MERCHANT AGREEMENT

AND

TERMS AND CONDITIONS

FOR

KYC/AML SERVICES

TABLE OF CONTENT

1 GENERAL

The KYC/AML Service is provided by the Company as part of the total product portfolio of the Company relating to ID services and other services for use at Merchant.

All terms and expressions in the list of definitions in the main part of the Merchant agreement shall be understood equal in these *Terms and conditions for KYC/AML Services to Merchant*, unless otherwise defined here.

2 DOCUMENTS

The Merchant Agreement includes the following documents:

Main body: This document

Appendix 1: Terms and condition for KYC/AML Services

Appendix 2 Data processing agreement for KYC/AML Services

In the event of inconsistency between the Main body and the appendices the latter will prevail. The DPA take precedence in cases related to handling of personal data.

3 DEFINITIONS

Agreement framework: The Merchant agreement with appendices including the Documentation made available on the Company's webpages.

Anti- Money Laundering Act: The always applicable Act relating to Measures to Combat Money Laundering and Terrorist Financing (the Anti-Money Laundering Act 1st of June. 2018 no 23. (Hvitvaskingsloven).

The Company: BankIDBankAxept AS.

Documentation: The Company's current documentation accessible for the Reseller in the Reseller portal.

Effective date: The date on which the Merchant agreement is signed by both Parties and the Merchant is approved by the Company.

Merchant: A legal entity, registered in the Enterprise Register for Legal Entities or similar public enterprise register.

Merchant agreement: The agreement with appendices entered with the Merchant regarding the right to use the Service.

Ordering routines: The Company's current procedures for ordering and changing the Services

Party: The Reseller, the Company, and the Merchant, collectively the Parties.

The Reseller: A Company which has an agreement with the Company for reselling the Services.

The Reseller portal: The internal portal for Resellers unlike the Company's public website.

The Service(s): The KYC/AML Services as described in the appendices to the Merchant agreement.

Terms and Conditions the Terms and conditions for the KYC/AML Services.

4 SCOPE

The Merchant agreement is entered between the Merchant and the Reseller on behalf of the Company.

The rights and obligations of the Parties are stated in the Merchant agreement with appendices.

The Merchant will be given access to the Service and Documentation for implementation in accordance with the Merchant agreement.

The Merchant agreement does not include other services or any commercial terms for delivery of any Service (price, etc.) from the Reseller.

5 PROCESSING OF PERSONAL DATA

5.1 Personal data

Each of the Parties must ensure that all processing of personal data in connection with the Merchant agreement shall be in accordance with the relevant public requirements, including personal data legislation.

By administration of the Merchant agreement, the Reseller will collect the name, email, and mobile phone number of contacts at the Merchant. The information will only be processed, disclosed to, and processed by the Company and its affiliates to the extent necessary to fulfil the Merchant agreement, and in accordance with the applicable relevant public law requirements.

5.2 Statistics

The Company may use data not defined as personal data, or otherwise protected, for statistical purposes. This applies to, but is not limited to, anonymized data, volume data, frequency measurements other information collected when providing the Service (Service Data). The Company may use service data for service purposes and the Merchant does not have ownership of such data.

6 CONFIDENTIALITY

Each Party shall comply with confidentiality and not disclose to third parties' confidential information that the Party has obtained from the other Parties in connection with the Merchant Agreement, the Service, the Company or the Reseller. Confidential information may only be used to fulfil the Party's obligations under the Merchant Agreement.

The Parties shall impose a duty of confidentiality on employees and aides (such as subcontractors and contractors) covering the requirements for confidentiality in the Merchant agreement.

The duty of confidentiality does not apply to matters made public by the Party itself.

This provision does not preclude the exchange of necessary information pursuant to law or because of the order from public authorities.

The duty of confidentiality also applies after the Merchant agreement has been terminated.

7 TERM AND TERMINATION

7.1 Term

The Merchant Agreement is in force at Effective date unless otherwise agreed and runs until it is terminated by one of the Parties or expires for other reasons.

7.2 Termination

The Merchant may terminate the Merchant agreement with three (3) months written notice.

