

Hva er GDPR?

Personvernforordningen, ofte kjent som GDPR står for General Data Protection Regulation, og det er en forordning vedtatt av Europaparlamentet og Rådet for Den europeiske union den 27. april 2016. Forordningen trådte i kraft den 25. mai 2018.

GDPR har som mål å styrke og samordne personvernreglene for enkeltpersoner i hele EU og EØS-området, samt å gi enkeltpersoner mer kontroll over sine egne personopplysninger.

Hovedmål med GDPR

1. Beskyttelse av personopplysninger:
 - GDPR etablerer regler for hvordan personopplysninger skal samles inn, lagres, behandles, og deles. Målet er å beskytte enkeltpersoners rett til privatliv.
2. Enhetlige regler:
 - GDPR søker å samordne personvernreglene over hele EU og EØS for å skape et ensartet regelverk som forenkler administrasjonen av personvernkravene for organisasjoner som opererer på tvers av landegrensene.
3. Styrking av enkeltpersoners rettigheter:
 - GDPR gir enkeltpersoner flere rettigheter, som retten til innsyn, rett til korrigering, rett til sletting (også kjent som «retten til å bli glemt»), rett til å begrense behandlingen av dataene sine, og rett til dataportabilitet.
4. Ansvarlighet for organisasjoner:
 - GDPR pålegger organisasjoner strengere krav til hvordan de håndterer personopplysninger, og de må være i stand til å dokumentere at de overholder forordningen.

Viktige begreper i GDPR

1. Personopplysninger:
 - All informasjon som kan brukes til å identifisere en person, enten direkte eller indirekte, som navn, e-postadresse, telefonnummer, IP-adresse, osv.
2. Behandling av personopplysninger:
 - All aktivitet som involverer personopplysninger, som innsamling, lagring, organisering, endring, gjenfinning, bruk, utlevering, eller sletting.
3. Behandlingsansvarlig:
 - Den personen eller organisasjonen som bestemmer formålet med og midlene for behandlingen av personopplysninger.
4. Databehandler:
 - Den personen eller organisasjonen som behandler personopplysninger på vegne av den behandlingsansvarlige.
5. Samtykke:
 - En frivillig, spesifikk, informert og utvetydig indikasjon på den registrertes ønsker, som gir samtykke til behandling av deres personopplysninger.

Viktige bestemmelser i GDPR

1. Rett til innsyn:
 - Enkeltpersoner har rett til å få tilgang til hvilke personopplysninger som er lagret om dem, og hvorfor de blir behandlet.
2. Rett til å bli slettet:
 - Personer kan be om at deres personopplysninger blir slettet hvis de ikke lenger er nødvendige for formålet de ble samlet inn for.
3. Rett til dataportabilitet:
 - Enkeltpersoner kan få sine personopplysninger overført til en annen organisasjon eller tilbake til seg selv i et strukturert, vanlig brukt og maskinlesbart format.
4. Databehandleravtaler:
 - Organisasjoner som bruker tredjepartsleverandører til å håndtere personopplysninger må ha formelle avtaler som sikrer at personvernreglene overholdes.
5. Personvern ved design og standardinnstillinger:
 - Organisasjoner må sikre at personvern er integrert i prosesser og systemer fra begynnelsen av ("privacy by design" og "privacy by default").
6. Meldingsplikt om brudd på personopplysninger:
 - Organisasjoner må melde brudd på personopplysninger til relevante tilsynsmyndigheter innen 72 timer etter at de har blitt kjent med bruddet.

Hvordan påvirker GDPR?

For enkeltpersoner

- Mer kontroll:
 - Du får større kontroll over dine personopplysninger og hvordan de brukes.
- Rettigheter:
 - Du kan be om innsyn, korrigering, sletting, eller begrensning av dine personopplysninger.
- Klage:
 - Du kan klage til datatilsynet hvis du mener dine rettigheter er blitt krenket.

For organisasjoner

- Lovpålagte krav:
 - Organisasjoner må følge GDPRs krav og være i stand til å dokumentere etterlevelse.
- Risiko og ansvar:
 - Brudd på GDPR kan medføre store bøter og juridiske konsekvenser.
- Forbedret personvern:
 - GDPR oppfordrer organisasjoner til å forbedre sine personvernpraksiser og skape mer transparente prosedyrer.

Hvem må overholde GDPR?

GDPR gjelder for alle organisasjoner som behandler personopplysninger av enkeltpersoner i EU og EØS, uavhengig av hvor organisasjonen er basert. Det betyr at internasjonale selskaper som opererer i EU/EØS må overholde GDPR-regelverket.

Viktige aktører

- Datatilsynet: Den nasjonale tilsynsmyndigheten som overvåker at GDPR etterleves. I Norge er dette Datatilsynet.