

Personvernforordningen

Personvernforordningen (GDPR – General Data Protection Regulation) er en forordning fra Den europeiske union (EU) som legger til grunn et nytt rammeverk for håndtering og vern av personopplysningene til EU-borgere.

Den introduserer nye forpliktelser og ansvar for samtlige foretak som håndterer personopplysninger og nye rettigheter til personer rundt hvordan personopplysningene deres samles inn, behandles og lagres.

GDPRs innvirkninger

Hvis foretaket deres er forpliktet samsvare med GDPR, er det en rekke faktorer som må vurderes. Vi anbefaler på det sterkeste å oppsøke juridisk veiledning for å avgjøre hva som kan være pålagt i deres spesifikke situasjon.



1. Forståelse rundt opplysninger

Det å gi skikkelig beskyttelse til opplysninger innebærer å vite hvordan disse behandles i foretaket – hvordan personopplysninger håndteres, deles, brukes, arkiveres og slettes. Det å forstå hva opplysningene dine er samt hvordan de brukes og lagres, er et grunnleggende krav for å kunne bygge bedriftens GDPR-strategi.

2. Avgjøre eierskap og ansvarsforhold

Det er viktig å fastsette en ansvarlig eier for personvernssamsvar. For enkelte foretak er det nødvendig å utpeke et personvernombud. GDPR introduserte også et nytt «ansvarlighetsprinsipp», som krever at foretak tilslutter seg et samsvarsprogram for vern. Foretak vil måtte utvikle interne retningslinjer for vern av opplysninger samt gi opplæring til ansatte.

3. Sikre et lovhjemlet grunnlag for behandling

Et annet element i GDPR som bedrifter må sikre at er dokumentert er de lovhjelmede grunnlagene for behandling av ulike typer personopplysninger dere håndterer. For eksempel, hvis dere bruker samtykke som grunnlag for behandling, vil dere være pålagt å vurdere hvordan dere innhenter disse og tydelig vise til hvordan og og når dette samtykket ble gitt.

4. Forstå rettighetene til de opplysningene gjelder

For å sikre at prosedyrene deres imøtekommer disse er det viktig å forstå rettighetene som personer har overfor personopplysningene sine. For eksempel har de som opplysningene gjelder retten til å få tilgang til personopplysningene sine samt retten til å korrigere, slette eller eksportere disse elektronisk. I enkelte tilfeller vil brukere også ha retten til å protestere mot automatiske beslutningstaking og profilering.

5. Sikre innebygd personvern

Innebygd personvern er for første gang et uttrykkelig lovpålagt krav, så det er viktig å begynne en vurdering av hvordan dette skal innføres i bedriftens virksomheter. I enkelte tilfeller er det også nødvendig å utføre en konsekvensvurdering for personvern.

6. Forberede seg på håndtering av brudd

Det å sikre at retningslinjene og prosessene for behandling av databrudd er oppdaterte og testet er avgjørende for et robust personvernprogram. Rettidig oppdagelse og rapportering av brudd til de riktige myndighetene er pålagt under GDPR, da bøter kan pålegges ved forsømmelse av rapportering såvel som selve bruddene.

7. Kommunisere vesentlig informasjon

Pass på at foretaket personvernerklæringer og andre merknader er oppdatert og at disse omfatter praksisen for personvern. Nye krav inkluderer detaljering av rettslig grunnlag for behandling og sikre at brukere er kjent med myndigheten de kan klage til ved problemer.

8. Jobbe med leverandører

Det å sikre samsvar med GDPR strekker seg ut forbi foretakets egne retningslinjer. Alle eventuelle tredjeparter som behandler personopplysninger på deres vegne må også etterkomme de nødvendige standardene for personvern. Noen spørsmål det kan være lurt å stille leverandører er:

- Har de robuste metoder for nettverks- og informasjonssikkerhet, og personvern?
- Retter de seg etter internasjonalt aksepterte standarder og bekrefter overholdelsen av disse?
- Hvordan kan de vise til en sterk innarbeidet kultur av tillit og sikkerhet? Hvilke kontrollmekanismer tilbyr de for å bidra til administrasjonen av opplysningene deres og imøtekomme forpliktelsene deres som behandlingsansvarlig?

Dropbox: Verner om opplysningene deres

Tillit er grunnlaget for det forholdet vi har med flere millioner mennesker og bedrifter over hele verden.

Vi setter pris på tiltroen du gir oss, og tar ansvaret for å beskytte dataene dine på alvor. For å gjøre oss fortjent til den tilliten du har, laget vi, og vil vi fortsette å utvikle, Dropbox med vekt på sikkerhet, overholdelse og personvern.

