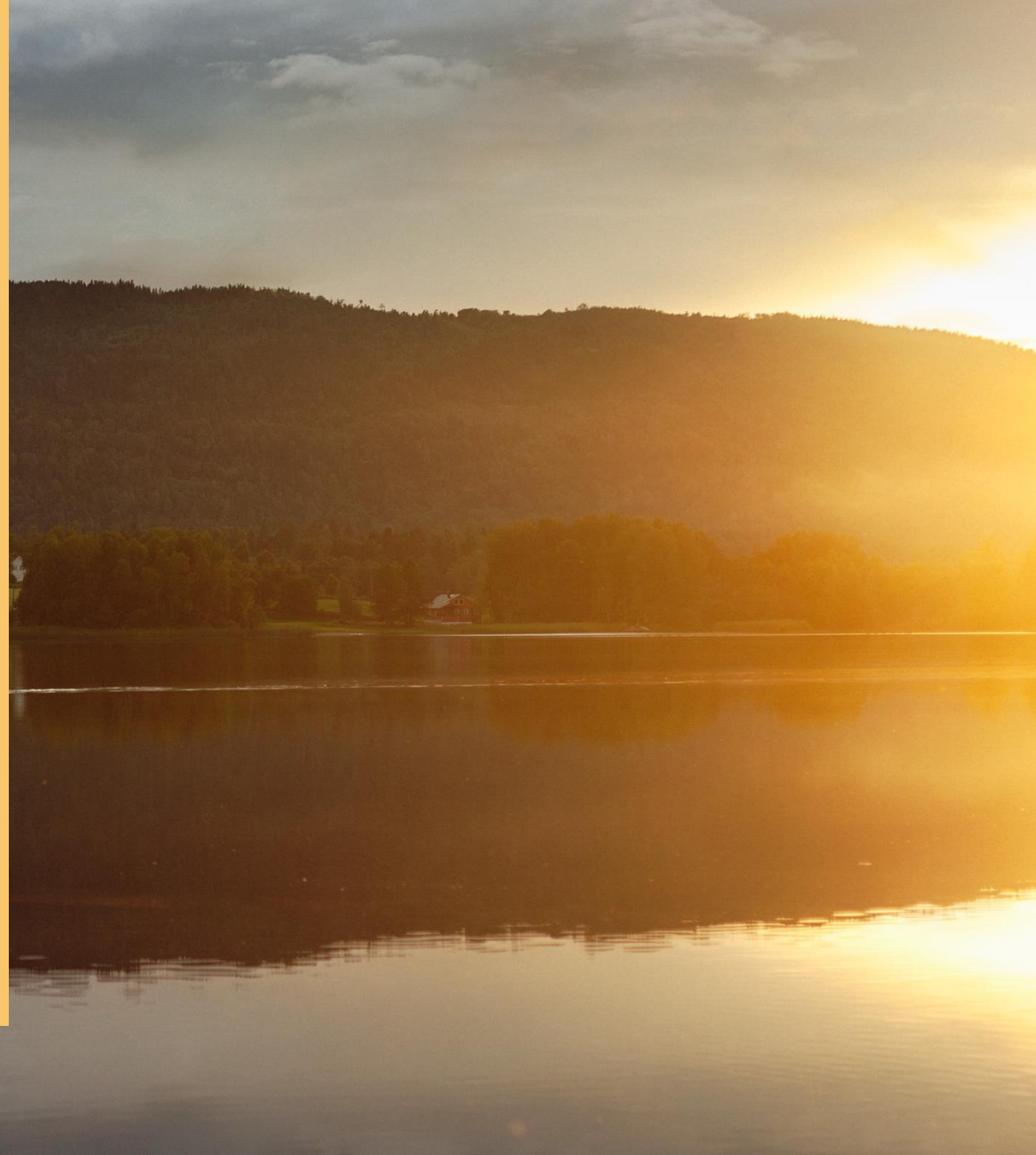




Innføring i personvern

04.06.2020

Henrik Lindgren Jensen og Linda Knutsen

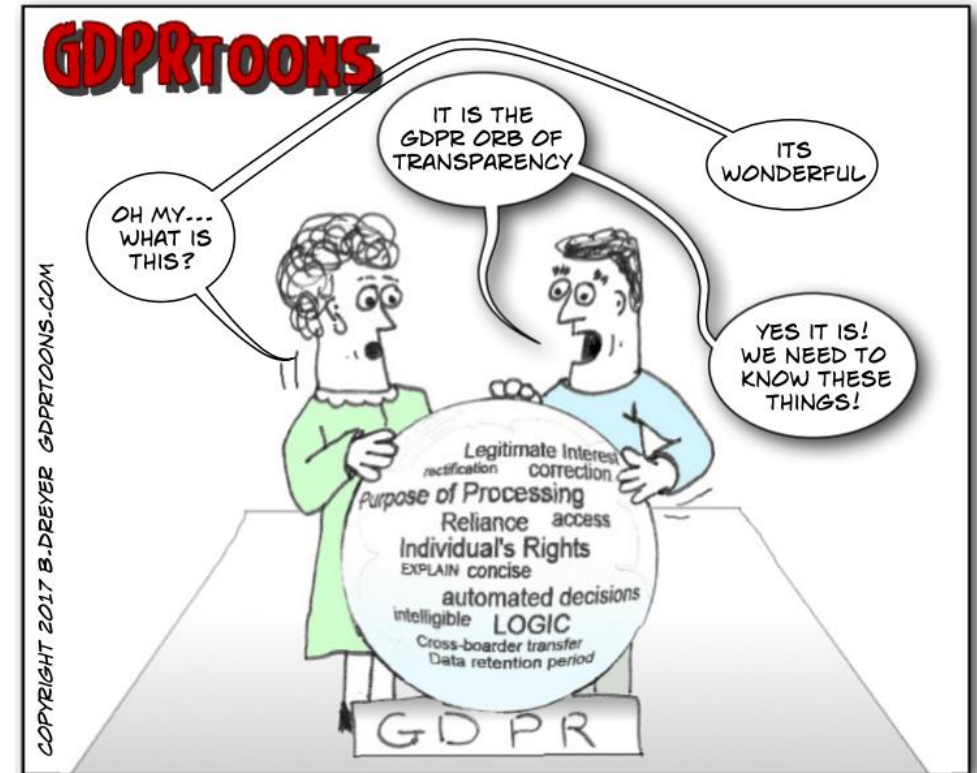


Kjøreregler for dagens kurs 😊

- ▶ Alle skrur av kameraet.
- ▶ Alle skrur av mikrofon.
- ▶ Spørsmål stilles i chat.
- ▶ Vi tar sikte på ca. 3-4 stopp underveis i presentasjonen for besvarelse av spørsmål, også de som er innsendt på forhånd.

Agenda

- ▶ Hva er personvern og personopplysninger?
- ▶ Hva er behandling av personopplysninger?
- ▶ Grunnleggende personvernprinsipper
