Personvern – et lederansvar

Bjørn Erik Thon | direktør

11.02.2019

Datatilsynet

Personvern anno 2019

11.02.2019

Teknologi og internasjonalisering

- Alt er digitalt, alt kan deles og alt kan gjenbrukes
  - 3,5 millioner Google-søk per minutt, 1,8 millioner snaps og 70017 timer film på Netflix
- Mennesker fases ut av beslutninger
  - Algoritmer, kunstig intelligens, automatiserte avgjørelser
  - Kunstig intelligens = ett sekund menneskelig hjerneaktivitet
- Personvernverdenen er internasjonal
  - Facebook, Google, Amazon, Uber, og Telenor, Schibsted og Helse Sør-Øst

Den gamle måten å tenke personvern på

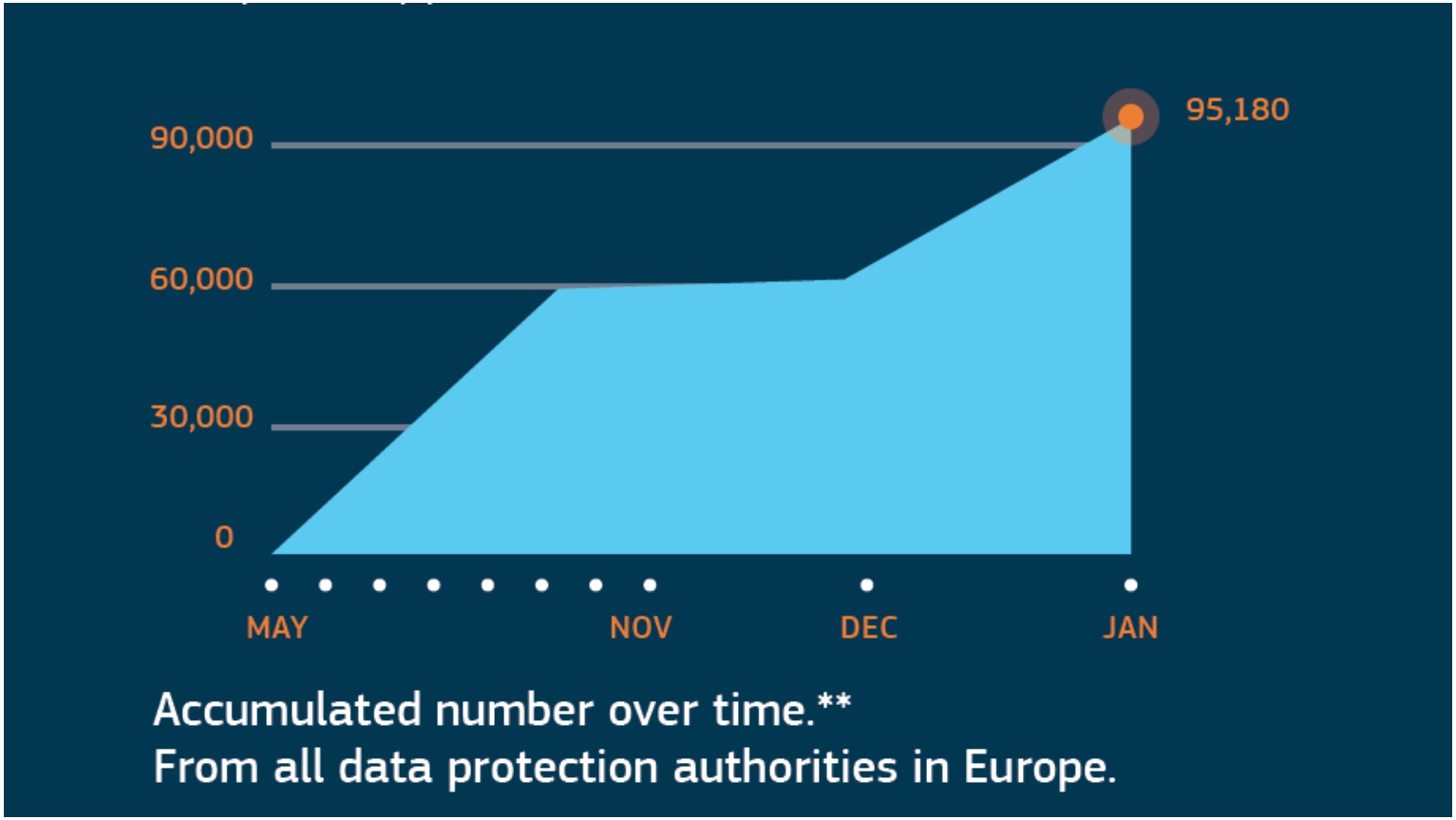
- Konsesjoner og forhåndstillatelser fra Datatilsynet
- Minst mulig registrering av data
- Ingen deling av data
- Personvern og informasjonssikkerhet er noe virksomhetene tar med «helt på slutten» av en utviklingsprosess, hvis de husker det
- Personvern er noe datafolk holder på med

Den nye måten å tenke personvern på

- Folk forventer at dataene deres blir brukt
- Fra ingen bruk av data, til *riktig bruk* av data
- Personvern må bygges inn helt fra starten av
- Godt informerte innbyggere med stor selvbestemmelse og bedre rettigheter balanserer makt

Statistikk fra EU: tall fra det første halvåret med GDPR

Antallet mottatte klager øker fra måned til måned



Klagene gjelder i hovedsak

These are the activities in which most complaints have been reported so far.

