MERCHANT AGREEMENT – BANKID SERVICES

INFORMATION ABOUT THE RESELLER AND THE MERCHANT

Reseller: [name]	**Merchant**: [name]
Org. nr.: [number]	Org. nr.: [*]
Address: [*]	Address: [*]
Post number and -place: [*]	Post number and -place: [*]

Issuer: [Name of Issuer] by [Name of joint Issuer]

Organisation number Issuer:

[*]

e-mail address: [*]

1 SERVICES INCLUDED IN THE MERCHANT AGREEMENT

On the terms and conditions stated in this Merchant agreement with appendices, the Merchant is granted a right to use of BankID Certificates for Merchants for the following Services:

[X] **BankID Biometrics/Substantial**

[X] **BankID High**

[_] Access to National identity number

[_] Access to additional information

[X] **KYC/AML Services**

TABLE OF CONTENT

1 SERVICES INCLUDED IN THE MERCHANT AGREEMENT 1
2 DOCUMENTS INCLUDED IN THE MERCHANT AGREEMENT 3
3 DEFINITIONS 3
4 SCOPE 4
5 PROCESSING OF PERSONAL DATA 4
6 CONFIDENTIALITY 5
7 TERM AND TERMINATION 5
8 TERMINATION FOR CAUSE 5
9 FORCE MAJEURE 6
10 AMENDMENTS 6
11 ASSIGNMENT 6
12 GOVERNING LAW AND DISPUTES 7
13 SIGNATURES 7
Contact persons and their power of Attorney 8
self-declaration from the Merchant regarding access to the national identity number of the Merchant's users: 10

2 DOCUMENTS INCLUDED IN THE MERCHANT AGREEMENT

The Merchant Agreement includes the following documents:

Main body: This document - including

- Contact persons and their power of attorney
- Self-declaration for the use of National identity number (if applicable)

Appendix 1: Specific Terms and Conditions for the Issuer's liability.

Appendix 2: The Standard terms and conditions for the use of BankID Services at Merchant.

Appendix 3: Specific Terms and Conditions for KYC/AML Services at Merchant.

Appendix 3A: Data processing agreement for KYC/AML Services at Merchant.

In the event of inconsistency between the Main body and the appendices the appendices take precedence in their numeric order. Specific terms take precedence before standard terms and the Main body.

3 DEFINITIONS

Agreement framework: The Merchant agreement with appendices, the Certificate Policy and the Documentation made available on the Company's webpages.

Bank ID Authentication: To confirm the identity of the sender or recipient through electronic message exchange/communication by using BankID Services.

BankID Certificate Electronic certificate(s) and associated software, which may be used for electronic message exchange, between parties where each of them holds a valid certificate. The certificate(s) may be used for e.g., electronic message exchange as part of authentication, signing, conclusion of agreements, payment mediation/payment order in banks, etc. The Term encompasses both certificates of natural and legal persons.

BankID Regulation: The regulation that sets out the rights, obligations, and responsibilities between issuers of BankID Certificates, Finance Norway Service Office, and Bits AS.

BankID Services: Any service and associated software connected to the brand BankID provided by the Company for further delivery from the Company or the Reseller to Merchant.

BankID Signature: An electronic signature according to the eIDAS Regulation which meets the requirements for advanced electronic signature based on a qualified electronic signature certificate.

Bits AS: The infrastructure company of the banking and finance industry, responsible for i.e., BankID regulations. Bits AS is the supervisory authority for the *BankID regulations* and the public legal requirements for the BankID Services.

Certificate holder: A physical person who has been issued with a BankID Certificate.

Certificate policy: The current policy for issuing and using BankID Certificates, available on the Company's BankID website.

The Company: BankIDBankAxept AS organization no.927 611 929.

Documentation: The Company's current documentation for testing, integration, implementation, use and modification of the BankID Services accessible for the Reseller.

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

Merchant: A legal entity, registered in the Enterprise Register for Legal Entities or similar public register within the EEA area, who have a customer relationship with a Norwegian bank.

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

Ordering routines: The Company's current procedures for ordering and changing the BankID Service(s).

Party: The Issuer, 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.

Secure electronic message exchange: Confirmation of the correct identity of the parties (authentication), securing the content against change (integrity), linking the message to a specific party (non-denital) and/or hiding the content from unauthorized persons (encryption).

Software(s): The associated software as an integral part of the BankID Service.

Trademark: Norwegian trademark register no 257727, 258031, 290364 and 290365.

Valid BankID Certificate BankID Certificate which has that has not been revoked or suspended and where the validity period has not expired.

