Standard kontraktsbestemmelser

Databehandleravtale

I henhold til artikkel 28 nr. 3 i forordning 2016/679 (GDPR)

mellom

Brukerstedet

heretter; den behandlingsansvarlige

og

Qrona.no AS (org. nr. 925614475)
Raveien 205

3184 BORRE

heretter; databehandler

hver omtalt som en «part» eller sammen som «partene»

1 Innhold

2 Innledning

1. Disse standard kontraktsbestemmelsene (Kontraktsbestemmelsene) fastsetter de rettigheter og plikter som gjelder når databehandleren behandler personopplysninger på vegne av den behandlingsansvarlige.
2. Kontraktsbestemmelsene er utformet med henblikk på partenes overholdelse av artikkel 28(3) i Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning - GDPR).
3. I forbindelse med leveranse av tjenesten Qrona.no vil databehandleren behandle personopplysninger på vegne av den behandlingsansvarlige i henhold til Kontraktsbestemmelsene.
4. Kontraktsbestemmelsene skal ha forrang over andre tilsvarende bestemmelser i andre avtaler mellom partene.
5. Fire vedlegg er inntatt i Kontraktsbestemmelsene, og vedleggene utgjør en integrert del av Kontraktsbestemmelsene.
6. Vedlegg A inneholder detaljer om behandlingen av personopplysninger, herunder behandlingens formål og art, typen personopplysninger, kategorier av registrerte og varigheten av behandlingen.
7. Vedlegg B inneholder den behandlingsansvarliges vilkår for databehandlerens bruk av underdatabehandlere og en liste over underdatabehandlere, som er godkjent av den behandlingsansvarlige.
8. Vedlegg C inneholder den behandlingsansvarliges instrukser for behandlingen av personopplysninger, minimum sikkerhetstiltak som skal implementeres av databehandleren og hvordan revisjoner av databehandleren og eventuelle underdatabehandlere skal gjennomføres.
9. Vedlegg D inneholder regulering av andre forhold som ikke er dekket av Kontraktsbestemmelsene.
10. Kontraktsbestemmelsene sammen med vedleggene skal oppbevares skriftlig, herunder elektronisk, av begge parter.
11. Kontraktsbestemmelsene fritar ikke databehandleren fra plikter som databehandleren skal følge etter personvernforordningen (GDPR) eller annen lovgivning.

3 Den behandlingsansvarliges rettigheter og plikter

1. Den behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger utføres i samsvar med GDPR (se artikkel 24 i

personopplysningsloven), personvernreglene i gjeldende EU eller Medlemsstats[1] personvernregler og Kontraktsbestemmelsene.

2. Den behandlingsansvarlige har rett og plikt til å fatte beslutninger om til hvilke(t) formål og med hvilke hjelpemidler behandlingen av personopplysninger skal skje.
3. Den behandlingsansvarlige skal være ansvarlig, for blant annet, å sikre at behandlingen av personopplysninger, som databehandleren er instruert i å utføre, har et rettslig grunnlag.

4 Databehandleren handler på instruks

1. Databehandleren skal kun behandle personopplysninger på dokumenterte instrukser fra den behandlingsansvarlige, med mindre det kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som databehandleren er underlagt. Slike instrukser skal være spesifisert vedlegg A og C. Senere instrukser kan også gis av den behandlingsansvarlige i løpet av behandlingen av personopplysninger, men slike instrukser skal alltid være dokumenterte og oppbevares i skriftlig form, herunder elektronisk, i overensstemmelse med Kontraktsbestemmelsene.
2. Databehandleren skal omgående underrette den behandlingsansvarlige dersom vedkommende mener at en instruks gitt av den behandlingsansvarlige er i strid med GDPR eller andre bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett.