- ▶ Behandlingsgrunnlag
- ▶ De registrertes rettigheter
- ▶ Ditt ansvar som ansatt i Oslo kommune
- ▶ Avvik



Alle snakker om det, men hva er egentlig personvern?

«Personvern handler om retten til et privatliv og retten til å *bestemme over egne personopplysninger*»

Datatilsynet

Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse

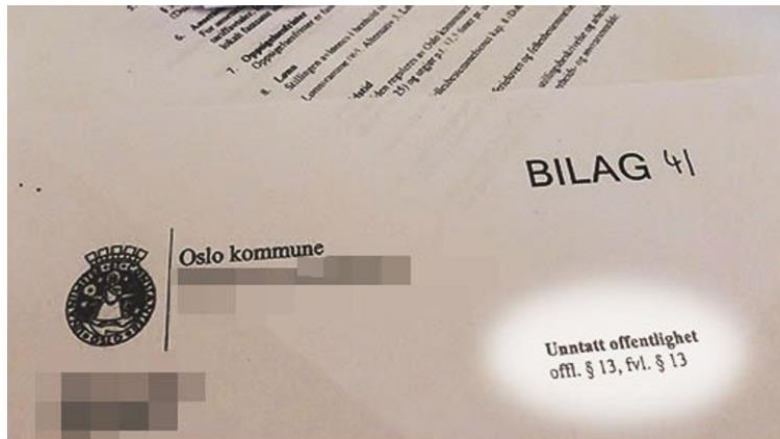
Europeiske menneskerettighetskonvensjonen (EMK) art. 8 og Grunnloven § 102



Hvorfor er personvern viktig for Oslo kommune?

