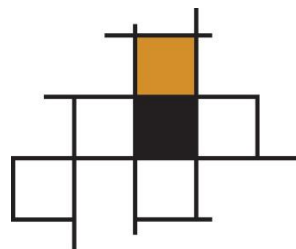


# Mikromarc, Bibliofil, eBokBib og GDPR (General Data Protection Regulation)



**BIBLIOTEK**  
SYSTEMER



**Bibliotekenes IT-senter**

## Innhold

1. Hva er GDPR? .....	3
2. Hva gjør biblioteksystemleverandørene for å etterleve GDPR? .....	3
Gjennomgang av opplysningene som lagres .....	3
Gjennomgang av at planer og sikkerhetsrutiner er i henhold til personvernforordningen og GDPR .....	3
Risikovurdering av håndteringen av personopplysninger .....	3
3. Hva bør kundene gjøre for å etterleve GDPR? .....	4
Samle inn og dokumentere samtykker .....	4
Sørge for oppdatert personvernerklæring .....	4
Bare benytte personlige brukere .....	4
Bare benytte høyeste sikkerhetsnivå på passordregimet .....	4
Sikre at det finnes databehandleravtaler med alle IT-leverandører og brukere av APler .....	5
Tilby innsyn, retting og sletting av lagrede personopplysninger .....	5
Vedlegg 1: Personopplysningene som samles inn .....	6
Vedlegg 2: Forslag til personvernerklæring .....	8
Behandlingsansvarlig .....	8
Personopplysninger som samles inn .....	8
Informasjonskapsler .....	9
Formål med lagring av personopplysningene .....	9
Hjemmel for lagring av personopplysningene .....	9
Utvexling av personopplysninger .....	9
Innsyn og sletting av personopplysninger .....	10
Kontaktperson for personvern .....	10
Vedlegg 3: Databehandleravtaler til signering .....	11

## 1. Hva er GDPR?

EUs forordning for personvern (GDPR) blir norsk lov i mai 2018. Vi får da nye regler for personvern i Norge. GDPR gir virksomheter nye plikter, og personene man behandler personopplysninger om får nye rettigheter. Dagens regelverk stiller krav til at alle skal ha rutiner for å etterleve personopplysningsloven. Når loven endres, må også rutinene endres.

Når man behandler personopplysninger, skal de registrerte ha informasjon. Kravene til denne informasjonen blir strengere når GDPR trer i kraft. Sentrale endringer ellers er også nye krav til vurdering av risiko ved behandling av personopplysninger, avvikshåndtering, samt nye rettigheter til de registrerte når det gjelder innsyn i - og sletting av - registrerte opplysninger. For **nye** systemer inneholder GDPR nye regler om innebygd personvern.

Biblioteksystemleverandørene har en rolle som databehandler for bibliotekene. En databehandler er en virksomhet som behandler personopplysninger på vegne av en annen virksomhet, den såkalt behandlingsansvarlige. Databehandlerens plikter følger av en databehandleravtale mellom den behandlingsansvarlige og databehandleren. GDPR stiller flere nye krav til innholdet i en databehandleravtale. GDPR gir blant annet databehandlere plikt til å:

- sørge for informasjonssikkerhet (artikkel 32)
- umiddelbart varsle den behandlingsansvarlige om avvik (artikkel 33)
- opprette personvernombud på lik linje med behandlingsansvarlig (artikkel 37)

## 2. Hva gjør biblioteksystemleverandørene for å etterleve GDPR?

Biblioteksystemleverandørene samarbeider om håndtering av personopplysninger i Nasjonalt lånerregister. For å oppnå størst mulig kvalitet på arbeidet har Bibliotekenes IT-senter og Bibliotek-Systemer AS også samarbeidet om deler av tilpasningen til GDPR.

### Gjennomgang av opplysningene som lagres

Bibliotekenes IT-senter og Bibliotek-Systemer AS har gjort en total gjennomgang av alle personopplysninger som lagres i systemene. Denne gjennomgangen danner grunnlaget for vurderinger av lovligheten av innsamlingen, rutiner knyttet til innsyn og sletting, samt risikovurderinger.

Denne oversikten kan også være nyttig underlag for kundenes egne vurderinger, og er i hovedtrekk vedlagt som vedlegg 1.

### Gjennomgang av at planer og sikkerhetsrutiner er i henhold til personvernforskriften og GDPR

Personvernforskriften stiller en rekke krav til blant annet sikkerhetsmål, sikkerhetsstrategi, avvikshåndtering, personellsikkerhet, fysisk sikkerhet, systemteknisk sikkerhet, dokumentetsikkerhet, konfidensialitet/taushetsplikt og sikkerhet hos underleverandører. Det er også krav om databehandleravtaler med underleverandører.

Bibliotekenes IT-senter og Bibliotek-Systemer AS har oppdatert rutiner og planverk for å komme i samsvar med GDPR. Vi har også dokumentert nye rutiner internt for varsling av behandlingsansvarlige og Datatilsynet ved avvik.

### Risikovurdering av håndteringen av personopplysninger

Bibliotekenes IT-senter og Bibliotek-Systemer AS har i 2018 gjort en risikovurdering av personopplysningene som lagres. Vi har identifisert en rekke tiltak som vil bli gjennomført i tiden framover, delvis i samarbeid knyttet til Nasjonalt lånerregister, og delvis hver for oss.

Oversikten over identifiserte tiltak er konfidensiell.

### 3. Hva bør kundene gjøre for å etterleve GDPR?

Som behandlingsansvarlig er kundene selv hovedansvarlig for å følge personvernloven, personvernforskriften og GDPR i behandlingen av personopplysninger. Systemleverandørene sitter med viktig underlag for å kunne oppfylle dette ansvaret, og vi har derfor valgt å gi noen råd nedenfor.

#### Samle inn og dokumentere samtykker

Bibliotekenes IT-senter og Bibliotek-Systemer har kartlagt personopplysningene som samles inn i systemene i vedlegg 1. Vi har ikke funnet opplysninger som er sensitive i lovens forstand, men mange opplysninger med potensial til å ha store negative konsekvenser om de kommer på avveie, for eksempel fødselsnumre og opplysninger om lån og reserveringer.

Basert på en konkret vurdering av opplysningene som samles inn, samt tidligere dialog med Datatilsynet om Nasjonalt lånerregister, mener vi at innsamlingen av opplysningene må baseres på informert samtykke fra den enkelte bruker. At samtykke er informert, krever både at det har et tilstrekkelig detaljnivå når det gjelder opplysningene som samles inn, og at informasjonen er forståelig for målgruppen.

Avgitt samtykke til behandling av personopplysninger gjelder til det blir trukket tilbake i henhold til GDPR artikkel 13 (2) bokstav c.

Det er ikke spesifikke krav til dokumentasjon for at informert samtykke er gitt, men bibliotekene må kunne sannsynliggjøre det. Vi anbefaler derfor bibliotekene å oppbevare underskrifter som dokumentasjon. På litt lenger sikt er Biblioteksystemleverandørene i dialog med Nasjonalbiblioteket om en felles tjeneste for elektronisk innhenting av samtykker.

Informasjon for innhenting av samtykker knyttet til Nasjonalt lånekort (<http://lanekortet.no/brosjyre.htm>) er utformet i samarbeid med Datatilsynet for en tid tilbake. Denne informasjonen bør etter vår oppfatning utvides slik at den dekker alle opplysningstypene i vedlegg 1 og/eller vedlegg 2.

#### Sørge for oppdatert personvernerklæring

Personopplysningsloven og GDPR gir den registrerte omfattende rettigheter til informasjon om hvilke personopplysninger som behandles, kilder for opplysningene, sikring av personopplysninger, utveksling av personopplysninger, hvem som er behandlingsansvarlig, formålet med behandlingen og den registrertes rettigheter.

For å ivareta disse rettighetene anbefaler Datatilsynet at det utarbeides en elektronisk personvernerklæring som legges på relevante nettsider (<https://www.datatilsynet.no/regelverk-og-skjema/lage-nye-losninger/personvernerklaering/>).

Mikromarc, Bibliofil og eBokBib vil få menyvalg for lenke til personvernerklæring i løpet av våren 2018. Opplysningene i personvernerklæringen bør tilpasses av den enkelte kunde, men vi vedlegger vårt eget utkast til tekst i vedlegg 2.

#### Bare benytte personlige brukere

GDPR inneholder bestemmelser om sikring, sporbarhet og ivaretagelse av integriteten til personopplysningene som registreres. For å ivareta dette anbefaler vi å bare benytte personlige brukere i systemene, og ikke fellesbrukere som «Skranke», «Katalog» osv.

#### Bare benytte høyeste sikkerhetsnivå på passordregimet

I Mikromarc er det mulig å stille inn formelle krav til passordstyrke og frekvens på bytte av passord. Bibliotekenes IT-senter anbefaler at det strengeste konfigurasjonsalternativet benyttes.

