Services, Project Results and Documentation or any part of them; and

14.1.3 any representation, statement or tortious act or omission (including negligence) arising under or in connection with this Agreement.

14.2 Except as expressly and specifically provided in this Agreement:

14.2.1 the Client assumes sole responsibility for all results, information and data obtained or derived from the use of the Services, Project Results and the Documentation, and for all conclusions drawn, and any actions and decisions taken or conducted from such use of the Services, Project Results and the Documentation by the Client. The Supplier shall have no liability for any damage caused by errors or omissions in any information, instructions or scripts provided to the Supplier by the Client in connection with the Services or Project Results or Documentation, or any actions taken by the Supplier at the Client's direction;

14.2.2 all warranties, representations, conditions and all other terms of any kind whatsoever implied by statute or common law are, to

the fullest extent permitted by applicable law, excluded from this Agreement; and

14.2.3 the Services and the Supplier Materials are provided on an "as is" basis.

14.3 Nothing in this Agreement shall exclude or limit the liability of the Supplier:

14.3.1 for death or personal injury caused by the Supplier's negligence; or

14.3.2 for fraud or fraudulent misrepresentation and gross negligence.

14.4 Subject to clause 14.3;

14.4.1 neither of the parties shall be liable whether in tort (including for negligence or breach of statutory duty), contract, misrepresentation, restitution or otherwise for (a) any loss of profits, (b) loss of business or sales, (c) loss of agreements or contracts, (d) regulatory fines or penalties, (e) loss or depletion of goodwill, (f) loss of anticipated savings, (g) loss of use or corruption of software and/or (h) similar losses or loss or corruption of data or information, or (i) pure economic loss, or for any (j) special, indirect or consequential loss, costs, damages, charges or expenses however arising under or in connection with this Agreement;

14.4.2 save for claims under an indemnity pursuant to clause 14.4.3, either party's total aggregate liability arising under or in connection with this Agreement in contract, tort (including negligence or breach of statutory duty), misrepresentation, restitution or otherwise with regard to the performance or contemplated performance of the Services in relation to any given event or series of connected events shall be limited to the Fees paid during the 12 month period immediately preceding the date on which the claim arose; and

14.4.3 in respect of claims under an indemnity, the aggregate liability of either party arising under or in connection with this Agreement shall be £6 million.

15 Restrictions

15.1 The Client or any of its Affiliates shall not, without the prior written consent of the Supplier, either directly or indirectly during the Term or for 6 months following the expiry of the Term:

15.1.1 approach any person who at any time during the Term was employed or engaged by the Supplier in the provision of the Services ("Restricted Employee"), with a view to offering them employment or any other form of engagement unless agreed in writing by the Supplier; or

15.1.2 employ or engage any Restricted Employee or seek to recruit them.

15.1.3 Nothing in this clause shall prevent the Supplier or the Client from undertaking recruitment advertising online or in the national, local or industry press and offering employment or engagement to any such person who responds to such advertising.

16 Confidentiality

16.1 Without prejudice to the obligations above, the Supplier shall keep strictly confidential and shall not disclose to any third party any Confidential Information of the Client or any other third parties which has been disclosed to the Supplier or made available to the Supplier, either directly or indirectly under or pursuant to this Agreement, nor use the same for any purpose other than the performance of the Services for which it has been engaged.

16.2 Without prejudice to the obligations above, the Client shall keep strictly confidential and shall not disclose to any third party any Confidential Information of the Supplier which has been disclosed to the Client either directly or indirectly under or pursuant to this Agreement, including all Supplier Materials provided as part of the Service under this Agreement.

16.3 The Supplier and the Client may disclose such information to their employees to the extent that the same have a need to know and only as strictly necessary for the performance of the Services. The Supplier and the Client shall ensure that all such persons are aware of and comply with these obligations of confidentiality.

16.4 To the extent that a party wishes to disclose the other's Confidential Information to an agent, adviser or contractor, the party wishing to disclose shall obtain the prior written consent of the other party (such consent not to be unreasonably withheld or delayed) provided that Client shall not provide the Supplier's Confidential Information to any person who is employed, retained or engaged in any capacity by an entity which provides regulatory reporting quality assurance or testing services.

16.5 Information shall not be considered Confidential Information where it: a) is or becomes publicly known otherwise than as a result of a breach of confidence or of this Agreement; or b) is already known to a party, as evidenced by reasonable written records and is not subject to any obligation of confidence, at the time of disclosure by the other party; or c) is lawfully obtained by a party without any obligation of confidence from a third party who is free to divulge the same; or d) is independently developed by a party, as evidenced by reasonable written records, without reference to the other party's Confidential Information.

16.6 The Supplier and the Client may disclose any Confidential Information of the other to the extent that it is required to be disclosed to any governmental or other authority or regulatory body or to the extent required by law, provided that the disclosing party notifies the other party prior to such disclosure, or where prior notice is not possible, immediately following such disclosure and that the disclosing party uses all commercially reasonable endeavours to ensure that such disclosure is made on a confidential basis.

16.7 Upon expiry or termination of this Agreement for whatever reason, the receiving party shall, and shall procure that its personnel shall, destroy forthwith (or at the disclosing party's written request, return forthwith to the disclosing party) all Confidential Information provided to it or other relevant third parties. For the avoidance of doubt, this requirement: (i) shall apply to any material or information in whatever form

including, but not limited to, electronic form and shall include all documentation provided under the terms of this agreement, notes, copies or extracts of the information or material; (ii) shall not apply to the Project Results. The receiving party shall, on request by the disclosing party, certify in writing that the provisions of this clause have been complied with. The above is without prejudice to each party's right to keep a copy of any information necessary to comply with legal and/or regulatory obligations.

16.8 The obligations of confidence herein shall remain in force indefinitely after any termination of this Agreement.

17 Notices

17.1 All notices shall be in writing and delivered by hand or sent by recorded delivery or registered post to the address stated at the top of this Agreement or such other address as shall be notified in accordance with this provision. If delivered by hand such notice shall be deemed served at the time of delivery. A postal notice which complies with this clause shall be deemed served 3 days after posting (excluding Saturdays, Sundays and bank and public holidays) if from and to an address in the United Kingdom and 7 days from the date of posting if from and/or to an address elsewhere.

