Signicat Services Agreement For UK G-Cloud 15

PARTIES:

Signicat B.V. ('**Signicat**')
Weena 327-329
3013 AL Rotterdam
The Netherlands

Business registration number:
24444001

THE PARTIES ACCEPT THE FOLLOWING:

1. DEFINITIONS AND INTERPRETATION

1.1 The definitions used in this Agreement indicated with a capital letter, whether single or plural, shall have the meaning set out below unless otherwise stated:

Affiliate – means any entity within the Party's company group, consisting of one or more parent companies together with one or more subsidiaries. A company is a parent company if it, owing to agreement or as owner of shares, has determinative influence over another company either alone or jointly with another entity. A company shall always be deemed to have determinative influence if the company (i) has a majority of the votes in such other company, or (ii) has the right to elect or remove a majority of the members of the board of directors of such other company.

Agreement - means the terms and conditions of the body of this agreement (sections 1 up to and including 15) and all the Appendices combined which shall apply in addition to the G-Cloud 15 framework terms. In case of conflict the G-Cloud 15 framework terms shall prevail.

Commercial Terms – means the commercial terms applicable to the Services to be provided by Signicat as set out in appendix 1.

Confidential Information - means the terms of this Agreement, and any information and documentation disclosed by, or on behalf of, either Party to the other Party or its Affiliates, either directly or indirectly, in writing or in any other manner, relating to each Party's and its Affiliates' business, suppliers and/or customers, including without limitation information about the Services, finances, know-how, designs, ideas, concepts, rights, future plans, projects, a Party's, its Affiliate's or its supplier's Intellectual Property Rights, and any other information and documentation that would reasonably be considered to have a confidential nature.

Contract Year - means a year during the term of this Agreement whereas the first contract year starts on the Effective Date and lasts for 365 days thereafter.

Customer Application – means the web and/or mobile applications which integrate the Signicat Services through APIs to provide Signicat's Services to the Customer's End Users.

Effective Date – means the date of the last electronic signature.

End Users – means a user of either user-facing applications provided by Signicat or the Customer Application via internet or via intranet, unless otherwise stated.

Force Majeure Event- means any event or circumstance beyond the reasonable control of either Party, which could not have been reasonably anticipated or avoided and that prevents either Party from fulfilling its obligations under this Agreement. Such events may include, but are not limited to, natural disasters (e.g., earthquakes, floods, fires), war, civil unrest, acts of terrorism, pandemics or other public health emergencies, (attempted) cyberattacks (e.g. denial-of-service attacks (DoS), hacking (attempts) of the Services or its technology, changes in law or regulation, government actions, strikes or labor disputes (excluding those specific to the affected Party's workforce), general internet failure, line delays, power failure or faults of any machines, Signicat's supplier(s), Identity Issuer and/or Third Party Provider's force majeure or the unavailability of such supplier and/or its product or service as part of the Service due to another reason, a supplier of Signicat that is in bankruptcy or under any insolvency laws or for re-organization, receivership or dissolution or other events of similar nature.

Identity Issuer – means any applicable issuer of electronic identity, as listed in appendix 1 and further specified in appendix 4.

Intellectual Property Rights – means any copyrights, software, products, technology, adaptation rights, publishing rights, reproduction rights, rights to communicate to the public, public performances,

synchronization rights, rights to be named as creator of the work(s), artist names, patents, utility models, circuitry, rights of patent, design patents, designs, trademarks, trade names, service marks, brands slogans, commercial symbols, logos, other designations, inventions, trade secrets, know-how and/or any other industrial and/or intellectual property rights of whatever nature in any part of the world, and applications thereof whether registered or not, as well as any application to register any of the aforementioned rights.

Parties – means Signicat and Customer.

Party – means Signicat or Customer as the case may be.

Security Requirements – means the security standards applicable to the Signicat Services as set out in appendix 8.

Service Description – means the description of Signicat Services as described in appendix 2.

Service Level Agreement – means the service level agreement applicable to the Signicat Services as set out in appendix 3.

Services – means all the services ordered by the Customer from Signicat under this Agreement as described in appendix 1.

Service Specific Terms – means the additional terms and conditions as set out in appendix 7 that apply to Signicat Services.

Signicat Services – means the services as described in the Service Description as ordered by the Customer from Signicat under this Agreement. The Signicat Services do not include the services from Identity Issuers or Third-Party Providers.

Sub-Suppliers – means the third parties as listed in appendix 9.

Third-Party Provider – means a provider of certain software services that Signicat acts as reseller for, as listed in appendix 1 and further specified in appendix 5.

Transaction - Each of the technical steps in a process initiated by an End User or machines that the Customer controls and to which the Customer has enabled access to the Signicat Services. A transaction has occurred once a process is initiated within Signicat Services.

1.2 In the construction of this Agreement including its appendices, unless the context requires otherwise the below applies:

Appendices:	the appendices form part of this Agreement;
Headings:	headings appear as a matter of convenience and do not affect the construction of this Agreement;
Including:	referring to anything after the word “including”, “include” or “includes” does not limit what else might be included and any such reference is without limitation to what else might be included;
Related Terms:	where a word or expression is defined in this Agreement, other parts of speech and grammatical forms of that word or expression have corresponding meanings;
Singular and Plural:	the singular includes the plural and vice versa;
Writing:	a reference to "written" or "in writing" includes all modes of presenting or reproducing words, figures, and symbols in a tangible and permanently visible form, such as e-mail, and other electronic means.

2. AGREEMENT AND APPENDICES

2.1 This Agreement is made as of the Effective Date between Signicat and the Customer. The Agreement governs the provision of the Services by Signicat to the Customer.

2.2 This Agreement consists of the following appendices which are hereby incorporated by reference into this Agreement:

Appendix 1	*Commercial Terms*
Appendix 2	*Signicat Services Service Descriptions*
Appendix 3	*Signicat Services Service Level Agreement*
Appendix 4	*Identity Issuer terms and conditions*
Appendix 5	*Third-Party Provider terms and conditions*
Appendix 6	*Data Processing Agreement*
Appendix 7	*Signicat Services Service Specific Terms*
Appendix 8	*Signicat Services Security Requirements*

2.3 In the event of inconsistencies, the terms and conditions of the body of this Agreement (sections 1 up to and including 15) prevail over the appendices except if an appendix states otherwise, and the appendices shall have priority in the above mentioned order except if an appendix states otherwise. The Data Processing Agreement shall at all times prevail over any other appendix.

3. GRANT OF LICENSE

3.1 Signicat grants to the Customer a non-exclusive, non-transferable, revocable, limited right to use the Services for the purpose of allowing End Users to access and use the Services in accordance with and for the duration of the Agreement. The Customer shall not permit any other than the Customer and/or End Users to access and use the Services and shall therefore not sublicense the Services to a third party unless explicitly otherwise agreed in the Agreement.

3.2 The Customer shall take reasonable precautions necessary to prevent any distribution of the Services to any third party other than the Customer Affiliate in accordance with section 5.1 and the End User.

3.3 There are no implied licenses granted under this Agreement and all rights, save for those expressly granted to the Customer hereunder, are expressly excluded and shall remain with and belong to Signicat and/or its licensors.

4. SIGNICAT'S RIGHTS AND OBLIGATIONS

4.1 Signicat will allocate sufficient and necessary competence in order to ensure its performance under this Agreement. Signicat will provide the Signicat Services with due care and skill, by using personnel possessing the appropriate training and experience to perform the necessary activities in a professional manner and in accordance with this Agreement, taking into consideration security, confidentiality, and compliance with applicable rules.

4.2 Signicat will provide reasonable efforts to offer the support, maintenance and service levels for the Signicat Services in accordance with the Service Level Agreement. Customer acknowledges and agrees that any due and payable service credits in accordance with the Service Level Agreement are Customer's exclusive remedies.

4.3 Signicat will procure and maintain, at its sole cost and expense, adequate and customary liability insurance coverage for the Signicat Services.

4.4 Signicat shall be allowed to take (technical) measures to protect the Services, or with a view to agreed restrictions in the duration of the right to use the Services, and to prevent access to Service features that are not part of the Agreement. Customer shall not be allowed to remove or evade such (technical) measures. Signicat will not be responsible for any errors or issues in using the Services, resulting from Customer's non-compliance with the foregoing.

5. THE CUSTOMER'S RIGHTS AND OBLIGATIONS

5.1 The Customer's Affiliates shall also be entitled to access and use the Services in which case a reference in this Agreement to Customer shall, where relevant, deemed to be a reference to the Customer Affiliate. However, any disputes shall be settled by and between the Customer and Signicat as provided in this Agreement. The Customer shall be fully responsible and liable for the Affiliate's fulfilment of its obligations or lack thereof in relation to the Services under this Agreement.

5.2 The Customer is solely responsible for any implementation of the integration between the Customer Application and the Signicat Services including any modification, amendment or addition of any API or sample code.

5.3 The Customer shall not initiate and use web-service calls and other measures to check status on the Signicat Services. The Customer will upon notice from Signicat end such calls and other measures and will be charged at the rates set out in the Commercial Terms.

5.4 The Customer is responsible for and ensures that the data, documents and texts provided to Signicat by the Customer to be processed by Signicat in the course of providing the Services, are correct, complete, adequate and in compliance with applicable laws and regulations and do not infringe any rights of third-parties. Customer agrees and understands that any inadequate, incorrect or incomplete data will negatively impact the Service. Signicat will in no event be liable for any damage, loss or costs incurred by Customer due to its non-compliance with this section. Customer will indemnify Signicat and its Affiliates for any damage, loss or costs incurred by Signicat due to Customer's non-compliance with this section.

5.5 The Customer acknowledges and accepts that it, and therefore not Signicat, is fully responsible and liable if the Services provided by Signicat to the Customer, are impacted due to the Customer using a third party for the integration of the Services into their or the Customer's system and due to such third party supporting the Services. The Customer shall indemnify Signicat for any damages caused to Signicat due to the use by the Customer of such third party. Signicat's obligations under the Agreement apply to the Customer and do therefore not provide any rights to the third party that integrates the Services into their or the Customer's system.

5.6 The Customer shall report suspicious activity, security incidents, unauthorized access attempts, or policy violations.

5.7 Signicat shall provide Customer the possibility to set-up, install and configure the Signicat Services in a sandbox environment. Customer is at all times responsible for testing whether or not the Signicat Service is ready for operational use for the Customer.

5.8 The use of the sandbox account environment must be reasonable, fair and in good faith. Customer must not use it in a way that could damage, disable, overburden, impair or compromise Signicat's systems or security or interfere with other sandbox account users. It is not permitted to repeatedly and unnecessarily access the sandbox account using robots or other similar technologies.

5.9 Except as expressly permitted herein or by law, Customer shall not, and shall not allow any third party to, attempt to alter or decipher any transmissions to or from the servers or the Services or look to subvert or adversely affect the operation, code and/or functionality of the Services in production or sandbox, may it be by attempting to reverse engineer, modify, hack, penetration test, fault find, analyse, tamper with, copy, alter, disassemble, decompile, seek to upload or introduce any malicious code, bugs or any other malware of any sort or in other ways. Neither shall the Customer, nor shall it allow a third party to, copy, make error corrections or otherwise modify or adapt the Services or remove from or change any designation concerning copyrights, trademarks, trade names or other Intellectual Property Rights, including any indications concerning confidential nature and/or secrecy.