The Reseller and the Company may terminate the Merchant agreement with six (6) months notification.

Furthermore, the Merchant agreement is terminated with reasonable notice if the Reseller is no longer (for any reason) an authorized Reseller of the Service.

8 TERMINATION FOR CAUSE

A Party has the right to terminate the Merchant agreement by written notice with immediate effect if:

a) A Party commits a substantial breach of the Merchant agreement with appendices.
b) The Merchant does not comply with the terms of the Agreement framework and does not rectify this within thirty (30) days from receiving a written notification.
c) The Merchant becomes petitioned for bankruptcy and such a bankruptcy petition is not averted within thirty (30) days.
d) The Merchant is declared bankrupt or discontinued or initiates debt negotiations, liquidation or related.

Substantial breach is for example, but not limited to, breach of payment obligations towards the Reseller or the Merchant uses the Services during infringement, illegal activities or in a manner that could damage the trust, the reputation or the goodwill of the Company or the Reseller.

9 FORCE MAJEURE

None of the Parties are liable for breach if an extraordinary situation outside a Party's control dismisses the Party's ability to fulfil the obligations of the Merchant agreement, and under Norwegian law is considered force majeure. The lapse of duty to fulfil the Merchant agreement lasts for as long as the extraordinary situation persists. The Parties are obliged to mitigate the effects of the extraordinary situation to the extent possible.

In the case of force majeure, the Merchant Agreement may be terminated if the situation lasts longer than thirty (30) days, calculated from the day the situation occurs.

10 AMENDMENTS

Minor changes in the content, terms and conditions related to any Service as described in the description on the Company's website and the Reseller portal may be changed unilaterally by the Company with two (2) weeks written notice provided that the changes do not affect the Merchant's use of the Services.

The Company may unilaterally change the Terms and Conditions of the Service with at least three (3) months' written notice.

Any changes of a material nature to the disadvantage of the Merchant shall be made with at least six (6) months' notice. A significant disadvantage is considered, for example, that the merchant must make significant changes to its systems in order to use the Service.

11 ASSIGNMENT

The Merchant may not assign the Agreement without the prior written consent of the Reseller, the Company, and the Issuer.

The Reseller and the Company may assign its rights and obligations hereunder (in whole or in part) without prior consent from the Merchant. The Merchant will be notified of the changes.

12 GOVERNING LAW AND DISPUTES

The Merchant agreement shall be interpreted in accordance with Norwegian law.

In the event of a dispute regarding interpretation or the legal effect of the Merchant agreement, the dispute shall be deemed to be resolved by negotiation. If such negotiations do not lead to any solution, each Party may file the dispute at ordinary courts.

Legal venue is Oslo.

APPENDIX 1 TERMS AND CONDITIONS FOR AML/KYC SERVICES TO THE MERCHANT

TABLE OF CONTENT

1 CONTENT OF THE SERVICES

The KYC/AML Services provides consists of three services:

1) "**Single search organization**" Customer measures when the customer relationship is created to obtain information needed for customer control of businesses and
2) "**Single search person**" to obtain information needed for customer control of private customers or to business role holders.
3) "**Continuous screening of persons**" For ongoing follow-up of private customers or role holders in a business. This service provides notice if one of the individuals being screened is sanctioned or becomes a PEP after the customer relationship begins.

Companies who have an obligation to report according to the Anti-Money Laundering Act and are obliged to confirm their customer's identity on the basis of valid identification when establishing customer relationships, cf. the Act relating to Measures to Anti- Money Laundering and Terrorist Financing (the Anti-Money Laundering Act), section 12.

If the customer is a legal person, the party subject to the duty to report must obtain a company certificate or perform additional inquiries in public records, in order to confirm the identity of the person acting on behalf of the customer and beneficial owners of the customer, cf. sections 13 and 14 of the Anti-Money Laundry Act, and on the basis of appropriate measures under anti-money laundering legislation conduct a risk assessment of the customer.

The Service may only be offered to businesses which are subject to reporting under the applicable Anti - Money Laundering legislation at any time.