Telemarketing

Promotional e-mails

Video surveillance/ CCTV

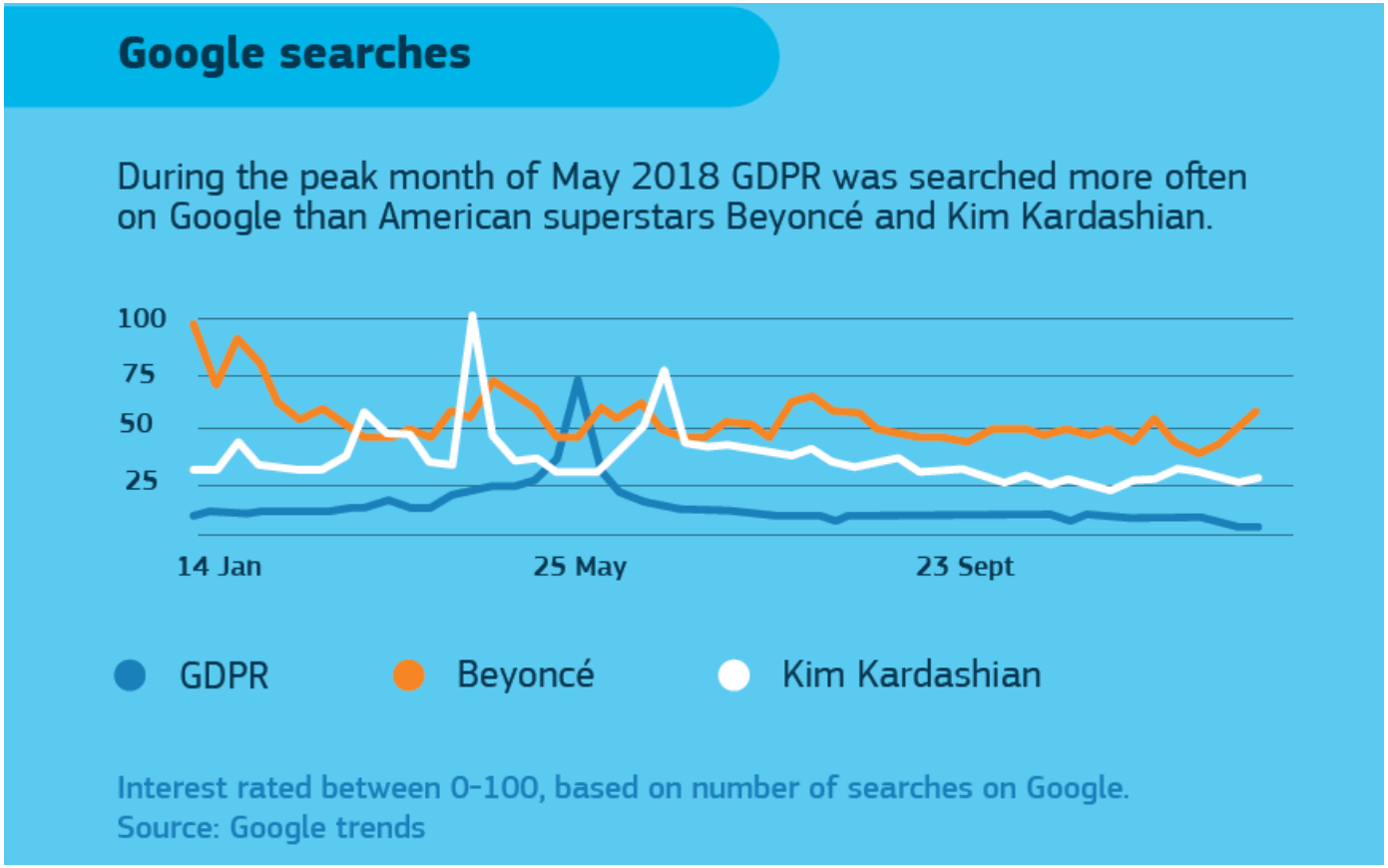
De første bøtene under GDPR

A social network operator for failing to secure users' data **EUR 20,000**

Sports betting café for unlawful video surveillance **EUR 5,280**

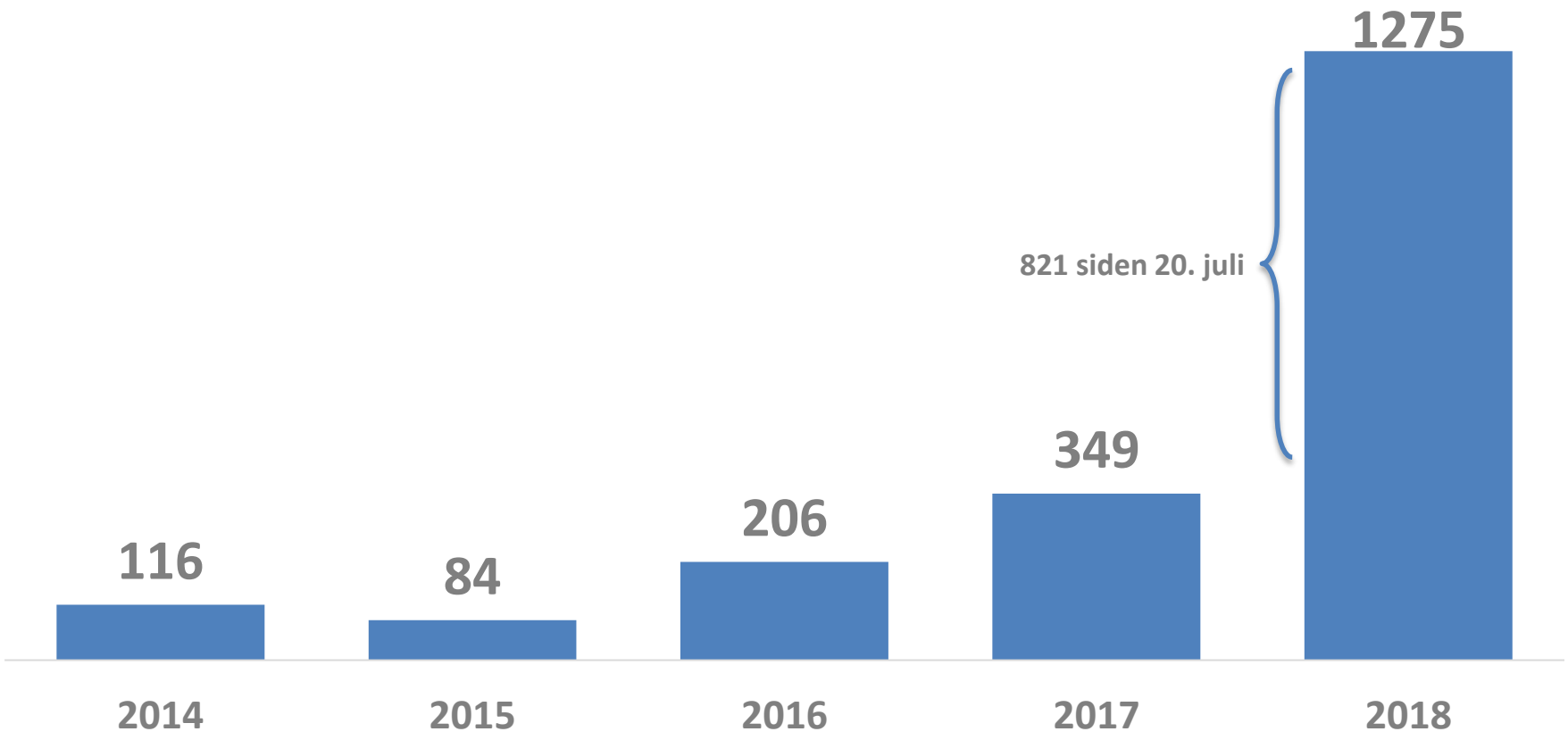
Google for lack of consent on Ads **EUR 50,000,000**