Ta kontakt med Brukerstøtte for hjelp til å endre passordregime.

I Bibliofil gis det frist til 1. juni 2018 for alle brukere å sette nytt sikkert passord. Brukerkonti hvor nytt passord ikke er satt innen fristen, blir automatisk låst.

Sikre at det finnes databehandleravtaler med alle IT-leverandører og brukere av APler Personvernlovgivningen og GDPR sier helt klart at det skal finnes databehandleravtaler mellom alle behandlingsansvarlige og alle som behandler personopplysninger på vegne av dem. Brukere av Mikromarc, Bibliofil og eBokBib må derfor ha databehandleravtaler med oss, **og andre som gis tilgang til personopplysningene**. Dette gjelder også organisasjoner som har tilgang til systemene gjennom APler.

Datatilsynet har laget en veileder for utforming av databehandleravtaler (<https://www.datatilsynet.no/regelverk-og-skjema/veiledere/databehandleravtale/>). Denne vil bli oppdatert med hensyn på GDPR i mars/april 2018.

Dersom ditt kundeforhold med oss er gammelt, kan det være at avtalen din ikke har blitt supplert med en databehandleravtale. Vedlegg 3 inneholder en oppdatert databehandleravtale som kan signeres og returneres til oss.

Tilby innsyn, retting og sletting av lagrede personopplysninger

Både gammel og ny personvernlovgivning har bestemmelser om rett til innsyn i lagrede personopplysninger, hvordan de er sikret og rett til å få dem korrigert eller slettet. Disse bestemmelsene er nå ytterligere skjerpet i GDPR. Datatilsynet har laget en mal for en slik innsynsbegjæring (<https://www.datatilsynet.no/globalassets/global/skjema-maler/innsynsmal.pdf>). Fristen for å svare på slike krav er satt til en måned.

Biblioteksystemene har i dag gode rutiner for retting av opplysninger og fullstendig sletting av alle opplysninger om en låner. De aller fleste opplysningene som samles inn i Mikromarc, Bibliofil og eBokBib er tilgjengelig for innsyn via sidene Meg&Mitt, Mappa Mi og Min Side i biblioteksystemenes ulike søkegrensesnitt på nett. Som dokumentert i vedlegg 1, finnes det enkelte detaljopplysninger og historiske opplysninger utover dette. Kontakt Brukerstøtte for bistand dersom dere mottar krav om fullstendig innsyn fra enkeltpersoner.

## Vedlegg 1: Personopplysningene som samles inn

Type	Personopplysning	Formål
Låner	System id	Unik låneridentifikator
Låner	Navn	Håndheve avtale om lån og tilgang til biblioteket
Låner	Strekkode	Autentisere for lån og tilgang til nett-tjenester
Låner	Nasjonalt lånernummer	Identifisere lånere som har Nasjonalt lånekort
Låner	Fødselsnummer	Unik låneridentifikator på tvers av systemer
Låner	Biblioteksenhet	Å identifisere enheten der låner plukker opp bestilt materiale
Låner	Lånergruppe	Håndheve riktige låneregler
Låner	Klasse	Gjøre lærere i stand til å følge opp elever i egen klasse
Låner	PIN/Passord	Autentisering for selvbetjeningsløsninger
Låner	Sperring	Identifisere lånere som ikke følger lånereglene
Låner	Sperreårsak	Identifisere hvilke regler låneren har brutt
Låner	Sperredato	Spore tidspunkt for sperring
Låner	Utløpsdato	Identifisere foreldede lånerposter for sletting
Låner	Fødselsdato	Forhindre lån av materiale låneren ikke er gammel nok til å låne
Låner	Kjønn	For statistikkformål
Låner	Foretrukket språk	For kommunikasjon med låneren på riktig språk
Låner	Foto	For identifikasjon i en utlånsituasjon
Låner	Melding til låner	Dersom låner har glemt noe etc.
Låner	Internt låner-memo	Brukes som biblioteket ønsker
Låner	Avtale om tilgang utenom åpningstid	For å gi låner tilgang til biblioteket utenom vanlig åpningstid.
Låner	Dato for avtale om tilgang utenom åpningstid	For sporing av adgangsavtalen
Låner	Bruker som innvilget avtale om tilgang utenom åpningstid	For sporing av adgangsavtalen
Låner	Permanent adresse	For påminnelser om lån, reserveringer og fjernlån
Låner	Midlertidig adresse	For påminnelser om lån, reserveringer og fjernlån
Låner	Telefonnummer	For personlig kontakt med låner
Låner	Mobilnummer	For påminnelser om lån, reserveringer og fjernlån
Låner	Fax-nummer	For bruk ved registrering av organisasjoner (foreldet?)
Låner	E-post-adresse 1	For påminnelser om lån, reserveringer og fjernlån
Låner	E-post-adresse 2	For påminnelser om lån, reserveringer og fjernlån
Låner	Motta e-post	For informasjon om lånerpreferanser
Låner	Kvitteringer på e-post	For informasjon om lånerpreferanser
Låner	Motta SMS	For informasjon om lånerpreferanser
Låner	Motta påminnelser	For informasjon om lånerpreferanser
Låner	Informasjon om foreldre	Slik at foreldre kan administrere barnas lån, reserveringer og gebyrer.
Låner	Informasjon om barn	Slik at foreldre kan administrere barnas lån, reserveringer og gebyrer.
Låner	Registreringsdato	For å kunne spore registreringen av låneren
Låner	Registrert av	For å kunne spore registreringen av låneren
Låner	Dato sist endret	For å kunne spore endringer i låneropplysningene
Låner	Sist endret av	For å kunne spore endringer i låneropplysningene
Låner	Integrasjon med NAVET (Skatteverket i Sverige)	For import og oppdatering av låneropplysninger (Brukes i Sverige)
Låner	NAVET status (Skatteverket i Sverige)	For import og oppdatering av låneropplysninger (Brukes i Sverige)