18 Term and Termination

18.1 This Agreement shall, commence on the Effective Date and shall continue in force until terminated in accordance with this Clause 18, and the aforesaid shall constitute the Term.

18.2 Either party may terminate the Agreement by giving not less than 3 month's written notice, such notice not to be served within 12 months of the start of the Service Period of the most recent Statement of Work.

18.3 Without prejudice to any other rights or remedies to which the parties may be entitled, either party may terminate the Agreement on immediate written notice to the other without liability to the other if:

18.3.1 the other party commits a breach of clauses 3.3, 3.4, 3.5, **Error! Reference source not found.**, 8.1, 9.1 14, and 16 of this Agreement that may constitute a material breach and (if such a breach is remediable) fails to remedy that breach within 7 days of that party being notified in writing of the breach; or

18.3.2 the withdrawal has been directed in writing by an Authority or in case the Supplier refuses to make any changes required under article 4.6.1 to comply with the provisions of the Authority. In the case provided above, the Client will only pay any amounts due for the Services provided until the effective date of withdrawal, excluding any claim for damages and/or compensation of any kind and/or reimbursement.

18.3.3 an order is made or a resolution is passed for the winding up of a party, or circumstances arise which entitle a court of competent jurisdiction to make a winding-up order in relation to a party; or

18.3.4 an order is made for the appointment of an administrator to manage the affairs, business and property of the

other party, or documents are filed with a court of competent jurisdiction for the appointment of an administrator of the other party, or notice of intention to appoint an administrator is given by the other party or its directors or by a qualifying floating charge holder (as defined in paragraph 14 of Schedule B1 to the Insolvency Act 1986); or

18.3.5 a receiver is appointed of any of the other party's assets or undertaking, or if circumstances arise which entitle a court of competent jurisdiction or a creditor to appoint a receiver or manager of the other party, or if any other person takes possession of or sells the other party's assets; or

18.3.6 the other party makes any arrangement or composition with its creditors, or makes an application to a court of competent jurisdiction for the protection of its creditors in any way; or

18.3.7 the other party ceases, or threatens to cease, to trade; or

18.3.8 the other party takes or suffers any similar or analogous action in any jurisdiction in consequence of debt.

18.4 On termination of this Agreement for any reason:

18.4.1 all licences granted under this Agreement shall immediately terminate;

18.4.2 without prejudice to clause 16.7, each party shall return and make no further use of any equipment, property, Documentation Confidential Information, and other items (and all copies of them) belonging to the other party;

18.4.3 the Supplier may destroy or otherwise dispose of any of the Client Data in its possession; and

18.4.4 the accrued rights of the parties as at termination, or the continuation after termination of any provision expressly stated to survive or implicitly surviving termination, shall not be affected or prejudiced.

18.4.5 Clauses 12, 13, 14, 16, 17 and 28 are to survive indefinitely following the termination of this contract.

18.4.6 In all cases of termination of the Agreement, the Supplier – if specifically requested by the Client – undertakes to provide the relevant Services for an additional period (up to twelve months, as required by the Client) from the date of termination of the contractual relationship, applying the related procedures, terms and conditions and subject to payment of the Fees.

18.4.6.1 Notwithstanding the foregoing, and without any additional financial burdens for the Client, the Supplier undertakes (in addition to that provided by legislation and by provisions of the competent authorities) to:

(i) cooperate with the Client in preparing and implementing a plan for the migration of the activities, on the understanding that, where the activities are subsequently performed by a third party appointed by the Client, and subject to any other specific agreements, the Supplier will be required only to assist the appointed third party in preparing and implementing said plan, with the costs borne by the Client subject to the Confidentiality obligations described above;

(ii) perform any activities required for the orderly

transfer of the activities to the Client or the third party appointed by it, guaranteeing the Services set out in the Agreement, until their final assignment subject to the Confidentiality obligations described above. It is understood that the Supplier shall not be required to train any personnel appointed to perform the services; however, the Supplier shall provide all the necessary information for a realistically competent operator to take over the activities provided that Confidential Information shall not be disclosed to the appointed competent operator;

(iii) return, within the date of conclusion of the migration, any information and documentation received and/or pertaining to the Client and which is still in its possession; and

(iv) cooperate with the Authorities to which the Client is submitted and to the relevant requests including the Resolution Authority.

19 Force Majeure

19.1 Neither party shall be liable to the other under this Agreement if it is prevented from or delayed in performing its obligations under this Agreement, or from carrying on its business, by acts, events, omissions or accidents beyond its reasonable control, including, without limitation, failure of a utility service or transport or telecommunications network, act of God, war, riot, civil commotion, , compliance with any law or governmental order, rule, regulation or direction, accident, provided that the other party is notified of such an event and its expected duration by the party declaring a force majeure event.

20 Waiver

20.1 A waiver of any right under this Agreement is only effective if it is in writing and it applies only to the party to whom the waiver is addressed and to the circumstances for which it is given.

20.2 Unless specifically provided otherwise, rights arising under this Agreement are cumulative and do not exclude rights provided by law.

21 Severance

21.1 If any provision (or part of a provision) of this Agreement is found by any court or administrative body of competent jurisdiction to be invalid, unenforceable or illegal, the other provisions shall remain in force.

21.2 If any invalid, unenforceable or illegal provision would be valid, enforceable or legal if some part of it were deleted, the provision shall apply with whatever modification is necessary to give effect to the commercial intention of the parties.

22 Entire Agreement

22.1 This Agreement and each Statement of Work issued hereunder, constitute the whole agreement between the parties and supersede any previous arrangement, understanding or agreement between them relating to the subject matter they cover.

22.2 Each of the parties acknowledges and agrees that in entering into this Agreement it does not rely on any

undertaking, promise, assurance, statement, representation, warranty or understanding (whether in writing or not) of any person (whether party to this Agreement or not) relating to the subject matter of this Agreement, the Statement of Work or other than as expressly set out in the same.

23 Assignment

23.1 Neither party shall assign, transfer, charge, sub-contract or deal in any other manner with all or any of its rights or obligations under this Agreement without the prior consent of the other party, which is not to be unreasonably withheld or delayed.

24 No Partnership or Agency

24.1 Nothing in this Agreement is intended to or shall operate to create a partnership between the parties, or authorise either party to act as agent for the other, and neither party shall have the authority to act in the name or on behalf of or otherwise to bind the other in any way (including, but not limited to, the making of any representation or warranty, the assumption of any obligation or liability and the exercise of any right or power.

