Hva er GDPR, og hva betyr det for din båtforening?

Internett har revolusjonert både hvordan vi kommuniserer og måten vi utfører hverdagslige gjøremål på. Nå skjer alt digitalt. Vi sender e-post, deler dokumenter, betaler regninger og handler varer, og hver gang oppgir vi personopplysninger på internett uten å ofre det en tanke.

Har du noen gang tenkt på hvor mye personlig informasjon du har lagret på Internett? Og hva som skjer med den informasjonen?

Det handler om bankopplysninger, kontakter, adresser, innlegg i sosiale medier, IP-adressen din og nettsidene du har besøkt – alt lagres digitalt.

Selskaper forteller deg at de samler inn denne typen informasjon slik at de kan yte bedre service og tilby mer målrettet og relevant kommunikasjon, alt for å gi deg en bedre kundeopplevelse.

Men hva er det egentlig de bruker opplysningene til?

Dette spørsmålet har blitt stilt og besvart i EU, og er grunnen til at det i mai 2018 trer i kraft en ny lov for personvern, **GDPR** (General Data Protection Regulation), som vil endre måten vi samler inn, bruker, håndhever og lagrer persondata.

I denne artikkelen hjelper vi deg med å forstå hva GDPR er, hvordan forordningen kommer til å påvirke din bedrift, samt at vi gir deg praktiske tips om hvordan du kan begynne å forberede deg på GDPR allerede i dag.

Hva er GDPR?

25. mai 2018 trer den nye europeiske personvernforordningen, **The General Data Protection Regulation** (GDPR), i kraft. Forordningen kommer til å implementeres i alle lokale personvernlover i hele EU og EØS-området. Den vil gjelde for alle selskaper som selger til- og lagrer personlig informasjon om europeiske statsborgere, inkludert selskaper på andre kontinenter. Den gir innbyggere i EU og EØS større kontroll over sine egne personopplysninger og sikrer at informasjonen beskyttes i hele Europa.

Ifølge GDPR-forordningen omfatter personopplysninger all informasjon som kan relateres til en person, f.eks. navn, bilde, e-postadresse, bankopplysninger, innlegg i sosiale medier, informasjon om din nåværende og/eller tidligere plasseringer, helseinformasjon eller IP-addressen til datamaskinen din.

Det skilles ikke mellom personopplysninger for individers private, offentlige eller jobbmessige roller – også i en B2B-situasjon er det enkeltpersoner som interagerer og deler informasjon med og om hverandre. Kundene i B2B-markedet er åpenbart selskaper, men relasjonene som håndterer forretningene består av enkeltpersoner.

Ifølge GDPR har enkeltpersoner:

1. Rett til tilgang

Loven gir enkeltpersoner rett til å kreve tilgang sine personopplysninger og til å vite hvordan informasjonen brukes av selskapet etter at den er samlet inn. Selskapet skal levere ut en kopi av disse personopplysningene, uten kostnad og i elektronisk format, dersom enkeltpersonen ber om dette.

2. Rett til å bli glemt

Hvis forbrukere ikke lenger er kunder, eller hvis de trekker tilbake samtykket de har gitt et selskap for å bruke vedkommendes personopplysninger, har forbrukeren rett til å få informasjonen slettet.

3. Rett til å overføre data

Individer har rett til å overføre opplysninger fra en tjenesteleverandør til en annen. Og dette må skje i et vanlig og maskinlesbart format.

4. Rett til å bli informert

Dette dekker alle typer innsamling av personopplysninger av selskaper, og enkeltpersoner må informeres før opplysningene samles inn. Forbrukerne må godkjenne at personopplysninger samles inn, og samtykke skal gis aktivt, ikke være underforstått.

5. Rett til å korrigere informasjon

Dette sikrer at enkeltpersoner kan oppdatere informasjonen hvis den er utdatert, ufullstendig eller feilaktig.

6. Rett til begrenset behandling

Enkeltpersoner kan be om at deres opplysninger ikke brukes i databehandling. Informasjonen kan fortsatt lagres men den skal ikke brukes.

