

## DATABASEHANDLERAVTALE

### 1. BAKGRUNN OG FORMÅL

Dette databehandlingssupplementet ("**Databehandleravtalen**") er en del av hovedavtalen ("**Hovedavtalen**") mellom Kunden (den "**Behandlingsansvarlige**") og Equoro Solutions AS og Equoro Issuer Services AS (sammen "**Databehandleren**"), der begge utgjør en "**Part**", samlet benevnt som "**Partene**".

1.1 Formålet med denne Databehandleravtalen er å fastlegge Partenes rettigheter og plikter vedrørende Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige under Hovedavtalen.

1.2 Denne Databehandleravtalen erstatter alle tidligere avtaler og bestemmelser Partene imellom hva gjelder personvern.

1.3 Med unntak for det som er spesifisert her, skal Hovedavtalens betingelser gjelde. I tilfelle uoverensstemmelse mellom Hovedavtalen og denne Databehandleravtalen når det gjelder forhold spesifikt knyttet til personvern, skal Databehandleravtalen gis forrang.

### 2. DEFINISJONER

2.1 I denne Databehandleravtalen skal følgende ord og uttrykk ha den betydning som er angitt nedenfor.

2.2 "**Gjeldende personvernregler**": Gjeldende lover og regler om personvern, inkludert personopplysningsloven og GDPR (fra og med 25. mai 2018).

## DATA PROCESSING AGREEMENT

### 1. BACKGROUND AND PURPOSE

This Data Processing Supplement (the "**Data Processing Agreement**") is part of the main agreement (the "**Main Agreement**") between the Client (the "**Data Controller**") and Equoro Solutions AS and Equoro Issuer Services AS (together the "**Data Processor**"), both of which constitute a "**Party**", collectively referred to as the "**Parties**".

The English text in this agreement is a direct translation of the Norwegian text. In the event of any discrepancies or conflicts between the Norwegian and English text, the Norwegian text shall prevail.

1.1 The purpose of this Data Processing Agreement is to determine the Parties' rights and obligations regarding the Data Processor's processing of personal data on behalf of the Data Controller under the Main Agreement.

1.2 This Data Processing Agreement supersedes all previous agreements and provisions between the Parties with respect to data protection.

1.3 Except as specified herein, the terms and conditions of the Main Agreement shall apply. In the event of any inconsistency between the Main Agreement and this Data Processing Agreement with regard to matters specifically related to data protection, the Data Processing Agreement shall take precedence.

### 2. DEFINITIONS

2.1 In this Data Processing Agreement, the following words and expressions shall have the meaning set out below.

2.2 "**Applicable Privacy Policy**": Current data protection laws and regulations, including the Personal Data Act and GDPR (as of May 25, 2018).

2.3 **"GDPR"**: EUs personvernforordning 2016/679.

2.4 **"Standardklausuler"**: Standardklausuler for overføring av personopplysninger til databehandlere etablert i tredjestater, etablert ved EU-kommisjonens vedtak av 5. februar 2010 og/eller som etablert av EU-kommisjonen eller en relevant tilsynsautoritet i henhold til GDPR artikkel 28(7) eller 28(8);

2.5 **"Underdatabehandler"**: En annen databehandler engasjert av Databehandleren.

2.6 **"Tredjestat"**: Et land utenfor EØS som EU-kommisjonen ikke har fastslått at sikrer et tilstrekkelig beskyttelsesnivå.

2.7 For øvrig skal ord og uttrykk ha samme mening som de er tillagt i GDPR.

### 3. OMFANG

3.1 Denne Databehandleravtalen gjelder alle personopplysninger som Databehandleren har mottatt, er gitt tilgang til eller har generert i forbindelse med Hovedavtalen.

3.2 Denne Databehandleravtalen skal, så langt den passer, også omfatte behandling av data som ikke er personopplysninger som Databehandleren har mottatt, er gitt tilgang til eller har generert i forbindelse med Hovedavtalen. Begrepet "personopplysninger" skal, så langt det passer, derfor også omfatte data som ikke er personopplysninger.

3.3 Databehandlingens formål og art, typen personopplysninger som behandles, samt kategorier av registrerte fremgår av Vedlegg 1.

