GDPR – personvern

Bakgrunn

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.

Det er viktig at man har et forhold til GDPR og at man må være klar over hvilken risiko virksomheten utsettes for ved å ignorere lovkravene rundt personvernordningen.

Så lenge virksomheten, "stor eller liten", driver enkeltpersonforetak eller er større virksomhet, behandler og oppbevarer personopplysninger på klienter, ansatte, medlemmer og andre er man pålagt å følge loven om personvern.

Man må også tenke på omdømme og tillit hos dine ansatte, kunder, leverandører og øvrige samarbeidspartnere om personopplysninger kommer på avveie.

Datatilsynet ser økt rapportering av avvik/sikkerhetsbrudd blant virksomheter, og få har minstekravene rundt GDPR på plass. Har man ikke GDPR på plass så bryter man altså lovverket. Det er Datatilsynet som agerer med sanksjoner og bøter dersom loven ikke overholdes.

Dokumentasjon krever ikke en dyr programvare. Det er tilstrekkelig med tekstbehandlingsdokument, men man må sørge for at dokumentasjonen er skriftlig og elektronisk.

Spørsmål og svar om GDPR

Hva er konsekvensene for ikke å følge lovverket om GDPR?

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 GDPR 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 også påløpe erstatningsplikt for den som bryter loven og erstatning for "tort og svie", samt at man kan få økt kontroll fra myndighetene.

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

Personvernerklæring på hjemmesiden er en god start, men er langt fra tilstrekkelig. Personvernerklæring er vesentlig å ha på hjemmesiden for å synliggjøre for besøkende at personvernet ivaretas. Du bør unngå å bruke personvernerklæring du finner gratis på nett, kopierer fra andre eller er standard i en hjemmesideløsning. Personvernerklæringen MÅ altså til enhver tid være tilpasset den enkelte virksomhet.

Hva må jeg ha klart ved eventuell kontroll fra Datatilsynet?

Først og fremst; vis fram at du tar GDPR på alvor, og at du jobber med **dokumentasjon**. Dokumentasjon er det som blir gjennomgått ved et eventuelt tilsyn. **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?

Med GDPR lovgivningen har personer vesentlige rettigheter. 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, så må du altså ha "ting på stell" i virksomheten. De som for eksempel skal ha innsyn i en personalmappe i virksomheten, 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. For øvrig skal det være en dedikert person, som er behandlingsansvarlig for personopplysninger, i virksomheten.

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, 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.

– At det mangler databehandleravtale.

– 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.

Trenger jeg databehandleravtale?

Du som virksomhet, eller 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, så etterspør dette. De som direkte behandler opplysninger på vegne av andre er lovpålagt å sørge for at det foreligger en databehandleravtale.

Hva er cookies og informasjonskapsler?

Stort sett alle nettpubliseringsverktøy 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.

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. 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 dett informeres og dokumenteres i virksomheten.

Er varsling en del av GDPR - personvernet?
Ja, det kan man si. Varsling er lovregulert for virksomheter som har ansatte og innleid arbeidskraft. Det kom ny lov på rutiner på varsling for kort tid tilbake.
Det skal derfor utarbeides egne rutiner for varsling. 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 og sanksjoner 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.