Nye personvernregler fra mai 2018, hva nå?

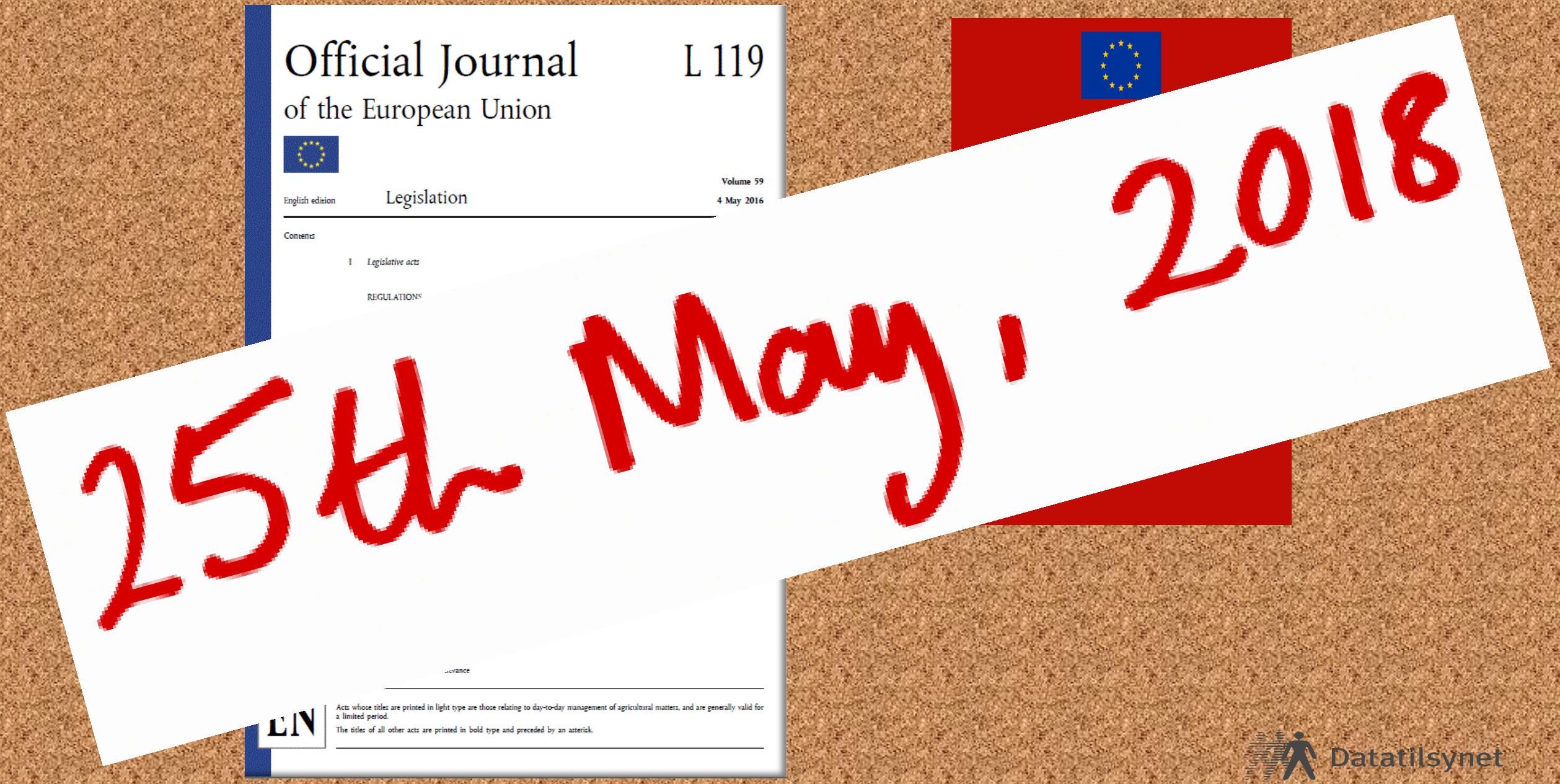
VOFO

8. Januar 2018

Hallstein Husand - Datatilsynet

Datatilsynet

atatilsynet


Official Journal
of the European Union
L 119
English edition
Legislation
Volume 59
4 May 2016
Contents
I Legislative acts
REGULATIONS
Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.
The titles of all other acts are printed in bold type and preceded by an asterisk.
25th May, 2018
Datatilsynet

