Personopplysninger og opplæring i kriminalomsorgen

Gullik Gundersen | juridisk rådgiver

06.05.2016

Datatilsynet

Tema

- Hva er personopplysninger
- Hvordan etterleve pliktene i loven

Hvem har ansvaret?

«Behandlingsansvarlig»

= Fylkeskommunen

= skoleeier

= rådmannen

~ delegasjon til skolens ledelse/rektor

Hva er personopplysninger?

Hva er personopplysninger?

- Personopplysninger er:
  - Opplysninger eller vurderinger
  - Som kan knyttes til en enkeltperson
- Direkte identifiserende:
  - Navn,
  - Fødselsnummer
  - Telefonnummer
- Indirekte identifiserende:
  - Alder
  - Adresse
  - Diagnose

Sensitive personopplysninger

- Definert i personopplysningsloven § 2 nr. 8
- Opplysninger om:
  - rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,
  - at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
  - helseforhold,
  - seksuelle forhold,
  - medlemskap i fagforeninger

Sensitive personopplysninger

- Definert i personopplysningsloven § 2 nr. 8
- Opplysninger om:
  - rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,
  - at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
  - helseforhold,
  - seksuelle forhold,
  - medlemskap i fagforeninger

Vilkår for å behandle personopplysninger

Den behandlingsansvarlig 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.

Vilkår for å behandle personopplysninger

Den behandlingsansvarlig 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.

Vilkår for å behandle personopplysninger

Den behandlingsansvarlig 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.

Vilkår for å behandle personopplysninger

Den behandlingsansvarlig 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.

Internkontroll og informasjonssikkerhet

Hva er internkontroll etter vårt regelverk

- Det handler om å sikre en forsvarlig behandling av personopplysninger
  - Å sikre den registrertes rettigheter
  - Å ivareta virksomhetens mål med behandlingen

- Ledelsens verktøy for å ivareta sitt ansvar etter lover og regler

- De ansattes verktøy for utføre oppgaver på forsvarlig og sikker måte

Hva er informasjonssikkerhet

- Informasjonssikkerhet dreier seg om å håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger

- Informasjonssikkerhet omfatter beskyttelse av:
  - **konfidensialitet** - uvedkommende får ikke tilgang på opplysningene
  - **integritet** - opplysningene endres ikke uautorisert eller utilsiktet
  - **tilgjengelighet** - opplysningene er tilgjengelige når tilgang er nødvendig

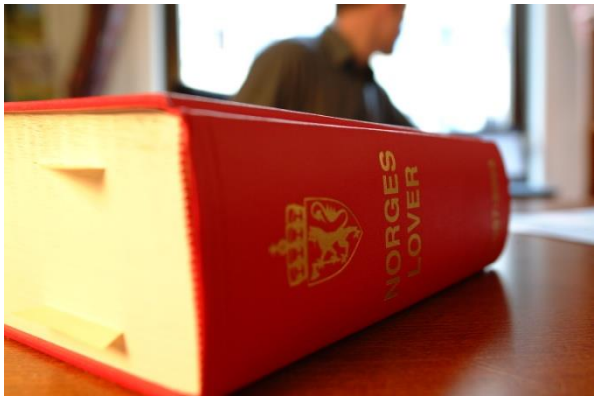
Regelverket - kortversjonen

”Den behandlingsansvarlige skal etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige…”

”Den behandlingsansvarlige skal dokumentere tiltakene”

”Dokumentasjonen skal være tilgjengelig…”

Rutiner for oppfyllelse av plikter
og de registrertes rettigheter



Rutiner for internkontroll

Rutinene bør utformes i henhold til en felles mal. Rutinene blir da enklere å bruke, og det blir lettere å vurdere om de er fullstendige. Følgende punkter kan benyttes for utforming av rutiner:

1. Hvorfor skal rutinen utarbeides, hva er hensikten med den?
2. Hvem er ansvarlig for å utføre de ulike aktivitetene?
3. Hva skal utføres av de ulike ansvarlige?
4. Hvordan skal aktivitetene utføres og hva kan man ikke gjøre?
5. Når skal de ulike aktivitetene utføres, eller under hvilke betingelser?
6. Hva er forventet resultat ved utførelse av rutinen?