The Service "Single search person" gives the Merchant access to the national identity number of the Person.

2 REQUIREMENTS FOR MERCHANT

The Reseller undertakes to ensure that Merchants who wish to enter into a Merchant agreement that includes the Service are subject to reporting duty under Section 4 of the Anti-Money Laundering Act and otherwise complies with the requirements in the *Specific terms and conditions for KYC/AML Service.*

3 THE QUALITY OF THE INFORMATION

The information is obtained from different sources and is provided directly from the Company to the Merchant. The information is obtained from different third parties, including the customer's BankID Certificate (national identity number), the National Registry (full name, national registry address), the Norwegian enterprise register (Enhetsregisteret) (organization number, company name, organizational details, registered address, name of CEO and board members etc.) and other third-party suppliers (beneficial owners, PEP and sanction lists)

The Company gives no guarantees that the information received by the Merchant being exhaustive, accurate and/or always updated.

4 DATA PROCESSING AGREEMENT (DPA)

The Merchant is data controller for the information acquired by using the Service and is solely responsible for own a legal basis for the processing and handling of personal data.

The Company is the data processor. The Reseller has a power of attorney to enter into a data processing agreement with the Merchant on behalf of the Company. By signing the Merchant agreement for the Services, the DPA is entered as a part of this.

5 REQUIREMENTS FOR THE MERCHANT'S USE OF INFORMATION FROM THE SERVICE

The Merchant may only use information received from the Service for its own activities. All use of information from the Service is at the Merchant's expense and risk. At all times, the Merchant shall process information received in accordance with the current requirements of public law, including the Personal Data legislation.

If the information is to be used for purposes other than customer control under the Anti-Money Laundering Act, or to fulfil an agreement with a person, the Merchant must obtain the person's express, voluntary, and informed consent for such use in accordance with the applicable legislation, including the Personal Data legislation.

The Merchant shall provide the Certificate holder with the necessary information of

- The purpose of the use of information.
- That the consent is voluntary,
- The relevant rights of the Certificate holder.
- other information required by applicable legislation, including the Personal Data legislation.

Furthermore, the Merchant shall have procedures for access to information, rectification, deletion, information security, internal control, etc. in accordance with applicable legislation, including the Personal Data legislation.

6 THE MERCHANT'S RESPONSIBILITIES IN ACCORDANCE WITH THE ANTI-MONEY LAUNDERING ACT

The Company is not an outsourcing contractor according to section 23 of the Anti-Money Laundering Act, and the Merchant will remain the entity subject to the reporting obligations in accordance with the Anti-Money Laundering legislation, with the responsibilities and duties that follow from the legislation.

Thus, the Merchant is obliged to assess the information provided and to ensure the necessary retention of this information in accordance with the provisions of the Anti-Money Laundering Act.

7 RESPONSIBILITY OF THE COMPANY/RESELLER

The information from the Service is provided "as is", and the Merchant is not given any guarantee that information is free from errors or defects. Neither the Company nor the Reseller are responsible for delayed delivery of credentials or information or errors in the content of the data provided and have no liability to the Merchant for the quality of the information from the base sources through the KYC/AML Service.

8 SERVICE LEVEL

Service level for the Services is described in the product literature on confluence.bankidnorge.no/ in a separate folder called "Service level AML" under "Anti-money laundering (AML)".

****

APPENDIX 2 DATA PROCESSING AGREEMENT

1 PARTIES AND ROLES

The Data Processing Agreement has been entered into between the Company, hereinafter referred to as "data processor" and the Merchant, hereinafter referred to as "data controller". The Reseller has the power of attorney from the Company to enter the DPA on behalf of the Company. The agreement is hereinafter referred to as the "Data Processor Agreement (DPA)".

2 THE PURPOSE OF THE DATA PROSESSING AGREEMENT (DPA)

The purpose of the DPA to regulate the data processor's processing of Personal Data including customer data for which the Merchant is the data controller when using KYC/AML Service. The processing includes collection, registration, assembly, storage, disclosure, or combinations of these.