Stor oppmerksomhet om nytt regelverk

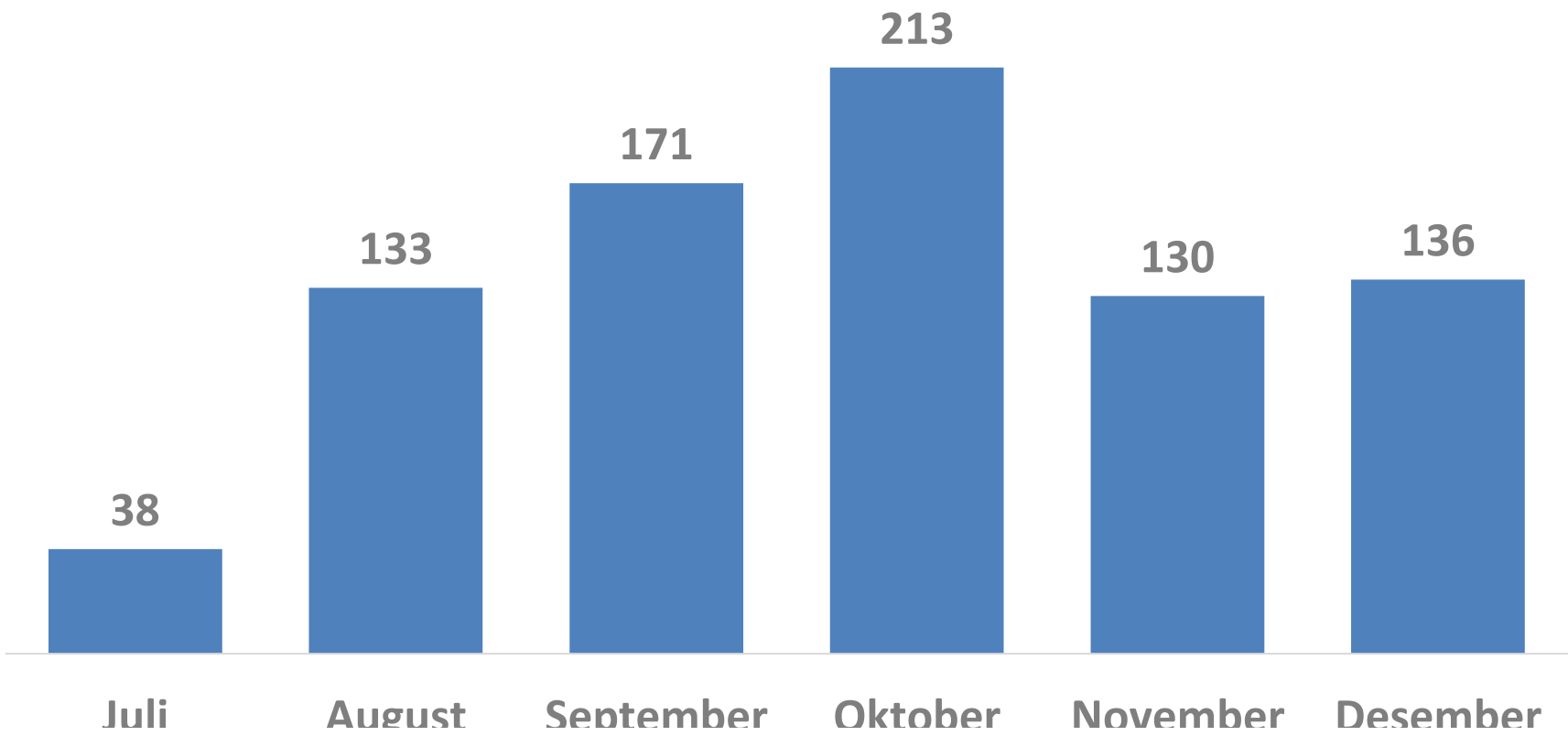


Norske forhold: Avviksmeldinger

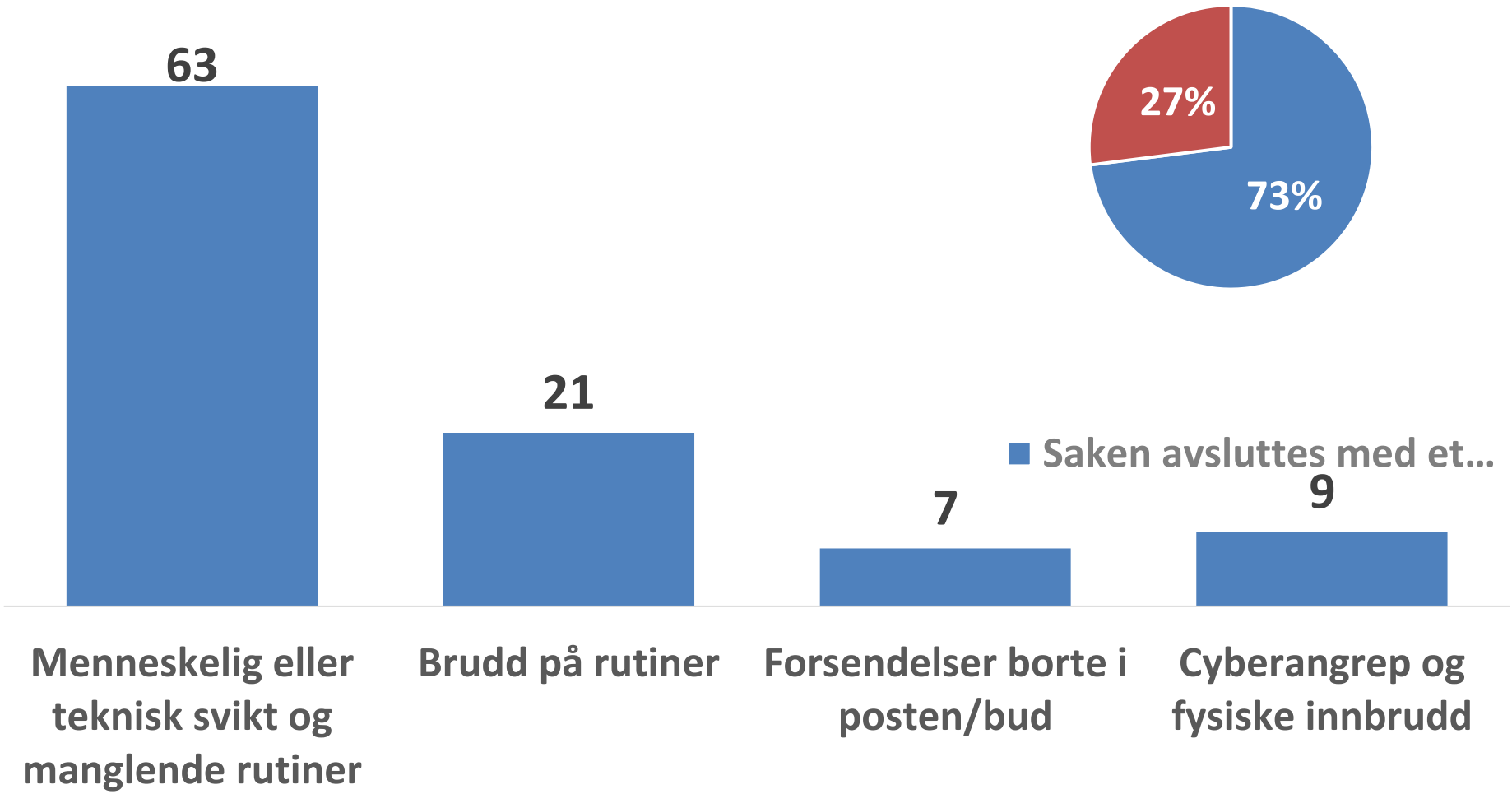
Kraftig vekst i antall avviksmeldinger etter 20. juli 2018