25 Third Party Rights

25.1 This Agreement does not confer any rights on any person or party (other than the parties to this Agreement and, where applicable, their successors and permitted assigns) pursuant to the Contracts (Rights of Third Parties) Act 1999.

26 Announcements

26.1 Subject to clause 26.2, no announcement, circular, advertisement, marketing or other publicity in connection with the Agreement, its subject matter, or any ancillary matter shall be made or issued by or on behalf of either party without the prior written consent of the other party.

26.2 The parties may, acting in good faith and using reasonable endeavours, agree the content of a joint press release which shall be announced as soon as reasonably practicable following the Effective Date or following the execution of each Statement of Work.

26.3 For the duration of the Term and for 12 months thereafter, the Supplier shall have a right to use the Client's name and trademark on the Supplier's website and marketing literature for the purpose of identifying the Client as a customer of the Supplier.

27 Variation

27.1 No variation of this Agreement shall be effective unless it is in writing and signed by the parties (or their authorised representative).

28 Jurisdiction

28.1 This Agreement and any disputes or claims arising out of or in connection with its subject matter are governed by and construed in accordance with the law of England.

28.2 The parties irrevocably agree that the courts of England have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this Agreement.

Signed for and on behalf of **Intesa Sanpaolo SPA**	Signed for and on behalf of **Kaizen Reporting Limited**
	Dario Crispini Dario Crispini (Mar 3, 2022 15:37 GMT)
Name:	Name: Dario Crispini
Title:	Title: Chief Executive Officer

KAIZEN
DELIVERING CONFIDENCE

SCHEDULE 1

SERVICES

A. TESTING

1.1 Reference Data Testing

1.1.1 Objective and Definition of Service

Counterparty reference data testing that checks that firms are:

1. Using the required identifiers available.
2. That the regulatory id (LEI, BIC etc.) is mapped to correct legal entity.

1.1.2 Deliverable Output

The Client will receive results in the following form within 6 weeks following receipt by Supplier of a complete data set of the relevant Client Data in respect of the period under review (as determined by the Test Frequency) or confirmation to process an incomplete data set on condition that processing of the reduced data set is feasible:

1. Executive written report for senior management that outlines and quantifies the issues identified in the applicable testing period.

2. Management Information metrics.

3. Detailed issues mapped to errant transactions.
The deliverable output is dependent on the timely delivery of Client Data and prompt and satisfactory responses to Supplier's queries by Client, and in the event of any delays in provision of such Client Data or assistance, the delivery timetable may be subject to reasonable adjustments.

The review service and deliverable output does not encompass investigation or management of the resolution of any of the issues identified during the course of the provision of the Services.

1.2 Accuracy Testing

1.2.1 Objective and Definition of Service

Tests all fields on open positions reported to the Trade Repository (TR) or on transactions reported to the National Competent Authority (NCA) for MiFID II, to identify where Client has reported data incorrectly. e.g.: Client has reported a valid price, instrument identifier or time but Supplier's testing will highlight whether the price is incorrect, with wrong identifier or at an incorrect time.

In addition to validation testing performed by Client and TRs, Supplier runs tests wherever possible using independent data sources including, pricing, reference data, and market venue data.

1.2.2 Deliverable Output

The Client will receive results in following form within 6 weeks following receipt by Supplier of a complete data set of the relevant Client Data in respect of the period under review (as determined by the Test Frequency) or confirmation to process an incomplete data set on condition that processing of reduced data set is feasible:

1. Executive written report for senior management that outlines and quantifies the issues identified in the applicable testing period.

2. Management Information metrics.

3. Detailed issues mapped to errant transactions.

The Deliverable output is dependent on the timely delivery of Client Data and prompt and satisfactory responses to Supplier's queries by Client, and in the event of any delays in provision of such Client Data or assistance, the delivery schedule may be subject to reasonable adjustments.

The review service and deliverables output does not encompass investigation or management of the resolution of any of the issues identified during the course of the provision of the Services.

1.3 **Advanced Regulatory Reconciliation**

1.3.1 Objective and Definition of service

- Reconcile all trades in Client's books and records against what has been reported to the Regulator to identify over, under reported and mismatched fields.

- Reporting eligibility criteria set by Regulator is independently applied.

- Data normalisation allows accurate paring and matching.

1.3.2 Deliverable Output

At the end of each period, (as determined by the Test Frequency) The Client will receive results in following form:

1. Executive written report for senior management that outlines and quantifies the issues identified in the applicable testing period.

2. Management Information metrics.

3. Detailed issues mapped to errant transactions.

The deliverable output is dependent on the timely delivery of Client Data and prompt and satisfactory responses to Supplier's queries by Client, and in the event of any delays in provision of such Client Data or assistance, the delivery schedule may be subject to reasonable adjustments.

The review service and deliverables output does not encompass investigation or management of the resolution of any of the issues identified during the course of the provision of the Services.

B. CONTROL FRAMEWORK

A complete regulatory reporting governance framework of supporting controls to promote the completeness, accuracy and timeliness of Client's regulatory reporting. It covers governance, accountability, training and guidance for MiFID II, EMIR, DFA and other G20 regimes.

Deliverables

• A reporting risk and accountability framework tailored to your firm

• All required policy and guidelines documentation

C. KAIZEN TRAINING

3.1. MiFIR Transaction Reporting

3.1.1 Objective and Definition of Service

Half-day CPD-accredited training course on the MiFIR transaction reporting process to provide candidates with a good core understanding of MiFIR transaction reporting requirements and the fields that comprise a transaction report. The course also includes an exam that will enable candidates to demonstrate their understanding of the transaction reporting requirements.

3.2 EMIR Trade Reporting

3.1.2 Objective and Definition of Service

Half-day CPD-accredited training course on the EMIR trade reporting process to provide candidates with a good core understanding of EMIR trade reporting requirements and covers the regulatory drivers, the reporting scope, trading scenarios and the key fields that comprise an EMIR trade report. The course also includes an exam that will enable candidates to demonstrate their understanding of the trade reporting requirements.

