Allmänna dataskyddsförordningen

Allmänna dataskyddsförordningen (GDPR) är en EU-förordning som fastställer ett nytt ramverk för hantering och skydd av EU-medborgarnas personuppgifter.

Den inför nya skyldigheter och förpliktelser för alla organisationer som hanterar personuppgifter och nya rättigheter för individer avseende hur deras personuppgifter samlas in, behandlas och lagras.

Effekter av GDPR

Om din organisation måste efterleva GDPR finns det ett antal faktorer som bör övervägas. Vi rekommenderar starkt att du söker rättslig rådgivning för att avgöra vad som kan krävas i just din situation.

1. Förstå dina data

För att kunna skydda data ordentligt måste du förstå hur de behandlas i din organisation – hur personuppgifter hanteras, delas, används, arkiveras och raderas. Att förstå vilka data som hanteras samt hur de används och lagras är ett viktigt krav för att bygga upp ditt företags GDPR-strategi.

2. Fastställa ägarskap och ansvarsskyldighet

Det är viktigt att identifiera en ansvarig ägare för efterlevnad av dataskyddet. I vissa organisationer måste ett dataskyddsombud utses. GDPR införde också en ny ”ansvarighetsprincip” som kräver att organisationer antar ett program för efterlevnad av dataskyddet. Organisationerna måste ta fram interna dataskyddspolicyer och utbilda personalen.

3. Säkerställa en rättslig grund för behandling

En annan GDPR-komponent som företag måste dokumentera är de rättsliga grunderna för att behandla de olika typer av personuppgifter som du hanterar. Om du till exempel använder samtycke som grund för behandling måste du fundera på hur samtycke ges och tydligt kunna visa hur och när det har getts.

4. Förstå de registrerades rättigheter

För att du ska kunna säkerställa att dina förfaranden tillgodoser dem måste se till att du förstår de rättigheter som människor har i förhållande till sina personuppgifter. Till exempel har de registrerade rätt att få tillgång till sina personuppgifter samt till att få dem rättade, raderade eller exporterade elektroniskt. Under vissa omständigheter har användare också rätt att invända mot automatiserat beslutsfattande och profilering.

5. Säkerställa inbyggt integritetsskydd

För första gången är inbyggt integritetsskydd ett uttryckligt lagstadgat krav, så det är viktigt att börja fundera på hur det kan integreras i ditt företags processer. Under vissa omständigheter är det också nödvändigt att göra konsekvensanalyser avseende integritet.

6. Förbereda hantering av incidenter

Att se till att policyer och processer för hantering av dataincidenter är uppdaterade och testade är avgörande för ett robust dataskyddsprogram. Enligt GDPR ska incidenter upptäckas och rapporteras till behöriga myndigheter så snabbt som möjligt och böter kan utkrävas för både utebliven rapportering och incidenter.

7. Kommunicera viktig information

Se till att de integritetspolicyer som din organisation har online samt andra meddelanden är uppdaterade och omfattar dataskyddspraxis. De nya kraven inbegriper att redogöra för den rättsliga grunden för din behandling och upplysa användarna om den myndighet de kan framföra klagomål till om ett problem uppstår.

8. Samarbeta med dina leverantörer

För att efterleva skyldigheterna i GDPR måste du se bortom din organisations egna policyer. Alla tredje parter som behandlar personuppgifter för din räkning måste också uppfylla de obligatoriska standarderna för dataskydd. Bland annat kan du vilja ställa följande frågor till dina leverantörer:

- Har de robusta strategier för nätverks- och informationssäkerhet, integritet och dataskydd?
- Efterlever de internationellt accepterade standarder och verifierar de efterlevnaden?
- Hur kan de påvisa en stark kultur av tillit och säkerhet? Och vilka kontroller erbjuder de för att hjälpa dig att hantera dina data och uppfylla dina skyldigheter som personuppgiftsansvarig?

Dropbox: skydda dina data

Förtroende utgör grunden för vårt förhållande med miljontals människor och företag världen över.

Vi värdesätter det förtroende du gett oss och tar vårt ansvar att skydda din information på yttersta allvar. För att förtjäna ditt förtroende, skapade vi Dropbox med emfas på säkerhet, efterlevnad och sekretess, och vi kommer även i fortsättningen utveckla tjänsten utifrån dessa principer.

