PERSONUPPGIFTSBITRÄDESAVTAL

1. BAKGRUND OCH SYFTE

Detta tillägg för behandling av personuppgifter (”**Personuppgiftsbiträdesavtalet**”) är en del av huvudavtalet (”**Huvudavtalet**”) mellan Kunden (den ”**Personuppgiftsansvarige**”) och Equro Group AS (”**Personuppgiftsbiträdet**”), där båda utgör ”**Part**”, gemensamt benämnda som ”**Parterna**”.

Den svenska texten i detta avtal är en direkt översättning av den engelska texten. Vid eventuella avvikelser eller konflikter mellan den svenska och engelska texten ska den engelska texten ha företräde.

1.1 Syftet med detta Personuppgiftsbiträdesavtal är att fastställa Parternas rättigheter och skyldigheter angående Personuppgiftsbiträdets behandling av personuppgifter för den Personuppgiftsansvariges räkning enligt Huvudavtalet.

1.2 Detta Personuppgiftsbiträdesavtal ersätter alla tidigare avtal och bestämmelser mellan Parterna avseende dataskydd.

1.3 Med undantag för vad som specificeras här, ska villkoren i Huvudavtalet gälla. Vid eventuella avvikelser mellan Huvudavtalet och detta Personuppgiftsbiträdesavtal avseende frågor som specifikt rör dataskydd, ska Personuppgiftsbiträdesavtalet ha företräde.

2. DEFINITIONER

2.1 I detta Personuppgiftsbiträdesavtal ska följande ord och uttryck ha den betydelse som anges nedan.

2.2 "**Tillämplig Integritetspolicy**": Aktuella dataskyddslagar och förordningar, inklusive lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och GDPR.

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 Equro Group AS (the "**Data Processor**"), both of which constitute a "**Party**", collectively referred to as the "**Parties**".

The Swedish text in this agreement is a direct translation of the English text. In the event of any discrepancies or conflicts between the Swedish and English text, the English 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 Act (2018:218) with supplementary provisions to the EU General Data Protection Regulation

2.3 "**GDPR**": EU:s allmänna dataskyddsförordning 2016/679.

2.4 "**Standardavtalsklausuler**": Standardavtalsklausuler för överföring av personuppgifter till personuppgiftsbiträden etablerade i tredjeland, fastställda av ett beslut från Europeiska kommissionen den 5 februari 2010 och/eller som fastställs av Europeiska kommissionen eller en relevant tillsynsmyndighet i enlighet med artikel 28(7) eller 28(8) i GDPR.

2.5 "**Underbiträde**": Ett annat personuppgiftsbiträde som anlitats av Personuppgiftsbiträdet.

2.6 "**Tredjeland**": Ett land utanför EES som inte har bedömts av Europeiska kommissionen att säkerställa en adekvat skyddsnivå.

2.7 I övrigt ska ord och uttryck ha samma betydelse som tilldelas dem i GDPR.

3. OMFATTNING

3.1 Detta Personuppgiftsbiträdesavtal gäller för alla personuppgifter som Personuppgiftsbiträdet har mottagit, fått tillgång till eller genererat i samband med Huvudavtalet.

3.2 Detta Personuppgiftsbiträdesavtal ska, i den mån det är tillämpligt, även omfatta behandling av data som inte är personuppgifter som Personuppgiftsbiträdet har mottagit, fått tillgång till eller genererat i samband med Huvudavtalet. Begreppet "personuppgifter" ska, i den mån det är tillämpligt, därför även omfatta data som inte är personuppgifter.

3.3 Syftet och arten av databehandlingen, typen av personuppgifter som behandlas, samt kategorier av registrerade framgår av Bilaga 1.

4. ALLMÄNNA SKYLDIGHETER

4.1 Personuppgiftsbiträdet garanterar att det har infört lämpliga tekniska och

and GDPR.

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

organisatoriska åtgärder för att säkerställa att behandlingen uppfyller kraven enligt gällande dataskyddsregler och skyddar de registrerades rättigheter, och att dessa åtgärder kommer att iakttas under hela avtalsperioden.

organizational measures to ensure that the processing meets the requirements in accordance with applicable data protection rules and safeguards the rights of the data subjects, and that these measures will be complied with throughout the contract period.

4.2 Personuppgiftsbiträdet ska endast behandla personuppgifterna för det syfte och inom den omfattning som anges i Bilaga 1 och i övrigt i enlighet med den Personuppgiftsansvariges dokumenterade instruktioner.

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 Personuppgiftsbiträdet ska omedelbart underrätta den Personuppgiftsansvarige skriftligen om det har rimlig grund att tro att (i) en instruktion från den Personuppgiftsansvarige kan leda till att Personuppgiftsbiträdet bryter mot gällande dataskyddslagstiftning, eller (ii) gällande lag inom EES kräver att Personuppgiftsbiträdet behandlar personuppgifter utöver den omfattning som fastställts av den Personuppgiftsansvariges dokumenterade instruktioner, om inte denna rätt förbjuder sådan underrättelse av skäl av stor allmänintresse (i vilket fall Personuppgiftsbiträdet ska underrätta den Personuppgiftsansvarige så snart domstolen tillåter det). Vid (i) eller (ii) ska Parterna diskutera i god tro hur frågan kan lösas utan att negativt påverka skyddet av de registrerades rättigheter.

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. ASSISTANS TILL PERSONUPPGIFTSANSVARIG

5.1 Personuppgiftsbiträdet ska, genom lämpliga tekniska och organisatoriska åtgärder, bistå den Personuppgiftsansvarige i den utsträckning det är möjligt för att uppfylla den Personuppgiftsansvariges skyldighet att svara på förfrågningar från de registrerade i syfte att utöva sina rättigheter enligt kapitel 3 i GDPR, inklusive rättigheter gällande information, tillgång, rättelse, radering, begränsning av behandling, dataportabilitet, invändningar och att inte bli föremål för automatiserade individuella beslut.

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 Med hänsyn till beskaffenheten av behandlingen och den information som finns tillgänglig för Personuppgiftsbiträdet, ska

5.2 With regard to the nature of the processing and the information available to the Data Processor, the Data Processor shall assist

Personuppgiftsbiträdet bistå den Personuppgiftsansvarige med skyldigheter enligt artiklarna 32 till 36 i GDPR, inklusive skyldigheter för datasäkerhet (som beskrivs närmare i avsnitt 6), anmälan av personuppgiftsincidenter (som beskrivs närmare i avsnitt 9), dataskyddsbedömning samt förhandsdiskussioner.

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

5.3 Personuppgiftsbiträdet ska inte kommunicera direkt med de registrerade eller med tillsynsmyndigheter, om inte detta har förhandsgodkänts av den Personuppgiftsansvarige. Personuppgiftsbiträdet ska omedelbart vidarebefordra alla förfrågningar eller klagomål som det kan få från de registrerade till den Personuppgiftsansvarige. Personuppgiftsbiträdet ska även omedelbart vidarebefordra alla förfrågningar från en tillsynsmyndighet som rör inspektioner, utredningar, eller tillgång till eller information om personuppgifter, om inte förbjudet enligt lag (i vilket fall Personuppgiftsbiträdet ska underrätta den Personuppgiftsansvarige så snart lagstiftningen tillåter).

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 Hjälp enligt avsnitt 5 ska tillhandahållas mot betalning enligt Personuppgiftsbiträdets ordinarie timtaxor.

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

6. TEKNISKA OCH ORGANISATORISKA SÄKERHETSÅTGÄRDER

6.1 Personuppgiftsbiträdet ska införa lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna mot oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt avslöjande eller åtkomst. Personuppgiftsbiträdet ska, som ett minimum, införa de åtgärder som krävs enligt artikel 32 i GDPR, samt de åtgärder som specificeras eller hänvisas till i Bilaga 2.

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 Personuppgiftsbiträdet ska inte avslöja eller göra personuppgifter tillgängliga för tredje parter utan den Personuppgiftsansvariges föregående skriftliga samtycke, med undantag för eventuella godkända underbiträden i den utsträckning de behöver uppgifterna för att kunna utföra sina uppgifter.

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 Personuppgiftsbiträdet ska säkerställa att alla personer som är auktoriserade att behandla personuppgifterna har åtagit sig att behandla uppgifterna konfidentiellt eller omfattas av en lämplig lagstadgad sekretessplikt. På begäran av den Personuppgiftsansvarige ska Personuppgiftsbiträdet tillhandahålla en kopia av sådana individers undertecknade sekretessavtal.

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

7. ANVÄNDNING AV UNDERBITRÄDEN

7.1 Den Personuppgiftsansvarige tillåter att Personuppgiftsbiträdet anlitar underbiträden. På begäran ska den Personuppgiftsansvarige få information om vilka underbiträden som anlitas samt var de behandlar personuppgifterna. Personuppgiftsbiträdet ska underrätta den Personuppgiftsansvarige om eventuella planer på att använda andra underbiträden eller byta underbiträden och ge den Personuppgiftsansvarige rätt att invända mot sådana ändringar eller kräva att detta Personuppgiftsbiträdesavtal avslutas.

