

Databehandleravtale

I henhold til gjeldende norsk personopplysningslovgivning og forordning (EU) 2016/679 av 27. april 2016, Artikkel 28 og 29, jf. Artikkel 32-36, inngås følgende avtale

mellom

Navn på institusjonen

SENJA BIBLIOTEK

(behandlingsansvarlig)

og

Navn på tjenesteleverandøren

Axiell Norge AS

(databehandler)

02.10.2019

1. Avtalens hensikt

Avtalens hensikt er å regulere rettigheter og plikter i henhold til gjeldende norsk personopplysningslovgivning og forordning (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.

Avtalen skal sikre at personopplysninger ikke brukes ulovlig, urettmessig eller at opplysningene behandles på måter som fører til uautorisert tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Avtalen regulerer databehandlers forvaltning av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse, i forbindelse med bruk av Mikromarc/CS-Library/Saga, heretter kalt biblioteksystemet.

Ved motstrid skal vilkårene i denne avtalen gå foran databehandlers personvernerklæring eller vilkår i andre avtaler inngått mellom behandlingsansvarlig og databehandler i forbindelse med bruk av biblioteksystemet.

2. Formålsbegrensning

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er å levere og administrere biblioteksystemet.

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan ikke brukes til andre formål enn levering og administrasjon av biblioteksystemet uten at dette på forhånd er godkjent av behandlingsansvarlig.

Databehandler kan ikke overføre personopplysninger som omfattes av denne avtalen til samarbeidspartnere eller andre tredjeparter uten at dette på forhånd er godkjent av behandlingsansvarlig, jf. punkt 10 i denne avtalen.

3. Instruks

Behandlingsansvarlig forplikter seg til å overholde alle plikter i henhold til gjeldende norsk personopplysningslovgivning som gjelder ved bruk av biblioteksystemet til behandling av personopplysninger.

Databehandler forplikter seg til å varsle behandlingsansvarlig dersom databehandler mottar instruks fra behandlingsansvarlig som er i strid med bestemmelsene i gjeldende norsk personopplysningslovgivning.

4. Opplysningstyper og registrerte

Databehandleren forvalter følgende personopplysninger på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av biblioteksystemet:

- For lånerne i biblioteksystemet lagres og behandles informasjon som er nødvendig for å identifisere låneren, som navn og adresse, samt informasjon om avtaler, valg og operativ status.

- For brukere av biblioteksystemet lagres og behandles navn og påloggingsinformasjon, valg og tilganger.
- I biblioteksystemets kataloginformasjon lagres og behandles informasjon om opphavspersoners navn og hvilke verk de assosieres med.
- Biblioteksystemet lagrer og behandler lånerens innloggingsinformasjon og valg låneren har gjort i nettjenestene i informasjonskapsler.
- Biblioteksystemet kan lagre og behandle i anonymisert form hvilke titler lånere har sett på i sesjonslageret for økt funksjonalitet i nettjenestene.

Personopplysningene gjelder følgende registrerte:

- Lånere registrert i biblioteksystemet.
- Brukere av biblioteksystemet tilknyttet behandlingsansvarlig.
- Bibliografisk informasjon registrert i biblioteksystemet.

5. De registrertes rettigheter

Databehandler plikter å bistå behandlingsansvarlig ved ivaretagelse av den registrertes rettigheter i henhold til gjeldende norsk personopplysningslovgivning.

Den registrertes rettigheter inkluderer retten til informasjon om hvordan hans eller hennes personopplysninger behandles, retten til å kreve innsyn i egne personopplysninger, retten til å kreve retting eller sletting av egne personopplysninger og retten til å kreve at behandlingen av egne personopplysninger begrenses.

I den grad det er relevant, skal databehandler bistå behandlingsansvarlig med å ivareta de registrertes rett til dataportabilitet og retten til å motsette seg automatiske avgjørelser, inkludert profilering.

6. Tilfredsstillende informasjonssikkerhet

Databehandler skal iverksette tilfredsstillende tekniske, fysiske og organisatoriske sikringstiltak for å beskytte personopplysninger som omfattes av denne avtalen mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Databehandler skal dokumentere egen sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, risikovurderinger og etablerte tekniske, fysiske eller organisatoriske sikringstiltak. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

Databehandler skal etablere kontinuitets- og beredskapsplaner for effektiv håndtering av alvorlige sikkerhetshendelser. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

Databehandler skal gi egne ansatte tilstrekkelig informasjon om og opplæring i informasjonssikkerhet slik at sikkerheten til personopplysninger som behandles på vegne av behandlingsansvarlig blir ivaretatt.

