

## **Rutine for informasjonssikkerhet for personopplysninger i BRIS**

# **RUTINE FOR INFORMASJONSSIKKERHET FOR PERSONOPPLYSNINGER I BRIS**

### **Innhold**

1. Innledning	2
2. Formålet med BRIS	2
3. Personopplysninger i BRIS	3
4. Roller	3
5. Rutiner for informasjonssikkerhet for personopplysninger	4
5.1 Krav til konfidensialitet	4
5.2 Krav til integritet	5
5.3 Krav til tilgjengelighet	5
6. Avviksmelding	6
7. Generelt om utlevering av opplysninger fra BRIS til andre	6

## 1. Innledning

Denne rutinen skal sikre at personopplysninger blir behandlet i samsvar med grunnleggende personvern hensyn, i henhold til krav i personopplysningsloven.

Rutinen omhandler også utlevering av alle opplysninger i BRIS, ikke bare personopplysninger.

Personopplysninger er opplysninger og vurderinger som kan knyttes til en enkeltperson. Det vil si at kun et fåtall av opplysningene i BRIS omfattes av denne rutinen. Hvilke opplysninger som er personopplysninger i BRIS er listet nedenfor.

Gjennom behandlingen av personopplysninger får DSB, brann- og redningsvesenene og 110-sentralene plikter som "behandlingsansvarlige" for personopplysninger i BRIS. "Behandlingsansvarlig" er den som bestemmer formålet med behandlingen av personopplysninger og hvilke midler som brukes, se utfyllende beskrivelse i personopplysningsloven § 1, jf. personvernforordningen artikkel 4 nr. 7.

"Behandling" av personopplysninger er enhver operasjon som gjøres med personopplysninger, enten automatisert eller ikke, innsamling, registrering, sammenstilling, lagring, bruk, utlevering m.m.<sup>1</sup>

## 2. Formålet med BRIS

Personopplysninger kan blant annet behandles dersom det foreligger hjemmel i lov. Brann- og eksplosjonsvernloven § 10 tredje ledd hjemler adgangen til å behandle personopplysninger innenfor formålet med BRIS.

Personopplysninger i BRIS skal kun behandles i henhold til formålet med BRIS, og heller ikke viderebehandles på en måte som er uforenlig med formålet.<sup>2</sup>

BRIS skal gi brann- og redningsvesenene i Norge et bedre grunnlag for å drive effektivt brannforebyggende arbeid, og for å utvikle egen virksomhet.  
BRIS skal gi lokale og nasjonale beslutningstakere nødvendig informasjon for videre utvikling av kommunenes brann- og redningstjenester i fremtiden.

Personopplysninger i BRIS om akutt forurensning videresendes til Kystverket. Kystverket er statlig forurensningsmyndighet hva gjelder akutt forurensning, og har ansvaret for å koordinere statlig, kommunal og privat beredskap i et nasjonalt beredskapssystem. Kystverket har etablert en beredskapsvaktordning for å ivareta beredskap mot akutt forurensning. Det finnes i tillegg en varslingsforskrift knyttet til akutt forurensning eller fare for akutt forurensning som beskriver varslingsrutinene. Denne sammen med varslingsinstruksen til brann- og redningsvesenet / 110-sentralene danner grunnlaget for varslingssystemet ved akutt forurensning. For å ivareta og kunne håndtere Kystverkets myndighetsområde på en god måte, er det nødvendig for Kystverket å kunne komme i rask kontakt med både varslingsperson og ansvarlig forurensere. Dette gjelder for eksempel dersom det er nødvendig med ytterligere informasjon om hendelse, utstedelse av pålegg for iverksettelse av

<sup>1</sup> Jf. personopplysningsloven § 1, jf. personvernforordningen artikkel 4 nr. 2.

<sup>2</sup> Jf. personopplysningsloven § 1, jf. personvernforordningen artikkel 5 nr. 1 bokstav b og artikkel 6 nr. 4.

tiltak og krav om refusjon dersom staten iverksetter tiltak. Med andre ord er det nødvendig for Kystverket å komme i kontakt med de som har kunnskap om hendelsen, og de som har forårsaket hendelsen.

