



Rett og slett - sletting av personopplysninger på arbeidsplassen

juridisk rådgiver Ole Martin Moe, Datatilsynet

14.09.2021

Hva skal vi snakke om?



- Kort om Datatilsynet
- Kort om personvernforordningen (GDPR)
- Sletting av personopplysninger på arbeidsplassen
- Innebygd personvern
- Hva ser Datatilsynet etter på tilsyn?
- Spørsmål og (forhåpentligvis) svar



Kort om Datatilsynet

- Opprettet 1980, lokalisert i Oslo
- Ca 70 medarbeidere
- Uavhengig forvaltningsorgan under KMD
- To roller – tilsynsorgan og ombud
- Fører tilsyn med personopplysningsloven og personvernforordningen (GDPR)
 - Helseregisterloven
 - Helseforskningsloven
 - Politiregisterloven
 - Lov om Schengen informasjonssystem
 - mv.
- Personvernnemnda er klageorgan for våre vedtak



Direktør Bjørn Erik Thon

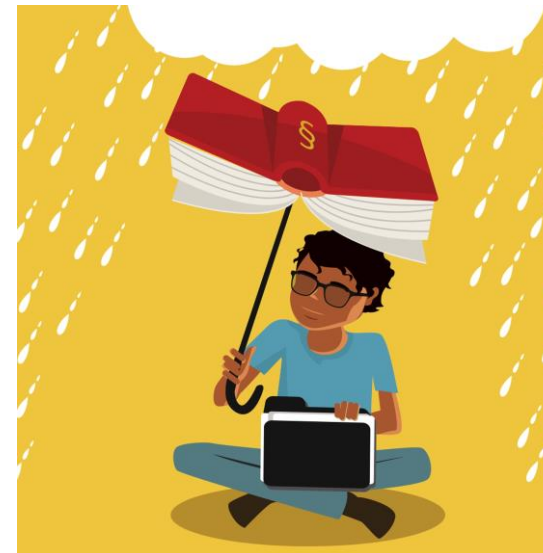


Kort om personvernforordningen (GDPR)

Personvernforordningen (GDPR)



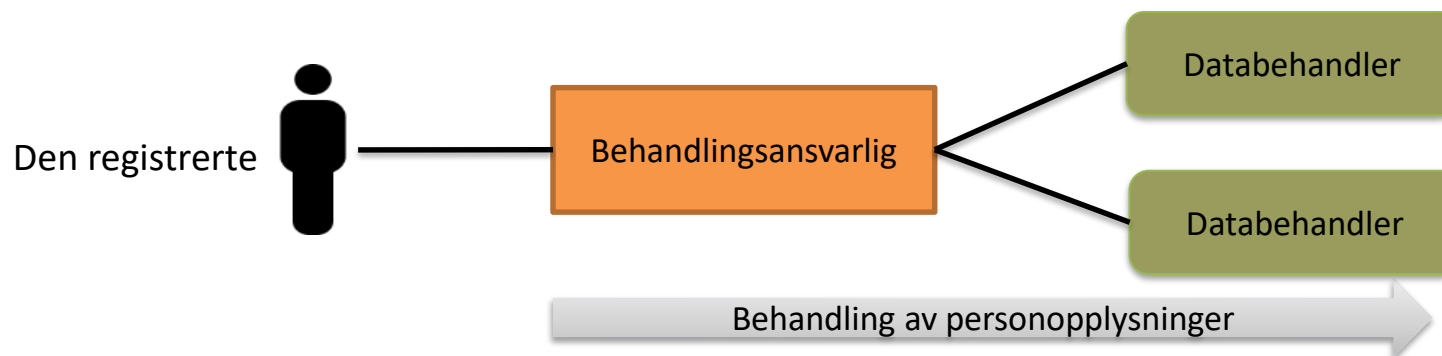
- Felleseuropeisk regelverk for behandling av personopplysninger
- Inkorporert i Norge gjennom personopplysningsloven (2018)
- Grunnleggende prinsipper for behandling av personopplysninger
- Mange rettigheter for «de registrerte» og mange plikter for de «behandlingsansvarlige»



Viktige begreper



- **Personopplysning:** Alle opplysninger og vurderinger som kan knyttes til en direkte eller indirekte identifiserbar person
- **Behandling (av personopplysninger):** Enhver prosessering (innsamling, organisering, lagring, endring, utlevering, sletting, etc.)
- **Den registrerte:** Enkeltperson som det behandles personopplysninger om
- **Behandlingsansvarlig:** Den som bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes
- **Databehandler:** En som behandler personopplysninger på vegne av, (og etter avtale med) den behandlingsansvarlige





Lovlighet, rettferdighet og åpenhet

Opplysningene skal behandles lovlig, rettferdig og åpen måte. Respekter de registrertes interesser og rimelige forventninger. Informasjon skal gis på en tilgjengelig og forståelig måte.

Formålsbegrensning

Opplysningene skal brukes for spesifikke, uttrykkelig angitte og berettigede formål. Opplysningene skal ikke brukes til andre uforenlige formål.

Dataminimering

Personopplysningene skal være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for.

Korrekte og oppdaterte

Opplysningene skal være korrekte og om nødvendig oppdaterte. Ukorrekte eller utdaterte personopplysninger skal rettes eller slettes.

Lagringsbegrensning

Det skal være rutiner som sikrer at det ikke er mulig å identifisere de registrerte lenger enn hva som er nødvendig for de formål de er samlet inn for.

Integritet og konfidensialitet

Personopplysninger sikres mot uautorisert eller ulovlig tilgang og mot utilsiktet tap, ødeleggelse eller skade. Det skal brukes egnede tekniske og organisatoriske tiltak.

Ansvarlighet

Den behandlingsansvarlige har ansvar for, og må kunne dokumentere, at personvernprinsippene blir etterlevd.



Sletting av personopplysninger på arbeidsplassen



- Personvernforordningen gjelder når arbeidsgiver behandler ansattes personopplysninger.
- Personopplysninger på arbeidsplassen kommer i mange former
 - Arbeidskontrakt, logger, bilder fra kameraovervåking, personalmappe, lønnsslipp, sykemeldinger ++
- Retten til sletting henger nært sammen med kravet til rettslig grunnlag.





- Når arbeidsgiver skal behandle personopplysninger må de ha:
 - Spesifikt og lovlig formål
 - F.eks. skatt og lønn, drive adgangskontroll, følge opp sykemeldinger, sikkerhetstiltak m.m.
 - Rettslig grunnlag (flere alternative, må finne det som passer formålet)
 - Rettslig forpliktelse (f.eks. skatt eller arkivplikt)
 - Nødvendig for å oppfylle avtale (f.eks. utbetaling av lønn)
 - Samtykke (obs: problematisk i arbeidsforhold)
 - Berettiget interesse (balansetest)
 - Sletting: hvor lenge arbeidsgiver kan behandle ansattes personopplysninger avhenger av formålet med behandlingen, og det rettslige grunnlaget

Retten (og plikten) til sletting



- Grunnleggende rettighet i personvernforordningen artikkel 17
 - Dataminimering og lagringsbegrensning
- Arbeidsgiver har ansvar for sletting av personopplysninger blant annet når:
 - «personopplysningene er ikke lenger nødvendige for formålet som de ble samlet inn eller behandlet for»
 - «den registrerte trekker tilbake samtykket som ligger til grunn for behandlingen...»
 - den registrerte protesterer mot behandlingen i henhold til artikkel 21 nr. 1, og det ikke finnes mer tungtveiende berettigede grunner til behandlingen, eller den registrerte protesterer mot behandlingen i henhold til artikkel 21 nr. 2
 - «personopplysningene er blitt behandlet ulovlig»
 - personopplysningene må slettes for å oppfylle en rettslig forpliktelse [...] som den behandlingsansvarlige er underlagt»
- Den registrerte kan be om sletting, men arbeidsgiver (behandlingsansvarlig) skal ha rutiner for å slette opplysninger på eget initiativ



Retten til å protestere



- De registrerte har rett til å protestere mot behandling av personopplysninger som har grunnlag i
 - Artikkel 6 nr. 1 bokstav e (oppgave i allmenhetens interesse)
 - Artikkel 6 nr. 1 bokstav f (berettiget interesse)
- Å protestere = å si at man ikke ønsker at arbeidsgiver behandler deres personopplysninger.
- Særlig aktuelt ved kontrolltiltak som kameraovervåking
- Hvis noen protesterer skal det enda mer til for at f.eks. kameraovervåking er lov.
 - Arbeidsgiver må lytte til den ansatte og forholdene de gjør gjeldende, og bevise at det finnes *ekstra tungtveiende grunner* for at kameraovervåkingen skal skje selv om en person har protestert. Hvis ikke arbeidsgiver kan bevise dette så må overvåkingen stoppe.





- Retten til sletting er ikke absolutt, og det kan oppstå behov for å lagre opplysninger lenger
- Et nytt formål kan forlenge lagringstiden, f.eks. ved tvist etter oppsigelse.
 - Obs: krav til forenlighet og nytt rettslig grunnlag.
- Unntak i art. 17 nr. 3 dersom det er nødvendig å lagre opplysninger videre for å:
 - «fastsette, gjøre gjeldende eller forsvare rettskrav»
 - oppfylle rettslig forpliktelse (f.eks. regnskapslovgivning)
 - oppfylle arkivplikt etter arkivlovens regler
 - m.m.
- Husk alltid lovlighet, dataminimering og nødvendighet; hvor mye opplysninger er det nødvendig å lagre videre og finn rettslig grunnlag. Dokumenter vurderingen.
- Personvernemnda: arbeidsgiver må påvise en *konkret og reell grunn* til fortsatt lagring. (PVN-2018-11 om sletting av innhold i personalmappe)



Retten (og plikten) til sletting forts.



- En grunnleggende forutsetning for compliance at arbeidsgiver har laget gode sletterutiner, og at sletting skjer automatisk der det er mulig.
- Bør også lages rutiner for regelmessig gjennomgang av lagrede opplysninger.





- Ansvarlighetsprinsippet
 - Arbeidsgiver må sikre og *påvise* at de etterlever personvernforordningen
 - Skriftlige rutiner for hvordan arbeidsgiver behandler personopplysninger, og dokumentasjon på vurderinger som er gjort
 - Rutiner sikrer forutsigbarhet for arbeidsgiver og arbeidstaker, og sikrer compliance
- Dataminimering
 - Aldri behandle flere opplysninger enn det som er nødvendig for å oppfylle formålet med behandlingen
- Lagringsbegrensning
 - Aldri lagre opplysninger lenger enn det som er nødvendig for oppfylle formålet med behandlingen.
 - Sletting skal vurderes fortløpende. Viktig med gode rutiner for sletting etter f.eks. avsluttet arbeidsforhold
- Integritet og konfidensialitet
 - Informasjonssikkerhet, tilgangsstyring m.m.





- Pålegg om sletting og overtredelsesgebyr (1 MNOK)
- Vegvesenet hadde et system der det ikke var mulig å slette opplysninger.
- Brudd på artikkel 17 (sletting) og artikkel 25 (innebygd personvern).

Aktuelle nyheter 2020

Varsel om overtredelsesgebyr til Statens vegvesen

Datatilsynet har varslet Statens vegvesen om pålegg og overtredelsesgebyr på fire millioner kroner. Saken gjelder manglende sletting av passeringsopplysninger i bomringen.

Statens vegvesen har ikke slettet passeringsopplysninger som brikkenummer, lokasjon og passeringstidspunkt i sin database. I det opprinnelige systemet for lagring av passeringer i bomringen, var det ikke mulig å slette passeringsopplysninger.

- Vegvesenet har behandlet personopplysninger ulovlig. Slettefunksjonen har manglet, og det er snakk om enormt mye informasjon som ikke har vært nødvendig å lagre, sier direktør Bjørn Erik Thon.



Kontaktperson

Janne Stang Dahl
kommunikasjonsdirektør



Kontor: [+47 22 39 69 03](tel:+4722396903)

Mobil: [+47 97 08 11 20](tel:+4797081120)

E-post: janne@datatilsynet.no

Eksempel – gammel lov - manglende sletting og ulovlig viderebehandling



[Lover og regler](#) / [Sentrale avgjørelser](#) / 2020

- Overtredelsesgebyr (400 000 NOK)
- Bruk av kameraopptak for sikkerhetsformål til å overvåke kontraktsparter, ansatte ++
- Manglende rettslig grunnlag, uforenlig formål, brudd på sletteplikten

Vedtak om overtredelsesgebyr til Statens vegvesen

Datatilsynet har gitt Statens vegvesen et overtredelsesgebyr på 400 000 kroner for å ha behandlet personopplysninger til formål som er uforenlige med det opprinnelige formålet, og for ikke å ha slettet kameraopptak etter 7 dager.



Innebygd personvern

Kravet til innebygd personvern



Personvernforordningen artikkel 25

- Personvern skal være med fra start når nye systemer for behandling av personopplysninger utvikles
- Personvern skal være standardinnstilling i behandlingssystemer

Et krav som inneholder hele personvernforordningen



- Det mest sentrale:
 - Sørge for at systemene dere bruker oppfyller personvernprinsippene og ivaretar de registrertes rettigheter
 - Personvern som standardinnstilling; systemet må settes opp slik at ikke flere personopplysninger enn nødvendig samles inn, ikke lagres lenger enn nødvendig, tilgangsstyring, tekniske begrensninger for bruken av opplysningene.
 - Formålet med standardinnstilling = å styre brukeren til en arbeidsmåte som gir bedre personvern
 - Informasjonssikkerhet, herunder risikovurderinger og tilgangsstyring. Hva slags opplysninger behandles i systemet?
- Veiledning på datatilsynet.no

Hva ser Datatilsynet etter på tilsyn?

Hva ser Datatilsynet etter?



- Ansvarlighetsprinsippet, jf. artikkel 5 nr. 2.
 - Skriftlige rutiner og dokumenterte vurderinger av personvernforordningen
 - Brudd på grunnleggende krav som rettslig grunnlag, informasjon til de registrerte eller informasjonssikkerhet?
 - Hvor alvorlige er konsekvensene for registrertes rettigheter og friheter, og er det mange berørte?
 - Konteksten personopplysningene er blitt behandlet (type virksomhet, kategorier personopplysninger og registrerte)
- indikasjoner på at virksomheten ikke har forstått sitt ansvar.
- GDPR forutsetter sterk forankring hos ledelsen.



Hva skjer når Datatilsynet banker på døra?



- (Vi banker som regel på postkassa...)
- Klagesaker og meldinger om brudd på personopplysningssikkerheten utgjør en stor del av saksmengden vår.
- Innhenting av informasjon fra den behandlingsansvarlige.
- Krav om redegjørelse – pålegg om å gi Datatilsynet informasjon om brudd på personopplysningssikkerheten eller forhold som fremgår av klagen, jf. personvernforordningen artikkel 58.
- Vurdering av saken
- Avslutning av sak eller varsel om vedtak (f.eks. pålegg, irettesettelse eller overtredelsesgebyr)
- Vedtak
- Eventuell klage og oversendelse til Personvernemnda

Jobber du med kunstig intelligens?

Usikker på personvernet?

Vi løser det sammen i sandkassa for ansvarlig KI.



søknadsfrist: 15. september

info, kriterier og søknadsskjema på:
datatilsynet.no/sandkasse



Datatilsynet

sandkasse@datatilsynet.no
telefon: +47 22 39 69 00

Spørsmål og svar

Takk for oppmerksomheten!

Ta gjerne kontakt med veiledningstjenesten vår ved spørsmål om personvernregelverket



postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no