   Insisterer den behandlingsansvarlige på at en instruks skal gjennomføres og denne er i strid med GDPR eller andre bestemmelser om vern av personopplysninger i unionsretten eller medlemsstatenes nasjonale rett og databehandler har gjort behandlingsansvarlig oppmerksom på dette, så har databehandler rett til å si opp avtalen med den behandlingsansvarlige.

5 Konfidensialitet

1. Databehandleren skal kun gi tilgang til personopplysninger, som behandles på vegne av den behandlingsansvarlige, til personer som er under databehandlerens myndighet og som er forpliktet til konfidensialitet eller er underlagt egnet lovfestet taushetsplikt, og kun i det nødvendige omfang. Listen over personer som har tilgang til personopplysningene skal regelmessig gjennomgås. Som følge av en slik gjennomgang skal tilgang til personopplysningene stenges dersom en slik tilgang ikke lenger er nødvendig for disse personene.
2. Databehandleren skal på anmodning fra den behandlingsansvarlige påvise at de involverte personene under databehandlerens myndighet er omfattet av ovennevnte konfidensialitetsplikt.

[1] Henvisning til “Medlemsstat” i Kontraktsbestemmelsene skal forstås som henvisning til EØS-land.

6 Sikkerhet ved behandlingen

1. Artikkel 32 i GDPR slår fast at, idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers friheter og rettigheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

   Den behandlingsansvarlige skal vurdere risikoen for fysiske personers rettigheter og friheter som omfattes av behandling og gjennomføre tiltak for å redusere risikoen. Avhengig av relevans, kan slike tiltak omfatte følgende:

   a. Pseudonymisering og kryptering av personopplysninger

   b. evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene

   c. evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse

   d. en prosedyre for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

2. I henhold til artikkel 32 i GDPR, skal databehandleren – uavhengig fra den behandlingsansvarlige – også vurdere risikoen for fysiske personer rettigheter og friheter som omfattes av behandlingen og gjennomføre tiltak for å redusere risikoen. I forbindelse med denne vurderingen må behandlingsansvarlig gi nødvendig informasjon til databehandleren som gjør det mulig for vedkommende å identifisere og vurdere slike risikoer.

3. Videre skal databehandleren bistå den behandlingsansvarlige i å sikre overholdelse av den behandlingsansvarliges plikter etter artikkel 32 i GDPR, ved å bl.a. å sørge for at den behandlingsansvarlige får informasjon om tekniske og organisatoriske tiltak som er gjennomført av databehandleren i henhold til artikkel 32 i GDPR, sammen med all annen informasjon, som er nødvendig for den behandlingsansvarlige til å overholde sine plikter etter artikkel 32 i GDPR.

   Hvis de identifiserte risikoene – etter den behandlingsansvarliges mening - krever implementering av ytterligere tiltak enn de som allerede er implementert av databehandleren, skal den behandlingsansvarlige, i vedlegg C, angi hvilke tilleggstiltak som skal iverksettes.

7 Bruk av underdatabehandlere

1. Databehandleren skal oppfylle betingelsene som er omtalt i artikkel 28(2) og (4) i GDPR, for å engasjere en annen databehandler (en underdatabehandler).

2. Databehandleren må derfor ikke engasjere en annen databehandler (underdatabehandler) for oppfyllelse av Kontraktsbestemmelsene uten at det på forhånd er innhentet en generell skriftlig tillatelse fra den behandlingsansvarlige.

3. Databehandleren har den behandlingsansvarliges generelle godkjenning til å engasjere underdatabehandlere. Databehandleren må varsle den behandlingsansvarlige skriftlig om eventuelle planer om å benytte underdatabehandlere eller utskifting av underdatabehandlere, minst 5 (fem) dager på forhånd, og dermed gi den behandlingsansvarlige muligheten til å motsette seg slike endringer før underdatabehandler(e) engasjeres. Lengere tid for å gi beskjed i forbindelse med spesifikke behandlingsaktiviteter kan inntas i vedlegg B. Listen over under-databehandlere som allerede er godkjent av den behandlingsansvarlige kommer frem i vedlegg B.

