RUTINE FOR INFORMASJONSSIKKERHET FOR PERSONOPPLYSNINGER I BRIS

Innhold

1. Innledning

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

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, jf. personopplysningsloven (pol.) § 2 nr. 4.

"Behandling" av personopplysninger inkluderer innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

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 brukes til senere formål som er uforenelig med dette formålet, uten at den registrerte samtykker[1]:

> 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 restverdiredning (RVR), videresendes Finans Norge. Formålet med å behandle disse opplysninger er at dette er brann- og redningsvesenets fakturagrunnlag for å få betalt for restverdiredning av Finans Norge.

Personopplysninger i BRIS om akutt forurensing, 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 brannvesenet / 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 forurenser. Dette gjelder for eksempel dersom det er nødvendig med ytterligere informasjon om hendelse, utstedelse av pålegg for iverksettelse av tiltak, krav om

[1] Jf. pol. § 11.

refusjon dersom staten iverksetter tiltak – med andre ord er det for Kystverket nødvendig 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 med forskrift og denne rutinen. Per 1. september 2016 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 forurenser (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

Restverdiredning (opplysninger sendes fra brannvesenet til Finans Norge)

- Navn på utrykningsleder
- Skadestedets adresse
- Navn, adresse og telefonnummer til forsikringstaker
- Kontaktperson i forsikringsselskap
- Navn fagleder RVR

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 til 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 forurenser.
- om navn på transportør ved farlig gods uhell er at DSB skal kunne ivareta og håndtere dette myndighetsområde.
- knyttet til restverdiredning er å sikre at fakturering til Finans Norge blir korrekt i forbindelse med avtalt berging av verdier.

4. Roller

DSB og brann- og redningsvesenet er begge behandlingsansvarlige[2] for personopplysninger i BRIS. De behandlingsansvarlige er ansvarlige for at personopplysningsloven og personopplysningsforskriften følges.

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
- Sammenstiller 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
- Sammenstiller 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 brannvesen i eget distrikt, hvis dette er avtalt lokalt.

DSB

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

5. Rutiner for informasjonssikkerhet for personopplysninger

Det fremkommer av personopplysningslovens §13 at det stilles krav om tilfredsstillende informasjonssikkerhet:

Den behandlingsansvarlige og databehandleren[3] skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet 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 Personvernnemnda.

[2] Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som brukes, jf. POL § 2 nr. 4.
[3] Databehandler er den som behandler personopplysninger på vegne av den behandlingsansvarlige, jf. POL § 2 nr. 5.

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 info om oppdrag fra 110-sentralen i eget ansvarsområde og oppdrag eget brannvesen har vært utalarmert til. 110 har tilgang til informasjon fra 110-sentralen om alle oppdrag i eget 110-distrikt. DSB har tilgang til all registrert informasjon om alle oppdrag.
- DSB oppretter og administrerer de lokale administratorene, som styrer roller og tilganger i eget brannvesen.
- 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

DSB	Brann- og redningsvesenet/110	Den enkelte bruker (alle nivåer)
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[4]

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:

DSB	Brann- og redningsvesenet	Den enkelte bruker
Skal ha tilfredsstillende rutiner/systemer for kontroll med at integriteten er ivaretatt	Skal ha på plass godkjennere som kvalitetssikrer innlagte opplysninger.	Sørge for at riktige opplysninger registreres etter beste evne

[4] Jf. Personopplysningsforskriften § 2-9.

		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
- 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[5]	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 DSB, via BRIS support.

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.

Resultatet fra avviksbehandlingen skal dokumenteres, jf personopplysningsforskriften § 2-6.

[5] 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% er max nedetid 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% er maks nedetid 50 timer pr. mnd). BRIS skal ikke være nede mer enn 4 timer sammenhengende.

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 offentlighetsloven, forvaltningsloven og annen relevant lovgivning.[6]
Hovedregelen etter offentlighetsloven (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.
Henvendelser fra den registrerte (det vil si den som en personopplysning kan knyttes til) har rett til informasjon om hvilke opplysninger om den registrerte som behandles og sikkerhetstiltakene ved behandlingen så langt innsyn ikke svekker sikkerheten, jf. pol § 18. Øvrige rettigheter står i bestemmelsen. Merk at også adresse er en personopplysning som kan knyttes til en person (den registrerte).

Utlevering av data til databehandlere:
En behandlingsansvarlig som lar andre få tilgang til personopplysninger, f.eks. en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i pol. § 13 og i denne instruksen/rutinen. Det skal da inngås en egen databehandleravtale.

Dette kan for eksempel være dersom brann- og redningsvesenet ønsker at eksterne skal bistå med analyse av data. De eksterne vil da innta rollen som databehandler.

[6] Lov 19. mai 2006 nr. 16 om rett til innsyn i dokument i offentleg verksemd (offentleglova), lov 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven).