

Den generelle forordning om databeskyttelse

Den generelle forordning om databeskyttelse (GDPR), er en EU-forordning (EU), der opretter nye rammer til håndtering og beskyttelse af personoplysninger fra EU-borgere.

Den introducerer nye forpligtelser og ansvar for alle organisationer, der håndterer data, og nye rettigheder for individer, om hvordan deres personoplysninger indsamles, behandles og lagres.

Virkningerne af GDPR

Hvis din organisation skal overholde GDPR, er der en række faktorer, der skal overvejes. Vi anbefaler stærkt at søge juridisk rådgivning for at afgøre, hvad der kan kræves i din specifikke situation.



1. Forstå dine data

Behørig beskyttelse af data kræver at man forstår, hvordan den behandles i ens organisation—hvordan personoplysninger behandles, deles, anvendes, arkiveres og slettes. En forståelse for hvad dine data er, og hvordan de anvendes og lagres, er et nøglekrav til opbygningen af din virksomheds GDPR-strategi.

2. Bestemmelse af ejerskab og ansvar

Det er vigtigt at identificere en ansvarlig ejer for overholdelse af databeskyttelse. For nogle organisationer er det nødvendigt at udnævne en databeskyttelsesrådgiver. GDPR indfører også et nyt princip af "ansvarlighed", der kræver at organisationer indfører et overholdelsesprogram for databeskyttelse. Det vil blive nødvendigt for organisationer at udvikle interne databeskyttelsespolitikker og give personaleuddannelse.

3. Sikring af et retsgrundlag for behandling

En anden komponent i GDPR, som virksomheder skal sørge for er dokumenteret, er retsgrundlagene til behandling af de forskellige typer personoplysninger, der håndteres. For eksempel, hvis du bruger samtykke som grundlag for behandling, skal du overveje, hvordan du får det og være i stand til klart at demonstrere, hvordan og hvornår det er blevet givet.

4. Forståelse for de registreredes rettigheder

For at sikre, at dine procedurer imødekommer dem, vil du sikre dig, at du forstår de rettigheder, folk har i forhold til deres personoplysninger. For eksempel har registrerede ret til adgang til deres personoplysninger, såvel som til at få dem rettet, slettet eller eksporteret elektronisk. Under visse omstændigheder har brugerne også ret til at gøre indsigelse mod automatisk beslutningstagning og profilering.

5. Sikring af privatlivsbeskyttelse gennem design

Privatlivsbeskyttelse gennem design er for første gang et eksplicit juridisk krav, så det er vigtigt at begynde at overveje, hvordan det kan bygges ind i dine forretningsprocesser. I nogle tilfælde er udførelsen af konsekvensanalyser for privatlivsbeskyttelse også nødvendig.

6. Forberedelse til brudstyring

Det er vigtigt for et robust databeskyttelsesprogram at sikre, at dine politikker og processer for databrud er ajourført og testet. GDPR kræver den rettidige opdagelse og rapportering af brud til de rette myndigheder, da bøder kan opkræves for rapporteringsfejl såvel som for brud.

7. Kommunikation af afgørende information

Sikring af at din organisations online privatlivspolitik og andre meddelelser er opdaterede og omfatter praksisserne for databeskyttelse. De nye krav omfatter specificering af retsgrundlaget for din behandling og at gøre brugere opmærksomme om den myndighed, som de kan klage til, skulle der opstå et problem.

8. Arbejde med dine udbydere

Opfyldelse af GDPR-forpligtelser strækker sig ud over din organisations egne politikker. Eventuelle tredjeparter, der behandler personoplysninger på dine vegne, vil også skulle opfylde de nødvendige databeskyttelsesstandarder. Nogle spørgsmål, som du måske vil stille dine udbydere omfatter:

- Har de solide praksisser for netværks- og informationssikkerhed, privatliv og databeskyttelse?
- Overholder de internationalt accepterede standarder og verificerer de deres overholdelse?
- Hvordan kan de dokumentere en stærk tillids- og sikkerhedskultur? Og hvilke kontroller tilbyder de for at hjælpe dig med at administrere dine data og opfylde dine forpligtelser som dataansvarlig?

Dropbox: Beskyttelse af dine data

Tillid er grundlaget for vores forhold til millioner af mennesker og virksomheder over hele verden.

Vi værdsætter din tillid og tager ansvaret for at beskytte dine personlige oplysninger alvorligt. For at gøre os værdig til din tillid har vi udviklet og vil fortsætte med at udvikle Dropbox med fokus på sikkerhed, overholdelse af standarder og beskyttelse af personlige oplysninger.