4. Dersom databehandleren engasjerer en underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige, skal de samme forpliktelsene som er fastsatt i Kontraktsbestemmelsene bli pålagt underdatabehandleren ved avtale eller et annet rettslig dokument i henhold til unionsretten eller medlemsstatenes nasjonale rett, der det særlig gis tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i Kontraktsbestemmelsene og GDPR.

   Databehandleren skal derfor være ansvarlig for at underdatabehandleren minimum overholder de forpliktelser som databehandleren er pålagt etter Kontraktsbestemmelsene og GDPR.

5. En kopi av underdatabehandleravtalen og eventuell etterfølgende endringer skal – på den behandlingsansvarliges forespørsel – oversendes den behandlingsansvarlige. Den behandlingsansvarlige har dermed mulighet til å sikre at de samme plikter for behandling av person-opplysninger pålegges underdatabehandleren. Bestemmelser om kommersielle forhold som ikke har betydning for behandling av personopplysninger under underdatabehandleravtalen, skal ikke sendes til den behandlingsansvarlige.

6. Databehandleren skal i sin avtale med underdatabehandleren sette inn den behandlingsansvarlige som begunstiget tredjepart i det tilfellet at databehandleren går konkurs, slik at den behandlingsansvarlige kan tre inn i databehandlerens rettigheter og gjøre dem gjeldende overfor underdatabehandleren, slik at den behandlingsansvarlige kan instruere underdatabehandleren om sletting eller tilbakelevering av personopplysningene.

7. Hvis underdatabehandleren ikke oppfyller sine databehandlingsforpliktelser, forblir databehandleren fullt ut ansvarlig overfor den behandlingsansvarlige for underdatabehandlerens

forpliktelser. Dette har ikke betydning for de registrertes rettigheter under GDPR, spesielt de rettigheter som er forutsatt i artikkel 79 og 82 – overfor den behandlingsansvarlige og databehandleren, inkludert underdatabehandleren.

8 Overføring av personopplysninger til tredjestater eller internasjonale organisasjoner

1. Enhver overføring av personopplysninger til tredjestat eller internasjonale organisasjoner av databehandleren skal kun finne sted på grunnlag av dokumenterte instrukser fra den behandlingsansvarlige og må alltid utføres i overensstemmelse med kapittel V i GDPR.
2. Dersom overføring til tredjestat eller internasjonale organisasjoner, som databehandleren ikke er blitt instruert til å foreta av den behandlingsansvarlige, som er påkrevet etter unionsretten eller medlemsstatenes nasjonale rett, som databehandleren er underlagt, skal databehandleren varsle den behandlingsansvarlige om nevnte rettslige krav før behandlingen, med mindre de rettslige kravene av hensyn til viktige allmenne interesser forbyr en slik underretning.
3. Uten dokumenterte instrukser fra den behandlingsansvarlige, kan databehandleren derfor ikke innenfor disse Kontraktsbestemmelser:
    a. Overføre personopplysninger til en behandlingsansvarlig eller databehandler i en tredjestat eller en internasjonal organisasjon
    b. overføre behandlingen av personopplysninger til en underdatabehandler i en tredjestat
    c. behandle personopplysningene i en tredjestat
4. Den behandlingsansvarliges instrukser vedrørende overføring av personopplysninger til en tredjestat inkludert, hvis relevant, overføringsgrunnlagene etter kapittel V i GDPR som de er basert på, skal inntas i vedlegg C.6.
5. Kontraktsbestemmelsene skal ikke forstås som standard personvernbestemmelser etter artikkel 46(2)(c) og (d) i GDPR, og Kontraktsbestemmelsene kan ikke benyttes som overføringsgrunnlag etter kapittel V i GDPR.

9 Bistand til den behandlingsansvarlige

1. Databehandleren bistår, så langt det er mulig, den behandlingsansvarlige ved hjelp av passende tekniske og organisatoriske tiltak med oppfyllelsen av den behandlingsansvarliges plikt til å svare på anmodninger om utøvelsen av den registrertes rettigheter fastsatt i kapittel III i GDPR.

   Dette innebærer, at databehandleren så langt som mulig skal bistå den behandlingsansvarlige i forbindelse med, at den behandlingsansvarlige skal sikre overholdelsen av:

a. opplysningsplikten ved innsamling av personopplysninger fra den registrerte
b. opplysningsplikten, hvis personopplysninger ikke er innsamlet fra den registrerte
c. den registrertes innsynsrett
d. retten til retting
e. retten til sletting («retten til å bli glemt»)
f. retten til begrensning av behandling
g. informasjonsplikt i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling
h. retten til dataportabilitet
i. retten til å protestere
j. retten til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisert behandling, herunder profilering

2. I tillegg til databehandlerens plikt til å bistå den behandlingsansvarlige i henhold til punkt skal 6.3., databehandleren videre, hensyntatt arten av behandlingen og informasjon som er tilgjengelig for databehandleren, bistå den behandlingsansvarlige med overholdelse av:

    a. den behandlingsansvarliges plikt til, uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde ifra om brudd på personopplysningssikkerheten til vedkommende tilsynsmyndighet, Datatilsynet, med mindre det er usannsynlig, at bruddet på personvernet vil medføre en risiko for fysiske personers rettigheter og friheter

    b. den behandlingsansvarliges plikt til uten ugrunnet opphold – å underrette den/de registrerte om brudd på personvernet, når et slikt brudd sannsynligvis vil innebære en høy risiko for fysiske personers rettigheter og friheter

    c. den behandlingsansvarliges plikt til forut for behandlingen å foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personvernet (en vurdering av personvernkonsekvenser)

    d. den behandlingsansvarliges plikt til å gjennomføre forhåndsdrøftelser med tilsynsmyndigheten, Datatilsynet, før behandling, såfremt en vurdering av personvernkonsekvenser viser, at behandlingen vil føre til høy risiko dersom den behandlingsansvarlige ikke treffer tiltak for å redusere risikoen

3. Partene skal i vedlegg C spesifisere de nødvendige tekniske og organisatoriske tiltak som databehandleren skal bistå den behandlingsansvarlige med i tillegg til omfang og om bistand er påkrevd. Dette gjelder de forpliktelser som er forutsatt i punkt 9.1. og 9.2.

10 Melding om brudd på personopplysningssikkerheten

1. I tilfelle brudd på personopplysningssikkerheten, skal databehandleren uten ugrunnet opphold etter å ha fått kjennskap til det, underrette den behandlingsansvarlige om at det er skjedd et brudd på personopplysningssikkerheten.
2. Databehandlerens underretning til den behandlingsansvarlige skal, om mulig, skje innen 24 timer etter databehandleren har fått kjennskap til bruddet på personopplysningssikkerheten for å overholde den behandlingsansvarliges plikt til å melde bruddet på personopplysningssikkerheten til relevant tilsynsmyndighet, Datatilsynet, jf. artikkel 33 i GDPR.
3. I henhold til punkt 9.2.a, skal databehandleren bistå den behandlingsansvarlige med å melde bruddet på personopplysningssikkerheten til vedkommende tilsynsmyndighet, Datatilsynet. Dette betyr at databehandleren skal bistå med å innhente informasjonen nedenfor som, i henhold til artikkel 33(3) i GDPR, skal tas med i den behandlingsansvarliges melding til vedkommende tilsynsmyndighet:
    a. Arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall berørte registreringer av personopplysninger
    b. de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten
    c. de tiltak som er truffet eller foreslått å bli tatt av den behandlingsansvarlige for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger.
4. Partene skal i vedlegg C angi hvilken informasjon databehandleren skal gi til den behandlingsansvarlige når denne bistår den behandlingsansvarlige i meldingen av bruddet på personopplysningssikkerheten til tilsynsmyndigheten, Datatilsynet.

