Brudd på personopplysningssikkerheten – hva vil Datatilsynet kreve av dokumentasjon?

…..og hvilke vurderinger gjør vi….

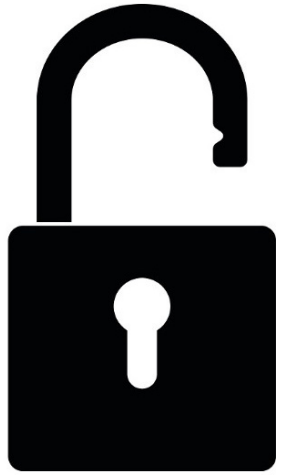
Kristine Stenbro, Senioringeniør, seksjon Teknologi, Sikkerhet og Tilsyn

Datatilsynet

Melding om brudd på personopplysningssikkerheten (art 33)

«brudd på personopplysningssikkerheten»:

…….er et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig (uautorisert) spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet (art. 4 nr. 12)



Når må melding sendes til Datatilsynet?

«Ved brudd på personopplysningssikkerheten …,

…med mindre bruddet ***sannsynligvis ikke vil medføre en risiko*** *for fysiske personers rettigheter og friheter.»*

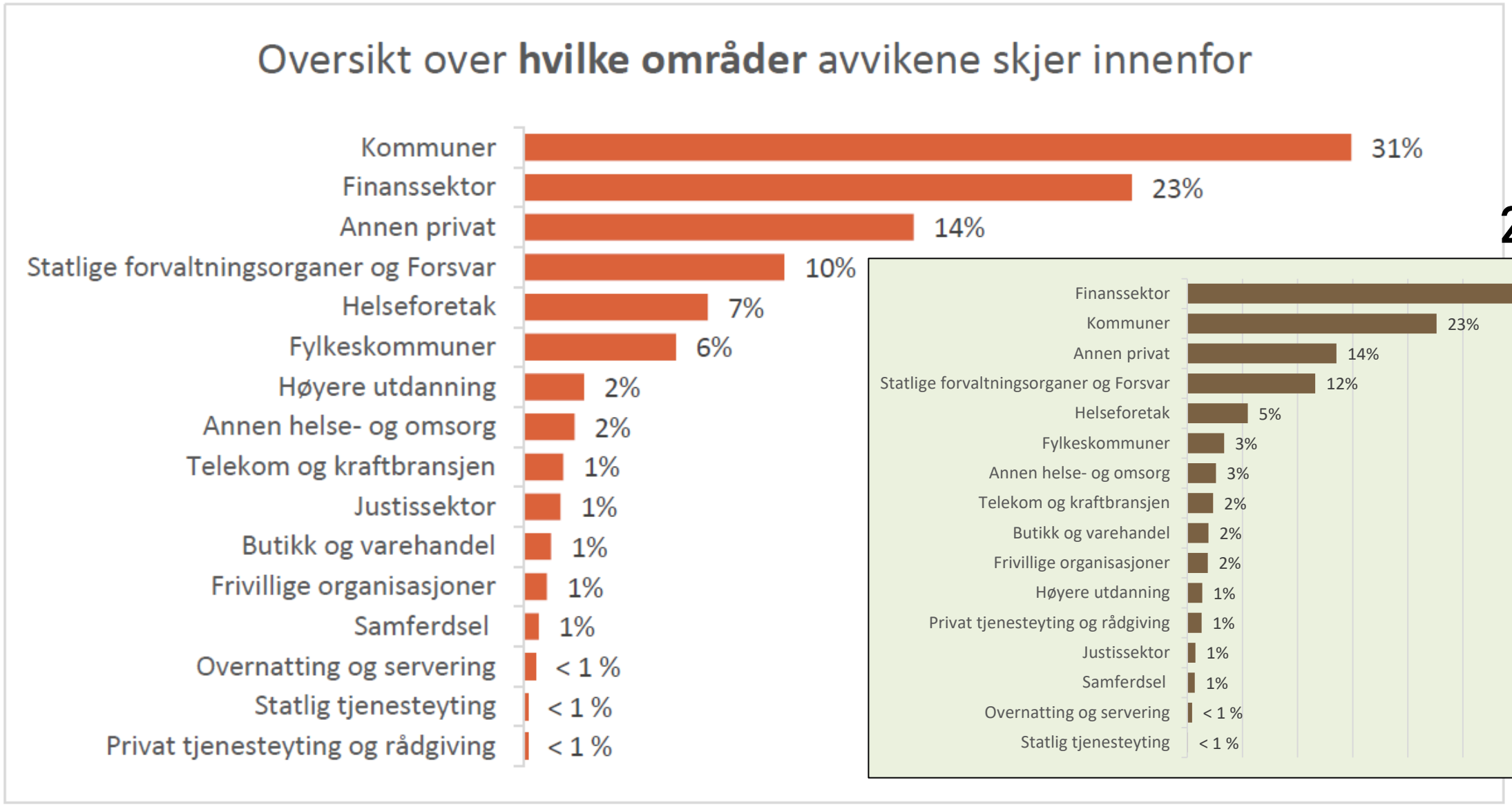
Lav terskel!

72 timer etter at man med **rimelig grad av visshet** har konstatert brudd…

Kan meldes trinnvis

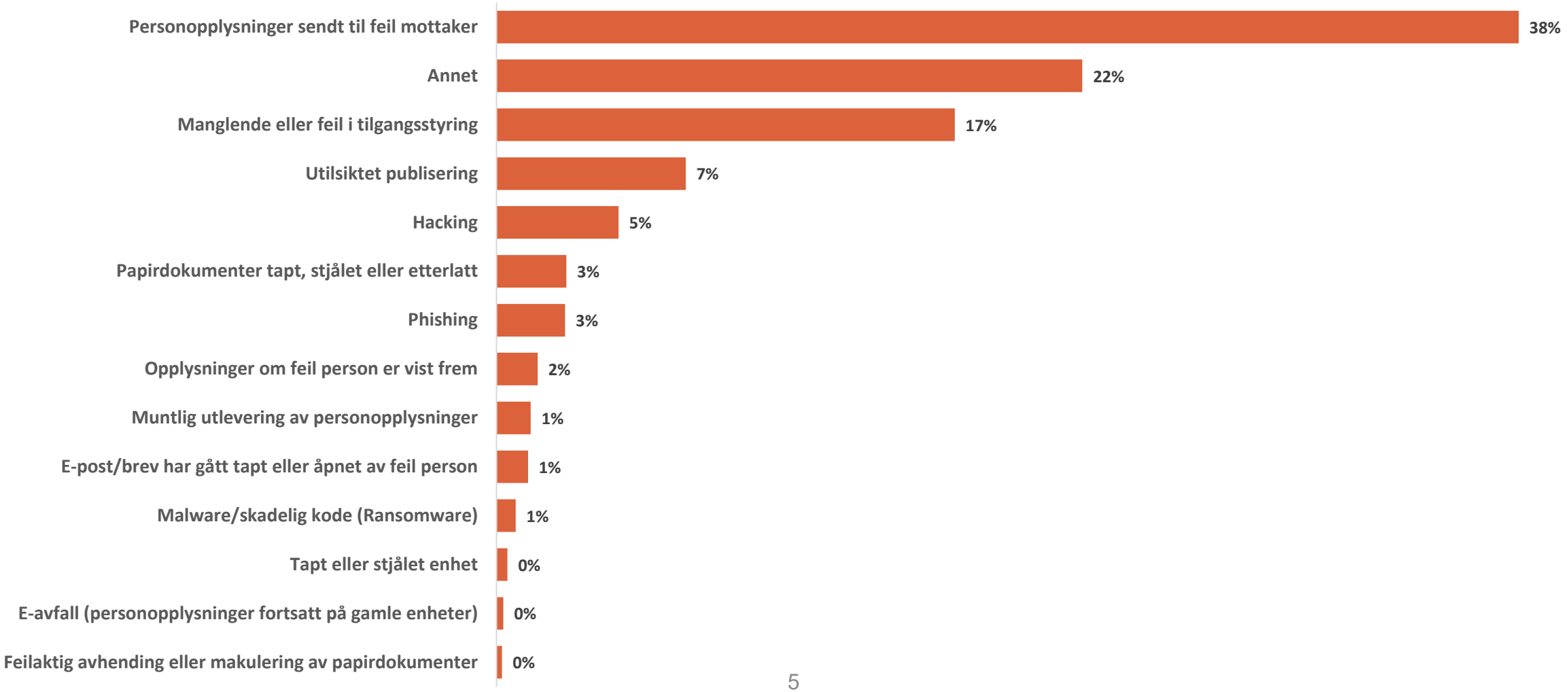
Ta kontakt om du trenger råd!

Avviksmeldinger til Datatilsynet 2020 – sektorvis fordeling



Hva slags brudd blir meldt– tall i prosent (2020)

Oversikt over hvilke **typer overtredelser** som er meldt inn



VG SPORTEN VG LIVE

INNENRIKS Innenriks

ØSTRE TOTEN DATAANGREPET DATAANGREP HACKING BRØR HELGESTAD

Søknader og saksbehandling kan hope seg opp i Østre Toten: – Saksbehandlerne får ikke opp noe på PC-ene sine

SAMLET TIL MØTE: Mandag kveld holdt krisestaben i Østre Toten møte. De ble oppdatert på arbeidet med å gjenskape datasystemene. Foto: ØSTRE TOTEN KOMMUNE

11. januar 2021, kl. 22:01

Av Erik Sørstelie

Innbyggere, bedrifter og organisasjoner må smøre seg med tålmodighet etter dataangrepet.

Ordfører Bror Helgestad sier det kan ta

Aktuell Sikkerhet

Alt skal bli bra, men det tar tid og blir dyrt

Østre Toten kommune har fått signaler om at det er veldig godt håp om å få tapte data tilbake etter hackerangrepet i helga. I likevel vil det ta lang tid før alt virker som normalt.

Kommunedirektør Ole Magnar Sletsrud og ordfører Bror Helgestad måtte tilbake på pauten og papir, i likhet med sine kolleger i Østre Toten kommune. (Foto: Jon Olav Andersen)

Kommunedirektør Ole M
blitt låst av hackere. Foto

Hackere ha
– Uakt

Hackere låste i helga de l
uaktuelt å etterkomme kr

Even Rise

PUBLISERT Mandag 11. januar 2021 –

Østre Toten kommune opplever nå at all data er kryptert og gjort utilgjengelig for de ansatte. Situasjonen er så alvorlig at det er satt krisestab.

Datatilsynets saksbehandling

Saksbehandlers innledende vurderinger:

- Gikk det lang tid før hendelsen ble oppdaget og deretter meldt til Datatilsynet?
- 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)
- Indikerer bruddet alvorlige mangler i internkontroll og informasjonssikkerhet?
- Har virksomheten hatt tilsvarende brudd tidligere?
- Er de igangsatte tiltakene tilstrekkelige og effektive?
- Er det gitt tilstrekkelig informasjon til de registrerte?

→ indikasjoner på at virksomheten ikke har forstått sitt ansvar
→ indikasjoner på at virksomheten ikke har lært

Behov for ytterligere informasjon – Krav om redegjørelse

Datatilsynets oppgave er å føre kontroll etter personopplysningsregelverket slik at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem.

For at Datatilsynet skal kunne vurdere saken, har vi behov for å be om nærmere opplysninger om hendelsen.

Med hjemmel i personvernforordningens artikkel 58 nr. 1 bokstav a) **ber Datatilsynet om å få oversendt følgende dokumentasjon:**

Status i avvikssaken og tilhørende tiltak

Vi ber om:

En oppdatert beskrivelse av status i den innmeldte avvikssaken (herunder spørsmål om saksspesifikke detaljer)

En oversikt over planlagte og iverksatte tiltak som kan bidra til å begrense konsekvensene av angrepet og hindre gjentagelse.

Vi vurderer:

- Alle nye relevante opplysninger
- Endret alvorlighetsgrad

- Relevante
- Effektive
- Tilstrekkelige

Informasjon til de berørte

Vi ber om:

En oppdatert status på planlagte og gjennomførte tiltak for å underrette berørte/registrerte om bruddet på personopplysningssikkerheten.