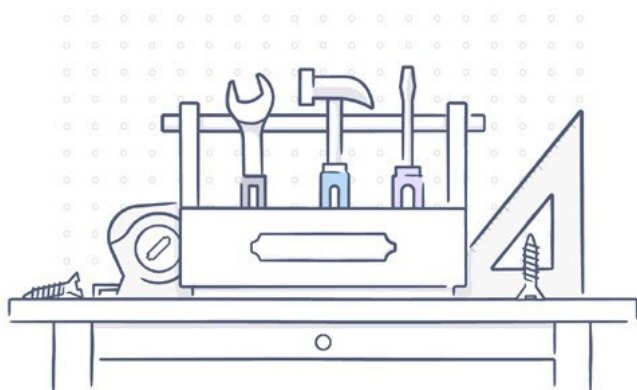
Sikkerhed: Beskyt og kontrollér

Beskyt: Arkitektur og informationssikkerhed

Dropbox er designet med en sikker, distribueret infrastruktur med flere beskyttelseslag, herunder sikker dataoverførsel, kryptering, netværkskonfiguration og kontroller på applikationsniveau fordelt på en skalerbar, sikker infrastruktur. Vores robuste rammer for styring af informationssikkerhed er designet til at vurdere risici og opbygge en sikkerhedskultur hos Dropbox. Vi gennemgår og opdaterer regelmæssigt sikkerhedspolitikker; giver vores ansatte sikkerhedsuddannelse; udfører applikations- og netværkssikkerhedstestning (inklusive penetrationstest); foretager risikovurderinger og overvåger overholdelsen af sikkerhedspolitikker. Fuldstændige detaljer kan findes i vores [DropboxBusinessSikkerhedsHvid-bog](#).

Kontrol: Bemyndigelse af IT-administratorer

Dropbox leverer de [kontrol- og synlighedsfunktioner](#), som IT-administratorer har brug for, og hjælper dig med lettere at administrere dine overholdelsesforpligtelser. Vores dashboard for administratorer gør det muligt for dig at overvåge teamaktivitet, se forbundne enheder og overvåge delingsaktivitet. Du kan skabe grupper for let at administrere teammedlemmers adgang til specifikke mapper og teammappe-administratoren giver dig synlighed og kontrol over teammapper, inklusive synkroniseringsadministration. Funktionen for linktilladelser betyder, at du kan beskytte delte links med kodeord, indstille udløbsdatoer for udstedelsen af midlertidig adgang samt begrænse adgangen til kun at omfatte dem i din organisation. Vores værktøj til kontooverførsel gør det nemt for dig at overføre filer fra én bruger til en anden, når ansvar ændrer sig. Fjernsletning gør det muligt for dig at rydde filer fra tabte eller stjålne enheder.



Overholdelse af standarder: Hav tillid til, og verificer

Overholdelse er en effektiv måde at validere en services troværdighed. Vi opfordrer til og forventer at du [verificerer](#), at vores sikkerhedspraksis overholder de mest accepterede [standarder og forskrifter](#) som ISO 27001, 27017, 27018 og SOC 1, 2 og 3. Vores uafhængige tredjepartsrevisorer tester vores kontroller og leverer deres rapporter og udtalelser - som vi deler med dig, når det er muligt. Mere information om de standarder, som vi overholder, og hvordan vi verificerer vores sikkerhedspraksis, findes på vores [complianceweb-side](#).

Beskyttelse af personlige oplysninger: Vores forpligtelse

Du ejer dine data, og uanset om det er dine personlige oplysninger eller arbejdsoplysninger, tager vi vores brugere tillid seriøst og arbejder hårdt for at sikre, at alle data i vores systemer er beskyttet. Vores [privatlivspolitik](#) beskriver klart, hvordan vi håndterer og beskytter dine oplysninger. Vi offentliggør en [gennemsigtslighedsrapport](#) og vores [principper for regeringsdataanmodninger](#) for at dele, hvor ofte vi modtager, gennemgår og besvarer disse anmodninger, og vi forsøger også at reformere love for at gøre dem mere beskyttende for dit privatliv.

Arbejder sammen for at holde dine data sikre

Dropbox arbejder med sine erhvervskunder for at holde deres data sikre. Vi træffer omfattende foranstaltninger for at beskytte vores infrastruktur, netværk og applikationer; uddanner medarbejdere i sikkerhed og privatlivspraksis; opbygger en kultur, hvor tillidsværdighed er den højeste prioritet og udsætter vores systemer og praksis for streng tredjepartstest og -revision. Kunder spiller også en nøglerolle i at sikre, at deres teams og data er beskyttede og sikre. Dropbox giver dig mulighed for at konfigurere, bruge og overvåge din konto på måder, der imødekommer din organisations behov for sikkerhed, privatliv og overholdelse. Vores [guide til delt ansvar](#) kan hjælpe dig med at forstå mere om, hvad vi gør for at holde din konto sikker, og hvad du kan gøre for at bevare synligheden og kontrollen over dit teams data.

Indholdet i denne vejledning er til for at hjælpe med adgang til information og udgør ikke juridisk rådgivning. Læsere bør, om nødvendigt, indhente deres egen juridiske rådgivning.

