



Vurdering av personvernkonsekvenser, databehandleravtaler og avvik

Gullik Gundersen, Eirin Oda Lauvset, Marte Skaslien og Martha Eike

Personvernforordningen tre måneder inn

Gullik Gundersen | rådgiver

Personvernforordningen i tall



- 931 avviksmeldinger i 2018, 461 etter 20. juli
- Ca. 700 ombud før 2018
- 1157 ombud registrert etter 20. juli 2018
- 291 kommuner har meldt inn ombud, av total 422 kommuner

Personvernforordningen i tall



- 10 bransjenormer (vet om ca. 30 under utarbeidelse), avventer internasjonale retningslinjer før disse kan behandles.
- Ca. 90 internasjonale saker som berører Norge
- Datatilsynet er ansvarlig myndighet for to saker.
- Ingen anmodninger om forhåndsdrøftelser
- Ingen saker om dataportabilitet



- Datatilsynet skal arbeide for en mer rettferdig maktbalanse mellom individet på den ene siden, og kommersielle aktører og det offentlige på den andre.
- Datatilsynet skal arbeide for å fremme personvernvennlig digitalisering, innovasjon og utvikling.
- Datatilsynet skal arbeide for at virksomheter blir kompetente, forstår viktigheten av godt personvern og etterlever regelverket.
- Datatilsynet skal bidra til at individet i større grad kan ivareta sitt eget personvern.
- Datatilsynet skal påvirke og ta lederrollen i noen utvalgte internasjonale prosesser for å fremme bedre personvern.
- Datatilsynet skal være et kompetent og fremtidsrettet *tilsyn*.

Hvordan skal vi jobbe de neste seks månedene?



- Kontroll med opprettelsen av personvernombud
- Forenklet veileder om internkontroll og informasjonssikkerhet rettet mot små og mellomstore virksomheter
- Ansvarlig for internasjonal veileder om innebygd personvern
- Videreutvikling av tilsynsmetodikk, og da særlig metodikk for å kunne føre tilsyn med algoritmer og kunstig intelligens
- Jobbe for innebygd personvern i utviklingen av kunstig intelligens

Vurdering av personvernkonsekvenser

Eirin Oda Lauvset | seniorrådgiver



Art. 5 Personvern- prinsippene



De registrertes rettigheter



- Informasjon (art 12-14)
 - Innsyn (art 15)
 - Korrigering (art 16 & 19)
 - Sletting/Retten til å bli glemt (art 17 & 19)
 - Rett til at personopplysninger begrensnings (ny, art 18 & 19)
 - Dataportabilitet (ny, art 20)
 - Innsigelse (ny, art 21)
 - Automatiserte avgjørelser, inkludert profilering (ny, art 22)
- } Forutsetning for de resterende rettigheter



Art. 12-22

Den registrertes friheter



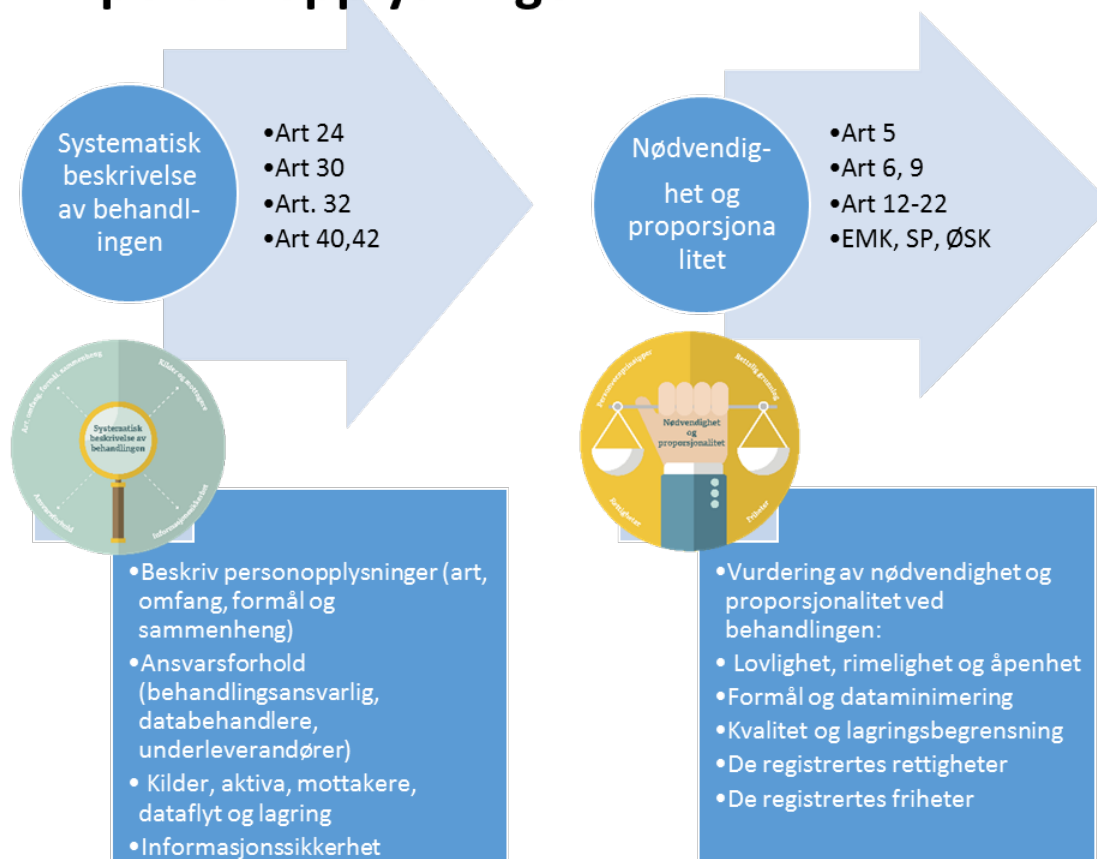
- Retten til privatliv
- Retten til kommunikasjon og kommunikasjonsvern
- Tanke- tros- og religionsfrihet
- Ytrings- og informasjonsfrihet