5.10 Customer will adhere to its responsibilities and will also follow up all reasonable instructions and guidelines issued by Signicat in connection with the Services and the Agreement.

5.11 In the event Signicat provides any accounts to the Customer, or allows Customer to use its own accounts, related to the Services, the use of such accounts and credentials by the Customer and its End Users is personal. The Customer must, and shall ensure that its End Users shall, keep the login factors and credentials strictly confidential and use these codes with due care. The use of said login factors shall be solely the responsibility and the risk of Customer. The Customer is responsible for the life cycle of the accounts, including removal if an End User no longer needs access, by self-service when possible or through Signicat's support when not. The Customer is responsible for setting its own password policies and ensuring an adequate level of security. The Customer shall always uniquely identify the End User and shall ensure that least privilege access is enforced. Customer shall report suspected credential breaches immediately.

6. FEES AND PAYMENT

6.1 All fees under this Agreement are set out in the Commercial Terms and shall be paid within the payment term as agreed upon in the Commercial Terms without claiming any rights of set-off, transfer cost, or counterclaim.

6.2 All fees under this Agreement are exclusive of customs, (financial) transfer costs, taxes, duties or excises in any form, all of which shall be borne by the Customer.

6.3 Payments that are overdue will be subject to the amount determined by applicable law pertaining to overdue payments, on the overdue balance. In the event that any payments are more than one (1) month overdue, Signicat may, at Signicat's discretion, upon notice to the Customer and without prejudice to any other rights and remedies and without liability to the Customer, suspend access to all or part of the Services until the invoices in question have been paid, except if and insofar the invoice is subject to a reasonable legal dispute between the Parties.

6.4 If part of the invoice is being disputed by the Customer, the undisputed part of the invoice shall be paid in accordance with the agreed upon payment term.

7. SECURITY AND COMPLIANCE

7.1 Parties shall perform their services and obligations under this Agreement in compliance with laws and regulations applicable to them. Signicat shall comply with the laws and regulations that apply to Signicat and to the offering of the Signicat Services by Signicat pursuant to this Agreement. Customer shall comply with the laws and regulations that apply to them and to the use of the Services. If Customer, as part of its usage of the Services, is obliged to follow specific laws and regulations, and this puts additional obligations or requirements on Signicat or the relevant Third Party Provider(s) or Identity Issuer(s) in respect of offering of the Services beyond what is already laid down in this Agreement, then Customer is responsible to inform Signicat of these specific laws and regulations. Signicat, and where applicable Third-Party Providers or Identity Issuers, must consent to comply with the additional obligations or requirements in advance and in writing and may charge reasonable cost related to compliance with such additional obligations and requirements.

7.2 Signicat provides the Signicat Services in accordance with the Security Requirements.

7.3 In particular, both Parties ensure to adhere to all applicable privacy laws and regulations pertaining to the

Signicat Services, including Regulation (EU) 2016/679 (the "**GDPR**"). The Parties will enter into the Data Processing Agreement, as set out in this Agreement.

7.4 In the event of security incidents, the Customer shall at all times immediately provide all cooperation requested by Signicat to investigate or rectify such incidents.

8. CONFIDENTIAL INFORMATION

8.1 The Party that receives Confidential Information shall keep it strictly confidential and limit access to such Confidential Information to only those of its employees, consultants, Affiliates, and any third parties and advisers to whom such access is reasonably necessary for the performance of this Agreement. The receiving party shall take all reasonable necessary actions to ensure that the companies and persons as referred to above respect the same level of obligations of confidentiality and non-disclosure as provided for in this Agreement.

8.2 The confidentiality obligations shall not apply to information that:

(i) was already in the possession of the receiving Party before receipt from the disclosing Party without an obligation of confidentiality;

(ii) was rightfully disclosed to the receiving Party by a third party without, as far as the receiving Party is aware of, a breach of any separate nondisclosure obligation;

(iii) is or becomes publicly available through no fault of the receiving Party (i.e. information in the public domain).

(iv) is independently developed by a Party without the use of the Confidential Information of the other Party as can be shown by documentary evidence.

8.3 Neither Party shall use or disclose to any other person or company than mentioned in this Confidential Information section, either during the term or after the termination of this Agreement, any Confidential Information except (i) in accordance with the other Party´s prior written consent or (ii) as required by law, court order, regulation, or governmental or regulatory agency provided that to the extent legally permissible and reasonably practicable the receiving Party makes commercially reasonable efforts to provide the disclosing Party with written notice of such disclosure as promptly as possible and uses reasonable efforts to limit such disclosure to the minimum required and obtain confidential treatment thereof.

8.4 All Confidential Information remains the property of the disclosing Party.

9. INTELLECTUAL PROPERTY RIGHTS

9.1 All Intellectual Property Rights belonging to a Party and its licensors as of the date of this Agreement, and all rights, title and interest to existing technology, products and works of each Party and its licensors and all accompanying and associated materials as of the date of this Agreement, shall remain exclusively with such Party or such Party's licensors.

9.2 All rights, title and interest to any Intellectual Property Rights in any Service, documentation or material provided or developed by Signicat or Signicat's licensors from time to time under this Agreement and all modifications thereto (whether made by Signicat, the Customer or third parties), shall remain exclusively with Signicat or Signicat's licensors. Customer acknowledges and agrees that it has no rights or claims of any type, other than the licenses granted under this Agreement, to the Services, all modifications (whether made by Signicat, the Customer, or third parties), trademarks, and the Intellectual Property Rights embodied therein. The Customer irrevocably waives and releases any claim to title and ownership rights (including copyright ownership) thereto and shall provide all reasonable assistance to ensure that the Intellectual Property Rights as referred to in this Intellectual Property Rights section shall vest in Signicat or the relevant Signicat licensor.

9.3 Customer shall not use any of Signicat's, Signicat's Affiliates, Third-Party Provider's, Identity Issuer's or Signicat's supplier's Intellectual Property Rights, for any other purpose than authorized in this Agreement. In particular, Customer shall not use such Intellectual Property Rights in order to promote its own business on web sites, in flyers or brochures, trade fairs, etc.

9.4 Neither Party or its Affiliates shall use the other Party's and/or its Affiliates name and logo as a reference on its or its Affiliates' website and marketing materials and campaigns without the prior written approval of the other Party.

10. INTELLECTUAL PROPERTY INDEMNITY

10.1 Signicat will defend at its own expense any suit or action brought against the Customer by a third party to the extent that the suit or action is based upon a third-party claim that the Signicat Services or the Customer's use thereof infringes such third party's Intellectual Property Rights. Signicat will pay those fees and costs associated with such suit or action (including reasonable costs for Customer to engage its own external legal counsel as well as costs pertaining to work to be performed by the Customer personnel due to such claim) and damages finally awarded provided that:

(i) the Customer promptly informs Signicat in writing of any such claim, demand, action or suit; and

(ii) Signicat is given control over the defence or settlement thereof and that the Customer co-operates in the defence or settlement. Signicat shall act reasonably and shall consult with the Customer before agreeing any settlement pursuant to this clause.

10.2 If a claim, demand, suit or action alleging infringement is brought, or Signicat believes one may be brought; Signicat shall at its expense choose one of the following options:

(i) modify the Signicat Services to avoid the allegation of infringement, while at the same time maintaining compliance with this Agreement;

(ii) obtain for the Customer at no cost to the Customer a license to continue distributing the Signicat Services in accordance with this Agreement free of any liability or restriction; or

(iii) if neither of the previous options are commercially feasible in Signicat's reasonable opinion, Signicat may terminate this Agreement with immediate effect upon written notice.

10.3 Notwithstanding the provisions above, Signicat shall have no responsibility for claims arising from:

(i) modifications of the Signicat Services by the Customer or any third party engaged by the Customer;

(ii) combination or use of the Signicat Services with the Customer or third-party hardware or software not supplied by Signicat and which Signicat could not reasonably have expected the Customer to use in relation to the Signicat Services and if such claim would not have arisen but for such combinations or use;

(iii) Signicat's modification of the Signicat Services in compliance with written specifications provided by the Customer;

(iv) use of other than the latest version of the Signicat Services provided to the Customer by Signicat if the use of the latest version would have avoided the infringement and Signicat has made the Customer aware of such fact; or

(v) use of the Signicat Services outside the scope of the rights granted to the Customer in this Agreement.

10.4 This Intellectual Property Indemnity section is subject to section 12 and states the sole liability of Signicat and the exclusive remedy of the Customer in connection with an infringement of Intellectual Property Rights.

11. WARRANTY DISCLAIMER

11.1 The Services are provided "as is" and "as available". Except as set forth in this Agreement, and to the extent permitted by law, Signicat disclaims all warranties, either express or implied, statutory or otherwise, including without limitation warranties of functionality, fitness for a particular purpose or non-infringement.

12. LIMITATION OF LIABILITY

12.1 Signicat is not liable towards (a) the Customer and (b) Customer's Affiliates for:

(i) errors or delays caused by the use of Identity Issuer services and Third-Party Provider services as further defined in Appendix 1, 4 and 5 or any other breach of the Agreement caused by the Identity Issuer or Third-Party Provider or its services;

(ii) loss caused by deficiencies in Services that are caused by the Customer's acts or omissions.

12.2 Neither Party shall be liable to the other Party in contract, tort, breach of statutory duty, indemnity, or otherwise, whatever the cause thereof, for any loss of data, profit, business or goodwill or any other indirect and/or consequential damages of any kind arising under or in connection with this Agreement.

12.3 The total and maximum liability of a Party during a Contract Year shall in no event exceed an amount equal to the total fees paid by the Customer to Signicat for the Services provided under this Agreement and Transaction contemplated by this Agreement during the 12 months preceding the first event that incurs liability in the relevant Contract Year.

12.4 The Parties acknowledge and agree that the purpose of the limitation of liability is to allocate and cap risk between them, and no provision of this Agreement (including any indemnity or compensation obligation) shall be construed so as to circumvent or override that limitation, except where such exclusion would render the limitation unenforceable at law.

12.5 The exclusions and limitations of liability of this limitation of liability section do not apply in case of death or injury to persons or to damages attributable to intent or gross negligence.

13. FORCE MAJEURE AND HARDSHIP

13.1 Any delay or failure in performance under this Agreement by the affected Party arising from a Force Majeure Event shall not be considered a breach of this Agreement, nor shall it give rise to any liability for damages,

penalties, or other claims against the affected Party.

13.2 The Party affected by a Force Majeure Event is entitled to suspend its obligations under this Agreement for the duration of the Force Majeure Event and shall take all reasonable actions to mitigate the impact of such suspension. The affected Party shall resume the performance of its obligations under this Agreement as soon as reasonably possible after the Force Majeure Event ceases to exist.

13.3 If the Force Majeure Event continues for a period exceeding 90 days, either Party may terminate this Agreement by giving 30 days written notice to the other Party. In the event of such termination, neither Party shall be liable to the other for any damages or losses incurred as a result of such termination, except for obligations that accrued prior to the Force Majeure Event.

