DATABEHANDLERAVTALE

1. BAKGRUNN OG FORMÅL

1.1 Denne Databehandleravtalen gjelder mellom

_____
Det ansvarlig bibliotek/organisasjon ("Behandlingsansvarlige")
og Nasjonalbiblioteket
("Databehandleren").

1.2 Formålet med denne Databehandleravtalen er å fastlegge partenes rettigheter og plikter vedrørende Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige i forbindelse med bruk av tjenesten **Nasjonalt låneregister og Bibliotekkortet** som leveres av Databehandleren.

2. DEFINISJONER

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

2.2 "**Gjeldende personvernregler**": Gjeldende lover og regler om personvern, inkludert personopplysningsloven og GDPR.

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

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

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

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

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

3. OMFANG

3.1 Denne Databehandleravtalen gjelder alle personopplysninger som Databehandleren har mottatt, er gitt tilgang til eller har generert i forbindelse med bruk av tjenesten **Nasjonalt låneregister og Bibliotekkortet**.

3.2 Databehandlingens formål og art, typen personopplysninger som behandles, samt kategorier av registrerte, fremgår av Vedlegg 1. Databehandleren skal behandle personopplysningene utelukkende for det formål og innenfor det omfang som er angitt i Vedlegg 1 og for øvrig i samsvar med den Behandlingsansvarliges dokumenterte instrukser.

4. GENERELLE PLIKTER

4.1 Den Behandlingsansvarlige skal etterleve sine forpliktelser etter gjeldende personvernregler, herunder ved å sørge for behandlingsgrunnlag og at de registrerte har mottatt nødvendig personverninformasjon.

4.2 Databehandleren garanterer å ha gjennomført egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i henhold til gjeldende personvernregler og ivaretar de registrertes rettigheter, og at disse tiltakene vil etterleves i hele avtaleperioden.

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

5. BISTAND TIL DEN BEHANDLINGSANSVARLIGE

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

5.2 Med hensyn til behandlingens art og den informasjon som er tilgjengelig for Databehandleren, skal Databehandleren bistå den Behandlingsansvarlige med forpliktelsene i henhold til GDPR artikkel 32 til 36, herunder forpliktelsene til datasikkerhet (som nærmere beskrevet i punkt 6), melding om brudd på personopplysningssikkerhet (som nærmere beskrevet i punkt 9), vurdering av personvernkonsekvenser, samt forhåndsdrøftinger.

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

6. TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

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

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

6.3 Databehandleren skal påse at alle personer som er autorisert til å behandle personopplysningene har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt. På forespørsel fra den Behandlingsansvarlige skal Databehandleren fremlegge kopi av slike personers signerte taushetsavtaler.

7. BRUK AV UNDERDATABEHANDLERE

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

7.2 I henhold til punkt 7.1 skal Databehandleren kun engasjere underdatabehandlere som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at databehandlingen oppfyller kravene etter gjeldende personvernregler og som sikrer de registrertes personvern.

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

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

8. INTERNASJONAL DATAOVERFØRING

8.1 Databehandleren kan kun overføre personopplysninger til tredjestater eller en internasjonal organisasjon dersom slik overføring oppfyller vilkårene i GDPR kapittel 5 og kun etter dokumenterte instrukser fra den Behandlingsansvarlige.

8.2 Databehandleren kan imidlertid overføre personopplysninger uten instruks hvis det kreves i henhold til gjeldende rett i EØS-området. I slike tilfeller skal Databehandleren underrette den Behandlingsansvarlige om nevnte rettslige krav før overføringen, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal Databehandleren underrette den Behandlingsansvarlige så snart retten tillater dette).

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

9. BRUDD PÅ PERSONOPPLYSNINGSSIKKERHETEN

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

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

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

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

c. formidle navn og kontaktinformasjon til personvernrådgiveren eller et annet kontaktpunkt hos Databehandleren for ytterligere innhenting av informasjon;

d. beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten;

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

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

9.3 Databehandleren skal så snart som mulig gjennomføre alle tiltak som beskrevet i punkt e. ovenfor, samt gjennomføre alle de tiltak som med rimelighet kreves for å unngå at det senere oppstår lignende brudd på personopplysningssikkerheten. Databehandleren skal tillate den Behandlingsansvarlige å undersøke, fastlegge årsaken til og å verifisere de tiltak som er gjennomført eller foreslått av den Behandlingsansvarlige for å håndtere bruddet på personopplysningssikkerheten. Databehandleren skal, så langt det er mulig, rådføre seg med den Behandlingsansvarlige med hensyn til de tiltak som skal gjennomføres samt overveie innspill fra den Behandlingsansvarlige i den forbindelse.

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

10. REVISJON

10.1 Databehandleren skal dokumentere, samt gjøre tilgjengelig for den Behandlingsansvarlige, informasjon som er nødvendig for å påvise etterlevelse av denne Databehandleravtalen og gjeldende personvernregler.

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

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

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

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

11. VARIGHET OG OPPSIGELSE

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

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

[signaturfelt på neste side]

For den Behandlingsansvarlige:

Behandlingsansvarliges
bibliotek/ organisasjon:

_____

Signatur:

_____

Navn:

_____

Dato:

_____

For Databehandleren:

Nasjonalbiblioteket

Signatur:

_____

Navn:

_____

Dato:

_____

VEDLEGG 1: DATABEHANDLINGENS OMFANG

Behandlingens formål
Formålet med databehandlingen er driften av Nasjonalt låneregister. En bruker kan enten registrere seg selv, eller få en ansatt ved et bibliotek til å registrere seg i dette registeret. Når informasjon er registrert ved et bibliotek kan informasjonen om en bruker utveksles med andre bibliotek om brukeren vil bli låner også der. Dette skjer kun med brukerens godkjenning.

Behandlingens art, hensikt og typen personopplysninger
Når en bruker innlemmes i Nasjonalt låneregister, mottar databehandleren følgende opplysninger:

- Lånernummer på Bibliotekkortet
- Forrige lånernummer hvis låneren har fått utstedt nytt
- Fullt navn
- Fødselsnummer (lagres i kryptert form)
- Fødselsdato
- Kjønn
- Pinkode i kryptert form
- Passord i kryptert form
- Primæradresse (folkeregistrert adresse)
- Midlertidig adresse med dato for hvor lenge den skal være gyldig
- 4 Telefonnumre: hjemme, jobb, mobil og primærkontakt
- E-postadresse med tilhørende flagg om den bør sjekke
- Hjemmebiblioteknummer
- Tilknyttede biblioteknumre
- Hvilket biblioteknummer opprettet kortet og når det ble gjort
- Hvilket biblioteknummer endret personopplysnignene sist og når det ble gjort
- Dato for når personopplysningene sist ble sjekket mot Folkeregisteret
- Dato for når låneren sist var aktiv
- Foresattknytning mellom foresattes og barnets lånernummer og felt for å si når og av hvem disse knytningene ble gjort
- Felt for å definere hvilket sikkerhetsnivå låneren ønsker å bruke ved autentisering
- Andre låneridenter knyttet til låneren, primært Feide ID, men kan også benyttes for andre identer ved behov (Pocket ID, skolekort ID) med datostempel for når det ble opprettet og når det skal slettes.

Ovennevnte opplysninger benyttes i mottaksøyeblikket til å verifisere en bruker med det formål å utstede Bibliotekkortet.

Følgende opplysninger lagres av Databehandleren:

- Lånernummer på Bibliotekkortet
- Forrige lånernummer hvis låneren har fått utstedt nytt
- Fullt navn
- Fødselsnummer (lagres i kryptert form)
- Fødselsdato
- Kjønn
- Pinkode i kryptert form
- Passord i kryptert form
- Primæradresse (folkeregistrert adresse)
- Midlertidig adresse med dato for hvor lenge den skal være gyldig
- 4 Telefonnumre: hjemme, jobb, mobil og primærkontakt
- E-postadresse med tilhørende flagg om den bør sjekkes
- Hjemmebiblioteknummer
- Tilknyttede biblioteknumre
- Hvilket biblioteknummer opprettet kortet og når det ble gjort
- Hvilket biblioteknummer endret personopplysnignene sist og når det ble gjort
- Dato for når personopplysningene sist ble sjekket mot Folkeregisteret

- Dato for når låneren sist var aktiv
- Foresattknytning mellom foresattes og barnets lånernummer og felt for å si når og av hvem disse knytningene ble gjort
- Felt for å definere hvilket sikkerhetsnivå låneren ønsker å bruke ved autentisering.
- Andre låneridenter knyttet til låneren, primært Feide ID, men kan også benyttes for andre identer ved behov (Pocket ID, skolekort ID) med datostempel for når det ble opprettet og når det skal slettes.