Vi vurderer:

- Er de berørte informert?
- Hvis nei, hvorfor ikke? (konkrete vurderinger)
- Er metoden for å informere egnet, effektiv og tilstrekkelig?
- Videre oppfølging av berørte

Internkontroll og styringssystem for informasjonssikkerhet

Vi ber om:

En oversikt over etablerte rutiner og prosedyrer for ivaretakelse av personopplysningssikkerheten fra kommunens internkontrollsystem og styringssystem for informasjonssikkerhet. (art 24 – påvise etterlevelse av regelverk)

Vi vurderer:

- Eksistens
- Ledelsesforankring
- Tilstrekkelighet
- Tilgjengelighet
- Forankring i organisasjonen
- Opplæring
- Vedlikehold
- Evaluering/revisjon

Hovedelementer – dokumentoversikt (eksempel)

Styringsdokument internkontroll

Styrende

Sikkerhetsmål og -strategi

Sikkerhetsorganisasjon

Ledelsens gjennomgang (rutine)

Rutiner for:
- Innhenting av samtykke
- Informasjon
- Innsyn
- Korrigering
- Sletting/retten til å bli glemt
- Begrenset behandling
- Innsigelse
- Dataportabilitet
- Automatiserte avgjørelser
- Særskilte rettigheter for beskyttelse av barns personvern

Gjennomførende

Risikovurdering

Beskrivelse av informasjonssystem

Sikkerhetstiltak, f.eks.:
- **Tilgangskontroll**
- **Logging**
- Informasjonshåndteringsrutine
- Sjekkliste nyansatt / slutter
- Taushetserklæring

Fysisk sikring

Driftsrutiner

Beredskapsplan

Sikkerhetsinstrukser

Opplæringsplaner

Ledelsens gjennomgang

Egenkontroll

Kontrollerende

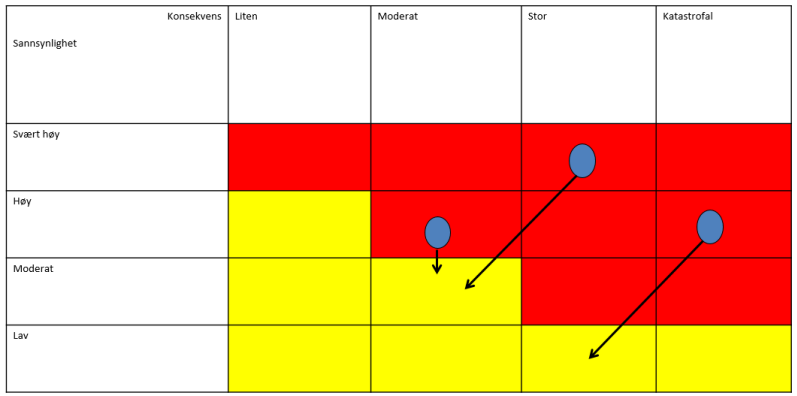
Avvikshåndtering

Sikkerhetsrevisjon

Risiko- og sårbarhetsanalyser

Vi ber om:

- Risikovurderingene som er utarbeidet for de berørte datasystemene/løsningene
- En oversikt over risikoreduserende tiltak og status på arbeidet med å implementere disse



Vi vurderer:

- Alder
- Tilstrekkelighet
- Konkrete risikoreduserende tiltak
- Oppfølgingsplan
- Evaluering og revisjon

Rutiner og prosedyrer - tilgangskontroll

Vi ber om:

Rutiner og prosedyrer for å tildele og terminere tilganger til «systemet/løsningen», herunder

a. hvilke tilgangsnivåer og roller som er etablert for å sikre at en bruker bare autoriseres for tilgang til det vedkommende har tjenestlig behov for

b. hvilke rutiner som er etablert for å revidere og oppdatere brukertilganger i henhold til endringer i tjenestlig behov og avslutning av arbeidsforhold

Vi vurderer:

- Eksistens
- Tilgjengelighet
- Organisasjonens kunnskap
- Etterlevelse
- Tilstrekkelighet

Rutiner og prosedyrer - aktivitetslogger

Vi ber om:

Rutiner og tekniske tiltak for å registrere, spore og kontrollere tilgang til opplysninger i «systemet», herunder

a. etablerte rutiner og mekanismer for å avdekke uautorisert tilgang til opplysninger

b. etablerte rutiner systematisk gjennomgang av aktivitetslogger

c. etablerte rutiner for å tildele og terminere tilgang til aktivitetslogger

d. etablerte rutiner for sletting av aktivitetslogger

Vi vurderer:

- Eksistens
- Tilgjengelighet
- Organisasjonens kunnskap
- Etterlevelse
- Tilstrekkelighet

