DRAMMEN
KOMMUNE

SAKSUTREDNING

Saknr.	22/18	Saksbeh.	Ellen M. Bowitz
Jour.nr	18/4093	Fagavd.	Drammen Eiendom KF
Mappe		Avgj. av	Styret i Drammen Eiendom KF
Møtedato	23.04.2018		

SAK 22/18: NY PERSONVERNLOV

Innstilling til: Styret i Drammen Eiendom KF

Forslag til vedtak:

Styret tar saken til orientering.

Gjermund Riise Brekke
daglig leder

Ellen M. Bowitz
administrasjonsleder

Drammen Eiendom KF

Ilebergveien 21, 3011 Drammen
Pb 450 Brakerøya, 3002 Drammen
Tlf. 32 04 30 00 Fax 32 20 30 10
drammen.eiendom.kf@drmk.no
www.drammen.kommune.no
Org. nr. 876 820 722

Saksutredning

Formål med saken
Hensikten med saken er å orientere om ny personvernlov og hvilke tiltak som gjennomføres for å kunne oppfylle lovkravene.

Innledning

EU har vedtatt nye regler om personvern (GDPR-forordningen) som trår i kraft den 25. mai 2018.
De gir virksomheter nye plikter, og personene man behandler personopplysninger om, de registrerte, får nye rettigheter.

Regelverket stiller krav om utarbeidelse av nye rutiner tilpasset ny lov.
Det er virksomhetens ledelse som har ansvaret for å utforme de nye rutinene, og alle i organisasjonen må kjenne til og følge opp de nye reglene.

GDPR-forordningen innebærer også langt strengere krav for innhenting og behandling av persondata, og regelverket åpner dessuten for betydelige bøter ved brudd på disse pliktene.

Drammen Eiendom KF har opprettet en arbeidsgruppe bestående av administrasjonsleder og økonomi-controller og som samarbeider med D-Stab i forbindelse med kartlegging og gjennomføring av tiltak. Deltakere fra øvrige avdelinger i Drammen Eiendom KF vil knyttes inn i prosjektet ved behov.

Tiltak for å imøtekomme lovkrav er påbegynt, men ikke ferdigstilt.

Saksfremlegg:

Rådmannen er behandlingsansvarlig og har det formelle ansvaret for behandling av personopplysninger. Det daglige ansvaret er delegert til virksomhetslederne og daglig leder i KF.

Drammen kommune ved Digitaliseringssjefen er i egenskap av rollen som sikkerhetsansvarlig kontaktpunkt for myndighetene (Datatilsynet) og de ansatte når det gjelder spørsmål og saker knyttet til behandling av personopplysninger.

Denne er ansvarlig for at internkontroll blir håndhevet i det daglige og skal ta initiativ til rapportering og utbedring ved sikkerhetsavvik, samt bidra til at daglig behandling av personopplysninger tilfredsstiller kvalitetskravene.

Personvernombud for Drammen kommune og deres kommunale foretak ble ansatt 01.03.2018.

«Strategi og retningslinjer for informasjonssikkerhet» er Drammen kommunes overordnede styrende dokument for informasjonssikkerhet. Dokumentet er retningsgivende for alle tjenestebrukere, ansatte og samarbeidspartnere, i tillegg til alle interkommunale samarbeidsløsninger.

Retningslinjene skal benyttes i alle formål der personer behandler eller har tilgang til data og/eller informasjon som eies eller forvaltes av Drammen kommune. Retningslinjene omfatter også alle tilganger til systemer som finnes i Drammen kommunes nettverk, og kravene til sikkerhet gjelder for all informasjon enten den er elektronisk eller papirbasert.

FREMDRIFT OG MILEPÆLER

	Fag systemer	Berørte
Kartlegging og risikovurdering av data/systemer som berører personopplysninger.	• Agresso økonomi/HR lønn • ESA (elektronisk sak-arkiv) • Office-programmer • Facilit • Andre (?)	Alle avdelinger
Utarbeidelse av «personvernerklæring» som skal vedlegges nye kontrakter til privatpersoner. Vurdere behov for «samtykke-erklæring»	• Facilit	Boligtjenesten Markedsavdeling
Utarbeide rutiner for internkontroll, for bevisstgjøring av hva/hvor vi behandler personopplysninger.	• KS- System	Alle avdelinger
Risiko og sårbarhetsanalyse. ROS-analyse er et verktøy for å identifisere uønskede hendelser og risikoen for at disse skal inntreffe. I denne sammenhengen vil slike hendelser være knyttet til personopplysninger og informasjonssikkerhet. ROS skal gjennomgås årlig. Kun endringer noteres.	• Excel	Alle avdelinger. Årlig gjennomgang.
Opplæring av alle ansatte		
Kartlegginger og analyser oversendes D-Stab, personvernombud.		Rådmann
Fremdrift:	Start- april 2018	Slutt – juni 2018

Det er omfattende kartleggingsarbeidet som skal til for å etterfølge nytt lovverk, og i utgangspunktet skal DK bistå i veiledning til dette arbeide. DK har uttalt at de ikke anser å kunne være ferdig med sine oppgaver til 25. mai som er ikraftsettelses dato for loven.

Daglig leders vurdering:

Vi jobber frem mot en ferdigstilling av prosjektet i juni 2018, noe vi synes er ambisiøst – tatt i betraktning omfanget og usikkerhet i markedet på hvordan dette skal løses.

Det vil fortløpende bli vurdert ekstern hjelp inn i prosjektet.

Vedlegg:

1. Strategi og retningslinjer for informasjonssikkerhet, Drammen kommune.
2. Datatilsynets punktliste til ny forordning

Strategi og retningslinjer for informasjonssikkerhet i Drammen kommune

Versjon:	Endret av:	Dato:	Endring:
1.0	Frank A. Baklid	13.9.17	

Innholdsfortegnelse

Formål og bruksområde

Strategi og retningslinjer for informasjonssikkerhet er Drammen kommunes overordnede styrende dokument for informasjonssikkerhet. Dokumentet er retningsgivende for alle tjenestebrukere, ansatte og samarbeidspartnere, i tillegg til alle interkommunale samarbeidsløsninger.

Retningslinjene skal benyttes i alle formål der personer behandler eller har tilgang til data og/eller informasjon som eies eller forvaltes av Drammen kommune. Retningslinjene omfatter også alle tilganger til systemer som finnes i Drammen kommunes nettverk, og kravene til sikkerhet gjelder for all informasjon enten den er elektronisk eller papirbasert.

Informasjonssikkerhet omfatter beskyttelse mot avvik med hensyn til:

1. konfidensialitet; sikkerhet for at kun autoriserte personer har tilgang til sensitiv informasjon, og at den ikke avsløres til uvedkommende
2. integritet; sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter
3. tilgjengelighet; sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov
4. sporbarhet; alle systemer som er installert i sikret sone skal ha funksjonalitet som gjør det mulig å konstatere, i ettertid, hva som er gjort i et dataanlegg/ informasjonssystem, herunder hvem som har fått tilgang til opplysningene

Informasjonssikkerhet omfatter tiltak rettet mot sikring av personopplysninger, iht Lov om personopplysninger med forskrifter, virksomhetssensitiv informasjon, iht Lov om offentlig forvaltning, offentlighetslov og arkivlov, samt Drammen kommunes driftssituasjon, tjenesteproduksjon og verdier.

Avgrensninger

Dette dokumentet omhandler sikkerhet knyttet til informasjonshåndtering, og omfatter ikke følgende:

- Beredskap
- Fysisk sikring utover sikring av at sensitiv informasjon ikke kommer på avveie
- Objektsikring
- HMS

Strategi og målsetning

Visjon

Drammen kommune skal være blant de fremste til å sikre både tilgjengelighet og sikkerhet i offentlige, digitale tjenester.

Målsetning

Innbyggere og ansatte har tillit til at kommunen sikrer trygg forvaltning av informasjon gjennom tilgang på riktig og forståelig informasjon, og har råderett over egne personopplysninger.

Fokusområder

Fokuset vårt for å nå dette målet er sikker informasjonsforvaltning og tilgang og tillit til digitale tjenester. Dette er områder som er forankret i digitaliseringsstrategien til Drammen kommune og en del av vår helhetlige satsing på digitalisering, der kommunen fokuserer på hvordan teknologi kan forenkle tilgangen til informasjon og tjenester, og bidra til at ansatte jobber smartere.

Økt tilgang stiller også økte krav til å sikre at kun relevante personer har tilgang til informasjonen. Vi har også slått fast at innbyggernes behov skal være førende for utviklingen, og i Drammen kommune skal vi danne det beste grunnlaget for at innbyggerne skal ha tillit til at opplysningene deres forvaltes på en sikker måte. Dette oppnår vi ved å sørge for, og å dokumentere at vi har kontroll over behandlingene vi utfører og gjør dokumentasjonen tilgjengelig for dem det gjelder. Vi skal også jobbe målrettet med informasjon om hvordan personopplysninger behandles i kommunen.

Sikker informasjonsforvaltning

Sikker informasjonsforvaltning handler om å gjennomføre systematiske tiltak for å sikre at vi har kontroll over opplysningene vi behandler på vegne av innbyggerne og de ansatte i kommunen. Lov om behandling av personopplysninger og andre relevante regelverk skal ivaretas i tråd med Datatilsynets veileder for rådmenn i norske kommuner. Sikker informasjonsforvaltning handler om at det er en kultur og bevissthet rundt verdien av informasjon blant de ansatte, og at alle til enhver tid vet hvordan ansvaret for informasjonssikkerheten er organisert. Dette oppnås gjennom å gjøre organiseringen tydelig og kjent, drive kompetanseheving og holdningsarbeid, og ved å sørge for felles rollebeskrivelser og fokus på informasjonssikkerhet. Kompetanse om informasjonssikkerhet skal være en del av den grunnleggende digitale kompetansen som alle ansatte i Drammen kommune skal besitte.

I Drammen kommune har vi organisert arbeidet med informasjonssikkerhet rundt linjeorganisasjonen. Det betyr at ansvaret for å følge opp informasjonssikkerhet er lagt der behandlingen foregår og der det faglige ansvaret er plassert. Rådmannen er øverste behandlingsansvarlige for kommunen. Digitaliseringssjefen er delegert ansvar og myndighet for informasjonssikkerhet og skal i samarbeid med Drammensregionen-IKT, sørge for at retningslinjer for informasjonssikkerhet overholdes og at mål for informasjonssikkerhet nås. Arbeidet organiseres i tett samarbeid med ledere, systemeiere og systemansvarlige i Drammen kommune. I tillegg vil internkontrollarbeidet organiseres i samarbeid med kommunens internkontroller, og personvernvurderinger og kompetanseheving i samarbeid med personvernombudet.

Tilgang og tillit til digitale tjenester

Systematisk etterlevelse og oppfølgning av personvern og informasjonssikkerhet i kommunen er ikke bare lovpålagt, men danner grunnlaget for den tilliten man har og får av innbyggerne. At innbyggerne har tillit til de digitale tjenestene er en forutsetning for at de skal ta i bruk tjenestene, og følgelig for at kommunen kan realisere de gevinstene man ønsker å oppnå gjennom digitalisering.

I tillegg til forutsetningen for tillit som legges gjennom fokuset på oversikt og kontroll, vil Drammen kommune bygge tillit ved å sikre at innbyggerne har råderett over egne personopplysninger. Den nye personvernforordningen danner en viktig ramme for å sikre dette, og kommunen har allerede startet jobben med å inkorporere kravene som innføres i norsk lov fra mai 2018. Blant annet ansettes det et

personvernombud felles for de tre kommunene som skal danne ny storkommune fra 2020. For Drammen kommune er det viktig å rendyrke ombudsrollen for å sikre at de registrertes rettigheter blir ivaretatt.

Kommunen jobber strategisk for å sikre at data som den forvalter på vegne av innbyggerne skal være tilgjengelig for dem det gjelder. Dette gjør vi ved å stille krav til leverandørene i våre utviklingsprosjekter både når det kommer til deling og sikring av data. I tillegg vil vi prioritere å benytte oss av fellesløsninger for offentlig sektor der dette er tilgjengelig. Fellesløsninger skal forenkle flyten av data mellom offentlige etater.

Rammer

Aktuelt lovverk

- Personopplysningsloven med forskrift
- Arkivloven med forskrift
- Særlovgivning
- eForvaltningsforskriften

Ny personvernforordning

EUs forordning for personvern ((EU) 2016/679) blir norsk lov i 2018. Det betyr at vi får nye regler for personvern i Norge. Det nye regelverket gir virksomheter nye plikter, samtidig som at personene som får sine personopplysninger registrert får nye rettigheter.

Dagens risikobilde

Som Stortingsmelding 27 (2015-2016), digital Agenda påpeker, er de fleste kritiske infrastrukturer og samfunnsviktige funksjoner i dag digitalisert, noe som medfører nye sårbarheter i samfunnet. Digitalisering har også medført at flere samfunnsområder er gjensidig avhengig av hverandre og situasjonen er blitt mer kompleks.

I dag stiller vi større krav til tilgang og brukervennlighet, både som privatpersoner og ansatte, og vi forventer å kunne utføre jobben vår på flere arbeidsflater enn tidligere. Dette er i tråd med samfunnsutviklingen der vi tar i bruk stadig flere teknologiske hjelpemidler og endringstakten er høy. Økt tilgang på informasjon medfører også større risiko for at informasjon skal kunne havne på avveie. Utviklingen gjør det i tillegg stadig mer utfordrende å ha oversikt over hvordan systemer snakker med hverandre, og på den måten knytter arbeidsoppgaver i ulike virksomheter og forskjellig programvare sammen.