4 SCOPE

The Merchant agreement is entered between the Merchant and the Company or the Reseller on behalf of the Company. The Parties rights and obligations are stated Merchant agreement with appendices and is legally binding for the Merchant when signed by authorized personnel in the Merchant's organization.

The Merchant agreement is legally binding for the Reseller, the Company, or the Issuer when the Issuer and/or the Company has approved the Merchant.

The Issuer is a Party in the Merchant agreement. The Issuer has, by signature of the Reseller on behalf of the Issuer, agreed to be committed by the rights and obligations of the Merchant agreement. The signature is stated Merchant agreement's front page. The Issuers rights and obligations as specified in Appendix 1 *Specific Terms and Conditions for the Issuer's liability.*

The Merchant will be given access to the BankID Service including and associated Software and Documentation for implementation in accordance with the Merchant agreement with appendices.

The Merchant agreement does not include other services or any commercial terms for delivery of the BankID Service (price, etc.). Conditions for such services are stated in separate agreement(s) between the Merchant and 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.

Disclosure of the Certificate holders' national identity number to the Merchant in connection with the Merchant's use of the BankID Service, requires legal basis. See applicant declaration form in the Merchant agreement Main body.

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 BankID 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 Party in connection with the Merchant agreement, including confidential information relating to the the BankID Service, the Software, the Company or the Issuer. 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 Reseller 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, agreements with the Issuer, 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.

If the Merchant is no longer a customer of the Issuer, the Merchant agreement terminates simultaneously.

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

7.3 Effects of the termination

In the event of termination of the Merchant agreement for any reason, the Merchant shall immediately destroy any software received, including any copies, for use of the BankID Service. The Merchant must simultaneously stop all use of the trademark.

The Merchant's BankID Service will be invalid for further use.

8 TERMINATION FOR CAUSE

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

- A Party commits a substantial breach of the Merchant agreement with appendices.
- 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.

- The Merchant no longer has a customer relationship to a Norwegian bank that is authorized to issue BankID and thus no longer has a valid BankID.
- The Merchant becomes petitioned for bankruptcy and such a bankruptcy petition is not averted within thirty (30) days.
- 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, the Merchant uses BankID Services or BankID Certificate in the course of infringement, illegal activities or in a manner that could impair the trust, the reputation or the goodwill of the BankID brand, the BankID Service, the Issuer, other issuers, the Reseller or the Company.

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 as 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.

The Parties are obliged to notify each other without undue delay in the event of a Force Majeure situation.

In the case of Force Majeure, each of the Parties may terminate the Merchant agreement 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 and supplement contained in the BankID Service as described in the product 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 BankID Services.

The Issuer and the Company may change the *Specific Terms and Conditions for the Issuers' liability* and the *Standard terms and conditions for the use of BankID Services at Merchant.* upon three (3) months written notice.

Any amendments of substantial nature of the Merchant damage shall be executed with at least six (6) months' notice. As substantial change is for example that the Merchant must carry out substantial changes in their systems to use the BankID Services.

The Issuer may unilaterally modify the *Specific Terms and Conditions for the Issuers' liability* according to the terms and conditions outlined in the *Specific Terms and Conditions for the Issuers' liability*.

To the extent of subjects related to the Merchant such as for example security conditions or orders from public authorities, the Company unilaterally and without prior notice, may change the Merchant agreement the extent necessary. The Company will in such situations as soon as possible after the change notify the Reseller or the Merchant directly.

11 ASSIGNMENT

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

The Reseller, the Company and the Issuer 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, 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.

A deviant dispute solution is agreed for disputes regarding the Issuer. See *Specific Terms and Conditions for the Issuers' liability.*

13 SIGNATURES

By signing the Merchant agreement, the Reseller confirms to the Issuer that the person(s) who have signed the Merchant agreement on behalf of the Merchant are authorized to sign or have been granted the power of attorney in accordance with the certificate of registration, which is no more than two (2) months old of the date of conclusion for this Merchant agreement.