### 4. GENERELLE PLIKTER

4.1 Databehandleren garanterer å ha gjennomført egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i henhold til gjeldende personvernregler og ivaretar de registrertes

2.3 **"GDPR"**: The EU General Data Protection Regulation 2016/679.

2.4 **"Standard Contractual Clauses"**: Standard Contractual Clauses for the transfer of personal data to processors established in third countries, established by a decision of the European Commission of 5 February 2010 and/or as established by the European Commission or a relevant supervisory authority pursuant to Article 28(7) or 28(8) of the GDPR.

2.5 **"Sub-Processor"**: Another Data Processor engaged by the Data Processor.

2.6 **"Third State"**: A country outside the EEA that has not been determined by the European Commission to ensure an adequate level of protection.

2.7 Otherwise, words and expressions must have the same meaning as attributed to them in GDPR.

### 3. SCOPE

3.1 This Data Processing Agreement applies to all personal data that the Data Processor has received, has been given access to or has generated in connection with the Main Agreement.

3.2 This Data Processing Agreement shall, as far as it is appropriate, also cover the processing of data that is not personal data that the Data Processor has received, has been given access to or has generated in connection with the Main Agreement. The term "personal data" shall, as far as appropriate, therefore also include data that is not personal data.

3.3 The purpose and nature of the data processing, the type of personal data processed, and the categories of data subjects are set out in Appendix 1.

### 4. GENERAL OBLIGATIONS

4.1 The Data Processor guarantees that it has implemented appropriate technical and organizational measures to ensure that the processing meets the requirements in accordance with applicable data protection

rettigheter, og at disse tiltakene vil etterleves i hele avtaleperioden.

4.2 Databehandleren skal behandle personopplysningene utelukkende for det formål og innenfor det omfang som er angitt i Vedlegg 1 og for øvrig i samsvar med den Behandlingsansvarliges dokumenterte instruks.

4.3 Databehandleren skal omgående underrette den Behandlingsansvarlige skriftlig hvis den har rimelig grunn til å tro at (i) en instruks fra den Behandlingsansvarlige kan medføre at Databehandleren bryter med gjeldende personvernlovgivning, eller (ii) gjeldende rett i EØS-området krever at Databehandleren behandler personopplysninger utover omfanget av den Behandlingsansvarliges dokumenterte instruks, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal Databehandleren underrette den Behandlingsansvarlige så snart retten tillater det). I tilfelle av (i) eller (ii) skal Partene i god tro diskutere hvordan problemet kan løses uten at det negativt påvirker vernet av de registrertes rettigheter.

## 5. BISTAND TIL DEN BEHANDLINGSANSVARLIGE

5.1 Databehandleren skal, ved hjelp av egnede tekniske og organisatoriske tiltak, bistå den Behandlingsansvarlige i den grad det er mulig å oppfylle den Behandlingsansvarliges plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i GDPR kapittel 3, herunder anmodninger om informasjon, innsyn, korrigering, sletting, begrensning av behandlingen, dataportabilitet, innsigelser, og det å ikke være underlagt automatiserte individuelle avgjørelser.

5.2 Med hensyn til behandlingens art og den informasjon som er tilgjengelig for databehandleren, skal Databehandleren bistå den Behandlingsansvarlige med forpliktelsene i henhold til GDPR artikkel 32 til 36, herunder forpliktelsene til datasikkerhet (som nærmere beskrevet i punkt 6), melding om brudd på

rules and safeguards the rights of the data subjects, and that these measures will be complied with throughout the contract period.

4.2 The Data Processor shall process the personal data exclusively for the purpose and within the scope set out in Appendix 1 and otherwise in accordance with the Data Controller's documented instructions.

4.3 The Data Processor shall promptly notify the Data Controller in writing if it has reasonable grounds to believe that (i) an instruction from the Data Controller may result in the Data Processor violating applicable data protection legislation, or (ii) applicable law in the EEA requires the Data Processor to process personal data beyond the scope of the Data Controller's documented instructions, unless this right prohibits such notification for reasons of important public interest (in which case in the event that the Data Processor shall notify the Data Controller as soon as the court so permits). In the event of (i) or (ii), the Parties shall discuss in good faith how the issue can be resolved without adversely affecting the protection of the rights of data subjects.