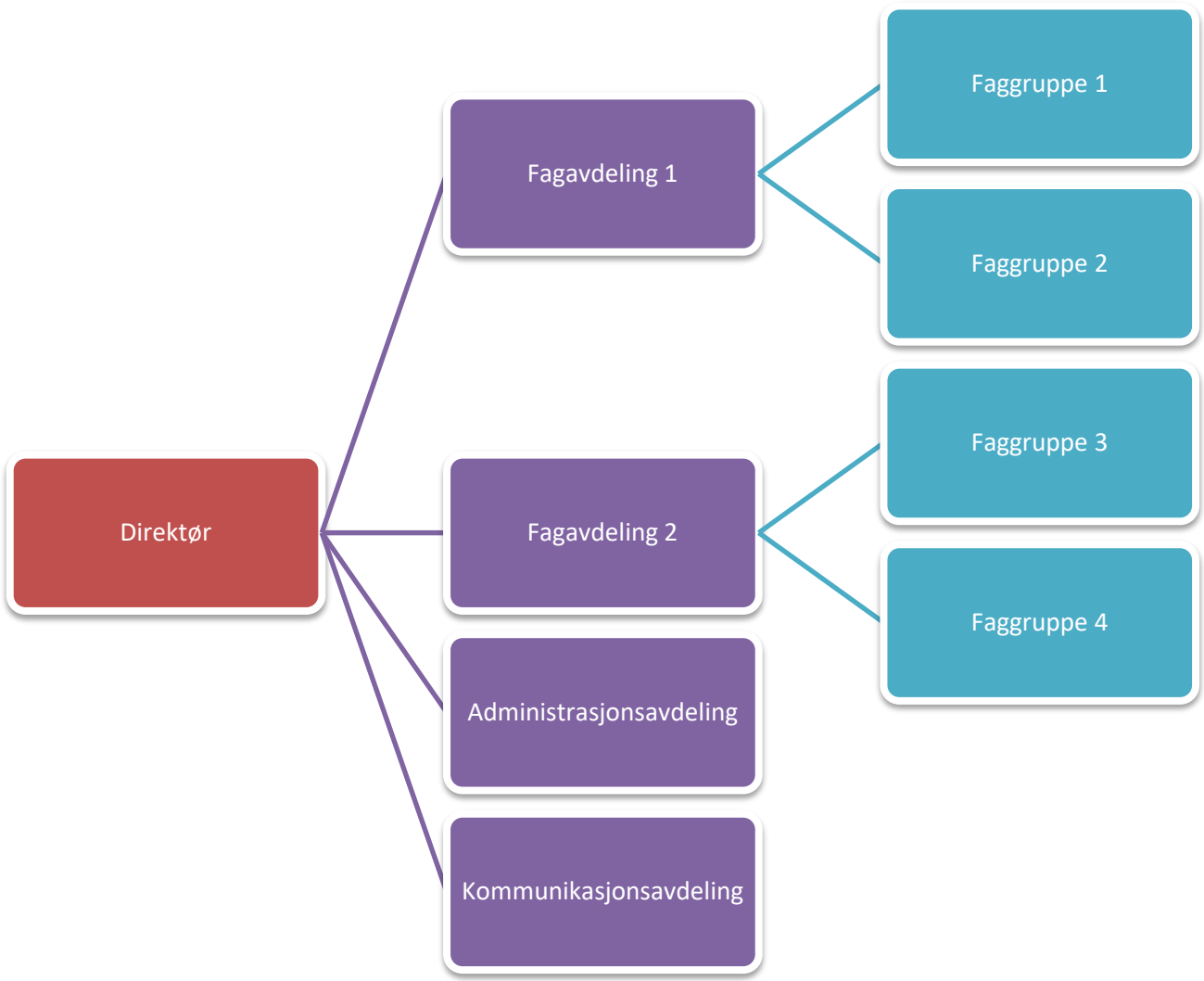
Agenda

- Bittelitt om Datatilsynet
- Hva er personvern og personopplysninger
- Bakgrunn for nye personvernregler
- De viktigste endringene fra i dag til 2018
- Hva nå?
  - ✓ våre forventninger og
  - ✓ råd om veien videre

To ord om Datatilsynet

Datatilsynet

- Opprettet 1980, lokalisert i Oslo
- I underkant av 50 medarbeidere
- Særlig uavhengig forvaltningsorgan under KMD
- To roller – forvaltning og ombud
- Regelverk:
  - ✓ Personopplysningsloven
  - ✓ Helseregisterloven
  - ✓ Helseforskningsloven
  - ✓ Politiregisterloven
  - ✓ Lov om Schengen informasjonssystem
- Personvernnemnda er klageorgan for våre vedtak



Litt om person(opplysnings)vern og behandling av personopplysninger

Hva er person(opplysnings)vern?

”Den enkeltes rett til å ha kontroll med egne personopplysninger”

- **Selvbestemmelse**
  - ✓ rett til selv å bestemme hvilke opplysninger som skal brukes, av hvem og til hvilke formål.