3.3 SFTR Reporting

3.1.3 Objective and Definition of Service

Half-day CPD-accredited training course on SFTR implementation from both sell-side and buy-side investment firms, corporate treasuries engaged in SFT business, CCPS, CSDs, triparty agents, agent lenders with own account SFT business or delegated reporting to deliver. Attendees will gain a detailed overview of the reporting requirements and an in-depth study of how to comply with the regulation, and will include a review of the scope, nature of reportable activities and how to complete reports. Appropriate controls, standards and industry wide engagements will also be discussed.

D. REPLAY TESTING AND CORRECTION

4.1 Replay Assurance Testing

4.1.1 Objective and Definition of Service

Testing of the fields of Transaction Reports corrected by Client of transactions that are proposed to be back reported by Client to the National Competent Authority (NCA), to identify where Client's back reports are incorrect.

In addition to validation testing performed by Client and TRs, Supplier runs tests wherever possible using independent data sources including, but not limited to, pricing, reference data, and market venue data.

Reconciliation of the unchanged fields between the original submission and the back report to ensure no change.

4.2.1 Deliverable Output

The Client will receive results in following form within a mutually agreed timeframe following receipt by Supplier of a complete data set of the relevant Client Data in respect of the period under review or confirmation to process an incomplete data set on condition that processing of reduced data set is feasible:

1. Executive written report for senior management that outlines and quantifies the issues identified in the applicable testing period.

2. Detailed issues mapped to errant transactions.

The Deliverable output is dependent on the timely delivery of Client Data and prompt and satisfactory responses to Supplier's queries by Client, and in the event of any delays in provision of such Client Data or assistance, the delivery schedule may be subject to reasonable adjustments.

The review service and deliverables output does not encompass investigation or management of the resolution of any of the issues identified during the course of the provision of the Services.

4.2 Replay File Correction

4.2.1 Objective and Definition of Service

Creation of corrections file for replay. This includes:

- Auto correct fields for replay where applicable
- Work with the Client to identify the correct values for replay where auto correction is not applicable
- Accuracy testing of final replay file

4.2.2 Deliverable Output

The Client will receive ISO 20022 format file for the Client to upload via its ARM and an audit summary report of corrections made and testing results.

4.3 Replay File Creation

4.3.1 Objective and Definition of Service

Creation of replay files for trades not previously reported to the NCA. This includes:

- Work with the Client to identify the correct data set and field values for file creation
- Accuracy testing of final replay file

4.3.2 Deliverable Output

The Client will receive ISO 20022 format file for the Client to upload via ARM and an audit summary report of trade creation file and testing results.

.

E. KAIZEN CONSULTANCY

Consultancy services in respect of regulatory reporting including but not limited to MiFID II, EMIR, DFA, other G20 regimes and SFTR. The Service may include reviewing a governance framework of supporting controls for completeness, accuracy and timeliness of Client's regulatory reporting and may cover governance, accountability, training and guidance.

SCHEDULE 2

TEMPLATE STATEMENT OF WORK

(1) **[ ]**, a company registered in [England and Wales] [with registration number [ ]] and LEI Code [ ] and whose registered office is situated at [ ] (the "**Client**"); and

(2) **KAIZEN REPORTING LIMITED**, a company registered in England and Wales with registration number 08362415 and LEI Code 254900RYLWYAV1Y93K81 and whose registered office is situated at 12 Groveland Court, London EC4M 9EH (the "**Supplier**"),

each a **"party"** to this Agreement and together the "**parties**".

This Statement of Work is entered into under the Master Services Agreement dated [ ] between parties and the Services as defined in Schedule 1 of the Master Services Agreement. The terms of the Statement of Work are as follows:

Statement of Work Number	
Statement of Work Date or SOW Date	
Service Period	
Services	Accuracy testing – MiFID II (Transaction reporting)
Test Frequency	
Fees	per annum (represents our standard fee of X per annum less a discount of X)
Contact	
Assumptions:	Up to: (expected volume)
Billing schedule	An invoice for 50% of the annual Fee to be sent to Client on or after the SOW Date An invoice for 16.67% of the annual Fee to be sent to Client 3 months after the SOW Date An invoice for 16.67% of the annual Fee to be sent to Client 6 months after the SOW Date An invoice for 16.67% of the annual Fee to be sent to Client 9 months after the SOW Date Thereafter; An invoice for 25% of the annual Fee to be sent to Client on or following each quarter day
Additional terms	Any volume in excess of the expected volume shall be charged in accordance with the Supplier's standard charges. Notwithstanding clause 18, this SOW will enter into force on the SOW Date and will continue to be in force until terminated by either party giving the other party not less than 3 (three) months prior written notice, such notice not to be served within 9 (nine) months of the SOW Date.

	Supplier may adjust the Fees on an annual basis by giving the Client not less than 120 (one hundred and twenty) days' prior written notice of such change. If the Client does not accept such adjustments to the Fees, notwithstanding clause 18.2 it has the right to serve written notice to terminate this SOW on the date the Fee adjustments go into effect.

Signed for and on behalf of Client	Signed for and on behalf of Kaizen Reporting Limited
Name:	Name:
Title:	Title:
Date:	Date:

KAIZEN
DELIVERING CONFIDENCE

STATEMENT OF WORK

(1) **[ ]**, a company registered in [England and Wales] [with registration number [ ]] and LEI Code [ ] and whose registered office is situated at [ ] (the "**Client**"); and

(2) **KAIZEN REPORTING LIMITED**, a company registered in England and Wales with registration number 08362415 and LEI Code 254900RYLWYAV1Y93K81 and whose registered office is situated at 12 Groveland Court, London EC4M 9EH (the "**Supplier**"),

each a **"party"** to this Agreement and together the "**parties**".

This Statement of Work is entered into under the Master Services Agreement dated [ ] between parties and the Services as defined in Schedule 1 of the Master Services Agreement. The terms of the Statement of Work are as follows:

Statement of Work Number	
SOW Date	
Service Commencement Date	
Services	Advanced regulatory reconciliation – MiFID II (Transaction reporting)
Test Frequency	Monthly
Fees	per annum (represents our standard fee of X per annum less a discount of X)
Contact	
Assumptions:	(expected source systems)
Billing schedule	An invoice for 50% of the annual Fee to be sent to Client on or after the SOW Date An invoice for 16.67% of the annual Fee to be sent to Client 3 months after the SOW Date An invoice for 16.67% of the annual Fee to be sent to Client 6 months after the SOW Date An invoice for 16.67% of the annual Fee to be sent to Client 9 months after the SOW Date Thereafter; An invoice for 25% of the annual Fee to be sent to Client on or following each quarter day

Additional terms	In the event of additional source systems, the supplementary Services shall be charged in accordance with the Supplier's standard charges. Notwithstanding clause 18, this SOW will enter into force on the SOW Date and will continue to be in force until terminated by either party giving the other party not less than 3 (three) months prior written notice, such notice not to be served within 9 (nine) months of the SOW Date. Supplier may adjust the Fees on an annual basis by giving the Client not less than 120 (one hundred and twenty) days' prior written notice of such change. If the Client does not accept such adjustments to the Fees, notwithstanding clause 18.2 it has the right to serve written notice to terminate this SOW on the date the Fee adjustments go into effect.