## 5. ASSISTANCE TO THE DATA CONTROLLER

5.1 The Data Processor shall, by means of appropriate technical and organizational measures, assist the Data Controller to the extent possible to fulfil the Data Controller's obligation to respond to requests made by the data subject for the purpose of exercising its rights set out in Chapter 3 of the GDPR, including requests for information, access, correction, deletion, restriction of processing, data portability, objections, and not being subject to automated individual decisions.

5.2 With regard to the nature of the processing and the information available to the Data Processor, the Data Processor shall assist the Data Controller with the obligations pursuant to Articles 32 to 36 of the GDPR, including the data security obligations (as further described in Section 6), notification of

personopplysningssikkerhet (som nærmere beskrevet i punkt 9), vurdering av personvernkonsekvenser, samt forhåndsdrøftinger.

5.3 Databehandleren skal ikke kommunisere direkte med de registrerte eller med tilsynsmyndigheter med mindre dette er forhåndsgodkjent av den Behandlingsansvarlige. Databehandleren skal umiddelbart videresende til den Behandlingsansvarlige forespørsler eller klager som den eventuelt mottar fra de registrerte. Databehandleren skal også umiddelbart videresende eventuelle forespørsler fra en tilsynsmyndighet som gjelder inspeksjoner, undersøkelser, eller tilgang til eller informasjon om personopplysninger, med mindre loven forbyr det (i så fall skal Databehandleren underrette den Behandlingsansvarlige så snart loven tillater det).

5.4 Bistand etter punkt 5 skal skje mot betaling i henhold til Databehandlerens alminnelige timepriser.

## **6. TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK**

6.1 Databehandleren skal gjennomføre egnede tekniske og organisatoriske sikkerhetstiltak for å verne personopplysningene mot utilsiktet eller ulovlig tilintetgjøring, tap, endring, ikke-autorisert utlevering eller tilgang. Databehandleren skal som et minimum gjennomføre de tiltakene som er påkrevd i henhold til GDPR artikkel 32, samt de tiltak som er angitt eller referert til i Vedlegg 2.

6.2 Databehandleren skal ikke utlevere eller tilgjengeliggjøre personopplysninger for tredjeparter uten skriftlig forhåndsgodkjennelse fra den Behandlingsansvarlige, med unntak for eventuelt godkjente underdatabehandlere i den utstrekning de har behov for opplysningene for å kunne utføre sine oppgaver.

6.3 Databehandleren skal påse at alle personer som er autorisert til å behandle personopplysningene har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt. På

personal data breaches (as further described in Section 9), data protection impact assessment, as well as prior discussions.

5.3 The Data Processor shall not communicate directly with the data subjects or with supervisory authorities unless this has been pre-approved by the Data Controller. The Data Processor shall immediately forward to the Data Controller any requests or complaints that it may receive from the data subjects. The Data Processor shall also immediately forward any requests from a supervisory authority relating to inspections, investigations, or access to or information regarding Personal Data, unless prohibited by law (in which case the Data Processor shall notify the Data Controller as soon as permitted by law).

5.4 Assistance pursuant to section 5 shall be provided against payment in accordance with the Data Processor's ordinary hourly rates.

## **6. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES**

6.1 The Data Processor shall implement appropriate technical and organizational security measures to protect the personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. The Data Processor shall, as a minimum, implement the measures required pursuant to Article 32 of the GDPR, as well as the measures specified or referred to in Appendix 2.

6.2 The Data Processor shall not disclose or make available personal data to third parties without the prior written consent of the Data Controller, with the exception of any approved sub-processors to the extent that they need the data to be able to perform their tasks.

6.3 The Data Processor shall ensure that all persons authorized to process the personal data have undertaken to treat the data confidentially or are subject to an appropriate statutory duty of confidentiality. At the request of the Data

forespørsel fra den Behandlingsansvarlige skal Databehandleren fremlegge kopi av slike personers signerte taushetsavtaler.

## **7. BRUK AV UNDERDATABEHANDLERE**

7.1 Den Behandlingsansvarlige tillater at Databehandleren engasjerer underdatabehandlere. På forespørsel skal den Behandlingsansvarlige motta informasjon om hvem underdatabehandlerne er, samt hvor de behandler personopplysningene. Databehandleren skal underrette den Behandlingsansvarlige om eventuelle planer om å benytte andre underdatabehandlere eller skifte ut underdatabehandlere og gi den Behandlingsansvarlige rett til å motsette seg slike endringer eller å kreve at denne Databehandleravtalen opphører.