The Reseller also confirms that the person(s) who have signed the Merchant agreement on behalf of Merchant have provided Reseller with proof of identification

Place and date	Place and date
For [name of the Reseller]:	**For** [name of the Merchant]:
[name]	[name]
[title]	[title]

On behalf of the Issuer, it is confirmed that the Issuer is committed by the rights and obligations of the Issuer explicitly stated in *Specific Terms and Conditions for the Issuers' liability* and *Standard terms and conditions for the use of BankID Services at Merchant.*

Place and date

For [Name of Issuer] represented by [Name of Joint Issuer] represented by Reseller:

[name in block letters]

[title in block letters]

CONTACT PERSONS AND THEIR POWER OF ATTORNEY

Merchant business information		
Merchant's business name:	Organisation number:	Unit/department:
Merchant's contact person		
Name:	Mobile phone number:	
E-mail:		
Power of attorney to receive (activation URL and installation code) and renew the BankID Service:		
Name 1:	Mobile phone number:	
E-mail (for receipt of the activation URL):		
Name 2:	Mobile phone number:	
E-mail (for receipt of the activation URL):		
Power of attorney to block/revoke the BankID Services:		
Name 1:	Mobile phone number:	
E-mail:		
Name 2:	Mobile phone number:	

E-mail:

Signatory(s) at Merchant:	
Name 1:	Email:
Name 2:	Email:
Name 3:	Email:
Name 4:	Email:
Name 5:	Email:
Name 6:	Email:

Signatory(s) Reseller:	
Name 1:	Email:
Name 2:	Email:
Name 3:	Email:

SELF-DECLARATION FROM THE MERCHANT REGARDING ACCESS TO THE NATIONAL IDENTITY NUMBER OF THE MERCHANT'S USERS:

As a Merchant we have the need to process our customers' national identity number in connection with _____ (purpose of the handling)

On the following specified legal base:

_____paragraph_____

We hereby declare that we will only obtain a national identity number as far as the specified legal basis. We understand that the national identity number cannot be collected for the registration of new customers, unless the Merchant obtain an informed consent from the Certificate holder.

We also declare that any subsequent processing of the received national identity number will not be processed in violation of the legal base, the Merchant agreement here or the rules of the Personal Data legislation.

If the Merchant has a duty of registration pursuant to Section 12 of the Anti-Money Laundering Act as a basis for processing the customer's national identity number, this self-declaration is considered as a statement from the Merchant that the Merchant is a reporting activity in accordance with Section 4 of the Anti- Money Laundering Act.

APPENDIX 1 SPECIFIC TERMS AND CONDITIONS FOR THE ISSUER'S LIABILITY

1 BACKGROUND

These *Specific terms and conditions for the Issuer's liability* govern the Issuer's liability towards the Merchant. The Issuer is stated as the Merchant's bank relation.

The Issuer has authorised the Company and those who the Company may, as per agreement with the Issuer, authorise to enter into a Merchant agreement with the Merchant on behalf of the Issuer. The *Specific terms and conditions for the Issuer's liability* is a part of the Merchant agreement.

All terms and expressions defined in Merchant agreement shall be considered similar in the *Specific terms and conditions for the Issuer's liability*, unless otherwise defined herein.

2 ROLE OF THE ISSUER

The Issuer is responsible for the issuing of the BankID to the Merchant.

2.1 The Issuer's control of an order

As soon as possible after receipt of the order of the BankID Merchant certificate, the Issuer will:

a) Verify that the Merchant is a customer of the Issuer or an affiliated bank.

b) Verify that the Issuer possesses and/or has received enough documentation to identify the Merchant and the Merchant's signatory/signatories.

c) Verify that the Reseller is listed on the Company's List of Resellers, available on the Company's website.

d) Verify that there are no significant errors or omissions of importance for the issuing of BankID Merchant certificate.

2.2 Routines and procedures

Ordering routines and procedures for Issuance are stated in the Service Manual available on the Company's website.

3 LIABILITY AND LIMITATION OFLIABILITY

3.1 Liability

The Issuer is only liable for direct losses suffered by the Merchant as a result of the Merchant incorrectly relying on someone else's BankID Certificate, if the Issuer, someone the Issuer is liable for (e.g., a subcontractor or assistant) or another issuer acted negligently in connection with issuing, using or validating the BankID Certificate.

In case of the following causes of damages, the Issuer must prove that the person(s) mentioned in the first section did not act negligently ("reverse burden of proof"):

a) BankID was issued to unauthorized receiver.

b) The mandatory required information entered was incorrect at the time of issuance.

c) BankID did not contain all the information required in accordance with the BankID Regulation.

d) Secure products and systems were not used for the issuance of BankID Merchant certificate and production of digital signatures, or

e) A loss notification or revocation of the BankID was not registered correctly, and hence this reason, an incorrect response was given to a validity check.

3.2 Limitation of liability

The Issuer is not liable for indirect losses (e.g., loss of profits or other consequential loss as a result of downtime) suffered by the Merchant, unless the loss was caused by gross negligent or wilful intent or omission by the Issuer or an entity for whom the Issuer is liable.