Signed for and on behalf of
Client

Name:

Title:

Date:

Signed for and on behalf of
Kaizen Reporting Limited

Name:

Title:

Date:

STATEMENT OF WORK

(1) **[ ]**, a company registered in [England and Wales] [with registration number [ ]] and LEI Code [ ] and whose registered office is situated at [ ] (the "**Client**"); and

(2) **KAIZEN REPORTING LIMITED**, a company registered in England and Wales with registration number 08362415 and LEI Code 254900RYLWYAV1Y93K81 and whose registered office is situated at 12 Groveland Court, London EC4M 9EH (the "**Supplier**"),

each a **"party"** to this Agreement and together the "**parties**".

This Statement of Work is entered into under the Master Services Agreement dated [ ] between parties and the Services as defined in Schedule 1 of the Master Services Agreement. The terms of the Statement of Work are as follows:

Statement of Work Number	
SOW Date	
Service Commencement Date	
Services	Reference Data Testing
Test Frequency	
Fees	per annum (represents our standard fee of X per annum less a discount of X)
Contact	
Assumptions:	Up to: (expected accounts)
Billing schedule	An invoice for 50% of the annual Fee to be sent to Client on or after the SOW Date An invoice for 16.67% of the annual Fee to be sent to Client 3 months after the SOW Date An invoice for 16.67% of the annual Fee to be sent to Client 6 months after the SOW Date An invoice for 16.67% of the annual Fee to be sent to Client 9 months after the SOW Date Thereafter; An invoice for 25% of the annual Fee to be sent to Client on or following each quarter day

Additional terms	Any accounts in excess of the expected account number shall be charged in accordance with the Supplier's standard charges. Notwithstanding clause 18, this SOW will enter into force on the SOW Date and will continue to be in force until terminated by either party giving the other party not less than 3 (three) months prior written notice, such notice not to be served within 9 (nine) months of the SOW Date. Supplier may adjust the Fees on an annual basis by giving the Client not less than 120 (one hundred and twenty) days' prior written notice of such change. If the Client does not accept such adjustments to the Fees, notwithstanding clause 18.2 it has the right to serve written notice to terminate this SOW on the date the Fee adjustments go into effect.

Signed for and on behalf of Client	Signed for and on behalf of Kaizen Reporting Limited
Name:	Name:
Title:	Title:
Date:	Date:

Schedule 3

Reference Charges

Time and materials:

- Senior Consultant £550 per hour or part thereof
- Consultant/ Senior Developer £300 per hour or part thereof
- Developer/ Data analyst £200 per hour or part thereof

Standard Charges:

As made available by Supplier from time to time

Exhibit A

Security Standards

Subject: Security Regulations

The provisions of this Annex supplement - insofar as applicable - the provisions of the Agreement /MSA to which they are attached, and the definitions contained therein apply to this document.

This Annex defines the control systems and the security standards that the Supplier undertakes to maintain active and efficient for the entire term of the Agreement under which it is required to process confidential data and information of the Client and/or of other companies of the Intesa Sanpaolo Group, in relation to the services that will actually be provided by it under the agreements in place with the Client and/or the other Companies of the Intesa Sanpaolo Group.

1. **Security standards to protect the information assets of the Intesa Sanpaolo Group**

1.1 In relation to all activities associated with the performance of an Agreement, the Supplier undertakes to adopt formal internal policies consistent with the current legislation and with the Security Standards as communicated from time to time and to ensure that such policies are release throughout its own organization.

1.2 The Supplier must process the data in accordance with the level of classification, with special reference to the confidentiality, and applying the agreed policies on data retention.

1.3 The Supplier acknowledges and agrees that data relating to the architecture and the configuration of the Client's IT systems, the security measures adopted by the latter and - in any event - data concerning any vulnerabilities found during the execution of the Service (the "Data") is confidential by nature (also pursuant to art. 98 CPI - Intellectual Property Code) and that any disclosure of said data to third parties may cause significant detriment to the Client and/or to other companies of the Intesa Sanpaolo Group, also in terms of exposure to hacking or reputational damage.

1.4 The Supplier acknowledges that any data, software, technical or regulatory documentation and ICT resources of the Client that are used to supply the service shall remain the exclusive property of the Client (and/or the other companies of the Intesa Sanpaolo Group and/or their licensors).

1.5 The Supplier acknowledges that violation of any of the security obligations reported in the present annex constitutes cause for the termination of the Agreement in according to the art. 1455 of the Civil Code.

1.6 The Supplier acknowledges, at any time, that the Client may withdraw permission to perform any activities on its own assets (including the data), subject to the provisions of the Agreement.

1.7 The Supplier undertakes, in any case of termination of the Contract, to delete - by using appropriate tools and technical solutions, duly documented - any data present on its systems or supports by reason of the Services previously provided to the Client.

1.8 The Supplier undertakes to return all assets to the Client (including data, licenses and equipment) within the agreed period.

1.9 The Supplier undertakes to apply best practices and generally accepted standards to any situation that is not covered by the required checks.

1.10 The Supplier undertakes to implement the security requirements described in this appendix also in cases where the Service is provided in smart working and/or telework mode. In case the personnel operate outside the territory of the country where the SUPPLIER's headquarter is located, they shall request prior authorization from the Client.

1.11 The Supplier, if it provides an outsourced service and identified as essential/important, undertakes to ensure throughout the duration of the Contract the respect of appropriate standards of computer security for the provision of the service; these standards must be proven by appropriate certifications (e.g. ISO27001, Report SOC1, Report SOC2).

