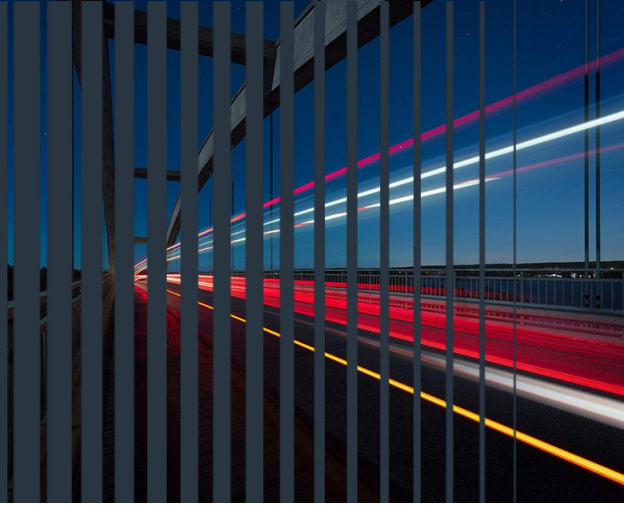
SIGNICAT



Software as a Service agreement

PARTIES:

Signicat AS ("Signicat")
Gryta 2 B
7010 Trondheim
Norway

You ("Customer")
User of Signicat Products or Services

Business registration number:
989 584 022 MVA

These Terms & Conditions (the "**Agreement**") between Signicat and you (the "**Customer**") (each a "**Party**", collectively the "**Parties**") governs the provision of the Signicat Services to the Customer. The "**Signicat Services**" means the SaaS-services, as ordered by the Customer from Signicat under this Agreement, and as described in the Service Description. The Signicat Services does not include the services from Identity Issuers or Third-Party Providers (as defined below).

By accepting this Agreement, either by accessing or using a Service (directly or through a marketplace), or authorizing or permitting any Employer or End-User to access or use a Service, you agree to be bound by this Agreement as of the date of such access or use of the Service (the "Effective Date").

In the event of inconsistencies, the main Agreement prevails over the Appendices, and the Appendices shall have priority in the abovementioned order, all with the exception that the Identity Issuers Appendix shall prevail to the extent the Identity Issuers Appendix explicitly provides so and that any Data Processor Agreement entered into shall prevail at all times.

APPENDIX 1 – COMMERCIAL TERMS

1 TERM OF THE AGREEMENT

This Agreement shall commence on the Effective Date and continue for an Initial Term of one (1) year. Thereafter the Agreement shall continue for successive periods equal to the Initial Term ("Additional Term(s)") unless terminated earlier in accordance with this Agreement. Either Party may terminate this Agreement without cause by giving the other not less than three (3) months' written notice prior to the expiry of the Initial Term or then current Additional Term. Further, the Customer shall be entitled to at any time for convenience terminate this Agreement by giving Signicat not less than three (3) months' written notice.

2 SIGNICAT SERVICES

Signicat service availability aim (SLA)	**99,5 %**

All prices in this appendix are exclusive of taxes.

Subscription fee

The first monthly subscription fee (Subscription Fee) will be invoiced after the Signicat Services are made available for the Customer. The Subscription Fee is thereafter invoiced at the start of each month.

Product overview	Methods	NOK
Signicat Sign Portal	Nordic eID, SMS OTP and InkSign	Included in price list below

Maximum number of 15 seats. Additional seats ordered, minimum of 2 seats per order.

Options	NOK
Per additional eID method	999,-
App domain	900,-

Service: Express	**Monthly subscription fee /NOK**
Product:	
Signicat Signature portal – max 15 seats	2495 NOK
Signing Methods:	
Nordic eID	Included
SMS OTP	Included
Handwritten signature	Included
eID merchant certificate (if applicable)	Included
Total order	2495 NOK

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

The Transaction Fee(s) includes third party transaction fees unless the Customer has a direct contractual relationship with the third party in question. The Transaction Fee is invoiced at the end of each month based on the actual number of Transactions.

Transaction fees	**NOK/trx**
Signed Document – Nordic eID	12,00
Signed Document - InkSign	6,00
Signed Document – SMS OTP	6,00
Notification SMS	1,50
Notification Email	0,00
Authentication – SMS OTP	2,00
Secure share instance	3,00
Login (auth transaction with context "share")	2,00

SUPPORT DETAILS

If the Customer requires assistance for support or other purposes, this will be calculated and charged per commenced half-hour according to the following rate:

	NOK/hour
Technical assistance in the Basic Support Period	1 350,-

3 CONTACT INFORMATION

Notifications pursuant to Appendix 6, the Data Processor Agreement, shall be submitted in writing to:

For Processor:
Name: Thomas Kjøglum
Position: Chief Security Information Officer
Phone number: +47 99 77 83 77
Email: thomas.kjoglum@signicat.com

4 PERSONAL DATA CHECKLIST

Personal name	
Personal contact information (Address, e-mail, phone number, etc.)	
Reference number / Customer number / Employee number	
Information of next of kind	
Information about children	
National identity number / Social security number	
Customer engagement details	
Details of insurance	
Financial information	
Medical or health information	
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	
Comments Additions not found above	

TERMS AND CONDITIONS

1 GRANT OF LICENSE

1.1 Signicat grants to the Customer a non-exclusive, non-transferable, revocable limited right to use the Signicat Services for the purpose of allowing "**End Users**" (A user of either user-facing applications provided by Signicat or the Customer Application via internet or via intranet, unless otherwise stated) to access and use the Signicat Services. End Users may only use the Signicat Services for its intended purpose as set out in the Service Description. Neither the Customer nor any End Users shall permit any other than End Users to access and use the Signicat Services.