The DPA shall ensure that personal data are processed in accordance with the purpose and that information about the data subjects is not used improperly or is unjustified and that the processing is carried out at all times in accordance with the Act of 15. June 2018 38 The Personal Data Act as implements the EU Regulation 2016/679 GDPR.

3 DESCRIPTION OF THE COLLECTED DATA

3.1 Categories of the registered

Persons who will and/or should be inspected in accordance with the Anti-Money Laundering Regulations ("**Persons**") of the Merchant by using KYC/AML Service.

3.2 Type of personal Information:

Data required to conduct public registry results services, postings to PEP lists ("politically exposed Person") and international sanctions lists through software supplied by the sub data processors to the main data processor includes:

- Full Name.
- National identity number
- Date and time of a Person's authentication or signing with BankID.
- Public registry address from the tax administration via Evrys Research Service.
- Whether a Person have a hidden address from the tax administration via Evrys Research Service.
- A Person's citizenship and birthplace from the tax administration via Evrys Research Service.
- If a Person is registered as an owner, general manager, auditor, accountant and/or has registered authorization for a legal entity via the Bisnodes Enterprise Information Research Service.
- Information from the PEP register from the Bisnodes Research Service.
- International sanctions list information from the Bisnodes Research Service.
- Unique identifier from BankID (BankID PID) for the Company end users.
- Electronic signatures from the Company's end users.

3.3 Processing included in the dpa

- Collecting the full name and national identity number from the certificate and the Company ' OIDC platform when a Person has been authenticated, or from a signed a document with BankID, and at the simultaneously collecting the date and time of such authentication or signing, and when the user of the Company ' systems calls on the service.

- Collection of registry data from the Norwegian Tax Administration (National Register) based on a Person's national identity number.
- Collection of enterprise information Bisnode registry data based on a legal entity's organization number.
- Collection of Bisnode registry data for PEP and sanctions lists based on Person's name and national identity number.
- Disclosure of the above-mentioned registry data from the Norwegian Tax Administration (National Register), and Bisnode to the data controller.
- Registration of logs of completed transactions in the service with the purpose of being able to invoice consumption, answering support inquiries and handling error situations that may arise from the Merchant or data providers (research services) in the solution provided by the Company, or their subcontractor(s). Logs contents the necessary information for tracking, invoicing, and troubleshooting a transaction, such as the basis of transaction time, the request status code, and the data reference numbers and the preceding BankID transaction.

4 THE FRAMEWORK FOR THE DATA PROCESSOR'S HANDLING OF PERSONAL DATA

The data processor's processing of the Personal Data must only be performed based on instructions from the data controller, unless otherwise is required by law.

The data processor must not disclose any information collected from the data controller's data to any third parties, i.e., others than the data controller or the data subject. The data processor is not entitled to use the collected information for any other purpose than to provide the service KYC/AML Service or meet requests from the data controller or the data subject regarding relocation or erasure. Exceptions may apply subject to applicable legislation or regulations.

5 PROCEDURES FOR ERASURE OF DATA, STATISTICS, ETC.

The data processor will store the above-mentioned log data for 3 months, for the purpose of invoicing the number of transactions to the data controller and being able to prove that a transaction has taken place. Then information is then automatically erased.

If the service "Continuous screening" is included in the Merchant's agreement on KYC/AML Service, the Person's name and national identity number should and/or should be checked according to the Anti-Money Laundering regulations until:

- The Person is reported out of the list subject to the service.
- The list of Persons is processed, and response is submitted to the Merchant.
- The Merchant terminates the service (i.e., upon expiry of the termination period)

6 DATA PROCESSOR OBLIGATIONS

The data processor shall follow the procedures and instructions from the data controller.

The data processor is obliged to notify the data controller if the data processor believes that an instruction is contrary to the Personal Data legislation.

The data processor is obliged to provide data controller access to its security documentation, and assist, for the data controller to fulfil its own responsibility under law and regulation.

The data processor will log all processing activities performed on behalf of the data controller, in accordance with. the requirements of the Personal Data Act and the EU Regulation 2016/679 art. 30 Nr. 2.