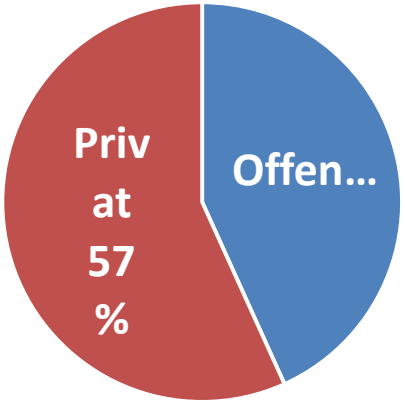
Avviksmeldinger siden 20.7.2018



Hvilke feil blir gjort – tall i prosent



Hvem melder avvik pr



Datatilsynets posisjon

Magasinet HELSE 2013-02.pdf

https://helse-midt.no/Documents/Magasinet_HELSE/Magasinet%20HELSE%202013-02.pdf

Apps | eyeWnder - Web Ad | forordningen | Statsbudsjettet | 25 Best Country and | 100 Essential America | M360 - Opoint techn | New Tab | European Data Prote | Nythun Høyfjellstue | Prop. 1 S (2018–2019

Av: BJØRN ERIK THON, direktør i Datatilsynet

Datatilsynets krav til nasjonalt helseregister:

– Svært god styring av tilgangen

Datatilsynet er for et faks-fritt helsevesen, for innovasjon, for bruk av mer og bedre IKT, for deling av pasientinformasjon og for samhandling i helsesektoren.

– Uten svært god styring helseregister trolig str krav til et privatliv, skr kommentaren til inter

«Årsaken til at det har stått dårlig til med IKT i helsevesenet, har ikke vært dagens lovgivning eller Datatilsynet, men en sektor som hang etter i IKT-utviklingen. Jeg vil derfor først fastslå dette: Datatilsynet er for et faks-fritt helsevesen, for innovasjon, for bruk av mer og bedre IKT, for deling av pasientinformasjon og for samhandling i helsesektoren.

Pasientbehandling handler om tillit. Pasienten må ha tillit til at legen har tilgang til all relevant informasjon og kan gi den aller beste behandlingen. Men for at pasienten skal gi all informasjon, må hun ha tillit til at legen respekterer sin taushetsplikt. Litt spissformulert kan vi si at legens taushetsplikt ikke lenger kan garanteres når pasientopplysningene legges inn i en journal på et sykehus. Dagens tilgangsstyring i helsevesenet er ikke god nok og gjør at helsepersonell kan se pasientopplysningene også hos pasienter de ikke behandler. Dette er et alvorlig problem.

Tilgangsstyringen har blitt bedre. Det pågår også flere interessante prosjekter på området. Det mest interessante er «Én innbygger - én journal». Tanken er tilforlatelig. Her er noen forutsetninger som må på plass for at et slikt prosjekt kan aksepteres fra et personvernståsted:

- Svært høy sikkerhet. Faren for [illegible] må ikke undervurderes. Ingen systemer er 100% sikre, og store, kompliserte systemer er også sårbare. De stadige problemene med Altinn er et eksempel.

- God tilgangsstyring. Fra Datatilsynets side er god tilgangsstyring en nøkkel til aksept. Uten et svært godt

- Logging av oppslag i journal, logganalyse og innsyn i hvem som har gjort oppslag. Ved å innføre slike tiltak og rettigheter vil den enkelte selv kunne sjekke hvem som har gjort oppslag i journalen.

- Innebygd personvern. Personvern må bygges inn i de tekniske løsningene fra starten, f. eks. innsynsrett, oppslag og god logganalyse.

Det ligger store personvernmessige utfordringer i forslaget. Jeg håper helseministeren tar i mot min invitasjon til tett dialog med Datatilsynet i alle faser av utviklingen.»

Grensegang og milepæler

hverdagen for pasienter og

[illegible]orge.no gir deg en [illegible]e helsehverdag

[illegible] du bruke enkle digitale verktøy som gjør det lett [illegible] i helsevesenet.
For eksempel på www.helsenorge.no, som driftes av Helsedirektoratet. Nedenfor ser du utdrag fra hjemmesiden, med en oversikt over selvbetjeningsmuligheter som finnes.