1.2 The Customer shall take all reasonable precautions necessary to: (i) prevent access to the Signicat Services by any individual who is not an End User; and (ii) prevent any distribution or redistribution of the Signicat Services in breach of this Agreement of which the Customer is aware of. Except as expressly permitted herein or by law, the Customer shall not modify, reverse engineer, disassemble, or decompile the Signicat Services or any software contained therein.

1.3 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.

2 SIGNICATS RIGHTS AND OBLIGATIONS

2.1 Signicat will offer the support, maintenance and service level as described in the Maintenance Appendix.

2.2 Signicat offers both ready-made web applications, plugins in third party systems and API's, libraries and sample code that demonstrate how the Customer may choose to integrate its web sites with the Signicat Services. However, the Customer is solely responsible for any implementation of integration between the "**Customer Application**" (The web and/or mobile applications which integrate the Signicat Services through APIs in order to provide Signicat's services to the Customer's End Users) and the Signicat Services including any modification, amendment or addition of any API or sample code.

3 THE CUSTOMERS RIGHTS AND OBLIGATIONS

3.1 The End Users right to use the Signicat Services is derived from the Customers right to use the Signicat Services. Therefore, the terms and conditions for the End Users must be equally protective for Signicat as the terms and conditions in this Agreement. The Customer will indemnify Signicat for any damages arising out of the Customer's breach of this obligation.

4 FEES AND PAYMENT

4.1 All fees under this Agreement shall be paid within fourteen (14) days of issue of an invoice by Signicat, unless specified otherwise in the Agreement.

4.2 All fees under this Agreement are exclusive of customs, taxes, duties or excises in any form, all of which shall be borne by the Customer.

4.3 Payments that are more than thirty (30) days 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 two (2) months overdue, Signicat may, at Signicat's discretion, without prejudice to any other rights and remedies and without liability to the Customer, suspend access to all or part of the Signicat Services until the invoices in question have been paid.

4.4 The fees will not change during the first 6 months after the Effective Date of the Agreement. Prices may thereafter be changed with 1 months' notice. Thereafter, the fees may be index regulated yearly without further notice in accordance with the Statistics Norway's (SSB) wage index for the Information and communication industry with the addition of two percentage points.

5 SECURITY AND COMPLIANCE

5.1 Both Parties shall perform their services and obligations under this Agreement in compliance with all applicable laws and regulations. A more detailed description of Signicat's policy and practice regarding security is set out in the Security Requirements. Signicat may suspend the Customer's use of the Signicat Services without liability, at any time, temporarily or permanently, in the event that the Customer's use of the Signicat Services is in breach of the applicable laws and regulations.

5.2 In particular, both Parties warrant to adhere to all applicable privacy laws and regulations pertaining to the Signicat Services, including Regulation (EU) 2016/679 (the "**GDPR**"). Further, by agreeing to this Agreement, the Parties also enter into the Data Processor Agreement.

6 CONFIDENTIAL INFORMATION

6.1 "**Confidential Information**" means the specific

terms of this Agreement, and any information disclosed by either Party to the other Party, either directly or indirectly, in writing or in any other manner, relating to each Party's business and/or customers, including without limitation confidential information about the Signicat Services. Confidential Information shall not include information (i) already in the possession of the receiving party without an obligation of confidentiality; (ii) hereafter rightfully furnished to the receiving party by a third party without a breach of any separate nondisclosure obligation; or (iii) publicly available without breach of this Agreement (i.e. information in the public domain).

6.2 Neither Party shall use, or disclose to any person, either during the term or after the termination of this Agreement, any Confidential Information except in accordance with the other party´s prior written consent or as required by law.

6.3 Signicat may distribute press releases about the cooperation between Signicat and the Customer as well as the launch of the Signicat Services only after the Customer's prior written consent. Such consent shall not be unreasonably withheld.

7 INTELLECTUAL PROPERTY RIGHTS

7.1 All "**Intellectual Property Rights**" (any copyrights, 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, and applications thereof) belonging to each Party as of the date of this Agreement, and all rights, title and interest to existing technology, products and works of each Party and all accompanying and associated materials as of the date of this Agreement, shall remain exclusively with such Party or such Party's licensors.

7.2 All right, title and interest to any software, products, technology and/or information in any service, documentation or material provided or developed by Signicat from time to time under this Agreement, shall remain exclusively with Signicat or Signicat's licensors. As between Signicat and the Customer, Signicat also owns and holds all Intellectual Property Rights and other rights to the non-personal log data in and from Signicat Services Transactions, which will be used in an aggregate manner that does not identify the Customer or any other legal or natural persons. Customer acknowledges and agrees that it has no rights or claims of any type, other than the licenses granted under this Agreement, to the Signicat Services, all modifications (whether made by Signicat, the Customer, or third parties), trademarks, the above mentioned log data, and the Intellectual Property Rights embodied therein, and the Customer irrevocably waives and releases any claim to title and ownership rights (including copyright ownership) thereto.