Rutiner og prosedyrer - avvikshåndtering

Vi ber om:

Gjeldende rutiner og prosedyrer for håndtering og oppfølging av avvik i forbindelse med brudd på fastlagte rutiner, herunder

a. kort beskrivelse av løsning for avvikshåndtering

b. tiltak for å sikre forståelse hos de ansatte

b. rutiner for revaluering og revisjon

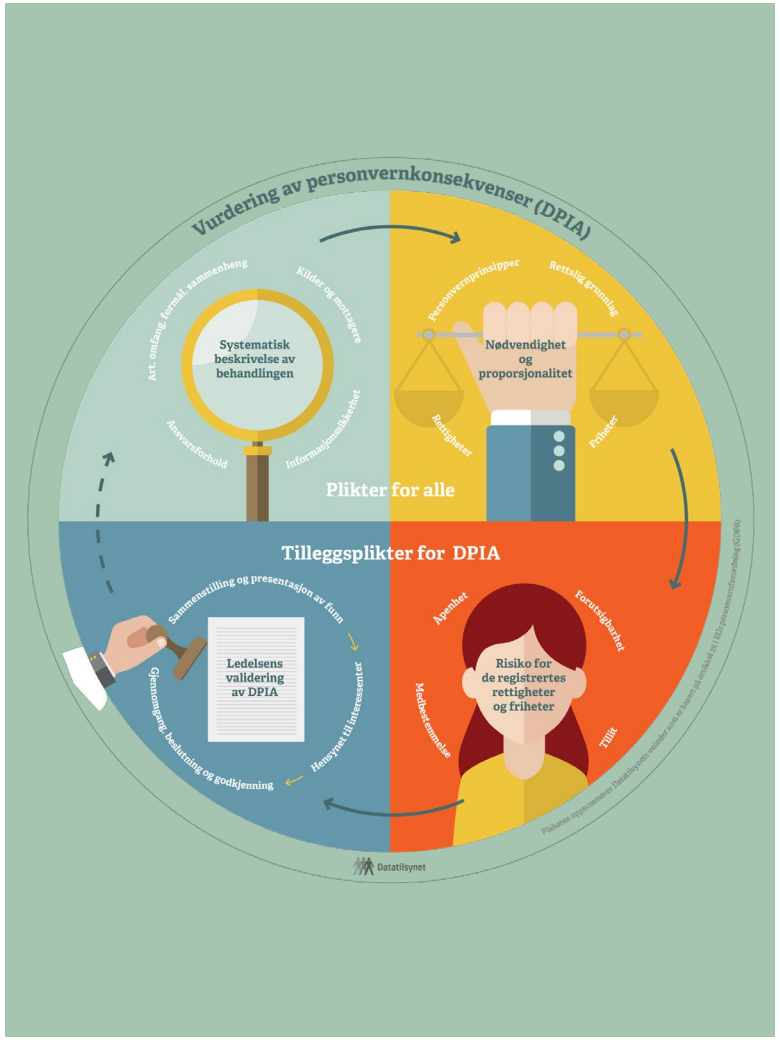
Vi vurderer:

- Eksistens
- Tilgjengelighet
- Opplæringstiltak
- Tilstrekkelig/hensiktsmessig

Annen relevant dokumentasjon

Vi ber også om:

- Behandlingsprotokoll
- Personvernkonsekvensvurderinger - DPIA
- Databehandleravtaler



Vurdering av alvorlighetsgrad

Relevante faktorer bestemmende for utfallet

Bruddets **karakter og varigheten av overtredelsen**, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd,

Grad av **forsettlighet eller uaktsomhet**

eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skadene

den behandlingsansvarliges eller databehandlerens **grad av ansvar**, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32,

eventuelle relevante **tidligere brudd på personopplysningssikkerheten**

graden av samarbeid med tilsynsmyndigheten

kategoriene av personopplysninger som er berørt

på **hvilken måte tilsynsmyndigheten fikk kjennskap** til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen,

overholdelse av godkjente atferdsnormer i henhold til artikkel 40 eller godkjente sertifiseringsmekanismer i henhold til artikkel 42 og **enhver annen skjerpende eller formildende faktor ved saken**

Takk for meg!

Datatilsynet

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

datatilsynet.no
personvernbloggen.no