Elavon

Gjør deg klar

En veiledning til personvernforordningen (GDPR)

elavon.no

Personvernforordningen (*General Data Protection Regulation*, GDPR) skal regulere personvern og håndtering av personopplysninger for enkeltpersoner i den europeiske unionen (EU) og EØS, hvor Norge også er inkludert. Denne veiledningen forklarer hva den nye forordningen innebærer, hvordan den vil påvirke enkeltpersoner og bedrifter, og forklarer deg alt du trenger å vite om den nye loven.

Sammendrag om GDPR

Når iverksettes den nye forordningen?

25. mai 2018

Hva er nytt?

Dette er nye rettigheter som gir personer tilgang til informasjon selskaper har om dem, forpliktelser for bedre datahåndtering for bedrifter og et nytt regime for bøter.

Hva er GDPR?

I januar 2012 fastsatte EU-kommisjonen planer for en personvernreform i hele EU for å gjøre Europa «klar for den digitale tidsalderen». Nesten fire år senere er det oppnådd enighet om hva dette innebærer og hvordan det skal iverksettes.

En av hovedkomponentene i reformene er innføringen av personvernforordningen. Dette nye EU-rammeverket gjelder for organisasjoner i alle medlemslandene og for globale bedrifter som driver forretninger med enkeltpersoner i EU.

GDPR er i bunn og grunn et nytt sett med regler som er utformet for å gi folk økt kontroll over opplysningene sine. Den tar sikte på å forenkle regelverket for handel, slik at både enkeltpersoner og bedrifter kan dra full nytte av den digitale økonomien.

Reformene er utformet for å gjenspeile den verdenen vi lever i nå, og bringer lover og forpliktelser over hele Europa opp til et nivå tilpasset internettalderen.

Nesten hvert eneste aspekt av livene våre dreier seg nesten uunngåelig rundt data. Fra sosiale medieselskaper, til banker, forhandlere og regjeringer – nesten hver eneste tjeneste vi bruker innebærer innsamling og analyse av personopplysningene våre. Ditt navn, din adresse, ditt betalingskortnummer m.m. samles inn, analyseres og – kanskje viktigst – lagres av organisasjoner. GDPR tar sikte på å harmonisere regulering over hele Europa for å gjenspeile landskapet i dagens datautveksling.

Hva betyr det for organisasjonen min?

GDPR vil gjelde for enhver organisasjon eller person som håndterer personopplysninger for personer i EU og EØS. Selskaper og enkeltpersoner utenfor EU og EØS som selger varer og tjenester til enkeltpersoner som bor i EU og EØS må også overholde den nye loven. Det betyr at nesten alle større selskaper i verden må være klare når GDPR trer i kraft og begynne å jobbe med sin strategi for å etterleve GDPR. GDPR gjelder for behandlingsansvarlige, for de med felles behandlingsansvar og for databehandlere, men forpliktelsene for rollene er forskjellige.

Er du en behandlingsansvarlig eller en databehandler?

De forskjellige vilkårene

Personvernlovgivningen har tre ulike kategorier, da ikke alle som håndterer personopplysninger er like: behandlingsansvarlig, felles behandlingsansvar og databehandler. Her er hva de innebærer:

Behandlingsansvarlig

En behandlingsansvarlig er enheten (en person eller et selskap) som bestemmer formålet med og metoder for behandling av personopplysninger.

Felles behandlingsansvar

Der to eller flere selskaper i fellesskap bestemmer formålene og metodene for behandling av personopplysninger, f.eks. at de i fellesskap bestemmer formålene/årsakene, anledningen, naturen, og omfanget og målene for databehandlingen.

Databehandler

Personen eller gruppen som behandler dataene på vegne av den ansvarlige. Databehandling er å innhente, registrere, tilpasse eller lagre personopplysninger.

Den samme enheten kan være både behandlingsansvarlig og databehandler, avhengig av omstendighetene. For eksempel vil et teknologiselskap som tilbyr betalingsbehandling til nettbutikker være databehandleren, og brukerstedet den behandlingsansvarlige. Men hvis dette teknologiselskapet pakker de samme personopplysningene for å gi målrettede kundesegmenter til annonsører, fungerer det som en behandlingsansvarlig.

GDPR plasserer de endelige juridiske forpliktelsene på en behandlingsansvarlig. Den behandlingsansvarlige skal opprettholde oppføringer på personopplysninger og hvordan de behandles. Dette gir et mye høyere nivå av juridisk ansvar hvis organisasjonen skulle oppleve databrudd.

Den behandlingsansvarlige vil også bli tvunget til å sikre at alle kontrakter med databehandlere etterlever GDPR.

Hva er personopplysninger og sensitive personopplysninger?