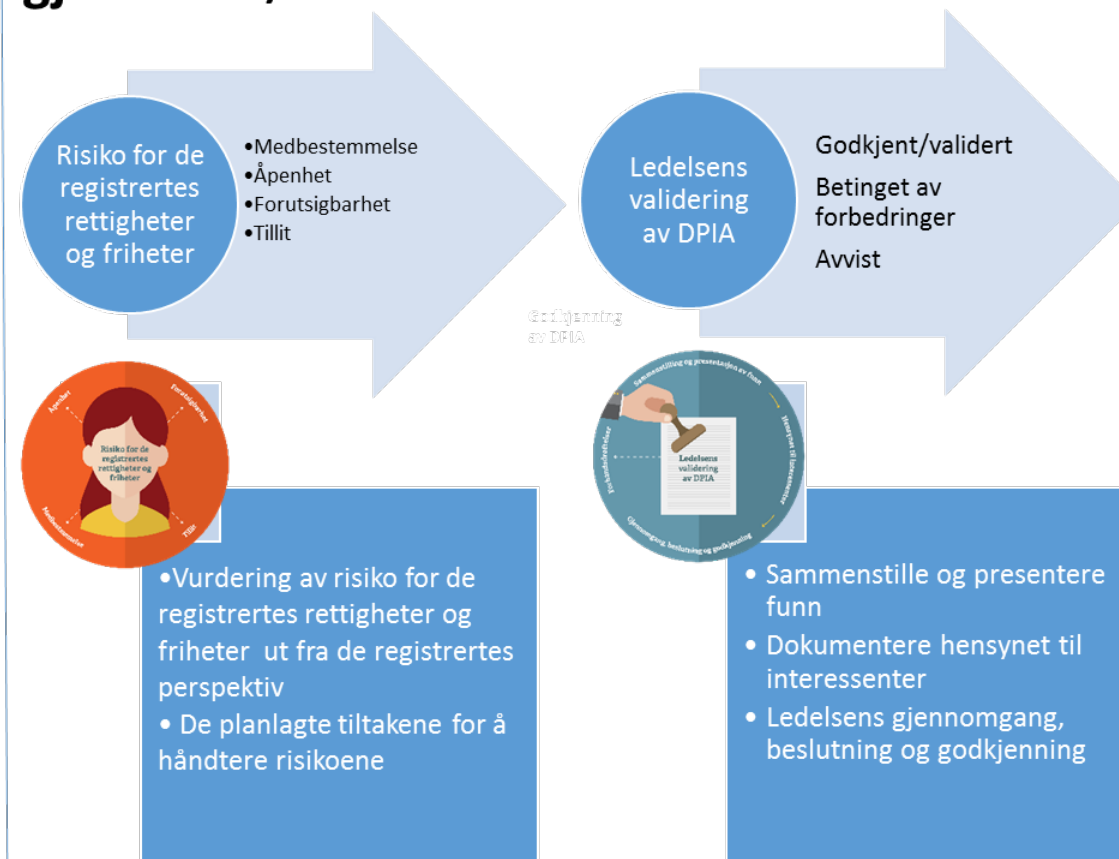
DPIA – en tilleggsplikt for særskilt inngripende behandlinger