Personvern-tabbe i Oslo kommune: Brettet ut sensitive dokumenter om 30 ansatte på nettsidene

Ved hjelp av et tastetrykk kunne hvem som helst laste ned et flere hundre sider stort dokument om en arbeidskonflikt fra Oslo kommunes nettsider. – Jeg er rystet, sier en av de ansatte som er rammet av tabben.



Til tross for at opplysningene er taushetsbelagte, ble de publisert på Oslo kommunes nettsider. Bildet er redigert av NRK for å hindre spredning av opplysningene.



Publisert 11. juni 2019 kl. 07:28
Oppdatert 11. juni 2019 kl. 09:21

[Lover og regler](#) / [Sentrale avgjørelser](#) / [2019](#)

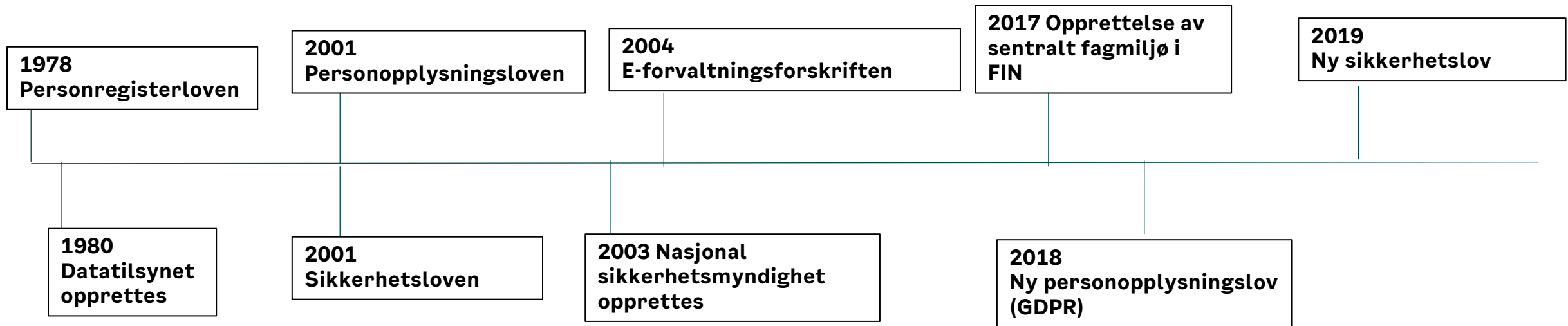
Gebyr til Oslo kommune Utdanningsetaten

Datatilsynet sendte i april 2019 varsel til Oslo kommune Utdanningsetaten om et overtredelsesgebyr for brudd på personopplysningssikkerheten i mobilapplikasjonen Skolemelding. I oktober ble det vedtatt et endelig gebyr på 1,2 millioner kroner.

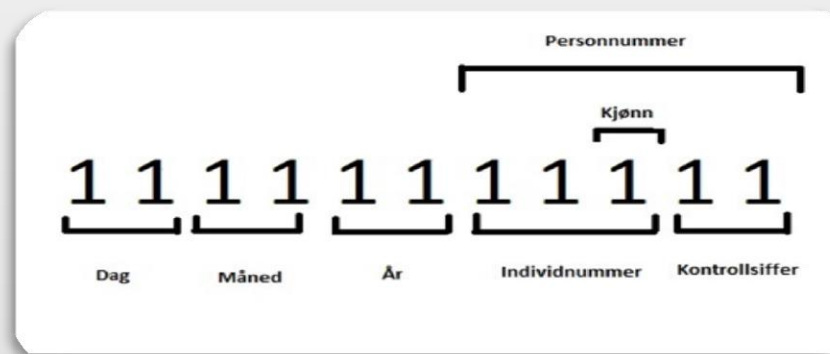
Gebyret blir gitt fordi kommunen ikke hadde gjennomført egnede tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. I vurderingen ble det lagt vekt på blant annet:

Publisert: 01.12.2019
Sist endret: 20.01.2020

Lovkrav knyttet til behandling av personopplysninger er ikke noe nytt



Hva er en personopplysning?