11 Sletting/retur av opplysninger

1. Ved opphør av tjenestene knyttet til behandling av personopplysninger, er databehandleren forpliktet til å slette alle personopplysninger som er behandlet på vegne av den behandlingsansvarlige og bekrefte overfor den behandlingsansvarlige at dette er gjort, med mindre EU-retten eller Medlemstatenes nasjonale rett foreskriver oppbevaring av personopplysningene.

12 Revisjon og inspeksjoner

1. Databehandleren skal gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise samsvar med artikkel 28 i

GDPR og sørge for å bidra til revisjoner, inkludert inspeksjoner utført av behandlingsansvarlige eller en annen revisor, som er autorisert av databehandleren.

2. Prosedyrene for den behandlingsansvarliges revisjoner av databehandleren og underdatabehandlere er regulert nærmere i vedlegg C.7 and C.8.
3. Databehandleren skal være pålagt å gi tilsynsmyndigheter, som etter relevant lovgivning skal ha tilgang til den behandlingsansvarliges og databehandlers lokaler, eller representanter som handler på vegne av slike tilsynsmyndigheter, tilgang til databehandlerens fysiske lokaler ved fremleggelse av egnet identifikasjon.

13 Partenes avtale om andre forhold

1. Partene kan avtale ytterligere bestemmelser vedrørende behandling av personopplysninger som spesifiserer f.eks. ansvar, så lenge disse bestemmelsene ikke er i direkte eller indirekte motstrid med Kontraktsbestemmelsene eller svekker de grunnleggende rettigheter og friheter for den registrerte og den beskyttelse som GDPR gir.

14 Ikrafttredelse og opphør

1. Kontraktsbestemmelsene trer i kraft fra den datoen begge parter har underskrevet.
2. Begge parter kan kreve Kontraktsbestemmelsene reforhandlet, ved lovendringer eller ved uhensiktsmessigheter i Kontraktsbestemmelsene.
3. Kontraktsbestemmelsene skal gjelde for så lenge det leveres tjenester knyttet til behandling av personopplysninger fra databehandleren. Så lenge det leveres tjenester for behandling av personopplysninger kan ikke Kontraktsbestemmelsene sies opp dersom ikke andre bestemmelser om behandling av personopplysninger er avtalt mellom partene.
4. Hvis leveranse av tjenestene for behandling av personopplysninger opphører, og personopplysningene slettes eller tilbakeleveres til den behandlingsansvarlige etter punkt 11.1. og vedlegg C.4, kan Kontraktsbestemmelsene sies opp med skriftlig varsel fra begge parter.

5. Underskrift

   For behandlingsansvarlig:

   Dette aksepteres ved å ta i bruk avtalen.

   For databehandleren

   Navn [NAVN]

Stilling [STILLING]

Dato [DATO]

Signatur [SIGNATUR]

15 Den behandlingsansvarliges og databehandlers kontaktpunkter

1. Partene kan kontakte hverandre ved følgende kontakter/kontaktpunkter:
2. Partene skal være forpliktet til å fortløpende informere hverandre om endringer i kontakter/kontaktpunkter. For databehandlers del ligger denne informasjonen i regnskapssystemet.

For den behandlingsansvarlige

Se faktura i Fiken

For databehandleren

Rolle: Daglig leder

Telefon: xx xx xx xx

E-post: nn@qrona.no

Vedlegg A Informasjon om behandlingen

A.1. Formålet med databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige:

Databehandler stiller sin tjeneste Qrona.no til disposisjon for sine kunder og den behandlingsansvarlige (kunden) behandler personopplysninger kun til smittesporing.

Databehandleren kan kun behandle personopplysninger gjort tilgjengelig av behandlingsansvarlig til de formål som er bestemt av behandlingsansvarlig og i samsvar med de vilkår som fremgår av denne avtalen.