8 WARRANTY DISCLAIMER

8.1 Except as set forth in Section 5.1 and 5.2, and to the extent permitted by law, Signicat and its suppliers disclaim all warranties, either express or implied, statutory or otherwise, including without limitation warranties of functionality, fitness for a particular purpose or non-infringement.

9 LIMITATION OF LIABILITY

9.1 For the avoidance of doubt, Signicat accepts no liability whatsoever towards (a) the Customer; (b) Customers and their End Users; or (c) any other third person, for:

(i) any loss caused by any transaction by use of the Signicat Services;

(ii) errors or delays that are outside Signicat's reasonable control, including without limitation denial-of-service attacks (DoS), general internet failure, line delays, power failure or faults of any machines;

(iii) loss caused by deficiencies in Signicat's Services that are caused by the Customer's acts or omissions; or

(iv) any loss suffered by the Customer because of loss of data caused by the Signicat Services, excluding remedial expenses incurred to restore lost data in the event the loss of data was caused by Signicat's failure to make backups and such backup obligation was explicitly agreed upon.

9.2 Neither Party shall be liable to the other Party in contract, tort or otherwise, whatever the cause thereof, for any loss of profit, business or goodwill or any other indirect damages of any kind arising under or in connection with this Agreement.

9.3 The total and maximum liability of a Party under any provision of this Agreement or any transaction contemplated by this Agreement shall in no event exceed an amount equal to the total amounts paid by the Customer to Signicat under this Agreement the last 12 proceeding months of the event that incurs liability, or EUR 100 000, whichever amount is the least.

9.4 The exclusions and limitations of liability of this Section 10 do not apply in case of death or injury to persons, damages attributable to breach of Section 7 (Confidentiality) or to damages

attributable to intent or willful recklessness of the respective Party's management.

10 TERM AND TERMINATION

10.1 This Agreement shall commence on the Effective Date and continue for an Initial Term as set out in the Commercial Terms. Thereafter the Agreement shall continue for successive periods equal to the Initial Term ("**Additional Term(s)**") unless terminated earlier in accordance with this Agreement.

10.2 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. The terminating Party shall be entitled to set the day upon which the Agreement terminates, provided that, in the event of termination by Signicat, Signicat shall always grant the Customer such time extension as is necessary in order for the Customer to be able to procure similar services from other suppliers in a seamless and orderly fashion, provided that such time not shall exceed six (6) months and that the Customer pays Signicat all applicable fees in such period.

10.3 The Parties right to terminate this Agreement for convenience is set out in the Commercial Terms.

10.4 This Agreement may be terminated by either party, 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.

10.5 This Agreement may be terminated by Customer subject to the conditions set out in the Data Processor Agreement Section 5.

10.6 Upon expiration or termination of this Agreement:

(i) The Customer shall immediately cease its use of the Signicat Services, and all licenses to End Users granted under this Agreement shall expire;

(ii) The due dates of all outstanding invoices shall automatically be accelerated so they become due and payable on the date of termination or expiration, even if longer terms have been previously agreed;

(iii) Each Party shall immediately cease all use of the other Party's and its supplier's trademarks and shall not thereafter use any mark which is confusingly similar to any trademark associated with the other party or its suppliers.

11 MISCELLANEOUS

11.1 Neither Party may assign this Agreement without the prior written consent of the other Party, which consent shall not be unreasonably withheld.

11.2 Neither Party shall be responsible for failure of performance due to causes beyond its control, including, but not limited to labour disputes and actions of any government agency, and other force majeure events defined by applicable law.

11.3 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.

11.4 Signicat's rights to be paid and Customer's obligations to pay Signicat all amounts due hereunder, as well as Sections 5, 6.1, 6.2, 7, 8, 9, 10.6, and 11 shall survive termination of this Agreement.

11.5 This Agreement shall be governed by and construed in accordance with the laws of the country where the Customer is registered (except the conflict of laws). 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 the country where the Customer is registered.

11.6 If any provision of this Agreement is declared invalid by any court or tribunal, the remaining provisions of this Agreement shall remain in effect.

11.7 This Agreement has been duly executed by both Parties by way of electronic signature.

This Agreement is valid and binding as of the date of the last [electronic signature] (the "**Effective Date**").