- **Informasjon**
  - ✓ hvis man ikke har rett til å samtykke, har man i det minste rett til å vite hvilke opplysninger som brukes, av hvem og til hvilke formål

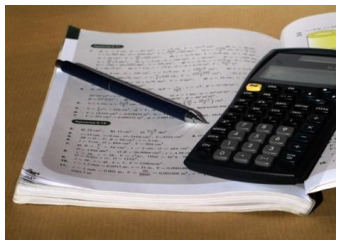
Personopplysninger er mer enn du kanskje tror….

Personopplysninger – hva er det?

Hallstein Husand
Sogstiveien 68B
1446 Drøbak
Tlf 908 21 845
hhu@datatilsynet.no

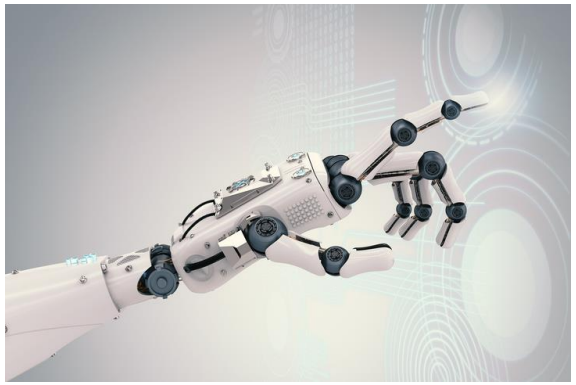
Oppvokst i Sømna, gift og 3 voksne barn

Datatilsynet
Tollbugata 3
0034 Oslo
datatilsynet.no
personvernbloggen.no
Twitter.com/datatilsynet



Fødselsnummer: `13087846271`
Telefonnummer: `22396900`
IP-adresse: `195.159.103.82`
Bilnummer: `BL 23456`
Bluetooth MAC: `17:35:52:78:4B:CA`
Wi-Fi-adresse MAC: `12:44:32:45:7B:C9`
Autpass-brikke-ID: `748392098327839 4`

Og utviklingen raser videre….



Litt om bakgrunnen for nye regler

Hvorfor nye regler for personvern, trenger vi det?

Nye rammer for behandling av personopplysninger! (EU 2016/679)

- Vedtatt i 2016 og vil tre i kraft 25.05.2018
- Hvorfor?
  - ✓ Styrke den europeiske borgers rettigheter
  - ✓ Gjøre det lettere å utveksle personopplysninger over landegrenser
  - ✓ Styrke tilliten til digitale tjenester
  - ✓ Sikre samarbeid mellom personvernmyndigheter
- Hvordan?
  - ✓ Gjennom en forordning
  - ✓ Erstatter nasjonal lovgivning
  - ✓ Direkte gjeldende i EU/EØS
  - ✓ Begrenset spillerom for nasjonale tilpasninger

Nye rammer for behandling av personopplysninger! (EU 2016/679)

- Vedtatt i 2016 og vil tre i kraft 25.05.2018
- Hvorfor?
  - ✓ Styrke den europeiske borgers rettigheter
  - ✓ Gjøre det lettere å utveksle personopplysninger over landegrenser
  - ✓ Styrke tilliten til digitale tjenester
  - ✓ Sikre samarbeid mellom personvernmyndigheter
- Hvordan?
  - ✓ Gjennom en forordning
  - ✓ Erstatter nasjonal lovgivning
  - ✓ Direkte gjeldende i EU/EØS
  - ✓ Begrenset spillerom for nasjonale tilpasninger

Nye rammer for behandling av personopplysninger! (EU 2016/679)

- Vedtatt i 2016 og vil tre i kraft 25.05.2018
- Hvorfor?
  - ✓ Styrke den europeiske borgers rettigheter
  - ✓ Gjøre det lettere å utveksle personopplysninger over landegrenser
  - ✓ Styrke tilliten til digitale tjenester
  - ✓ Sikre samarbeid mellom personvernmyndigheter
- Hvordan?
  - ✓ Gjennom en forordning
  - ✓ Erstatter nasjonal lovgivning
  - ✓ Direkte gjeldende i EU/EØS
  - ✓ Begrenset spillerom for nasjonale tilpasninger

Nye rammer for behandling av personopplysninger! (EU 2016/679)

- Vedtatt i 2016 og vil tre i kraft 25.05.2018
- Hvorfor?
  - ✓ Styrke den europeiske borgers rettigheter
  - ✓ Gjøre det lettere å utveksle personopplysninger over landegrenser
  - ✓ Styrke tilliten til digitale tjenester
  - ✓ Sikre samarbeid mellom personvernmyndigheter
- Hvordan?
  - ✓ Gjennom en forordning
  - ✓ Erstatter nasjonal lovgivning
  - ✓ Direkte gjeldende i EU/EØS
  - ✓ Begrenset spillerom for nasjonale tilpasninger

Nye rammer for behandling av personopplysninger! (EU 2016/679)