A.2. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skal relatere seg til (behandlingens gjenstand):

Drift, backup og support.

A.3. Behandlingen omfatter de følgende typer personopplysninger om de registrerte:

Navn, telefon, Bedrift/arrangement/forening besøkt på gitt tidspunkt.

A.4. Behandlingen omfatter følgende kategorier registrerte:

Gjester/kunder/besøkende

A.5. Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig kan utføres når Kontraktsbestemmelsene får virkning. Behandlingen har følgende varighet:

Databehandlers behandling av personopplysninger på vegne av den behandlingsansvarlige skjer så lenge abonnementet mellom behandlingsansvarlig og databehandleren løper.

Vedlegg B Underdatabehandlere

B.1. Godkjente underdatabehandlere

Ved inngåelse av Kontraktsbestemmelsene gir den behandlingsansvarlige tillatelse til bruk av følgende underdatabehandlere:

Underdatabehandler	Lokasjon	Tjenester	Beskrivelse av behandlingen

Den behandlingsansvarlige skal ved inngåelse av Kontraktsbestemmelsene gi tillatelse til bruk av de ovennevnte underdatabehandlere for behandlingen beskrevet for denne. Databehandleren skal ikke ha rett til – uten den behandlingsansvarliges eksplisitte skriftlige tillatelse – å engasjere en underdatabehandler for «annen» behandling enn den som er blitt avtalt eller benytte en annen underdatabehandler til å foreta den beskrevne behandlingen.

B.2. Varsel for godkjennelse av underdatabehandlere

Behandlingsansvarlig kan motsette seg bruk av ny underdatabehandler med fem (5) dagers skriftlig melding etter mottak av varsel fra databehandler. Dersom behandlingsansvarlig motsetter seg bruk av ny underdatabehandler, kan databehandler avslutte kundeforholdet med behandlingsansvarlig. Dersom databehandler ikke ønsker å avslutte kundeforholdet, kan databehandler velge å videreføre kundeforholdet ved å fortsatt bruke den underdatabehandleren som ble benyttet på det tidspunktet varselet ble gitt.

Vedlegg C Instrukser for behandling av personopplysninger

C.1. Omfanget av/instrukser for behandlingen

Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig utføres av databehandleren på følgende måte:

Behandling:	*Ansvarlig/utføres av:*
Innsamling av personopplysninger ved oppstart	*Behandlingsansvarlig*
Opplasting av personaldata i skytjenesten	*Databehandler*
Lagring i database i skytjenesten	*Databehandler*
Sikkerhetskopiering av databasen	*Databehandler*
Utlevering av personopplysninger – kun til smittevernmyndighet eller behandlingsansvarlig	*Databehandler*
Fysisk sletting etter avsluttet leiekontrakt	*Databehandler*

C.2. Sikkerhet ved behandlingen

Databehandleren er berettiget og forpliktet til å ta beslutninger om tekniske og organisatoriske sikkerhetstiltak som skal iverksettes for å sørge for det nødvendige (og avtalte) sikkerhetsnivået.

Databehandleren skal likevel – i alle tilfelle og minimum – implementere følgende tiltak som er avtalt med den behandlingsansvarlige:

Kun autorisert personell i Qrona.no har tilgang til løsningen. Alle ansatte er underlagt taushetsplikt. Det tas jevnlig backup av databasen. Alle regsistrerte blir automatisk slettet fra databasen etter 10 dager og backuper eldre enn 10 dager slettes.

3. Bistand til den behandlingsansvarlige

Databehandleren skal såfremt det er mulig – innenfor omfanget og i den grad bistanden er spesifisert nedenfor – bistå den behandlingsansvarlige i henhold til punkt 9.1 and 9.2 ved å implementere de følgende tekniske og organisatoriske tiltak:

Qrona. no vil ut fra formålet ikke være i stand til å bistå den behandlingsansvarlige med å sikre den registrertes rettigheter i henhold til artikkel 12 til 23 i personopplysningsloven. Denne løsningen er laget som en følge av at man ønsker å registrere besøkende noe man i en normal situasjon ikke ønsker. Og registreringen skjer med besøksstedets berettigede interesse som lovgrunnlag.