APPENDIX 2 – SERVICE DESCRIPTION

Signicat Sign Portal

Signicat Sign Portal is a standalone web application solution for digital signing needs. Signicat Sign Portal allows users to log into a solution where documents can be uploaded and sent for signing to end users, and where signed documents can be retrieved thereafter. The solution does not require any integration nor installations at the user's end, and the application is operated as a cloud service by Signicat. Signicat Sign Portal gives easy access to Signicat's powerful signing engine, where amongst others a multitude of different signing methods are supported.
Signicat Sign Portal consists of the following main solution components:

Component	Description
Signicat Sign Portal web application	Signicat Sign Portal web application is a cloud-hosted solution which amongst others supports user management, signing request overview, sending out documents for signing, notifications when documents get signed, and retrieving signed documents. The Signicat Sign Portal web application uses the Signicat Notification Engine and Signicat Signing Engine to send out requests for signing and getting documents signed by end users
Signicat Sign	Signicat Sign offers a multitude of different signing methods, supporting eIDAS-compliant electronic signatures on Advanced and Qualified levels. Signicat Sign Portal web application uses Signicat Sign to produce signatures on documents.
Signicat Notification Engine	Signicat Notification Engine supports notification to end users in the e-mail and SMS channels. Signicat Notification Engine is used for sending signing requests to end users, as well as reminders and other communication to end users from the Signicat Sign Portal web application
Signicat Secure Share	Signicat Secure Share is a solution for sending files and documents securely to designated identifiable recipients. Files and documents are encrypted, and recipients need to identify themselves using electronic ID in order to decrypt and access the contents. If the feature is enabled, Signicat Sign Portal web application uses Signicat Secure Share in order to securely transfer signed documents to end users after the signature process is finished

Signicat Sign Express

Signicat Sign Express is an API solution for digital signing. Signicat Sign Express allows companies to integrate a digital signing process seamlessly into their web pages, apps and business systems. Documents can be sent to the API for direct integration into a web application, or alternatively Signicat Sign Express can send out the document for signing via e-mail and/or SMS. Signicat Sign

Express offers rich configuration possibilities, where the signing experience can be tailored to meet the specific needs in a given business process. Signicat Sign offers a multitude of different signing methods, such as Nordic eIDs, SMS OTP and handwritten signatures on screen ("InkSign"). Certain optional add-on services in conjunction with a signature process are also supported by Signicat Sign. Signicat Sign Express consists of the following main solution components:

Component	Description
Signicat Signing Engine Express	Signicat Signing Engine Express offers a multitude of different signing methods, such as Nordic eIDs, SMS OTP and handwritten signatures on screen ("inksign"). Also, it handles packaging of signed documents into the eIDAS compliant format PAdES (PDF Advanced Electronic Signatures).
Signicat Notification Engine	Signicat Notification Engine supports notification to end users in the e-mail and SMS channels. Signicat Notification Engine is used for sending signing requests to end users, as well as reminders and other communication to end users as specified in API requests (ie. configuration for notifications in connection with a signature request can be controlled through the API).

Signicat Identification Express

Signicat Identification Express is an API solution for secure end user identification/authentication. Signicat Identification Express allows companies to integrate a digital identification process seamlessly into their web pages, apps and business systems. Signicat Identification Express allows companies to connect to several electronic ID schemes through one point of integration and in a harmonized way. Certain optional add-on services in conjunction with an identification process are also supported by Signicat Identification Express. Signicat Identification Express supports two different integration interfaces, allowing companies to choose the integration solution that best fits their business needs.
Signicat Identification Express consists of the following main solution components:

Component	Description
Signicat Identity Hub Express	Signicat Identity Hub Express consists of integrations with multiple identity providers and identification methods, supporting all major Nordic eID schemes as well as SMS OTP and social media login providers.
Signicat Identification Express REST API	Signicat Identification Express REST API is an integration interface for accessing Signicat Identity Hub Express' identity methods in a unified, harmonized way. Signicat Identification Express REST API supports different types of end user flows depending on the underlying support in the identity provider's mechanisms, and a harmonized way of retrieving verified identity data from an identification process.
Signicat Identification Express OpenID Connect service	Signicat Identification Express OpenID Connect service is an integration interface for accessing Signicat Identity Hub in a fully standardized way, conforming to the OpenID

	Connect industry standard. Signicat Identification Express and provides possibilities for creating Single Sign On services across several sites

Signicat Information Services Express

Signicat Information Services Express is an API solution for retrieval of verified information about a person or a company, supporting multiple sources for different use-cases. The service allows companies to have one integration point for multiple sources, and to retrieve verified information in a simple and normalized way to build business processes utilizing the information attributes. Information attributes can be used for instance to enrich the data set from an identification process, and for performing an onboarding of an end user. Examples of data sets that can be made available through Signicat Information Services Express include person address, PEP/sanction matching results and company information for the purpose of AML compliant onboarding processes.

Signicat Information Services Express consists of the following main solution components:

Component	Description
Signicat Lookup Hub Express	Signicat Lookup Hub Express consists of integrations with multiple information sources, both for person and company lookups, supporting sources for address verification as well as company information and AML related data sets.
Signicat Information Services Express REST API	Signicat Information Services Express REST API is an integration interface for accessing Signicat Lookup Hub Express' lookup methods/information sources in a unified, harmonized way. Signicat Lookup Hub Express REST API allows easy integration of multiple information sources and a harmonized way of retrieving verified data sets enriching a person or company identity, to be used eg. in conjunction with an identification process to establish a new customer relationship

Signicat Secure Share

Signicat Secure Share is an API solution for secure sharing of files and documents to recipients over the e-mail and SMS channels. Files and documents can be sent to the API, and the service encrypts the contents securely, before recipients are notified with an e-mail and/or SMS that they have received personal contents to be downloaded upon identification. The recipients' identities are pre-specified by the sender by use of either mobile number for SMS OTP authentication, national ID number or eID unique identifier, and only intended recipients can download the protected contents after having proved a matching identity. When the end user logs in with a suitable identity method, and upon matching identity, contents are decrypted, and the end user can download the contents. The solution can be integrated in any business process where it is important to protect the contents transferred to an end user, and where e-mails with open attachments are not an option due to security requirements.