- Vedtatt i 2016 og vil tre i kraft 25.05.2018
- Hvorfor?
  - ✓ Styrke den europeiske borgers rettigheter
  - ✓ Gjøre det lettere å utveksle personopplysninger over landegrenser
  - ✓ Styrke tilliten til digitale tjenester
  - ✓ Sikre samarbeid mellom personvernmyndigheter
- Hvordan?
  - ✓ Gjennom en forordning
  - ✓ Erstatter nasjonal lovgivning
  - ✓ Direkte gjeldende i EU/EØS
  - ✓ Begrenset spillerom for nasjonale tilpasninger

Hva skjer a’ (i Norge)?

iapp News Connect Train Certify Resources Conferences Join

Survey: 61 percent of companies have not started GDPR implementation

Jun 7, 2017 Save This

Ryan Chiavetta

Is your company getting ready for the General Data Protection Regulation? If so, it might be in the minority. That's because, according to research conducted by TrustArc, the answer is likely no.

Why the name cha

Babel also discussed his company's rebranding, moving fro TRUSTe to TrustArc, w Privacy Tech. "As we th about who we were," he explained, "th were providin

Arc, formerly known as mpanies across several panies broke down into

IT-sikkerhetssjef i Atea, Thomas Tømmernes.

De som ikke har fått med seg dette risikerer bøter på inntil 20 millioner euro

Bare to prosent av bedriftsledere har satt seg inn i EUs nye personvernregler som innføres til neste år.

TU STORY LABS Dette er en annonse. Journalistene i Tu.no er ikke involvert i produksjonen.

TIKK, TAKK: Er du klar for EUs personvernforordning? Illustrasjon: iStock

Klokken tikker mot 25.05.18. Er du klar for GDPR?

HVA ANDRE MENER: EU vedtok i fjor ny personvernforordning som skal erstatte dagens personlovgivning. De fleste virksomheter vet lite eller ingenting om dette, et mindretall har startet arbeidet, og noen håper nok det går over, skriver kronikkforfatter.

TERJE WOLD, DND

Publisert: fredag 31. mars 2017, kl.00:15
Endret: 03. april 2017, kl.11:16

Norske bedrifter er dårlig forberedt på personvernlov

Én av fire selskaper er ikke forberedt på den nye personvernloven, viser en fersk undersøkelse.

Hva skjer hos myndighetene i Norge?

- Innlemmelse i EØS avtalen (Justisdepartementet/ EFTA)
- Innføring i norsk lov (Justisdepartementet/Kommunal og Moderniseringsdepartementet – høringsfrist var 15. oktober)
  - ✓ Ny personopplysningslov
  - ✓ Forordningen i sin helhet som Annex (inkorporasjon)
- Endelig Norsk oversettelse
- Kommentar utgave

- Datatilsynet
  - ✓ Eget internprosjekt
    - IKT
    - Juridisk
    - WEB (nytt nettsted introdusert i sommer)
    - Personvernombud
    - Kommunikasjon

  - ✓ Deltar i internasjonalt arbeid og bidrar til utredninger

Forordningen (GDPR), litt om hva og hvordan

Finne oversikt

- *Artikkel 1*
  - ✓ **Formål og mål**
- *Artikkel 2*
  - ✓ **Materielt virkeområde**
- *Artikkel 3*
  - ✓ **Geografisk virkeområde**
- *Artikkel 4*
  - ✓ **Definisjoner**
- *Artikkel 5*
  - ✓ **Prinsipper for behandling av personopplysninger**
- *Artikkel 6*
  - ✓ **Behandlingens lovlighet**

Bedre rettigheter for enkeltpersoner

Retten til å bli glemt og motsette seg profilering

Dataportabilitet

Bedre informasjon og oversikt

Klager kan rettes til Datatilsynet i landet man bor i

Nettjenester må innhente foreldres samtykke

Nye sanksjoner

Alle norske virksomheter får nye plikter

- Alle må finne ut hva regelverket betyr
- Nye rutiner er et ledelsesansvar
- Alle ansatte skal følge nye rutiner

