Ruter

Reglement for behandling av Personopplysninger i Ruter

Reglementet gjelder for Ruter As (Ruter), heretter kalt behandlingsansvarlig. Innholdet i databasene eies av Ruter i sin helhet, mens eierskapet til databasene varierer, se vedlegg 1-10, samt 12.

Ved et eventuelt opphør av Ruters drift vil reglementet gjelde inntil videre for et annet selskap som i det vesentlige viderefører driften til Ruter

Reglementet er utarbeidet på grunnlag av Personopplysningsloven, og forskrifter i medhold av loven, se særlig Kap II og III. Reglementet er tilpasset de personopplysninger som lagrer i databaser og filer.

Reglementet er oppdatert…

Nærværende reglement er godkjent av Ruters ledelse ved Administrerende og Vise Administrerende Direktør og Prosesseier for støtte/ Prosesseier for utvikling og drift IT. Alle vedlegg må godkjennes av de nevnte personer.

Oslo den 4/5 - 2009

Bernt Reitan Jensen
Administrerende Direktør

Runar Hannevold
Vise Administrerende Direktør

Innhold:

Vedlegg

1 Del I STYRENDE DOKUMENTASJON

1.1 Virksomhetens mål og policy i forhold til personopplysningsloven (pol).

Det overordnede mål med personopplysningsloven er angitt i lovens § 1 som er sitert under:

§ 1. Lovens formål
Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger.
Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.

Det er opprettet rutiner for å sikre at kravene i personopplysningsloven til enhver tid overholdes, se DEL II og III. Alle ansatte i Ruter skal gjøres kjent med rutinene for behandling av personopplysninger, og skal ha tilgang til dokumentasjonen for intern kontroll av systemet. Dokumentasjonen skal også være tilgjengelige for Datatilsynet og Personvernnemnda ved en eventuell kontroll.

1.2 Forholdet til personopplysningsloven (pol) § 11

Ruter legger stor vekt på at behandlingen av personopplysninger tilfredsstiller lovens krav, særlig med henblikk på dens § 11 som vektlegger at personopplysninger skal behandles i forhold til saklige behov og konkret definerte formål. Ordlyden i § 11 fremkommer under:

§ 11 Grunnkrav til behandling av personopplysninger

Den behandlingsansvarlige skal sørge for at personopplysningene som behandles

- ***a) bare behandles når dette er tillatt etter § 8 og § 9,***
- *b) bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet,*
- *c) ikke brukes senere til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker,*
- *d) er tilstrekkelige og relevante for formålet med behandlingen, og*
- *e) er korrekte og oppdatert, og ikke lagres lenger enn det som nødvendig ut fra formålet med behandlingen, jf. §§ 27 og 28.*

Senere behandling av personopplysningene for historiske, statistiske eller vitenskapelige formål anses ikke uforenlig med de opprinnelige formålene med innsamlingen av opplysningene, jf første ledd bokstav c, dersom samfunnets interesse i at behandlingen finner sted, klart overstiger ulempene den kan medføre for den enkelte.

1.3 Ansvar

Det formelle ansvaret for behandlingen av personopplysninger påhviler Ruter As ved administrerende direktør.

1.4 Plikter for bedriften etter personopplysningsloven

Personopplysningsloven pålegger Ruter en rekke plikter. Alminnelige plikter er:

- Å ha hjemmel/grunnlag for å behandle personopplysninger
- Å ha hjemmel/grunnlag for behandling av sensitive personopplysninger
- Tilfredsstille grunnkrav til behandling av personopplysninger
- Ivareta informasjonssikkerhet
- Ivareta intern kontroll
- Trygge databehandlerens rådighet over personopplysninger
- Ivareta frist for å svare på henvendelser om informasjon m.v.
- Gi korrekt rett til innsyn
- Oppfylle informasjonsplikt når det samles inn opplysninger
- Respektere rett til å reservere seg mot direkte markedsføring
- Retting av mangelfulle personopplysninger
- Ikke lagre unødvendige personopplysninger

Gjennom dokumentasjon og interne rutiner for bruk av personopplysninger skal kravene oppfylles, se nærmere del II og del III.

Det formelle ansvaret for behandlingen av personopplysninger påhviler daglig leder. Daglig leder kan delegere det praktiske arbeidet med dette. Arbeidet er delegert etter nærmere beskrivelse i sikkerhetsreglementets avsnitt 3.

1.5 Manuelt register

Dersom det er opprettet et manuelt register skal man, ved behandlingen av opplysninger, som ligger lagret i registeret, overholde samme sikkerhetskrav som elektroniske behandling så langt det passer.

