Policy nummer: 5-000	**Policy for personvern**	Gyldig fra: xx.04.2024
Policyeier: Personvernombudet		Sist revidert: xx.04.2024
Godkjent av: Jernbanedirektøren		Versjonsnummer: 1

1. Formål

Formålet med policyen er å beskrive overordnende føringer og prinsipper, roller og ansvar, samt eierskap til oppgaver for å sikre at behandling av personopplysninger håndteres i tråd med de kravene som gjelder.

2. Gjelder for

Dette dokumentet gjelder for alle ansatte, men beskriver i særlig grad roller og ansvar til ledere i Jernbanedirektoratet.

3. Definisjoner

Begrep	Beskrivelse av begrep
Personvern	Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger.
Personopplysninger	Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»).
Særlige kategorier av personopplysninger	I personvernopplysningsloven er det definert en rekke kategorier av opplysninger som det skal mer til å kunne behandle enn andre opplysninger (Sensitive personopplysninger). Artikkel 9 og 10 i personvernforordningen.
Personvernprinsipper	Personvernforordningen fastsetter noen grunnleggende prinsipper som skal etterleves. Artikkel 5 i forordningen.
De registrerte	Den som personopplysningene omhandler.
Personvernombudet	Personvernombud er et uavhengig ombud og har som oppgave å bidra til at behandlingsansvarlige følger gjeldende krav til behandling av personopplysninger.
Behandlingsgrunnlag	All bruk av personopplysninger må ha et behandlingsgrunnlag (et rettslig grunnlag) for å være lov. Artikkel 6 i personvernforordningen.
Behandlingsaktivitet	Aktivitet som innbefatter behandling av personopplysninger.
Behandlingsprotokoll	En oversikt over behandlingsaktiviteter.
Behandlingsansvarlig	Den behandlingsansvarlige er den som bestemmer hvorfor og hvordan personopplysninger behandles. Jernbanedirektøren er overordnet behandlingsansvarlig.
Databehandler	Leverandør som behandler personopplysninger på vegne av direktoratet og hvor det er inngått databehandleravtale.
Databehandleravtale	Forholdet mellom en behandlingsansvarlig virksomhet og databehandleren skal være regulert i en databehandleravtale. Avtalen skal sikre at personopplysningene blir behandlet i samsvar med regelverket og setter en klar ramme for hvordan databehandleren kan behandle opplysninger.
Avvik	Brudd på personopplysningssikkerheten.
Brudd på personopplysningssikkerheten	Er et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til

	personopplysninger som er overført, lagret eller på annen måte behandlet. **Brudd på konfidensialitet**, det vil si at det har vært en utilsiktet eller ulovlig utlevering av, eller tilgang til, personopplysninger. **Brudd på integritet**, det vil si at det har vært en utilsiktet eller ulovlig endring av personopplysninger. **Brudd på tilgjengelighet**, det vil si der det har vært et utilsiktet eller ulovlig tap av tilgang til, eller sletting av personopplysninger.
DPIA	En vurdering av personvernkonsekvenser. Dersom det er sannsynlig at en planlagt behandling vil føre til høy risiko for de registrertes rettigheter og friheter skal den som er ansvarlig for behandlingen vurdere hvilke konsekvenser behandlingen har for personvernet. (DPIA = Data Protection Impact Assessment)

4. Føringer og prinsipper

a. Lover og regler

Personopplysningsloven er en norsk lov med formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven gjennomfører EUs personvernforordning i norsk rett. Forordningen er dermed en del av personopplysningsloven og gjelder som norsk lov.

b. Personvernprinsippene

Jernbanedirektoratet skal behandle personopplysninger slik at de grunnleggende prinsippene for behandling av personopplysninger etterleves. Prinsippene følger av personopplysningsloven (forordningens artikkel 5).