«GDPR er ikke et nytt IKT prosjekt» – Torgeir Waterhouse IKT-Norge

Skjerpede plikter for virksomhetene

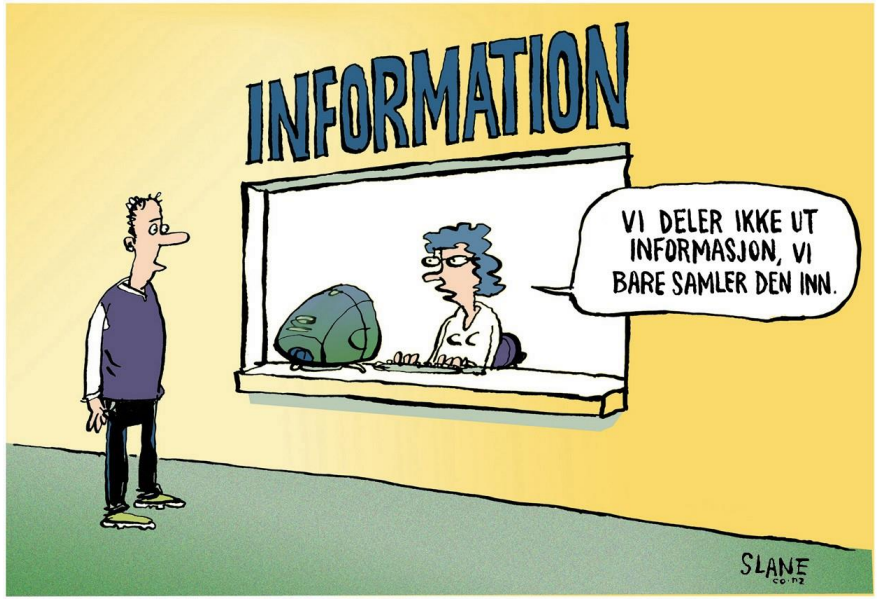
- **Tydeligere krav til informasjon og samtykke**
- **Innebygd personvern og personvern som standardinnstilling**
- **Vurdering av personvernkonsekvenser**
- **Forhåndsdrøftelser**
- **Obligatorisk med personvernombud**
- **Avvikshåndtering**
- **Bransjenormer og sertifisering**
- **Skjerpede plikter for databehandlere**
- **Dataportabilitet og automatiske avgjørelser**
- **Europeisk samarbeid**

Samtykke

- Et samtykke skal være frivillig, spesifikt, informert og utvetydig erklært
- Det må ikke være tvil om at den registrerte uttrykker sin vilje til å samtykke i behandlingen
  - Hva samtykke gjelder (behandlingen), hvem den behandlingsansvarlige er og formål med behandlingen.
  - Den registrertes inaktivitet/passivitet kan aldri kunne anses som et lovlig samtykke
    - Taushet, forhåndsavkrysset felter eller inaktivitet bør derfor ikke utgjøre samtykke

Alle skal ha en forståelig personvernerklæring

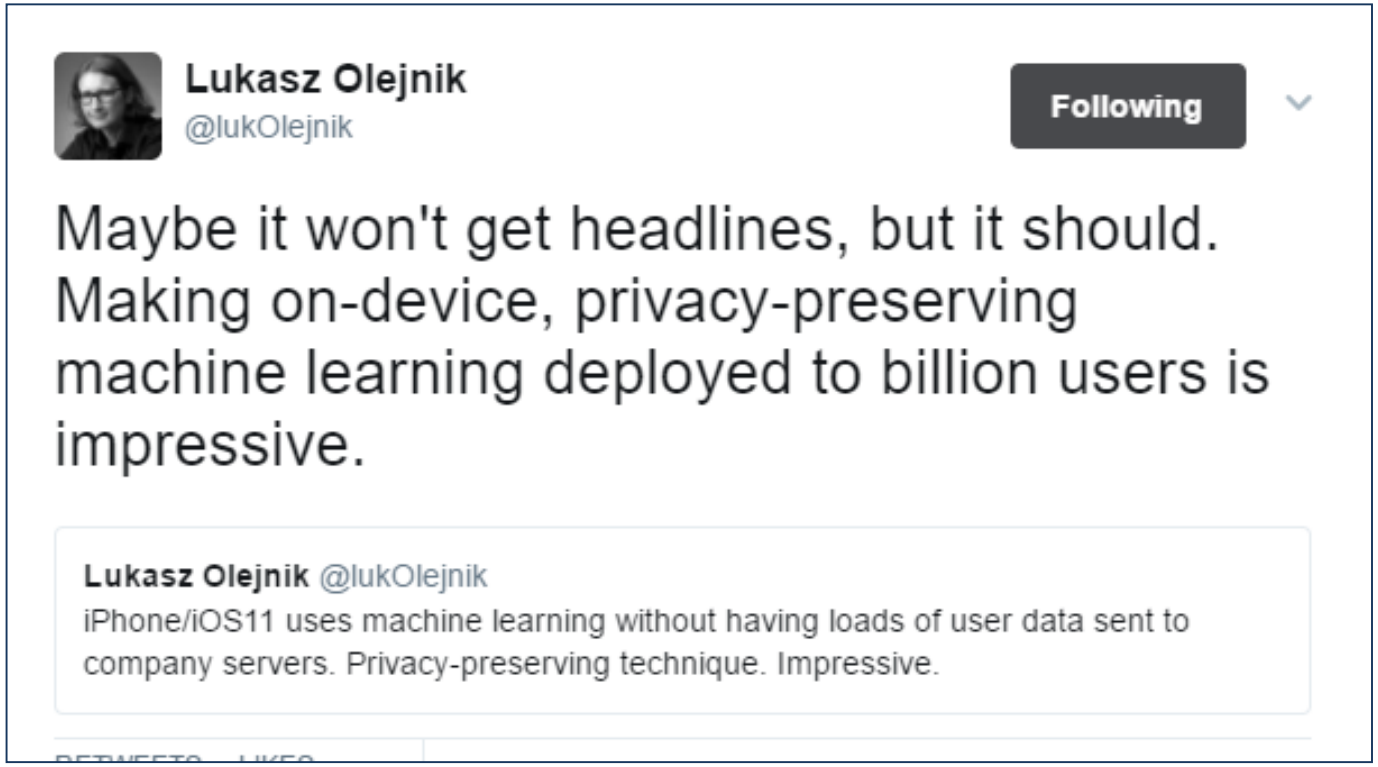
- Informasjonen skal være lett tilgjengelig
- Klart språk som er tilpasset leserens nivå
- Stilles krav til hvilke opplysninger som skal gis