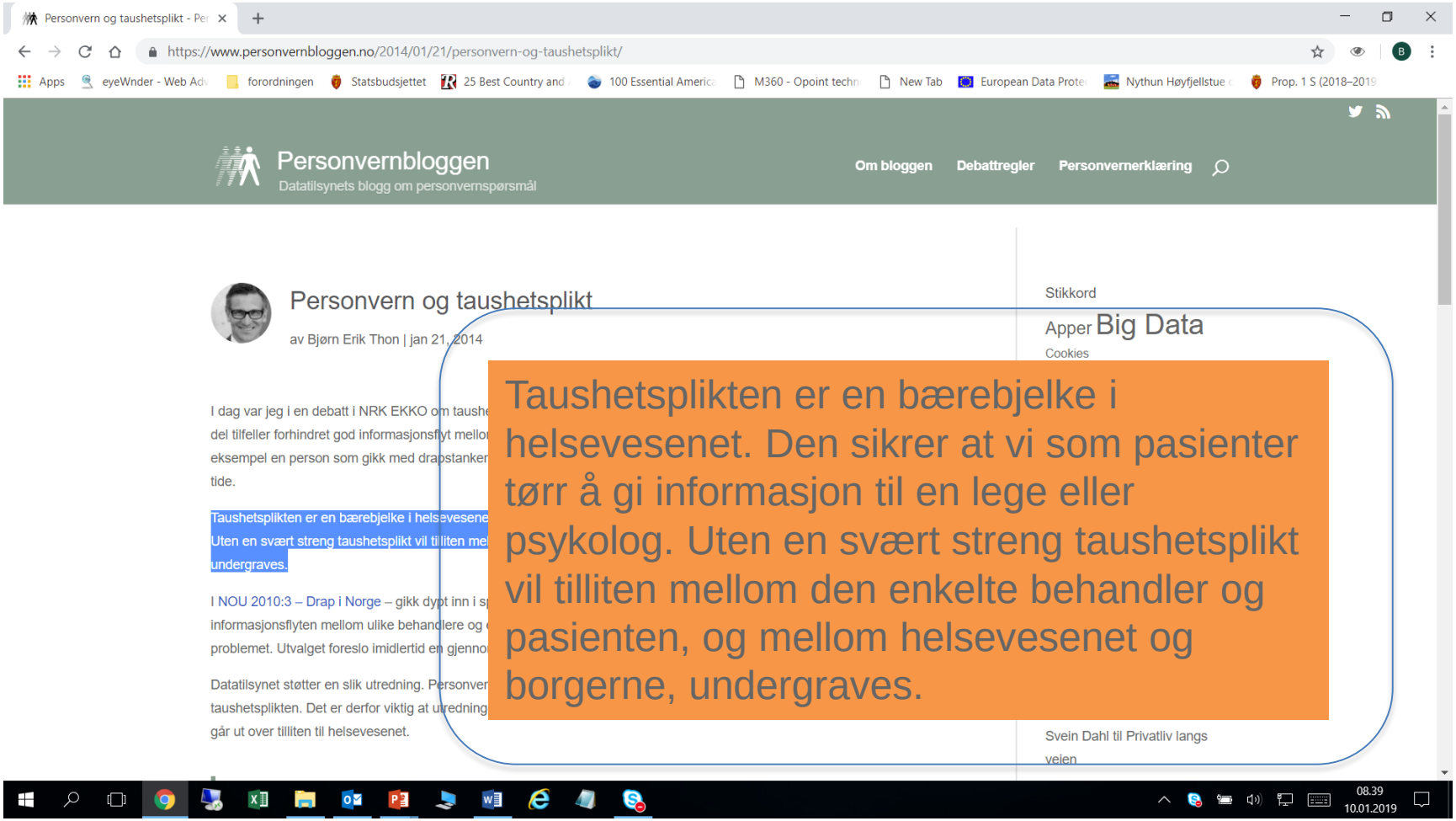
Mine egenandeler: Her finner du egenandeler som er registrert på deg under egenandelstak 1.

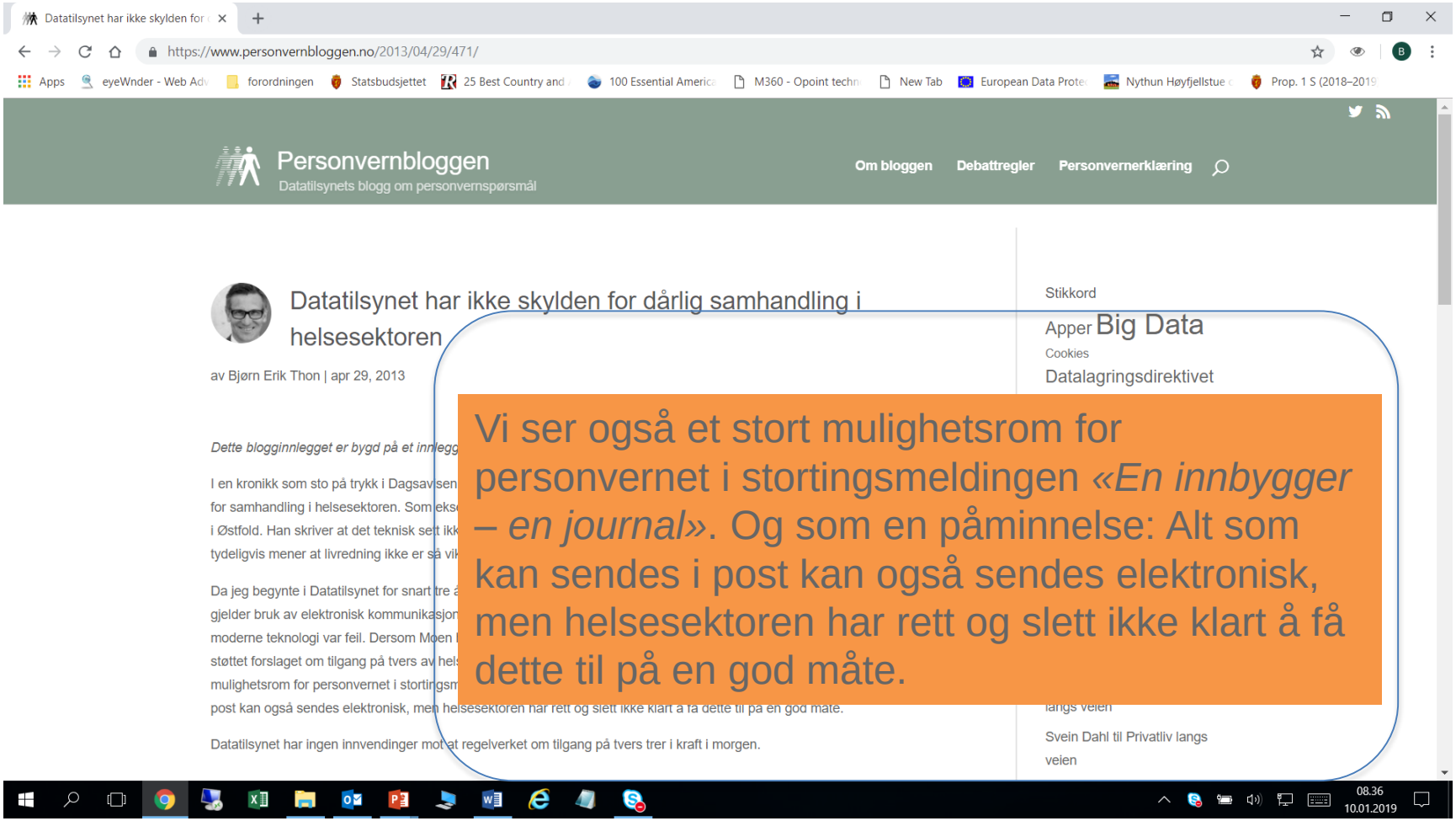
e-resept: Nå får du e-resept over hele landet. Det innebærer at legen sender resepten elektronisk, direkte til apoteket.

Mine vaksiner: Mine vaksiner gir deg mulighet til å skrive ut et vaksinasjonskort på norsk og engelsk. Du kan også se vaksinasjonsstatus for deg selv og dine barn.

08.16
10.01.2019

For dette handler ikke om proteiner og enzymer. Det handler om deg og meg, om oss. Vi må derfor få denne debatten ut av fagmiljøene, og inn i brede samfunnslag, inn i politikken. Da kan vi få en fredelig og fin revolusjon der folket er med, ikke mot. Og vi må begynne med et bredt utvalg, av genetikere, filosofer, jurister og andre kloke mennesker, som skal peke ut en vei videre.


Personvern og taushetsplikt - Per
https://www.personvernbloggen.no/2014/01/21/personvern-og-taushetsplikt/
Personvernbloggen
Datatilsynets blogg om personvernspørsmål
Om bloggen
Debattregler
Personvernerklæring
Personvern og taushetsplikt
av Bjørn Erik Thon | jan 21, 2014
I dag var jeg i en debatt i NRK EKKO om taush
del tilfeller forhindret god informasjonsflyt mello
eksempel en person som gikk med drapstanker
tide.
Taushetsplikten er en bærebjelke i helsevesene
Uten en svært streng taushetsplikt vil tilliten me
undergraves.
I NOU 2010:3 – Drap i Norge – gikk dypt inn i s
informasjonsflyten mellom ulike behandlere og
problemet. Utvalget foreslo imidlertid en gjenno
Datatilsynet støtter en slik utredning. Personver
taushetsplikten. Det er derfor viktig at utredning
går ut over tilliten til helsevesenet.
Stikkord
Apper Big Data
Cookies
Svein Dahl til Privatliv langs veien
Taushetsplikten er en bærebjelke i helsevesenet. Den sikrer at vi som pasienter tørr å gi informasjon til en lege eller psykolog. Uten en svært streng taushetsplikt vil tilliten mellom den enkelte behandler og pasienten, og mellom helsevesenet og borgerne, undergraves.
08.39
10.01.2019


Datatilsynet har ikke skylden for
https://www.personvernbloggen.no/2013/04/29/471/
Personvernbloggen
Datatilsynets blogg om personvernspørsmål
Om bloggen
Debattregler
Personvernerklæring
Datatilsynet har ikke skylden for dårlig samhandling i helsesektoren
av Bjørn Erik Thon | apr 29, 2013
Stikkord
Apper Big Data
Cookies
Datalagringsdirektivet
Svein Dahl til Privatliv langs veien
Vi ser også et stort mulighetsrom for personvernet i stortingsmeldingen «En innbygger – en journal». Og som en påminnelse: Alt som kan sendes i post kan også sendes elektronisk, men helsesektoren har rett og slett ikke klart å få dette til på en god måte.
08.36
10.01.2019

Blodsukkermåling

- *Takk for eposten din, der du forteller en sterk historie om hvordan barnet din forhindres fra å delta i normale aktiviteter på grunn av sykdommen sin. Jeg kan ikke helt forstå hvorfor du legger skylden på oss for at hun ikke kan bruke Dexcom, ettersom vi ikke har noen beslutningsmyndighet når det gjelder slik bruk. Men uavhengig av det: historien din har gjort sterkt inntrykk på meg, og jeg har brukt formiddagen til å forsøke å nøste opp i hva som har skjedd, og hva som må til for at det skal gis tillatelse til bruk av denne typen medisin-teknisk utstyr. Jeg vil derfor gjerne at du ringer meg for en prat, som kan jeg fortelle hvor saken står, og hva vi i Datatilsynet kan gjøre for at saken finner en god løsning.*

Hva sier egentlig GDPR?