Dette er plikter for alle som behandler personopplysninger



Dette er plikter kun for de som skal gjennomføre DPIA



Vurdering av risiko for de registrertes rettigheter og friheter



Art. 35.7 c



- **Medbestemmelse** – reell innflytelse på hvordan opplysningene blir behandlet (valgfrihet, reservasjon, innsigelse, sperring, portabilitet, etc)
- **Åpenhet** – reell og ærlig åpenhet (informasjon, innsyn og reell mulighet til å mene noe om det som foreslås)
- **Forutsigbarhet** – minimere kompleksiteten til en behandling
- **Tillit** – grunnleggende for vellykket digitalisering av tjenester

Mål: Gjennomføre vurdering av personvernkonsekvenser for den registrertes rettigheter og friheter, bestemme tiltak for å redusere HØY risiko



- Data kan deles i samspill med innbyggeren (fullmaktsordninger)
- Innbyggeren kan bli informert og utøve sine rettigheter på nett (innsyn, retting, sletting, innsigelse, trekke samtykke)
- Innhente de registrertes syn på behandlingen/drøfte løsninger
- Mulighet for å spisse tilgang til personopplysninger (kun relevante data blir delt, tilgang til bestemte personer i bestemt tidsrom)
- Automatisk sletting/anonymisering
- Tekniske og administrative tiltak for å hindre kobling mellom datasett
- Illustrasjoner på dataflyt



En skoleeier/kommune vurderer å gå til innkjøp av en programvare som skal gjøre det enklere for dem å gi elevene individuelt tilpasset opplæring. Konkret vurderer de programvare for å forstå og forbedre læringsprosesser gjennom automatisert innhenting og analyse av data fra alle elevens digitale enheter/applikasjoner, samt profilering av elevene.

- Identifiser de **rettigheter og friheter** som kan bli begrenset med den planlagte prosesseringen.
- Identifiser **tiltak** som kan redusere risikoen for at elevenes rettigheter og friheter skal begrenses.

Når trenger man databehandleravtale?

Marte Skaslien | rådgiver

Hvem er behandlingsansvarlig?



- Den som bestemmer formålet og de avgjørende virkemidlene
- Organisasjonsform ingen betydning
- Virksomheten som helhet er ansvarlig, og ikke enkeltpersoner

Hvem er databehandler?



- Det avgjørende er at en databehandler behandler personopplysninger **på vegne av andre**.
- Organisering uten betydning. Kan både en virksomhet, en fysisk person.
- «På vegne av andre» tilsier at det er snakk om en ekstern virksomhet eller personer. Ikke egne ansatte.

Når foreligger det et databehandleroppdrag?

Og hvem er i så fall behandlingsansvarlig og databehandler?



Er den andre virksomheten en databehandler?

- Krever en skriftlig databehandleravtale. (Artikkel 28)

Er den andre virksomheten selvstendig behandlingsansvarlig for opplysningene de mottar?

- Krever et behandlingsgrunnlag for å utlevere personopplysningene. (Artikkel 6 og eventuelt 9)

Hvem bestemmer formål og midler?



Formål

- Hvorfor skjer denne behandlingen?
- Hvem tok initiativet til å behandle disse personopplysningene?
- Alltid behandlingsansvarlig som bestemmer

Midler

- Hvem bestemmer hvilke personopplysninger man trenger?
- Hvem bestemmer hvordan opplysningene skal behandles og når de skal slettes?
- Databehandleren kan bestemme midler som ikke er avgjørende

Hva sier loven eller avtalen?



Loven kan bestemme hvem som er behandlingsansvarlig

- Direkte eller indirekte

Avtalen kan bestemme hvem som er behandlingsansvarlig

- Hva er avtalt mellom partene?

Hva slags ytelse eller oppdrag skal leveres/utføres?



Er det snakk om et databehandleroppdrag eller i realiteten et annet type oppdrag?