13.4 If, due to circumstances beyond the reasonable control of Signicat — including but not limited to substantial increases in infrastructure, energy, or compliance costs, material changes in exchange rates, taxes, or applicable laws, or other events that fundamentally alter the commercial balance of this Agreement (each a "Hardship Event") — the continued provision of the Services becomes excessively onerous, Signicat may notify the Customer and request good faith negotiations to adjust the affected terms (including pricing, scope, or performance obligations) to restore that balance. Pending the outcome of such negotiations, Signicat may reasonably suspend the affected obligations, and if the Parties fail to reach agreement within thirty (30) days of such notice, Signicat may terminate the affected portion of the Agreement, or the Agreement in full if materially impacted, without liability. This Hardship section applies to circumstances that do not constitute a Force Majeure Event but render performance commercially impracticable.

14. TERM AND TERMINATION

14.1 This Agreement may be terminated by either Party at any time if the other Party is in material breach of any term or condition of this Agreement and such breach continues unremedied for a period of thirty (30) days after the Party in breach has been notified of such breach by the other Party by means of a written notice. A breach under the Service Level Agreement is not considered to be a material breach.

14.2 This Agreement may be terminated by either Party in the following cases: in accordance with the force majeure section above, if a receiver is appointed for the other Party or its property, if the other Party makes an assignment for the benefit of its creditors, any proceedings are commenced by, for or against the other Party under any bankruptcy, insolvency or debtor's relief law, or actions are taken to liquidate or dissolve the other Party.

14.3 Signicat shall have the right to terminate the Agreement at any time without being liable for any costs or damages on Customer's side in the event of Customer's non-compliance with, or due to Signicat having to comply with, sanction lists or any regulation thereof.

14.4 Upon expiration or termination of this Agreement:

(i) The Customer shall immediately cease its use of the Services and related Intellectual Property Rights, and all licenses granted under this Agreement shall expire;

(ii) Signicat undertakes to deliver to the Customer all information that is stored at/with Signicat or in Signicat's possession or control that the Customer requests and that is of relevance for the Customer, provided that Signicat reserves the right to charge the Customer on a time and material basis for such requests;

(iii) Each Party will return to the other Party or destroy (if so, authorized in writing by the other Party) all Confidential Information concerning the other Party in the respective Party's possession or control, and

(iv) Each Party shall immediately cease all use of the other Party's trademarks.

15. MISCELLANEOUS

15.1 This Agreement shall not be altered, modified or amended, except in writing executed by both Parties.

15.2 No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.

15.3 This Agreement is made solely between, and is for the sole benefit of, the Parties and their permitted successors, and no other person or entity shall have any rights or remedies under or by reason of this Agreement. The Customer's Affiliates and End Users shall therefore not have any direct rights against the Signicat, and Signicat shall have no obligations to them under this Agreement.

15.4 Signicat may transfer, assign and novate this Agreement without the prior written consent of the other Party to an Affiliate.

15.5 The notices or other communications shall be effective upon receipt and shall be deemed to be received by a Party: (i) if delivered personally or sent by courier, upon delivery at the address of the relevant party; (ii) upon

verification of receipt via e-mail, or; (iii) if sent by registered letter, unless actually received earlier, on the third business day after posting.

15.6 The Parties acknowledge that their relationship shall be that of an independent contractor, and nothing contained in this Agreement shall be construed as establishing any agency, employment relationship, partnership or joint venture between Signicat and the Customer. The Parties shall represent themselves to all third parties and neither Party has the right to bind the other in any manner whatsoever.

15.7 Signicat's rights to be paid and Customer's obligations to pay Signicat all amounts due hereunder, as well as the Definitions, Confidential Information, Intellectual Property Rights, Warranty Disclaimer and Limitation of Liabilities sections and the relevant articles of the Terms and Termination and Miscellaneous sections and any other section of this Agreement that by their nature survive the termination of this Agreement shall survive termination of this Agreement.

15.8 Each of the Parties to the Agreement expressly represents and warrants to the other Party that it has full power and authority to enter into the Agreement and has not assigned, encumbered, or in any manner transferred any of the claims covered by the Agreement.

15.9 This Agreement shall be governed by and construed in accordance with Dutch law with the exclusion of the United Nations Convention on Contracts for the International Sale of Goods. References to any legislation in this document are construed as references to such legislation as amended or re-enacted or as otherwise modified from time to time. Any dispute, controversy or claim arising out of or in connection with this contract, or the breach, termination or invalidity thereof, shall be settled by the courts of Rotterdam. Parties shall however attempt in good faith to resolve promptly any dispute arising out of or relating to this Agreement by negotiation. If any provision of this Agreement is declared invalid by any court or tribunal, the remaining provisions of this Agreement shall remain in effect and Parties shall try to come to an alternative provision that will be as close as possible to and replace the invalid provision.

15.10 This Agreement, including any order forms, constitutes the entire agreement between the Parties and supersedes all prior agreements as to the Services. This Agreement has been duly executed by both Parties by way of electronic signature.

APPENDIX 1 – COMMERCIAL TERMS

As per G-Cloud 15 Framework Agreement and Call-Off Contract

APPENDIX 2 – SERVICE DESCRIPTION

As per G-Cloud 15 Framework Agreement and Call-Off Contract

APPENDIX 3 – SIGNICAT SERVICES SERVICE LEVEL AGREEMENT

As per G-Cloud 15 Framework Agreement and Call-Off Contract

APPENDIX 4 - IDENTITY ISSUER TERMS AND CONDITIONS

Not used in G-Cloud 15 Framework Agreement

.

APPENDIX 5 - THIRD-PARTY PROVIDER TERMS AND CONDITIONS

Services of Third-Party Providers

Subject to the terms and conditions as set out and referred to below, the Customer may use the services of the Third-Party Providers as referred to in Appendix 1.

Third-Party Provider terms and conditions

(i) The Customer acknowledges and agrees that the Third-Party Provider terms and conditions as set out in this Appendix, which includes Third-Party Provider specific terms and conditions ("**Third-Party Provider Terms**"), apply in addition to and prevail in the event of a conflict over the relevant parts of the rest of this Agreement.

(ii) The Customer acknowledges and accepts that the Third-Party Provider may change the Third-Party Provider Terms. Consequently, the Customer acknowledges and accepts that the Third-Party Provider Terms as set out in this Agreement may be changed accordingly.

(iii) The Customer further acknowledges and agrees that Signicat can only offer the identification data or software for as long as Signicat has a valid agreement with the Third-Party Provider in question, in the absence of which the relevant Third-Party Provider services shall be terminated without Signicat incurring any liabilities. Signicat shall in that case and where possible suggest an alternative Third-Party Provider service replacing the terminated one.

(iv) Signicat is not liable towards (a) the Customer and (b) Customer's Affiliates for errors or delays caused by the use of Third-Party Provider services as further defined in Appendix 1 and this Appendix 5 or any other breach of the Agreement caused by the Third-Party Provider or its services, except if and insofar Signicat is able to successfully claim the losses and damages of the Customer and Customer Affiliates occurred as a consequence thereof from the relevant Third-Party Provider.

(v) The terms and conditions applicable to support, maintenance and availability in Appendix 3 do not apply to the services from the Third-Party Providers. Signicat will provide support and maintenance services for the services from Third-Party Providers only to the extent Signicat receives the corresponding support and maintenance services from the Third-Party Provider in question. Such support and maintenance services will be provided by Signicat after the Customer has made a request to Signicat pursuant to the Agreement. The Customer can be provided with the terms and conditions applicable to support, maintenance and availability for each of the Third-Party Providers upon request. However, for the avoidance of doubt, such terms and conditions apply between Signicat and the Third-Party Provider in question, and therefore only provide an indication of the support, maintenance and availability that the Customer may receive through Signicat. Consequently, such terms and conditions do not constitute a binding legal obligation on Signicat or the respective Third-Party Provider.

IPROOV TERMS

ARTICLE 1. IPROOV SERVICES

Introduction

iProov Limited ("iProov") has a service called "Onboarding Service" which enables facial verification.

Description of the Onboarding Service

The Onboarding Service consists of a hosted software-as-a-service platform ("Platform"), the capabilities of which can be consumed through appropriate use of the defined API endpoints in conjunction with SDKs and iProov software that facilitates access to the Platform ("Front-end Software"). References to "Onboarding Service" in these terms include SDKs and Front-end Software.

Onboarding Service

The Onboarding Service consists of:

1. Enrolment - Enrol request with face image to enrol a trusted user against a secure pseudonym using a photo containing a face image. This request is orchestrated via the ReadID SaaS Server as defined in the ReadID Services Specific Terms to the Agreement; thus the Customer does not initiate this request directly to iProov:
   a. the submission of a single image via trusted server-server connection, which complies with the minimal requirements for photo enrol;
   b. subsequent enrolment of the trusted user image against the secure pseudonym.
2. Verification - Subsequent request to verify an End User against a secure pseudonym:
   a. capture and transmission to iProov servers of imagery of the End User, by an SDK or other Front-end Software provided and licensed by iProov and running on the End User device;
   b. analysis of the received End User imagery to determine the likelihood that the End User is:
      i) the person whose image is enrolled in the source face image; and

ii) the person present in front of the End User device at the time of transmission;
c. comparison of these likelihoods with one or more threshold levels, producing a result of pass or fail;
d. communication of this pass/fail result, together with other information, including an image of the End User, by means of a secure internet channel.

A maximum of three verification requests is allowed for each enrol request.

Versions of the Onboarding Service
The Onboarding Service is available in two versions related to how the Onboarding Service determines if the person is present in front of the End User device (step 2 b (ii) above): Dynamic Liveness and Express Liveness. Whether one or both versions are part of the Agreement is specified in the commercial terms section.

Dynamic Liveness (formerly known as "Genuine Presence Assurance")
The Onboarding Service can be used for Dynamic Liveness (DL). DL is designed to detect different types of spoof attacks including, using artefacts or images presented to the camera, synthetic videos or replayed imagery of previous verification sessions injected into the device sensors. iProov's proprietary Flashmark method uses controlled illumination, with light generated by the device screen, to create a set of unique signals from the light patterns reflected from the End User's face. This enables a judgement to be made about the genuineness of the End User's biometric.

The sequence of colours that illuminate the End User's face is unique on each verification attempt. This sequence is determined by a code generated on servers deployed by iProov and sent to the device shortly before authentication begins. The combination of the End User's face and the unique illumination sequence creates a short video which is captured and sent to iProov during the scanning process. This represents a "One-Time Biometric", which is not intended to be reused and is intended to be difficult to forge.

Express Liveness (formerly known as "Liveness Assurance")
The Onboarding Service can use the Express Liveness ("EL") technology. For EL the system asks the End User to align his/her face in front of the camera of the device. Visual feedback is provided to the End User during the alignment process. As the End User aligns his/her face a small number of frames are captured. These frames are then processed by a number of subsystems which aim to establish whether the appearance of the face in front of the camera, and the change in the appearance across the frames, are consistent with a bonafide user or an attack. In addition, the frames are processed by the face matching system which compares the appearance of the face against a stored enrolled face image.