Den typen opplysninger som anses som personlige under eksisterende lovgivning inkluderer navn, adresse og bilder. GDPR utvider definisjonen av personopplysninger slik at opplysninger som en IP-adresse kan være en personopplysning under visse omstendigheter. Den inkluderer også sensitive personopplysninger som genetiske og biometriske data, som kan identifisere en enkeltperson.

Personopplysninger

Opplysninger relatert til en levende enkeltperson som kan identifiseres direkte eller indirekte, for eksempel:

- Navn
- Telefonnummer
- E-postadresse
- Betalingskortnummer

Sensitive personopplysninger

Personopplysninger som inneholder informasjon som:

- Den registrertes rase eller etniske opprinnelse
- Politiske meninger
- Religiøs tro eller annen overbevisning av liknende natur
- Fagforeningsmedlemskap
- Fysisk eller psykisk helse eller tilstand
- Seksualliv

Hva GDPR angir

Det finnes 99 artikler i GDPR. Disse spenner fra generelle bestemmelser, ansvaret til den behandlingsansvarlige, felles behandlingsansvar og ansvaret til databehandleren, til samarbeid med tilsynsmyndigheter.

Viktige endringer som kan påvirke organisasjonen din inkluderer:

- **Innebygget personvern** – personvern må fra starten av bygges inn i forretningsprosesser og -systemer og leveres som standard
- **Retten til å bli glemt** – brukere kan be om at opplysningene deres slettes; de kan også be om at en kopi skal sendes til en tredjepart
- **Obligatorisk varsel ved brudd på personopplysningssikkerheten –** enkelte brudd på personopplysningssikkerheten må nå rapporteres til myndighetene innen 72 timer, og til berørte personer umiddelbart
- **Bøter ved manglende etterlevelse** – GDPR tillater bøter på opptil 20 millioner euro eller 4 % av selskapets årlige globale omsetning, avhengig av hvilket beløp som er størst

Hvordan ser etterlevelse av GDPR ut?

Det finnes ingen overordnet tilnærming for å forberede GDPR.

Hver bedrift må undersøke akkurat hva som må til for å etterleve. Dette er det viktig å forstå enten du er databehandler eller behandlingsansvarlig. De fleste selskaper vil trolig være begge, avhengig av de spesifikke dataene de mottar.

Hvordan forberede seg

- Begynn med å få en forståelse av hvilke personopplysninger dere har og hvem som har tilgang til dem
- Begrens tilgang basert på forretningsbehov og implementer overvåking for å oppdage uautorisert tilgang
- Utfør en vurdering av hvilke etterlevelses- og sikkerhetskontroller dere har på plass for å samle inn og beskytte opplysningene, hvor effektive de er, og hvor det finnes hull
- Utvikle en plan for å forbedre sikkerhetsprogrammet deres ved å fokusere på mennesker, prosess og teknologi
- Iverksett en varslingsprosess ved brudd på personopplysningssikkerheten, inkludert hendelsesdeteksjon og responsmuligheter
- Noen organisasjoner må også ha en personvernansvarlig (*Data Protection Officer*, DPO)

PCI DSS-rammeverket støtter etterlevelse av GDPRs sikkerhetskrav

GDPR beskriver ikke et etterlevelses-/sikkerhetsrammeverk i detalj. Betalingskortindustriens datasikkerhetsstandarder (*Payment Card Industry Data Security Standards*, PCI DSS) gir imidlertid et nyttig utgangspunkt for et program for etterlevelse og administrering av personopplysninger. Ved å erstatte ett ord («kortholder» med «personopplysninger») innenfor de 12 hovedkravene for PCI DSS, vil man få en logisk oppbygning fra «betaling» til «personlig» for tilnærming til etterlevelse av GDPRs sikkerhetskrav:

Mål	Krav
Bygge og opprettholde et sikkert nettverk	1. Installere og opprettholde en brannmurkonfigurasjon for å beskytte **personopplysninger** 2. Ikke bruk systemgitt standard passord eller andre standard sikkerhetsparametere som tilbys av leverandører
Beskytte kortholderdata	3. Beskytte lagrede **personopplysninger** 4. Kryptere overføring av **personopplysninger** over åpne, offentlige nettverk
Opprettholde et styringsprogram for sårbarhet	5. Bruke og regelmessig oppdatere antivirusprogramvare eller -programmer 6. Utvikle og vedlikeholde sikkerhetssystemer og -applikasjoner
Implementere strenge tiltak for tilgangskontroll	7. Begrense tilgang til **personopplysninger** etter forretningsmessig «behov for å vite» 8. Tilordne en unik ID til hver av personene som har datatilgang 9. Begrense fysisk tilgang til **personopplysninger**
Overvåke og teste nettverk regelmessig	10. Spore og overvåke all tilgang til nettverksressurser og **personopplysninger** 11. Teste sikkerhetssystemer og -prosesser regelmessig
Opprettholde retningslinjer for informasjonssikkerhet	12. Opprettholde retningslinjer angående informasjonssikkerhet for alt personell

Hvis dere etterlever PCI DSS og behandler alle personopplysningene deres og viktige data på samme måte som dere behandler kortholderdata, er dere godt på vei. PCI DSS dekker ikke alt som er fastsatt av GDPR, men gir et nyttig utgangspunkt for håndtering av datasikkerhet (artikkel 32 EU GDPR – «Sikkerhetsbehandling»).