C.4. Lagringsperiode/sletterutiner

Personopplysninger om gjester/kunder lagres kun i ti (10) dager.

Alle sikkerhetskopier av databasen vil slettes/overskrives etter 10 dager.

C.5. Behandlingssted

Behandling av personopplysninger etter Kontraktsbestemmelsene skal ikke utføres på andre lokasjoner enn de følgende uten at det foreligger skriftlig forhåndssamtykke fra den behandlingsansvarlige:

Qrona. no er en skytjeneste. All behandling for databehandlers del foregår innenfor EU/EØS-området. Alle ansatte hos databehandler sitter fysisk innenfor EU/EØS- området. Hva angår underdatabehandlerne (inkludert støttesystemene) fremkommer dette av listen i B.1. Lagringsstedet for Qrona.nos database befinner seg i Irland.

C.6. Instrukser for overføring av personopplysninger til tredjestat

Overføring til tredjestater eller internasjonale organisasjoner kan kun finne sted dersom det foreligger nødvendige garantier for et tilstrekkelig beskyttelsesnivå for personvern i henhold til Gjeldende personvernregler. Med mindre annet er avtalt mellom Partene kan slik overførsel kun finne sted med grunnlag i:

a) en av EU-kommisjonens beslutninger om tilstrekkelig beskyttelsesnivå i henhold til personvernforordningen artikkel 45; eller
b) en databehandleravtale som inkorporerer standard personvernbestemmelser som angitt i personvernforordningen artikkel 46 (2) (c) eller (d) (EU Model clauses); eller
c) bindende virksomhetsregler (Binding Corporate Rules) i henhold til personvernforordningen artikkel 47.

Overføring til tredjestat eller internasjonale organisasjoner vil for Qrona.nos del ikke være aktuelt.

C.7. Fremgangsmåte for den behandlingsansvarliges revisjoner, inkludert inspeksjoner, av behandlingen av personopplysninger som utføres av databehandleren

Databehandleren skal hvert tredje år, for egen regning, innhente fra en uavhengig tredjepart en revisjonserklæring eller et sertifiseringsbevis vedrørende databehandlerens overholdelse av GDPR, eller Medlemsstatenes nasjonale rett og Kontraktsbestemmelsene.

Partene har avtalt at de følgende typer revisjonserklæringer/sertifiseringsbevis kan benyttes for overholdelse av Kontraktsbestemmelsene:

relevante deler av "ISO27k Information seccurity program maturity assessment tool.xlsx"- skjemaet til www.ISO27001security.com som ligger under https://www.iso27001security.com/html/toolkit.html.

Sertifiseringsbevisene skal uten ugrunnet opphold oversendes den behandlingsansvarlige til informasjon. Den behandlingsansvarlige kan bestride frekvensen, omfanget og/eller metodikken for rapporten og kan i et slikt tilfelle anmode om ny revisjon/inspeksjon med endret frekvens, omfang og/eller annen metodikk.

Basert på resultatene av en slik revisjon/inspeksjon, kan den behandlingsansvarlige be om ytterligere tiltak for å sikre overholdelse av GDPR, eller Medlemsstatenes nasjonale rett og Kontraktsbestemmelsene.

Den behandlingsansvarlig eller den behandlingsansvarliges representanter skal i tillegg ha tilgang til å inspisere, herunder fysisk inspisere, lokasjonene hvor behandlingen av personopplysninger gjennomføres av databehandleren, inkludert fysiske lokaler samt systemer benyttet for og knyttet til behandlingen. Slik inspeksjon skal utføres når den behandlingsansvarlige anser det påkrevet.