Låner	Boken-kommer-låner	For å kunne følge opp eldre låner i hjemmet
Låner	Siste aktivitetsdato	For å kunne spore inaktive låner som er kandidater til å slettes i systemet.
Låner	Aktive lån	For å være i stand til å følge opp lånt materiale
Låner	Kortvarig informasjon om historiske lån (oppbevares i 2 uker etter innlevering)	For å kunne kreve kompensasjon om deler av materialet er ødelagt eller savnet
Låner	Historiske lån	For å kunne gi låner opplysninger om tidligere lånt materiale (Boken kommer). Dette krever særskilt samtykke fra låneren.
Låner	Aktive reserveringer	For å kunne varsle låner når materialet ankommer biblioteket.
Låner	Historiske reserveringer	For statistikk, forbindelsen til låner er brutt.
Låner	Utlånsmeldinger	For å kunne dokumentere at purringer er sendt låneren, samt unngå at krav foreldes.
Låner	Fjernlånsbestillinger	Slik at låner kan motta materiale fra et annet bibliotek
Låner	Tidsskriftbestillinger	Slik at låner automatisk kan motta nye tidsskrifthefters
Låner	Søkeord (med IP-adresse)*	For å kunne forbedre biblioteksystemets søkemuligheter, samt feilsøking. Lagringen er helt anonym når Mikromarc driftes av Bibliotekenes IT-senter på grunn av bruk av lastbalanserer/proxy.
Låner	Websidestatistikk (Med IP-adresse og/eller strekkode)*	For å kunne forbedre biblioteksystemets søkemuligheter, samt feilsøking. Lagringen er helt anonym når Mikromarc driftes av Bibliotekenes IT-senter på grunn av bruk av lastbalanserer/proxy.
Bruker (I tillegg til Låner)	Brukernavn	For autentisering for bruk av klienter
Bruker (I tillegg til Låner)	Passord	For autentisering for bruk av klienter
Bruker (I tillegg til Låner)	Katalogtilgang	For å kunne tildele differensierte rettigheter
Bruker (I tillegg til Låner)	Enhetstilgang	For å kunne tildele differensierte rettigheter
Bruker (I tillegg til Låner)	Brukergrupper	For å kunne tildele differensierte rettigheter
Bruker (I tillegg til Låner)	Poster opprettet av bruker	For at endringer skal være sporbare
Bruker (I tillegg til Låner)	Dato posten ble opprettet	For at endringer skal være sporbare
Bruker (I tillegg til Låner)	Poster bruker har oppdatert	For at endringer skal være sporbare
Bruker (I tillegg til Låner)	Dato for oppdatering av post	For at endringer skal være sporbare
Bruker (I tillegg til Låner)	Tilgangsavtale signert av bruker	For at avtaler om tilgang utenfor ordinær åpningstid skal være sporbare i forhold til brukeren som har inngått avtalen.
Bruker (I tillegg til Låner)	Dato for tilgangsavtale	For at avtaler om tilgang utenfor ordinær åpningstid skal være sporbare i forhold til brukeren som har inngått avtalen.
Bibliografisk informasjon	Forfatternavn/Navn på person ansvarlig for verk	Mulighet for å søke og vise informasjon om verk
Bibliografisk informasjon	Fødselsår	Mulighet for å søke og vise informasjon om verk
Bibliografisk informasjon	Dødsår	Mulighet for å søke og vise informasjon om verk
Bibliografisk informasjon	Nasjonalitet	Mulighet for å søke og vise informasjon om verk
Bibliografisk informasjon	Titler og nummer assosiert med navn	Mulighet for å søke og vise informasjon om verk
Bibliografisk informasjon	Relasjon til verk	Mulighet for å søke og vise informasjon om verk