1.6 Krav til informasjonssikkerheten, pol § 13, forskriftens kap2.

Etter personopplysningsloven § 13 og tilhørende forskrift kap. 2. er Ruter pliktige å sørge for tilstrekkelig tiltak for å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene. I den forbindelse er det utarbeidet følgende:

Sikkerhetsmål: Beskriver formålet med behandlingen av personopplysninger og overordnede føringer for bruk av informasjonsteknologi
Sikkerhetsstrategi: Beskriver valg og prioriteringer i sikkerhetsarbeidet
Sikkerhetstiltak: Beskrivelse av konkrete tiltak
Risikovurdering: Beskriver nivået for akseptabel risiko og sannsynligheten og konsekvenser av et sikkerhetsbrudd

Disse dokumentene finnes i dokumentasjonen under del II "informasjonssikkerhet".

Reglementet består av dette hoveddokument, og 14 vedlegg. Sikkerhetsreglementet har 4 hoveddeler. Denne delen omhandler den styrende informasjonen. Del II handler om informasjonssikkerhet. Del III tar for seg gjennomførende dokumentasjon, her beskrives bl.a. hvordan de ulike avdelingene og team skal behandle den informasjon de arbeider med. Del IV angir rutiner for kontroll og avviksbehandling.

All dokumentasjon må oppbevares sammen med reglementet. All rapportering om sikkerhetsbrudd må oppbevares som vedlegg 14 til dokumentet. Reglementet og den påkrevde dokumentasjon skal gjelde så lenge databasen i nåværende eller fremtidig form er i bruk. Utskrift fra hendelseslogg skal oppbevares av administrator. Dokumentasjon må oppbevares i minst tre år. Utskrift fra hendelsesliste skal oppbevares i 3 måneder.

Endringer i reglementet må godkjennes av Ledergruppen. Leder for Faggruppen for IKT og personvern skal rådspørres i slike spørsmål.

1.7 Utlevering, outsourcing

I utgangspunktet kan Ruter ikke utlevere opplysninger om kunder eller ansatte. Utlevering kan likevel skje dersom Ruter har hjemmel for det, eksempler på slik hjemmel angis i den enkelte instruksen. Generelt gjelder at Ruter må rette seg etter kjennelser som pålegger utlevering. Ved utlevering av personopplysninger med hjemmel i Offentleglova må det vurderes om innholdet er så personlig at de likevel må unntas. For å få bistand i slike vurderinger, kontaktes leder for Faggruppen for IKT og personvern, internadvokat eller arkivar.

All overføring per e-post skal krypteres dersom dataene er av sensitiv art.

Dersom Ruter benytter tredjepart til å behandle personopplysninger for seg, er ansvaret likevel Ruters. Personopplysningene kan derfor kun overføres til tredjepart så fremt det

foreligger en underskrevet databehandleravtale. Eksempel på databehandlere er Trafikanten, faktureringsselskap eller IKT-driftsselskap. Mal for databehandleravtale fås ved forespørsel av lederen for Faggruppen IKT sikkerhet og personvern. Virksomhet som får overført data fra Ruter kan ikke overføre dataene videre, uten Ruter utrykkelige godkjennelse Overføringen må skje på en hensiktsmessig måte slik at Ruters sikkerhetskrav mht. dataenes integritet, konfidensialitet, og tilgjengelighet overholdes.

2 Del II INFORMASJONSSIKKERHET

2.1 Formålet med personopplysningene

2.1.1 Generelt

Fellesnevneren for behandlingene av personopplysninger i Ruter er at de er nødvendig for å løse pålagte oppgaver om formidling av ulike transporttjenester i Oslo og Akershus, samt deler Buskerud og Østfold. I tilegg brukes databasene i forbindelse med den interne administrasjonen i bedriften.

Servere er når ikke annet er nevnt plassert hos IKT Administrator, som i avtale med behandlingsansvarlig forplikter seg til å følge sikkerhetsreglementet i utførelsen av de IKT tjenester som til enhver tid skal leveres.

I vedlegg 1 gis oversikt over databaser, systemer hvor personopplysninger blir behandlet med angivelse av systemeier, som er den som har det daglige eierskapet til den enkelte behandling av personopplysninger..

Informasjonssikkerheten ivaretas bl a ved at administrator ivaretar bruken av Ruter-nettet på følgende måte:

- Generelt overvåkes helsetilstanden på nettverk og servere. Dette innbærer stort sett sjekk på om komponenter er "oppe" eller "nede", om spesielle servicer kjører, om porter er tilgjengelige, om nettverk og servere er overbelastet, osv.
- Den tekniske overvåkningen brukes ikke slik at informasjon føres tilbake til enkeltpersoner. Dersom identifikasjon skal iverksettes, vil dette først bli gjort etter kjennelse fra retten eller annen lovhjemmel.

Innsyn i ansattes E-post, filer og loggfiler på internett, skal ikke behandles uten at det er konkret mistanke om bruk som er i strid med Ruters IKT håndbok eller norsk lov med forskrifter. De ansatte i Ruter skal få informasjon om en slik behandling, og har rett til bistand av fagforeningen. For nærmere prosedyre vises til IKT håndboken. Alt dette er beskrevet nærmere i dette reglementet.

Det skal gjennomføres risikovurderinger og sikkerhetsrevisjoner jevnlig. Dette er nærmere beskrevet i avsnitt 2.8 og 3.5.

Risikovurderingen skal vise trusselbildet mot Ruter og sannsynlighet for brudd på IKT sikkerheten og eventuelle konsekvenser av brudd.

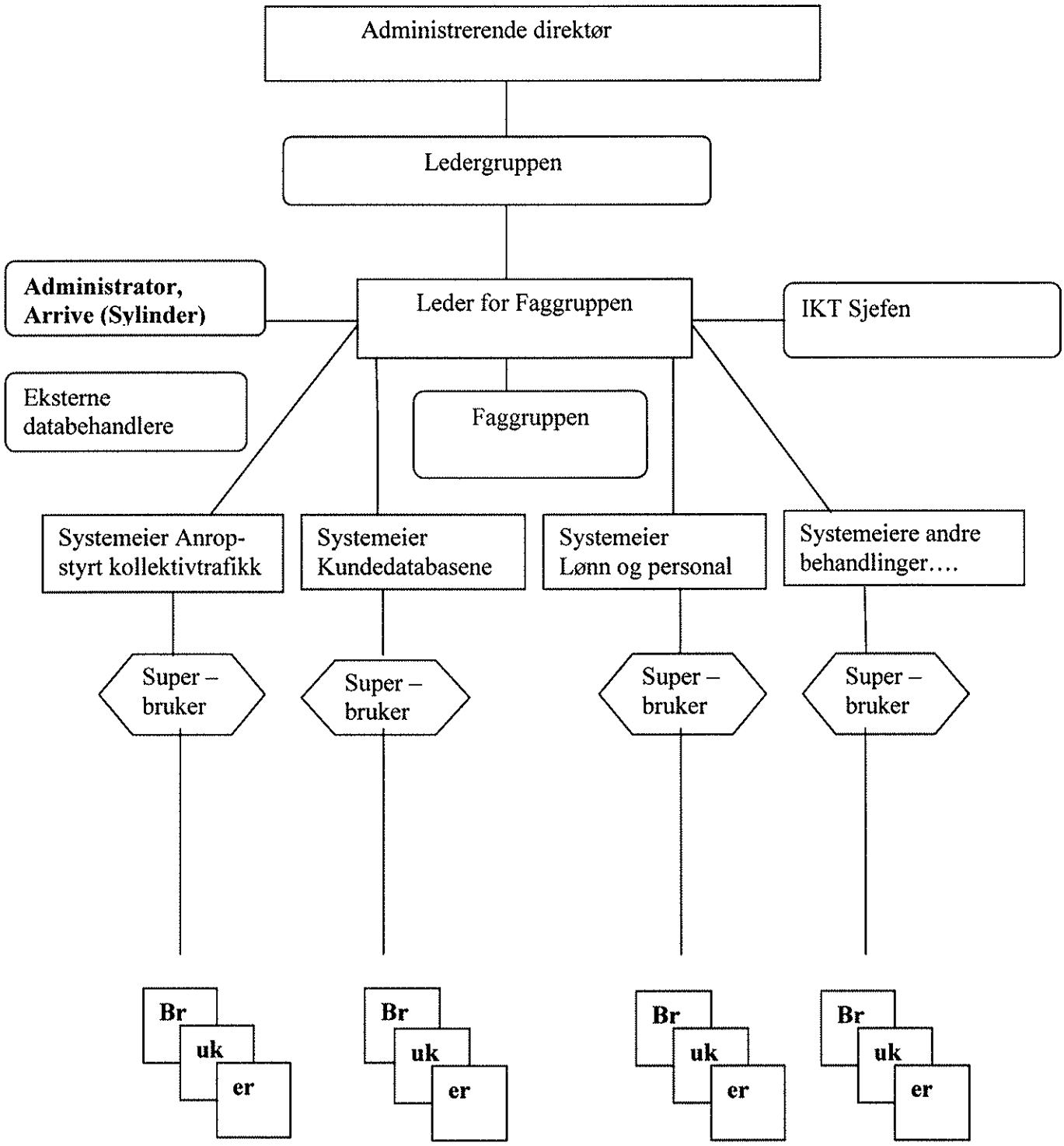
Sikkerhetsrevisjonene skal vise systemenes faktiske robusthet.

2.2 Personvernansvar i organisasjonen

Administrerende Direktør og Ledergruppen

Administrerende direktør har det øverste ansvar for at personopplysningsloven med tilhørende forskrifter blir fulgt. Administrerende direktør er assistert av en ledegruppe, som består av prosesseiere. Sammen skal de være en pådriver i sikkerhetsarbeidet. Ledergruppen vil det fatte nødvendige vedtak for å bedre sikkerheten i organisasjonen. Den faktiske oppfølgningen av sikkerhetsreglementet er delegert til Leder for faggruppen IKT-sikkerhet og personvern og den enkelte systemeier. Administrerende direktør rapporterer til styret i organisasjonen.

Figuren på neste side beskiver ansvars og oppgavefordelingen. Den nærmere presentasjonen av involverte ressurser følger på side 10.



Prosesseier kan delegere myndighet til prosessleder for drifte og utvikle IT.

IKT sjefen har bl a ansvar for innkjøp, drift, oppdatering, og kondemnering av alt IKT utstyr og software i Ruter. Han skal sørge for den nødvendige kontinuitetsplanlegging i organisasjonen, og har også ansvar for at nytt utstyr og programvare tilfredsstiller de krav til sikkerhet, som er utarbeidet i organisasjonen, og er kompatibelt med eksisterende system.

Leder for Faggruppen IKT sikkerhet og personvern har fått delegert det daglige ansvaret for IKT sikkerheten. Han må i den forbindelse samarbeide aktivt med IKT-sjefen for å synliggjøre svakheter i sikkerheten, sørge for at den årlige egenkontrollen blir gjennomført og besørge nødvendige eksterne sikkerhetsrevisjoner. Lederen for Faggruppen for IKT Sikkerhet og Personvern kan, i samarbeid med IKT-sjefen, autorisere endringer som er nødvendige av hensyn til sikkerheten og iverksette strakstiltak ved sikkerhetsbrudd. Større og grunnleggende endringer i systemene kan likevel ikke foretas uten godkjennelse ledergruppen. Han rapporter til Vise Adm. Direktør. Lederen for faggruppen fungerer også som personvernombud for organisasjonen, og skal i den forbindelse påse at bedriften har tilstrekkelig intern dokumentasjon og et nødvendig kontrollsystem, samt gi rådgivning og opplæring.

Faggruppen for IKT Sikkerhet og Personvern skal håndtere de praktiske problemstillingene rundt behandlingen av personopplysninger og virksomhetskritiske opplysninger i bedriften. Gruppen betegnes også "Faggruppen". Faggruppen skal konsulteres ved oppstart av en ny eller endret behandling av personopplysninger, eller før gjennomføring av markedsaktiviteter. Faggruppens medlemmer skal følge opp arbeidet med personvern i sine respektive avdelinger og team.

Administrator: Administrator, et godkjent IKT konsulent og driftsselskap, har ansvaret for drift og vedlikehold av hardware og software som brukes ved behandlingen av personopplysningene. Administrator skal sørge for at hardware og software til enhver tid er sikret i henhold til kravene i dette dokumentet, og de krav som er beskrevet i driftsavtalen med administrator. Administrator skal på rapportere om nødvendige oppgraderinger av de systemer som behandler personopplysninger i organisasjonen, og iverksette nødvendige strakstiltak for å bøte på feil eller sikkerhetsmangler. Tiltakene rapporteres til IKT sjefen og lederen for faggruppen.

Systemeier innehar det daglige eierskap til den enkelte behandling. Systemeier skal ha tilstrekkelig faglig kunnskap til systemet og er ansvarlig for at utstyr og software benyttes slik det er tiltenkt. Systemeier kan ta initiativ til anskaffelse av ny hardware eller software, samt endringer i eksisterende systemer, men må få godkjennelse fra IKT sjefen før eventuell anskaffelse og installasjon. Slike spørsmål skal om mulig og nødvendig forelegges Faggruppen. Dersom det oppstår feil eller mangler ved databasen kan systemeier i samarbeid IKT sjefen iverksette tiltak, som ikke truer den generelle sikkerhetsprofilen til organisasjonen. Dersom sikkerhets hensyn tilsier strakstiltak kan han unntaksvis gjøre det på egen hånd. Systemeier rapporterer årlig, og ved oppdagelse av sikkerhetsfeil, til lederen for faggruppen. Systemeier skal på oppdrag av ledelsen autorisere pålitelige brukere i databasen.

Eksterne behandlere og leverandører av hardware og software er underlagt samme krav som øvrige aktører som er nevnt i reglementet, se vedlegg 7.

Superbruker kan i tillegg til ordnær bruk av databasen gjøre mindre tilpasninger, som for eksempel å endre optimeringsparametere på systemet. **Bruker** kan ikke gjøre endringer på systemet. Brukeren skal rapportere til systemeier om feil eller mangler som truer sikkerheten til databasen.

2.3 Sikkerhetsmål

Formålet bak Ruters sikkerhetsreglementet er å beskytte personvernet til den enkelte ved behandling av personopplysninger. Med personvern menes bl a den enkeltes interesse av å bestemme over og kontrollere opplysninger om seg selv samt å sikre den registrertes rettigheter etter personopplysningsloven. Dessuten skal reglementet så langt det passer ivareta sikkerheten knyttet til virksomhetskritiske opplysninger.

Ruter har som en grunnlegende verdi at organisasjonen skal være pålitelig, ha kundefokus og være lærende.

Alle behandlinger av personopplysninger i Ruter må ha et gyldig behandlingsgrunnlag, se Personopplysningsloven §§ 11,8 og 9, se for øvrig nedenfor i avsnitt 5.

