Leder1.no
- hjelp for ledere


GDPR står for **General Data Protection Regulation**. Denne er ment for å beskytte og ivareta opplysninger som bedrifter, foreninger, idrettslag, borettslag, organisasjoner og andre samler inn av personopplysninger og data.

**GDPR er pålagt for alle virksomheter som behandler personopplysninger.**

Med andre ord så gjelder lovverket praktisk talt alle, men bare 3 av 10 virksomheter blant små og mellomstore virksomheter har GDPR på stell. GDPR må dokumenteres for Datatilsynet, ved kontroll, og det skal framkomme hvordan dere sikrer personvernet til ansatte, klienter og andre samarbeidspartnere.

Det er virksomheter som har respekt for personvernet og lovverket som sørger for å ha GDPR dokumentasjon på plass. **Å ivareta personvernet er en del av kvalitetsarbeidet i virksomheten.**

Alle ønsker at personopplysninger blir tatt vare på, og at virksomheten har rutiner dersom opplysninger kommer på avveie. Som virksomhet må man ta ansvar og dokumentere hvordan personvernet håndteres for å unngå sanksjoner og bøter.

## Leder1 sin leveranse av dokumentasjon

Leder1 er en av få aktører, foruten advokater, som leverer GDPR dokumentasjon og fungerer som personvernrådgiver for virksomheter.

Vi er uavhengig, innfører rutiner og vi holder oss oppdatert slik at man kan tilføre virksomheten dokumentasjonskravene.

**Vår GDPR dokumentasjon er kvalitetssikret av juridisk personell.** Leder1 tilbyr to ulike alternativer for at virksomheter får GDPR på stell.

### Alternativ 1:

**Vi gjør jobben for dere.**
Vi sørger vi for å produsere virksomhetens personvernerklæringer, veiledere, varslingsrutiner, protokoller, internkontroll mm. Med det bidrar vi med å opprettholde dokumentasjonsplikten i henhold til Datatilsynets føringer. Leder1 fungerer også som kontaktledd mot Datatilsynet ved hendelser og eventuelle sikkerhetsbrudd.

**Leder1 gjennomfører GDPR dokumentasjonen, komplett, for deres virksomhet til en engangskostnad på kr. 1.990, - eks. mva**.

### Alternativ 2:

**Tilpass dokumentasjonen selv, etter veiledning og beskrivelser.**
For å imøtekomme kravene fra Datatilsynet, har vi sammensatt et sett av dokumentmaler og skjema som inkluderer veiledere, protokoller, sjekklister, personvernerklæringer, internkontroll mm, og som gjør at du følger lovverket rundt GDPR dokumentasjon. I dette produktet inngår også dokumenter for lovpålagte varslingsrutiner.

**Det inngår support ved kjøp av dette produktet.**

**Prisen for dokumentene og skjemaene er kr. 700,- eks. mva, som engangskostnad**.
Bestilling av dokumentene kan gjøres til avsenders epostadresse. Faktura utstedes etter leveranse. Dokumentene kan også kjøpes direkte på vår nettside Leder1.no – GDPR dokumentasjon

## Her får du svar på det du trenger å vite om GDPR i virksomheten

### Er GDPR, loven om personvern kjent for virksomhetene?

Ja, mange virksomheter kjenner til loven og GDPR, men langt i fra alle. Siden GDPR ble innført tilbake i 2018, er det mange virksomheter som ennå ikke har dokumentasjonskravene på stell. Det kan gjerne skyldes flere faktorer som blant annet manglende kompetanse på hva man må gjøre, ressurser og tid.
Men man kan av den grunn ikke ignorere lovverket rundt personvern.

Føler du at du ikke har kompetanse rundt GDPR, så anbefales det at du tar kontakt med en personvernrådgiver eller advokat for å rådføre deg om GDPR.

### Hva er konsekvensene for ikke å følge lovverket om personvernet?

GDPR handler først og fremst om trygghet for dine ansatte, klienter og samarbeidspartnere. Deretter er det virksomhetens renomme og tillit som kan svekkes om ikke man har GDPR på stell. Du må som virksomhet sørge for at du ivaretar sikkerheten til de du samler inn personopplysninger på. Det skal ikke være noen virksomheter som har "råd" til å unngå å ta personvernet på alvor. Man skal også tenke på at man som virksomhet kan bli klaget inn til Datatilsynet om ikke lovverket overholdes.