The Onboarding Service using EL is intended to determine whether an End User performing a facial verification transaction is a real person, and the same person that was enrolled with the enrolled image.

Article 2 Requirements

The photographic portrait image must:
a. conform to international standard ISO/IEC 19794 Information technology — Biometric data interchange formats — Part 5: Face image data (supporting ICAO 9303 passports and ISO 18013 Driving Licences);
b. be substantially in focus and un-obscured by flare or watermarks; and
c. have a minimum of 85 pixels between the eyes.

The link between the End User device and the iProov servers must be 500kb/s or faster. The End User device must be equipped with a screen and front-facing camera, running Android 5.0 or above, or iOS 12 or above, and must not be on a list of excluded devices.

The list of excluded devices, and of devices with known issues, for the Onboarding Service is at https://github.com/iProov/android/wiki/Known-Issues.

The Onboarding Service has capacity constraints. These constraints are expressed as a maximum number of requests to the iProov endpoints, being maximum 1 Transaction per second and 12 Transactions per minute. iProov is entitled but not obliged to reject ("throttle") any Transactions that would cause the maximum number of requests to endpoints to be exceeded. Customer can request Signicat to increase or change the capacity constraints. Signicat can charge extra fees for adhering to such a request and is under no obligation to agree to such a request.

Customer acknowledges and accepts that in the event the requirements are not met, the Onboarding Service cannot be provided.

Customer will update the relevant Onboarding Service SDKs within a reasonable period (and in any event not more than six (6) months after the release by iProov of the Onboarding Service SDKs version in question), and thus also update its offering in the App Store, Play Store and other outlets. Where iProov acknowledges (acting

reasonably) that a new version of the Onboarding Service SDKs that it releases is not reasonably fit for purpose, the above mentioned reasonable period will be suspended until such time as the issuing of that SDK with the relevant failures is corrected. Signicat shall inform the Customer of such a situation.
Access to the Onboarding Service for versions of Onboarding Service SDKs that are not on the latest release may be blocked, but only if there is a technical or security reason to do so.

Article 3 Ceasing support

Customer acknowledges that iProov shall be entitled to cease the support of (a) third party operating systems (such as an iOS or Android version) with which the Onboarding Service interacts where this is commercially appropriate and/or because of security concerns and/or because of technical concerns (and unless there is an urgent technical or security reason threat that reasonably inhibits this, the cessation of such support will be announced at least three months in advance), and (b) to bring to an end support and the facility to use specific SDKs and APIs (for which unless there is an urgent technical or security reason threat that reasonably inhibits this iProov will provide six months' notice of cessation).

Article 4 Personal Data

Customer acknowledges and accepts that iProov processes Personal Data in the United Kingdom in order to provide the Onboarding Services.

Customer is controller and iProov is a sub-processor, with regard to providing the Onboarding Service.

Personal data processed by iProov

iProov is a Sub-processor, providing their Onboarding Service. It retains records of facial verifications to enhance customer service, maximise performance for users and mitigate risks arising from attack.

Retained records enable iProov to:

- evolve and improve the systems that are designed to provide protection and verification.
- support the customer service processes of our clients.
- undertake forensic investigation on attacks or suspected breaches.

The standard data retention period for Onboarding Transactions not suspected to be fraudulent is 30 days. Transactions identified as potentially fraudulent, which are likely to contain evidence of attacks and images of attackers, are normally retained for one year (unless deemed genuine).

The longer retention period for potentially fraudulent Transactions and certain other data denoted below is to help detect patterns of experimental attack by criminals. These can occur at a low frequency over an extended period. Sophisticated criminals are likely to try to experiment undetected by exploiting short retention periods, and a longer retention period is intended to help protect users and the customers against such threats.

Description of Data	Personal Data	Special Category Personal Data	Onboarding: Data deletion for Personal & Special Category Personal Data	Purpose
Enrol Photo		X	Normal: 30 days	1) To enable identification and help in the prevention of potentially fraudulent activity not identified at the time of capture. 2) Non-repudiation - to allow forensic investigation of the validity of a verification is challenged.
Enrol Photo		X	Normal: 30 days	1) To enrol and or verify a user 2) To enable identification of and analysis of potentially fraudulent activity not identified at the time of capture. 3) To allow forensic investigation of the validity of a verification/enrollment if challenged. 4) To monitor and improve system performance 5) Non-repudiation - to allow forensic investigation if the validity of a verification is challenged.
Verification video and images		X	Potentially Fraudulent: 1 year or until there are no	1) To enrol and or verify a user.

			longer reasonable grounds to believe the claim is fraudulent.	2) To enable identification of and analysis of potentially fraudulent activity not identified at the time of capture. 3) To allow forensic investigation of the validity of a verification/enrollment if challenged. 4) To monitor and improve system performance. 5) To help in preventing fraudulent attempts against the data controller & data subject.
Biometric template (can be used for matching but not to regenerate the initial imagery)		X	6 months	1) To enrol and/or verify a user. 2) To allow audit and investigation of suspected fraudulent authentication attempts. 3) To help prevent fraudulent attempts by or against the data subject or data controller. 4) To monitor and improve system performance.
Pseudonymised username provided by Signicat	X		Anonymisation is accomplished by deletion of this parameter by Signicat and/or customer	To allow biometric profile to be linked to enroll and/or verification attempts
Internal iProov identifier to pseudonymised username provided by customer	X		Ceases to be personal data when Pseudonymised username is anonymised	Associating data to Pseudonymised username
api_key identifier provided to the device by iProov – cannot be used to identify any other user activity	X		6 months	To permit linking of multiple authentication session attempts by a single user for the purpose of fraud detection, analysis and performance monitoring
private_key identifier provided to the device by iProov– cannot be used to identify any other user activity	X		6 months	To permit linking of multiple authentication session attempts by a single user for the purpose of fraud detection, analysis and performance monitoring
Internal identifier provided by iProov to identify device api_key	X		Ceases to be personal data when api_key is deleted	Associated data to api_key
IP Address of the User on the User's network	X		12 months	1) To help in the prevention of potentially fraudulent activity not identified at the time of capture. 2) To allow troubleshooting and support. 3) To help prevent fraudulent attempts by or against the data subject or data controller. Note: Customer and/or Signicat can choose not to have IP addresses visible to iProov by running all traffic via a reverse proxy.

Sub-processors for the Orchestrated Service Provider service provision by iProov:

Name and Company House Number	**Address**	**Registration country**	**Outsourcing Type**	**Outsourcing function**	**Data Location**
Microsoft Ireland Operations Limited 256796	South County Industrial Park, Dublin 18, Ireland	Ireland	Public Cloud Provider	Hosting of iProov Servers	EEA
iProov Limited 07866563	14 Bank Chambers, 25 Jermyn Street, London	United Kingdom	Subcontractor	Facial verification	EEA, United Kingdom
Google Ireland Limited 368047	Gordon House, Barrow Street, Dublin 4, Ireland	Ireland	Public Cloud Provider	Hosting of iProov Servers	EEA

Amazon Web Services EMEA SARL B186284	38 Avenue John F. Kennedy, L-1855 Luxembourg	Luxembourg	Public Cloud Provider	Hosting of iProov Servers	EEA

VERIFF TERMS

Article 1. Service description

1.1 Veriff ÖU ("Veriff") provides through Signicat verification and fraud prevention services as set forth in the Service Description and as agreed between Parties ("**Veriff Document Verification Service**").

1.2 Customer is aware and accepts that the quality of data and the quality of verification by using the Veriff Document Verification Service will be considerably lower than by using ReadID NFC.

1.3 When the Veriff Document Verification Service is combined with facial verification which is orchestrated by Signicat, the Veriff Document Verification Service can be used to extract and crop the face image from the document and the facial verification can be applied based on that cropped face image. For clarity, section 1.2 above also applies to the cropped face image.

1.4 Industry Cross links are an optional feature.

Article 2. Definitions

2.1 The definitions used in these Veriff terms shall have the meaning set out below or as defined in the body of the Agreement:

Customer Data	means the content and data that the Customer, either directly or indirectly through Signicat, makes available to Veriff through the Veriff Document Verification Service;
Customer Personal Data	means any personal data contained in the Customer Data, including but not limited to: (i) the names and contact details of the End Users; (ii) details of the End Users' documents (identification document, driver's license, utility bill, as relevant), including photo of the document, document type, number, date of issue and date of expiry, content of extracted fields depending on the chosen Veriff Document Verification Service features; (iii) photographs, videos and audio recordings of the End Users captured via the Veriff Document Verification Service; (iv) facial biometric data relating to the End Users; (v) the results of the identity verification / authentication process conducted through the Veriff Document Verification Service; (vi) the End Users' device's and Veriff Document Verification Service usage data, including the duration of the End User's use of the Veriff Document Verification Service, activity in the Veriff Document Verification Service, IP address, domain name, software and hardware attributes, general geographic location (e.g. city, state, country); and (vii) any other personal data that Veriff processes on behalf of the Customer in connection with the Customer's use of and access to the Veriff Document Verification Service;
Restrictive Activities	means products, services, content, and activities, including the sale, manufacture, distribution, or promotion of, and related to: pornographic or sexually explicit information, firearms, alcohol, tobacco, or other recreational drugs, and medical cannabis;
Sanction Laws	means sanctions administered or enforced by the OFAC, the United States Nations Security Council, the European Union, including, without limitation, designation on OFAC's Specially Designated Nationals and Blocked Persons List or OFAC's Foreign Sanctions Evaders List or any other sanction laws, rules or regulations that may apply to the Veriff Document Verification Service;
Sanction List	means any list of international sanctions administered or enforced by the OFAC, the United Nations Security Council, the European Union, including, without limitation, designation on OFAC's Specially Designated Nationals and Blocked Persons List or OFAC's Foreign Sanctions Evaders List or any other applicable list of sanctioned, embargoed, blocked, criminal, or debarred persons maintained by any U.S. or non-U.S. Government;

Service Description:	the Veriff Document Verification Service descriptions, which is currently found at https://www.veriff.com/service-description/ver-VSD-2301 (or such successor site), which may be amended from time to time. Data extraction may comprise cropping of the face image from the identity document.

Article 3. Use of the Veriff Document Verification Service

3.1 The Customer must notify Signicat when it is engaged in Restricted Activities. Signicat and Veriff may object to the use of the Veriff Document Verification Service within Restricted Activities on reasonable grounds and justification.

3.2 The Customer recognises and understands that Veriff is constantly innovating the Veriff Document Verification Service and finding new ways to improve it with new features and services. The Customer acknowledges and agrees that no warranties, representations or other commitments are given in relation to the continuity of certain functionalities of the Veriff Document Verification Service; provided, however, that Veriff warrants that it will not materially decrease the overall functionality of the Veriff Document Verification Service.

3.3 In the event Signicat or Veriff reasonably and in good faith suspects that the Customer and/or End User(s) are in material breach of the Agreement, then Signicat will provide notice to the Customer of such suspected material breach; provided, however, that in the event Signicat or Veriff reasonably and in good faith suspect that the material breach will result in an ongoing or persistent violation of applicable law, then the Customer acknowledges, that Signicat, and where relevant Veriff, may disable access to all or any part of the Veriff Document Verification Service by Customer and/or End User, without prejudice to other rights under the Agreement. Upon remediation of the suspected material breach, Signicat, and where relevant Veriff, may re-enable access to the Veriff Document Verification Service.