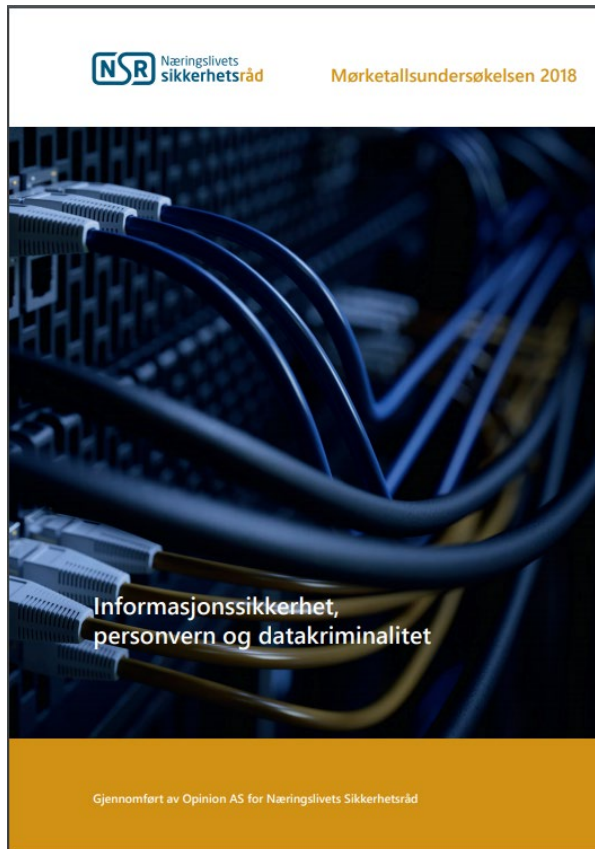
- Bli det behandlet personopplysninger?
- Er formålet med oppdraget **helt eller delvis** å behandle personopplysninger?
- Er den andre parten bundet av egne regler for hvordan opplysningene skal behandles?

Avviksmeldinger til Datatilsynet

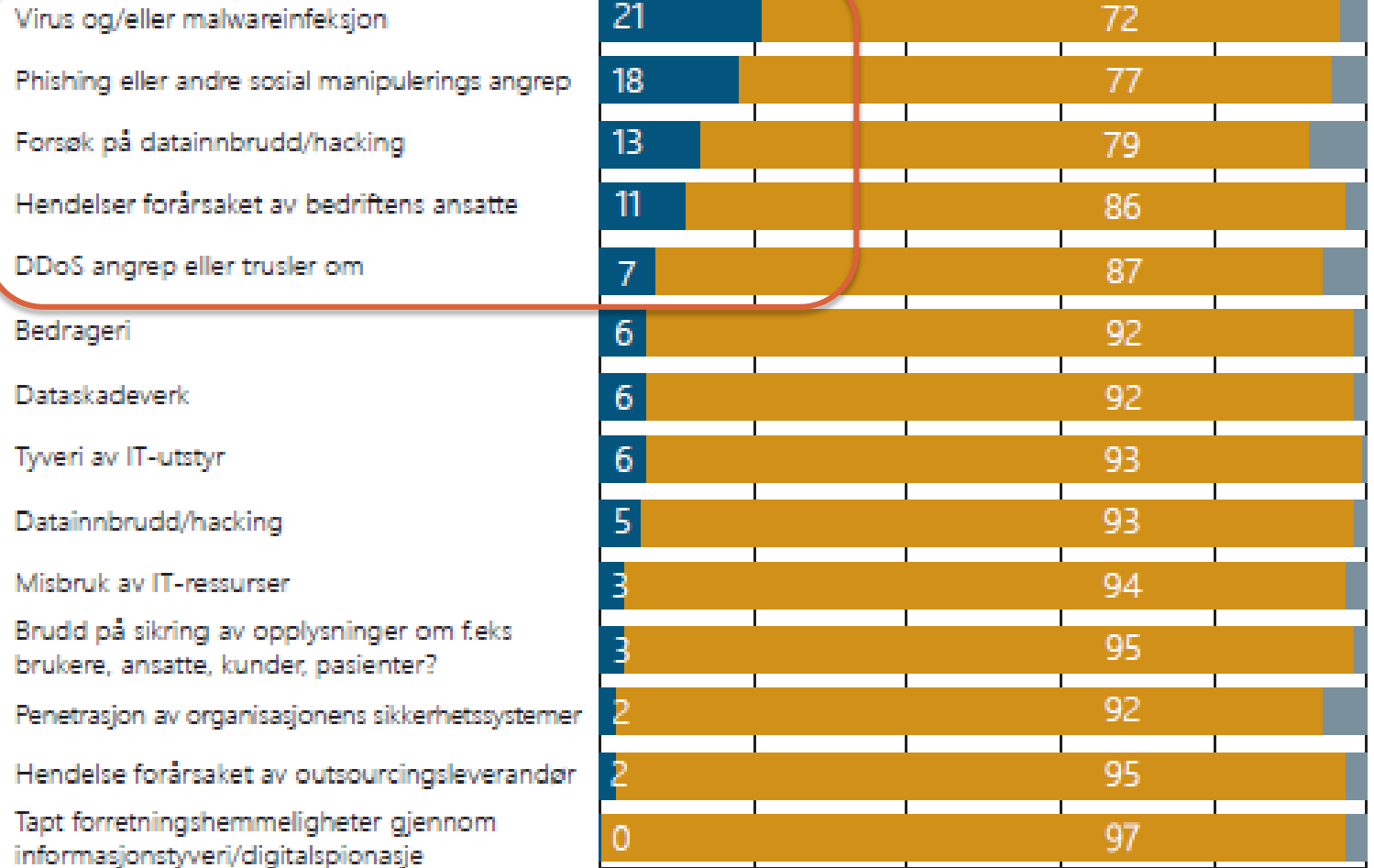
Martha Eike | fagdirektør

Spørsmål: Jeg vil nå lese opp noen mulige informasjonssikkerhetshendelser og ber deg svare ja eller nei på om virksomheten har vært utsatt for disse i kalenderåret 2017? (n=1500)

Vanligste sikkerhets- hendelser i fjor



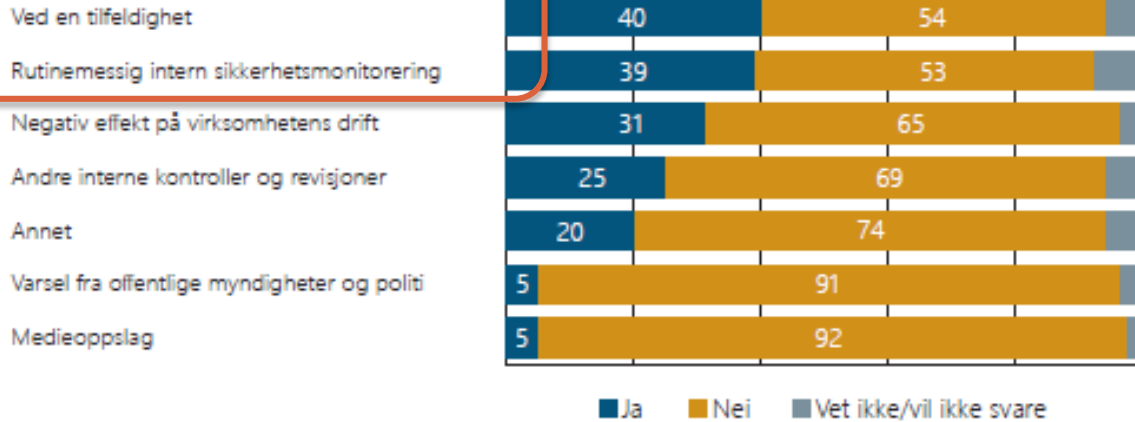
Figur 5



■ Ja ■ Nei ■ Vet ikke

Spørsmål: Var noe av følgende årsak til at hendelsen ble oppdaget? (n=572)

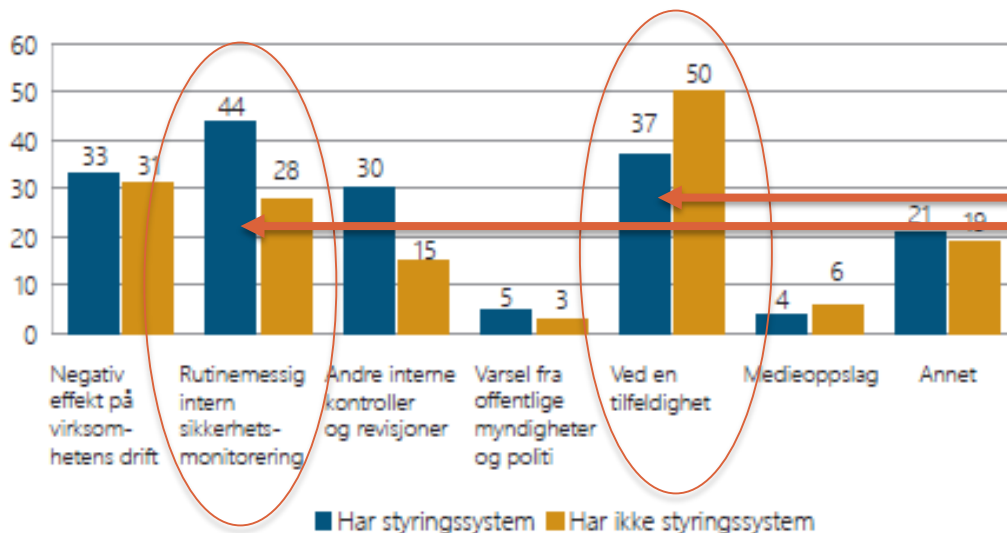
Figur 12



Vanligste årsak til at hendelsen ble oppdaget var ved en tilfeldighet (eller flaks!)