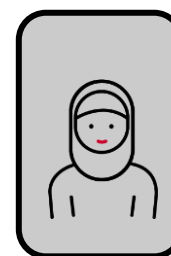
Særlige kategorier av personopplysninger



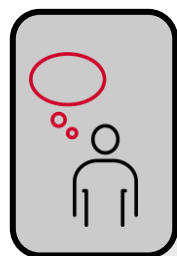
rasemessig eller
etnisk opprinnelse



politisk oppfatning



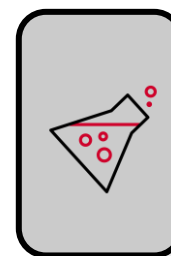
religion



filosofisk
overbevisning



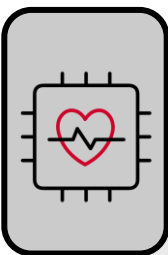
fagforeningsmedlems
kap



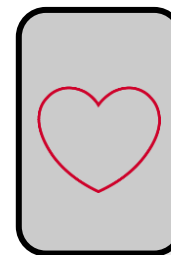
genetiske
opplysninger



biometriske
opplysninger med det
formål å entydig
identifisere noen



Helseopplysninger



Seksuelle forhold,
seksuell orientering

Spørsmål?



Hva er en behandling av personopplysninger?

innsamling

registrering

Organisering

strukturering

lagring

tilpasning eller
endring

gjenfinning

utlevering ved
overføring

tilgjengeliggjøring

sammenstilling

begrensning

sletting

tilintetgjøring

mm.



Grunnleggende personvernprinsipper



Lovlighet, rettferdighet og åpenhet

Personopplysninger behandles lovlig, rettferdig og åpent for den registrerte



Ansvarlighet

Virksomheter har ansvar for å opptre i samsvar med forordningen



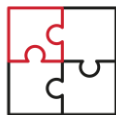
Formålsbegrensing

Personopplysninger behandles kun til spesifiserte, eksplisitte og legitime formål



Konfidensialitet og integritet

Personopplysninger behandles på en sikker måte som sikrer mot utilsiktet ødeleggelse, skade eller tap



Riktighet

Personopplysninger skal være så korrekte og oppdaterte som nødvendig for å oppnå formålet med behandlingen



Lagringsbegrensing

Personopplysninger lagres ikke lengre enn nødvendig for formålene de behandles for



Dataminimering

Personopplysninger som innsamles er relevante, tilstrekkelig og begrenset til det som er nødvendig for formålene



Behandlingsgrunnlag

- ▶ Behandling av personopplysninger er kun lovlig om man har behandlingsgrunnlag



Hjemmel i lov/forskrift

- Rettslig plikt /offentlig myndighet
- Klarhetskrav



Samtykke

- frivillig
- spesifikt
- informert
- utvetydig
- aktiv handling
- dokumenterbart
- like lett å trekke tilbake som å gi



Avtale

- Den registrerte må være del av avtalen
- Nødvendig for å utføre den etterspurte tjenesten