The Issuer is not liable for damages resulting from the use of the BankID Servicesnin violation of restrictions in the agreed scope, which has been clearly stated towards someone who has relied on the BankID Certificate.

Furthermore, the Issuer is not liable for any loss resulting from the Merchant using the BankID Merchant certificate or Software in violation of the Merchant agreement, the Documentation, or the relevant BankID regulations, including if the Merchant performs unauthorised modification or manipulation of the BankID Service or the Software.

No matter the forthgoing, the Issuer's liability is limited to the maximum amount of NOK 100,000, - per transaction.

The Issuer's liability also lapses to the extent the Merchant has its losses covered by others, e.g., the Issuer of an abused BankID Certificate.

4 CHANGES TO THE TERMS

The Issuer and the Company may change these *Specific terms and conditions for the Issuer's liability* at reasonable notice, including the limitation of liability to NOK 100,000 per transaction, cf. section 3.2 above.

5 ARBITRATION AND VENUE

Any dispute, controversary or claim that arises to the interpretation or legal effect of these *Specific terms and conditions for the Issuer's liability*, shall be attempted resolved through negotiations.

If such negotiations do not proceed, the dispute will be finally settled by arbitration in accordance with the Norwegian Arbitration Act. The arbitration will be conducted in Oslo.

The arbitration process and arbitration decisions in any arbitration are subject to the duty of confidentiality.

APPENDIX 2 STANDARD TERMS AND CONDITIONS FOR THE USE OF BANKID SERVICES AT MERCHANT

TABLE OF CONTENT

1 BANKID 14
2 REGULATIONS AND ROLES 14
3 USE OF BANKID 15
4 MERCHANT REQUIREMENTS 15
5 NOTIFICATION OF SIGNIFICANT CONDITIONS 16
6 TERMS AND CONDITIONS MERCHANT'S COLLECTION OF NATIONAL IDENTITY NUMBERS. 16
7 CONTROL, DELIVERY AND INSTALLATION OF BANKID 17
8 SAFETY PROCEDURES - USE, ACCESS, CONTROL AND BLOCKING 17
9 EXPIRATION AND RENEWAL OF BANKID 18
10 VALIDITY CHECK AND VALIDATION OF SIGNATURES 18
11 MAINTENANCE AND NEW VERSIONS 18
12 INTELLECTUAL PROPERTY RIGHTS AND LICENSE TERMS 19
13 MARKETING 19
14 USE OF THE INFORMATION IN THE BANKID SERVICE 19
15 ERROR OR DELAYS IN BANKID AND SOFTWARE 20
16 LIABILITY 20
17 CHANGES TO THE MERCHANT AGREEMENT OR THE STANDARD TERMS 21

8

1 ABOUT BANKID

BankID is an electronic ID solution (eID) in Norway issued by Norwegian banks and can be used for authentication (login) and signing.

The Certificate holder signature certificates are qualified and are based on Public Key Infrastructure (PKI).

The eTrust (signing) service is registered with the National Communications Authority (Nkom) and on the EU's Trusted list of Trust Service Providers. A BankID certificate meets the requirements for qualified certificates for natural persons and for advanced electronic signature and for advanced electronic signature according to the Norwegian law on electronic trust services and regulation (EU) 910/2014 (eIDAS).

BankID for physical persons has two levels of trust ("High" and "Substantial/Biometrics").

BankID High shall comply with the eID Regulations of eID at the trust level High and is also a trust service based on qualified certificates of electronic signatures. BankID High is used for authentication with the strictest security requirements, and for payment and signing documents.

BankID Biometrics can be used in situations where strong customer authentication (SKA) and/or another two-factor authentication are required. BankID Biometrics can be used in combination with BankID at level High ("Step up").

For more information about the BankID Services, see product information on the Company's website.

The user site's own solution for BankID Services must be adapted to the level of trust based on the parameters that follow BankID High and BankID Biometrics, respectively.

BankID inneholder blant annet følgende opplysninger:

1. Designation of Issuer.
2. Information about the Merchant's company name and Norwegian organization number or another unique identifier.
3. Valid period for the Certificate.
4. Data needed to verify the Merchant's digital signature.
5. The issuer's (or Issuer's partner's) digital signature.
6. Data that uniquely identifies the individual BankID Service (serial number).

The above information will be available to the Reseller, the Company, and the Issuer.

BankID is managed by several actors. Rights, duties, and responsibilities are divided between the actors and are enshrined in legislation and regulations. The Issuer's liability is regulated in BankID Regulations and is described exhaustively in the Appendix *Specific Terms and Conditions for the Issuer's liability*.