3.4 Signicat, and where relevant Veriff, have the right to suspend the Veriff Document Verification Service without prejudice to any other rights and remedies available, without any prior notification, if:

(a) the Customer, or the End User is in a material or persistent breach of any of terms of the Agreement;

(b) Veriff's Intellectual Property Rights are infringed in any way;

(c) Customer or the End User breaches any relevant applicable law;

(d) Customer or the End User is, in the opinion of Signicat or Veriff, engaged in any fraud or dishonesty or act in a way which, in the opinion of Signicat or Veriff, may bring or is likely to bring Signicat or Veriff into disrepute or is materially adverse to the Signicat or Veriff interests.

Article 4. Customer obligations

4.1 Customer will not (a) make or give any representations, warranties or similar promises about the Veriff Document Verification Service to any third party, including its End Users, unless otherwise agreed to with Signicat in writing, (b) make the Veriff Document Verification Service available to, or use the Veriff Document Verification Service for the benefit of, anyone other than Customer, (c) access, store, distribute or transmit any virus through the Veriff Document Verification Service, (d) reverse engineer, modify, adapt, copy, duplicate, reproduce, create derivative works from, frame, mirror, hack, or otherwise attempt to gain unauthorized access to the Veriff Document Verification Service or its related systems or networks, (e) sublicense, resell, timeshare, or similarly exploit the Veriff Document Verification Service, (f) access the Veriff Document Verification Service in order to build a competitive product or service, or (g) authorize or permit the End User or any third party to engage in the aforementioned activities.

4.2 Customer will (a) remain responsible for individuals, including End Users', use of the Veriff Document Verification Service in compliance with the Agreement, (b) promptly notify Signicat upon becoming aware of any unauthorized access or use of the Veriff Document Verification Service, (c) obtain and maintain all necessary licenses, notices, consents, and permissions (specifically including, to the extent applicable, notice and consent to collect and use biometric data) necessary for Customer to provide the Veriff Document Verification Service to End Users under the terms of the Agreement, (d) use the Veriff Document Verification Service only in accordance with applicable laws and regulations (including, but not limited to, any laws relating to the collection and retention of biometric data, such as the Illinois Biometric Information Privacy Act (BIPA) and the Texas Capture and Use of Biometric Identifiers), (e) be responsible for the legality of any Customer Data, and (f) use the Veriff Document Verification Service only in accordance with the Service Description. Upon request from Signicat, Customer will provide evidence that any required notices and consents referenced in (c) herein were provided or collected (as applicable). In the event Customer becomes aware of any known or reasonably

suspected breach of this section, then Customer shall promptly notify Signicat, and shall promptly remediate the breach.
4.3 The Customer hereby represents and warrants that the Customer has all necessary rights, titles and consents, in each case as necessary to allow Signicat and Veriff to use the Customer Data in accordance with the Agreement. The Customer shall be responsible to maintain a backup of the Customer Data (where applicable) and Signicat nor Veriff shall be responsible or liable for the deletion, correction, alteration, destruction, damage, loss, or failure to store any Customer Data.
4.4 Customer confirms to have adopted reasonable risk-based procedures to ensure that Customer will not cause Signicat or Veriff to violate applicable economic, trade or financial Sanctions Laws. In that regard, in the absence of general or specific authorizations under applicable laws, Customer has adopted reasonable risk-based procedures to ensure that Customer will not cause Signicat or Veriff to facilitate, directly or indirectly, transactions involving: (i) any national or resident of or entity formed under the laws of or located in any country or region subject to Sanction Laws; (ii) any person who appears on any Sanctions List; (iii) any entity that is 50% or more owned, individually or in the aggregate, directly or indirectly, by, is controlled by (including without limitation by virtue of such person being a director or owning voting shares or interests), or acts, directly or indirectly, for or on behalf of, any person or entity on a Sanctions List; or (iv) any entity or individual that is otherwise the subject of any applicable sanctions, suspensions, or embargoes. Customer shall, subject to applicable law, notify Signicat, in writing and immediately upon discovery, of any known or suspected violation of the Sanctions Laws in relation to the Veriff Document Verification Services, including providing notification (a) with regard to any transaction facilitated by or involving Veriff that is confirmed to have involved an individual or entity subject to the descriptions in sections (i) through (iv) of this section for which there is no apparent authorization under applicable law; and (b) if the known or suspected violation is committed by Customer or any of its officers, directors, investors, employees, contractors, senior managers, partners, owners, principals or any agent acting on behalf of Customer.
4.5 The Customer grants Signicat, Veriff and their Affiliates a worldwide, non-exclusive, limited term licence to access, copy, perform, distribute, display, download, and use Customer Data (a) exercise its rights and obligations under the Agreement, (b) to provide, maintain, and update the Veriff Document Verification Service, (c) to prevent or address service or technical problems, or at Customer's request in connection with a support request, and (d) producing statistical reports and research in an anonymised and aggregated manner that cannot identify the Customer, nor the End Users (whereas such output forms part of Veriff's intellectual property).
4.6 Customer shall inform Signicat and Veriff on any notice of security incident to the public or End Users beforehand.

Article 5. Processing of Personal Data

5.1 Veriff applies bias mitigation measures appropriate to the Veriff Document Verification Service. Upon request by Customer to Signicat, Veriff may provide reasonable assistance to the Customer with regard to the measures applied.
5.2 By purchasing Industry CrossLinks or a functionality that is part of the Veriff Document Verification Service that includes Industry Crosslinks, Customer consents to Veriff using Customer Personal Data for Industry Crosslink checks for other Veriff customers in the same industry.
5.3 Veriff has the right to delete, blur or make unreadable in any other way the personal data or identification documents presented during the verification session that are not necessary for the provision of the Veriff Document Verification Service unless specifically agreed otherwise for Customer.
5.4 In any case, after 14 calendar days as of the date of termination of the Agreement, personal data processed by Veriff shall no longer be available.
5.5 Customer is controller and Veriff is a sub-processor, with regard to providing the Veriff Document Verification Service.
5.6 Customer acknowledges and accepts that Veriff provides follow the sun support.

Personal data processed by the Orchestrated Service Provider (Veriff)

The below table provides an overview of the Personal Data that is processed by the Orchestrated Service Provider, supplemental to what Signicat processes itself. Where below it says Customer this can, when applicable, also mean the Customer's customer.

Topic	Answer
Subject matter of the processing of personal data	Veriff shall process Customer Personal Data only as necessary to provide the Orchestrated Service pursuant to the Agreement and as further instructed in a documented manner by the Customer in its use of the Orchestrated Service.
The categories of personal data to be processed and transferred	Customer Personal Data as is processed pursuant to the Agreement and the DPA. Note that for the provision of the Orchestrated Service, no special categories of personal data are transferred to the Customer (i.e. no biometric data). Veriff will process all Customer Personal Data submitted to the Orchestrated Service during a Session. For clarity, regardless of the Orchestrated Service purchased, if Customer Personal Data is submitted to the Orchestrated Service, that information will be processed by Veriff in the provisioning of the Orchestrated Service during the Data Retention Period.
	For managing the Customer relationship, the Parties make its representatives work related contact details available to each other. Also, the Parties' exchange of the Customer's representatives work related contact details.
The categories of data subjects to whom personal data relates	Data subjects whose personal data is made available by the Customer to Veriff, including, but not limited to: End Users and natural persons authorized by the Customer to use the Orchestrated Service.
	Customer's representatives
Special categories of personal data to be processed.	Biometric data used for the Orchestrated Service provision, such as amongst others for 1-n identification and age estimation as part of Veriff Orchestrated Service and Risk Labels as described in Annex 1.
Data Retention Period	Customer acknowledges that Veriff's data retention practices vary by Orchestrated Service offering and by type of Personal Data submitted to the Orchestrated Service. Veriff's data retention practices are detailed https://www.veriff.com/data-retention/ver-VDR-2301. Except as otherwise agreed in writing by the parties, the retention timelines specified below for the IDV Service and in the Data Retention Page for the particular features / services that are not a component of the IDV Service will apply. The default retention period for IDV Service offered to new Customers signed after the effective date of this amendment is: (i) 30 days within the Orchestrated Service for all Customer Personal Data; and (ii) 0 days in archive for Customer Personal Data. Parties agree that the customized retention period stipulated in the previous sentence is not applicable to (i) the Orchestrated Service/Feature "Backup" available in the Data Retention Page and (ii) the Customer Personal Data retained for current Customers which entered into Order Forms prior the effective date of this amendment and/or which renew the Order Form after the effective date of this amendment, unless agreed otherwise upon renewal.
Restrictions and safeguards applicable to special categories of personal data	As a rule, no personal data belonging to special categories of personal data is being transferred to the Customer.
The frequency of the transfer	Data transfer is ongoing for the duration of the Agreement
Purpose(s) of the data transfer and further processing	Data transfer is necessary for the provision of the Orchestrated Service.
	Data transfer necessary for managing the mutual relationship and assistance as agreed upon in the DPA.
Nature of the transfer	In the context of the Orchestrated Service, the transfer mainly constitutes of making the End User's personal data available to the Customer in Veriff's Customer back office and allowing the Customer to download / request extraction of all of the End User related data visible in the Customer back office.

	In the context of managing the Customer relationship, the transfer mainly constitutes of making the Parties's and the Customer's representatives work related contact details available to each other during mutual communications

Sub-processors for the Orchestrated Service Provider service provision by Veriff:

Name and Company House Number	Address	Registration country	Outsourcing Type	Outsourcing function	Data Location
Google Cloud EMEA 368047	Gordon House, Barrow Street, Dublin 4, Ireland	Ireland	Public Cloud Provider	Media processing services	EEA
Amazon Web Services EMEA SARL B186284	38 Avenue John F. Kennedy, L-1855 Luxembourg	Luxembourg	Public Cloud Provider	Provides storage, computing and media processing	EEA
Twilio Ireland Limited*	25-28 North Wall Quay, Dublin 1, Ireland	Ireland	Communications	Provides end-user communication solutions	EEA, storage in US
Messente Communications OÜ*	Akadeemia tn 3, 51003 Tartu, Estonia	Estonia	Communications	Provides end-user communication solutions	EEA, transfer for third country networks
Hotjar Limited	Dragonara Business Centre, 5th Floor, Dragonara Road, Paceville St Julian's STJ 3141, Malta	Malta	Development	Facilitates fixing bugs and improving client UX	EEA
Veriff ÖU	Niine tn 11, Põhja-Tallinna linnaosa, 10414 Tallinn, Harju maakond, Estonia	Estonia	Subcontractor	Provide functions for Veriff's identity verification service provision	EEA
Veriff Spain S.L.	Avenida Diagonal 123, 00805 Barcelona, Spain	Spain	Subcontractor Affiliate	Provide functions for Veriff's identity verification service provision	EEA
Veriff UK Ltd	at 9th Floor, 107 Cheapside, London, EC2V 6DN, United Kingdom	UK	Subcontractor Affiliate	Provide functions for Veriff's identity verification service provision	UK
Veriff Inc.*	251 Little Falls Drive Wilmington, New Castle County Delaware 19808-1674 State of Delaware, United States	USA	Subcontractor Affiliate	Provide functions for Veriff's identity verification service provision	US

* Sub-processor will not be used when the Customer is based in the EEA or United Kingdom.