- Det er et europeisk regelverk, som skal praktiseres likt i alle EU/EØS-land
- Det er et svært generelt regelverk, som gjelder alle sektorer, alle bransje, private og offentlige aktører
- Det er et store behov for veiledning, fortolkninger og utvikling av praksis
- Det er også handlingsrom for nasjonal særlovgivning

Hva er personvern?

- Behandlingsgrunnlag, som kan være lov, forskrift, vedtak gitt med hjemmel i lov eller samtykke
- Konfidensialitet; at dataene er sikre
- Tilgjengelig; at de som skal ha tilgang til dataene faktisk får det
- Integritet; at vi kan stole på dataene
- Åpenhet om hva som samles inn, og hva dataene brukes til

Hva handler denne debatten om?

- Personvern
- Informasjonssikkerhet
- Pasientsikkerhet
- Taushetsplikt
- Tilgang på tvers
- Skylagring
- Forskning og publisering
- Anskaffelseskompetanse av medisinsk-teknisk utstyr
- Etablering av registre
- Utredning av, eller mangel på utredning av personvernkonsekvenser (DPIA)
- Lokale og nasjonale problemstillinger
- Og deler av debatten handler om interne forhold på OUS

Et forsøk på å rydde i problemstillingene

- Hvilke av de nevnte utfordringene skyldes GDPR?

- Hvis regelverket tolkes ulikt i ulike land, er det to alternativer:
  - «Vi» tolker loven feil
  - De andre tolker loven feil

- Hvordan kan vi løse dette?
  - Vi finner ut av det
  - Vi spør våre europeiske kollegaer, og begynner med de nordiske
  - Vi går en ny runde på lovtolkningen

Et forsøk på å rydde i problemstillingene

- GDPR er et helt nytt regelverk, som ikke er «ferdig tolket»

- Men dette er bare ett av flere viktige regelsett, og vi opplever at hva som reguleres av hvilke regler, sauses sammen

- Hva er personvern, hva er taushetsplikt, hva er informasjonssikkerhet, hva er forskning, hva er anskaffelser, hva er helsehjelp?

Pasientsikkerhet og personvern anno 2019

- Vi har et regelverket som møter en ny teknologisk utvikling, i form av stordata, kunstig intelligens, persontilpasset medisin og skytjenester, for å nevne noe

- Og hvordan nærmer vi oss dette?

- Vi er på langt nær «ferdig tenkt» på dette området

Aktørbildet – hvem har ansvaret for fortolkning av regelverket?

- OUS
- Helsetilsynet
- Helsedirektoratet
- Helse- og omsorgsdepartementet
- Sykehuspartner
- Datatilsynet
- Direktoratet for e-helse

Og sikkert andre interessenter…

- Pasientorganisasjoner
- Pasientombud
- Brukerombud

Skytjenester

- Sannsynligvis kan alle typer data lagres i skyløsninger
- Lærdom fra Helse Sør-Øst –saken (Bulgaria-saken)
  - Risikovurderinger
  - Eierskap til prosesser
  - Sikkerhetsledelse
- Lagringssted, og type data må inngå i vurderingen

Publisering

- Kan man publisere pseudonyme data?
- Hva er pseudonyme data…….
- ….og hva er avidentifiserte data, direkte identifiserbare data, aggregerte data, anonyme data og data som er anonyme på forskers hånd?
- Begrepet brukes ulikt i ulike lover, ikke samme definisjon i GDPR som i norsk særlovgivning

Publisering – hva kan Datatilsynet gjøre?

- Hva er begrunnelsen for påstanden om at man ikke kan publisere forskningen sin?

- Vi må få fram begrunnelsen, og plassere ansvaret der det hører hjemme

- Vi har gjerne dialog med de involverte, de som «eier» fortolkningen, og det inkluderer oss selv

Noen (selvfølgelige) generelle betraktninger

- Vi må opp av skyttergravene
- Vi må lytte til hverandre, og ikke tillegge hverandre motiver vi ikke har
- Vi må snakke sammen
- Vi må respektere at vi har ulike roller
- Vi har en fellesnevner i *tillit*

Hva kan vi gjøre med de øvrige utfordringer?

- Vi må få problemstillingene opp på bordet, og fra nå av, ikke gjennom avisens spalter

- Vi må skaffe oversikt over hvor de ulike diskusjonene hører hjemme, og hvem som er rette adressat til å bidra til gode løsninger
  - Rundebordskonferanser
  - Veiledningsmøter
  - Veiledere
  - Rundskriv
  - Bransjenorm

Hva kan vi gjøre?

- Reglene må tolkes likt, det er veldig uheldig at ulike HF tolker reglene ulikt
- Kanskje må også regelverket utvikles videre, eller presiseres, eller tolkes annerledes enn vi har gjort til nå
- Vi har avtalt møte med Helse- og omsorgsdepartementet, vi vil fortsette dialogen med OUS og andre HF'er, om det er ønskelig
- Personvern, og Datatilsynet, må og vil være en del av løsningen