Personopplysninger skal:

a. Lovlighet, rettferdighet og gjennomsiktig

Det må finnes et rettslig grunnlag for den behandlingen en virksomhet ønsker å gjøre. Forordningens artikkel 6 regulerer i hvilke tilfeller det skal anses lovlig å behandle personopplysninger. Minst ett av vilkårene i denne bestemmelsen må være oppfylt for at behandlingen er tillatt. Dersom det behandles sensitive personopplysninger, må i tillegg minst ett av vilkårene i artikkel 9 være oppfylt.

b. Formålsbegrensning

Ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist. Alle formål skal være forklart på en måte som gjør at alle berørte har samme entydige forståelse av hva personopplysningene skal brukes til. At formålet skal være legitimt innebærer at det i tillegg til å ha et rettslig grunnlag også skal være i samsvar med øvrige etiske og rettslige samfunnsnormer.

c. Dataminimering

Prinsippet om dataminimering innebærer å begrense mengden personopplysninger som hentes inn og behandles til det som er nødvendig for å oppnå formålet.

Riktighet
Personopplysninger som behandles skal være korrekte. Opplysningene skal også oppdateres hvis det er nødvendig.

Lagringsbegrensning
Prinsippet om lagringsbegrensning innebærer at personopplysninger skal lagres slik at de slettes eller anonymiseres når de ikke lengre er nødvendige for formålet de ble innhentet for.

Integritet og konfidensialitet
Personopplysninger skal behandles slik at opplysningenes integritet og konfidensialitet beskyttes.

Ansvarlighet
Prinsippet om ansvarlighet understreker den behandlingsansvarliges ansvar for å opptre i samsvar med reglene for *behandling av personopplysninger*. Direktoratet må også kunne vise at den faktisk opptrer i samsvar med reglene, ved eksempelvis tilsyn.

c. Krav

Krav som følger av personopplysningsloven:

- Direktoratet skal ha et regelverk som sikrer etterlevelse av personvernet, og som følges i det daglige.
- Direktoratet skal føre en protokoll over alle behandlingsaktiviteter de har ansvar for.
- De registrertes rett til innsyn, sletting og retting skal ivaretas. Personvernerklæringen skal ivareta de registrertes rett til informasjon.
- Informasjonssikkerheten ved behandling av personopplysninger skal være tilfredsstillende.
- Risikovurderinger skal gjennomføres og oppdateres ved behov.
- Vurdering av personvernkonsekvenser (DPIA) skal gjennomføres og oppdateres ved behov.
- Direktoratet skal ta skal hensyn til personvern i alle utviklingsfaser av et system eller en løsning (innebygd personvern).
- Direktoratet skal inngå en databehandleravtale når underleverandør benyttes.
- Direktoratet skal ha et regime for å håndtere brudd på personopplysningssikkerheten.

5. Roller og ansvar

Ansvar og roller for å ivareta personvernet i direktoratet håndteres i all hovedsak i tråd med linjeprinsippet. Dvs. at ansvar og myndighet følger lederlinjen. I tillegg er enkelte avdelinger gitt et særskilt ansvar for ulike aktiviteter.

Overordnet sett betyr dette at lederlinjen er ansvarlig for at alle former for behandling av personopplysninger er i tråd med kravene som gjelder; fra å påse at innhenting er lovlig til at opplysningene faktisk slettes.

Vi utvikles mot en stadig mer datadrevet transportsektor, noe som blant annet innbefatter tettere tverrsektorielt samarbeid om data. Slike aktiviteter kan innbefatte deling og bruk av personopplysninger direkte eller indirekte. Disse aktivitetene omfattes av personvernlovgivningen på samme måte som øvrige aktiviteter og med samme ansvarslinje.

J**ernbanedirektøren** har det overordnede ansvaret for at personvernet i Jernbanedirektoratet håndteres i tråd med de krav og prinsipper som gjelder.

Jernbanedirektøren beslutter denne policyen.