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 Enligt avsnitt 7.1 får Personuppgiftsbiträdet endast anlita underbiträden som infört lämpliga tekniska och organisatoriska åtgärder för att säkerställa att databehandlingen uppfyller kraven i gällande dataskyddsregler och för att skydda de registrerades integritet. Personuppgiftsbiträdet ska genomföra lämpliga kontroller av underbiträdena för att verifiera deras nivå av dataskydd. Personuppgiftsbiträdet ska förse den Personuppgiftsansvarige med rapporter från sådana kontroller.

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 Personuppgiftsbiträdet ska ingå ett skriftligt avtal med varje underbiträde som ålägger denne egna skyldigheter gällande skydd av personuppgifter. Om underbiträdet anlitas för att utföra specifika databehandlingsaktiviteter för den Personuppgiftsansvariges räkning, ska Personuppgiftsbiträdet genom skriftligt avtal ålägga underbiträdet samma skyldigheter gällande skydd av personuppgifter som anges i detta Personuppgiftsbiträdesavtal. På begäran av den Personuppgiftsansvarige ska Personuppgiftsbiträdet tillhandahålla kopior av

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-

avtal med underbiträden. Dock kan affärs- och annan affärskänslig information maskeras.

7.4 Personuppgiftsbiträdet är fullt ansvarigt för underbiträdets utför av sina skyldigheter.

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. INTERNATIONELL DATAÖVERFÖRING

8.1 Personuppgiftsbiträdet får endast överföra personuppgifter till ett tredjeland eller en internationell organisation enligt dokumenterade instruktioner från den Personuppgiftsansvarige. Personuppgiftsbiträdet kan dock göra detta om det krävs enligt gällande lag inom Europeiska ekonomiska samarbetsområdet. I sådana fall ska Personuppgiftsbiträdet underrätta den Personuppgiftsansvarige om de rättsliga kraven före överföringen, om inte sådan rätt förbjuder sådan underrättelse av skäl av stort allmänintresse (i vilket fall Personuppgiftsbiträdet ska underrätta den Personuppgiftsansvarige så snart domstolen tillåter det).

8.2 Om användningen av ett godkänt underbiträde kräver överföring av personuppgifter till ett tredjeland, och sådana överföringar har godkänts av den Personuppgiftsansvarige, godkänner den Personuppgiftsansvarige att Personuppgiftsbiträdet ingår standardavtalsklausuler i oförändrad form med underbiträdet på den Personuppgiftsansvariges vägnar, om detta är nödvändigt för att uppfylla kraven enligt gällande dataskyddsförordningar. Så snart ett sådant avtal har ingåtts ska underbiträdet tillhandahålla en kopia därav till den Personuppgiftsansvarige. Alla sådana standardklausuler ska automatiskt upphöra att gälla vid uppsägning av detta Personuppgiftsbiträdesavtal.

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. PERSONUPPGIFTSINCIDENTER

9.1 Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om varje överträdelse av detta Personuppgiftsbiträdesavtal eller säkerheten för personuppgifter. Meddelandet ska lämnas senast 36 timmar efter att Personuppgiftsbiträdet blev medvetet om

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.

överträdelsen.

9.2 Meddelande om en personuppgiftsincident måste åtminstone, i den mån det är relevant:

a. beskriva överträdelsens art, inklusive, om möjligt, kategorierna och det ungefärliga antalet berörda registrerade, samt kategorierna och det ungefärliga antalet berörda personuppgiftsposter;

b. innehålla, om möjligt, identiteten på de berörda registrerade;

c. vidarebefordra namn och kontaktuppgifter till den relevanta kontaktpunkten hos Personuppgiftsbiträdet för vidare informationsinsamling;

d. beskriva de sannolika konsekvenserna av personuppgiftsincidenten;

e. beskriva de åtgärder som vidtagits eller föreslagits för att hantera överträdelsen, inklusive, om relevant, åtgärder för att minska eventuella skadliga effekter;

f. inkludera annan information som krävs för att den Personuppgiftsansvarige ska kunna följa den tillämpliga integritetspolicyn.

9.3 Personuppgiftsbiträdet ska, så snart som möjligt, genomföra alla åtgärder som beskrivs i punkt e. ovan, samt genomföra alla åtgärder som rimligen krävs för att undvika liknande personuppgiftsincidenter i framtiden. Personuppgiftsbiträdet ska tillåta den Personuppgiftsansvarige att undersöka, fastställa orsaken till och verifiera de åtgärder som genomförts eller föreslagits av den Personuppgiftsansvarige för att hantera personuppgiftsincidenten. Personuppgiftsbiträdet ska, i möjligaste mån, samråda med den Personuppgiftsansvarige om de åtgärder som ska genomföras och överväga synpunkter från den Personuppgiftsansvarige i detta avseende.

9.4 Endast den Personuppgiftsansvarige har rätt att informera den relevanta tillsynsmyndigheten och de berörda

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 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

registrerade om en personuppgiftsincident. Personuppgiftsbiträdet ska avstå från att informera allmänheten eller tredje parter om någon överträdelse av säkerheten för personuppgifter.

breach. The Data Processor shall refrain from informing the public or third parties of any breach of personal data security.

10. REVISION

10.1 Personuppgiftsbiträdet ska dokumentera och göra tillgänglig för den Personuppgiftsansvarige den information som är nödvändig för att visa att detta Personuppgiftsbiträdesavtal och tillämpliga integritetsregler efterlevs.

10. AUDIT

10.1 The Data Processor shall document, as well as make available to the Data Controller, information that is necessary to demonstrate compliance with this Data Processing Agreement and applicable privacy rules.

10.2 Personuppgiftsbiträdet ska möjliggöra och bidra till revisioner av Personuppgiftsbiträdets behandlingsaktiviteter som utförs av den Personuppgiftsansvarige eller av en annan inspektör på den Personuppgiftsansvariges begäran. Personuppgiftsbiträdet ska också möjliggöra och bidra till revisioner av tillsynsmyndigheter.

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 Personuppgiftsbiträdet ska själv eller via en annan inspektör som är auktoriserad av Personuppgiftsbiträdet regelbundet genomföra revisioner av sina behandlingsaktiviteter. Personuppgiftsbiträdet ska överlämna kopior av revisionsrapporter från sådana revisioner till den Personuppgiftsansvarige. Den Personuppgiftsansvarige ska ha rätten att överlämna sådana revisionsrapporter till sina externa revisorer och tillsynsmyndigheter.

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 Personuppgiftsbiträdet ska omedelbart underrätta den Personuppgiftsansvarige om det mottar en begäran från en myndighet om att lämna ut personuppgifter som behandlas enligt detta Personuppgiftsbiträdesavtal. Om det inte krävs enligt lag, får Personuppgiftsbiträdet inte följa en sådan begäran utan den Personuppgiftsansvariges föregående skriftliga medgivande.

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 Om en revision avslöjar någon avvikelse från skyldigheterna i detta Personuppgiftsbiträdesavtal, ska Personuppgiftsbiträdet åtgärda sådana avvikelser så snart som möjligt (och, om tillämpligt, säkerställa att relevant underbiträde gör detsamma). Den Personuppgiftsansvarige kan kräva att hela eller delar av

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

behandlingsaktiviteterna tillfälligt stoppas tills framgångsrik återställning bekräftas.

10.6 Varje part täcker sina egna kostnader i samband med en revision.

11. ANDRA PERSONUPPGIFTSANSVARIGA

11.1 Personuppgiftsbiträdet erkänner att personuppgifterna även kan behandlas för den Personuppgiftsansvariges koncernbolag/kunder/klienters räkning. Sådana andra personuppgiftsansvariga har samma rättigheter som den Personuppgiftsansvarige som är avtalspart, och de kan genomdriva detta Personuppgiftsbiträdesavtal som om de vore avtalspartner. Denna genomdrivning ska dock ske genom den Personuppgiftsansvarige som är avtalspart.

11.2 Den Personuppgiftsansvarige kan vidarebefordra instruktioner från sådana andra personuppgiftsansvariga, och Personuppgiftsbiträdet ska agera i enlighet med sådana instruktioner som om de vore den Personuppgiftsansvariges egna.

11.3 Den Personuppgiftsansvarige kan vidarebefordra all dokumentation och information som mottagits från Personuppgiftsbiträdet till sådana andra personuppgiftsansvariga.

12. SÄRSKILT FÖR FÖRETAG MED VÄRDEPAPPER REGISTRERADE HOS EURONEXT SECURITIES OSLO

12.1 Det betonas särskilt att Euronext Securities Oslo och Equro Issuer Services AS som kontoförande institut är gemensamt personuppgiftsansvariga för personuppgifter i samband med registreringsaktiviteterna. Euronext Securities Oslo Registreringsregler 2.5.4 (Personopplysninger) innehåller specifika bestämmelser om behandling av personuppgifter, vilka de registrerade företagen måste följa.

