NY PERSONDATALOV (GDPR)

– HVAD BETYDER DET FOR DIN VIRKSOMHED?

WEBCRM, SEPTEMBER 2017

Indholdsfortegnelse

Overblik	3
Hvad indebærer GDPR?	4
Hvorfor er GDPR så vigtigt for alle virksomheder?	7
Hvordan skal min virksomhed forholde sig til GDPR?	8
CRM & GDPR	10
FAQ	11

Overblik

Den 25/05 2018 træder en ny persondatalov i kraft. Loven, som bliver gældende i Danmark og resten af EU, benævnes officielt The General Data Protection Regulation (GDPR).

Formålet med den nye lovgivning er at give EU's borgere bedre kontrol over deres personlige dataforhold. Dette skal tilsikres via en række skærpelser der stiller nye og større krav til, hvordan man håndterer data som virksomhed.

Overholder man ikke den nye GDPR-lovgivning kan man som virksomhed tildeles en bøde på op til 4% af ens årlige omsætning.

Derfor er det vigtigt at du allerede nu begynder at kigge på, hvordan I indsamler og anvender personlige data til kommercielt brug i jeres forretning.

Som CRM-leverandør er webCRM naturligvis stærkt fokuseret på at tilsikre, at vores løsning hjælper din virksomhed med at leve op til GDPR. Således er vi i fuld gang med at udvikle en proces der gør denne overgang så enkel og overskuelig som muligt.

Hvad indebærer GDPR?

Den 25. maj 2018 træder den nye europæiske persondataforordning (GDPR) i kraft.

Den nye lovgivning giver borgerne i EU større kontrol over deres egne personlige data og sikrer, at deres information håndteres sikkert og beskyttet i hele Europa - uanset om databehandlingen finder sted i EU eller ej.

GDPR er EU's måde at give enkeltpersoner, kunder og leverandører mere magt over egne data. Samtidig betyder det færre datamuligheder for de virksomheder og organisationer, som indsamler og anvender data til kommercielt brug.

Når GDPR træder i kraft d. 25/05 2018 har alle enkeltpersoner i EU følgende rettigheder, hvad angår de data, der indsamles om dem:

DER SKAL ALTID GIVES TYDELIGT SAMTYKKE

Virksomheder må ikke behandle de personlige data om en enkeltperson, medmindre personen frivilligt har givet specifikt, informeret og entydigt samtykke herom enten i en erklæring eller ved en klart bekræftende handling.

RETTEN TIL ADGANG

Dette giver enkeltpersoner ret til at anmode om adgang til egne personlige data og til at få at vide, hvordan deres data anvendes af virksomheden efter de er indsamlet.

Virksomheden har pligt til at udlevere en kopi af alle de personlige data man besidder om vedkommende, såfremt personen anmoder om det. Udleveringen skal være gratis og i elektronisk format.

RETTEN TIL AT BLIVE GLEMT

Hvis en person ikke længere er kunde hos en virksomhed, eller hvis de tilbagetrækker deres samtykke til, at virksomheden må anvende deres personlige data, har de ret at få deres data slettet permanent.

RETTEN TIL AT FÅ OVERFØRT DATA

Enkeltpersoner har ret til at få overført deres data fra én serviceudbyder til en anden. Dette skal ske i et almindeligt brugt og maskinlæsbart format.

RETTEN TIL AT BLIVE INFORMERET

Denne ret gælder enhver form for indsamling af data som foretages af en virksomhed. En person skal altid informeres før en indsamling af data sker. Personen skal give tilladelse til (opt-in), at deres data indsamles. Samtykket skal være frivilligt og eksplicit - det må ikke have karakter af at være underforstået.

RETTEN TIL AT FÅ INFORMATION TILRETTET

Dette sikrer at enkeltpersoner kan få deres data opdateret, hvis denne er forældet eller på nogen måde utilstrækkelig.

RETTEN TIL AT BEGRÆNSE ANVENDELSE

Enkeltpersoner kan anmode om, at deres data ikke anvendes i praksis. Deres data må opbevares, men må ikke anvendes af virksomheden.

RETTEN TIL AT BLIVE UNDERRETTET

Sker der et brud på datasikkerheden som kan kompromittere et individs personlige data, har personen ret til at blive underrettet indenfor 72 timer fra bruddet opdages af virksomheden.

RETTEN TIL AT GØRE INDSIGELSE MED OMGÅENDE VIRKNING

Der er ingen undtagelser til denne regel. Al behandling af data skal stoppe lige så snart en anmodning modtages. Dette inkluderer retten til at få stoppet behandling af data til markedsføringsmæssige formål. Denne ret skal kommunikeres tydeligt til en hver enkeltperson, når en dialog indledes.