Ved brudd på regelverket så er det Datatilsynet som gir virksomheten sanksjoner og bøter. Ved grove brudd så kan bøtene bli store. Det kan påløpe erstatningsplikt for den som bryter loven, man kan få økt kontroll fra myndighetene, og i verste fall risikere tvangsavvikling.
Selv om du oppbevarer begrenset info om personer, så må GDPR være på plass i virksomheten.

## Finnes det standard dokumentasjon for GDPR?

Nei, dessverre. Det er slik at den enkelte virksomhet må internt tilpasse GDPR og håndtering av personopplysninger.
Virksomheter samler inn ulike opplysninger om enkeltpersoner, basert på behov og årsak til at informasjon innhentes. Likeledes må også varslingsrutiner tilpasses virksomheten selv. Det er heller ikke mange aktører som leverer GDPR dokumentasjon, annet enn advokater, så det kan være lurt å kontakte en ekstern aktør som kan bidra virksomheten.

## Hvilke fordeler har virksomheten med å dokumentere GDPR arbeidet?

Ved å dokumentere viser dere at virksomheten følger lovverket og gjør tiltak for å sikre personopplysninger.
Det medfører at personer kan føle seg trygge på virksomheten ivaretar GDPR på en forsvarlig måte.
Det bidrar også til å trygge virksomhetens renomme og tillit.
Samtidig er forebygging av mulige brudd på personvernet med på skalere ned risikoer, og minimalisere tiltak ved eventuelle hendelser.

Ikke minst så bidrar dokumentasjonen til å beskytte virksomheten mot mulige brudd, hvor konsekvensene kan bli store i form av bøter og sanksjoner.

Se for deg ditt kundeforhold til en leverandør. **Hva forventer du av dem når de oppbevarer personopplysninger om deg?**
Alle ønsker selvsagt at personopplysninger blir tatt vare på, og at virksomheten har rutiner dersom opplysninger kommer på avveie.
Som virksomhet må man ta ansvar og dokumentere hvordan personvernet håndteres.

## Hva er behandlingsgrunnlag?

Enkelt sagt så er behandlingsgrunnlag årsaken til hvorfor informasjon om personer innhentes, og hva de skal brukes til. Man må altså ha en rettslig grunn for å oppbevare opplysninger. Dette står beskrevet i artikkel 6 om GDPR. (Kilde: Lovdata).

## Er jeg innenfor lovverket når jeg har personvernerklæring på hjemmesiden min?

Personvernerklæring på hjemmesiden er en god start, men er langt fra tilstrekkelig. En personvernerklæring er ikke godt nok når du må dokumentere rutiner rundt personvernet i virksomheten.

## Skal ansatte også ha personvernerklæring?

Definitivt. Virksomheter oppbevarer ofte mye informasjon om den ansatte. Dette kan være opplysninger som er nødvendig i forbindelse med lønn, sykdom, referater fra medarbeidersamtaler og andre oppfølgingsmøter som for eksempel i forbindelse med prøvetid.
Personvernerklæringen tilpasses etter hvilken informasjon virksomheten innhenter fra den ansatte.
Man må også huske på den ansatte må informeres dersom virksomheten deler ansattopplysninger med samarbeidspartnere.
(Regnskapskontor, lønnssystem, programvare, IT konsulenter mv.)

## Hva må jeg ha klart ved eventuell kontroll fra Datatilsynet?

Først og fremst; vis fram at du tar personvernet på alvor, og at du jobber med **informasjon** og **dokumentasjon**.
Dokumentasjon er viktig å ha på plass for å redusere risikoen for at virksomheten bryter loven, unngår overtredelser, bøter og omdømmetap.

## Hva er rettighetene til en person som vi oppbevarer opplysninger på?

Ved forespørsel, er virksomheten forpliktet til å gi fra seg all informasjon som er registrert på en person. Dette er personens innsynsrett.
Likeledes kan personer be om å bli slettet eller at informasjonen som oppbevares skal begrenses, endres eller overføres til andre virksomheter.
Ved henvendelser fra personer, må du altså ha "ting på stell" i virksomheten.
De som for eksempel skal ha innsyn i en personalmappe, må forholde seg til reglene i offentleglova og forvaltningsloven.
Det betyr at medarbeidere som ikke har saklig grunn til å se opplysningene, heller ikke skal ha tilgang.
Virksomheten må dedikere personer som skal ha tilgang til opplysninger om ansatte.