2. **Contact persons for security issues**

2.1 The Supplier and the Client, in order to share the tasks and responsibilities related to the implementation of the Information Security policy, shall communicate to each other the names of the persons appointed to manage the activities covered by the Agreement and in particular to manage the aspects of information security.

2.2 Save as provided otherwise by the party making the appointment, the contact person appointed to manage the contractual activities is also responsible for maintaining liaison with the company structures tasked with the management of all aspects of information security. The Client and the SUPPLIER undertake to notify each other promptly of any changes in relation to the above.

2.3 The Client and the Supplier shall agree appropriate communication, coordination and management procedures on occurrence of events that may compromise data security and/or business continuity and/or contractually defined service levels.

3. **Staff and organization of the Supplier**

3.1 Having regard to the staff involved in the performance of the contractual obligations (including collaborators working in any capacity), the Supplier undertakes, also in respect of information security, for the entire duration of the Contract, to:

(a) ensure that its staff members are appropriately qualified for the tasks they perform and, where required, to employ appropriately certified personnel;

(b) ensure that its staff members receive the training necessary to perform their tasks, as well as adequate information concerning the provisions of the above section1;

(c) implement appropriate policies concerning the segregation of duties when assigning tasks;

(d) (d) assign tasks and responsibilities to its staff members in a manner so as to ensure that key internal and external threats, also internet-related, are effectively monitored;

(e) Adopt formal and secure procedures to immediately revoke user credentials and ensure that all tools used to perform the contractual activities are returned, including badges, keys and other means of access, identification or authentication, when any of its staff members are transferred to other roles or their employment contract is terminated.

3.2 The Supplier undertakes to cooperate with the Client to ensure appropriate coordination with the roles and procedures defined internally by the Client in connection with the risk analysis process and the data management system.

3.3 The Supplier undertakes to maintain (a) a list of the sites in which are hosted (i) the data, (ii) the services and (iii) data centers used by the Supplier to provide the Service and (b) a document indicating the number of staff members who have access to data of the Client and/or of the Concerned Companies, and to update this document at regular intervals and provide a copy to the Client and/or to the Concerned Companies, upon written request of the Client and/or any of the companies involved.

3.4 The Supplier promptly undertakes to notify the Client of the need to transfer resources and data (including backups) from one site/data center (belonging to the Supplier or to a third party) to another and to implement in the new data center the same security measures as in the primary site. It is however understood that the Client must previously authorize the transfer of resources and data from one site/data center to another.

Furthermore, the Supplier undertakes to implement in the new center the same security measures as the ones of the primary site. Any prohibitions / restrictions on the movement of resources and data that may already be foreseen in the Agreement remain unaffected.

3.5 In any case of change in the Supplier organization (also due to transfer's events or changes of sub-contractors, or change of technologies or architectures of sub-contractors) that may affect the level of integrity, availability and confidentiality of data, the Supplier must notify the Client in advance to allow the execution of appropriate assessments and verifications, also by means of audit.

3.6 The Supplier undertakes not to introduce changes (technological, on the services organization and the supply chain) that can be decrease the security of the Service.

4. **Physical and logical security of the Supplier**

4.1 As specified above - in respect to its own company services that are in any case related or linked to the performance of the Services under the Agreement, the Supplier undertakes to adopt legally compliant security measures to manage user credentials and access privileges, with provisions for:

(a) unique and personal user profiles;
(b) secure management of user credentials at regular intervals, mandatory modification at first time access, assurance that credentials cannot be re-used over time and automatic password strength tests;
(c) criteria and policies to ensure that access and user credentials are release in accordance to the segregation of duties criterion;
(d) criteria and policies to ensure that access is denied if access privileges have not explicitly been given and to ensure compliance with the principle of least privilege;
(e) criteria and policies concerning the levels of access privileges, which at least make a distinction between authority to access production data and authority to access and carry out maintenance on systems, software and the network.
(f) tools and policies concerning the safekeeping of data received and storage media so as to prevent loss and accidental access by third parties.

4.2 The Supplier guarantees that physical security measures will be implemented (locked rooms, clean-desk policy, safe storage of media received...) at all critical sites used for or in connection with the Service supplied (and in the routes from or to such sites). If the Service is provided on the premises of the Client and/or of the other companies of the Intesa Sanpaolo Group, the Supplier undertakes to make correct use of the procedures present and to report any deficiencies/malfunctions.

4.3 The destruction of data/media on termination of contractually envisaged activities, or upon specific request by the Client, shall take place in accordance with procedures and standards that meet the security requirements of the related contractual service and/or communicated in time by the Client.

4.4 The Supplier undertakes to adopt appropriate procedures to separate the data, which it manages on behalf of the Client from data it manages on behalf of other customers to ensure the confidentiality, availability and integrity of such data.

4.5 The Supplier undertakes to send a detailed technical description of the methodology it intends to use – in the execution of the Contract - to deliver the Service, and to implement and manage physical, organizational and IT security measures for the protection of the Client's assets, and aimed

at guaranteeing a service that is compliant with the level of classification required - with particular regard to procedures and tools for:

(a) The management of the life cycle (provisioning / deprovisioning), of user credentials (end users and administrators), and of the related problems of profiling in case of their access to systems, applications and networks;
(b) Guaranteeing adequate levels of authentication, authorization and tracking, in case of remote access to the Client's IT assets;
(c) The physical and logical protection of the Supplier's Data Center;
(d) The protection from malicious software;
(e) The management of basic and application software patching, fixing and upgrading;
(f) The management and keeping of storage media;
(g) The controlled disposal of assets with the adoption of systems for the secure deletion of information from storage media;
(h) The tracking and management of events relevant to safety according to the external normative provisions on the subject;
(i) The implementation of adequate data isolation mechanisms between data managed by the Supplier on behalf of the Client and data managed on behalf of its other customers, to guarantee their confidentiality and integrity".