### 3. Personopplysninger i BRIS

Alle personopplysninger som til enhver tid behandles i BRIS, omfattes av personopplysningsloven og denne rutinen. Per 1. januar 2020 gjelder dette følgende personopplysninger:

#### *Brukerne av BRIS*

- Fødselsnummer
- Navn
- E-postadresse
- Mobilnummer

#### *Opplysninger fra 110-sentralene*

- Operatør-id (kun i rapporter)

#### *Oppdragsrapportering*

- Hendelsesstedets adresse fra oppdragshåndteringsverktøyet på 110-sentralene
- Innmelders navn og telefonnummer (fra Vision), er kun unntaksvis fylt ut (vises kun i 110-fullrapport)
- Ansvarlig forurensere (organisasjon, kontaktperson, e-post-adresse, telefonnummer)
- Varslingsperson for akutt forurensing (organisasjon, kontaktperson, e-post-adresse, telefonnummer)
- Navn på transportør ved uhell som involverer farlig gods (foretak, men kan være enkeltmannsforetak)
- Fra matrikkelen
  - Bygningens bygningsnummer
  - Bruksenhetsnummer
  - Navn på eier av bygget
- Fra Brønnøysundregisteret
  - Navn på virksomheten det startet å brenne i (kan knyttes til enkeltperson hvis navn på selskapet er knyttet til navn på person)
  - Bedriftsnummer på virksomheten det startet å brenne i

#### *Formålet med behandlingen av personopplysningene:*

- om brukerne i BRIS og opplysninger fra 110-sentralene er å ivareta hensynet til konfidensialitet og datakvalitet.
- om hendelsesstedets adresse, matrikkel- og Brønnøysundregisteropplysninger er å bidra til utførelsen av brannforebyggende arbeid og beredskapsarbeid på lokalt nivå.
- om forurensning er at Kystverket skal kunne ivareta og håndtere Kystverkets myndighetsområde på en god måte, og det er da nødvendig for dem å kunne komme i rask kontakt med både varslingsperson og ansvarlig forurensere.
- om navn på transportør ved farlig gods uhell er at DSB skal kunne ivareta og håndtere dette myndighetsområde.

### 4. Roller

DSB og brann- og redningsvesenet er begge behandlingsansvarlige<sup>3</sup> for personopplysninger i BRIS. De behandlingsansvarlige er ansvarlige for at personopplysningsloven følges.

---

<sup>3</sup> Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger og hvilke midler som brukes, se utfyllende beskrivelse i personopplysningsloven § 1, jf. personvernforordningen artikkel 4 nr. 7.

DSB, brann- og redningsvesenet og 110-sentralen behandler flere av de samme opplysningene på ulike måter og nivåer. Noen plikter som behandlingsansvarlig er felles, mens noen plikter er forskjellige som følge av ulike roller i BRIS. Rollefordelingen under skal bidra til en tydeliggjøring av ansvar.

### Brann- og redningsvesenene

- Registrerer informasjon om oppdraget
- Godkjenner oppdraget
- Sammenstillter og analyserer informasjon om egne oppdrag innenfor formålet til BRIS
- Registrerer og gir tilgang til brukere i eget brann- og redningsvesen og andre brann- og redningsvesen dersom dette er avtalt.

### 110-sentralene

- Registrerer informasjon om oppdraget i 110-sentralens oppdragshåndteringsverktøy
- Sammenstillter og analyserer informasjon om egne oppdrag (informasjon fra 110-sentralen om alle oppdrag i eget distrikt) innenfor formålet med BRIS
- Kan ha roller som lokal administrator eller "brukerstøtte" for brann- og redningsvesen i eget distrikt, hvis dette er avtalt lokalt.

### DSB

- Registrerer og gir tilgang til lokale administratorer av løsningen
- Vedlikeholder spørreskjema og den tekniske løsningen
- Lagrer data
- Ansvarlig for "teknisk sikkerhet"
- Brukerstøtte
- Sammenstillter og analyserer informasjon om alle oppdrag innenfor formålet med BRIS.

## 5. Rutiner for informasjonssikkerhet for personopplysninger

Det stilles krav om tilfredsstillende personopplysningssikkerhet i personopplysningsloven §1, jf. personvernforordningen artikkel 5 og 32:

Den behandlingsansvarlige og databehandleren<sup>4</sup> skal gjennom egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene ved behandling av personopplysninger.

For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernemnda.

### 5.1 Krav til konfidensialitet

Konfidensialitet innebærer å sikre at personopplysninger bare er tilgjengelig for de som skal ha tilgang, dvs uvedkommende ikke skal få tilgang til dem. Konfidensialiteten i BRIS sikres på ulike måter:

- Rollene i BRIS styrer hvilke data den enkelte har tilgang til. Brann- og redningsvesenet har tilgang til informasjon om oppdrag fra 110-sentralen i eget ansvarsområde og oppdrag eget brann- og redningsvesen har vært utalarmert til. 110-sentralen har tilgang til informasjon om alle oppdrag i eget 110-distrikt. DSB har tilgang til all registrert informasjon om alle oppdrag.

<sup>4</sup> Databehandler er den som behandler personopplysninger på vegne av den behandlingsansvarlige, jf. personopplysningsloven § 1, jf. personvernforordningen artikkel 4 nr. 8.

- DSB oppretter og administrerer de lokale administratorene, som styrer roller og tilganger i eget brann- og redningsvesen.
- Det enkelte brann- og redningsvesen og 110-sentral er ansvarlig for at kun brukere ansatt i brann- og redningsvesenet/ 110-sentralen har tilgang til BRIS.
- Det er personlig brukernavn og valgt passord i BRIS. Det er egne krav til passord.
- Oppdrag i BRIS kan kun komme fra 110-sentralen, ikke opprettes manuelt i BRIS.

#### *Krav til konfidensialitet*

<b>DSB</b>	<b>Brann- og redningsvesenet/110</b>	<b>Den enkelte bruker (alle nivåer)</b>
Det skal årlig gjennomføres en gjennomgang for å sikre at kun ansatte i DSB har aktive roller i BRIS	Det skal årlig gjennomføres en gjennomgang for å sikre at kun ansatte i brann- og redningsvesenet har aktive roller i BRIS	Passord og brukernavn er personlig og skal ikke overdras andre
	Brukere som ikke lengre arbeider i brann- og redningsvesenet skal settes til inaktive	Skal ikke lagre eller overføre rapporter med personopplysninger slik at de kan bli tilgjengelige for uvedkommende
	Godkjenne databehandlere og ha kontroll med og system for overføring av informasjon fra BRIS til disse	Ikke bringe informasjon fra BRIS ut av virksomheten uten etter avtale med behandlingsansvarlig
		Er pålagt taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig. Taushetsplikten omfatter også annen informasjon med betydning for informasjonssikkerheten <sup>5</sup>

## 5.2 Krav til integritet

Integritet innebærer å sikre at personopplysninger ikke endres uautorisert eller utilsiktet. BRIS inneholder ulike mekanismer for å sikre at personopplysninger ikke endres uautorisert eller utilsiktet:

- Personlig pålogging
- Rolle som godkjenner internt i brann- og redningsvesenet, som skal stå for kvalitetssikring av data som registreres
- Logg som viser hvem som har endret opplysninger i BRIS

#### *Krav til integritet:*

<b>DSB</b>	<b>Brann- og redningsvesenet</b>	<b>Den enkelte bruker</b>
Skal ha tilfredsstillende rutiner/systemer for kontroll med at integriteten er ivaretatt	Skal ha på plass godkjennerne som kvalitetssikrer innlagte opplysninger.	Sørge for at riktige opplysninger registreres etter beste evne
		Ikke oppgi brukernavn eller passord til andre

## 5.3 Krav til tilgjengelighet

Prinsippet om tilgjengelighet innebærer at personopplysninger skal være tilgjengelig for det formålet de er tiltenkt. Hensynet til tilgjengelige personopplysninger er i BRIS ivaretatt på ulike måter:

- Driftsovervåking

<sup>5</sup> Jf. Forvaltningsloven § 13 og personopplysningsloven §1, jf. personvernforordningen artikkel 32.

- Serverredundans
- Brann- og redningsvesenet har tilgang til all informasjon om egne hendelser
- Support eller brukerstøtte ivaretas innenfor normal arbeidstid. Det er ikke krav til 24/7 oppetid av systemet.