C.8 Fremgangsmåter for revisjoner, inkludert inspeksjon av behandlingen av personopplysninger som utføres av underdatabehandlere

Databehandleren skal hvert tredje år, for egen regning, innhente et sertifiseringsbevis eller selv gjennomføre en revisjon av underdatabehandlerens overholdelse av GDPR, eller Medlemsstatenes nasjonale rett og Kontraktsbestemmelsene.

Partene har avtalt at de følgende typer sertifiseringsbevis/Self Assessment-skjema kan benyttes for overholdelse av Kontraktsbestemmelsene:

relevante deler av "ISO27k Information seccurity program maturity assessment tool.xlsx"- skjemaet til www.ISO27001security.com som ligger under https://www.iso27001security.com/html/toolkit.html.

Self Assessment- skjemaet eller sertifiseringsbeviset skal uten ugrunnet opphold oversendes den behandlingsansvarlige til informasjon. Den behandlingsansvarlige kan bestride frekvensen, omfanget og/eller metodikken for rapporten og kan i slikt tilfelle anmode om ny revisjon/inspeksjon med endret, omfang og/eller annen metodikk.

Basert på resultatene av en slik revisjon/inspeksjon, den behandlingsansvarlige kan be om ytterligere tiltak for å sikre overholdelse av GDPR, eller Medlemsstatenes nasjonale rett og Kontraktsbestemmelsene.

Dokumentasjon for slike inspeksjoner skal uten ugrunnet opphold overendes den behandlingsansvarlige til informasjon. Den behandlingsansvarlige kan bestride frekvensen, omfanget og/eller metodikken for rapporten og kan i et slikt tilfelle anmode om ny inspeksjon med endret frekvens, omfang og/eller annen metodikk

Vedlegg D Ytterligere bestemmelser avtalt mellom partene

Ytterligere revisjoner og inspeksjoner ref. C.7

Bestrider behandlingsansvarlig frekvensen, omfanget og/eller metodikken for rapporten og ber om ytterligere revisjon/inspeksjon med endret frekvens, omfang og/eller annen metodikk, vil alle kostnader knyttet til dette bli belastet den behandlingsansvarlige.

Ytterligere revisjoner og inspeksjoner ref. C.8

Bestrider behandlingsansvarlig frekvensen, omfanget og/eller metodikken for rapporten og ber om ytterligere revisjon/inspeksjon med endret frekvens, omfang og/eller annen metodikk, vil alle kostnader knyttet til dette bli belastet den behandlingsansvarlige.

Ansvar

Den part som er ansvarlig («den Ansvarlige Part») erkjenner at en registrert som har blitt påført skade for brudd på forpliktelsene som påhviler den Ansvarlige Part under personopplysningsloven, kan kreve erstatning direkte fra denne iht. GDPR

artikkel 82. Dersom en av partene har betalt full erstatning for skaden, skal reglene om regress i henhold til GDPR artikkel 82 nummer 4 og 5 gjelde for krav om regress mellom partene.

Databehandler skal være ansvarlig for skade forårsaket av behandlingen, kun dersom vedkommende ikke har oppfylt forpliktelsene i denne databehandleravtalen og hvis databehandleren eller en eventuell underleverandør har opptrådt utenfor eller i strid med lovlige instruksjoner fra den behandlingsansvarlige, eller dersom databehandleren har misligholdt sine forpliktelser etter personopplysningsloven.

Ansvarsbegrensningene i Tjenesteavtalen gjelder tilsvarende for denne databehandleravtalen. Ansvarsbegrensninger i Tjenesteavtalen gjelder dog ikke for krav om erstatning eller andre kostnader som skyldes databehandlerens eller behandlingsansvarliges grove uaktsomhet eller forsettlige forsømmelse.

Begge parter skal fritas for erstatningsansvar fra den annen part dersom vedkommende godtgjør at vedkommende på ingen måte er ansvarlig for hendelsen som førte til skaden.