5. **Secure use of the Supplier's systems**

5.1 The Supplier undertakes to ensure the management of the following activities:

(a) IT security and/or business continuity events through the identification, containment, reporting, notification and analysis of information security and/or business continuity events, identifying an appropriate escalation list. In particular, it commits itself to informing the Client, as soon as reasonably practicable and not later than 48 hours, in the person of the Operating Representative, even during non-working hours, of any significant event occurred in relation to the security of information concerning the service subject of the Contract, also sending the appropriate document (Information Set) as an appendix to this Annex;

(b) comply with the response times to security incidents agreed in the Contract;

(c) adopt, for the provision of Services to the Client, IT platforms and solutions that are not in "end of support" (e.g. operating systems or database server versions no longer supported by the reference vendor;

(d) security patch management, by means of controlled updating processes and timing appropriate to the seriousness of the vulnerability, not exceeding six months (in accordance with current legislation) and less than 5 days in the most serious cases;

(e) antivirus management, via regular updates in accordance with the specifications of the antivirus system used;

(f) change management: implementation of authorisation processes for permission to make changes;

(g) controlled data erasure, using secure systems to delete data from storage media;

(h) prohibition of issue press releases expressly naming Client (also through channels such as media, social media, regulators, …) that concern any IT security incidents affecting the Client, without first agreeing with the Client the contents and timing of the communication.

5.2 The Supplier undertakes to implement SPF and DKIM protocols (and possibly DMARC as well) for all its corporate mail domains. Furthermore, in case the SUPPLIER shall provide services involving the sending of e-mails, on behalf of the Client's corporate sub-domains (e.g. comunicazioni@intesasanpaolo.com), the Supplier undertakes to implement the DMARC (Domain-based Message Authentication, Reporting and Conformance) protocol.

5.3 The Supplier undertakes to use strong encryption systems in particular for data at Rest AES256 protocol and for data in transit the TLS1.2 protocol.

6. **Data backup**

6.1 The Supplier undertakes to regularly backup the data associated with the contractual activities (including configuration data relating to devices and systems), ensuring that:

(a) backup copies are kept in a secure fireproof and intrusion-proof area;

(b) backup copies can be recovered and dedicated recovery tests are performed at regular intervals;

(c) User data are kept separate from the configuration data to be backed up.

6.2 The Client reserves the right to access the data backups of the Client associated with the Services made by the Supplier by forwarding prior written request to the Supplier.

6.3 The Supplier undertakes to store and migrate the Client's data in specific countries indicated by the Client itself and, furthermore, undertakes to agree with the Client to the channel through which the migration of the data must be performed.

7. **Tracking**

7.1 The Supplier undertakes to perform the following activities in a systematic and formalized manner, in accordance with laws in force:

(a) Tracking of the software used for or in connection with the performance of the contractual services;

(b) Tracking of the systems and devices used for or in connection with the contractual services.

The event records generated by the authentication systems must indicate the "username" used, the date and time of the event ("timestamp"), a description of the event (e.g. the processing system or software used, whether it is a log-in or log-out event, error condition, the communication line or computer terminal used) and the system on which the "username" has operated. In particular, if the recorded data refers to bank transactions that are processed and covered by the Decisions of the Italian Data Protection Authority regarding "*regulations* on *circulation of information in the banking sector and tracking of banking operations"* (Decision n. 192 of 2011 and following Decisions), the following data must also be tracked:

- The identifier of the customer referred to in the transaction;
- The type of contractual relationship in place with the customer.

7.2 The tracking results must be stored in a secure manner so as to ensure auditability, readability, integrity, reliability and the availability of the information on request (also directly by the Audit function of Intesa Sanpaolo S.p.A.).

7.3 The Supplier shall ensure the traceability of all accesses and changes made to data, also for inspection purposes.

8. **Software development and maintenance**

8.1 In the case of software development or maintenance or activities that involve writing/modifying the software used by the Client and/or the other companies of the Intesa Sanpaolo Group, the Supplier undertakes to use secure software development techniques which include, at least, the validation of input data, internal processing validation checks, message and output validity checks, use of best practice in relation to the specific programming language or development environment used. For the whole duration of the Agreement, the Supplier undertakes to comply with the software secure coding

guidelines listed in the Open Web Application Security Project (OWASP) and the CWE/SANA Top 25 time by time in force. The Supplier also undertakes to comply with the internal regulation document "Security measures for the safe development of the software" time by time in force.

8.2 If the development relates to application within the scope of PCI-DSS, the Supplier undertakes to keep its team members up to date on secure code development techniques through appropriate training initiative on, at least, an annual basis.

8.3 Insofar as the aforementioned activities are carried out in environments which are managed by the Supplier, the latter shall ensure:

(a) The presence of a change management procedure for ICT applications and resources that formally defines and guarantees control over changes, replacements or technological adjustments;

(b) The logical separation between the development environment and all other environments relevant to the company;

(c) That the development, testing and production environments dedicated to the Client and/or the other companies of the Intesa Sanpaolo Group are separated, at least in logical terms, from the environments used for the Supplier's other customers so as to ensure confidentiality and integrity.

(d) Run the tests in an objective, verifiable and repeatable manner

(e) Do not use the proprietary production data of the Client (and/or the Intesa Sanpaolo Group) for testing activities unless appropriately anonymized;

(f) Produce a complete documentation of the tests carried out in security areas;

(g) Access to "production" data or in any to case personal data should be limited to cases of actual and real need (e.g. "emergency corrective maintenance"), limited to the time strictly necessary and in any case specifically and previously agreed upon.

9. **Connection to the systems managed by the Client**

9.1 In the case of activities which involve connecting the Supplier's equipment to the Client's networks and/or systems, the Supplier (save as specifically provided in relation to said equipment under sections 1, 4 and 5 above) undertakes:

(a) Use only the dedicated access networks (where made available by the Client) or those networks which are separated from the internal network managed by the Client (and/or the other companies of the Intesa Sanpaolo Group);

(b) Use such connections, and the IDs, passwords and "user credentials" provided, only for the purposes strictly necessary to complete the contractual activities;

(c) Use secure connections (including VPN or encryption tools), where made available by the Client, if the connection is via open networks (internet, Wi-Fi...).

9.2 The Supplier acknowledges and agrees that the Client (and/or the Parent Company Intesa Sanpaolo S.p.A.) may review accesses and uses of the connection as part of an audit, and may request information on the technical characteristics of the equipment used.