APPENDIX 6 - DATA PROCESSING AGREEMENT

PARTIES: the Controller and the Processor

THE PARTIES HAVE AGREED UPON THE FOLLOWING:

1. **DEFINITIONS**

1.1 Unless otherwise stated in this DPA, the definitions used herein shall have the meaning given to it in the body of the Agreement or as per below:

DEFINITIONS	
Agreement	means the agreement between the Controller and the Processor for the provisioning of the Services to which agreement this DPA is added as Appendix 6.
Applicable Data Protection Law	means all applicable laws and regulations governing privacy, data protection and the processing of Personal Data including, to the extent applicable but not limited to, the UK General Data Protection Regulation (the "**UK GDPR**") and the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**") and any national legislation implemented under the UK GDPR and GDPR.
Controller	means the legal entity determining, alone or jointly with others, the purpose for and the means of the processing of Personal Data: in the Agreement also referred to as the **Customer.**
Data Subject	means an identified or identifiable natural person whom or about whom Personal Data is collected.
DPA	means this Data Processing Agreement.
Personal Data	means any information relating to an identified or identifiable natural person processed by the Processor on behalf of the Controller.
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.
Processor	means the legal entity processing Personal Data on behalf of the Controller pursuant to this DPA: in the Agreement also referred to as **Signicat**.
Sub-Processor	means a third-party engaged by the Processor to process Personal Data.

2. **SCOPE AND PURPOSE OF THE DATA PROCESSING**

2.1 The Processor shall process Personal Data on behalf of the Controller only for the purpose of performing the tasks imposed on the Processor by the Controller pursuant to the Agreement.

2.2 Controller shall ensure that the content, the use and the instructions for the processing of Personal Data by Controller through Processor as intended in the Agreement is not unlawful, is in compliance with all applicable legislation, including but not limited to the Applicable Data Protection Law, and does not infringe on the rights of any third party. Controller will indemnify and hold Processor harmless against any and all claims of third parties, those of the data protection authority in particular, resulting in any way from not complying with this guarantee.

2.3 This DPA covers any category of Personal Data processed by the Processor in providing the Services to the Controller under the Agreement. A specification of the subject matter and duration of the processing, the type of Personal Data the Processor will process, the category of Data Subjects involved as well as the nature and purpose of processing is set out in the Personal Data Checklist as attached to the DPA.

2.4 Controller will provide all information required by Processor to meet its obligation to maintain a complete record of all categories of processing activities carried out on behalf of Controller.

3. CONTROLLER'S INSTRUCTIONS

3.1 The Processor shall process Personal Data only on documented instructions from the Controller, unless required to do so by applicable law to which the Processor is subject. In this case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this. Subsequent instructions may also be given by the Controller throughout the duration of the processing of Personal Data. These instructions shall always be documented.

3.2 The Processor shall immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringes Applicable Data Protection Law.

4. TRANSFER OF PERSONAL DATA

4.1 The Processor shall ensure that any transfer of Personal Data shall be done in accordance with the relevant and applicable transfer mechanisms as set out in Applicable Data Protection Law.

4.2 If the processing carried out by the Processor should include the transfer of Personal Data to a third country which is not recognised by the European Commission to have an adequate level of protection in accordance with Applicable Data Protection Law, the Controller and the Processor and/or where relevant the Processor and Sub-Processor shall, if other applicable transfer mechanisms do not apply, enter into the relevant and applicable module of the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the Applicable Data Protection Law.

4.3 Notwithstanding the foregoing, the Processor may disclose Personal Data, and therefore process and /or transfer Personal Data to a third country or an international organization, if required by Applicable Data Protection Law, in which case the Processor shall notify the Controller of such legal requirement before processing, unless the law in question prohibits such information.

5. ASSISTANCE TO THE CONTROLLER

5.1 The Processor shall notify the Controller without undue delay of any request it received from a Data Subject in relation to Personal Data processed under the Agreement. The Processor is allowed to inform the Data Subject about such notification to the Controller. Apart from that, the Processor shall not respond to the Data Subject's request except on the documented instructions of the Controller or as required by applicable law to which the Processor is subject, in which case the Processor shall to the extent permitted by the applicable law inform the Controller of that legal requirement before the Processor responds to the request.

5.2 The Processor shall, if reasonably requested by the Controller and where reasonably possible for the Processor and to the extent necessary, assist the Controller in:

(i) fulfilling its obligations regarding the Data Subject's requests to exercise their rights;
(ii) conducting the necessary data protection impact assessments pursuant to the Applicable Data Protection Law;
(iii) consulting the relevant supervisory authority prior to processing where the data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate such risks;
(iv) the obligation to ensure that Personal Data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the Personal Data it is processing is inaccurate or has become outdated;
(v) as far as applicable, the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing of Personal Data under the Agreement; and
(vi) where relevant, the notification of the relevant supervisory authority and/or Data Subject in case of a Personal Data Breach.

5.3 Signicat is allowed to charge Customer for costs associated with the assistance provided by Signicat in accordance with this section 5

6. USE OF SUB-PROCESSORS

6.1 The Processor shall ensure that any Sub-Processor is bound by terms ensuring a similar level of data protection to the terms of this DPA. The Processor shall remain fully responsible to the Controller for the performance of the Sub-Processor's obligations in accordance with its agreement with the Processor.

6.2 As of the Effective Date, the Controller agrees that the Processor has engaged the Sub-Processor(s) listed in the Agreement. The Processor is responsible towards the Controller for the engaged Sub-Processors.

6.3 The Processor may not use a new Sub-Processor without notifying the Controller in writing at least 30 days before the new Sub-Processor starts processing any Personal Data. The Controller may, within 90 days after being notified of the engagement of a new Sub-Processor, object to the engagement by terminating the Agreement if it can demonstrate that the new Sub-Processor will not meet the requirements set out in the Applicable Data Protection Law. This termination right is Controller's sole and exclusive remedy if Controller objects to any new Sub-Processor. The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object.

7. SECURITY AND CONFIDENTIALITY

7.1 The Processor shall fulfill the requirements for technical and organisational security measures stipulated in the Applicable Data Protection Law. The Processor shall at least implement the technical and organizational measures as specified in the Security Requirements.

7.2 The Processor and the Processor's personnel shall observe confidentiality regarding the processing of Personal Data and any documentation accessed under this DPA. The Processor shall not disclose Personal Data in any way to any employee or third party without the prior written approval of the Controller, except where (i) the disclosure is in accordance with the instructions from the Controller, where (ii) Personal Data needs to be disclosed to a competent public authority to comply with a legal obligation, or (iii) the disclosure is in accordance with the Agreement and this DPA. This section shall survive expiration or termination of this DPA.

7.3 The Processor shall take reasonable steps to ensure the reliability of any personnel and Sub-Processor who may have access to Personal Data processed pursuant to the Agreement and this DPA, ensuring in each case that access is strictly on a need-to-know basis.

8. INSPECTION AND AUDITS

8.1 The Processor conducts an annual audit by an independent auditor to assess the Processor’s compliance with Applicable Data Protection Law and this DPA.

8.2 The Processor shall, upon the Controller’s reasonable prior written notice, submit its relevant processing systems and supporting documentation to demonstrate compliance with its obligations under this DPA and the Applicable Data Protection Law. The Processor shall also allow for and contribute to inspections and audits that the Controller or an auditor mandated by the Controller may require for the review of such compliance. In the event of any such inspection or audit, the Processor shall provide reasonable assistance to the Controller on a time and material basis.

8.3 If an inspection or audit reveals or confirms that processing pursuant to this DPA is unlawful or otherwise conducted in a manner not compliant with the Applicable Data Protection Law, the Parties shall take immediate action to ensure future compliance with the Applicable Data Protection Law.

9. NOTIFICATION OF DATA BREACHES

9.1 The Processor shall, without undue delay after becoming aware of it, notify the Controller of a Personal Data Breach. Such notification shall contain, at least:

(i) A description of the nature of the Personal Data Breach including the categories and approximate number of Data Subjects and Personal Data records concerned;
(ii) The contact details where further information about the Personal Data Breach can be obtained;
(iii) The likely consequences of the Personal Data Breach; and
(iv) The measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, measures to mitigate its possible adverse effects.

9.2 If and insofar it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

9.3 The Processor shall cooperate with the Controller and take such reasonable commercial steps as instructed by the Controller to assist in the investigation, mitigation and remediation of Personal Data

Breaches involving the Processor.

9.4 Processor is never held to report a Personal Data Breach with the Data Protection Authority and/or the Data Subject. Processor will not be responsible nor liable for the (timely and correctly) notification obligation to the relevant supervisor and/or Data Subjects, as meant in Section 33 and 34 GDPR.

10. LIABILITY

10.1 Subject to the limitations of liability of the Agreement, the Processor is liable solely for claims, costs (including reasonable expenses for legal services), loss, fines, expenses or damages incurred by the Controller as a result of the Processor's breach of this DPA, including non-compliance with the Applicable Data Protection Law.

11. TERM AND TERMINATION

11.1 This DPA is effective as from the Effective Date of the Agreement and will remain in effect as long as the Processor processes Personal Data on behalf of the Controller under the Agreement and it expires without further notice after the Processor fulfilled its obligations under section 11.4 and 11.5.

11.2 In the event of a material breach of this DPA and/or Applicable Data Protection Law the Controller has the right to instruct the Processor to suspend the processing of Personal Data with immediate effect until the breach has been cured or the processing of Personal Data terminated.

11.3 The Controller has the right to terminate the Agreement if:

(i) The processing of Personal Data by the Processor has been suspended by the Controller pursuant to section 11.2 and if the breach is not cured within reasonable time;
(ii) The Processor is in material breach of this DPA and/or Applicable Data Protection Law;
(iii) The Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding the processing of Personal Data under this DPA.

11.4 In case of expiry or termination of the Agreement, the Processor shall, at the Controller's request, return all Personal Data and copies thereof to the Controller or delete or destroy in a secure and definite/irreversible manner, insofar reasonably possible, all Personal Data and upon request certify that it has done so.

11.5 The Processor may continue to retain Personal Data after expiry or termination of the Agreement and this DPA if strictly necessary to comply with laws applicable to the Processor, or if Personal Data is stored in backup and it will constitute a disproportionate effort to delete such backup before deletion occurs in accordance with the Processor's ordinary backup routines. If so, the Processor will only securely store, but not actively use, such retained Personal Data, and the Processor shall for such retained Personal Data continue to comply with this DPA.

11.6 The obligations laid down in this Data Processing Agreement which, by their nature, are designed to continue after termination, will remain in force also after the termination of this Data Processing Agreement.

12. CONTACT INFORMATION

Notifications pursuant to this DPA shall be submitted in writing to:

For Controller:

Name:	<<contactinfo_Name>>
Position:	<<contactinfo_Title>>
Phone number:	<<contactinfo_MobilePhone>>
Email:	<<contactinfo_Email>>

For Processor:

Name:	Privacy team
Email:	**privacy@signicat.com**

PERSONAL DATA CHECKLIST

This checklist states the details of processing Personal Data by Signicat.