\*For sentraldriftskunder slettes søkelogger regelmessig av Bibliotekenes IT-senter.

## Vedlegg 2: Forslag til personvernerklæring

Denne personvernerklæringen forteller om hvordan Bibliotekenes IT-senter AS samler inn og bruker personopplysninger på vegne av våre kunder. Bibliotekenes IT-senter er databehandler for et stort antall bibliotek i Norge, Sverige, Finland og England.

### Behandlingsansvarlig

Administrerende direktør i Bibliotekenes IT-senter er *behandlingsansvarlig* for virksomhetens *behandling av personopplysninger*. Der det daglige ansvaret er delegert, kommer det fram under hvert enkelt punkt. Delegeringen omfatter kun oppgavene og ikke ansvaret. Erklæringen inneholder opplysninger du har krav på når det samles inn personopplysninger (personopplysningsloven § 19) og generell informasjon om hvordan vi behandler personopplysninger (personopplysningsloven § 18 1.ledd).

### Personopplysninger som samles inn

Mikromarc lagrer følgende personopplysninger om bibliotekenes lånere:

- Navn
- Adresse
- Evt. midlertidig adresse
- Fødselsdato
- Kjønn
- Telefonnumre
- E-postadresser
- Valg knyttet til om meldinger ønsket mottatt på e-post, SMS eller som brev
- Lånergruppe (barn, voksen osv)
- Foretrukket språk
- Strekkode
- PIN/passord
- Hjemmebibliotek
- Informasjon om Nasjonalt lånekort er tilknyttet Nasjonalt lånekort
- Fødselsnummer (dersom Nasjonalt lånekort er tilknyttet Nasjonalt lånekort eller låneren aksepterer det)
- Klasse (dersom låner er skoleelev)
- Informasjon om barn (dersom biblioteket og låneren ønsker det)
- Informasjon om foreldre (dersom biblioteket og låneren ønsker det)
- Opplysning om evt. sperring for lån, samt årsak til sperringen og dato for sperringen
- Utløpsdato for Nasjonalt lånekort
- Foto av låneren (bare i noen bibliotek)
- Melding til låneren
- Intern melding om låneren (interesseområder og lignende)
- Opplysninger om eventuell avtale om adgang til biblioteket utenom ordinær arbeidstid
- Aktive lån
- Historiske lån inntil 14 dager etter innlevering, lenger ved individuell avtale med låneren
- Utlånsmeldinger (utsendte purringer, erstatningsbrev, reserveringsbrev)
- Aktive reserveringer
- Aktive fjernlånsbestillinger
- Løpende bestillinger av nye tidsskrifthefter
- Bruk av nettsted (nettstedloggene slettes ukentlig)
- Informasjonskapsler



## Informasjonskapsler

Informasjonskapsler (cookies) er små tekstfiler som plasseres på din datamaskin når du laster ned en nettside.

I Mikromarc brukes informasjonskapsler i følgende tjenester:

- Mikromarc Websøk
- Mikromarc Mobilweb
- Mikromarc+ for personale

Informasjonskapslene brukes til å forbedre brukeropplevelsen, blant annet å huske påloggingsopplysninger.

Bibliotekenes IT-senter bruker ikke informasjonskapsler til å generere statistikk, og vi kan dermed ikke spore din bruk av Mikromarc tilbake til deg som enkeltperson. Mikromarc bruker cookies, også kalt informasjonskapsler. En informasjonskapsel er en liten tekstfil som lagres på din datamaskin og inneholder informasjon.

Lagring og bruk av informasjon er ikke tillatt med mindre brukeren er informert om og har godtatt at informasjonen lagres, målet med lagringen og måten informasjonen blir brukt. Ved å fortsette å bruke Mikromarc godtar du at informasjonskapsler lagres i din datamaskin, siden de fleste nettleserprogrammer automatisk godtar å lagre disse.