7.2 I henhold til punkt 7.1 skal Databehandleren kun engasjere underdatabehandlere som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at databehandlingen oppfyller kravene etter gjeldende personvernregler og som sikrer de registrertes personvern. Databehandleren skal gjennomføre egnede kontroller av underdatabehandlerne for å verifisere deres databeskyttelsesnivå. Databehandleren skal fremlegge rapporter fra slike kontroller for den Behandlingsansvarlige.

7.3 Databehandleren skal inngå skriftlig avtale med hver underdatabehandler som pålegger egne forpliktelser med hensyn til vern av personopplysninger. Når underdatabehandleren er engasjert for å utføre spesifikke databehandlingsaktiviteter på vegne av den Behandlingsansvarlige, skal Databehandler ved skriftlig avtale pålegge underdatabehandleren de samme forpliktelsene med hensyn til vern av personopplysninger som fastsatt i denne Databehandleravtalen. På forespørsel fra den Behandlingsansvarlige skal Databehandleren fremlegge kopi av avtaler med underdatabehandlere. Forretningsmessig og annen forretnings sensitiv informasjon kan dog sladdes.

7.4 Databehandleren har fullt ansvar for underdatabehandlerens utførelse av sine forpliktelser.

Controller, the Data Processor shall provide a copy of such individual's signed non-disclosure agreements.

## **7. USE OF SUB-PROCESSORS**

7.1 The Data Controller allows the Data Processor to engage sub-processors. Upon request, the Data Controller shall receive information about who the sub-processors are, as well as where they process the personal data. The Data Processor shall notify the Data Controller of any plans to use other sub-processors or replace sub-processors and give the Data Controller the right to object to such changes or to demand that this Data Processing Agreement be terminated.

7.2 Pursuant to section 7.1, the Data Processor shall only engage sub-processors who implement appropriate technical and organizational measures to ensure that the data processing meets the requirements of applicable data protection rules and to ensure the privacy of the data subjects. The Data Processor shall carry out appropriate checks on the sub-processors to verify their level of data protection. The Data Processor shall provide reports of such checks to the Data Controller.

7.3 The Data Processor shall enter into a written agreement with each sub-processor that imposes its own obligations with regard to the protection of personal data. Where the sub-processor is engaged to carry out specific data processing activities on behalf of the Data Controller, the Data Processor shall, by written agreement, impose on the sub-processor the same obligations with respect to the protection of personal data as set out in this Data Processing Agreement. At the request of the Data Controller, the Data Processor shall provide a copy of agreements with sub-processors. However, business and other business-sensitive information can be redacted.

7.4 The Data Processor is fully responsible for the sub-processor's performance of its obligations.

## **8. INTERNASJONAL DATAOVERFØRING**

8.1 Databehandleren kan kun overføre personopplysninger til en tredjestat eller en internasjonal organisasjon etter dokumenterte instruksjoner fra den Behandlingsansvarlige. Databehandleren kan imidlertid gjøre dette hvis det kreves i henhold til gjeldende rett i EØS-området. I slike tilfeller skal Databehandleren underrette den Behandlingsansvarlige om nevnte rettslige krav før overføringen, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal Databehandleren underrette den Behandlingsansvarlige så snart retten tillater dette).

8.2 Dersom bruk av en godkjent underdatabehandler krever overføring av personopplysninger til en tredjestat, og slike overføringer er godkjent av den Behandlingsansvarlige, gir den Behandlingsansvarlige Databehandleren fullmakt til å inngå standardklausuler i uendret form med underdatabehandleren på vegne av den Behandlingsansvarlige dersom dette er nødvendig for å tilfredsstille krav etter gjeldende personvernregler. Så snart en slik avtale er inngått skal underdatabehandleren fremlegge en kopi av denne for den Behandlingsansvarlige. Alle slike standardklausuler skal automatisk opphøre ved opphøret av denne Databehandleravtalen.

## **9. BRUDD PÅ PERSONOPPLYSNINGSSIKKERHETEN**

9.1 Databehandleren skal gi skriftlig melding til den Behandlingsansvarlige om eventuelle brudd på denne Databehandleravtalen eller personopplysningssikkerheten. Meldingen skal gis senest 36 timer etter at Databehandleren ble oppmerksom på bruddet.