Databehandler skal dokumentere opplæringen av egne ansatte i informasjonssikkerhet. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

7. Taushetsplikt

Kun ansatte hos databehandler som har tjenstlige behov for tilgang til personopplysninger som forvaltes på vegne av behandlingsansvarlig, kan gis slik tilgang. Databehandler plikter å dokumentere retningslinjer og rutiner for tilgangsstyring. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig.

Ansatte hos databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til i henhold til denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør. Taushetsplikten omfatter ansatte hos tredjeparter som utfører vedlikehold (eller liknende oppgaver) av systemer, utstyr, nettverk eller bygninger som databehandler anvender for å levere eller administrere biblioteksystemet.

Norsk lov vil kunne begrense omfanget av taushetsplikten for ansatte hos databehandler og tredjeparter.

8. Tilgang til sikkerhetsdokumentasjon

Databehandler plikter å gi behandlingsansvarlig tilgang til all sikkerhetsdokumentasjon som er nødvendig for at behandlingsansvarlig skal kunne ivareta sine forpliktelser i henhold til gjeldende norsk personopplysningslovgivning.

Databehandler plikter å gi behandlingsansvarlig tilgang til annen relevant dokumentasjon som gjør det mulig for behandlingsansvarlig å vurdere om databehandler overholder vilkårene i denne avtalen.

Ansatte hos behandlingsansvarlig har taushetsplikt for konfidensiell sikkerhetsdokumentasjon som databehandler gjør tilgjengelig for behandlingsansvarlig.

9. Varslingsplikt ved sikkerhetsbrudd

Databehandler skal uten ubegrunnet opphold varsle behandlingsansvarlig dersom personopplysninger som forvaltes på vegne av behandlingsansvarlig utsettes for sikkerhetsbrudd som innebærer risiko for krenkelser av de registrertes personvern.

Varslet til behandlingsansvarlig skal som minimum inneholde informasjon som beskriver sikkerhetsbruddet, hvilke registrerte som er berørt av sikkerhetsbruddet, hvilke personopplysninger som er berørt av sikkerhetsbruddet, hvilke strakstiltak som er iverksatt for å håndtere sikkerhetsbruddet og hvilke forebyggende tiltak som eventuelt er etablert for å unngå liknende hendelser i fremtiden.

Behandlingsansvarlig er ansvarlig for at varsler om sikkerhetsbrudd fra databehandler blir videreformidlet til Datatilsynet.

10. Underleverandører

Databehandler plikter å inngå egne avtaler med underleverandører til biblioteksystemet som regulerer underleverandørenes forvaltning av personopplysninger i forbindelse med levering og administrasjon av biblioteksystemet.

I avtaler mellom databehandler og underleverandører skal underleverandørene pålegges å ivareta alle plikter som databehandleren selv er underlagt i henhold til denne avtalen. Databehandler plikter å forelegge avtalene for behandlingsansvarlig etter forespørsel.

Databehandler skal kontrollere at underleverandører til biblioteksystemet overholder sine avtalemessige plikter, spesielt at informasjonssikkerheten er tilfredsstillende og at ansatte hos underleverandører er kjent med sine forpliktelser og oppfyller disse.

Behandlingsansvarlig godkjenner at databehandler engasjerer følgende underleverandører i forbindelse med levering og administrasjon av biblioteksystemet:

Databehandler har engasjert selskapet Purity IT AS som leverandør av sikkerhetskopieringstjenester.

Databehandler kan ikke engasjere andre underleverandører enn de som er nevnt ovenfor uten at dette på forhånd er godkjent av behandlingsansvarlig.

Databehandler er erstatningsansvarlig overfor behandlingsansvarlig for økonomiske tap som påføres behandlingsansvarlig og som skyldes ulovlig eller urettmessig behandling av personopplysninger eller mangelfull informasjonssikkerhet hos underleverandører til biblioteksystemet.

11. Overføring til land utenfor EU/EØS

Personopplysninger som databehandler forvalter i henhold til denne avtalen, vil ikke bli overført til mottakerland utenfor EU/EØS.