VEDLEGG 2: TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

Databehandleren skal som et minimum gjennomføre alle de tiltak som er angitt eller henvist til nedenfor.

Personopplysninger
Kun personopplysninger, adresseinformasjon og autentiseringsinformasjon lagres om sluttbruker i Nasjonalt lånerregister. Nasjonalt lånerregister verken behandler eller lagrer opplysninger om sluttbrukers låneforhold ved bibliotekene hen er tilknyttet.

Krypteringstiltak
Alle tjenester er begrenset til bruk over HTTPS. Dette gjelder både tjenester rettet mot sluttbruker og API-tilgang for de forskjellige systemene som kommuniserer med Nasjonalt lånerregister. Krypteringsprotokoller for HTTPS slås av fortløpende når de regnes som usikre. Per 2023 kreves TLSv1.2 eller høyere.
I Nasjonalt lånerregister er fødselsnummer (AES-256-CBC), pinkode (AES) og passord (SHA-512/PBKDF2) kryptert.

Tiltak for å sikre personopplysningenes fortrolighet
Kun autoriserte personer i Bibliotek-Systemer As har direkte/lavnivå tilgang til tjenesten som forvalter personopplysningene. Deres tilgang er for å sikre pålitelig drift og sikring av tjenesten.
Personopplysningene utveksles på systemnivå med godkjente systemleverandører på vegne av sine bibliotek. For at disse skal kunne utveksle data med tjenesten må de ha to autorisasjonskoder. Den ene er en systemleverandørspesifikk kode, den andre er det spesifikke bibliotekets autorisasjonskode fra Base Bibliotek. Disse kodene "hashes" og brukes som autorisasjonskode for å få tilgang til Nasjonalt lånerregister. Dette sikrer at hver enkelt systemleverandør kan kun kommunisere med tjenesten på vegne av sine kunder (systemleverandør for biblioteket må være registrert i Base Bibliotek).
Utveksling av personopplysninger begrenses videre ved at bibliotekene kun får basisopplysninger før sluttbruker er knyttet til det aktuelle biblioteket. Disse personopplysningene er begrenset til kun nødvendig informasjon slik at biblioteket kan sikere at personene som skal knyttes til biblioteket en den samme som er registrert i Nasjonalt låneregister.
Andre bibliotekrelaterte tjenester som trenger tilgang til å kunne autentisere sluttbrukere av Bibliotekkortet bruker begrensede API-kall. Hver enkelt leverandør vil få en egen autorisasjonskode og personopplysningene disse får tilgang til er begrenset til sjekk av pinkode og passord, alder, sluttbrukers hjemmebibliotek (biblioteknummer) og hvilke bibliotek (biblioteknummer) sluttbrukeren eventuelt er tilknyttet.
Sluttbruker kan få innsyn i sine personopplysninger på bibliotekkortet.no. dette krever bruk av to-faktorautentisering.

Tilgangskontroll for sluttbruker
Sluttbruker vil autentisere seg på bibliotekkortet.no ved hjelp av lånekortnummer og passord, Feide eller ID-porten. Sluttbruker vil kunne velge ønsket sikkerhetsnivå fir autentiseringen og dette skal ligge til grunn for innlogging i bibliotekenes tjenester for denne sluttbrukeren.

Tiltak for å sikre personopplysningenes integritet
Personopplysningene oppdateres automatisk mot Folkeregisteret for å sikre at de er oppdaterte. Opplysningene som synkroniseres er fullt navn, kjønn og bostedsadresse.

Tiltak for å sikre tilgjengeligheten til personopplysningene
Tjenesten er sikret med flere lag med redundans og backup.

Tiltak ved sletting
Når sluttbruker slettes i Nasjonalt låneregister blir det sendt varsel til sluttbruker med liste over tilknyttende bibliotek slik at sluttbruker eventuelt kan ta kontakt med bibliotekene for å be om å bli slettet også hos disse.
Når sluttbruker slettes blir alle personopplysningene i Nasjonalt låneregister slettet. Lånekortnummeret (N-nummeret) blir beholdt i databasen for å sikre at lånekortet ikke kan gjenbrukes.