## Er det behov for personvernombud i virksomheten?

Flere offentlige myndigheter og organer er pålagt å opprette eget personvernombud.
I tillegg er også mange virksomheter pålagt å ha eget ombud, dersom det behandles svært sensitive personopplysninger. Flere og flere virksomheter benytter seg også av ekstern personvernrådgiver. Ved å benytte en ekstern personvernrådgiver får dere kontroll med GDPR, samtidig som det frigir ressurser og ikke minst tid.

Ellers skal det være en dedikert person fra virksomheten som må være behandlingsansvarlig for personopplysninger.

## Trenger jeg GDPR når jeg ikke har hjemmeside?

Ja, selv om du ikke har hjemmeside i virksomheten, har du et ansvar så fremt du behandler personopplysninger på klienter, medlemmer, ansatte og andre.
Har du ikke egen hjemmeside må opplysninger om personvernet til klienter og andre som henvender seg til virksomheten framkomme på annen måte.
Om du kun markedsfører deg gjennom ulike oppføringer, som anbudstjenester eller andre, så må du synliggjøre at personvernet ivaretas gjennom personvernerklæring der du annonserer.
Kort sagt; om du ikke har hjemmeside, så kan du ikke fraskrive deg ansvaret du har som virksomhet når det gjelder GDPR.

## Trenger jeg GDPR når jeg tar vare på "bare noen få" personopplysninger?

Ja, selv om du bare samler inn få personopplysninger må du uansett ha GDPR i virksomheten.
Man kan gjerne tenke at man som virksomhet oppbevarer lite opplysninger, men gjør du egentlig det?
Behandler man opplysninger på ansatte, klienter og andre, så oppbevares det ofte mye og gjerne sensitiv informasjon.

## Hva er et sikkerhetsbrudd?

**Et sikkerhetsbrudd kan forekomme dersom:**

– Virksomheten ikke har fullstendig oversikt over behandling av personopplysninger.

– Ikke autoriserte personer får tilgang til personopplysninger.

– At en ansatt bevisst, eller ubevisst, videresender informasjon som er av sensitiv art.

– At du eller en ansatt blir frastjålet, mister eller har forlagt en telefon, PC, minnepenn, ansattperm eller en klientperm som inneholder personopplysninger.

– Hackerangrep / dataangrep som gjør at opplysninger kommer på avveie. Hacking og svindel er svært utbredt blant små og mellomstore virksomheter.

– At det mangler databehandleravtale med regnskapskontoret, programvaretilbydere eller andre virksomheten benytter.

– Å kaste eller kvitte seg med personopplysninger uten at disse makuleres eller slettes.

**Dersom et sikkerhetsbrudd oppstår er du som virksomhet pålagt å melde inn dette til Datatilsynet innen 72 timer.**

## Trenger jeg databehandleravtale?

Du som virksomhet, eller de som benytter virksomheter som behandler personopplysninger på vegne av deg, må opprette en databehandleravtale.
(Dette kan være regnskapskontoret, IT leverandører og andre). Om ikke dine samarbeidspartnere har opprettet databehandleravtale med dere, må dere etterspørre dette. De som direkte behandler opplysninger på vegne av andre er lovpålagt å sørge for at det foreligger en databehandleravtale.

## Er E-post kommunikasjon en del av GDPR?

Absolutt.  Epost er omfattet av GDPR. Dette kan være noe kompleks, så her bør virksomheten ha gode rutiner.
Hva gjør dere dersom epost med sensitiv informasjon forsvinner? Om du er usikker på hvordan du skal håndtere personopplysninger i e-postkommunikasjon, anbefales det at du tar kontakt med en juridisk person eller personvernrådgiver.
Da vil du få råd og veiledning for å sikre at din virksomhet oppfyller kravene og beskytter personopplysningene på en forsvarlig måte.