Ivareta vitale interesser

- Svært snevert
- Liv og død/stor helsefare



Utøve oppgave i allmenhetens interesse/ offentlig myndighet

- Offentlig myndighet
- Noen tilfeller private virksomheter
- Lovlig



Berettiget interesse

- Lovlig
- Klart definert
- Minst inngripende mulighet
- Interesseavveining

Rett til innsyn



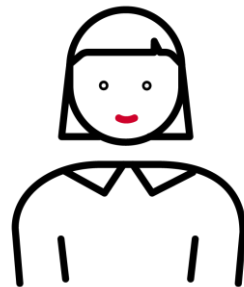
Rett til retting



**Rett til
sletting**

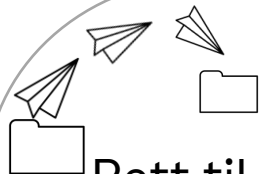


**Rett til å bli
informert**



Den registrertes rettigheter

Rett til å
protestere



**Rett til
dataportabilitet**

**Rett til å motsette
seg profilering**



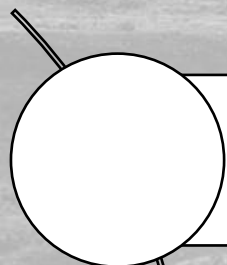
Rett til begrensning



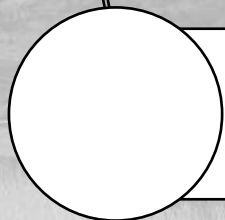
Spørsmål?

- Der noen søker om tilskudd fra en ordning som er regulert av en forskrift eller andre regler – hva er behandlingsgrunnlaget for å behandle personopplysningene deres og hvorfor. Hva hvis særlig kategorier personopplysninger må oppgis?
- Hvis noen registrerer seg for å få en tjeneste eller søke på noe via en nettside der samtykke er nødvendig for behandlingen. Hvordan skal samtykket innhentes i praksis for at det skal være tilstrekkelig? Holder det med en boks som man klikker i der opplysningene i GDPR art 13 oppgis ved siden av? Ved art 9 a) – samtykke – kreves da lenke til for eksempel altinn med eget skjema der – og hvordan ordenes i så fall dette?
- Ved bruk av samtykke må vi vurdere om det er ujevn maktbalanse mellom virksomheten og den registrerte for å se om frivilligheten i samtykket er reel. Har dere noen konkrete eksempler på situasjoner der maktubalanse ikke foreligger og der det foreligger?
- Art 6 nr.1 c) – Hva kan grunnlaget brukes til og hvilken begrensning ligger det i praksis i «på den registrertes anmodning».

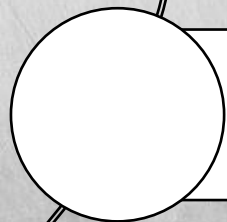
Ditt ansvar som ansatt



Følge retningslinjer og rutiner



Taushetsplikt



Gi beskjed hvis du oppdager avvik



Oslo

Følge retningslinjer og rutiner

- ▶ Vi bør ha et bevisst forhold til hvilke personopplysninger vi behandler.
- ▶ Vi bør kjenne til om det eksisterer spesielle regler for de verktøyene vi benytter.
- ▶ Vi bør kjenne til hvilke roller som eksisterer i virksomheten.

Taushetsplikt

- ▶ Alle som jobber i offentlig forvaltning har taushetsplikt
- ▶ Vi som ansatte plikter å hindre at andre får adgang eller kjennskap til det vi i forbindelse med tjenesten eller arbeidet får vite om noens *personlige forhold*.
- ▶ Gjelder også informasjon om tekniske innretninger, drifts- og forretningsforhold osv.
- ▶ Enkelte unntak

Forvaltningsloven §13 <https://lovdata.no/lov/1967-02-10/§13>





Hva er et avvik?



Hva sier regelverket?



Hvorfor skal vi melde
avvik internt?



Eksempler på avvik.

Hva er et avvik?

- ▶ Kort sagt: uønsket hendelse som berører personopplysninger!
- ▶ Brudd på konfidensialitet, integritet og/eller tilgjengelighet (K I T)
 - Hva betyr egentlig det?

Hva sier regelverket?

- Generelle bestemmelser om ansvarlighet og krav til informasjonssikkerhet
- Nærmere bestemmelser om:
 - når avviket skal meldes til Datatilsynet
 - plikten til å informere de berørte registrerte
 - plikten til å dokumentere vår interne behandling av avviket



Hvorfor er det viktig å melde avvik internt?

- ▶ Hindre misbruk eller skade!
- ▶ Tillit og omdømme!
- ▶ 72 timers frist!