Avdelingsdirektører er ansvarlig for å påse at personvernlovgivningen etterleves innenfor egen avdeling. Dette betyr blant annet at:

- Den enkelte avdelingsdirektør er overordnet ansvarlig for behandlingsaktivitetene innenfor eget område.
- Den enkelte avdelingsdirektør er overordnet ansvarlig for å håndtere avvik som oppstår innenfor eget område.
- Den enkelte avdelingsdirektør er ansvarlig for å gjennomføre DPIA innenfor eget område dersom krav til dette foreligger.

Organisasjonsdirektør er i tillegg ansvarlig for:

- at direktoratet har etablert og vedlikeholder system for informasjonssikkerhet, samt ansvarlig for å fasilitere risikovurderinger knyttet til personvern i tråd med de kravene som gjelder.
- at direktoratet har innebygd personvern (og personvern som standardinnstilling) i systemer som benyttes av direktoratet.
- å bistå ved inngåelse av databehandleravtale samt kvalitetssikre avtalens innhold. Tilsvarende gjelder ved behov for endringer i allerede inngåtte avtaler. Som en del av dette må det kvalitetssikres at overføring av personopplysninger ut av EØS skjer på et lovlig grunnlag.
- at direktoratet har etablert et system for å fange opp forordninger og andre lovpålagte krav som innføres og som vil ha betydning for direktoratets arbeid med personvern, samt ansvar for å gjøre kravene kjent.
- at direktoratet har etablert systemer og rutiner for innsyn, retting og sletting.
- å etablere samt vedlikeholde personvernerklæring (intern)

Kommunikasjonsdirektør er ansvarlig for:

- å etablere og vedlikeholde en oversikt over samtykkeerklæring til bildebruk
- å sikre at direktoratet sin bildebank er i henhold til personopplysningsloven
- å etablere samt vedlikeholde personvernerklæring (ekstern)

Seksjonssjefer er ansvarlige for å påse at personvernlovgivningen etterleves innenfor egen seksjon. Dette betyr blant annet:

- å påse at medarbeidere har tilstrekkelig kompetanse.
- å ivareta det operative ansvaret for behandlingsaktiviteter innenfor egen seksjon. Dette innebærer blant annet å kvalitetssikre at behandlingen som sådan er lovlig, dvs. at det foreligger behandlingsgrunnlag, at det foreligger et eksplisitt formål, at det er etablert nødvendige organisatoriske og tekniske tiltak mv., jfr. prosedyre for innmelding av behandlingsaktiviteter.
- å ivareta det operative ansvaret for innmelding og oppfølging av avvik som oppstår innenfor eget område, jfr. prosedyre for innmelding og oppfølging av brudd på personopplysningssikkerheten.
- å ivareta den praktiske oppfølgingen på vegne av avdelingsdirektør knyttet til å gjennomføre DPIA, jfr. prosedyre for å utrede personvernkonsekvenser.

Rektor for Norsk fagskole for lokomotivførere har et særlig ansvar for å ivareta krav til behandling av personopplysninger knyttet til studenter, opplæring og innleide personell (instruktører med videre).

Kontraktseier skal inngå databehandleravtale der leverandør behandler personopplysninger på vegne av direktoratet.

Kontraktseier eller den som er gitt et oppfølgingsansvar for kontrakten skal håndtere brudd som varsles av leverandør, jfr. prosedyre for innmelding og oppfølging av brudd på personopplysnings-sikkerheten.

Alle ansatte skal håndtere personopplysninger på en sikker og forsvarlig måte.

Personvernombud er et uavhengig ombud og har som oppgave å bidra til at behandlingsansvarlige følger gjeldende krav til behandling av personopplysninger. Personvernombudet skal involveres i spørsmål som gjelder vern av personopplysninger, jfr. Personvernombudets oppgaver.

6. Eierskap og implementering av policyen

Jernbanedirektøren har godkjent denne policyen. Personvernombudet er ansvarlig for utforming og implementering.

Policyen er gyldig fra tidspunktet den er godkjent av jernbanedirektøren.