## Hva er Cookies og informasjonskapsler?

Stort sett alle nettpubliseringsverktøy (hjemmesider) bruker Cookies for å registrere innloggingsdetaljer, antall besøk på siden og hvordan man beveger seg på et nettsted. Svært mange bruker også Cookies fra Google Analytics, som er et verktøy som gir mer detaljert informasjon om brukermønstre på en hjemmeside. Besøkende på nettsiden din skal informeres om det benyttes Cookies. Les mer om Ekomloven her.

En erklæring som framkommer på hjemmesiden, og som omhandler Cookies, er på langt nær tilstrekkelig for å informere klienter som besøker
hjemmesiden din. Du må i tillegg ha en egen personvernerklæring.

## Vi har kameraovervåking i virksomheten, hvordan forholder vi oss til det?

Det kan være et legitimt behov for å ha kameraovervåking, som for eksempel å unngå innbrudd og tyverier for å sikre verdier. Samtidig så er det viktig å tenke på at arbeidstakere har rett til privatliv. Om en virksomhet vurderer å sette opp kamera på arbeidsplassen, er det nødvendig at man setter seg inn i regelverket og sørger for at kravene rundt kameraovervåking og lyd er oppfylt. Kravene SKAL være oppfylt før kameraovervåkingen settes i gang.
Om virksomheten allerede har kameraovervåking, så må man kontrollere om gjeldende krav følges, og at det informeres og dokumenteres i virksomheten.

## Er varsling en del av GDPR – personvernet?

Ja, absolutt. Varsling er lovregulert for virksomheter som har ansatte og innleid arbeidskraft. Det skal derfor utarbeides egne rutiner for varsling i virksomheten. Ved forhold som er kritikkverdige på arbeidsplassen, som for eksempel brudd på personvernet, skal man varsle. Dette er regulert i lovverket.

## Er det mye jobb for virksomheten min å overholde GDPR?

Jobben kan bli vesentlig større om du får tilsyn, sanksjoner og bøter for ikke å ha GDPR på stell. Det viktigste er at du etter beste evne forsøker å følge Datatilsynets føringer på hvordan man skal utøve best mulig GDPR arbeid i virksomheten. Føler du at det er vanskelig å begynne jobben med å få til GDPR, så benytt en ekstern aktør som bistår deg. Advokater eller en personvernrådgiver kan være greit å kontakte.
(Leder1 har en relativt stor kundegruppe av advokater som benytter våre dokumentmaler for å bistå virksomheter).

## EU-forordningen om kunstig intelligens (Artificial Intelligence Act)

Kunstig intelligens (AI) er noe man forholde seg til i alle typer virksomheter. Nå innføres loven om AI Act også i Norge. Det er viktig at man setter seg inn i den nye lovgivningen om AI Act.
AI bør være en del av virksomhetens GDPR, og rutiner om bruk av AI bør være på plass på lik linje som virksomhetens personvernpolicy.

Virksomheten må derfor sørge for å ha en plan rundt hvordan dere skal forholde dere til AI Act. Derfor bør det innføres rutiner allerede nå.
En framgangsmåte kan være å starte med å kartlegge hvordan dere har tenkt å benytte AI i bedriften.

**Om så er tilfelle, må dere;**
– kartlegge ledelsen og ansattes tekniske kompetanse.
– sørge for at ledelse og ansatte som skal benytte AI må defineres med rolle og navn.
– legge en plan for å innhente grundig kompetanse og forståelse av hva AI er.
– forstå regler, gi opplæring og definere hvordan AI skal brukes i virksomheten.
– definere hvilke verktøy rundt AI som skal benyttes og hvordan de skal brukes.
– sørge for å holde dere oppdatert på verktøy og kompetanse.

Bruk av AI i virksomheten må uansett dokumenteres, og det er ledelsen som har overordnet ansvar for at regler om AI overholdes.
Det er ulovlig å bruke AI løsninger som bryter europeiske rettigheter og verdier. Dersom regler ikke følges, kan virksomheter få sanksjoner og høye bøter.

Virksomheten kan også helt velge bort bruk av AI. Virksomheten selv må avklare:
**Vil bruk av AI være en del av virksomhetens policy framover? Hva skal vi bruke det til, og hvorfor?** Å velge bort bruk av AI, er noe som også må dokumenteres.