Menneskelig arbeidskraft i en organisasjon vil alltid utgjøre en risiko mot informasjonssikkerheten. Dette kan være egne ansatte eller innleid arbeidskraft. Utro tjenere er en åpenbar risiko mot konfidensialiteten til informasjonen en organisasjon forvalter. Det er imidlertid vel så høy risiko for at mangel på kompetanse og dermed feil bruk av informasjonssystemene skal utgjøre en trussel som at noen bevisst går inn for å lekke informasjon.

Tilgangen på teknologi som samler inn og bearbeider data øker stadig. Gevinstene med Big Data, Stordata, er mange. Prinsippene om formålsbestemthet som sier at data bare brukes til det formålet de er samlet inn for, og dataminimalisering, som tilsier at man ikke samler inn mer data enn man

trenger, og at dataene slettes etter bruk, blir tilsvarende viktige og mer utfordrende å forholde seg til. Med ny personvernforordning kommer krav om innebygget personvern. For å møte kravet må kommunen gjøre både tekniske og organisatoriske grep for å sikre at personopplysningsloven overholdes. Dette omfatter for eksempel avidentifisering (pseudonymisering) av opplysninger og at vi har personvern som standardinnstilling. Når personvern er standardinnstilling, behandler kommunen kun personopplysninger som er nødvendig for det konkrete forholdet som vurderes der og da.

En aktuell trussel mot informasjonssikkerheten utenfra er løsepengevirus og phising – fisking etter informasjon via for eksempel e-post. Ved å besvare svindel e-post og avsløre informasjon om for eksempel kredittkort, risikerer virksomheter og tappes for penger. Løsepengevirus spres også gjennom e-post. Ansatte lures til å trykke på linker som sprer skadelig programvare og krypterer innholdet i filer og bilder. For å få tilgang til innholdet igjen kreves løsepenger. Den eneste måten å forsvare seg mot slikt virus er å ha back-up av informasjonen. Ansatte i Drammen kommune har blitt utsatt for løsepengevirus og det er tidkrevende å rydde opp. Slike angrep blir stadig bedre utført og vanskeligere å gjennomskue. Det er derfor vanskelig å eliminere trusselen. Drammen kommune vil senke risikoen gjennom informasjonskampanjer til alle ansatte med eksempler og generelle råd til forhåndsregler.

Vi har også vært utsatt for angrep som gjør at internettlinjen overbelastes og all kontakt med internett blokkeres (DDoS-angrep). Dette innebærer at alle tjenester som er avhengige av internett slutter å fungere. Når vi gjør oss mer avhengig av internett for å få tilgang til vår egen informasjon, gjør vi oss samtidig mer sårbare for slike angrep. Dette er det viktig å kartlegge risikoen for, og ha gode tiltak mot når vi følger opp Digital Agendas oppfordring om alltid å vurdere skytjenester når vi etablerer nye eller oppgraderer eksisterende fagsystemer eller digitale tjenester.

En annen aktuell risiko er å ikke ha tilstrekkelig å kontroll over hvilke data vi som virksomhet håndterer, hva dataene betyr, hvilke begreper som er benyttet, hva de kan brukes til, hvilke prosesser de inngår i og hvem som kan bruke dem. Når en slik oversikt kan dokumenteres og er tilgjengelig, har vi ifølge Digital Agenda «orden i eget hus». Dette er grunnleggende krav som allerede følger av regelverk om internkontroll, informasjonssikkerhet, personvern og arkiv. Som behandlingsansvarlig gjelder selvsagt også kravene når vi setter ut tjenester.

Organisering

Ansvaret for informasjonssikkerhet

Ansvaret for informasjonssikkerheten følger linjeledelsen.

Rådmannen har det øverste administrative ansvaret for informasjonssikkerheten i kommunen. Rådmannen skal legge til rette for en hensiktsmessig sikkerhetsorganisering, gjennomføre årlig gjennomgang av sikkerhetsmål og -strategi, samt gjennomføre årlige sikkerhetsrevisjoner.

Den enkelte virksomhetsleder har et selvstendig tilsyns-, sikkerhets- og kontrollansvar for virksomhetens bruk av tekniske løsninger for informasjonshåndtering.

Hver systemeier gjennomfører risikoanalyser på sine respektive systemer for å kunne klassifisere informasjon ut fra hvor kritisk den er for virksomheten. Informasjonssikkerhetsansvarlig er ansvarlig for oppfølging i forbindelse med ledelsens gjennomgang.

Den enkelte ansatte har et selvstendig ansvar for at bruk av virksomhetens tekniske løsninger, utstyr og behandling av informasjon skjer i overenstemmelse med de til enhver tid gjeldende retningslinjer for informasjonssikkerhet.

Behandlingsansvaret

Rådmannen er behandlingsansvarlig og har det formelle ansvaret for behandling av personopplysninger. Det daglige ansvaret er delegert til virksomhetslederne.

Digitaliseringssjefen er i egenskap av rollen som sikkerhetsansvarlig kontaktpunkt for myndighetene (Datatilsynet) og de ansatte når det gjelder spørsmål og saker knyttet til behandling av personopplysninger.

Rollen som sikkerhetsansvarlig

Rådmannen har det overordnede og juridiske ansvaret for informasjonssikkerhet i kommunen, og er eier av retningslinjer for informasjonssikkerhet i Drammen kommune. Ansvaret for forvaltningen av retningslinjene er delegert til digitaliseringssjefen, i rollen som sikkerhetsansvarlig. Alle endringer i retningslinjene skal dokumenteres, og signeres av sikkerhetsansvarlig.

Sikkerhetsansvarlig er ansvarlig for at internkontrollen blir håndhevet i det daglige, og skal ta initiativ til rapportering og utbedring ved sikkerhetsavvik, samt bidra til at daglig behandling av personopplysninger tilfredsstiller kvalitetskravene. Sikkerhetsansvarlig skal støtte ledelsen og tilrettelegge for en enhetlig og helhetlig tilnærming i arbeidet med informasjonssikkerhet

Videre skal sikkerhetsansvarlig støtte virksomhetsledere i deres arbeid med informasjonssikkerhet og være en ressurs for øvrig i virksomhetens kontinuerlige internkontrollarbeid på informasjonssikkerhetsområdet.

Alle som behandler informasjon på vegne av kommunen er ansvarlig for sikkerheten i eget arbeid.

Ansvarsfordeling med D-IKT

D-IKT som virksomhet er å anse som databehandler for Drammen kommune og har særskilte plikter knyttet til den rollen. Disse pliktene reguleres i en egen tjenesteleveringsavtale mellom partene.

Medarbeidere i D-IKT er ansatt i Drammen kommune og omfattes også av retningslinjene i dette dokumentet. D-IKT skal gjennom etablerte rutiner sikre at IT-miljøet er kontinuerlig beskyttet og oppdatert. D-IKT er organisert med en egen sikkerhetsansvarlig i 100 prosent stilling. I tillegg har D-IKT et personvernombud som rapporterer til daglig leder.