Det finnes to typer informasjonskapsler: Den ene typen lagrer en fil på brukerens datamaskin. Denne filen brukes normalt til å huske brukerens preferanser og innstillinger mellom sesjoner. Den andre typen er en temporær fil som bare lagres under aktiv bruk og blir slettet så fort nettleservinduet lukkes. Ingen personlig informasjon om brukeren blir lagret. I Mikromarc brukes begge typene informasjonskapsler til henholdsvis å lagre brukerens språkvalg og å beskytte mot dataangrep.

Hvis du ikke godtar bruk av informasjonskapsler, kan bruk av informasjonskapsler skruses av i innstillingene til nettleserprogrammet. Imidlertid bruker Mikromarc informasjonskapsler til å sikre bruken av applikasjonen, og det å ikke godta informasjonskapsler vil gjøre at mye av nettstedet ikke vil fungere. Det anbefales derfor ikke.

## Formål med lagring av personopplysningene

Personopplysningene lagres for at bibliotekene skal kunne administrere utlån av bøker og annet materiale til lånerne, samt andre tjenester.

## Hjemmel for lagring av personopplysningene

Hovedgrunnlaget for behandlingen av personopplysningene finnes i personvernforordningens (GDPR) Artikkel 6 1 a): «Den registrerte har gitt samtykke til behandling av sine personopplysninger for ett eller flere spesifikke formål». Du skal ha fått informasjon om lagring av personopplysninger og gitt ditt samtykke da du ble registrert som låner.

I noen tilfeller bygger også lagringen på GDPR artikkel 6 1 c): «Behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt». Bibliotekene er pålagt å samle inn statistikk over bruken av biblioteket. Denne statistikken kan ikke identifiseres på personnivå og avleveres til Nasjonalbiblioteket.

## Utteksling av personopplysninger

I Norge utveksles adresseopplysninger og enkelte andre personopplysninger med Nasjonalt lånerregister, en database som gjør det mulig og effektivt å benytte samme lånekort i mange forskjellige bibliotek i Norge. Det utveksles bare opplysninger om lånerne som har gitt særskilt samtykke til å være registrert i Nasjonalt lånerregister. Det utveksles ikke opplysninger om lån, reserveringer, gjeld, svartelister og andre forhold mellom låner og det enkelte bibliotek.

Nasjonalbiblioteket og biblioteksystemleverandørene i Norge står bak Nasjonalt lånerregister, og det foreligger databehandlingsavtale mellom partene.

### Innsyn og sletting av personopplysninger

Du kan kreve innsyn i personopplysningene som lagres om deg, og du kan også kreve opplysningene rettet eller slettet innen en måned. Vær oppmerksom på at lagring av noen opplysninger er nødvendig for at du kan være låner ved biblioteket.

Menyvalget Meg & Mitt gir innsyn til nesten all informasjon biblioteksystemet har lagret om deg. Ta kontakt med ditt bibliotek dersom du ønsker utvidet innsyn i personopplysninger eller ønsker sletting av personopplysninger.

### Kontaktperson for personvern

Bibliotekenes IT-senter AS og datterselskapene Bibliotekscentrum AB og Open Library Solutions AB er databehandler for bibliotek i Norge Sverige og Finland. Ta kontakt med ditt bibliotek dersom du har spørsmål om lagring av personopplysninger.

Bibliotekenes IT-senter, Bibliotekscentrum og Open Library Solutions er ansvarlig for utvikling og drift av biblioteksystemet Mikromarc. Spørsmål om utvikling og drift av systemet kan rettes til sikkerhetsansvarlig og personvernombud Jonny Karlsen i Bibliotekenes IT-senter (e-post: [jonny.karlsen@bibits.no](mailto:jonny.karlsen@bibits.no), telefon +47 22 08 98 00).

## 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

.....

(behandlingsansvarlig)

og

Navn på tjenesteleverandøren

Bibliotekenes IT-senter AS

(databehandler)

## 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. Instruksjer

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 instruksjer 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 lånere 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 net tjenestene i informasjonskapsler.
- Biblioteksystemet kan lagre og behandle i anonymisert form hvilke titler lånere har sett på i sesjonslageret for økt funksjonalitet i net tjenestene.

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 ivarettatt.

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 verneting

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

\*\*\*

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

Sted og dato

Oslo, 18. april 2018

På vegne av behandlingsansvarlig

På vegne av databehandler



.....

(underskrift)

Kjetil Hillestad

Adm. Dir.