Signicat Secure Share consists of the following main solution components:

Component	Description

Signicat Secure Share REST API	Signicat Secure Share REST API is the integration interface for the service, where the sender can send in documents and files to be shared and specify the identity of end users eligible to download the contents.
Signicat Identification Express	Signicat Identification Express is used for performing secure identification of recipients of shared contents
Signicat Notification Engine	Signicat Notification Engine supports notification to end users in the e-mail and SMS channels. Signicat Notification Engine is used for sending requests to end users for downloading shared contents, as well as reminders to end users as specified in API requests (ie. configuration for notifications in connection with a share request can be controlled through the API).

Signicat Deposit

Signicat Deposit is an API solution for creation of deposit accounts in conjunction with tenancies for the Norwegian market and in accordance with Norwegian tenancy regulations. The Signicat Deposit solution provides the possibility to create deposit accounts in Signicat's partner bank Easybank. The solution allows for onboarding of the end users (tenants) to happen de-coupled from Signicat's partner bank's interface, meaning that the deposit account creation process can happen seamlessly integrated into a web page or app where the business process takes place, and the end user can complete the process in the same interface. The solution also supports seamless destruction of the deposit account when the tenancy agreement is terminated, with support for both split payments and complete release of deposit amount. Also, the solution supports combined signature of both tenancy agreement and deposit account agreement, so that the landlord can have their standard tenancy agreement signed as part of the deposit account creation process.

Signicat Deposit consists of the following main solution components:

Component	Description
Signicat Sign Express	Signicat Sign Express is used for signing tenancy and account agreements in relation to the deposit account creation process
Signicat Notification Engine	Signicat Notification Engine supports notification to end users in the e-mail and SMS channels. Signicat Notification Engine is used for sending requests to end users related to pending tasks (such as account destruction), where the end user must carry out eg. a digital signature to complete the process
Signicat Deposit REST API	Signicat Deposit REST API is the integration interface for the service, where the landlord can specify necessary details about the tenancy agreement and create a request for the end user (tenant) to carry out onboarding to the bank and subsequent creation of the deposit account. Statuses for the deposit account are also supported, so that the landlord can know in near-realtime when e.g. the deposit amount has been paid in full

APPENDIX 3 – MAINTENANCE

1 SUPPORT, MAINTENANCE AND SLA

1.1 Signicat shall provide technical surveillance of the Service and is responsible for the daily operations as well as incident monitoring and handling. Signicat shall notify the Costumer without undue delay when becoming aware of incidents relating to the Service and implement reasonable measures to find and correct the malfunction.

1.2 Signicat's service availability aim as set out in The Commercial Terms does not include incidents or errors of any kind resulting from circumstances related to Signicat's (i) Customers, or (ii) sub-suppliers. If such incidents affect the Signicat Services, Signicat shall assist in identifying the cause of and rectifying the incident.

1.3 Support services from Signicat are available in Community for all customers and for customers having extended support as listed in the Commercial Terms support is available from Monday to Friday 08.00-16.00 CE(S)T all Working Days in Norway, and a maximum of 8-hour response time to incidents. The availability of support and the 8-hour response time may be adjusted upon request from the Costumer and subject to remuneration.

1.4 Signicat reserves the right to perform maintenance, upgrades, service, etc. related to the Signicat Services from Tuesday and Thursday from 00.00 – 07.00, and the Customer acknowledge and agree that this might cause unavailability, interruptions, or changes to the service. Signicat shall notify the Costumer 48 hours in advance of such maintenance work and by best efforts reduce potential inconvenience.

2 KEY DEFINITIONS

Time – Unless otherwise stated all times (in this Agreement and its Appendices) are in Central European Time (CE(S)T).
Working Day – Any day except Saturday, Sunday or a day defined as a public holiday in Norway.
Working Hour – An hour within the timeframe 08:00 – 16:00 CE(S)T all Working Days.

APPENDIX 4 – IDENTITY ISSUERS TERMS

General terms and conditions applicable to the services from Identity Issuers

(i) The Identity Issuers provide electronic identification solutions that may be used for authentication and signing (the "**Identity Issuers Services**"). Subject to the Identity Issuer Terms below, the Customer may use the Identity Issuers Services. The Customer acknowledges and agrees that the Identity Issuers Terms applies in addition to the terms of this Agreement and that the Identity Issuers Terms shall prevail in the event of conflict.

(ii) The Customer is always responsible for becoming approved and qualified as a receiver of the

relevant certificates, keys and passwords from the Identity Issuers.