7. Rett til å motsette seg behandling

Dette inkluderer retten til å motsette seg behandling av personopplysninger til bruk i direkte markedsføring. Det er ingen unntak for denne regelen, og all behandling må stoppes så fort denne forespørselen er mottatt. Denne rettigheten må kommuniseres tydelig til enkeltpersoner i starten av enhver kommunikasjon.

8. Rett til å bli varslet

Hvis det har vært datainnbrudd som kan få følger for enkeltpersoners opplysninger, har personen rett til å få vite dette i løpet av 72 timer etter at innbruddet ble oppdaget.

GDPR er EUs måte å gi individer, enten de er prospekter, kunder, underleverandører eller ansatte mer oversikt og kontroll over sine egne personopplysninger og redusere makten til organisasjonene som samler inn og bruker slike opplysninger for egen vinning (egen fortjeneste). Det er ikke et forsøk på å forhindre eller komplisere forretningen, men skape mer bevissthet og åpenhet rundt hvordan personopplysninger lagres og brukes.

Forretningsmessige konsekvenser av GDPR

Denne nye personvernforordningen gir forbrukeren mer makt, og arbeidet med å overholde forordningen legges på selskaper og organisasjoner.

Kort sagt gjelder GDPR for alle selskaper og organisasjoner som er etablert i EU, uansett om databehandlingen foregår i EU eller ikke. Også organisasjoner som ikke er etablert i EU vil bli underlagt GDPR. Hvis virksomheten tilbyr varer og/eller tjenester til EU-statsborgere, er den underlagt GDPR.

Alle organisasjoner og selskaper som jobber med personopplysninger bør ha et personvernombud eller en controller som jobber med GDPR internt.

Det er strenge straffer for selskapene og organisasjonene som ikke overholder GDPR. Bøtene er på opptil **4 % av årlig global omsetning eller 20 millioner euro, det av alternativene som utgjør den høyeste summen.**

Mange tror ar GDPR bare handler om IT, men det er langt fra tilfellet. Forordningen får omfattende konsekvenser for hele virksomheten, inkludert håndteringen av salgs - og markedsføringsaktiviteter.

Konsekvensene av GDPR for kundebehandling

Betingelsene for å innhente samtykke vil bli strengere under GDPR. Det vil kreves samtykke for både lagring og behandling av persondata. Enkeltpersoner kan når som helst trekke tilbake sitt samtykke.

Det må gis eget separat samtykke for ulike markedsføringsaktiviteter. Dette innebærer at du må kunne besvise at enkeltpersoner har gitt samtykke til for eksempel å motta et nyhetsbrev. Samtykket må avgis ved at det foretas en aktiv handling. Dette medfører at man ikke lenger kan ha forhåndsavkryssede bokser for at det kan sies å foreligge et gyldig samtykke.

Disse endringene medfører at bedrifter må håndtere salgs- og markedsføringsaktiviteter annerledes enn tidligere. Selskapene må se over sine interne prosesser, løsninger og webskjemaer for å oppfylle nye regler for lagring og bruk av persondata, samt etterlevelse av lov og «beste praksis».
For at en potensiell kunde skal kunne registere seg som mottaker av kommunikasjon må de fylle ut et skjema (webskjema) og aktivt krysse av i en rute for aksept av lagring av persondata, og en annen for aksept på mottak av kommunikasjon.

Organisasjoner må kunne bevise at samtykke ble gitt i tilfeller der enkeltpersoner nekter å ha akseptert å bli kommunisert til. Dette innebærer at alle data som samles inn må ha et «revisjonsspor» som er tidsstemplet og at man i detalj kan rapportere hva kontakten har samtykket til, når og hvordan.

Hvis du kjøper prospect/markedsføringslister, er du fortsatt ansvarlig for å få korrekt samtykkeinformasjon, selv om en leverandør eller outsourcet partner var ansvarlig for å samle inn opplysningene. I B2B-verdenen møter selgere potensielle kunder på en messe, de utveksler visittkort og når de kommer tilbake til kontoret legger de inn kontaktene i selskapets e-postliste. I 2018 kommer ikke dette lenger til å være mulig å gjøre uten at personen skriftlig bekrefter at dette er OK. Selskaper må finne nye metoder for å samle kundeinformasjon.

Forberedelser til mai 2018

En viktig komponent i GDPR-forordningen er innbygd personvern.