Forbered sjekkliste for etterlevelse av GDPR

- ☐ Etabler et arbeidsprogram for å lage en oversikt over prosessene deres relatert til personopplysninger.
- ☐ Ha en prosess hvor dere risikovurderer egne opplysninger.
- ☐ Ha en forståelse for hvor og hvordan dere deler personopplysninger med tredjeparter, og sørg for at dere har de riktige kontraktene på plass for å overholde GDPR.
- ☐ Vurder sikkerhetsprogrammet deres når det kommer til informasjon som personopplysninger, inkludert tredjeparter dere deler disse dataene med.
- ☐ Opptre i overensstemmelse med betalingskortindustriens datasikkerhetsstandarder (PCI DSS) for grunnleggende sikkerhet rundt personopplysninger og kortholderdata.
- ☐ Sørg for at informasjonen og samtykkespråket dere bruker til kundene er åpent, klart, entydig og skrevet på vanlig språk.
- ☐ Skisser en plan for å etterleve de mer komplekse rettighetene til de registrerte, inkludert rettigheter til tilgang, rettigheter til korrigering, rettigheter til dataportabilitet og rettigheter til sletting.
- ☐ Etabler et system for å identifisere om, når og hvor brudd skjer, og hvordan dere skal håndtere dette.
- ☐ Ha en juridisk etterforsker for PCI (*PCI Forensic Investigator*, PFI) klar ved et eventuelt brudd relatert til kortopplysninger.

Hva er konsekvensene ved manglende etterlevelse?

Bedrifter som ikke har iverksatt tiltak for å sikre at behandlingen av personopplysningene deres oppfyller de nye forpliktelsene under GDPR, kan bli ansvarlig for bøter relatert til manglende etterlevelse. Disse bøtene kan pålegges både behandlingsansvarlige og databehandlere.

Manglende etterlevelse av GDPR kan resultere i bøter på opptil 20 millioner euro eller 4 % av hovedselskapets årlige globale omsetning, et tall som for noen kan bety millioner eller det å bli slått konkurs.

Bøtene vil avhenge av bruddets alvorlighetsgrad og om selskapet vurderes til å ha tatt etterlevelse og forskrifter rundt sikkerhet på alvor.

Den maksimale boten på 20 millioner euro eller 4 % av global omsetning, avhengig av hvilket beløp som er størst, er for overtredelser av rettighetene til de registrerte, uautorisert internasjonal overføring av personopplysninger og manglende innføring av prosedyrer eller ignorering av forespørsler om tilgang til opplysningene deres.

Den nedre grensen, på 10 millioner euro eller 2 % av global omsetning, vil gjelde selskaper som misbruker opplysninger på andre måter. De inkluderer, men er ikke begrenset til, manglende rapportering ved brudd på sikkerheten rundt personopplysninger, manglende implementering av innebygget personvern og manglende sikring av at personvern utføres i første fase av et prosjekt, og etterlevelse ved utnevning av en personvernansvarlig (hvis aktuelt).

Spørsmål du kanskje må ta stilling til:

- Hvordan får vi samtykke fra ansatte?
- Nøyaktig hva skal jeg registrere i forbindelse med prosesseringsaktiviteter?
- Er vi den behandlingsansvarlige for informasjon om ansatte som vi sender videre til pensjons- og trygdeaktører?
- Hvordan passer PCI DSS inn i alt dette og er den nyttig?
- Trenger vi en personvernansvarlig (DPO)?
- Hva gjør vi med alle markedsføringsdataene våre?

Kontakt oss nå på **brukersted@elavon.com** for mer informasjon.

La oss jobbe sammen

Vi gjør det mulig. **Dere får det til å skje.**

brukersted@elavon.com

+47 24 15 99 19 **elavon.no**

Elavon Financial Services DAC Norway Branch - Organisasjonsnummer 991 283 900.
Besøksadresse: Karenlyst Allé 11, 0278 Oslo; Postadresse: Postboks 354 Skøyen, 0213 Oslo, Norge.
Hovedkontor: Elavon Financial Services DAC, Irsk organisasjonsnummer 418442; Besøksadresse: Building 8, Cherrywood Business Park, Loughlinstown, Co. Dublin, D18 W319, Irland.
Elavon Financial Services DAC Norway Branch opererer under det registrerte varemerket Elavon Merchant Services, er regulert av Irlands sentralbank.
Y2633v10118