(iii) The Customer is responsible for passing on certificates, keys and passwords to Signicat received from Identity Issuers. Further, Signicat may notify the Customer of certain certificates, keys and passwords from third parties that the Customer must pass on to Signicat, provided that the Customer is entitled to pass on such information.

(iv) Any new certificates replacing certificates already provided shall be passed on to Signicat without undue delay. If the Customer receives information from an Identity Issuer which it has reason believe is relevant for the fulfilment of this Agreement, or if the Customer has reason to believe any certificates, keys or passwords are incorrect, this information shall without undue delay be passed on to Signicat via the Signicat Portal.

(v) The Customer acknowledges and accepts that the Identity Issuers may change the Identity Issuers Services, as well as the Identity Issuers Terms. In the event of such changes, Signicat will inform the Customer in writing without undue delay. Additionally, the Customer agree that the Customer and its Affiliates shall, when providing their services, inform that their services are supported by the Identity Issuer Services, and that Signicat shall approve the manner in which the Identity Issuer Services is presented to the End Users, such approval not to be unreasonably withheld.

NORWEGIAN BANKID

1. TERMS AND CONDITIONS FOR BANKID

In furtherance of the Agreement, the Parties agree to add the following agreements pertaining BankID to the Agreement as part of Appendix 4:

(i) Merchant Agreement BankID

(ii) Standard Terms and Conditions for BankID (Distribution Agreement)

(iii) Terms and Conditions for Issuers Liability

In case of conflict between the Agreement and the above-mentioned agreements, the latter shall prevail.

1.1 THE CUSTOMER'S COMPLIANCE

The Customer are responsible for ensuring that the service(s), which use the BankID service(s), is in accordance with rules and regulations for Norwegian BankID, and with applicable law, and do not include discriminating, pornographic or otherwise offending material.

Customer acknowledge and agree that Signicat and BankID Norway is entitled to terminate or suspend the right to use the BankID service(s) with immediate effect in the event of any breach of the obligations set out in this section 1.1.

APPENDIX 5 – THIRD-PARTY TERMS

General terms and conditions applicable to the services from Third Party Providers.

(i) Subject to the Third-Party Terms below, the Customer may use the identification data, or the software delivered by the Third-Party Providers.

(ii) The Customer acknowledge and agree that the Third-Party Terms applies in addition to the terms of the Agreement and that these terms shall prevail in the event of conflict.

(iii) The Customer further acknowledge and agree that Signicat can only offer the identification data or software for as long as Signicat's has a valid agreement with the Third-Party Provider in question.

(iv) For the avoidance of doubt, the terms and conditions applicable to support, maintenance and availability in Appendix 3 does 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 as 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 does not constitute a binding legal obligation on part of neither Signicat nor the Third-Party Provider in question.

APPENDIX 6 – DATA PROCESSOR AGREEMENT

Data Processing Agreement

Between

"Customer" (Controller)

and

Signicat AS (Processor)

(each a "**Party**", collectively the "**Parties**")

1 Definitions

Agreement	This Data Processing Agreement.
Applicable Data Protection Law	All privacy laws and regulations in the country where Controller or Processor is registered, hereunder but not limited to national laws based on the European Union Regulation (EU) 2016/679 (the "GDPR").
SaaS Agreement	The agreement between the Controller and the Processor under which the Processor provide the services the processing forms a part of.
Controller	The legal entity determining, alone or jointly with others, the purpose for and the means of the processing of Personal Data pursuant to this Agreement: The Customer pursuant to the SaaS Agreement.
Personal Data	Any information relating to an identified or identifiable natural person processed by the Processor on behalf of the Controller.
Processor	The legal entity processing data on behalf of the Controller pursuant to this Agreement: Signicat AS.

2 Purpose

This Agreement shall reflect the Parties agreement with respect to their rights and obligations pursuant to the Applicable Data Protection Law, and concerns the Processor's use of Personal Data on behalf of the Controller, including collection, recording, alignment, storage and disclosure or a combination of such uses. This Agreement is enclosed as an exhibit to and forms a part of the SaaS Agreement.

This Agreement shall ensure that Personal Data is protected from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access when transmitted, stored or otherwise processed.

3 Scope and purpose of the data processing

The Processor shall process Personal Data on behalf of the Controller solely for the purpose of performing the tasks imposed on the Processor by the Controller pursuant to the SaaS Agreement, as part of the agreed delivery of services under the SaaS Agreement. The Parties further agree that any processing of Personal Data contemplated by this Agreement shall be conducted in accordance with the requirements set forth in the Applicable Data Protection Law, this Agreement, and the SaaS Agreement.

This Agreement covers any category of Personal Data. A specification on which Personal Data the Processor will process is set out in the Personal Data Checklist in Appendix 1.

4 The Processor's obligations

4.1 General

When processing Personal Data on behalf of the Controller, the Processor shall comply with any documented routines and instructions stipulated by the Controller at any given time, and the Processor shall process Personal Data in compliance with Applicable Data Protection Law and the Agreement including the Security Requirements Appendix.

Nothing in this Agreement shall be interpreted as preventing the Controller from taking the necessary steps to comply with the Applicable Data Protection Law.