Behandlingsformål knyttet til hver behandling av personopplysninger finnes i vedlegg 1. Det skal kun benyttes opplysninger som er saklig begrunnet i Ruters virksomhet og som er relevante i forhold til det enkelte formål. Faggruppen for IKT sikkerhet og personvern skal konsulteres ved oppstart og endring av behandling av personopplysninger i Ruter.

Sikkerhetsmålene skal oppnås gjennom:

- Intern opplæring
- Interne prosedyrer
- Konfigurasjon av datasystemer og valg av tekniske løsninger

2.3.1 Integritetskrav

De innsamlede opplysninger skal ikke endres på en utilsiktet måte, eller av uvedkommende personer. Konfigurasjon i databaser som gjør det mulig å registrere nye opplysningstyper skal ikke gjøres uten det er tatt en personvernmessig vurdering av behovet for og formålet med slik endring.

2.3.2 Opplysningskvalitet

Opplysningene skal samles inn fra pålitelige og relevante kilder og skal være så korrekte og fullstendige som overhodet mulig. Opplysningene skal i tillegg behandles på en

grundig og forsvarlig måte, som sikrer at resultatet av behandlingen er tilnærmet helt nøyaktig.

2.3.3 Konfidensialitetskrav

Opplysningene skal kun være tilgjengelig for dem som har autorisert adgang. Uvedkommende skal ikke få elektronisk tilgang til opplysningene ved for eksempel "hacking" via internett. Uvedkommende skal heller ikke få tilgang til selve datautstyret.

2.3.4 Tilgjengelighetskrav

Tilgjengelighetskrav skal sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov, samt kundens innsynsrett.
Databasene må være innrettet slik at opplysningene er tilgjengelig i den sentrale driftstiden mellom kl 0700 og 16.00.

Krav til konfidensialitet og integritet skal gjennomgående prioriteres høyere enn kravet til tilgjengelighet. Ved behandling av sensitive data må det i alminnelighet stilles høye krav til systemsikkerhet, jf Personopplysningsforskriften.

2.4 Sikkerhetsstrategi

Ruter arbeider aktivt for å overholde de fastsatte sikkerhetsmål, bla ut fra følgende strategi.

2.5 Grunnlag for behandling av personopplysninger

Det er ikke adgang til å starte opp en ny type behandling, eller å utvide en behandling av personopplysninger i Ruter uten at behandlingen er vurdert av Ledergruppen og Faggruppen. Behandlingen må være tillatt etter Personopplysningsloven §§ 11, jfr. og 9.

Før oppstart av en behandling av personopplysninger skal man angi et gyldig behandlingsgrunnlag, samt utarbeide nærmere retningslinjer i form av en instruks for den aktuelle behandling.

Dersom behandlingen krever samtykke skal det innhentes skriftlig på forhånd. Samtykket må være avgitt på frivillig grunnlag, og den som skal registreres skal kunne gi sitt uttrykkelige samtykke på tilstrekkelig informasjon om behandlingen.

Det skal bla gis opplysninger om hvem som er behandlingsansvarlig, behandlingsgrunnlaget, og hva slags personopplysninger som skal registreres i den aktuelle databasen.

Dersom behandlingsgrunnlaget er "nødvendig for å ivareta en berettiget interesse", skal det på forhånd foretas en interesseavveining mellom bedriftens ønsker og hensynet til personvernet til den enkelte. Ved behandling av sensitive opplysninger som helseopplysninger og fagforeningsmedlemskap skal saken det alltid vurderes om behandlingen er konsesjonspliktig. Konsesjon må søkes i god tid før oppstart av behandlingen.

Alle saker om i gangsetting eller endring av behandling av personopplysninger (inkl markedsaktiviteter) skal forelegges Faggruppen for IKT Sikkerhet og personvern til vurdering.

Ved behandlinger som involverer de ansatte skal tillitsvalgte gis anledning til å uttale seg, jfr. Arbeidsmiljøloven § 9-1, de aktuelle fagforeninger skal også involveres. Alle behandlinger skal for øvrig skje i samsvar med reglene i Personopplysningsloven og Sikkerhetsreglementet.

Før man kan starte opp med en behandling av personopplysninger så skal det finnes en teknisk løsning som sikrer sletting av personopplysninger i samsvar med Personopplysningsloven § 28.

2.5.1 Integritet

Kun autoriserte brukere har tilgang til databasene. IKT-sjefen kan autorisere endringer i databasens konfigurasjon, som kan påvirke registreringen av personopplysningstyper i databasen, etter å ha tatt opp spørsmålet med Ledergruppen. Han skal på forhånd forelegge saken til vurdering av lederen av Faggruppen for IKT sikkerhet og personvern. Databasens konfigurasjon kan likevel bare endres dersom det er nødvendig for å oppfylle formålet med behandlingen.

.

Dersom det er nødvendig må ny eller utvidet konsesjon søkes, for øvrig må melding inngis til personvernombudet. Endringer i databasens konfigurasjon skal kunne dokumenteres.

2.5.2 Konfidensialitet

2.5.2.1 Fysisk Sikring

Kun autorisert personale hos administrator har tilgang til datautstyret. Ruters ledergruppe, den enkelte systemeier og Leder for faggruppen IKT-sikkerhet og personvern skal kunne få tilgang til datautstyret. Alt IT utstyr med servere og lignende er plassert hos administrator v/ firmaet Digiplex på Ulven, og kun autorisert personale hos administrator har tilgang til det.

2.5.2.2 Elektronisk sikring

Databasene er beskyttet av Ruters nettets generelle sikkerhetstiltak som for eksempel brannmur i forhold til internett, se beskrivelsen i vedlegg 8 Risikovurdering. Systemeier og administrator har ansvaret for at ingen uvedkommende personer får tilgang til brukernavn, passord og lisenskort og annet som er nødvendig for å få tilgang til databaser og filer som inneholder personopplysninger.

Brudd på sikkerheten, se avsnitt 3.5, skal kunne loggføres.

2.5.2.3 Leverandørers tilgang

Leverandør kan få tilgang å gjøre nødvendige endringer i basen enten ved oppmøte, se vedlegg 10, eller til en sikker linje til serveren for autoriserte brukere hos leverandøren. Ruters ledelse og administrator skal påse at leverandørens og eksterne behandleres omgang med de registrerte personopplysningene er begrenset til det nødvendige for arbeidet, se vedlegg 12.

2.5.3 Tilgjengelighet

Databasene må være innrettet slik at det ved langvarige avvik på tilgjengelighet skal kunne brukes alternative elektroniske eller manuelle behandlinger, noe som også er viktig for å sikre kundens innsynsrett etter Personopplysningsloven § 18.

2.6 Sletting

Det er kun tillatt å behandle personopplysninger så lenge behandlingsgrunnlaget tilsier at opplysningene blir behandlet.

Følgende lover kan likevel tilsi at opplysningene oppbevares lenger.

Bokføringsloven:
Primærbilag – 10 år
Sekundære regnskapsbilag – 3+ ca0,5 år (tiden til neste generalforsamling)

Arkivloven:
Gjelder bl a for enkeltvedtak og annet verneverdig materiale. Lagring på ubestemt tid.
Andre lover, f eks Foreldelsesloven med 3 år foreldelse av b la refusjonskrav.

2.7 Risikovurdering

2.7.1 Generelt

Systemeier skal påse at det blir gjennomført en risikovurdering for hver database, som skal vise trusselbildet mot Ruters behandlinger og sannsynligheten for sikkerhetsbrudd, samt eventuelle hvilke konsekvenser et slikt brudd vil kunne ha for Ruter og den som er registrert hos Ruter. Sikkerhetsbrudd er handlinger som står i strid med de rutinene som er beskrevet i eller i medhold av dette reglementet. I Personopplysningsforskriften § 2-6 omhandles sikkerhetsbrudd som avvik.

Vurderingen skal utføres av administrator, som rapporterer til Leder for faggruppen IKT-sikkerhet og personvern. Vurderingene skal foretas hvert annet år, eller ved vesentlige endringer i behandlingen av personopplyninger. Vurderingen skal sammenlikne den faktiske bruk og drift av databasene med de krav som sikkerhetsreglementet og lov med forskrifter stiller til behandlingen. Administrator skal beskrive det aktuelle risikonivå, som må være i samsvar til de krav til sikkerhet som er beskrevet i avsnitt 3 og 4, samt Personopplysningsloven med forskrifter.

2.7.2 Risikovurderingens innhold

Risikovurderingene relaterer seg til Ruters datautstyr, konfigurasjon, applikasjoner og sikkerhetstiltak på vurderingspunktet. Senere endringer i utstyr eller konfigurasjon som

fører til vesentlige endringer må vurderes på nytt. Den enkelte systemeier må rapportere om slike endringer til Leder for faggruppen IKT-sikkerhet og personvern, som har ansvar for at ny risikovurdering blir foretatt ved behov.

Vurderingen skal vise:

Risikofaktorer ved aktuell eller planlagt fremtidig bruk.
Faren for sikkerhetsbrudd.
Konsekvensene av sikkerhetsbrudd.

Risikonivået må stå i forhold til den type personopplysninger som behandles i databasen. Det er derfor akseptabelt med et noe høyere risikonivå for data som ikke er sensitive for kunden, da det vil ha mindre alvorlige konsekvenser for kunden om dataene ved en uforutsett feil skulle komme på avveie. Grunnleggende krav til sikkerhet må likevel alltid være ivaretatt. Ny vurdering skal foretas ved vesentlige endringer i datautstyret, databasen eller Ruter nettet.

Risikovurderinger skal foretas jevnlig, fortrinnsvis hvert år. Så langt er de utført av eksternt IKT-driftsselskap og har så langt vist akseptabelt risikonivå for alle de ovennevnte databaser, se vedlegg 8 for utførte risikovurderinger. Risikovurderinger skal bli oppbevart hos Ruter så lenge den aktuelle behandlingen foregår.