Krav om innebygd personvern

Det minst personverninngripende alternativet som standard:

- mengde
- omfang
- lagringstid
- tilgjengelighet



Plikt til å vurdere risiko og personvernkonsekvenser

- Risikovurderinger skal alltid foretas som en del av internkontrollen
  - ✓ Identifiser behandlinger som vil kunne medføre en **høy risiko** for personvernet

- Hvis høy risiko, krav om å utføre en **vurdering av personvernkonsekvensene (DPIA)**

- I tilfelle man er i tvil anbefaler vi å utføre en DPIA.

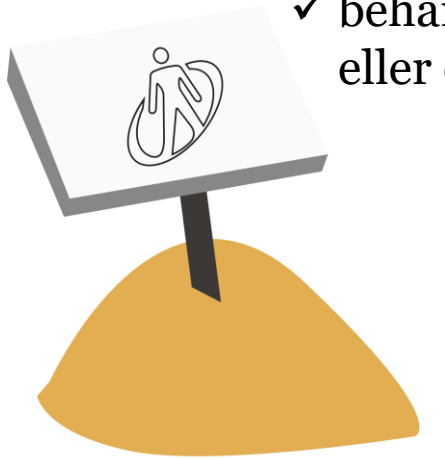
Fra forhåndskontroll til risikobasert *egenkontroll*

- Risikovurderinger skal alltid foretas som en del av internkontroll jf. art. 32(1)
  - ✓ Identifisere behandlinger som vil kunne medføre en **høy risiko** for personvernet
  - ✓ Der behandlingen vil kunne resultere i høy risiko, plikter behandlingsansvarlig/databehandler å gjennomføre en **vurdering av personvernkonsekvensene (DPIA)**
  - ✓ Den behandlingsansvarlige skal identifisere **risikoreduserende tiltak**
- Der risikoen ikke kan håndteres av den behandlingsansvarlig på en tilfredsstillende måte, skal forhåndsdrøftelser (*prior consultation*) igangsettes, jf. art 36
  - ✓ Gi råd
  - ✓ Bruke andre virkemidler (pålegg, sanksjoner)
  - ✓ Forby behandlingen

Personvernombud

Disse må ha ombud:

- Alle offentlige virksomheter (unntatt domstoler)
- Virksomheter som har som kjerneaktivitet å gjøre følgende i stor skala:
  - ✓ regelmessig og systematisk overvåke personer
  - ✓ behandle sensitive personopplysninger eller opplysninger om straffbare forhold

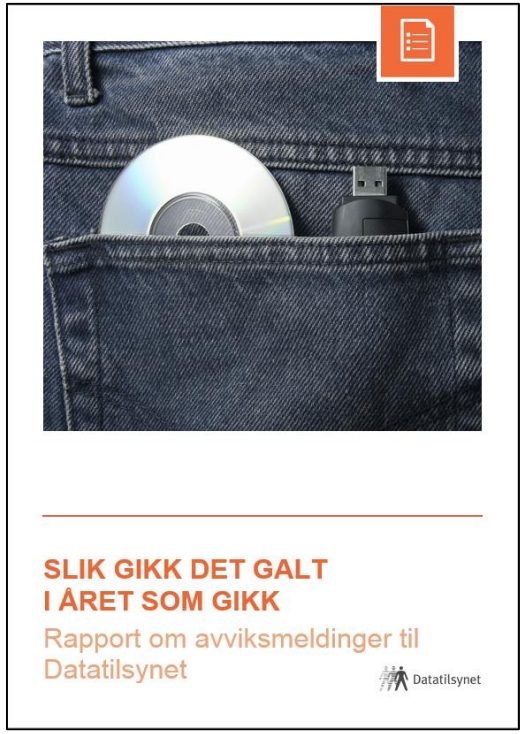


Strengere krav til personvernombudene

- Krav til kompetanse
- Skal involveres og rapportere til høyeste ledelsesnivå
- Ombudet skal ikke instrueres eller straffes
- Oppgavene omfatter å gi råd, overvåke etterlevelse og være kontaktpunkt