The Processor shall specify to the Controller where the Personal Data is stored at any time and shall ensure that the Personal Data is stored and processed within the EU/EEA.

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, in the event that such

processing / transfer is required by Applicable Data Protection Law, in which case the Processor shall notify the Controller of the legal requirement in question before processing unless the law in question prohibits such notification due to important grounds of public interests.

4.2 Assistance to the Controller

The Processor shall provide assistance to the Controller in fulfilling its duties under the Applicable Data Protection Law, including without limitation the Controllers obligations towards data subjects to ensure their right to information, access, rectification, erasure, restriction of processing, and data portability, to the extent such assistance is necessary for the Controller to be compliant with Applicable Data Protection Law.

5 Use of Sub-Processors

Processor shall ensure that any Sub-Processor (a "**Sub-Processor**"), and its sub-contractor, is bound by terms in accordance with the Applicable Data Protection Law.

Anyone who performs assignments on behalf of the Processor including processing of Personal Data shall be made familiar with the Processor's contractual and legal obligations and fulfill the applicable requirements. Thus, the Processor is obliged to enter into a Data Processor Agreement with any Sub-Processor.

As of the effective date of this Agreement, the Controller acknowledges and agrees that the Processor has entered into an agreement with Sub-Processor(s) listed in the Main Agreement, and hereby consents to the use of such Sub-Processors.

The Processor may not use a subcontractor to process Personal Data 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 both the Agreement and the Main Agreement if it can demonstrate that the new Sub-Processor will not meet the requirements set out in GDPR. This termination right is Controller's sole and exclusive remedy if Controller objects to any new Sub-Processor.

6 Security

The Processor shall fulfill the requirements for technical and organization security measures stipulated in the Applicable Data Protection Law, and shall comply with the Security Requirements Appendix to the SaaS Agreement. The documentation shall be made available upon the Controller's request.

The Processor shall report to the Controller any discrepancies between this Agreement and the requirements set out in the Applicable Data Protection Law.

The Processor shall, if reasonably requested the Controller and to the extent necessary, assist the Controller in (i) complying with the Applicable Data Protection Law; (ii) conducting the necessary data protection impact assessments pursuant to the Applicable Data Protection Law, and (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.

7 Audits

The Processor shall regularly conduct audits for systems and services covered by this Agreement to assess the Processors compliance with the Applicable Data Protection Law. The same applies to Sub-Processors.

The Processor shall provide the Controller with its audit reports upon request. The same applies to audit reports of Sub-Processors. Such audit reports are subject to confidentiality obligations.

In addition to the provision of the audit reports, the Processor shall on Controller's reasonable request provide access to the Processors relevant processing systems, facilities and supporting documentation to conduct audits and inspections in accordance with Applicable Data Protection Laws. Such an audit will be conducted by an independent recognized third-party audit firm during regular business hours, with reasonable notice and reasonable confidentiality reports. The audit reports are subject to confidentiality obligations. These provisions regarding access to relevant processing systems, facilities and supporting documentation does also apply to Sub-Processor(s). In the event of any such inspection or audit, each Party shall provide all reasonable assistance to the other Party on a time and material basis.

If an audit reveals or confirms that the processing pursuant to this Agreement 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.

8 Confidentiality

The Processor and the Processor's personnel shall observe unconditional confidentiality as regards the processing of Personal Data pursuant to this Agreement and any documentation accessed under this Agreement. 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, or where (ii) Personal Data need to be disclosed to a competent public authority to comply with a legal obligation.

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

This provision shall survive expiration or termination of this Agreement.

9 Notification of non-compliance and data breaches

Processor shall give an initial notification to the Controller without undue delay, and at the latest within twentyfour (24) hours, if the Processor:

a) cannot, for any reason, comply with its obligations in this Agreement; or

b) becomes aware of any circumstance or change that is likely to have a substantial adverse effect on the Processor's or its Sub-Processors' ability to meet its obligations in this Agreement.

The Processor shall, as soon as possible or at the latest within twentyfour (24) hours after becoming aware of it, notify the Controller of 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 or similar Personal Data breaches. Thereafter, the Processor shall contribute to and reasonably cooperate with the Controller to obtain the following information:

a) describe the nature of the personal data breach including the categories and approximate number of data subjects and personal data records concerned;
b) communicate the name and contact details of the Processor's data protection officer or other contacts where further information can be obtained;
c) describe the likely consequences of the personal data breach; and
d) describe 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.

The Processor shall co-operate with the Controller and take such reasonable steps as are directed by the Controller to assist in the investigation, mitigation and remediation of personal data breaches involving the Processor.

10 Liability

Subject to the limitations of liability of the SaaS Agreement, the Processor is liable 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 Agreement, including non-compliance with the Applicable Data Protection Law.

11 Term

This Agreement remains valid for as long as the SaaS Agreement is in force and terminates automatically upon the termination or expiration of the SaaS Agreement. The Processor may not process Personal Data on behalf of the Controller following the termination or expiration of this Agreement.

In the event of a material breach of this Agreement or the Applicable Data Protection Law, the Controller is entitled to terminate this Agreement with immediate effect and may instruct the Processor to cease further processing of the Personal Data in question with immediate effect.