3 DEL III GJENNOMFØRENDE DOKUMENTASJON

3.1 Instrukser for bruk for den enkelte behandling

Det er utarbeidet instrukser for hver avdelings/team og deres behandling av personopplysninger. Alle forutsettes å sette seg inn i de instrukser som er relevant for sitt arbeid. Dersom det er bemerkninger til den enkelte instruks, skal disse tas med opp med leder for Faggruppen for IKT sikkerhet og personvern som kan ta saken videre.

3.1.1 Instruks for bruk av personopplysninger om kunder

Se vedlegg 2 for en fullstendig beskrivelse av bruk av personopplysninger om kunder

3.1.2 Instruks for bruk av personopplysninger ved anropstyrt kollektivtrafikk (Trapeze databasen)

Se vedlegg 3 for en fullstendig beskrivelse av instruks for bruk av personopplysninger ved anropstyrt kollektivtrafikk

3.1.3 Instruks bruk av personopplysninger ved utstedelse av skolebillett

Se vedlegg 4 for en fullstendig beskrivelse av instruks bruk av personopplysninger ved utstedelse av skolebillett.

3.1.4 Instruks for bruk av personopplysninger ved lønn og personaladministrasjon

Se vedlegg 5 for en fullstendig beskrivelse av instruks bruk av personopplysninger ved lønn og personaladministrasjon.

3.1.5 Instruks for bruk av sjåføropplysninger fra SIS

Se vedlegg 6 for en fullstendig beskrivelse av instruks bruk av personopplysninger fra SIS.

3.1.6 Generell instruks for behandling av personopplysninger, IKT Håndboken

Det er utarbeidet en IKT håndbok, hvor bla innsyn i ansattes e-post og filer behandles nærmere. Denne følger som vedlegg 7

3.2 Sikkerhetstiltak

3.2.1 Generelt

Sikkerhetstiltak kan iverksettes av IKT-sjefen, leder for Faggruppen Leder for faggruppen IKT-sikkerhet og personvern, og systemeier. Tiltakene skal gjennomføres i samarbeid med administrator. Tiltakene skal sikre at strategien gjennomføres, og skal bla iverksettes ved påviste svakheter i sikkerheten hos Ruter. Ved ekstern sikkerhetsrevisjon skal det eller de aktuelle systemene testet på nytt etter at sikkerhetstiltakene er iverksatt.

Sikkerhetstiltakene må generelt fungere uavhengig av medarbeidernes handlinger, for eksempel i form av applikasjonskontroll.

3.2.2 Iverksatte tiltak

Det er kun ekstern elektronisk adgang til server via en kryptert fast eller en ISDN/ADSL linje. Server er beskyttet av brannmur, se nærmere i vedlegg 8. De fleste databaser er plassert hos en sentral administrator, se vedlegg 8 Risikovurdering for en nærmere beskrivelse.

Det er gitt instruks for bruk av IKT- systemene. Det er også fastsatt en konkret ansvarsfordeling i organisasjonen, som bla skal sikre at sikkerhetsreglementet etterleves, og at nødvendige endringer blir iverksatt. Under angis konkrete sikkerhetstiltak.

Krav til sikkerhet er også spesifisert i SLA kravene i driftsavtalen mellom Arrive og Ruter Ruters IKT leverandør følger ISO 27002

3.2.2.1 Supplerende sikkerhetstiltak

Supplerende sikkerhetstiltak iverksettes dersom det viser seg å være nødvendig, for eksempel ved avvik, se del III avsnitt 3,5 med endringer i databasen/ IKT systemet. Tiltakene iverksettes i samsvar med ansvarsfordelingen i kapittel 3. Behovet av nye sikkerhets tiltak skal vurderes fortløpende av Systemeier og Leder for faggruppen IKT-sikkerhet og personvern. Sistnevnte tar opp saken med IKT-sjefen, eventuelt ledergruppen. Disse må ved godkjennelse av endringer eller nye behandlinger vurdere om Ruters sikkerhetskrav er i varetatt, samt at endringen ikke medfører svakheter i systemet som står i strid med Personopplysningsloven. Dokumentasjon vedlegges reglementet, og merkes som vedlegg 13.

3.2.2.2 Fysisk sikring

Servere, som databasene ligger lagret på er låst inn på egnet sted, som kun er tilgjengelig for autorisert personale hos administrator. Serverrommet er brannsikret, vannsikret og holder riktig temperatur, samt fuktnivå for oppbevaring av servere og lignende elektroniske lagringsmedier.

3.3 Kontroll og avviksbehandling

3.3.1 Egenkontroll

Det skal hvert år eller for øvrig etter behov undersøkes om de personopplysninger som er registrert i Ruters databaser for behandling av personopplysninger behandles i tråd med lovens krav. Administrerende direktør har delegert ansvaret til Leder for faggruppen IKT-sikkerhet og personvern i samarbeid med den enkelte Systemeier. Dersom systemeier ikke medvirker ved kontrollen skal spørsmålet tas opp IKT-sjefen. Dersom noen del av behandlingen utføres av en ekstern virksomhet skal driftsansvarlig i virksomheten rapportere til Ruter, eller eventuelt delta direkte ved kontrollen.