Tjenesteavtalen mellom Drammen kommune og D-IKT stadfester driftsansvaret for de system der D-IKT er leverandør. Ansvaret som driftsleverandør innebærer blant annet:

- Bidra til avviksrapportering når det er nødvendig.
- Innhente godkjennelse fra systemeier før større tekniske endringer utføres.
- Etterleve gjeldende tekniske og administrative driftsrutiner.
- Å sørge for at vedtatte sikkerhetsmål, kriterier for akseptabel risiko og sikkerhetsstrategi blir fulgt opp ved investeringer i og drift av IT-løsninger
- Registrere og dokumentere all autorisert og forsøk på uautorisert bruk av IT-løsninger som inneholder personopplysninger
- Registrere og dokumentere alle sikkerhetshendelser/brudd som gjelder IT-løsninger
- Bistå virksomheter og utviklingsprosjekt ved risikovurderinger av IT-sikkerhet og iverksetting av IT-tekniske sikringstiltak
- Tilrettelegge for ledelsens gjennomgang

Gjennom eierstrategien for D-IKT er det regulert at D-IKT skal utarbeide nødvendige planer og gjennomføre tiltak for å sikre leveranse av gode, trygge og stabile IKT-tjenester. D-IKT har ansvaret for å overvåke kommunens IKT-systemer for å sikre unødig nedetid. I tillegg til dette overvåker Norsk Helsenetts organ, HelseCERT, Drammen kommunes systemer gjennom sensorer plassert hos D-IKT.

D-IKT rapporterer til sikkerhetsansvarlig og skal registrere avvik slik at kommunen til enhver tid har god kontroll og oversikt.

Databehandleransvaret

En databehandler er en virksomhet som behandler personopplysninger på vegne av kommunen (behandlingsansvarlig).

Det skal foreligge en databehandleravtale mellom behandlingsansvarlig og databehandler for alle systemer hvor det registreres personopplysninger. Det er systemeier som signerer databehandleravtalen på vegne av kommunen. Databehandlerens plikter følger av denne avtalen.

Den kommende forordningen vil inneholde selvstendige plikter for databehandlere. Disse pliktene kommer altså i tillegg til pliktene databehandlere har etter dagens databehandleravtaler.

Forordningen vil blant annet gi databehandlere plikt til å

- sørge for informasjonssikkerhet
- umiddelbart varsle den behandlingsansvarlige om avvik
- opprette rollen som personvernrådgiver på lik linje med behandlingsansvarlig

Databehandler har også plikt til å si fra til den behandlingsansvarlige dersom de mener at instruksjonene de får fra behandlingsansvarlige er i strid med forordningen eller personvernrett for

øvrig. Selv om databehandlere får nye plikter, er det viktig å understreke at den behandlingsansvarlige fremdeles har hovedansvaret for behandlingen av personopplysninger. Den behandlingsansvarlige kan bare velge en databehandler som gir tilstrekkelige garantier for at personvernreglene følges.

Brudd på disse pliktene kan føre til sanksjoner fra Datatilsynet. Dersom brudd på reglene medfører tap for den registrerte, vil både den behandlingsansvarlige og databehandleren være erstatningsansvarlige (solidaransvar).

Databehandleravtale

Hvis behandlingsansvarlig setter ut hele eller deler av behandlingen av personopplysninger til andre virksomheter (databehandlere) skal forholdet mellom virksomhetene reguleres i en databehandleravtale (personopplysningsloven § 13, jf. § 15). Avtalen kan enten være frittstående eller integrert i en annen avtale. Detaljgraden i databehandleravtalen vil kunne variere basert på hvilke opplysninger som behandles.

Den behandlingsansvarlige skal forsikre seg om at databehandler oppfyller kravene til tilfredsstillende informasjonssikkerhet etter loven (jf. personopplysningsloven § 15).

Drammen kommune benytter en virksomhetstilpasset variant av Datatilsynets mal som utgangspunkt for nye databehandleravtaler.

Forvaltning og oppfølging av databehandleravtalen ligger til systemeierrollen.

Underleverandører

En underleverandør behandler personopplysninger på vegne av en databehandler. Kommunen skal godkjenne alle underleverandører skriftlig, enten ved spesifikk godkjenning eller ved generell godkjenning som betyr at databehandler fortløpende informerer kommunen om hvilke underleverandører den planlegger å bruke. Kommunen kan på sin side motsette seg de enkelte underleverandørene.

Forholdet mellom databehandler og underleverandøren skal reguleres i en avtale mellom kommunen og databehandleren. Dersom underleverandøren ikke følger reglene, er det databehandleren som er ansvarlig for dette ovenfor kommunen.

Systemeier

Systemeier har det overordnede ansvaret for at kommunen forvalter og bruker systemet i henhold til lov og forskrift. Dette inkluderer hensynet til informasjonssikkerhet, og omfatter blant annet:

- Oppnevne en systemansvarlig for hver systemløsning
- Inngå (signere) kontrakter med leverandører og følge opp avtaler som er inngått
- Utarbeide tiltaksplaner for avvik
- Sende skriftlige avviksmeldinger til Datatilsynet
- Gjennomføre risiko- og sårbarhetsanalyser
    - jevnlig for alle eksisterende systemløsninger
    - ved endringer av eksisterende systemløsninger
    - for alle nyanskaffelser

- Gjennomføre sikkerhetsrevisjoner og rapportere resultatet fra disse, skriftlig, til sikkerhetsansvarlig

Utøvende Systemeier

I enkelte tilfeller kan det være hensiktsmessig at myndigheten til å utøve systemeierskapet delegeres videre i linjen. I slike tilfeller skal dette dokumenteres skriftlig.

Systemansvarlig

Systemansvarlig er fagansvarlig med delegert myndighet fra linjeleder.

Systemansvarlig har det utøvende ansvaret for å:

- implementere systemet
- gjøre seg kjent med den risikoen som eventuelt er identifisert
- implementere de risikoreduserende tiltakene som systemeier har besluttet.
- oppdatere rutiner for håndtering av avvik
- rapportere risiko for avvik
- rapportere faktiske avvik til systemeier og sikkerhetsansvarlig
- etablere krav til passord og rutiner for passordbytte
- etablere eller anskaffe også beredskapsrutiner for håndtering av driftsstans for driftssensitive systemer
- ha tilgang til hendelsesloggen i systemer der dette finnes, og besørge tilstrekkelig kravsetting om hendelseslogging ved nyanskaffelser
- opprette tilganger etter bestilling fra systemeier, fjerne unødvendige tilganger og føre etterprøvbar og skriftlig oversikt over hvilke tilganger som er gitt
- følge opp superbrukere

Virksomhetsleders ansvar

Virksomhetsleder har ansvaret for at alle medarbeidere har kunnskap om taushetsplikt, offentlighetslov og personvern.

Det er virksomhetsleders ansvar å være den som fremmer en sikkerhetskultur blant sine ansatte og skal gå foran som en god rollemodell. I praksis handler det om å:

- sørge for at vedtatte sikkerhetsmål, kriterier for akseptabel risiko og sikkerhetsstrategi blir fulgt opp og at kravene til risikohåndtering i egen virksomhet etterfølges
- øke bevisstheten om risiko knyttet til informasjonssystemer og nettverk
- informere om retningslinjer, rutiner, tiltak og prosedyrer for avvikshåndtering og sikre en oppfølging av sikkerhetsbrudd og avvik i egen virksomhet
- sørge for at sikringstiltak blir iverksatt dersom risikovurderingene viser at informasjonssikkerheten ikke er tilfredsstillende
- sørge for at alle brukere er kjent med de rutiner som til enhver tid gjelder for behandling av informasjonsverdier
- sørge for at sikkerhetsansvarlig får nødvendig bistand ved gjennomføring av sikkerhetsrevisjoner
- skape tillit til informasjonssystemer og nettverk og til måten de benyttes på

- sørge for at ressurser bevilges til planlegging, gjennomføring og oppfølging av pålagte oppgaver for virksomheten
- ha oversikt over hvilke informasjonsverdier og IT-løsninger enheten er ansvarlige for
- utøve ledelse som bidrar til en forståelse i egen virksomhet for sikkerhetsrelaterte problemer og å respektere etiske verdier
- bestille tilgang til og ha en oversikt over den enkelte ansattes tilganger
- sørge for at tilganger avsluttes dersom medarbeidere avslutter sitt arbeidsforhold til Drammen kommune
- gjennomføre en årlig sjekk av alle tilganger

Det stilles krav til at ansatte har nødvendig kompetanse til å benytte de fagsystem som funksjoner og roller krever for å utøve arbeidet innenfor de rammer virksomheten opererer i. Spørsmål om digital kompetanse skal være en del av medarbeidersamtalen.

Ansattes ansvar og rettigheter

Ansatte i Drammen kommune er pålagt taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig. Taushetsplikten skal også omfatte annen informasjon med betydning for informasjonssikkerheten (personopplysningsforskriften § 2-10). Alle ansatte i Drammen kommune som håndterer beskyttelsesverdig data skal undertegne taushetserklæring.

Ansatte i Drammen kommune har ikke lov til å oppsøke fortrolig informasjon de har tilgang til gjennom arbeidsplassen som ikke er nødvendig for at han eller hun skal utføre jobben sin. Det vil si at alle skal ha tjenstlig behov for bevisst å slå opp på en bestemt sak og kan ikke lese saker som ikke er offentlig eller relevant for de oppgavene en skal utføre.

Drammen kommune skal være en åpen og tilgjengelig kommune. Den ansatte plikter å følge de retningslinjene for dokumentføring som gjelder i sin sektor eller virksomhet, og til enhver tid bidra til at kommunen overholder aktuelt regelverk som offentlighetslov og personvernlov. Informasjon som er offentlig skal gjøres tilgjengelig via fagsystem og innsynsløsningen.

Mange ansatte bidrar til å spre kunnskap og informasjon om kommunens tjenester via sosiale medier, og kommunen skal være til stede på slike plattformer. Det er spesielt viktig at de som bruker sosiale medier i sitt arbeid forsikrer seg om det ikke spres fortrolig informasjon. Ansatte må også være bevisst at de som privatperson kan forbindes med Drammen kommune, og oppfordres til å ta dette i betraktning når en vurderer å kommentere, støtte eller poste innlegg på sosiale medier som kan knyttes til kommunen. Alle ansatte skal få en innføring i kommunens etikkplakat med etiske normer for ansatte, folkevalgte og styrerepresentanter i kommunale foretak i Drammen kommune. Etikkplakaten gjelder også som retningslinjer for aktivitet på nett og i håndtering av kommunens eiendom.

Det følger av kommunens arbeidsreglement at «kommunens utstyr m.v. må behandles med størst mulig varsomhet, slik at ødeleggelse og unødvendig slitasje ikke oppstår. Ved uforsiktig omgang med materiell kan arbeidstaker pålegges erstatningsansvar».

Alle som er ansatt i Drammen kommune som bruker elektroniske verktøy i utførelsen av arbeidsoppgavene sine plikter å gjøre seg kjent med verktøyene og gi beskjed dersom de har behov for mer opplæring enn det som har vært tilbudt. Arbeidsplassen skal legge til rette for at alle får den

opplæringen de har behov for. Evnen til å håndtere fagsystem er en grunnleggende kompetanse og en forutsetning for at kommunen skal kunne ivareta informasjonssikkerheten.

Kommunen er som arbeidsgiver pålagt å behandle en del opplysninger om ansatte og tidligere ansatte. Dette følger av arbeidsmiljøloven, regnskapsloven og likningsloven. Se Datatilsynets veileder om personvern på arbeidsplassen for mer informasjon om hvilken type opplysninger dette gjelder. Som med personopplysninger vi registrerer om innbyggere, finnes regler for hvor lenge opplysningene om de ansatte kan oppbevares og når de skal slettes. Som ansatt har man som hovedregel krav på å gjøre seg kjent med hva personalmappen inneholder, og skal informeres dersom det legges ny informasjon i mappa. Unntak framkommer av Personopplysningsloven § 23. Den ansatte kan henvende deg til nærmeste leder ved ønske om innsyn. Om ønskelig kan «mal for innsyn i personalmappe» fra Datatilsynet benyttes. Arbeidsgiver skal besvare henvendelsen innen 30 dager. Når en ansatt slutter skal arbeidsgiveren gjennomgå personalmappen og slette unødvendig informasjon.

Graden av loggføring av aktivitet i kommunens ulike datasystemer varierer fra system til system. Ved anskaffelse av nye systemer der sensitive opplysninger behandles vil dette være et krav. Loggføring av aktivitet i systemene er en måte å utføre internkontroller, og sikre tilstrekkelig informasjonssikkerhet. Loggen skal for eksempel benyttes til å kontrollere at ansatte ikke sjekker opplysninger de ikke har tjenstlig behov for, og for at det skal være etterprøvbart hvem som har utført hvilke oppgaver i fagsystemene.

På samme måte som i privatlivet, legger vi igjen mange personopplysninger i form av ulike digitale spor i arbeidslivet. Datatilsynet har utarbeidet en Veileder om kontroll og overvåkning i arbeidslivet. Personopplysninger omfatter mer enn det vi tenker over, og kan være opplysninger om atferdsmønstre, personlighet, meninger eller smak. Det kan være detaljopplysninger om når du kommer på jobb, hvor du beveger deg i løpet av en dag, og hva du søker etter på nettet. Det er krav om at virksomheter skal føre internkontroll på flere områder, for eksempel krav etter HMS-lovgivningen, helse- og omsorgslovgivningen, næringsmiddellovgivningen og lovgivningen om personvern og informasjonssikkerhet. Etter personopplysningsloven kan innsamling og bruk av personopplysninger bare skje til uttrykkelig angitte formål. Det skal altså være klart på forhånd hvorfor personopplysningene skal samles inn, og hva de videre kan brukes til. Innsamlingen kan ha flere formål, men kan ikke brukes til noe som ikke er forenlig med dette formålet senere. Dersom formålet endres må det gis informasjon om dette, og informasjonen som ble samlet inn før formålet ble endret kan ikke gjenbrukes uten at det gis samtykke til dette. Berørte arbeidstakere skal informeres om formålet med kontrolltiltak før det innføres, varigheten av det, praktiske konsekvenser og hvordan tiltaket vil bli gjennomført.

De vanligste kontrollrutinene på en arbeidsplass er tidsregistrering, adgangskontroll, innsyn i e-post eller kameraovervåkning. Med den teknologiske utviklingen kommer det imidlertid stadig flere muligheter til å følge med på de ansatte. Sporings- eller GPS-system i biler er et aktuelt område. Dette blir ofte tatt i bruk for å kunne styre hvor de ansatte skal kjøre (flåtekontroll) for å få mest mulig effektiv utnyttelse av tiden. Det er ikke tillat å bruke informasjon som er samlet inn for flåtekontroll for å kontrollere opp mot den ansattes timeregistrering, med mindre dette er et formål som er beskrevet før innsamlingen av disse opplysningene ble gjort og de ansatte er informert om det.

Etablering av sikkerhetsforum

For å sikre oppfølging av avvik og kompetanse- og informasjonsdeling vil Drammen kommune opprette et sikkerhetsforum bestående av sikkerhetsansvarlig i kommunen, rådgiver fra dSTAB og sikkerhetsansvarlig i D-IKT. I tillegg skal personvernombud, beredskapssjef og pressesjef være representert.

Forebyggende tiltak

Personvernrådgiver

Ett av kravene i den nye personvernforordningen som blir norsk lov i mai 2018, er at alle offentlige etater skal ha en personvernrådgiver. Rollen til en personvernrådgiver kan sammenlignes med dagens personvernombud. Rådgiveren kan være ansatt i kommunen eller tilknyttes via en profesjonell tredjepart. Det er et absolutt krav at rådgiveren skal være uavhengig. Det er kommunens ansvar å sørge for at personvernrådgiveren ikke mottar instruksjoner om hvordan han eller hun skal utføre arbeidet sitt. Personvernrådgiveren kan ikke avskjediges eller straffes for å utføre sine oppgaver.

Personvernrådgiveren skal involveres i alle saker hvor behandling av personopplysninger i virksomheten berøres. Personvernrådgiveren skal også samarbeide med, og være kontaktpunkt for, tilsynsmyndigheten, samt være kontaktpunkt for de registrerte. I kommunens tilfelle gjelder det både innbyggere og ansatte.

Personvernerklæring og samtykkeerklæring

Personvernerklæringer skal inneholde tydelig informasjon om hvilke behandlinger av personopplysninger som gjøres, hva som er formålet med behandlingen samt om behandlingsgrunnlaget er gitt ved lovhjemmel eller ved den registrertes samtykke.

Personvernerklæringer og samtykkeerklæringer skal presenteres for brukeren på en måte som klart skiller innholdet fra annet innhold og formuleres med et klart, lettfattelig språk.

Digital kompetanse og sikkerhetskultur

«Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og adferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsadferd» - et sitat hentet fra Nasjonal sikkerhetsmyndighets definisjon av sikkerhetskultur. Det handler om å øke bevisstheten om risiko knyttet til informasjonssystemer og nettverk, om policy, rutiner, tiltak og prosedyrer som er tilgjengelig for å ta hånd om disse risikoene, og om behovet for at de vedtas og iverksette. Når en sikkerhetskultur er etablert, vil det være en stor tillit blant alle ansatte til informasjonssystemer og nettverk og til måten de utvikles og benyttes på. Ansatte kan forstå sikkerhetsrelaterte problemer og kjenner til retningslinjer, rutiner og prosedyrer vedrørende sikkerhet i informasjonssystemer og nettverk.

En digital adferd kommer ikke av seg selv, men gjennom langsiktig satsning på å bevisstgjøre om risiko, informere om hva som er god sikkerhetsatferd, overføre kunnskap og motivere for en ønsket adferd, skapes en sikkerhetskultur. Kulturbygging fordrer kompetanse og forståelse i alle ledd, fra konsernnivå til ledere og ansatte.

Digital kompetanse skal bygges i alle ledd og sikkerhetsansvarlig er ansvarlig for at det tilrettelegges for opplæring. Konsernledelsen og virksomhetsledere er alle ansvarlig for at det settes av tilstrekkelig med tid til opplæring i organisasjon, og den enkelte virksomhetsleder er selv ansvarlig for kompetansebygging i sin virksomhet.

De registrertes rettigheter

Med ny personvernforordning presiseres rettighetene til personene hvis opplysninger er registrert i større grad enn det som har vært tilfelle med dagens lovverk. I forhold til norsk lovgivning blir ikke rettighetene vesentlig mer omfattende, men de blir tydeligere. Kravet til behandlingsansvarlig om å være tydelig blir også økt. Informasjon om hvilket formål personopplysninger er samlet inn for og hvordan de blir behandlet, samt hvilke rettigheter den registrerte har, skal være lettere tilgjengelig og enklere å forstå.

Som nå blir det krav om samtykke for å registrere personopplysninger for mange, men ikke alle tilfeller. Den som får sine personopplysninger registrert skal motta tydelig informasjon om retten til å trekke dette samtykket. Det skal være like enkelt å trekke samtykket som å gi det. Det kommer også økte krav til hva som kan defineres som et gyldig samtykke. Dersom det ikke er godt nok opplyst hva en samtykker til vil det ikke anses som gyldig. Personer under 16 år kan ikke gi samtykke; de må ha autorisasjon fra foresatte for å gi samtykke.

En annen presisering med stor konsekvens for de behandlingsansvarlige, er de registrertes rett til å bli glemt eller få slettet personopplysninger. Dette er en rettighet som eksisterer i dagens lovverk men som får mer fokus. Med ny forordning pålegges i tillegg den behandlingsansvarlige å varsle eventuelle behandlingsansvarlige som opplysningene er overført til om at det er kommet et ønske om å bli slettet. En ny rettighet for den registrerte blir retten til å be om å flytte personopplysninger fra en behandlingsansvarlig til en annen, omtalt som dataportabilitet. Denne retten gjelder for registreringer som er basert på samtykke, og ikke for behandlinger som er nødvendige for å gjennomføre oppgaver i samfunnets interesse eller under offentlig myndighetsutøvelse. Dette sammenlignes med retten til å beholde og flytte telefonnummeret du er gitt hos en teleoperatør til en annen.

Internkontroll

Å etablere internkontroll betyr at virksomheter som omfattes av loven må iverksette systematiske tiltak for å sørge for å følge loven og tilhørende regelverk. Internkontroll innenfor informasjonssikkerhet handler om styring med og kontroll på hvordan vi behandler personopplysninger. Dokumentasjon av de interne rutinene for hvordan denne kontrollen utøves og hvorfor, er en forutsetning for god internkontroll. Det er ledelsens ansvar å etablere et godt system for internkontroll, og dokumentasjonen av dette systemet skal være tilgjengelig for de ansatte i virksomheten og Datatilsynet. Drammen kommune skal følge Datatilsynets veileder for etablering av internkontrollsystem. I veilederen vises det til en tredeling av dokumentasjonsplikten i styrende dokumentasjon, gjennomførende dokumentasjon og kontrollerende dokumentasjon.

Den **styrende dokumentasjonen** er en beskrivelse av internkontrollsystemet som inneholder policy og målsetning, identifiserte krav og plikter, intern organisering og myndighet. «Strategi og retningslinjer for informasjonssikkerhet i Drammen kommune» er vår styrende dokumentasjon.

Prosedyrer og arbeidsinstrukser som kommunens «Roller og ansvarsbeskrivelse innenfor systemforvaltning», er eksempler på dokumentasjon som definerer hvem som har ansvaret for hva, og utgjør **styringssystemets gjennomførende dokumentasjon**. Systemdokumentasjon som kan dokumentere at systemer hvor personopplysninger lagres eller behandles er konfigurert på en slik måte at kommunens mål og retningslinjer for informasjonssikkerhet er implementert, er også dokumentasjon på hvordan vi gjennomfører informasjonssikkerhet eller ivaretar personvernet.

Denne typen dokumentasjonen skal verifisere at virksomhetens mål og policy for informasjonssikkerhet er implementert og er i samsvar med mål og retningslinjer.

Kontrollerende dokumentasjon skal på sin side bidra til at avvik fra mål og retningslinjer (styringsdokumentasjon) oppdages og rettes, og har til formål å verifisere at aktivitetene har foregått i samsvar med fastsatte prosedyrer og instrukser (gjennomførende dokumentasjon). Eksempler er rapporter, sjekklister, skjema for avviksrapportering og logg.

Fellessystemer og krav til elektronisk forvaltning i det offentlige

Dette er sentralt for arbeidet med personvern og informasjonssikkerhet fordi kommunen har eksplisitt ansvar for å ivareta dokumentenes autentisitet, integritet og tilgjengelighet. Informasjonssikkerhetsaspekter knyttes både til systemløsninger, rutiner, kontrollfunksjoner og personalets tilganger som brukes i dokumentbehandlingen.

Det offentliges plikt til å ha et arkiv er fastsatt i arkivlova. Formålet med arkivlova deles inn i to hoveddeler hvor bevaring står sentralt på den ene siden, og dokumentasjonsverdi av rettslig og forvaltningsmessig art på det andre. Av de retningslinjer som omtales over utledes følgende krav vedrørende arkivhåndtering:

I kommunen er arkivansvaret en del av det overordnede administrative ansvaret som er tillagt rådmannen. Dette innebærer at rådmannen skal:

- Legge forholdene til rette for at arkivarbeidet blir oppfylt,
- foreta nødvendig oppfølging og
- oppnevne en arkivansvarlig med ansvar for det daglige arkivarbeidet. For Drammen kommune er det byarkivaren som har arkivansvaret og arkivtjenesten utøves av Byarkivet.

Krav til dokumentasjon i sikkerhetsarbeidet

- Resultater fra gjennomgang av sikkerhetsledelsen skal dokumenteres (personopplysningsforskriften § 2-4).
- Resultater fra risikovurderinger skal dokumenteres (personopplysningsforskriften § 2-4).
- Resultater fra sikkerhetsrevisjoner skal dokumenteres (personopplysningsforskriften § 2-5).
- Resultater fra avviksbehandling skal dokumenteres (personopplysningsforskriften § 2-6).
- Sikkerhetstiltak skal dokumenteres (personopplysningsforskriften § 2-15).
- Rutiner for bruk av informasjonssystemer og annen informasjon med betydning for informasjonssikkerheten skal dokumenteres (personopplysningsforskriften § 2-16).
- Dokumentasjon skal lagres i minst fem - 5 - år fra det tidspunkt dokumentet ble erstattet med ny gjeldende utgave (personopplysningsforskriften § 2-16).
- Registrering av autorisert bruk av informasjonssystemer og av forsøk på uautorisert bruk, skal lagres i minst tre - 3 - måneder. Det samme gjelder registreringer av alle andre hendelser med betydning for informasjonssikkerheten (personopplysningsforskriften § 2-16).
- Autorisert bruk av informasjonssikkerhetssystemet skal registreres (personopplysningsforskriften § 2-8).
- Forsøk på uautorisert bruk av informasjonssystemet skal registreres (personopplysningsforskriften § 2-14).

For øvrig gjelder kommunens øvrige krav til informasjonsforvaltning og dokumenthåndtering.

Krav til dokumenthåndtering generelt

Kravene til dokumenthåndtering reguleres av flere lover med forskrifter:

- Lov om arkiv (arkivlova)
- Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)
- Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven)
- Lov om behandling av personopplysninger (personopplysningsloven)
- Forskrift om offentlige arkiv (arkivforskriften)
- Forskrift til offentleglova (offentlegforskrifta)

I tillegg kommer krav som er regulert i særlovgivning, herunder:

- Personopplysningsloven,
- helseregisterloven,
- helsepersonelloven,
- pasientrettighetsloven,
- arbeidsmiljøloven,
- regnskapsloven,
- pliktavleveringsloven og
- sikkerhetsloven.

Testing og evaluering av sikkerhet

Informasjonssikkerhet skal ivaretas gjennom den daglige driften i kommunen. En stor del av dette handler om å ha gode rutiner og sørge for at disse er kjent i organisasjonen. I tillegg til de oppgavene som allerede er nevnt gjøres tekniske tiltak for å sikre at ikke andre enn de som har autorisert tilgang får adgang til systemet. Dette kan handle om arkitektur, brannmurer, tilstrekkelig loggføring og oversikt over hvem som har tilgang til personopplysningene, penetrasjonstesting og om tiltak mot virus og skadelig programvare.

For å oppnå tilfredsstillende kontroll, må det i tillegg gjennomføres faste gjennomganger av sikkerheten. Sikkerhetsrevisjon er en komplett revisjon av kommunens datasikkerhet, og skal utføres på årlig basis for å verifisere at de sikkerhetstiltak som er besluttet etablert, faktisk er iverksatt og fungerer etter sin hensikt. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik. Resultatet av sikkerhetsrevisjoner danner grunnlaget for eventuelle endringer i sikkerhetsmål og –strategier, og inngår i prosedyre for ledelsens gjennomgang.

Kommunens ledelse har ansvar for å gjennomføre ledelsens gjennomgang. I denne forbindelse har sikkerhetsansvarlig også ansvaret for at sikkerhetsmål og sikkerhetsstrategi blir gjennomgått i den hensikt å sikre at de dekker kommunens behov.

Risikovurdering

Det skal føres oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger.

Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for, og konsekvenser av, sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.

Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko forbundet med behandling av personopplysninger.

Begreper

Anvendelighet: Anvendelig dokumentasjon kan gjenfinnes, hentes frem, presenteres og tolkes. I ettertid bør den kunne presenteres i direkte forbindelse med aktiviteten eller transaksjonen som ga opphav til den.

Avidentifiserte (pseudonymiserte) personopplysninger: Opplysninger der navn, fødselsnummer og andre direkte personentydige kjennetegn er fjernet og erstattet av en kode, slik at opplysningene ikke umiddelbart kan knyttes til en enkeltperson.

Autentisitet: Autentisitet betyr ekthet eller opprinnelighet. Autentisk dokumentasjon har vi når vi kan bevise at informasjonen er hva den hevder å være, at den er produsert eller sendt av den personen som hevder å ha produsert eller sendt den, og at den er produsert eller sendt på det påståtte tidspunktet.

Avvik: Bruk av informasjonssystemer som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik.

Behandlingsansvarlig: Den som bestemmer formålet ved behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. I kommunen er rådmannen behandlingsansvarlig.

Databehandler: Den som behandler personopplysninger på vegne av den behandlingsansvarlige.

Integritet: At dokumentasjon har integritet innebærer at den er fullstendig og uendret.

Personopplysninger: Opplysninger og vurderinger som kan knyttes til en eller flere enkeltpersoner.

Personvernforordning: Forordning om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger.

Personvernrådgiver: En personvernrådgiver (tidligere personvernombud) er en ressursperson som styrker virksomhetens kunnskap og kompetanse om personvern. Personvernrådgivere er under utførelse av sitt virke et uavhengig ombud hvis oppgave er å sikre at den behandlingsansvarlige i hele eller nærmere avgrensede deler av virksomheten følger personopplysningsloven med forskrift. Personvernrådgiveren skal også føre en oversikt over opplysningene som nevnt i Personopplysningsloven § 32.

Registrert: Personen som opplysningene kan knyttes til.

Tilgjengelighet: At informasjonen er tilgjengelig ved (rettmessig) behov.

Nye personvernregler fra 2018. Hva betyr det for din virksomhet?

Hva blir nytt?

1

Alle norske virksomheter får nye plikter
Alle virksomheter må sette seg inn i den nye lovgivningen og finne ut hvilke nye plikter som gjelder dem. Ledelsen må sørge for å få på plass rutiner for å overholde de nye pliktene. Alle ansatte må følge de nye rutinene når reglene trer i kraft.

2

Alle skal ha en forståelig personvernerklæring
Informasjon om hvordan din virksomhet behandler personopplysninger skal være lett tilgjengelig og skrevet på en forståelig måte. Det nye lovverket stiller strengere krav til informasjonens form og innhold enn dagens lovgivning. All informasjon som gis til barn, skal tilpasses barnas forståelsesnivå.

3

Alle skal vurdere risiko og personvernkonsekvenser
Dersom et tiltak utgjør en stor risiko for personvernet, må virksomheten også utrede hvilke personvernkonsekvenser det kan ha. Hvis utredningen viser at risikoen er stor og dere selv ikke kan redusere den, skal Datatilsynet involveres i forhåndsdrøftelser.

4

Alle skal bygge personvern inn i nye løsninger
De nye reglene stiller krav til at nye tiltak og systemer skal utarbeides på en mest mulig personvernvennlig måte. Dette kalles innebygd personvern. Den mest personvernvennlige innstillingen skal være standard i alle systemer.

5

Mange virksomheter må opprette personvernombud
Alle offentlige og mange private virksomheter skal opprette personvernombud. Et personvernombud er virksomhetens personvernekspert, og et bindeledd mellom ledelsen, de registrerte og Datatilsynet. Ombudet kan være en ansatt eller en profesjonell tredjepart.

6

Reglene gjelder også virksomheter utenfor Europa
Virksomheter som holder til utenfor Europa må også følge forordningen, dersom de tilbyr varer eller tjenester til borgere i et EU- eller EØS-land. Dette gjelder også om de ikke direkte tilbyr tjenester, men kartlegger adferden til europeiske borgere på nett. De som er etablert i flere land i Europa, skal bare trenge å snakke med personvernmyndighetene i det landet der de har sitt europeiske hovedkvarter.

7

Alle databehandlere får nye plikter
Databehandlere er virksomheter som behandler personopplysninger på oppdrag fra den ansvarlige virksomheten. Ofte er det snakk om leverandører av IT-tjenester. De nye reglene pålegger databehandlere å ha rutiner for innsamling og bruk av personopplysninger. Databehandlere skal også si ifra til oppdragsgiveren sin hvis de får instrukser som er i strid med loven. Oppdragsgiver skal også godkjenne databehandlerens underleverandører. Databehandlere kan også bli holdt økonomisk ansvarlig sammen med oppdragsgiver.

8

Alle bør samarbeide i egne nettverk og følge bransjenormer
De nye reglene oppmuntrer til sektorvis utforming av retningslinjer og bransjenormer. Om dere følger bransjenormer, vil dere ha de viktigste rutinene på plass. Datatilsynet skal godkjenne bransjenormene.

9

Alle får nye krav til avvikshåndtering
Reglene for håndtering av sikkerhetsbrudd blir strengere. Forordningen stiller krav til når det skal varsles, hva varselet skal inneholde og hvem som skal varsles. Kort sagt skal man si fra raskere og oftere enn man gjør i dag.

10

Alle må kunne oppfylle borgernes nye rettigheter
Den enkeltes rett til å kreve at hans eller hennes personopplysninger slettes blir styrket. Dette kalles «retten til å bli glemt». Norske og europeiske borgere vil blant annet kunne kreve å ta med seg personopplysningene sine fra en leverandør til en annen i et vanlig brukt filformat. Dette kalles «dataportabilitet». De kan også motsette seg profilering. Alle henvendelser fra borgere skal besvares innen en måned.

Hva bør dere gjøre nå?

1

Ha oversikt over hvilke personopplysninger dere behandler
Alle virksomheter som samler inn eller bruker personopplysninger skal ha oversikt over hvilke personopplysninger det er snakk om, hvor de kommer fra og hva som er det rettslige grunnlaget for behandlingen. Sørg for å ha en slik oversikt. Det er et krav som gjelder også etter dagens lov.

2

Sørg for å oppfylle dagens lovkrav
Overgangen til de nye reglene blir lettere om dere etterlever kravene i personopplysningsloven, som gjelder i Norge i dag. Har dere gode rutiner for internkontroll som fungerer etter hensikten og er kjent i organisasjonen, er det lettere å få oversikt over hva dere må endre.

3

Sett dere inn i det nye regelverket
Dere finner forordningsteksten på Datatilsynets nettsider. Der fyller vi også på med artikler om de nye reglene etter hvert som vi utarbeider dem.

4

Lag rutiner for å følge de nye reglene
Gå gjennom rutinene dere har for behandling av personopplysninger. Oppdater dem etter nytt regelverk der det trengs. Dokumenter de nye rutinene, og legg en plan for nødvendige endringer. Er systemene deres laget for å ivareta kravet til innebygd personvern, dataportabilitet og personvern som standardinnstilling? Klarer dere å fange opp og besvare henvendelser fra borgerne innen én måned? Endringer i systemer og rutiner tar tid. Begynn allerede nå!

datatilsynet.no/forordning