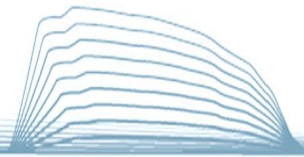




GDPR

Hammerfest kommune



Begynnelsen

Nye personvernregler fra 2018. Hva betyr det for din virksomhet?

Hva blir nytt?

- 1**
Alle norske virksomheter får nye plikter
Alle virksomheter må sette seg inn i den nye lovgivningen og finne ut hvilke nye plikter som gjelder dem. Ledelsen må sørge for å få på plass rutiner for å overholde de nye pliktene. Alle ansatte må følge de nye rutineene når reglene trer i kraft.
- 2**
Alle skal ha en forståelig personvern-erklæring
Informasjon om hvordan din virksomhet behandler personopplysninger skal være lett tilgjengelig og skrevet på en forståelig måte. Det nye lovverket stiller strengere krav til informasjonens form og innhold enn dagens lovgivning. All informasjon som gis til barn, skal tilpasses barnas forståelsesnivå.
- 3**
Alle skal vurdere risiko og personvernkonsekvenser
Dersom et tiltak utgjør en stor risiko for personvernet, må virksomheten også utrede hvilke personvernkonsekvenser det kan ha. Hvis utredningen viser at risikoen er stor og dere selv ikke kan redusere den, skal Datatilsynet involveres i forhåndsdrøftelser.
- 4**
Alle skal bygge personvern inn i nye løsninger
De nye reglene stiller krav til at nye tiltak og systemer skal utarbeides på en mest mulig personvernnøye måte. Dette kalles innebygd personvern. Den mest personvernnøye innstillingen skal være standard i alle systemer.
- 5**
Mange virksomheter må opprette personvernombud
Alle offentlige og mange private virksomheter skal opprette personvernombud. Et personvernombud er virksomhetens personvernekspert, og et bindeledd mellom ledelsen, de registrerte og Datatilsynet. Ombudet kan være en ansatt eller en profesjonell tredjepart.
- 6**
Reglene gjelder også virksomheter utenfor Europa
Virksomheter som holder til utenfor

Europa må også følge forordningen, dersom de tilbyr varer eller tjenester til borgere i et EU- eller EØS-land. Dette gjelder også om de ikke direkte tilbyr tjenester, men kartlegger adferden til europeiske borgere på nett. De som er etablert i flere land i Europa, skal bare trenge å snakke med personvernmyndighetene i det landet der de har sitt europeiske hovedkvarter.

- 7**
Alle databehandlere får nye plikter
Databehandlere er virksomheter som behandler personopplysninger på oppdrag fra den ansvarlige virksomheten. Ofte er det snakk om leverandører av IT-tjenester. De nye reglene pålegger databehandlere å ha rutiner for innsamling og bruk av personopplysninger. Databehandlere skal også si ifra til oppdragsgiveren sin hvis de får instruksjoner som er i strid med loven. Oppdragsgiver skal også godkjenne databehandlerens underleverandører. Databehandlere kan også bli holdt økonomisk ansvarlig sammen med oppdragsgiver.

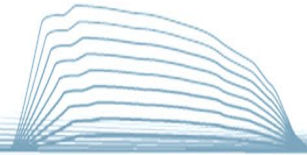
- 8**
Alle bør samarbeide i egne nettverk og følge bransjenormer
De nye reglene oppmuntrer til sektorvis utforming av retningslinjer og bransjenormer. Om dere følger bransjenormer, vil dere ha de viktigste rutineene på plass. Datatilsynet skal godkjenne bransjenormene.

- 9**
Alle får nye krav til avvikshåndtering
Reglene for håndtering av sikkerhetsbrudd blir strengere. Forordningen stiller krav til når det skal varsles, hva varselet skal inneholde og hvem som skal varsles. Kort sagt skal man si fra raskere og oftere enn man gjør i dag.

- 10**
Alle må kunne oppfylle borgernes nye rettigheter
Den enkeltes rett til å kreve at hans eller hennes personopplysninger slettes blir styrket. Dette kalles «retten til å bli glemt». Norske og europeiske borgere vil blant annet kunne kreve å ta med seg personopplysningene sine fra en leverandør til en annen i et vanlig brukt filformat. Dette kalles «dataportabilitet». De kan også motsette seg profilering. Alle henvendelser fra borgere skal besvares innen en måned.

Hva bør dere gjøre nå?

- 1**
Ha oversikt over hvilke personopplysninger dere behandler
Alle virksomheter som samler inn eller bruker personopplysninger skal ha oversikt over hvilke personopplysninger det er snakk om, hvor de kommer fra og hva som er det rettslige grunnlaget for behandlingen. Sørg for å ha en slik oversikt. Det er et krav som gjelder også etter dagens lov.
 - 2**
Sørg for å oppfylle dagens lovkrav
Overgangen til de nye reglene blir lettere om dere etterlever kravene i personopplysningsloven, som gjelder i Norge i dag. Har dere gode rutiner for internkontroll som fungerer etter hensikten og er kjent i organisasjonen, er det lettere å få oversikt over hva dere må endre.
 - 3**
Sett dere inn i det nye regelverket
Dere finner forordningsteksten på Datatilsynets nettsider. Der fyller vi også på med artikler om de nye reglene etter hvert som vi utarbeider dem.
 - 4**
Lag rutiner for å følge de nye reglene
Gå gjennom rutineene dere har for behandling av personopplysninger. Oppdater dem etter nytt regelverk der det trengs. Dokumenter de nye rutineene, og legg en plan for nødvendige endringer. Er systemene deres laget for å ivareta kravet til innebygd personvern, dataportabilitet og personvern som standardinnstilling? Klarer dere å fange opp og besvare henvendelser fra borgerne innen én måned? Endringer i systemer og rutiner tar tid. Begynn allerede nå!
- datatilsynet.no/forordning



Progresjon

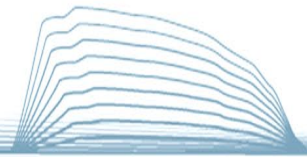
Juni 2017

satte samme en GDPR-gruppe bestående av IT-sikkerhetsansvarlig, arkiv, helse, IT-sjef og intranettanv.

- foretok en kartlegging

Høst 2017

Gjennomgikk ulike dokumenter for informasjonssikkerhet, deltok på konferanse i GDPR (KINS) og fordelte sektorene mellom oss i forhold til prosedyrer



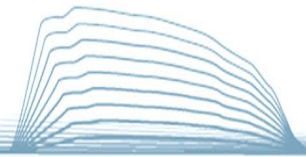
Progresjon forts.

Jan. 2018

Begynte å se på dette med **protokoll over behandlingsaktiviteter, personvernerklæring, personvernombud og arkivplan.**

Feb. 2018

Valgte oss QM+ som **protokoll for behandlingsaktiviteter** og satte oss frister for å levere et revidert dokument for Informasjonssikkerhet og **personvernerklæringer.**



Progresjon forts.

Mars 2018

Personvernombudet på plass

Personvernerklæring med
tilhørende prosedyrer for intern bruk
på plass

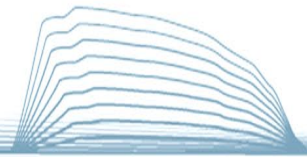
Personvernerklæring til hjemmesiden
på plass.

April 2018

50 prosedyrer revidert og på plass

Dokumentet for Informasjonssikkerhet
ferdig og sendt til godkjenning i
ledergruppen

Rutine for innsyn i personopplysninger
påbegynt og diskutert

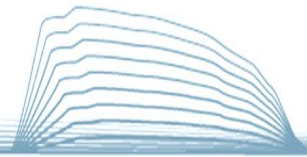


Progresjon forts.

Mai og juni 2018

Siste gjennomgang av **protokoll over behandlingsaktiviteter** sammen med gruppen for denne gang.

Deler av gruppen har møter med Hammerfest Havn og Hammerfest Parkering ang. **Personvernombud** og **behandlingsaktiviteter**.



ROS / DPIA (Data Protection Impact Assessments)

- Mobil omsorg – hjemmetjenesten
- Clean Pilot – renholdstjenesten
- Hjelpemiddelbasen – Ergo-fysio
- IKT – digitalisering
(kommunesammenslåing)