Hvorfor er GDPR så vigtigt for alle virksomheder?

GDPR handler grundlæggende om at skabe mere tillid og gennemsigtighed mellem virksomheder og EU's borgere. Du skal som borger have tillid til, at den virksomhed som har dine data, anvender dem på en måde som du er indforstået med.

Som nævnt indledningsvis, er der hårde straffe i vente for de virksomheder og organisationer som ikke lever op til GDPR. Man kan således blive tildelt en bøde på op til 4% af den årlige globale indtjening eller 20 millioner EUR - afhængigt af hvilket beløb der er højest.

Udover at beskytte de personlige data, opfordres alle virksomheder og organisationer, som håndterer personlige data, også til at udpege en databeskyttelsesansvarlig som skal sikre, at virksomheden lever op til GDPR.

Hvordan skal min virksomhed forholde sig til GDPR?

GDPR gør sig gældende uanset om din virksomheds kunder er forbrugere eller andre virksomheder. Lovgivningen tager udgangspunkt i den enkelte borgers rettigheder - uanset hvilken kontekst dine data om den pågældende person er registreret i. At overholde GDPR er altså lige vigtigt for alle typer af virksomheder.

Derfor er det vigtigt at din virksomhed har etableret klare retningslinjer, politikker og processer for datahåndtering. Vi anbefaler at din virksomhed gennemgår følgende 5 øvelser:

1. SAFETY FIRST

Sørg for at udvikle og implementere sikkerhedsforanstaltninger i hele jeres infrastruktur, så I er garderet mod datasikkerhedsbrud. Det er afgørende at I får etableret et sikkerhedssystem som kan beskytte mod databrud og, at I handler hurtigt og informerer alle relevante personer og myndigheder, hvis der skulle ske et datasikkerhedsbrud.

Sørg også for at tjekke dine leverandører. Outsourcing af tjenester fritager dig ikke for ansvar. Du skal sikre dig, at de også har de rigtige sikkerhedsforanstaltninger på plads.

2. FÅ KORTLAGT JERES DATA

Gå allerede nu i gang med at kortlægge hvor alle de personlige data, som din virksomhed anvender, kommer fra, hvor og hvordan I gemmer denne information og sørg for at dokumentere, hvordan I anvender disse data. I skal identificere præcis hvor alle personlige data findes, hvem der har adgang, og om der er nogen risiko for datamisbrug eller uautoriseret adgang.

3. PRIORITÉR HVAD DER SKAL GEMMES

Gem ikke mere information end nødvendigt og slet data som ikke bruges. Hvis din virksomhed indsamler store mængder data uden noget bestemt formål eller behov, kan det ikke fortsætte, når GDPR træder i kraft. GDPR tilskynder en mere disciplineret behandling af personlige data.

I oprydningsprocessen bør I overveje:

- Hvorfor gemmer vi denne data?
- Hvad ønsker vi at opnå ved at indsamle disse kategorier af personlig information?

4. GENNEMGÅ DIN DOKUMENTATION

Når GDPR træder i kraft skal alle enkeltpersoner aktivt give samtykke til både indsamling og behandling af deres data. Du bliver derfor nødt til at gennemgå alle dine databeskyttelseserklæringer og tilpasse dem, hvor der er behov for det.

5. SØRG FOR AT ETABLERE PROCEDURER FOR HÅNDTERING AF PERSONLIGE DATA

Som gennemgået tidligere, har alle enkeltpersoner 9 grundlæggende rettigheder når GDPR træder i kraft.

Du bør etablere retningslinjer og procedurer for, hvordan du vil håndtere hver af disse situationer:

- Hvordan kan enkeltpersoner give samtykke på lovlig vis?
- Hvad er proceduren hvis en person ønsker at få sine data slettet?
- Hvordan vil du sikre at det sker på tværs af alle platforme, og at data bliver slettet permanent?
- Hvordan vil du håndtere situationer hvor en person ønsker at få overført sine data?
- Hvordan vil du få bekræftet, at den person, som beder om at få overført sine data, er den person, han eller hun giver sig ud for at være?
- Hvad er kommunikationsplanen i tilfælde af et databrud?

CRM & GDPR

Den 25/05 2018 skal alle virksomheder der opererer i EU have en plan på plads for håndteringen af hver af de 9 databeskyttelsesrettigheder. Derfor har de behov for et system, hvor de kan opbevare samtykker, partneraftaler såvel som kundedata. webCRM giver jer naturligvis mulighed for at håndtere denne data i et GDPR-kompatibelt CRM system.

Vi tager GDPR meget seriøst og er i fuld gang med at udvikle de nødvendige tilføjelser til webCRM, der gør, at du som vores kunde har alle muligheder for at være fuldt ud GDPR-kompatibel d. 25/05 2018.