9.2 Melding om brudd på personopplysningssikkerheten må minst, i den grad det er relevant:

a. beskrive arten av bruddet, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene

## **8. INTERNATIONAL DATA TRANSFER**

8.1 The Data Processor may only transfer personal data to a third country or an international organization on documented instructions from the Data Controller. However, the Data Processor may do so if required by applicable law in the European Economic Area. In such cases, the Data Processor shall notify the Data Controller of said legal claims prior to the transfer, unless such right prohibits such notification for reasons of important public interest (in which case the Data Processor shall notify the Data Controller as soon as the court so permits).

8.2 If the use of an approved sub-processor requires the transfer of personal data to a third country, and such transfers have been approved by the Data Controller, the Data Controller authorizes the Data Processor to enter into standard contractual clauses in unchanged form with the sub-processor on behalf of the Data Controller if this is necessary to satisfy requirements under the applicable data protection regulations. As soon as such an agreement has been concluded, the sub-processor shall provide a copy thereof to the Data Controller. All such standard clauses shall automatically terminate upon termination of this Data Processing Agreement.

## **9. PERSONAL DATA SECURITY BREACHES**

9.1 The Data Processor shall notify the Data Controller in writing of any breach of this Data Processing Agreement or the security of personal data. The notification shall be given no later than 36 hours after the Data Processor became aware of the breach.

9.2 Notification of a breach of personal data security must at least, to the extent relevant:

a. describe the nature of the breach, including, where possible, the categories and approximate number of data subjects affected, and the categories and approximate number of



av og omtrentlig antall personopplysningsposter som er berørt;

b. inneholde, når det er mulig, de berørte registrertes identitet;

c. formidle navn og kontakinformasjon til et relevant kontaktpunkt hos Databehandleren for ytterligere innhenting av informasjon;

d. beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten;

e. beskrive de tiltak som er truffet eller foreslått for å håndtere bruddet, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger;

f. inkludere annen informasjon som kreves for at den Behandlingsansvarlige kan overholde gjeldende personvernregler.

9.3 Databehandleren skal så snart som mulig gjennomføre alle tiltak som beskrevet i punkt e. ovenfor, samt gjennomføre alle de tiltak som med rimelighet kreves for å unngå at det senere oppstår lignende brudd på personopplysningssikkerheten.

Databehandleren skal tillate den Behandlingsansvarlige å undersøke, fastlegge årsaken til og å verifisere de tiltak som er gjennomført eller foreslått av den Behandlingsansvarlige for å håndtere bruddet på personopplysningssikkerheten.

Databehandleren skal, så langt det er mulig, rådføre seg med den Behandlingsansvarlige med hensyn til de tiltak som skal gjennomføres samt overveie innspill fra den Behandlingsansvarlige i den forbindelse.

9.4 Kun den Behandlingsansvarlige har rett til å informere den relevante tilsynsmyndigheten og de berørte registrerte om brudd på personopplysningssikkerheten. Databehandleren skal avstå fra å informere allmennheten eller tredjepart om brudd på personopplysningssikkerheten.

## 10. REVISJON

10.1 Databehandleren skal dokumentere, samt gjøre tilgjengelig for den Behandlingsansvarlige, informasjon som er

personal data items affected;

b. contain, where possible, the identity of the data subjects concerned;

c. pass on name and contact details to the relevant contact point at the Data Processor for further information collection;

d. describe the likely consequences of the personal data breach;

e. describe the measures taken or proposed to deal with the breach, including, if relevant, measures to reduce any harmful effects;

f. include other information required for the Data Controller to comply with the applicable Privacy Policy.

9.3 The Data Processor shall, as soon as possible, implement all measures as described in point e. above, as well as implement all measures reasonably required to avoid similar breaches of personal data security occurring in the future. The Data Processor shall allow the Data Controller to investigate, determine the cause and to verify the measures implemented or proposed by the Data Controller to address the Personal Data breach. The Data Processor shall, as far as possible, consult with the Data Controller regarding the measures to be implemented and consider input from the Data Controller in this regard.

9.4 Only the Data Controller has the right to inform the relevant supervisory authority and the affected data subjects of any personal data breach. The Data Processor shall refrain from informing the public or third parties of any breach of personal data security.