The data controller, unless otherwise agreed or provided by law, has the right to access and disclose the Personal Data processed and the systems used for this purpose. The data processor is obliged to provide the necessary assistance to the information.

The data processor shall make available to the data controller all information necessary to confirm the compliance of the obligations in the Personal Data Act and the Eu Regulation 2016/679 Art 30.

7 CONFIDENTIALITY

The data processor is subject to confidentiality of documentation and Personal Data that is been accessed in accordance with the DPA. Only employees who are subject to confidentiality and have the necessary knowledge of routines for the use of the information system shall have access to the Personal Data. The duty of confidentiality also applies after termination of the DPA.

8 USE OF SUB CONTRACTOR

If the data processor performs its obligations under this DPA using another data processor (sub data processor) a separate DPA must be entered between the data processor and the sub data processor. The DPA between the data processor and the subcontractor are subject to the same obligations of protection of Personal Data as this DPA.

The data processor utilizes Idfy Norway AS for the operation of the service, which in turn utilizes Orange As as subcontractor of the Software's operational solution. The data processor has a data processing agreement with Idfy Norway AS, which also has a data processing agreement with Orange.

The data processor utilizes Bisnode Norway AS as a subcontracted data processor for KYC/AML Service services "continuous screening". Bisnode Norway AS again uses Trapets AB in Sweden. The data processor has a data processing agreement with Bisnode Norway AS, which also has a data processing agreement with Trapets AB.

The data controller gives the data processor a general permission to use the sub data processor for the processing of Personal Data under this DPA. If the data processor changes one or more of the sub-processors or intends to replace sub data processors, the data processor shall notify the data controller to give the data controller an option to refuse the changes or terminate the DPA.

9 THE RIGHTS OF THE REGISTERED

Inquiries from the data subject about the registered information shall be handled by the data controller. The data processor shall assist the data controller in fulfilling the obligation of the data controller to respond to the data subject's request for access, erasure, etc. of the information.

10 SECURITY

The data processor shall comply with the requirements for security measures set out under the Personal Data Act, including EU regulation 2016/679 Art 32.

The data processor shall have procedures and have sufficient measures to meet the requirements. The documentation shall be available upon the data controller's request.

11 NOTIFICATIONS OF DISCREPANCY

Each party is responsible for notifying the other Party without undue delay if a breach of the Data Protection Provisions is detected. In case of severe violations, notification must take place immediately.

In the event of a breach of the DPA or Personal Data legislation, the data controller may order the data processor to stop the further processing of the Personal Data with immediate effect.

The discrepancy processing under the Personal Data Act and the EU Regulation 2016/679 Art 33 be performed by the data processor reporting the discrepancy to the data controller. The data controller has the obligation to give notification to the Data Protection Authority

12 SECUTRITY AUDITS

The data controller may agree with the data processor to carry out up to yearly security audits for systems and similarly covered by this DPA and *Specific terms and condition for KYC/AML Service*. The audit can include review of routines, sample controls, more extensive facility controls and other appropriate control measures. The data controller documents the results of the security audit.

13 TERM AND TERMINATION

The agreement applies for as long as the data processor processes Personal Data on behalf of the data controller

Termination follows the Merchants use of the KYC/AML Service services.

14 EFFECTS OF TERMINATION

Upon termination of the Merchant Agreement, the data processor is obliged to return all Personal Data received on behalf of the data controller covered by this DPA.

The Parties will agree upon a time schedule for when the data processor shall delete or properly destroy all documents, data, storage media, etc., containing information covered by the DPA. This also applies to any backups.

The data processor shall document in writing that deletion and or destruction have been carried out in accordance with the Agreement within 30 days of the termination of the DPA.

Any costs of printing and copies of data will be charged to the data controller.

15 OTHER RIGHTS AND OBLIGATIONS

This DPA shall not extend the data controller's opportunities of sanctions, including liability for the data processor, other than what arise from the Merchant agreement with appendices.

In the event of a transfer of the Merchant agreement including KYC/AML Service to any other party, this DPA shall be transferred accordingly.

*****

End of Document.