- ▶ Bidrar til å forbedre virksomheten (vi lærer av feil)
- ▶ Det er positivt å si ifra om avvik
- ▶ Vet du som ansatt hvem du skal melde avvik til?



Eksempler på brudd:

Personopplysninger kan være på avveier

Personopplysninger til elever og lærere i fylkeskommunen kan ha kommet på avveier. Dette skyldes et sikkerhetsbrudd hos en av fylkeskommunens leverandører.

Sikkerhetsbruddet har skjedd hos selskapet Conexus, som leverer den skybaserte programvaren «Conexus Engage». Tre fylkeskommuner er berørt av hendelsen.

Vurderer anmeldelse

IT-systemet har informasjon om elever, lærere og enkelte ansatte i fylkesadministrasjonene. Fra 23. mars til 5. mai har det vært mulig å hente ut personidentifiserbar informasjon fra systemet. Til sammen inneholder skyløsningen persondata fra over 40 000 personer fra de tre fylkene.

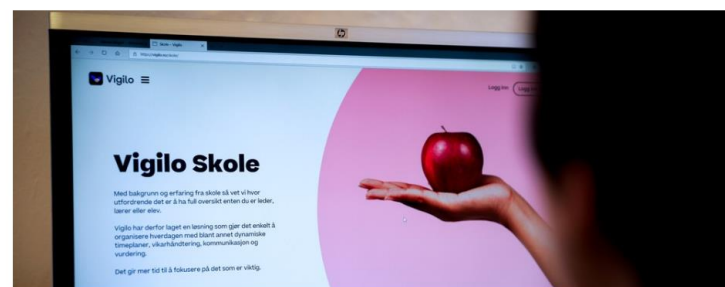


Pe
ho
Fo



Vigilo-saka: Datatilsynet varslar bot på 3 millioner kroner til Bergen kommune

Foreldre fekk tilgang til opplysningar om barn på hemmeleg adresse. No vil Datatilsynet gi Bergen den største data-bota til ein kommune nokon gong.



Helse Sør-Øst: Innrømmer at utenlandske IT-arbeidere fikk tilgang til sensitive pasientdata

De siste ukene har titalls IT-arbeidere i Asia og Øst-Europa hatt tilgang og utvidete rettigheter til datasystemet til Helse Sør-Øst, viser informasjon NRK har innhentet. De har hatt mulighet til å hente ut pasientdata til 2,8 millioner nordmenn.



Anne Cecilie Remen
Journalist

Line Tomter
Journalist

Publisert 3. mai 2017 kl. 06:37
Oppdatert 3. mai 2017 kl. 10:23

Artikkelen er mer enn ett år gammel.

Itseforetak. Over 2,8 millioner nordmenn hører til her. Alt av gret på dataservere. Nå skal driften av infrastrukturen flagges ut til

Bergit Sønstebo Svendsen
@bergit
Journalist

Adrian Nyhammer Olsen
@nyhammerolsen
Journalist

Publisert 20. mai kl. 17:00

Varsel om overtred Statens vegvesen

Datatilsynet har varslet Statens vegvesen om overtredelsesgebyr på 1,6 millioner kroner. Tilsynet har vurdert at personopplysningssikkerheten i datasystemene som blir brukt i grunnskolen i kommunen har vært mangelfull.

[Lover og regler](#) / [Sentrale avgjørelser](#) / 2019

Endelig vedtak om gebyr til Bergen kommune

Datatilsynet har sendt endelig vedtak til Bergen kommune om et overtredelsesgebyr på 1,6 millioner kroner. Tilsynet har vurdert at personopplysningssikkerheten i datasystemene som blir brukt i grunnskolen i kommunen har vært mangelfull.



Oslo

overtredsgebyr på 500 000 kroner for å ha lagret pasientopplysninger utenfor journalsystemet ved kommunens sykehjem/helsehus fra 2007 til november 2018.



Spørsmål?



Oslo

Takk for oppmerksomheten!

- ▶ Ta kontakt:
- ▶ Linda Mari Knutsen: linda.mari.knutsen@byr.oslo.kommune.no
- ▶ Henrik Lindgren Jensen: henrik.jensen@byr.oslo.kommune.no