## 10. AUDIT

10.1 The Data Processor shall document, as well as make available to the Data Controller, information that is necessary to demonstrate

nødvendig for å påvise etterlevelse av denne Databehandleravtalen og gjeldende personvernregler.

10.2 Databehandleren skal muliggjøre og bidra ved revisjoner av Databehandlerens behandlingsaktiviteter som utføres av den Behandlingsansvarlige eller av annen inspektør på fullmakt fra den Behandlingsansvarlige. Databehandleren skal også muliggjøre og bidra ved revisjoner fra tilsynsmyndigheter.

10.3 Databehandleren skal, på egen hånd eller via annen inspektør på fullmakt fra Databehandleren, foreta jevnlige revisjoner av sine behandlingsaktiviteter. Databehandleren skal oversende kopi av revisjonsrapporter fra slike revisjoner til den Behandlingsansvarlige. Den Behandlingsansvarlige skal ha rett til å fremlegge slike revisjonsrapporter til sine eksterne revisorer og tilsynsmyndigheter.

10.4 Databehandleren skal umiddelbart varsle den Behandlingsansvarlige hvis den mottar forespørsel fra en myndighet om å utlevere personopplysninger som er behandlet under denne Databehandleravtalen. Med mindre loven krever det, skal Databehandleren ikke etterkomme en slik forespørsel uten skriftlig forhåndsgodkjenning fra den Behandlingsansvarlige.

10.5 Dersom en revisjon avdekker avvik fra forpliktelsene i denne Databehandleravtalen, skal Databehandleren så snart som mulig avhjelpe slike avvik (og, hvis relevant, påse at den relevante underdatabehandleren gjør det samme). Den Behandlingsansvarlige kan kreve at hele eller deler av behandlingsaktivitetene midlertidig opphører til vellykket utbedring er bekreftet.

10.6 Hver av partene dekker sine egne kostnader forbundet med en revisjon.

## **11. ANDRE BEHANDLINGSANSVARLIGE**

11.1 Databehandleren anerkjenner at personopplysningene også kan behandles på vegne av den Behandlingsansvarliges konsernselskaper/kunder/klienter. Slike andre behandlingsansvarlige har samme rettigheter som den Behandlingsansvarlige som er

compliance with this Data Processing Agreement and applicable privacy rules.

10.2 The Data Processor shall enable and contribute to audits of the Data Processor's processing activities carried out by the Data Controller or by another inspector on the authority of the Data Controller. The Data Processor shall also enable and contribute to audits by supervisory authorities.

10.3 The Data Processor shall, on its own or via another inspector authorized by the Data Processor, carry out regular audits of its processing activities. The Data Processor shall transmit copies of audit reports of such audits to the Data Controller. The Data Controller shall have the right to submit such audit reports to its external auditors and supervisory authorities.

10.4 The Data Processor shall immediately notify the Data Controller if it receives a request from an authority to disclose personal data processed under this Data Processing Agreement. Unless required by law, the Data Processor shall not comply with such a request without the prior written consent of the Data Controller.

10.5 If an audit reveals any deviations from the obligations of this Data Processing Agreement, the Data Processor shall remedy such deviations as soon as possible (and, if applicable, ensure that the relevant sub-processor does the same). The Data Controller may require all or part of the processing activities to be temporarily suspended until successful remediation is confirmed.

10.6 Each party will cover its own costs associated with an audit.

## **11. OTHER DATA CONTROLLERS**

11.1 The Data Processor acknowledges that the personal data may also be processed on behalf of the Data Controller's group companies/customers/clients. Such other data controllers have the same rights as the Data Controller who is a contracting party, and they



avtalepart, og de kan håndheve denne Databehandleravtalen som om de var avtaleparter. Slik håndheving skal imidlertid skje gjennom den Behandlingsansvarlige som er avtalepart.

11.2 Den Behandlingsansvarlige kan videresende enhver instruks fra slike andre behandlingsansvarlige, og Databehandleren skal handle i samsvar med slike instruksjoner som om de var den Behandlingsansvarliges egne.

11.3 Den Behandlingsansvarlige kan videresende enhver dokumentasjon og informasjon mottatt av Databehandleren til slike andre behandlingsansvarlige.