The Standard terms and conditions for the use of BankID Services at Merchant only apply to the use of BankID Services at Merchants.

Issuance of BankID to physical persons (Certificate holder) is not included in the Merchant agreement.

2 REGULATIONS AND ROLES

BankID Regulation are a multilateral contractual framework that establishes rights and obligations between issuers of BankID (participants), Finans Norge Servicekontor and Bits AS (hereinafter referred to as Bits). The Issuer enters into an agreement on the use of BankID with its own customers (Certificate

holder). The issuer is registered as a supplier of eID and eTrust with the National Security Authority (Nkom).

Bits determines regulations for BankID, sets certificate policies and sets requirements for BankID towards Issuers. The issuance of BankID certificates is in addition always regulated by the applicable legislation and associated regulations.

The Company provides software and infrastructure that enables banks to provide ID and trust services to the market in accordance with separate agreement with the Issuer.

The Standard terms and conditions for the use of BankID Services at Merchant apply to BankID Biometrics and BankID High as described in the product descriptions in on the Company's website.

The use of BankID Services in addition to what is specified in the Merchant agreement with appendices requires a separate agreement with the Company.

3 USE OF BANKID SERVICES

BankID Services can be used to ensure electronic message exchange between two or more parties by confirming the correct identity of the parties (authentication). BankID Biometrics is used based on technical specification.

In order to secure the content against change and link the message to a specific party (signing), BankID High must be used. If BankID Biometrics is attempted to be used outside its scope, the system will automatically perform step-up to BankID High.

BankID Services can only be used to issue new electronic identification based on data collected by the Merchant itself. The Merchant shall not issue new physical or electronic identification based on data obtained from the Certificate holder's use of BankID Certificate. The use of BankID Services for first-time authentication and then using other authentication mechanisms in later logins can only take place in accordance with the whitelist from the Company made available in the Reseller portal.

Use beyond what is stated above requires a separate agreement with the Company.

4 MERCHANT REQUIREMENTS

4.1 Provision of the BankID Services

BankID Services may only be used by Merchants registered in the Enterprise Register for Legal Entities or a corresponding public register within the EEA and who have a customer relationship with an authorized BankID issuer.

BankID Services may only be delivered to Merchants who meet the applicable requirements in the *Standard terms and conditions for the use of BankID Services at Merchant.*

4.2 Technical requirements for Merchant

Merchant must use the BankID OIDC delivery platform as an integration point for BankID Biometrics.

The Certificate holder can activate the service by providing biometrics/PIN, as well as verifying their identity. The identity can be verified by e.g., logging in with BankID High or scanning passports.

If the identity is confirmed with BankID High a regular check is carried out to verify that the underlying BankID High certificate is still valid.

4.3 Refusal of issuance of BankID

The Reseller, the Company and/or the Issuer may refuse the issuance of BankID to a Merchant when, in the reasonable opinion of the Merchant, the Company or the Issuer, there is a factual reason. Factual reasons, among other things, is:

a) The Merchant's activities and/or use of BankID is in violation of *the Standard terms and conditions for the use of BankID Services at Merchant*, Norwegian law or regulations, requirements, and guidelines of the Norwegian authorities or

b) The Merchant's activities or use of BankID may be undermining confidence in:

   (i) BankID Services, an issuer or the Company, or

   (ii) BankID brand, the reputation or goodwill of the Company.

5 NOTIFICATION OF SIGNIFICANT CONDITIONS

The Merchant shall notify the Reseller as soon as possible of changes in the information provided by the Merchant at the conclusion of the Merchant agreement, including the organization number, address, company name, contact persons ownership, etc.

If the information about the Merchant is incorrect, the Merchant shall, without undue delay, notify the Reseller or the Company after the testing of the BankID Services has been carried out. The Reseller shall, within a reasonable time, ensure that the information is corrected.

If the transaction volume for the Merchant's use of the BankID Service for one or more periods will be or will be significantly higher than normal, the Merchant shall, as soon as possible, after the it became aware of this notify the Reseller of such increased transaction volume. Upon request from the Reseller and/or the Company, the Merchant is obliged without undue delay to deliver forecasts of the expected transaction volume for a specified period.

6 TERMS AND CONDITIONS MERCHANT'S COLLECTION OF NATIONAL IDENTITY NUMBERS.

National identity numbers can only be provided to Merchants that can confirm that available information in BankID Services alone is not sufficient to obtain secure identification of the Certificate holder, and who already has a legal basis for obtaining the Certificate holder's national identity number. The Certificate holder must give consent to the Merchant on the use of national identity numbers. Merchant is Data Controller for the collection of the national identity number. The processing must be in accordance with applicable data protection legislation at all times.