12. Sikkerhetsrevisjoner og konsekvensutredninger

Databehandler skal jevnlig gjennomføre sikkerhetsrevisjoner av eget arbeid med sikring av personopplysninger mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Databehandler skal gjennomføre sikkerhetsrevisjoner av informasjonssikkerheten i biblioteksystemet. Sikkerhetsrevisjoner skal omfatte databehandlers sikkerhetsmål og sikkerhetsstrategi, sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, etablerte tekniske, fysiske og organisatoriske sikringstiltak og arbeidet med informasjonssikkerhet hos underleverandører til biblioteksystemet. Det skal i tillegg omfatte rutiner for varsling av behandlingsansvarlig ved sikkerhetsbrudd og rutiner for testing av beredskaps- og kontinuitetsplaner.

Databehandler skal dokumentere sikkerhetsrevisjonene. Behandlingsansvarlig skal gis tilgang til revisjonsrapportene.

Dersom en uavhengig tredjepart gjennomfører sikkerhetsrevisjoner hos databehandler, skal behandlingsansvarlig informeres om hvilken revisor som benyttes og få tilgang til oppsummeringer av revisjonsrapportene.

Databehandler skal bistå behandlingsansvarlig dersom bruk av biblioteksystemet medfører at behandlingsansvarlig har plikt til å utrede personvernkonsekvenser før biblioteksystemet tas i bruk/settes i gang, jf. forordning (EU) 2016/679 av 27. april 2016, Artikkel 35 og 36.

Databehandler kan bistå behandlingsansvarlig ved iverksetting av personvernforebyggende tiltak dersom konsekvensutredningen viser at dette er nødvendig.

13. Tilbakelevering og sletting

Ved opphør av denne avtalen plikter databehandler å slette og tilbakelevere alle personopplysninger som forvaltes på vegne av behandlingsansvarlig i forbindelse med levering og administrasjon av biblioteksystemet. Behandlingsansvarlig bestemmer hvordan tilbakelevering av personopplysningene skal skje, herunder hvilket format som skal benyttes.

Databehandler skal slette personopplysninger fra alle lagringsmedier som inneholder personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig. Sletting skal skje ved at databehandler skriver over personopplysninger i rimelig tid etter avtalens opphør. Dette gjelder også for sikkerhetskopier av personopplysningene.

Databehandler skal dokumentere at sletting av personopplysninger er foretatt i henhold til denne avtalen. Dokumentasjonen skal gjøres tilgjengelig for behandlingsansvarlig.

Databehandler dekker kostnader i forbindelse med sletting av de personopplysninger som omfattes av denne avtalen. Utgifter for tilbakelevering av personopplysninger dekkes av behandlingsansvarlige.

14. Mislighold

Ved mislighold av vilkårene i denne avtalen som skyldes feil eller forsømmelser fra databehandlers side, kan behandlingsansvarlig si opp avtalen med øyeblikkelig virkning. Databehandler vil fortsatt være pliktig til å tilbakelevere og slette personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til bestemmelsene i punkt 13 ovenfor.

Behandlingsansvarlig kan kreve erstatning for økonomiske tap som feil eller forsømmelser fra databehandlers side, inkludert mislighold av vilkårene i denne avtalen, har påført behandlingsansvarlig, jf. også punkt 5 og 10 ovenfor.

15. Avtalens varighet

Denne avtalen gjelder så lenge databehandler forvalter personopplysninger på vegne av behandlingsansvarlig.

Avtalen kan sies opp av begge parter med en gjensidig frist på tolv måneder.

16. Kontaktpersoner

Kontaktperson hos databehandler for spørsmål knyttet til denne avtalen er sikkerhetsansvarlig hos databehandler Jonny Karlsen.

Kontaktperson hos behandlingsansvarlig for spørsmål knyttet til denne avtalen er:

17. Lovvalg og vernetting

Avtalen er underlagt norsk rett og partene vedtar Oslo tingrett som vernetting. Dette gjelder også etter opphør av avtalen.

Denne avtale er i 2 – to eksemplarer, hvorav partene har hvert sitt.

Sted og dato

Oslo, 02. oktober 2019

På vegne av behandlingsansvarlig

På vegne av databehandler



KRISTIN STRAND IDÉN
biblioteksjef.
(underskrift)



Kjetil Hillestad
Adm. Dir.
(underskrift)

02.10.2019