## **12. SPESIELT FOR SELSKAPER MED VERDIPAPIRER REGISTRERT I EURONEXT SECURITIES OSLO**

12.1 Det understrekes spesielt at Euronext Securities Oslo og Equuro Issuer Services AS som kontofører er sammen behandlingsansvarlige for personvernopplysninger i forbindelse med Registreringsvirksomheten. VPS regelverket 2.5.4. (Personopplysninger) har spesifikke bestemmelser i forbindelse med behandling av personvernopplysninger, som de registrerte selskaper må forholde seg til.

## **13. VARIGHET OG OPPSIGELSE**

13.1 Denne Databehandleravtalen gjelder så lenge Databehandleren behandler personopplysninger på vegne av den Behandlingsansvarlige i forbindelse med Hovedavtalen.

13.2 Ved opphør eller oppsigelse av Databehandleravtalen skal Databehandleren, dersom den Behandlingsansvarlige ønsker det, slette eller tilbakelevere alle personopplysninger til den Behandlingsansvarlige og slette eksisterende kopier, og bekrefte overfor den Behandlingsansvarlige at dette er gjort, med mindre gjeldende rett i EØS-området krever at Databehandleren lagrer personopplysningene (i så fall skal Databehandleren besørge sikker lagring, men ikke aktivt behandle, personopplysningene, og skal slette personopplysningene så snart loven tillater dette).

may enforce this Data Processing Agreement as if they were contracting parties. However, such enforcement shall take place through the Data Controller who is a contracting party.

11.2 The Data Controller may forward any instructions from such other data controllers, and the Data Processor shall act in accordance with such instructions as if they were the Data Controller's own.

11.3 The Data Controller may forward any documentation and information received by the Data Processor to such other data controllers.

## **12. ESPECIALLY FOR COMPANIES WITH SECURITIES REGISTERED WITH EURONEXT SECURITIES OSLO**

12.1 It is particularly emphasized that Euronext Securities Oslo and Equuro Issuer Services AS as the account operator, are joint controllers of personal data in connection with the Registration activities. The Euronext Securities Oslo Registration Rules 2.5.4. (Personal Data) contain specific provisions regarding the processing of personal data, which the registered companies must adhere to.

## **13. DURATION AND TERMINATION**

13.1 This Data Processing Agreement applies as long as the Data Processor processes personal data on behalf of the Data Controller in connection with the Main Agreement.

13.2 Upon termination or termination of the Data Processing Agreement, the Data Processor shall, if the Data Controller so wishes, delete or return all personal data to the Data Controller and delete existing copies, and confirm to the Data Controller that this has been done, unless applicable law in the EEA requires the Data Processor to store the personal data (in which case the Data Processor shall ensure secure storage, but not actively process, personal data, and shall delete the personal data as soon as permitted by law).

## **VEDLEGG 1: DATABEHANDLINGENS OMFANG**

### **Behandlingens formål**

Formålet med databehandlingen er at Databehandleren skal kunne utføre sine forpliktelser i henhold til Hovedavtalen.

### **Behandlingens art og hensikt**

Ivaretagelse av lovpålagt krav til aksjebok/eierregister og tilhørende skatterapportering, avhengig av hvilke tjeneste kunden har bestilt.

### **Kategorier av registrerte**

Personer som har eller har hatt eierforhold hos den den Behandlingsansvarlige eller Behandlingsansvarlige kunder.

### **Typen personopplysninger**

Navn, adresse, fødselsnummer/annen skatterelatert ID, beholdning av verdipapirer samt transaksjonshistorikk og utbetalingshistorikk.

For meglerløsningskunder vil Databehandleren i tillegg lagre data om kundenes finansielle situasjon, erfaring fra finansprodukter og relevant bakgrunn.

## **APPENDIX 1: SCOPE OF DATA PROCESSING**

### **Purpose of the processing**

The purpose of the data processing is for the Data Processor to be able to perform its obligations under the Main Agreement.

### **Nature and purpose of the processing**

Compliance with statutory requirements for share register/owner register and associated tax reporting, depending on which service the customer has ordered.

### **Categories of data subjects**

Persons who have or have had ownership of the Data Controller or Data Controller's customers.

### **The type of personal data**

Name, address, national identity number/other tax-related ID, holdings of securities, and transaction history and payment history.

For broker solution customers, the Data Processor will also store data about the customers' financial situation, experience with financial products and relevant background.