### Krav til tilgjengelighet

DSB	Brann- og redningsvesenet/ 110	Den enkelte bruker
Legge til rette for at systemet til enhver tid oppfyller krav til oppetid <sup>6</sup>	Melde brudd på tilgjengelighet, altså at BRIS er nede.	Melde brudd på tilgjengelighet

## 6. Avviksmelding

Brudd på kravene til informasjonssikkerhet skal sendes som skriftlig avviksmelding til Datatilsynet via Altinn.no. DSB skal ha en kopi av avviksmeldingen via BRIS support. Krav til meldingens innhold og 72-timers regelen følger av personopplysningsloven § 1, jf. personvernforordningen artikkel 33.

Eksempler på hendelser som skal meldes:

- Felles hendelser for brudd på konfidensialitet, integritet og tilgjengelighet.
  - innbrudd i virksomhetens lokaler eller nettverk.
  - uvedkommendes bruk av brukerkonti.
  - angrep av virus eller andre ondsinnede program.
- Brudd på konfidensialitet (personopplysninger kommer på avveie).
  - tap av bærbart utstyr.
  - tap av lagringsmedium.
  - utilsiktet utlevering av ansattopplysninger via e-post.

Den behandlingsansvarlige skal dokumentere ethvert brudd på personopplysningssikkerheten, herunder de faktiske forhold rundt nevnte brudd, virkningene av det og hvilke tiltak som er truffet for å utbedre det. Denne dokumentasjonen gjør det mulig for Datatilsynet å kontrollere samsvar med artikkel 33.

## 7. Generelt om utlevering av opplysninger fra BRIS til andre

Både DSB, det enkelte brann- og redningsvesen og 110-sentral mottar henvendelser om utlevering av opplysninger fra BRIS, uavhengig av om det er personopplysninger eller ikke. Dette kan for eksempel være henvendelser om statistikk eller opplysninger om enkeltoppdrag. Her følger en overordnet oversikt over hvilke generelle krav som gjelder til både DSB, brann- og redningsvesenet og 110-sentralene når det gjelder utlevering av opplysninger til andre.

DSB, brann- og redningsvesenet, 110-sentral
Skal vurdere innsyn og utlevering av opplysninger i BRIS etter offentleglova, forvaltningsloven og annen

<sup>6</sup> BRIS skal være tilgjengelig 24 timer i døgnet, 7 dager i uken (24/7). Den gjennomsnittlige oppetiden skal være 95 % eller mer. Oppetiden regnes pr. måned (95 % innebærer max nedetid på 36 timer pr. mnd).

Web servicen for mottak av hendelser (BRT) skal være tilgjengelig 24 timer i døgnet, 7 dager i uken (24/7). Den gjennomsnittlige oppetiden skal være 93 % eller mer. Oppetiden regnes pr. Måned (93 % innebærer maks nedetid på 50 timer pr. mnd).

BRIS skal ikke være nede mer enn 4 timer sammenhengende.

relevant lovgivning. <sup>7</sup>
Hovedregelen etter offentleglova (offl.) er at det skal gis innsyn, jf. offl. § 3. Unntak fra innsyn krever at det er hjemmel for unntaket og at det er behov for å unnta innsyn i opplysningene.
Den registrerte (det vil si den som en personopplysning kan knyttes til) har rett til informasjon om behandlingen, jf. personopplysningsloven § 1, jf. artikkel 13 og 14.  Den registrerte har også rett til å få en bekreftelse på om personopplysninger om vedkommende behandles, og dersom dette er tilfellet har vedkommende krav på innsyn i personopplysningene og den opplyste informasjonen i personopplysningsloven § 1, jf. personvernforordningen artikkel 15.  Merk at også bostedsadressen til enkeltpersoner er en personopplysning.

Utlevering av data til databehandlere:

Et databehandleroppdrag forutsetter at formålet med oppdraget helt eller delvis går ut på å behandle personopplysninger på vegne av en annen, eksempelvis dersom eksterne skal bistå brann- og redningsvesenet med analyse. De eksterne vil da innta rollen som databehandler. Omfattende tilgang, for eksempel kontinuerlig fjerntilgang, vil også normalt medføre at det foreligger en databehandlerrelasjon. Se for øvrig personopplysningsloven §1, jf. personvernforordningen artikkel 32. Datatilsynet har veiledning på sine hjemmesider: <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/behandlingsansvarlig-og-databehandler/?id=11276>

---

<sup>7</sup> Lov 19. mai 2006 nr. 16 om rett til innsyn i dokument i offentlig verksemd (offentleglova), lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven).