



Nye personvernregler

Norsk arkivråds høstseminar 2017,
Oslo 19. oktober 2017

Helge Veum, Avdelingsdirektør

25th of May

2018

Nye personvernregler

Personvernforordningen

GDPR

Regulation (EU) 2016/679

Hva er personvern?

- Beskyttelse av privatlivets fred
- Ivaretagelse av den personlige integritet
- Retten til å bestemme over egne personopplysninger



Retten til å være i fred

Bakgrunn – personvernregelverk



Personopplysningsloven og personopplysningsforskriften 2000
(2001)



Nye norske personvernregler 2018

EUs personverndirektiv 1995



EUs personvernforordning 2016



Bakgrunn – EUs arbeid med nytt regelverk



- Arbeidet startet i 2012
- Vedtatt i 2016 og trer i kraft i 2018
- Felles regelverk for personvern i Europa
- Styrke den europeiske borgers rettigheter
- Gjøre det lettere å utveksle personopplysninger over landegrenser
- Styrke tilliten til digitale tjenester
- Sikre samarbeid mellom personvernmyndigheter



Official Journal

of the European Union



English edition

Legislation

Volume 59
4 May 2016

Contents

I Legislative acts

page

REGULATIONS

- * **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (¹)** 1

DIRECTIVES

- * **Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by** 89

Regelverket er på høring

<https://www.regjeringen.no/no/dokumenter/horing-om-utkast-til-ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett/id2564300/>



Regjeringen.no

Søk  Meny 

Høring om utkast til ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett

Høring | Dato: 06.07.2017 | Justis- og beredskapsdepartementet

Justis- og beredskapsdepartementet sender med dette på høring et forslag til ny personopplysningslov, som gjennomfører EUs personvernforordning i norsk rett. Departementet foreslår at forordningen gjennomføres i norsk rett ved inkorporasjon, det vil si at forordningen gjøres gjeldende som norsk rett gjennom en henvisnings-bestemmelse i den nye personopplysningsloven. Videre foreslår departementet lovbestemmelser som utfyller bestemmelsene i forordningen.

Status: På høring

Høringsfrist: 16.10.2017

Hva blir nytt?



- Krav i regelverket:
 - Innebygd personvern og personvern som standardinnstilling
 - Vurdering av personvernkonsekvenser
 - Tydeligere krav til informasjon og samtykke
 - Strengere sanksjoner
- Strategier for etterlevelse av regelverket:
 - Obligatorisk med personvernombud
 - Risikobasert tilnærming
 - Forhåndsdrøftelser
 - Bransjenormer og sertifisering
 - Europeisk samarbeid

Alle norske virksomheter får nye plikter



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



Alle bør ha en forståelig personvernerklæring

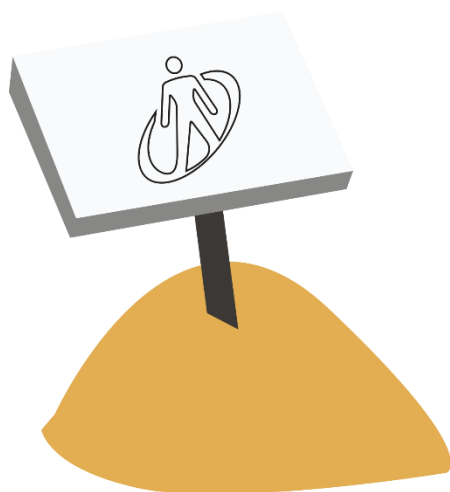


- Informasjonen skal være lett tilgjengelig
- Klart språk som er tilpasset leserens nivå
- Stilles krav til hvilke opplysninger som skal gis





- Personvernombudsordningen går fra frivillig til obligatorisk
- Alle offentlige virksomheter (unntatt domstolene)
- 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



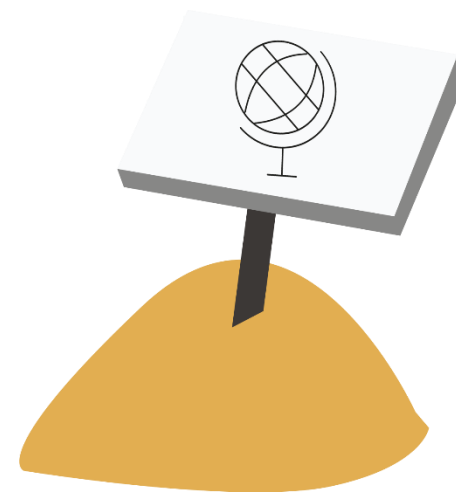
- Krav til kompetanse
- Skal involveres og rapportere til høyeste ledelsesnivå
- Ombudet skal ikke instrueres eller straffes for rollen som ombud
- Oppgavene omfatter å gi råd, overvåke etterlevelse og være kontaktpunkt