Det er forskjell på virksomheter med og uten styringssystem for informasjonssikkerhet når det gjelder årsaker til at hendelsen ble oppdaget.

Figur 13



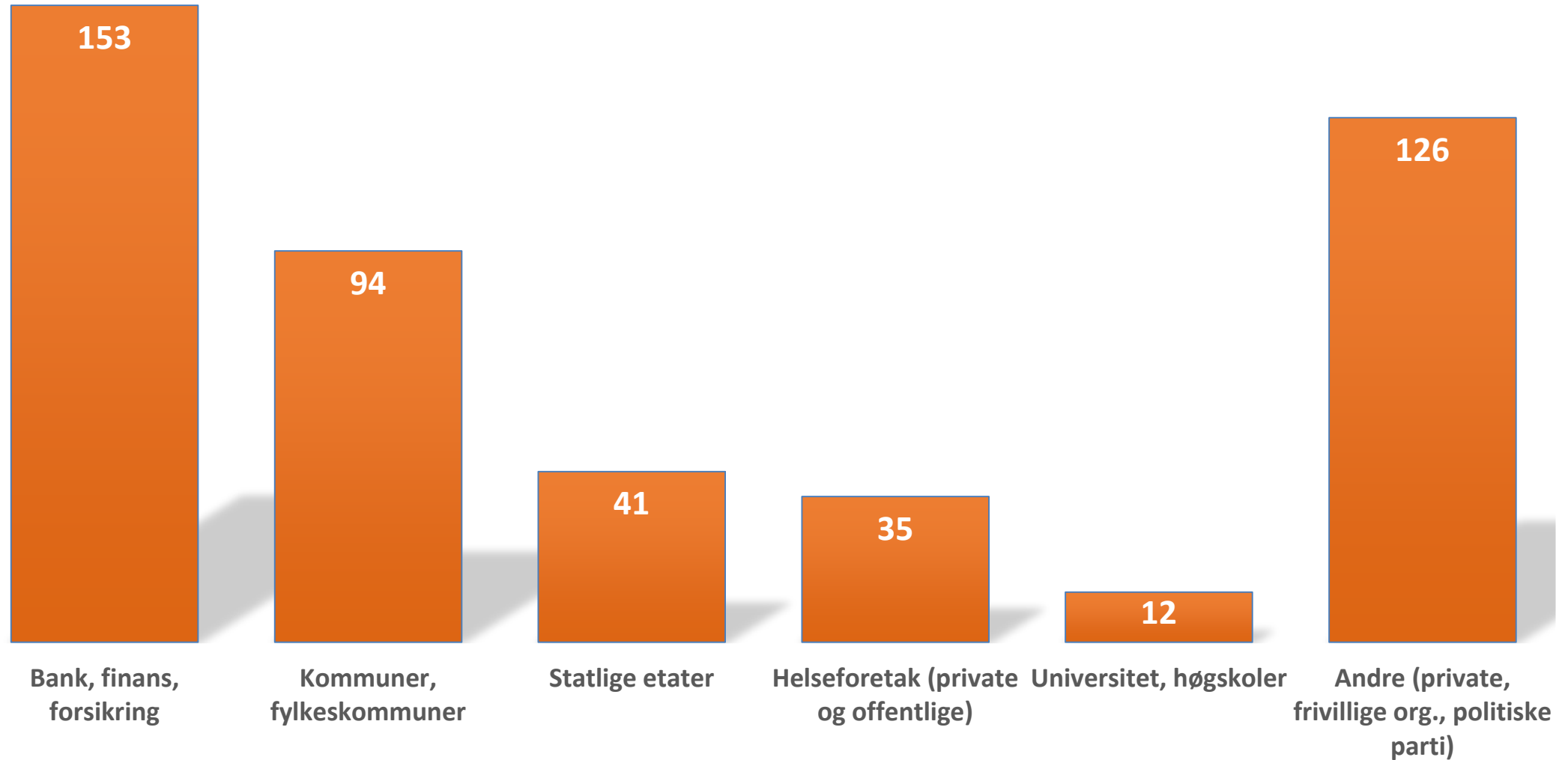
Virksomheter med internkontroll eller styringssystem baserer seg mindre på tilfeldigheter og mer på intern sikkerhetsmonitorering

Antall meldte avvik fra 2014 til i dag



Hvem melder avvik?

20. juli – 19. oktober





UVEDKOMMENDE: Slik ser det ut når noen logger inn i «eFeide»-løsningen. Kommunen mener uvedkommende har fått tilgang til et administratorpassord til systemet. FOTO: SKJERMDUMP

Kommunen beskriver datainnbrudd som «rampestreker»

Uvedkommende skal ha utgitt seg for å være rektor, sendt falsk melding og endret informasjon i datasystemet. «Flere tegn kan indikere at hendelsen er «rampestreker» utført av elever ...», står det i avviksmeldingen kommunen sendte til Datatilsynet.



Stiftelsen Elden driver med sang, dans, spel og videreformidling av straffesaksdokumenter. (Foto: Skjermdump fra Stiftelsen Eldens hjemmeside)

Straffesaker sendes feil hele tiden

Søndag mottok amatørteateret Elden på Røros en omfattende straffesak som skulle til advokatfirmaet med samme navn.

Kjetil Kolsrud

3 okt 2018 kl. 06:00

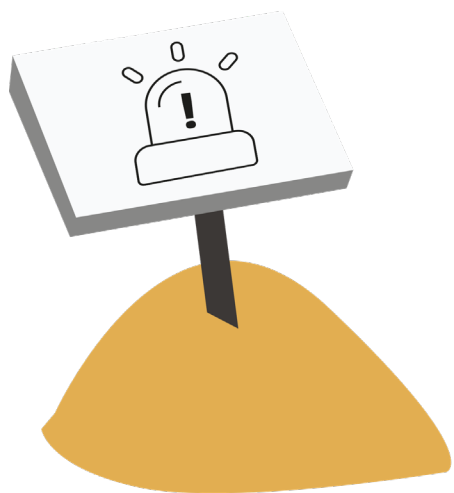
Oppdatert: 3 okt 2018 kl. 13:26

Torsdag i forrige uke opplevde Rett24 å bli tilsendt straffesaksdokumenter via Altinn. Dokumentene skulle egentlig til forsvareren, men Oslo politidistrikt hadde ved et uhell forvekslet advokatfirmaets organisasjonsnummer med Rett24s organisasjonsnummer.

...men mange skyldes feilsendte e-poster...
«menneskelig svikt»



Når må virksomheten sende melding om avvik til Datatilsynet?



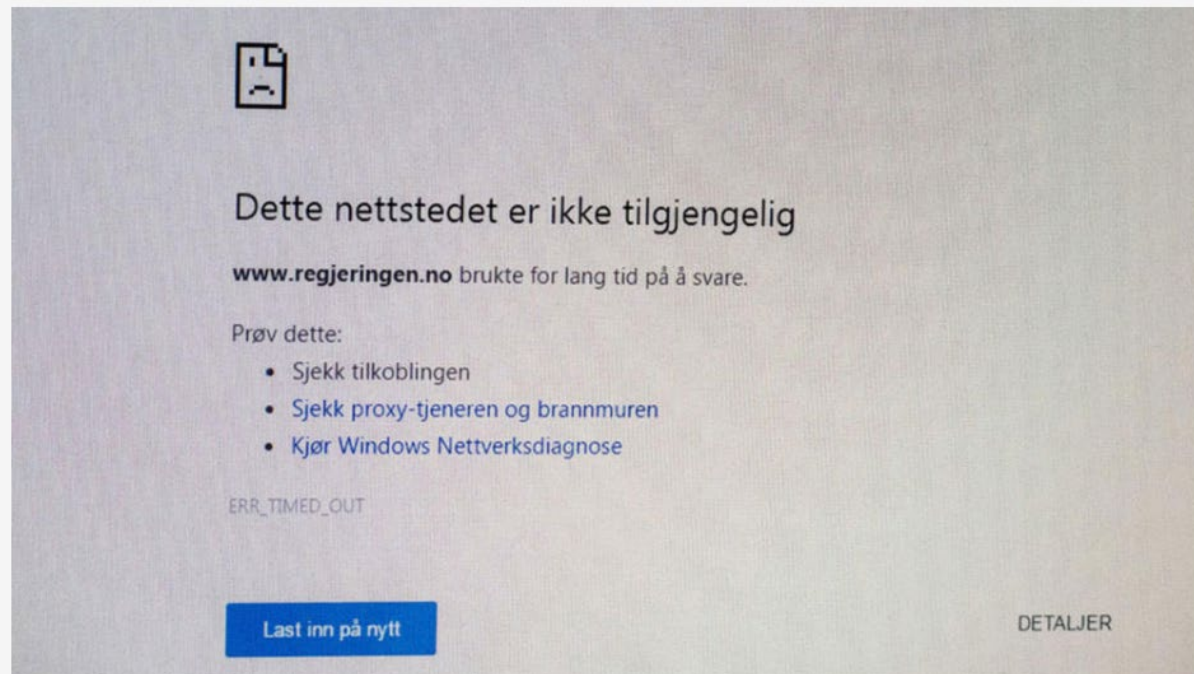
Ikke bare konfidensialitet, men også tilgjengelighet og integritet