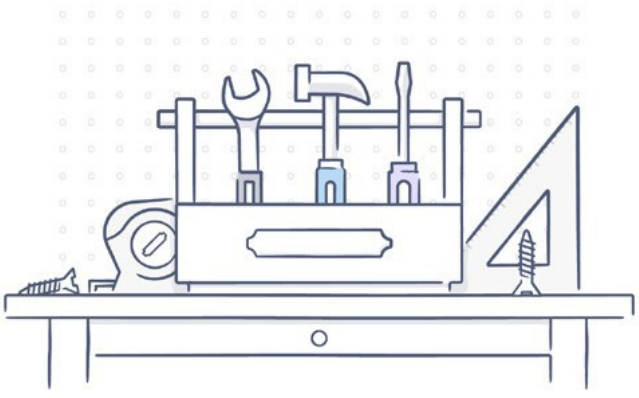
Säkerhet: Skydd och kontroll

Skydda: arkitektur och informationssäkerhet

Dropbox har utformats med en säker, distribuerad infrastruktur med flera skyddslager, inbegripet säker dataöverföring, kryptering, nätverkskonfiguration och kontroller på applikationsnivå som distribueras över en skalbar, säker infrastruktur. Vårt robusta ramverk för hantering av informationssäkerhet har utformats för att bedöma risker och bygga en säkerhetskultur hos Dropbox. Vi granskar och uppdaterar säkerhetspolicyer regelbundet, utbildar vår personal i säkerhet, säkerhetstestar applikation och nätverk (inbegripet penetrationstester), gör riskbedömningar samt övervakar efterlevnaden av säkerhetspolicyer. Mer information finns i Dropbox Business Security White Paper.

Styra: stärka IT-administratörer

Dropbox tillhandahåller de kontroll- och synlighetsfunktioner som IT-administratörer behöver och hjälper dig att enklare hantera efterlevnadsskyldigheterna. Med vår adminpanel kan du övervaka teamets aktivitet, visa anslutna enheter och granska delningsaktivitet. Du kan skapa grupper för att enkelt hantera teammedlemmarnas åtkomst till specifika mappar, och teammapphanteraren ger dig synlighet och kontroll över teammappar, inbegripet synkhantering. Funktionen för länkbehörigheter innebär att du kan lösenordsskydda delade länkar, ställa in utgångsdatum för att ge tillfällig åtkomst och begränsa åtkomst till dem inom din organisation. Med vårt verktyg för kontoöverföring kan du enkelt överföra filer från en användare till en annan när ansvar ändras. Med fjärradering kan du ta bort filer från borttappade eller stulna enheter.



Efterlevnad: Förtroende och verifiering

Efterlevnad är ett effektivt sätt att kontrollera en tjänsts trovärdighet. Vi uppmuntrar och förväntar oss att du kontrollerar att våra säkerhetsrutiner efterlever de mest accepterade standarderna och föreskrifterna som ISO 27001, 27017, 27018 samt SOC 1, 2 och 3. Våra oberoende tredjepartsgranskare testar våra kontroller och tillhandahåller rapporter och åsikter – som vi delar med dig när det är möjligt. Mer information om de standarder vi efterlever och hur vi verifierar våra säkerhetsrutiner finns på vår webbplats om efterlevnad.

Sekretess: Vårt åtagande

Du äger dina data och oavsett om det är personlig eller jobbrelaterad information tar vi våra användares förtroende på allvar och arbetar hårt för att se till att alla data i våra system skyddas. Vår integritetspolicy beskriver tydligt hur vi hanterar och skyddar din information. Vi publicerar en insynsrapport och våra principer om dataförfrågningar från statliga myndigheter för att dela med oss av uppgifter om hur ofta vi tar emot, granskar och svarar på dessa förfrågningar. Vi försöker även reformera lagarna så att de värnar bättre om din integritet.

Samarbete för att hålla dina data säkra

Dropbox arbetar tillsammans med sina företagskunder för att hålla deras data säkra. Vi vidtar omfattande åtgärder för att skydda vår infrastruktur, vårt nätverk och våra applikationer: vi utbildar personalen i säkerhets- och integritetsrutiner, bygger en kultur där tillförlitlighet har högsta prioritet och låter våra system och rutiner genomgå rigorös tredjepartstestning och -revision. Kunderna spelar också en avgörande roll för att se till att deras egna team och data är skyddade och säkra. Med Dropbox kan du konfigurera, använda och övervaka ditt konto på sätt som efterlever din organisations säkerhets-, integritets- och efterlevnadsbehov. Vår guide om delat ansvar kan hjälpa dig att förstå mer om vad vi gör för att hålla ditt konto säkert och vad du kan göra för att bibehålla synlighet och kontroll för ditt teams data.