Eksempler på rutiner

Rutiner for

- Innhenting av samtykke
- Informasjon
- Vurdering av opplysningenes kvalitet
  - Tiltak for å behandle korrekte opplysninger
  - Tiltak for å forhindre innsamling av unødvendige opplysninger
- Retting
- Innsyn
- Utlevering
- Sletting
- Melding og konsesjon

Forskriften § 3-1

Saksbehandlere skal…

- Ikke avgjøre hvordan opplysningen skal sikres
- Forskånes fra å være i tvil om hvordan han skal håndtere opplysningene
  - Vite hvilke rutiner som finnes
  - Vite hvem som er ansvarlig for å gi hjelp
  - Vite hvem som skal orienteres om problemer
- Følge ledelsens rutiner
- Rapportere avvik
  - Avvik fra rutiner
  - Manglende eller ufullstendige rutiner

Det skal være lett å gjøre det rette

Utgangspunktet for arbeid med risiko

- Personopplysningslovens regler om sikkerhet tar utgangspunkt i den behandlingsansvarliges skjønn
- Skjønnet skal utøves gjennom risikovurderinger
  - Sannsynlighet
  - Konsekvens
- Risiko skal måles opp imot akseptabelt risikonivå – hvilke avvik kan ledelsen akseptere?

Risikovurdering

- Formålet med risikovurdering er å sikre at den risiko som avdekkes ved behandling av personopplysninger er innenfor de akseptkriterier virksomheten har fastlagt.
- Risiko betegner forholdet mellom sannsynligheten for at en uønsket hendelse vil inntreffe og konsekvenser av en slik hendelse.
- Virksomheten skal gjennomføre risikovurdering ved endringer i forhold som kan påvirke informasjonssikkerheten, for eksempel
  - endringer i behandlinger
  - endringer i informasjonssystem
  - endringer i trusselbildet
- Risikovurderingen skal dokumenteres.

Forskriften § 2-4

Risikovurderinger – trinn for trinn

1. Kartlegg og klassifiser behandlinger av personopplysninger
2. Identifiser uønskede hendelser (og årsaker til hendelser)
3. Konsekvensvurdering
4. Sannsynlighetsvurdering (letthet)
5. Vurdering opp mot akseptabel risiko
6. Tiltak for å redusere risiko

Kartlegge virksomhetens behandlinger

Virksomheten skal ha oversikt over personopplysningene

- Nødvendig for å ivareta sine plikter.
- Grunnlag for sikkerhetsmål og sikkerhetsstrategi.
- Underlag for risikovurderinger.

Informasjon Formål	Behandlings-grunnlag	Melding/ Konsesjon	Klassifikasjon	Sikkerhets-tiltak	Lagring og kommuni-kasjon	Opplysningenes omfang	Avdeling	Databehandler
Lønn og personal: lønnsopplysninger personalopplysninger	Personopplysning sloven, § 8f	Unntatt i forskriftens § 7-16	Person-opplysninger			Ca. 130 ansatte		
Barnevern: vurdering og tiltak	Barnevernloven, § 3-1	Meldt 14.01.2009	Sensitive person-opplysninger			Ca. 68 barn og foresatte		
Helseopplysninger: pasientjournal	Helsepersonel-loven § 39	Meldt 14.01.2009	Sensitive person-opplyninger			Ca. 413 pasienter		
Elevadministrasjon elever / foresatte lærere	Opplæringsloven § 13-5		Person-opplyninger			Ca. 219 søkere		
Hendelsesregister: logg over brudd	Personopplysning sloven, § 13	Unntatt i forskriftens § 7-11	Person-opplyninger			Arkivlogg, nettverkslogg og serverlogg, PC-logger		

Eksempel på risikomatrise

Konsekvens: Sannsynlighet:	Liten	Moderat	Stor	Katastrofal
Svært høy				
Høy	Informasjon med lavt beskyttelsesbehov på avveier.	En dags bortfall av sikkerhetskopiering. Ukjente mennesker i kontorlokalene		
Moderat	Utilgjengelighet av personalsystem i 24 timer	Budsjettinformasjon på avveier.	Styreinformasjon på avveier.	Konkurransesensitiv informasjon på avveier.
Lav			Sensitive opplysninger om en ansatt på avveier. Uautorisert endring av opplysninger om en ansatt	Sensitive opplysninger om alle ansatte på avveier.

Takk for meg!

Datatilsynet

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

datatilsynet.no
personvernbloggen.no

ggu@datatilsynet.no | 22 39 69 28