Purpose of processing: provisioning of the Signicat Services to enable the Customer to authenticate or identify the End User or obtain certain information about a person.

Nature of processing: the Signicat Services are provided as Software-as-a-Service using Signicat's hosting providers as listed in this Agreement.

Categories of data subjects: End Users, persons authenticating or identifying themselves with the Customer or persons of which the Customer obtains certain information (example: Customer's customer, employees of the Customer)

Categories of Personal Data: the following Personal Data is processed according to the Data Processing Agreement.

Personal name	
Personal contact information (Address, e-mail, phone number, etc.)	
Reference number / Customer number / Employee number	
Date of birth	
Information on next of kin	
Information about children	
National identity number / Social security number	
Details of insurance	
Financial information	
Medical or health information	
Genetic data	
Biometric data	
Information about sexual relationships	
Information relating to litigation and criminal offenses	
Information on racial or ethnic background	
Information on political, philosophical or religious beliefs	
Information on union membership	
Device or connectivity information (IP address, device fingerprint, mobile phone subscription, etc.)	
PEP status, sanction status, adverse media or criminal records	
Family information	
Comments/ Additions not found above	

The selected personal data information is hereby confirmed by signing the Agreement.

APPENDIX 7 – SERVICE SPECIFIC TERMS

Unless otherwise stated in this Appendix, the Service Specific Terms set out in this Appendix apply in additions to the terms and conditions of the body and the Appendices (except for Appendix 4 and 5) to this Agreement. The Service Specific Terms prevail in the event of a conflict with the other terms.

READID SERVICE SPECIFIC TERMS

1 DEFINITIONS

1.1 The definitions used in these ReadID Service Specific Terms shall have the meaning set out below or as defined in the body of the Agreement:

Application(s)	means the mobile software application(s), (i) developed by Customer with the ReadID SDK, (ii) installed on a mobile device used by an End User, and (iii) that communicate(s) with the ReadID SaaS server;
Data	means any and all data processed by the Customer through use of the ReadID services, including but not limited to the Machine-Readable Zone or Visual Inspection Zone of scanned identity documents and/or the content of the contactless chips. Data may include personal data. Data explicitly does not include ReadID Analytics Data;
Documentation	means the documentation, including API documentation, technical guides and manual, for the use of ReadID (which may be amended by Signicat from time to time);
ReadID (Technology)	means the Signicat technology described in these ReadID Service Specific Terms enabling a Customer to process Data for its internal identity document interpretation and/or verification purposes. The definition of ReadID includes but is not limited to all ReadID programs, database structure, Documentation, source codes, object codes, variations, memory maps, algorithms, plans, charts, graphs, and other materials now or hereafter relating to or incorporated therein together with all future revisions to or updates thereof and all technical and operating manuals and any other Documentation relating to it. The definition includes the ReadID SaaS Server, ReadID SDK, ReadID API and ReadID Ready App. The definition does not include the Application or Data;
ReadID Analytics Data	means the anonymous aggregated analytical statistics regarding the use of ReadID by Customer and/or its End Users. These analytical statistics do not include personal data;
ReadID API	means the technical interface linked to the ReadID SaaS Server which allows the Customer to use ReadID;
ReadID Ready App	means an application that may be provided by Signicat and which is installed by End User on request of Customer on a mobile device of an End User, which communicates with the ReadID SaaS Server;
ReadID SDK	means a Software Development Kit (SDK) that may be provided by Signicat to Customer to enable Customer to develop its own Application(s) which communicates with the ReadID SaaS Server;
ReadID SaaS Server	means the ReadID server, on which the ReadID Technology is installed and running, provided by Signicat to Customer as a service (Software-as-a-Service), hosted in the public cloud, and includes a management portal;
Requirements	means the technical requirements with respect to the ReadID Technology, necessary to be able to use the ReadID service, or other technical or functional limitations as further specified in these ReadID Service Specific Terms and/or the Documentation;
Test(ing) Document(s)	means documents which can be made available by Signicat for use in testing by Customer, that resemble from an ICAO NFC chip and MRZ perspective genuine identity documents (passport, identity card, residence permit).

2 SERVICE DESCRIPTION

Signicat can provide the ReadID services as described below. Which of those services are part of the Agreement is described in the Commercial Terms.

ReadID SDKs
ReadID SDKs are so-called native SDKs. ReadID provides 2 types of SDKs: ReadID VIZ for capturing the Visual Inspection Zone and Machine-Readable Zone, and ReadID NFC for reading and verification of the chip.

On iOS and Android the default version of the SDK is the SDK UI that implements a best-practice user experience and unhappy flow handling including screens, animations and user guidance. For exceptional cases

which require an SDK without user guidance, the SDK Base must be used. Use of the SDK Base must be explicitly contractually agreed in the Commercial Terms due its increased implementation complexity.

ReadID SDK version	SDK Type	SDK name
SDK UI (default)	ReadID VIZ	VIZ SDK UI
	ReadID NFC	NFC SDK UI
SDK Base	ReadID VIZ	VIZ SDK Base
	ReadID NFC	NFC SDK Base

ReadID Ready App
The ReadID Ready App is a ready-to-use app. It implements MRZ scanning and NFC reading, with the verification of the chip being done at the ReadID SaaS Server. The Customer has to implement a website and/or app to get a ReadID Ready App token from the ReadID SaaS Server, and use this to initiate the ReadID Ready App.

The ReadID Ready App can be provided in three different versions (Basic, Branded, Enterprise).

ReadID Ready App Version	Description
ReadID Ready App Basic	The Basic version of the ReadID Ready App does not contain any branding for the Customer. The Basic version of the ReadID Ready App is provided to End Users by Signicat via the Play Store and/or App Store using Signicat's or an Affiliates', ReadID branding.
ReadID Ready App Branded	The Branded version of the ReadID Ready App extends the Basic version in that it displays Customer branding after the ReadID Ready token is known (for example after a QR scan). The Customer needs to configure the branding via the management portal.
ReadID Ready App Enterprise	The Enterprise version is provided in the Play Store and/or App Store using Customer branding and does not display any ReadID branding (white label). Unless agreed otherwise, the Enterprise version is provided in the Play Store and/or App Store under an account of the Customer. The Customer is responsible for setting up the account and the app listing. The Customer will provide developer accounts to the Play Store and/or App Store for Signicat to upload new ReadID Ready App versions. The Customer is responsible for the actual promotion of the new version to production. The Customer will promptly do this when a new version is available, after doing appropriate testing. The Customer understands that if this is not done promptly that the ReadID Ready App may not work properly or not work at all. The exact procedure is described in the Documentation and Signicat may change this over time.

ReadID SaaS Server
The Application and ReadID Ready App connect with the ReadID SaaS Server which is provided to the Customer as a SaaS solution, including an API and management portal. The Customer must use the management portal to configure the Application and/or ReadID Ready App. Signicat may impose Transaction limits of the use of the ReadID SaaS Server for performance or other reasons. The Customer is provided with separate accounts for production and non-production use. The latter is referred to as sandbox or pre-production, and production use is strictly not allowed on pre-production.

The ReadID SaaS Server is provided in 2 versions:

ReadID SaaS Server version	Description
Multi-tenant (default)	Other Customers are using the same environment.
Single-tenant	The environment will not be shared with other Customers.

Use of the Single-tenant must be explicitly contractually agreed in the Commercial Terms due its increased implementation complexity.

Capturing the Visual Inspection Zone and Machine-Readable Zone
The ReadID VIZ SDK or the ReadID Ready App enables the End User to use the device camera of their mobile device to capture the Visual Inspection Zone (VIZ, also called data page), including a scan of the Machine-

Readable Zone, of ICAO DOC 9303 compliant identity documents (TD1, TD2 and TD3) and ISO18013 compliant electronic driving licenses using Optical Character Recognition (OCR) technology. When relevant and configured, this is both front and back data page. Customer can only use the ReadID VIZ SDK as part of a session in which ReadID NFC (or an optical verification service from a Third-Party Provider, Identity Issuer service or Signicat, if applicable) is also used, or is expected to be used by the End User.

Reading and verification of the chip
The ReadID NFC SDK and/or ReadID Ready App enables the End User to read the contactless chips in identity document that are ICAO 9303 compliant, such as electronic passports, identity cards and residence cards. The verification and interpretation of the data in the chip is done by ReadID SaaS Server.

Specifically, ReadID implements for ICAO 9303 compliant identity documents:

- the Basic Access Control security mechanism;
- the PACE access control security mechanism (PACE-GM and PACE-IM with key derived from the Machine Readable Zone or from the Card Access Number);
- the Passive Authentication security mechanism (HT, DS and CS);
- the Active Authentication security mechanism;
- the Chip Authentication (EAC-CA) security mechanism; and
- the reading and interpretation of the chip content: DG1 (personal and document information), DG2 (face image), D7 (written signature, if present), DG11 (additional personal information, if present), DG12 (additional document information, if present) and DG13 (issuing authority dependent, if present).

In addition, ReadID implements the reading and verification of the contactless chip in Dutch electronic driver's licences (ISO 18013 compliant)). Specifically, ReadID implements for Dutch electronic driving licences:

- the Basic Access Protection security mechanism;
- the Passive Authentication security mechanism;
- the Active Authentication security mechanism;
- the Chip Authentication (EAC-CA) security mechanism and
- the reading and interpretation of the chip content: DG1 (personal and document information), DG6 (face image) and DG11 (additional personal information).

Signicat provisions as part of the ReadID SaaS Server with reasonable efforts a list of country certificates that it considers trusted and are used for verification purposes. This list is provided as-is, and it is the responsibility of the Customer to decide to trust or not trust these country certificates. New country certificates may be missing, or some countries may not provide their country certificates in a manner that Signicat can include them in a trusted manner. At request of the Customer Signicat provides information on the sources of the country certificates. The process of gathering the certificates may change at the discretion of Signicat. Any and all use of the list provided by Signicat is at all times for Customer's own account and risk.

ReadID NFC Light
The NFC capability of ReadID can be provided in a Light version which means that the NFC capability is limited to chip reading and interpretation of the chip content. There are no verification capabilities available and the raw data groups are not available to the Customer. The ReadID SDK UI and ReadID Ready App support ReadID Light. SDK Base does not.

Digital Travel Credential verification
The ReadID SaaS Server can verify and interpret eMRTD-bound Digital Travel Credentials - Virtual Component (DTC-VC) that are ICAO 9303 conformant. Unless specified otherwise, each DTC-VC uploaded to the ReadID SaaS Server is billable as a Transaction.

Android support
ReadID functions for Android 7.0 and higher, on smart phones and tablets with NFC. Signicat will stop supporting Android versions when this is commercially unreasonable and/or because of security concerns and/or because of technical concerns. The Customer will be notified through the change log of this. Unless there is an urgent technical or security reason that reasonably inhibits this, dropping support for an Android version will be announced at least one month in advance.