Alle får nye krav til avvikshåndtering

- Strengere regler enn i dag
- Melde avvik innen 72 timer
- Stilles krav til innholdet i avviksmeldingen
- De berørte skal varsles i klart språk



Bransjenormer og Sertifisering

- Medlemsland, tilsyn, European DataProtection Board (EDPB) og EU-Kommisjonen skal oppmuntre til utarbeidelse av bransjenormer.
- Sertifiseringsmekanismer
  - Segl og merker
  - Prosedyrer for å utstede sertifisering, basert på kriterier fra Datatilsynet eller EDPB
  - EDPB skal ha et offentlig register
  - En sertifisering gjelder for maks tre år, men kan fornyes eller trekkes t
  - Sertifiseringsorgan, akkreditert av Datatilsynet
    - Krav til organ som kan akkrediteres
  - Kommer veiledning fra Artikkel 29-gruppen

Databehandlere får nye plikter (art 28)

- Egne rutiner for behandling av personopplysninger – dokumentere etterlevelse
- Si ifra om instrukser er i strid med loven
- Underleverandører skal godkjennes
- Melde avvik til behandlingsansvarlig
- Behandle personopplysninger ihht databehandleravtale
- Kan bli erstatningspliktige

Nye «rettigheter»

- Dataportabilitet (art. 20)
  - Dersom man behandler personopplysninger basert på samtykke, kan den registrerte kreve å ta med seg opplysningene sine til en annen virksomhet.
    - ✓ Dersom det er teknisk mulig, kan den registrerte kreve at den behandlingsansvarlige sørger for å overføre opplysningene til den nye virksomheten.
    - ✓ Opplysningene skal være i et strukturert, allment brukt og maskinlesbart format.
    - ✓ Retten til dataportabilitet gjelder ikke for behandlinger som er nødvendige for å gjennomføre oppgaver i samfunnets interesse eller under offentlig myndighetsutøvelse.

- Automatiserte avgjørelser og profilering
  - Adgangen til å ta i bruk automatiserte avgjørelser, altså avgjørelser basert på algoritmer, er snevret inn etter de nye reglene.
  - Automatiserte avgjørelser (herunder profilering) som «har rettsvirkning eller på tilsvarende vis betydelig påvirker han/hun», er kun tillatt:
    - ✓ når det er nødvendig for å inngå eller for å gjennomføre en avtale med det registrerte,
    - ✓ når det er hjemlet i lov som samtidig stadfester tilfredsstillende garantier for personvernet eller
    - ✓ når det er basert på samtykke.

  - Sensitive personopplysninger kan kun brukes etter
    - ✓ samtykke
    - ✓ lovhjemmel
    - ✓ vesentlig offentlig interesse

Reglene gjelder også virksomheter utenfor Europa

- Alle som tilbyr varer eller tjenester til EU- eller EØS-borgere
- De som kartlegger EU- eller EØS-borgeres adferd på nett
- Virksomheter skal kunne forholde seg til en personvernmyndighet
- Den registrerte skal kunne klage i eget land
- Personvernmyndigheter skal samarbeide

Sanksjoner – overtredelsesgebyr (art. 83)

- Brudd på behandlingsansvarliges (også databehandleres) forpliktelser
  - ✓ 10 millioner euro, eller 2% årlig global omsetning
- Overtredelse av grunnprinsippene (inkludert samtykke)
  - ✓ 20 millioner euro, eller 4% av årlig global omsetning
- Overtredelse av påbud fra Datatilsynet
  - ✓ 20 millioner euro, eller 4% av årlig global omsetning