## **VEDLEGG 2: TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK**

Databehandleren skal som et minimum gjennomføre alle de tiltak som er angitt eller henvist til nedenfor. Databehandleren kan ikke uten skriftlig samtykke fra den Behandlingsansvarlige gjøre endringer i disse tiltakene som reduserer graden av datasikkerhet. Databehandleren skal kontinuerlig arbeide for å forbedre sikkerhetstiltakene og sørge for at de oppdateres i takt med den teknologiske utviklingen.

### **Pseudonymiseringstiltak**

Pseudonymisering vil si behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsinformasjon, forutsatt at slik tilleggsinformasjon oppbevares separat og er gjenstand for tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar person.

I databasestrukturen er data i den utstrekning det er teknisk mulig lagret mot en systemID fremfor direkte identifiserbare verdier.

### **Krypteringstiltak**

Kryptering er prosessen med koding av data på en slik måte at bare autoriserte personer har tilgang til opplysningene.

Alle dokumenter lastet opp i interne systemer lagres med asynkron kryptering for å hindre uautorisert tilgang.

### **Tiltak for å sikre personopplysningenes fortrolighet**

For å sikre personopplysningenes fortrolighet benyttes strenge autentiseringer ved innlogging for å kontrollere tilgang. Tilgangskontrollen vil i hovedsak være basert på BankID.

### **Tiltak for å sikre personopplysningenes integritet**

Alle endringer i opplysningene overvåkes og loggføres og det gjennomføres systematiske

## **APPENDIX 2: TECHNICAL AND ORGANISATIONAL SECURITY MEASURES**

The Data Processor shall, as a minimum, implement all the measures specified or referred to below. The Data Processor may not, without the written consent of the Data Controller, make changes to these measures that reduce the degree of data security. The Data Processor shall continuously work to improve the security measures and ensure that they are updated in line with technological developments.

### **Pseudonymization measures**

Pseudonymization means the processing of personal data in such a way that the personal data can no longer be linked to a specific data subject without the use of additional information, provided that such additional information is stored separately and is subject to technical and organizational measures that ensure that the personal data cannot be linked to an identified or identifiable person.

In the database structure, data is stored against a system ID rather than directly identifiable values to the extent technically possible.

### **Encryption measures**

Encryption is the process of encoding data in such a way that only authorized people have access to the information.

All documents uploaded to internal systems are stored with asynchronous encryption to prevent unauthorized access.

### **Measures to ensure the confidentiality of personal data**

To ensure the confidentiality of personal data, strict authentications are used when logging in to control access. Access control will mainly be based on BankID.

### **Measures to ensure the integrity of personal data**

All changes to the information are monitored and logged, and systematic checks are carried

kontroller mellom registrerte opplysninger mot sentrale registre (DSF og Foretaksregistret) for å sikre at eventuelle endringer oppdateres.

out between registered information against central registers (the DSF and the Register of Business Enterprises) to ensure that any changes are updated.

**Tiltak for å sikre tilgjengeligheten til personopplysningene**

For å sikre løpende tilgjengelighet til dataene har Databehandler backuprutiner som sikrer lagring av data.

**Measures to ensure the availability of personal data**

To ensure ongoing availability of the data, the Data Processor has backup routines that ensure the storage of data.

**Tiltak for å sikre robusthet i behandlingssystemene og -tjenestene**

Selskapets servere står i sikrede lokaler med redundant strøm og nettilgang. Det foreligger egne rutiner for katastrofegjenoppretting fra ekstern backup dersom ekstraordinære hendelser skulle inntreffe og slike tiltak må iverksettes.

**Measures to ensure the robustness of treatment systems and services**

The company's servers are located in secured premises with redundant power and internet access. There are separate routines for disaster recovery from external backup if extraordinary events should occur and such measures must be implemented.

**Andre datasikkerhetstiltak:**

For å sikre løpende sikkerhet i våre løsninger og tjenester anvender vi til enhver tid siste utprøvde teknologi. Videre er alle tekniske installasjoner sikret bak brannmurer og tiltakene vurderes årlig gjennom sikkerhetsrevisjon.

**Other data security measures:**

To ensure ongoing security in our solutions and services, we always use the latest tested technology. Furthermore, all technical installations are secured behind firewalls and the measures are assessed annually through security audits.