Problems may occur with specific smart phones due to the NFC implementation, or with new Android versions. In that case, if possible and commercially reasonably, ReadID will be updated. Examples of problems are phones that do not support NFC-B. There may be smart phones or tablets on which ReadID does not function or functions less efficiently.

Signicat is not responsible nor liable for ReadID not functioning properly in the situations described above.

iOS support

ReadID will work on the current iOS version and one version lower, unless there are specific reasons to not support this one version lower. As an exception, ReadID will not work for iOS versions below 15. There may be iPhones and iPads on which ReadID does not function, or not function properly, because the NFC capability is not present or not suitable, including problems with certain types of identity documents.

Signicat is not responsible nor liable for ReadID not functioning properly in the situations described above.

Supported identity documents
There may be identity documents that are not, or not fully, standard compliant or otherwise cause problems when scanning, reading or verifying them. In that case, if possible and commercially reasonably, ReadID will be updated. For some documents Signicat may not have the correct country certificate to be able to execute passive authentication. Some identity documents may not work with certain smart phones or tablets.

Signicat is not responsible nor liable for ReadID not functioning properly in the situations described above.

Test Documents
Test Documents can be made available, for use in testing by Customer. Using these Test Documents for anything other than testing or demo-ing a system with ReadID is not allowed.

Unless otherwise specified, Test Documents are from the invented jurisdiction “Utopia” and, when chipped, signed by a country certificate from Utopia that is configured to be acceptable in ReadID non-production servers, but not configured to be accepted in production servers.

Test Documents can be configured with certain personal and document data as provided by Customer, specifically name, date of birth, date of expiry and face image. Test Documents can be provided to fail a specific security mechanism, for example, cloning detection always fails. The face image can be the face image of the actual tester, so the typically subsequent step of face verification will pass.

In the event that customization to a Test Document is requested which is not possible in the current configuration, then Customer and Signicat will discuss if Signicat can still provide such customization, and Signicat will charge the costs involved in such customization (only after explicit email consent from Customer). Since availability of Test Documents depends on suitable chips being available in the market, Signicat is never obliged to provide Testing Documents.

3 CUSTOMER'S AND SIGNICAT’S RIGHTS AND OBLIGATIONS

3.1 Signicat may at all times and at its own discretion upgrade and update ReadID, including the ReadID SDK, ReadID Ready App and ReadID SaaS Server and inform the Customer thereof in accordance with the Service Level Agreement.

3.2 Customer will, where applicable, update to the latest version of ReadID SDK and ReadID Ready App on the mobile device within 2 (two) months after release of the latest version (the “Current SDK or App Release”), and thus also update its Applications, and if applicable the ReadID Ready App Enterprise, in the App Store, Play Store or similar. Customer accepts the risks and responsibility if Customer is not on a Current SDK or App Release, including degraded performance.

3.3 Signicat may at all times and at its own discretion block access to the ReadID SaaS Server for versions of the Applications, ReadID SDK and ReadID Ready App that are not on Current SDK or App Release. Signicat will inform the Customer before doing so. Customer understands and accepts that in incidental cases versions other than the Current SDK or App Release may not be interoperable with the ReadID SaaS Server because of security and/or technical reasons, requiring an immediate update.

3.4 In case the Customer is on a single-tenant ReadID SaaS Server and delayed server updates or upgrades for more than 1 (one) month, then Customer accepts the risks and responsibility for not being on a current ReadID SaaS Server release, including degraded performance.

3.5 Signicat shall not be liable for any claims, damages or costs arising out of any availability, reliability, timelines, quality, suitability and quality of the App Store, Play Store or similar. Customer shall indemnify, defend, and hold harmless Signicat from any claim, proceeding, loss or damages resulting from and/or related to any availability, reliability, timelines, quality, suitability and quality of the App Store, Play Store or similar.

3.6 Customer acknowledges that the ReadID services are subject to export controls under the laws and regulations of the United States, the United Nations Security Council, the European Union, Her Majesty’s Treasury

from the United Kingdom and other countries (as applicable), and that the ReadID services may include technology controlled under export and import regulations, including encryption technology. Customer agrees to comply with such laws and regulations.

3.7 Signicat may provide the Customer with third-party software or may deliver third-party software to the Customer as part of the ReadID SDK and/or ReadID Ready App. That third-party software may be governed by the open-source licence conditions or other conditions of those third parties that may be relevant for the Customer. If Customer rejects those third-party conditions, Parties will negotiate in good faith a viable solution. If Parties do not agree on a viable solution, Customer may terminate the Agreement.

3.8 This third-party software does not comprise software or material, which is subject to license terms such as the GNU General Public License, whereby the combination of an open-source software with a non-open-source software shall entail that the combination of software shall be open source ("viral effect"). A list of third-party software is provided in the Documentation provided with each version of the ReadID SDK and ReadID Ready App. Parties do not consider the following, non-exclusive list, open source licenses to have a viral effect: LGPL, Apache 2.0, MIT, BSD, Unicode License Agreement – data files and software, OpenSSL License, SSLeay.

3.9 By using the ReadID service, Customer grants Signicat a free, unencumbered, non-exclusive, perpetual license to use anonymous Data in connection with both improving the ReadID service and/or statistical purposes, including to create ReadID Analytics Data.

3.10 Customer is responsible for meeting the Requirements. Signicat is not responsible nor liable for ReadID not functioning properly when the Requirements are not adhered to.

3.11 ReadID Analytics Data shall not be returned to the Customer or destroyed by Signicat upon termination of the Agreement and shall be Signicat's Intellectual Property Right.

4 CONFIGURATION

4.1 If ReadID SDK is provided as part of this Agreement, then Customer is responsible for the development of an Application and responsible for the configuration thereof. If the ReadID Ready App is provided as part of this Agreement, then Customer is responsible for the configuration thereof.

4.2 Signicat shall provide Customer the possibility to set-up, install and configure the ReadID services in a pre-production environment. Customer is at all times responsible for testing whether the ReadID service is ready for operational use.

5 SERVICE LEVEL AGREEMENT

5.1 The Service Level Agreement set out in Appendix 3 only applies to production use of ReadID. Support for non-production use, e.g., demos or testing, is limited to the Service Level Agreement Basic Support Period and is provided as-is.

APPENDIX 8 – SECURITY REQUIREMENTS

1 SCOPE AND PURPOSE

The following information security requirements apply to Signicat's processing of Customer's data or otherwise delivery of the operational services by Signicat to Customer.
These requirements shall ensure that Signicat handles all Customer information with security in mind, and Signicat delivered services are protected to ensure confidentiality, integrity and availability.

2 INFORMATION SECURITY GOVERNANCE

Signicat shall have a documented Information Security Management System (ISMS) aligned with ISO 27001:2022 (or subsequent versions), or a set of policies to that effect, and Signicat shall, prior to entering into this Agreement and subsequently upon Customer's request and reasonable advance notice, provide documentation thereof to the Customer.
The ISMS, or set of policies, shall have top level management commitment.
Signicat shall have a documented risk management process, with supporting procedures and controls that are effective and operational.

3 ISMS REQUIREMENTS

Signicat's ISMS, or set of policies, shall as a minimum have the following requirements implemented, and Signicat shall, prior to entering into this Agreement and subsequently upon Customer's request and reasonable advance notice, provide documentation thereof to the Customer.

3.1 Organization of Information Security

Information security responsibilities must be defined and allocated.

3.2 Information Asset Management

Customer Information assets shall be identified, classified and protected according to their classification.

3.3 Human Resources Security

A background check shall be completed for all full-time, part-time employees and temporary consultants.

3.4 Access Control

The principle of least privilege shall be applied, both in design and implementation of access controls and provisioning of user and system access rights.
Requirements for access control to a system or Customer's information shall be aligned with the information classification of the assets to be protected.
A formal process for user registration and de-registration shall be used.
A formal process for user access provisioning shall be used.
User IDs of users who have left the organization shall immediately be disabled or removed.
When a user changes role or responsibilities in the organization, any assigned access rights that are no longer needed shall be removed.

3.5 Operations Security

There must be written operating procedures for all systems that process, store or in some other way handles Customer's information. The procedures shall ensure that the Customer's information is handled and stored in compliance with information security policies, regulatory requirements and contractual obligations including protection of its availability, confidentiality, authenticity, and integrity.
Changes to the organization, business process, information processing facilities, supplier relationships, internal processes and systems that affect information security shall be controlled.
Development, testing, and operational environments shall be separated, logically or physically.
Backups shall be taken of all relevant information according to availability and integrity requirements, taking confidentiality requirements into account.
Appropriate logging, monitoring, and auditing facilities to enable acting on security events shall be employed.
Event logs of user activities, exceptions, faults and information security shall be kept in systems and networks that is, or contains, Customer's information. These logs shall be reviewed regularly.
Measures to limit attacking surfaces, using techniques such as sandboxing, firewalling and server hardening shall be implemented.
All changes to operational software, applications and program libraries shall be performed by trained administrators.
All software shall be tested, approved and undergo a risk assessment prior to installation.
All updates and changes to systems, software, application and program libraries shall be recorded.

3.6 Incident Management

There shall exist procedures for incident management.
All employees and contractors shall report information security events and weaknesses to point of contact as quickly as possible.
All information security incidents and weaknesses shall be reported to interested parties as quickly as possible.
The analysis and resolving of all incidents shall be evaluated to reduce the likelihood or impact of future incidents.
All information security incidents, and the response, shall be recorded.

3.7 Physical and Environmental Security

Physical areas that contain Customer's information and information processing facilities shall be defined, classified, and documented.
For locations that contain Customer's information and information processing facilities the following shall be in place:

1. Windows and doors of such areas shall be closed and locked at all times and restricted to authorized personnel only and visitors shall always be accompanied.
2. Such access for authorized personnel shall be annually reviewed, shall be updated when necessary, and revoked when necessary.
3. An intruder detection system shall be active when the physical location is unattended, and this system shall be tested annually.
4. The intruder detection system shall be connected with a guard central that offers guard dispatch.
5. An audit trail of access to the area or facilities shall be securely maintained and monitored.

4 SECURITY TESTING

Signicat shall conduct relevant periodical security testing of its systems.
Signicat shall, upon Customer's request and reasonable advance notice, provide documentation that such test has been conducted, with the result. The information related to other customers or details from findings which could not, in any conceivable way, impact the security of the Customer's information or the services under this Agreement in the result may be masked.
The Customer may perform security tests against Signicat's solutions upon Signicat's approval.

APPENDIX 9 – LIST OF SUB-PROCESSORS

Business Name	Company Registration Number	Address	Service	Processing	Data Location
Signicat AS and affiliates (available upon request)	NO989584022	Beddingen 16, 7042 Trondheim, Norway	Delivery of Signicat Services and data processing.	End user personal data, as defined in the DPA Appendix Checklist with the Processor.	EU/EEA, UK
Amazon Web Services EMEA SARL	B186284	38 Avenue John F. Kennedy, L-1855 Luxembourg	Hosting of ReadID Servers	End user personal data, as defined in the DPA Appendix checklist with the Processor	UK or EU/EEA
Google Ireland Limited	368047	Gordon House, Barrow Street, Dublin 4, Ireland	Hosting services and core systems	Alternative for End User Personal Data as defined in the DPA Appendix Checklist	UK or EU/EEA