«Ved brudd på personopplysningssikkerheten ..., med mindre det er lite trolig at bruddet vil medføre en risiko for fysiske personers rettigheter og friheter.»

Definisjon: «*brudd på personopplysningssikkerheten*» - er et brudd på sikkerheten som fører til *utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til* personopplysninger som er overført, lagret eller på annen måte behandlet (art. 4 nr. 12)

Art. 33

Omfattende hackerangrep i USA satte regjeringen.no ut av spill



ANGREPET: Hackere som angrep amerikanske servere førte mest sannsynlig til at nettsiden regjeringen.no var ustabil fredag. Foto: NTB Scanpix Foto: NTB Scanpix

Regjeringens informasjonskanal var delvis nede fredag kveld etter et svært omfattende hackerangrep i USA. FBI etterforsker saken men aner ikke hvem som står bak.

Guri G. Oppegård

22.10.2016 (Oppdatert: 22.10.2016)

Et brudd på personopplysningssikkerheten er et brudd på sikkerheten, men et brudd på sikkerheten er ikke alltid et brudd på personopplysningssikkerheten.

Sørg for å ha interne rutiner for hendelseshåndtering uansett.

Kilde: tv2.no

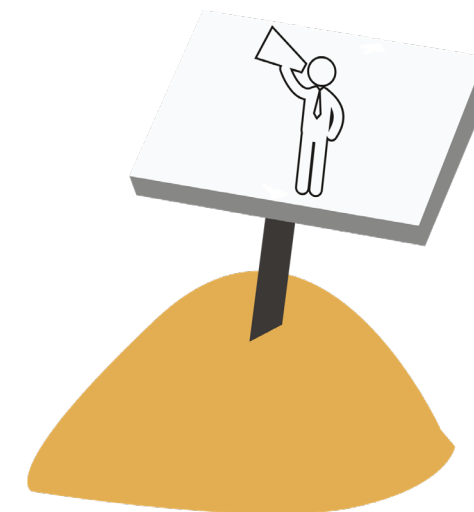


Dersom det er sannsynlig at bruddet vil medføre en høy risiko...

- Berørte skal informeres så raskt som mulig, slik at de skal kunne foreta seg noe for å begrense skaden.
- Bruk den kanal som det er størst sjanse for å nå ut til den berørte (f.eks. telefon, SMS, e-post, brev..)

Unntak i kravet om varsling:

- Eksisterende tiltak som gjør informasjonen uleselig, f.eks. kryptering
- Tiltak i ettertid som sikrer at den høye risikoen ikke lengre vil oppstå
- Uforholdsmessig innsats. Må i stedet informere offentlig eller tilsvarende.



Art. 34

Når er det høy risiko



Risiko er høy når det er sannsynlig at bruddet kan føre til (f.eks.):

- Diskriminering
- Identitetstyveri eller svindel
- Økonomisk tap
- Skade på omdømme

Brudd som innebærer personopplysninger som avslører (f.eks.):

- Rase eller etnisk opprinnelse
- Politisk oppfatning
- Religion eller filosofisk tro
- Fagforeningstilhørighet
- Opplysninger om genetikk, helse eller sexliv
- Straffedommer og lovovertrедelser eller relaterte sikkerhetstiltak

kan medføre skade for den registrerte

Faktorer – ved vurdering av risiko



- Type brudd
- Art, sensitivitet og mengde data
- Hvor lett er det å identifisere den enkelte
- Alvorlighetsgrad av konsekvenser for den enkelte
- Spesielle egenskaper hos den enkelte
- Antall berørte enkeltpersoner
- Spesielle egenskaper hos den behandlingsansvarlige

Takk for oppmerksomheten!



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

datatilsynet.no
personvernbloggen.no

@datatilsynet