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



Alle må kunne oppfylle borgernes nye rettigheter



- Retten til å bli glemt
- Rett til at personopplysninger begrenses
- Systemer må oppfylle krav til dataportabilitet
- Strengere regler for automatiserte avgjørelser
- Håndtere henvendelser fra borgere innen 1 måned





Krav til informasjonssikkerhet og internkontroll
i nytt regelverk

Art. 32 – Security of processing

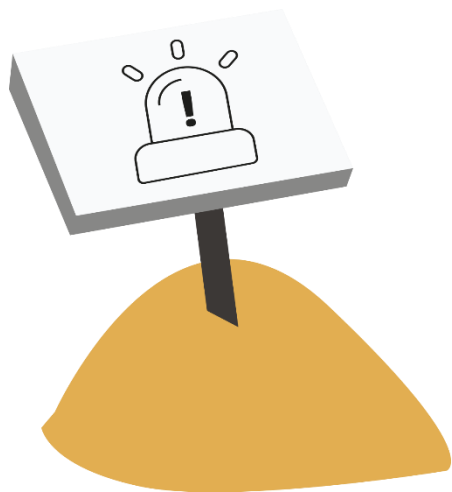


- Risikovurdering
- Sikkerhetstiltak
 - Pseudonymisering og kryptering av personopplysninger
 - Sikre vedvarende K, I, T og robusthet
 - Gjenoppretting av tilgjengelighet og tilganger ved hendelser
 - Jevnlig testing, vurdering og evaluering
- Bransjenormer eller godkjent sertifiseringsordning
 - Element for å vise etterlevelse
- Tiltak for å sørge for at behandling kun skjer på instruks fra behandlingsansvarlig

Alle får nye krav til avvikshåndtering

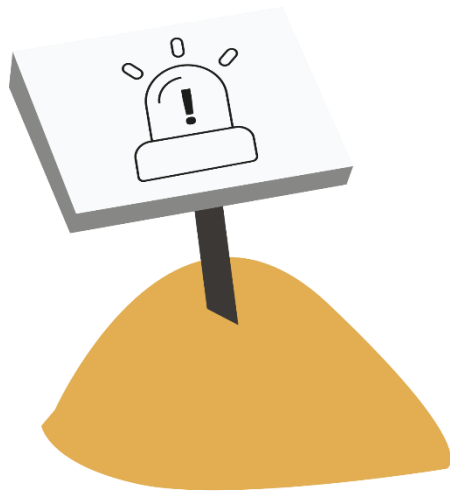


- Strengere regler enn i dag
- Melde avvik innen 72 timer
- Stilles krav til innholdet i avviksmeldingen
- De berørte skal varsles i klart språk





- Eksplisitt i mange bestemmelser
- Generell plikt i Art. 24
«Responsibility of the controller»
- Oversikt over behandlingsaktiviteter
Art. 30
- Forholdsmessighet
- Være i stand til å vise etterlevelse



Alle databehandlere får nye plikter

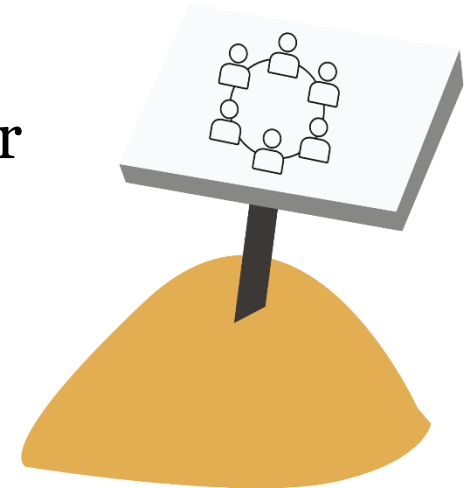


- Egne rutiner for behandling av personopplysninger
- Si ifra om instruksjer er i strid med loven
- Underleverandører skal godkjennes
- Melde avvik til behandlingsansvarlig
- Kan bli erstatningspliktige



Bransjenormer – verktøy for etterlevelse

- Sektorvis utforming av retningslinjer
- Sikrer at de viktigste rutinene er på plass
- Flere fordeler ved å følge disse
- Datatilsynet skal godkjenne bransjenormer



Innebygd personvern og DPIA

Innebygd personvern og som standard – Art 25



- Tekniske og organisatoriske tiltak
 - pseudonymisering
- Utformet for å ivareta personvernprinsipper
 - minimalisering
- Det minst personverninngrepene alternativet som standard:
 - mengde
 - omfang
 - lagringstid
 - tilgjengelighet





Veileder

Programvareutvikling med innebygd personvern

Veilederen skal hjelpe norske virksomheter å forstå og etterleve kravet om innebygd personvern i de nye personvernreglene. Den er utarbeidet i samarbeid med sikkerhetsekspertene og programutviklere i privat og offentlig sektor. Veilederen har også vært på høring i flere virksomheter og organisasjoner.



Skriv ut veileder

Innhold

- 1 [Programvareutvikling med innebygd personvern](#)
- 2 [Om veilederen](#)
- 3 [Innebygd personvern - hva er det?](#)
- 4 [Opplæring](#)
- 5 [Krav](#)

Vurdering av personvernkonsekvenser - Data protection impact assessment (DPIA)



- En systematisk prosess
- identifiserer og evaluerer...
- potensielle personvernkonsekvenser hvordan dere kan unngå trusler mot hvilke tiltak dere må innføre for å avverge trusler mot personvernet

Hva nå?

Hva bør alle virksomheter gjøre nå?



- Sørg for å ha oversikt over hvilke personopplysninger de behandler
- Sørg for å oppfylle dagens lovkrav
- Sette seg inn i det nye regelverket
- Lage rutiner for å følge de nye reglene





[Regelverk og avgiftsletter](#) / [Nye personvernregler](#) /

Nye personvernregler fra 2018

[Hva betyr de nye personvernreglene for din virksomhet? >](#)

[Når får vi vite mer om de nye personvernreglene fra EU? >](#)

[Hva betyr nytt lovverk for deg som er personvernombud? >](#)



Nye regler for kommunikasjonsvern (ePrivacy)

EU-kommisjonen har vedtatt et utkast til en forordning for personvern og elektronisk kommunikasjon (ePrivacy). Reguleringsen er nødvendig for å møte kravene i de nye personvernreglene som gjelder fra mai 2018.

[Hovedspunkter fra EU-kommisjonens forslag til nye kommunikasjonsvernregler >>](#)



Nye personvernregler fra 2018

[Les mer](#)

Nyheter

- 14.04.2016**
Personvernforordningen vedtatt i EU
Denne uken vedtok EU-parlamentet personvernforordningen. Det betyr at alle EU-land får ny og enhetlig personvernlovgivning fra 2018. Dette er den største endringen innen personvernlovgivning i Europa på over 20 år. [>](#)
 - 09.03.2016**
Hvem gjør hva frem mot ny personvernforordning? [>](#)
 - 16.12.2015**
Ny forordning for personvern gir flere rettigheter [>](#)
 - 15.06.2015**
Enighet om ny personvernforordning [>](#)
- [Se alle salene >>](#)



Forordningens tekst

Her finner du lovtaksten som er vedtatt i EU og publisert i "The Official Journal of the European Union"

Forordningen ble formelt vedtatt i EU-institusjonene den 14. april 2016 og vil tre i kraft 25. mai 2018.

[Forordningsteksten på engelsk >>](#)
[Forordningsteksten på dansk >>](#)
[Forordningsteksten på svensk >>](#)



Lurer du på noe?

Har du spørsmål om de nye reglene? Send en e-post til Datatilsynets veiledningsjeneste: nyesregler@datatilsynet.no

Du kan også møte deg på vårt nyhetsbrev. Da holder vi deg oppdatert på de nye reglene og andre personvern saker.