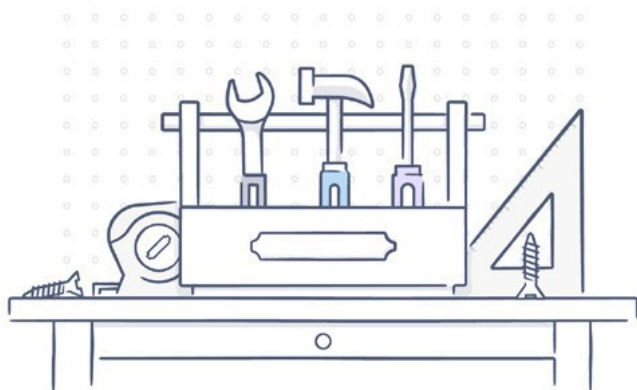
Sikkerhet: Beskytt og kontroller

Vern: Arkitektur og informasjonssikkerhet

Dropbox er utviklet med en sikker, distribuert infrastruktur med flere sikkerhetslag, bl.a. sikker dataoverføring, kryptering, nettverkskonfigurerings og kontroll på app-nivå distribuert på tvers av en skalerbar, sikker infrastruktur. Det robuste rammeverket vårt for styring av informasjonssikkerheter utviklet for risikovurdering og bygging av en sikkerhetskultur hos Dropbox. Vi går gjennom og oppdaterer sikkerhetsretningslinjene våre regelmessig, gir ansatte sikkerhetsopplæring, utfører testing av applikasjoner og nettverk (bl.a. inntrengingstesting), utfører risikovurderinger og overvåker samsvar med retningslinjer for samsvar. Fullstendig informasjon finnes i [Whitepaperet om sikkerhet i Dropbox Business](#).

Kontroll: Styrk IT-administratører

Dropbox tilbyr [funksjoner for kontroll og synlighet](#) som IT-administratører trenger og hjelper dere med å håndtere samsvarskravene på en enklere måte. Administratorpanelet vårt lar deg overvåke teamaktivitet, vise tilknyttede enheter og kontrollere delingsaktivitet. Grupper kan opprettes for enkel administrering av teammedlemmers tilgang til spesifikke mapper, og teammappeverktøyet gir synlighet og kontroll over teammapper, bl.a. synkroniseringsadministrasjon. Funksjonen for koblingstillatelser gir muligheten til å passordbeskytte delte koblinger, angi utløpsdatoer for å gi midlertidig tilgang samt begrense tilgangen til disse innen for foretaket. Verktøyet vårt for kontooverføring gjør det enkelt å overføre filer fra én bruker til en annen når ansvarsforholdene endrer seg. Ekstern sletting gjør det mulig å slette filer fra tapte eller stjålne enheter.



Overholdelse: Tillit og verifisering

Samsvar er en effektiv måte å bekrefte påliteligheten til en tjeneste. Vi anbefaler og forventer at dere [bekrefter](#) at sikkerhetsmetodene våre samsvarer med de mest utbredte [standardene og ordningene](#) som ISO 27001, 27017, 27018 og SOC 1, 2, og 3. De uavhengige tredjeparts-kontrollørene våre tester kontrollene våre og tilbyr rapporter og oppfatninger – som vi deler med dere når enn det er mulig. Mer informasjon om standardene vi samsvarer med og hvordan vi bekrefter sikkerhetsmetodene våre er tilgjengelig på [complianceweb-siden](#) vår.

Personvern: Vår forpliktelse

Dere er eiere av egne data, og uavhengig av hvorvidt det gjelder personlige eller jobbrelevante opplysninger tar vi brukeres tillit på alvor og jobber hardt for å sikre at all data på våre systemer beskyttes. [Personvernerklæringen vår](#) gir en tydelig beskrivelse på hvordan vi håndterer og verner om opplysningene deres. Vi utgir en [gjennomsiktighetsrapport](#) samt [prinsippene](#) for myndigheters anmodninger om opplysninger for å vise hvor ofte vi mottar, gransker og svarer på slike anmodninger. Vi vil også forsøke å bidra til lovreformer som gir økt personvern.

Arbeide sammen for å sikre dataene deres

Dropbox arbeider sammen med forretningskunder for å sikre dataene deres. Vi tar i bruk omfattende tiltak for å beskytte infrastruktur, nettverk og applikasjoner, gir opplæring til ansatte angående metoder for sikkerhet og personvern, bygger en kultur hvor det å være tiltrodd er høyeste prioritet samt utsetter systemene og metodene våre for strenge testing og kontroll fra tredjeparter. Kunder spiller også en viktig rolle i å sikre at teamene og dataene deres beskyttes og er sikre. Dropbox gjør det mulig å konfigurere, bruke og overvåke kontoen på måter som oppfyller kravene for sikkerhets, personvern og samsvar i foretaket deres. Vår [veiledning for delt ansvar](#) kan gi en bedre forståelse av hva vi gjør for å sikre kontoene deres og hva dere kan gjøre for å opprettholde synlighet og kontroll over team-data.

Innholdet i denne veiledningen er ment for å gjøre tilgangen til informasjon enklere, og gjelder ikke som juridisk veiledning. Lesere bør anskaffe egen juridisk veiledning etter behov.