In dialogue with the Certificate holder, the Merchant is obliged to provide information about the legal basis for using a national identity number.

The Merchant shall provide the Issuer with a reasoned declaration that the conditions for requesting the delivery of a national identity number are in place and that the delivery and any subsequent processing of the national identity number will not be used in violation of the Merchant agreement with attachments or personal data legislation. The Issuer, Reseller or Company may at any time require the Merchant to document that it complies with the conditions for processing the national identity number.

A separate "Declaration from the Merchant requesting to access the national identity number for Certificate holders" is included in the Merchant agreement.

7 CONTROL, DELIVERY, AND INSTALLATION OF BANKID

7.1 Control

Upon receipt of BankID Service (both upon direct receipt to the Merchant or receipt of the Distributor on behalf of the Merchant), the Merchant shall immediately check that the contained information matches the order. The Reseller shall check the information about the Merchant and uncover errors or defects.

The Reseller shall without undue delay notify the Company/Issuer in the event of errors or omissions.

7.2 Delivery and installation

BankID Service is usually disclosed to the Reseller's contact person on behalf of the Merchant.

The Merchant shall install, integrate, and test in accordance with the Documentation, and otherwise ensure the safety of its own systems. The Reseller and/or the Company may verify that the BankID Service has been installed and upgraded in a satisfactory manner, and the Merchant is obliged to provide the Reseller and/or the Company with the necessary access to relevant systems in this regard.

The Merchant shall only use any software, machine equipment or safety equipment provided in the Documentation.

In a separate agreement with the Merchant, the Reseller may assist the Merchant with installation, integration, and testing, etc.

8 SAFETY PROCEDURES - USE, ACCESS, CONTROL AND BLOCKING

8.1 Usage, access, and control

The BankID Service may only be used in accordance with the terms of the Agreement framework.

The BankID Service shall not be transferred or otherwise entrusted to, or used by, anyone other than the Merchant. Passwords and other procedures must not be disclosed to unauthorized persons.

8.2 Situations of loss

The Merchant must notify the Reseller in writing as soon as possible after the Merchant has detected or suspected that the BankID Service, and/or its password and/or code has gone astray or that unauthorized persons have gained knowledge of the password/code. The notification should contain a description of the situation and, as far as possible, the incident at hand.

8.3 Blocking

The Merchant shall not use the BankID Service and/or approve any use after loss situations have occurred but assist in such a way that the BankID Service is blocked as quickly as possible.

The Reseller shall ensure that a Merchant's BankID Service that is, or can be expected to be, misused or that no longer contains correct information is blocked (suspended or revoked).

Furthermore, the Reseller, the Company and/or the Issuer may block the Merchant's BankID Service if, in the reasonable opinion, there is a factual reason, including that the BankID Service are, or can be expected to be, misused, used for illegal activities, or no longer contain correct information.

Factual grounds also applies if the Merchant's use of BankID Service may be suitable for undermining confidence in.

- BankID brand, an issuer or the Company, or
- BankID Service, the Reseller, an issuer's or the Company's reputation or goodwill.

The Reseller may, by proxy from the Merchant, request a hold/revocation of BankID Service that has not been used for 6 months.

9 EXPIRATION AND RENEWAL OF BANKID SERVICE

9.1 Expiration Alert

The Company shall notify the Reseller of the expiry date in connection with monthly invoicing. The Reseller shall notify the Merchant of the need for renewal of BankID Service no later than 1 month before the expiry date. Notification is made to the person who is registered as eligible for signature pursuant to the Merchant agreement.

9.2 Renewal

If the Issuer must be involved in the renewal, the Reseller shall send an order to the Issuer. The order shall contain all the necessary information in order to carry out the renewal.

The same rules and procedures for renewal apply as for issuing a new BankID Service.

10 VALIDITY CHECK AND VALIDATION OF SIGNATURES

Systems for validity control have been established. The Merchant shall always carry out validity checks in accordance with the Documentation.

A register of valid BankID Service has also been established, as well as for BankID Service which has been suspended or revoked (invalid). The registered information will be retained for at least ten (10) years after the validity period for BankID Service has expired or been revoked.

Information about valid and suspended/revoked BankID Service will be exchanged to the Issuer and other authorized issuers.

The information will only be used to verify that the Merchant's BankID Service is valid and that its use is in accordance with the Agreement framework.

Signatures correctly packaged in the Company's supported formats may be validated with open tools or using available software from the Company.