13. VARAKTIGHET OCH UPPSÄGNING

13.1 Detta Personuppgiftsbiträdesavtal gäller så länge Personuppgiftsbiträdet behandlar personuppgifter på den Personuppgiftsansvariges vägnar i samband

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 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 Equro 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.

med Huvudavtalet.

13.2 Vid upphörande eller avslutande av Personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet, om den Personuppgiftsansvarige så önskar, radera eller återlämna alla personuppgifter till den Personuppgiftsansvarige och radera befintliga kopior, och bekräfta för den Personuppgiftsansvarige att detta har utförts, såvida inte gällande lagstiftning inom EES kräver att Personuppgiftsbiträdet lagrar personuppgifterna (i vilket fall Personuppgiftsbiträdet ska säkerställa säker lagring, men inte aktivt behandla personuppgifterna, och ska radera personuppgifterna så snart det tillåts enligt lag).

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).

BILAGA 1: OMFATTNING AV DATAPROCESSEN

Syftet med behandlingen
Syftet med databehandlingen är att möjliggöra för Personuppgiftsbiträdet att fullgöra sina skyldigheter enligt Huvudavtalet.

Behandlingens art och syfte
Efterlevnad av lagstadgade krav för aktiebok/ägarregister och tillhörande skatterapportering, beroende på vilken tjänst kunden har beställt.

Kategorier av registrerade
Personer som har eller har haft ägande i den Personuppgiftsansvarige eller den Personuppgiftsansvariges kunder.

Typ av personuppgifter
Namn, adress, personnummer/annat skatterelaterat ID, innehav av värdepapper samt transaktionshistorik och betalningshistorik.

För kunden med mäklartjänster kommer Personuppgiftsbiträdet även att lagra data om kundens ekonomiska situation, erfarenhet av finansiella produkter och relevant bakgrund.

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.

BILAGA 2: TEKNISKA OCH ORGANISATORISKA SÄKERHETSÅTGÄRDER

Personuppgiftsbiträdet ska, som ett minimum, införa alla de åtgärder som specificeras eller hänvisas till nedan. Personuppgiftsbiträdet får inte, utan den Personuppgiftsansvariges skriftliga godkännande, ändra dessa åtgärder på ett sätt som minskar graden av datasäkerhet. Personuppgiftsbiträdet ska kontinuerligt arbeta för att förbättra säkerhetsåtgärderna och säkerställa att de uppdateras i takt med teknologiska framsteg.

Åtgärder för pseudonymisering

Pseudonymisering innebär behandlingen av personuppgifter på ett sådant sätt att de inte längre kan kopplas till en specifik registrerad utan användning av ytterligare information, förutsatt att sådan ytterligare information lagras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte kan kopplas till en identifierad eller identifierbar person.

I databasstrukturen lagras data mot ett system-ID snarare än direkt identifierbara värden i den utsträckning det är tekniskt möjligt.

Åtgärder för kryptering

Kryptering är processen att koda data på ett sådant sätt att endast behöriga personer har tillgång till informationen.

Alla dokument som laddas upp till interna system lagras med asynkron kryptering för att förhindra obehörig åtkomst.

Åtgärder för att säkerställa konfidentialitet av personuppgifter

För att säkerställa konfidentialiteten av personuppgifter används strikt autentisering vid inloggning för att kontrollera åtkomst. Åtkomstkontroll kommer huvudsakligen att baseras på BankID.

Åtgärder för att säkerställa integritet av personuppgifter

Alla ändringar i uppgifterna övervakas och loggas, och systematiska kontroller genomförs mellan registrerade uppgifter och centrala

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 out between registered information against

register (befolkningsregistret och företagsregistret) för att säkerställa att eventuella ändringar uppdateras.

Åtgärder för att säkerställa tillgänglighet av personuppgifter
För att säkerställa kontinuerlig tillgänglighet av uppgifterna har Personuppgiftsbiträdet backup-rutiner som garanterar lagringen av data.

Åtgärder för att säkerställa robusthet i behandlingssystem och tjänster
Företagets servrar är placerade i säkra lokaler med redundant strömförsörjning och internetåtkomst. Det finns separata rutiner för katastrofåterställning från extern backup om extraordinära händelser inträffar och sådana åtgärder måste genomföras.

Andra säkerhetsåtgärder för data
För att säkerställa fortsatt säkerhet i våra lösningar och tjänster använder vi alltid den senaste testade teknologin. Dessutom är alla tekniska installationer skyddade bakom brandväggar och åtgärderna bedöms årligen genom säkerhetsrevisioner.

central registers (the DSF and the Register of Business Enterprises) to ensure that any changes are updated.

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.

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.

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.