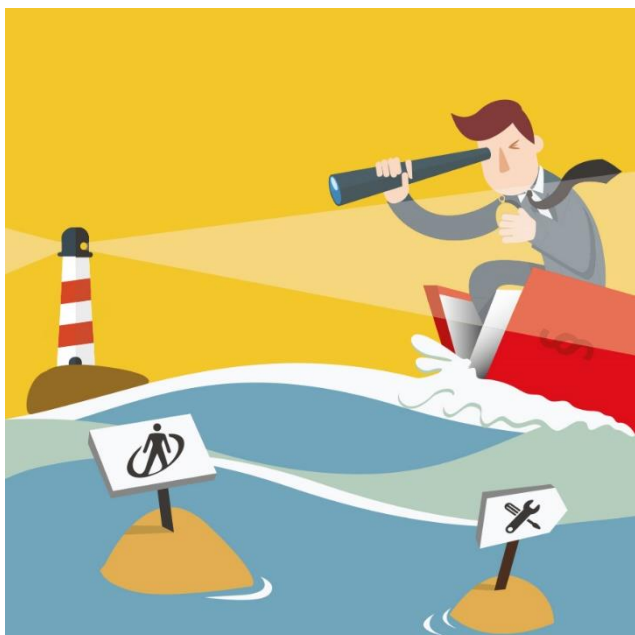
[Send oss en e-post om du lurer på noe >>](#)
[Meld deg på Datatilsynets nyhetsbrev >>](#)



Veiledning fra EUs personverngruppe

EUs rådgivende organ i personvernsspørsmål, Artikkel 29-gruppen, vedtok i desember uttalelser om flere av de nye personvernreglene. De har også laget FAQ eller "ofte stilte spørsmål" til hver av uttalelsene. Gruppen har også offentliggjort hvilke veiledere de vil utarbeide i 2017.

[Les mer og last ned de første tre veilederne >>](#)
[Plan for veiledere fra Artikkel 20-gruppen >>](#)



Nye personvernregler fra 2018

Hva betyr det for din virksomhet?



Til ledere med ansvar for personvern, sikkerhet og utvikling

Er du klar for nytt regelverk?

I 2018 blir dagens personvernregelverk erstattet av EUs personvernforordning. Norske virksomheter bør derfor begynne å forberede seg på nye personvernregler allerede nå. Før de nye reglene trer i kraft må dere sørge for at dere har:

- 1 Internkontroll og oversikt over hvordan dere behandler personopplysninger**
Fra 2018 må ikke bare behandlingsansvarlige, men også databehandlere ha oversikt over behandling av personopplysninger.
- 2 Systemer, tjenester og løsninger som oppfyller prinsippene om innebygd personvern**
Velg den mest personvernvennlige innstillingen som standard. Bygg personvernet inn ved blant annet å begrense mengden informasjon som samles inn, pseudonymisere opplysninger så raskt som mulig, være åpen om innsamling og bruk av opplysninger, og tenke sikkerhet i alle utviklingsfaser (innebygg sikkerhet).
- 3 Systemer som er tilpasset for dataportabilitet**
Alle registrerte skal som hovedregel kunne ta med seg personopplysninger de selv har oppgitt, fra en virksomhet til en annen. Systemene dere bruker må være tilpasset for overføring og mottak av opplysninger.
- 4 Tilfredsstillende informasjonssikkerhet**
Gjennomfør risikovurderinger og få på plass tekniske og organisatoriske tiltak som pseudonymisering og kryptering. Systemene må sikre konfidensialitet, integritet, tilgjengelighet og robusthet. Sørg for at tilgjengelighet og tilgang til personopplysningene dere behandler gjenoprettes på en sikker måte etter hendelser. I tillegg må dere ha prosedyrer for å teste, vurdere og evaluere at tiltakene både er effektive og ivaretar sikring av alle personopplysninger virksomheten behandler.
- 5 Rammeverk og rutiner for å vurdere personvernkonsekvenser**
Dersom et tiltak er inngripende, skal dere vurdere personvernkonsekvensene ved tiltaket ved hjelp av en Privacy Impact Assessment (PIA) før det iverksettes. Er risikoen høy og umulig for dere å redusere, skal Datatilsynet involveres i forhåndsdrøftelser.
- 6 Rutiner for avvikshåndtering**
Forordningen stiller strengere krav til avvikshåndtering enn dagens regelverk. Ved brudd på sikkerheten skal dere varsle Datatilsynet innen 72 timer, og vi skal varsles oftere enn før. I tillegg skal dere informere alle som er berørt av sikkerhetsbruddet. Databehandlere skal også varsle behandlingsansvarlig umiddelbart ved avvik.

Takk for oppmerksomheten!



Datatilsynet

postkasse@datatilsynet.no

Telefon: +47 22 39 69 00

datatilsynet.no

personvernbloggen.no