12 Termination

Upon notification of termination of the SaaS Agreement, the Processor shall have all Personal Data processed on behalf of the Controller available for downloading pursuant to this Agreement in a format agreed on between the Parties, and in accordance with reasonable industry standards.

The Processor shall further delete or destroy in a secure and definite/irreversible manner all physical mediums that contain Personal Data processed

under this Agreement, at the latest on the date that the termination of the SaaS Agreement takes effect.

13 Notifications

The Parties shall ensure that the Parties have up to date notification and contact information.

14 Entire agreement

This Agreement, as well as the SaaS Agreement with appendices, constitutes the entire agreement between the Parties with respect to the subject matter hereof (the Processor's processing of Personal Data on behalf of the Controller) and, upon its effectiveness, shall supersede all prior agreements, understandings and arrangements, both oral and written, between the Parties with respect to such subject matter.

15 Governing law and legal venue

Unless otherwise agreed through the SaaS Agreement, this Agreement is governed by Norwegian law, and any disputes arising from or relating to this Agreement shall be subject to the exclusive jurisdiction of Norwegian courts.

APPENDIX 7 – SECURITY REQUIREMENTS

1. SCOPE AND PURPOSE

The following information security requirements applies to Signicat's processing of Customer's data or otherwise delivery of the operational services delivered to Customer.
These requirements shall ensure that Signicat handles all Customer information with security in mind, and Supplier 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 27001:2013 (or subsequent versions), or a set of policies to that effect, and Signicat shall, prior to entering into this Contract and subsequently upon Customer 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 Contract and subsequently upon Customer request and reasonable advance notice, provide documentation thereof to the Customer.
The information security requirements listed below also applies to sub-suppliers of Signicat.

3.1. Organization of Information Security

Information security responsibilities must be defined and allocated.

3.2. Information Asset Management

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 and temporary employees.

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 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 processes, store or in some other way handles customer's information. The procedures shall ensure that information is handled and stored in compliance with information security policies, regulatory requirements and contractual obligations.
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.
Backup shall be taken of all information according to availability and integrity requirements, taking confidentiality requirements into account.
There shall be kept event logs of user activities, exceptions, faults and information security events in systems and networks that is, or contains, customers' information. These logs shall be reviewed regularly.
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 exists 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

Areas that contain information and information processing facilities shall be defined, classified, and documented.
Windows and doors shall be closed and locked at all time.
Physical access shall be restricted to authorized personnel only and visitors shall always be accompanied.
Physical access during office hours shall be restricted by a personal access card and PIN.
Physical access rights shall be annually reviewed, shall be updated when necessary, and revoked when necessary.
An intruder detection system shall be active when the location is unattended and this system shall be tested annually.
The intruder detection system shall be connected with a guard central that offer guard dispatch.
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 request and reasonable advance notice, documentation that such test has be 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 deliverables under this Contract in the result may be masked.
The Customer may perform security tests against Signicat's solutions upon Signicat's approval.

APPENDIX 8 – LIST OF SUB-SUPPLIERS (OTHERS THAN IDENTITY ISSUERS AND THIRD-PARTY PROVIDERS)

Business name	Company registration number	Address	Service	Processing	Legal basis
Microsoft Ireland Operations, Ltd.	IE256796	Carmenhall Road Sandyford, Dublin 18, Ireland	Hosting services and core systems	End user personal data as defined in the DPA Appendix Checklist	DPA
Basefarm AS	NO982211743	Nydalen Allé 37 A, 0484 Oslo, Norway EU/EEA	Hosting services and core systems	End user personal data as defined in the DPA Appendix Checklist.	DPA
H1 Communication AB	556730-0610 (SE)	Öneslingan 5, 832 51 Frösön, Sweden	Support services (ticket handling, call center, e-mail support)	Customer contacts (e-mail, phone), end user personal data as defined in the DPA Appendix Checklist	DPA
Salesforce salesforce.com EMEA Limited	05094083	Floor 26 Salesforce Tower, 110 Bishopsgate EC2N 4AY London, United Kingdom	Support and incident management	Customer contacts are registered in Salesforce CRM system with name, email address and phone number.	DPA/SCC – EU/EEA and UK
Gainsight	10662016	WeWork Fox Court, 14 Grays Inn Rd, London WC1X 8HN, United Kingdom	Customer Success tool	Customer contact mail address, unless generic email is provided.	DPA & Privacy Shield
Zendesk, Inc.		1019 Market Street, San Fransisco, CA 94103, USA	Support and incident management	Customer support e-mails are processed in Zendesk, with e-mail address/phone number and name of requestor.	DPA & Privacy Shield
46elks AB	556838-8184 (SE)	SMEDSGRÄND 4, 753 20 Uppsala, Sweden	SMS Gateway (primary)	End user phone number.	DPA
Twilio Inc.		375 Beale Street, Suite 300, San Francisco, CA 94105	SMS Gateway (secondary)	End user phone number	DPA & Privacy Shield
Mailgun Technologies, Inc.		535 Mission St. 14th Floor San Francisco, CA 94105, USA	Hosting of mail server for notification emails	End user e-mail address	DPA & Privacy Shield