Omfanget av kontrollen:

- Kontrollen skal beskrive om den faktiske bruken og administrasjon av databasen, samsvarer med det angitte formål for behandlingen, samt Ruters sikkerhetsmål og strategi i reglementet.
- Dataens kvalitet i de enkelte databaser og filer skal vurderes.
- Det skal også undersøkes om kunden rent faktisk har fått den tjenesten som er formålet med den elektroniske behandlingen.
- Alle avvik med hensyn til tilgjengelighet (tilgangen til dataene) og konfidensialitet, samt integritet (riktige og fullstendige data) skal gjennomgås og beskrives. Tilsvarende gjelder endringer i behandlingen av personopplysning, og eventuelle iverksatte eller foreslåtte tiltak.

Leder for faggruppen IKT-sikkerhet og personvern har ansvar for at kontrollen utføres **innen 20. mai hvert år.** Resultatene av kontrollen rapporteres til Prosessleder for Støttefunksjoner, som ved behov gjennomgår den med Personvernansvarlig. Rapporten skal presenteres for Prosesseierteamet **innen 15. juni hvert år.**

3.3.2 Ledelsens kontroll

Ruters ledelse skal hvert år foreta en gjennomgåelse av sikkerhetsmål, strategi og tiltak, samt organisering for å kontrollere at disse er i samsvar med virksomhetens mål og offentlige sikkerhetskrav. Kontrollen skal omfatte:

a) Resultat fra egenkontrollen, eventuelt den eksterne sikkerhetsrevisjonen, spesielt med hensyn til om sikkerhetsmål og strategi overholdes.
b) Hvorvidt innsynsretten til registeret har vært sikret i praksis, og at kundene har fått den nødvendige informasjon om behandlinger som er utført i organisasjonen.
c) Gjennomgang av risikovurderingen etter del II kapittel 6.

d) Vurdering av endringer i offentlige sikkerhetskrav, og om eventuelle pålegg fra Datatilsynet er oppfyllet etter rapport fra leder for Faggruppen for IKT Sikkerhet og personvern. Kontrollen og pålegget skal dokumenteres, se vedlegg. Dersom behandlingen av personopplysninger er endret under det foregående år skal Ledergruppen kontrollere om det er gitt nødvendig melding til Personvernombudet eller om omfanget av gitte konsesjoner dekker behandlingen. Ny melding eller konsesjonssøknad skal kunne dokumenteres, se vedlegg 13.

e) Vurdering av vesentlige tiltak for å bedre sikkerheten eller for å avhjelpe avvik.

Ledelsen skal i henhold til konsesjonen for databasen for anropstyrt kollektivtrafikk bekrefte overfor datatilsynet at behandlingen skjer i overensstemmelse med søknaden og personopplysningsloven. Dokumentasjon vedlegges reglementet – se vedlegg 13.

3.4 Sikkerhetstester

Det skal gjennomføres jevnlige sikkerhetsrevisjoner, ved eksternt IKT-firma. Dette skal utføres av andre enn Ruters vanlige driftsleverandør. Se vedlegg 9 for gjennomførte sikkerhetstester.

Dersom det avdekkes punkter som må utbedres skal fremgangsmåten og ansvaret for utbedringen beskrives samt dokumenteres, se vedlegg 9. Avviksskjema kan benyttes.

3.5 Sikkerhetsbrudd (avvik)

Bruk av databasene som er i strid med reglementet, og de iverksatte sikkerhetstiltak, behandles som sikkerhetsbrudd eller avvik. Sikkerhetsbrudd kan for eksempel være at uautoriserte personell har fått tilgang til personopplysningene i databasen eller at en samarbeidspartner bruker dataene til et annet formål enn det som er beskrevet i del III avsnitt 2. Alle systembrukere er pliktig til å melde fra om avvikende bruk til systemeier.

Systemeier skal sørge for at administrator iverksetter strakstiltak for å gjenopprette den normale tilstand, og kan unntaksvis sørge for iverksettelse av slike tiltak på egen hånd. Samme rett har Leder for faggruppen IKT-sikkerhet og personvern. Systemeier skal vurdere konsekvensene av avviket, og om det er nødvendig å fastsette nye tiltak for å hindre nye sikkerhetsbrudd. Slike tiltak kan være å oppgradere teknologien, begrense antallet brukere, eller å legge databasen på en server som ikke er oppkoblet mot internett.

Systemeier skal rapportere avviket, strakstiltakene og foreslåtte tiltak til IKT-sjefen og til leder for Faggruppen for IKT Sikkerhet og personvern. Leder for Faggruppen for IKT Sikkerhet og personvern rapporterer deretter til ledelsen som skal beslutte ytterligere tiltak som anses nødvendige uten unødig opphold.

Datatilsynet skal informeres dersom avviket har ført til at konfidensielle opplysninger er blitt utlevert til uautoriserte personer.