11 MAINTENANCE AND NEW VERSIONS

The Merchant will receive written notice of a new version of BankID and the Software no later than three (3) months before it must be used by the Merchant.

The notification should contain information about

- when and where a new version of BankID and/or software is made available, and
- when the Merchant may access the test environment, and
- which versions are supported after the change.

The Merchant is obliged to install and/or integrate new versions of BankID Service and/or the Software within the deadline set by Company.

12 INTELLECTUAL PROPERTY RIGHTS AND LICENSE TERMS

BankID is copyrighted and a registered trademark. All intellectual property rights, such as, but not limited to, patents, copyrights, trademarks, and design rights of BankID Services, the Trademark, the Software and associated Documentation and the BankID Policy are the property of the Company and/or its licensors, subcontractors or affiliates.

The Merchant is granted a limited, non-exclusive, non-transferable, revocable license to use the Trademark, the BankID Service, the Software and the Documentation in connection with the provision, installation, integration, and use of BankID Service as further stated in the Documentation and is not granted any intellectual property rights, in whole or in part, to BankID Service, the Trademark, the Software or any associated Documentation. The Merchant is not entitled to make any changes (in the event of further development or otherwise).

The Software may only be used on, and integrated with, the technical platforms and systems set out in the Documentation. The Merchant may copy the Software to the extent necessary for the purpose, including making necessary backups.

BankID Services may only be used in connection with the Merchant's own business and cannot be forward licensed.

The Reseller and/or the Company has the right to control that the license terms are complied with, and the Merchant is obliged to provide the Reseller and/or the Company with the necessary access to the Merchant's systems and use of BankID Service and the Software in the event of such control.

13 MARKETING

The Merchant has the right and obligation to use the Trademark when using BankID Service and to highlight that the Merchant uses BankID Services in its activities. The presentation of the Trademark shall have the form, format, color, and quality in accordance with requirements set out in the Company's profile manual at any given time and only used in accordance with the guidelines set out on the Company's website at any time.

The Reseller and/or the Company has the right to disclose that the Merchant uses BankID Services in its activities on its website and in other relevant marketing.

14 USE OF THE INFORMATION IN THE BANKID SERVICE

When using BankID Service, the information will be included in the message exchange between the Merchant and the Certificate holder. The information may be made available to the Certificate holder. Other information about the Merchant in connection with the use of BankID Service will only be disclosed to other Certificate holders if the Reseller, the Company, or the Issuer has a statutory duty of disclosure or there is an express consent from the Merchant and the Certificate holder.

The Merchant agrees, upon entering into the Merchant agreement, that the Reseller and/or the Company may receive, use and store information from the Issuer about the number of transactions per transaction type used in the BankID Service at the Merchant.

The information shall only be used to establish and maintain a register of the Merchants and their transactions for invoicing of the Merchant and further development of the BankID Service and handed out to the Reseller and/or the Company's partners to the extent necessary for billing purposes.

The information is received, stored, used, or disclosed for as long as necessary or permitted by relevant legislation.

15 ERROR OR DELAYS IN BANKID SERVICES AND SOFTWARE

Unless otherwise specifically agreed with the Reseller, BankID and its software are provided "as is", and the Merchant is not guaranteed that the BankID Service and/or the Software is free of errors. There is no guarantee that the BankID Service and associated Software will work with third-party products, unless explicitly stated in the Documentation.

The Reseller has no liability for defects in or delayed delivery of BankID Service and its associated Software without a separate agreement.

16 LIABILITY

The Reseller and/or the Company is not liable for any use of BankID Services that is in violation of the *Standard terms and conditions for the use of BankID Services at Merchant*, recommendations from the Company and/or Reseller or Regulations, Bits AS and legislation or orders from the public authority.

Claims from the Merchant in connection with the Merchant agreement, BankID Service, the Software or shall be directed to the Reseller. If the Merchant files a claim for compensation due to circumstances resulting from errors or defects in BankID Services from the Company and/or the Issuer, the Reseller shall forward the claim to the Company.

16.1 The Merchant's liability

The Merchant is liable for the losses of the Reseller, the Company and/or the Issuer in accordance with general liability rules for losses resulting from the negligent use of BankID Service, Software, Documentation and losses arising out of actions or omissions in accordance with Agreement framework.

The Merchant is responsible for its own subcontractors. The Merchant shall, in agreement with any subcontractors, impose responsibility on the subcontractors for ensuring that their own deliveries meet the requirements of the Agreement framework.

According to general liability legal rules, the Merchant is further liable for any dispositions made by someone who has been given the opportunity, by intentional or negligent action or omission on the part of the Merchant, to dispose of the Merchant's BankID Service or the Software.

16.2 The Issuer's liability

The Issuer's liability is exhaustively regulated in *Specific terms and conditions for the Issuer's liability.*

The Merchant may file any claims against the Issuer in accordance with the *Specific Terms of Issuer's liability* to the Company, which will process the claim on the Issuer's behalf. The Company is only the case officer for the Issuer and is not deemed to have assumed any independent responsibility for the requirements the Merchant may have in accordance with the *Specific Terms of Issuer's liability.*

16.3 The Reseller and the Company's liability

Between the Reseller and the Company, general tort for control liability rules applies. A Party may be reimbursed for its direct loss if the other Party cannot prove that the cause of the injury-causing incident was beyond his control. Subcontractors are considered to be within a Party's control sphere.

If the loss-triggering event is beyond the subcontractor's control, it is considered a third party's sphere of control that cannot be invoked against neither the Company nor the Reseller.

16.4 Limitation of liability

Regardless of the foregoing, indirect losses are not covered. Indirect losses are, for example, but not limited to, loss of profit, loss of data or other consequential loss as a result of downtime unless the loss

is due to gross negligence or intentional action by the Reseller/Company and/or any Reseller/Company is in control of.

Under no circumstances is neither the Company nor the Reseller liable for losses resulting from circumstances that is included in the *Special Conditions of the Issuer's liability*. Any such claim shall be directed to the Issuer or to the Company on behalf of the Issuer.

Neither Party is liable for any losses resulting from the Merchant using the BankID Service, the Software, the Documentation in violation of the Agreement framework, including making unwarranted alteration or manipulation of BankID Service or the Software.

The Company/Reseller's liability lapses to the extent that the Merchant has had its loss covered by others, for example by the Issuer or issuer of the misconducted BankID Service.

The Reseller's/Company's total liability to the Merchant under the Merchant agreement with respect to one or more incidents (whether connected or not), shall not in any case exceed an amount the total amount of compensation a Party may claim during the term of the Merchant agreement is limited to an amount equal to the consideration invoiced between the Parties in the 12 months prior to the date of claim for compensation.

If the BankID Service has not been completed in the last 12 months prior to the date of claim for compensation was made, the total amount of compensation that may be claimed by a Party is limited to an amount equal to the average monthly amount already invoiced, with upward adjustment to 12 months.

The limitation of liability does not apply to circumstances resulting from gross negligence or willful intent.

17 CHANGES TO THE MERCHANT AGREEMENT OR THE STANDARD TERMS

Minor change in the content and terms relating to the BankID services and supplements described in the Documentation on the Company's BankID website and in the Reseller portal may be changed unilaterally with two (2) weeks' written notice provided that the change does not have consequences for the Merchant's use of the BankID Service.

The Company may unilaterally change the *Standard terms and conditions for the use of BankID Services at Merchant* with three (3) months' written notice.

Substantial changes of a material nature to the disadvantage of the Merchant shall be notified with at least six (6) months' notice.

The Issuer may unilaterally change the contents of the *Specific Terms and Conditions for the Issuer's liability* on terms set out in Appendix 1.

18 ENTRY INTO FORCE

The Terms and conditions enter into force on 15.8.2022 and apply until they are replaced by new terms and conditions.

****

APPENDIX 3 SPECIFIC TERMS AND CONDITIONS FOR AML/KYC SERVICES TO MERCHANT

TABLE OF CONTENT

1 GENERAL 23
2 CONTENT OF THE SERVICES 23
3 REQUIREMENTS FOR MERCHANT 23
4 THE QUALITY OF THE INFORMATION 23
5 DATA PROCESSING AGREEMENT (DPA) 24
6 REQUIREMENTS FOR THE MERCHANT'S USE OF INFORMATION FROM THE SERVICE 24
7 THE MERCHANT'S RESPONSIBILITIES IN ACCORDANCE WITH THE ANTI-MONEY LAUNDERING ACT 24
8 RESPONSIBILITY OF THE COMPANY/RESELLER 24
9 SERVICE LEVEL 24

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 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.

3 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*.

4 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.

5 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.

6 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.

7 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.

8 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 Service.

9 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 3A 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.

4 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.

5 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.

6 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)

7 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.

8 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.

9 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 Basefarm as a 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 Basefarm.

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.

10 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.

11 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.

12 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

13 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.

14 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.

15 EFFECTS OF TERMINATION

Upon termination of this 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.

16 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.