10. **Credentials or tools owned by the Client**

10.1 In all cases in which the Supplier is provided with credentials, IT tools or IDs and other means of access (e.g. badges, keys, smart cards, digital certificates, etc...) to access the systems of the Client (and/or of the other companies of the Intesa Sanpaolo Group), the Supplier - in accordance with the applicable provisions of law - shall:

(a) Provide assurance as to the ability and reliability of the person assigned to the task for which the credentials/tools are being provided;

(b) Ensure that such credentials/tools are kept safe, never made available to third parties and used only to perform the services under the Agreement;
(c) Ensure that no copies are made, unless authorized by the Client;
(d) Ensure that the credentials and tools provided are used solely by the assignees; in all case in which - in accordance with current regulations - the assignee changes, a document shall be undersigned to confirm such change;
(e) Promptly notify the Client of any loss of the credentials/tools (even temporary) and of any potential breaches of the provisions above;
(f) Notify the Client of any other event (e.g. termination of employment Agreement; redeployment...) which results in such credentials or tools being no longer necessary

10.2 In all cases where the Supplier operates on systems or procedures of the Client (and/or the Companies of the Intesa Sanpaolo Group) that involve the use of multi-factor authentication tools (strong-authentication) requiring the use of mobile devices, the Supplier is bound to provide to its involved staff smartphones with features compatible with the Client's standards and that allows SMS and data traffic reception, elements enabling the use of multi-factor authentication tools used by the Client to control and authorize access to its IT systems. The phone number associated with the smartphone must be assigned exclusively to the worker and will be recorded by the Client's Operating Representative in the Client's Security Phone Book. It is the Supplier's responsibility to report promptly any change of assignment.

11. Administrators

11.1 The Supplier shall maintain an updated list of the "system administrators" authorized to work with the Client's data or systems and shall provide these details upon request and/or in accordance with the agreed frequency.

11.2 The Supplier shall conduct the required reliability checks in advance and any other regular checks required under the laws in force, providing an account of such checks whenever requested.

11.3 Access to the information system of the Client (and/or of the Intesa Sanpaolo Group) by the personnel with administrative privileges requires access with 2-factor authentication on mobile devices. Therefore please refer to point 10.2.

12. Auditability and checks

12.1 The Supplier shall conduct regular audits to verify the efficiency of the security systems. The Supplier shall allow the independent assessment and verification of conformity with the agreed provisions, for example, by providing a certification that states the compliance with the industry-specific standards or an audit report.

12.2 The above sentence does not affect the right to conduct direct audits and/or to make requests for information required by law or by the Agreement in favor of the Client, its auditors and by the Authorities and/or Institutions, and in the event of a security incidents and as part of a periodic verification of compliance with the regulatory and contractual provisions.

12.3 The Supplier shall cooperate to perform the audit and any case allow the subjects indicated in the article above to interview its staff (in compliance with current legislation and regulations) and may access:

(a) All information and documents associated with the services;

(b) The systems, the instruments, the network, the databases, the business continuity plans and any other information relating to the services;
(c) The structures and areas in which the service is supplied.

12.4 The Supplier, upon explicit written request by the Client, commits itself to support the Client in the performance of Assessments aimed at certifying the presence of adequate safeguards in the field of Information Security, Operational Continuity and Data Protection. Within the Assessments, the Supplier commits himself to share punctual evidences requested by the Client.

12.5 The Supplier agrees and accepts that the Internal Audit Function of the parent company Intesa Sanpaolo S.p.A. has the right to perform direct audits for all contractual relationship relating to one of the Intesa Sanpaolo Group legal entities.

12.6 The Supplier undertakes, if required, to prepare the appropriate remediation plans to eliminate any unconformities within and no later than the agreed time frames.

13. Vulnerability Assessment and Penetration Test

13.1 The Supplier shall ensure the performance, by specialized personnel and according to industry best practices, of internal Vulnerability Assessment activities at least every six months on the scope of the Services provided to the Client.

13.2 The Supplier shall guarantee the performance, by specialized personnel and according to industry best practices, of internal Penetration Tests at least yearly, on the scope of the Services provided to the Client.

13.3 The Supplier shall also grant to the Client the right to examine upon request of the Client a summary of the results of Vulnerability Assessment and Penetration Tests carried out internally on the scope of the Services provided to the Client, and associated remediation plans on identified vulnerabilities.

14. Additional security requirements

In the case of cloud services or Services delivered remotely, in addition to the clauses in the previous paragraphs, at least the following requirements must be guaranteed:

14.1 In case in which the Client does not use its own audit resources and in any case in which the service is not concerning an Important Operating Function (FOI) or a Critical Components of the Information System (CCSI), the Client can use at least one of the following tools:

(a) Pooled audits organized jointly with other Clients of the Supplier;

(b) Third-party certifications and third party's or Supplier's audit reports;

14.2 The Supplier undertakes to implement the security checks specified in the cloud controls matrix provided by the Client, defined by the CSA CCM (Cloud Security Alliance Cloud Controls Matrix) framework. Furthermore, the Supplier undertakes to provide, on request of the Client, the documentation and evidence necessary to confirm compliance.

14.3 The Supplier undertakes to notify the Client, via the appointed contact persons for security issues set out in section 2 above (Contact persons for security issues), about the impossibility to implement any of the checks envisaged in the cloud controls matrix.

This commitment must be maintained even after entering into the Agreement.

14.4 The Supplier undertakes to prepare a specific documentation describing the internal management procedures of the changes in production and the related roles/rights/responsibilities within the Cloud.

14.5 The Supplier undertakes to implement open encryption methods (3.4AES, AES, etc.) to protect data in case they need to pass through public networks (e.g. Internet).

Intesa Sanpaolo KR MSA - Rev. ISP 15.02.2022 AB Execution Version 020322

Final Audit Report 2022-03-03

Created:	2022-03-03
By:	Kaizen People Team (people@kaizenreporting.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAKTzHAreMJsUIlJlUqxAOwq6LHN8GFAhF

"Intesa Sanpaolo KR MSA - Rev. ISP 15.02.2022 AB Execution Version 020322" History

Document created by Kaizen People Team (people@kaizenreporting.com)
2022-03-03 - 2:50:26 PM GMT- IP address: 52.19.175.132

Document emailed to Dario Crispini (dario.crispini@kaizenreporting.com) for signature
2022-03-03 - 2:51:11 PM GMT

Email viewed by Dario Crispini (dario.crispini@kaizenreporting.com)
2022-03-03 - 3:37:34 PM GMT- IP address: 52.19.175.132

Document e-signed by Dario Crispini (dario.crispini@kaizenreporting.com)
Signature Date: 2022-03-03 - 3:37:54 PM GMT - Time Source: server- IP address: 52.19.175.132

Agreement completed.
2022-03-03 - 3:37:54 PM GMT