Innbygd personvern krever at alle avdelinger i et selskap grundig gjennomgår personopplysningene de innehar og hvordan de håndterer dem. Det er mange endringer selskaper må foreta for å oppfylle kravene for GDPR. Her er noen første steg for å komme i gang:

1. Kartlegg selskapets personopplysninger

Få oversikt over hvor alle lagrede personopplysninger i hele selskapet stammer fra, og dokumenter hva du bruker opplysningene til. Identifiser hvor opplysningene finnes, hvem som har tilgang til dem og om de utsettes for noen risiko ift deling etc.

2. Bestem hvilke personopplysninger du må beholde

Ikke behold mer informasjon enn du behøver, og fjern alle opplysninger som ikke brukes. Hvis selskapet samler inn masse data uten noe bestemt formål vil du ikke kunne fortsette med dette når GDPR trer i kraft. GDPR oppfordrer til en mer disiplinert behandling av personopplysninger.

I oppryddingsprosessen bør du spørre deg selv:

- Nøyaktig hvorfor lagrer vi disse opplysningene i stedet for å slette dem?
- Hvorfor lagrer vi alle disse opplysningene?
- Hva forsøker vi å oppnå ved å samle inn alle disse kategoriene av personopplysninger?
- Er den økonomiske vinningen ved å slette denne informasjonen større enn ved å kryptere den?

3. Få på plass sikkerhetstiltak

Innfør og iverksett tiltak for å sikre infrastrukturen og forhindre datainnbrudd. Dette innebærer å få på plass rutiner for raskt kunne varsle enkeltpersoner og myndigheter dersom det blir innbrudd.

Sørg også for å kontrollere dette hos dine leverandører. Outsourcing fritar deg ikke fra ansvaret. Du må kontrollere at de også har de rette sikkerhetsrutinene på plass.

4. Se gjennom dokumentasjonen din

Under GDPR må enkeltpersoner gi aktivt samtykke til kjøp og behandling av sine egne personopplysninger. Dette medfører at et forhåndsavkrysset felt ikke er tilstrekkelig til at det skal kunne sies å foreligge et gyldig samtykke. Du må gå gjennom alle personvernerklæringer og opplysninger og justere dem der det er nødvendig.

5. Etablere prosesser for håndtering av personopplysninger

Som tidligere nevnt har enkeltpersoner flere grunnleggende rettigheter ifølge GDPR.

Du må etablere retningslinjer og prosedyrer for hvordan du skal håndtere hver av disse situasjonene.

For eksempel:

1. Hvordan kan enkeltpersoner gi et juridisk samtykke?

2. Hva er prosessen hvis en enkeltperson ønsker å slette personopplysninger?
3. Hvordan kan du være sikker på at dette gjøres i alle plattformer og at informasjonen virkelig slettes?
4. Hvis en enkeltperson ønsker å overflytte sine personopplysninger, hvordan gjennomfører du dette?
5. Hvordan kan du bekrefte at personen som ba om å få personopplysningene overflyttet er den han eller hun utgir seg for?
6. Hva er kommunikasjonsplanen dersom dere skulle utsettes for et datainnbrudd?

Oppsummering

Data er verdifull valuta i det moderne samfunnet.

Samtidig som GDPR skaper ufordringer og hodebry for oss som selskaper og organisasjoner, åpner forordningen også for nye muligheter.

Selskaper som viser at de verdsetter enkeltpersoners personvern (utover å oppfylle kravene i forordningen), som åpent forteller hvordan de bruker opplysningene, som utvikler og implementerer nye og bedre metoder for å håndtere kundedata i hele livssyklusen opplever mer tillit og får mer lojale kunder.

Deadlinen i mai 2018 virker kanskje langt unna akkurat nå, men før du vet ordet av det har dagen kommet. Hvis du ikke allerede har startet forberedelsene, oppfordrer vi deg til å starte nå.

Sett av tid til å forstå hva du behøver å gjøre for å kunne oppfylle kravene og bruk de praktiske tipsene som vi har delt i denne artikkelen som hjelp til å komme i gang.

Etterpå lager du en handlingsplan for prosessen frem til GDPR kravene iverksettes, slik at du har full kontroll i forkant av mai 2018 og kan svare på alle spørsmål fra kunder som gjelder de nye kravene.