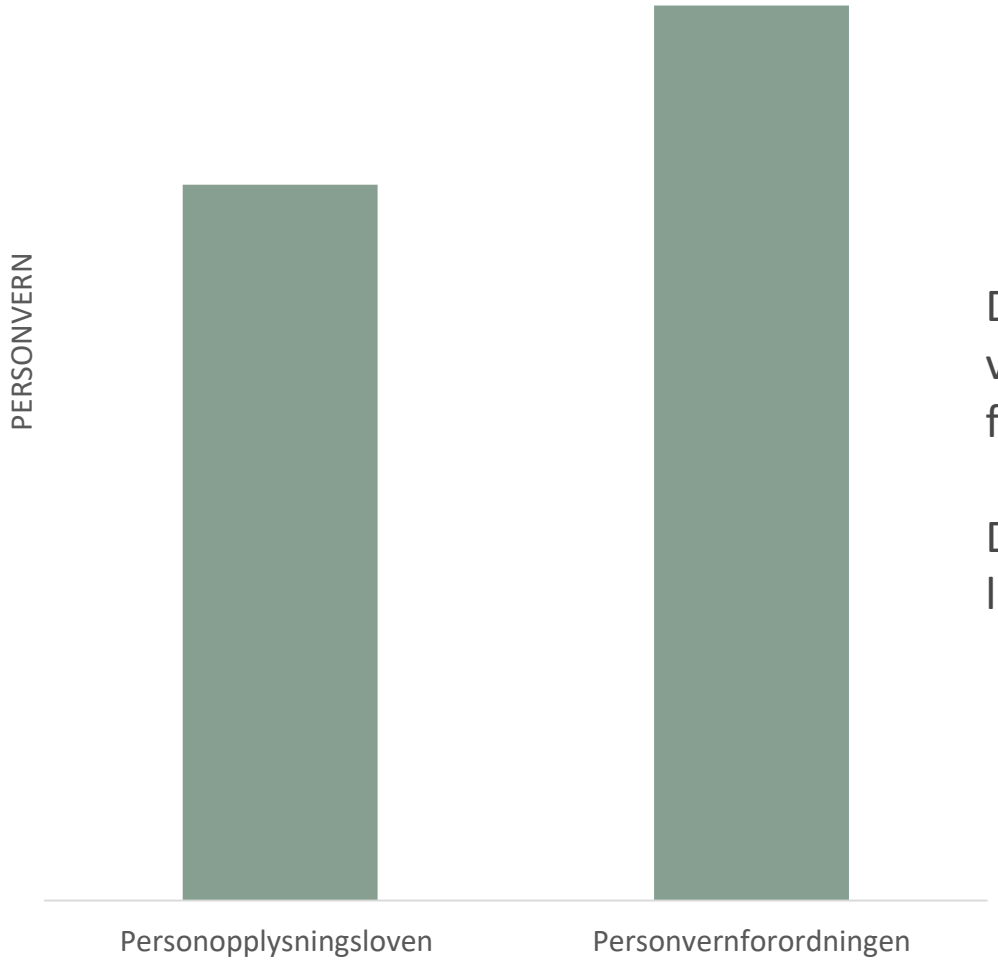
- For offentlige virksomheter
  - ✓ Ikke besluttet og skal avgjøres nasjonalt
  - ✓ I høring til ny lov er det foreslått at også offentlige virksomheter skal kunne ilegges overtredelsesgebyr, men da med kun faste summer (ikke %)

Hva nå da, der det for seint eller kanskje for tidlig?

Datatilsynets forventninger til dere…

1. At dere vet noe om hva personvern er
2. At dere vet hvem «deres registrerte» er
3. At dere vet hvilke opplysninger dere har om de registrerte og hvor disse opplysningene kommer fra
4. At dere vet hvorfor dere trenger akkurat disse opplysningene om de registrerte
5. Om dere vet om dere kan gjennomføre oppgavene med færre opplysninger
6. At dere vet hvem i deres organisasjon som beslutter om opplysninger skal slettes/rettes
   - Vet dere hvem som teknisk sett kan gjennomføre endringene?
   - Vet dere hvor lang tid det tar å endre eller slette?
7. At dere vet hvor dere og alle andre i organisasjonen finner informasjon om internkontrollsystem og rutiner for informasjonssikkerhet og hvordan dette kan hjelpe dere i arbeidshverdagen

Om de nye reglene



Dersom man følger dagens lov, er veien til etterlevelse av forordningen kortere.

Dersom man ikke følger dagens lov, har man et problem……

……og ja

- Det er mange ting å ta tak i, man skal ha…..
  - ✓ oversikt over hvilke opplysninger man forvalter og behandler
  - ✓ oversikt over hvor de er og hvem som har tilgang
  - ✓ et tilstrekkelig internkontrollsystem
  - ✓ rutiner for informasjonssikkerhet
  - ✓ kjennskap til hele GDPR
  - ✓ en realistisk oppfatning av de særkravene i GDPR
- ……..står man der så ligger man godt an
- ……..står man ikke der, så er nok veien noe lengre

- **Uansett hvor man står, så ikke bli stående**

- «Driveren bak dette er muligheten for at Datatilsynene kan ilegge veldig store gebyrer etter det nye regelverket»

  - ✓ Vi håper driveren skal være respekten for den enkeltes personvern

Det handler om tillit

The glory of friendship is to the outstretched hand, nor the kindly smile, nor the you of companionship; it is the spiritual inspiration that comes to one when he discovers that someone else believes in him, and is willing to trust him, Graham Greene (1904-91)

Hallstein Husand
fagdirektør
hhu@datatilsynet.no

Følg oss:
datatilsynet.no
personvernbloggen.no
Twitter.com/datatilsynet