Allerede i dag giver vores løsning jer mulighed for at leve op til de langt de fleste af GDPR-kravene – dette forudsætter selvfølgelig, at jeres løsning er opsat rigtigt. Vi vil løbende opdatere løsningen, således at både I og vi kan leve op til GDPR inden den nye lovgivning træder i kraft. Samtidig gør vi alt vi kan for at sikre os, at det bliver så nemt som muligt for jer, at få foretaget de nødvendige ændringer. Vi arbejde således på at bygge GDPR direkte ind i brugeroplevelsen af vores løsning.

Har du yderligere spørgsmål til vores arbejde med den nye persondatalov er du meget velkommen til at kontakte os. Alternativt kan du tilmelde dig vores månedlige nyhedsbrev. Her vil vi løbende informere om udviklingen indenfor GDPR og guide dig til, hvordan du skal forholde dig til dette som CRM-bruger.

FAQ

Hvornår træder GDPR i kraft?
GDPR blev godkendt og vedtaget af EU-parlamentet i april 2016. Forordningen træder i kraft efter en to-årig overgangsperiode, og i modsætning til et direktiv kræver GDPR ingen godkendelse af de nationale lovgivende forsamlinger. Dette sikrer at GDPR træder i kraft i maj 2018 på tværs af EU.

Hvem bliver påvirket af GDPR?
GDPR gælder ikke kun for organisationer der opererer inden for EU. Organisationer uden for EU er også forpligtet til at overholde GDPR, såfremt de tilbyder varer eller tjeneste-ydelser til EU-borgere. Det gælder for alle virksomheder, der behandler og opbevarer persondata for borgere der er bosat i EU, uanset virksomhedens beliggenhed.

Hvad er sanktionerne for manglende overholdelse?
Virksomheder kan tildeles bøder på op til 4% af deres årlige globale omsætning, eller € 20 millioner, for at overtræde GDPR - afhængigt af hvilket beløb der er højest. Dette er den maksimale bøde, der kan pålægges for de mest alvorlige overtrædelser, for eksempel hvis en virksomhed ikke har tilstrækkeligt kundesamtykke til at behandle data. Der er her tale om en "lag-tilgang" til bøder: f.eks. kan et selskab idømmes en bøde på 2% af den årlige omsætning for ikke at have deres optegnelser i orden (artikel 28), uden at under-rette tilsynsmyndigheden og registrerede om overtrædelser. Det er vigtigt at bemærke, at disse regler gælder for både "data-controllerer" og "data-processorer". Dette indebærer at cloud-virksomheder ikke er fritaget for GDPR-håndhævelse.

Hvad definerer persondata?
Enhver oplysning relateret til en fysisk person eller "datasubjekt", som kan bruges til direkte eller indirekte at identificere personen. Det kan være alt fra et navn, et foto, en e-mailadresse, bankoplysninger, indlæg på sociale medier, medicinsk information eller en computers IP-adresse.

Hvad er forskellen mellem en "data-processor" og en "data-controller"?
En controller er den agent, der bestemmer formålene, betingelserne og midlerne til behandling af personoplysninger, mens processoren er den agent, der behandler personlige data på vegne af controlleren.

Har dataprocessorer brug for "eksplicit" eller "utvetydig" registreret samtykke?
Kravene til samtykke er blevet højnet således, at virksomheder ikke længere vil kunne udnytte lange og "ulæselige" vilkårsdokumenter der er fulde af retsforbehold. Fremadrettet skal anmodningen om samtykke leveres på en forståelig og let tilgængelig måde. Samtykket skal være klart og kunne skelnes fra andre forhold og tilvejebringes i en forståelig og let tilgængelig form ved hjælp af klart og almindeligt sprog. Derudover skal det være lige så let at tilbagetrække samtykke som det er at give det.

Hvad er forskellen mellem en forordning og et direktiv?
En forordning er en bindende retsakt. En forordning skal anvendes i sin helhed i hele EU, mens et direktiv er en lovgivningsakt, der fastlægger et mål, som alle EU-lande skal opnå. Det er imidlertid op til de enkelte lande at bestemme hvorledes det skal ske. Det er vigtigt at bemærke, at GDPR er en forordning, i modsætning til den tidligere lovgivning, som er et direktiv.

Skal min virksomhed udpege en Data Protection Officer (DPO)?
DPO'er skal udpeges for: 1) offentlige myndigheder, 2) organisationer, der beskæftiger sig med systematisk overvågning og 3) organisationer, der beskæftiger sig med behandling af følsomme personoplysninger på en større skala (artikel 37). Hvis din virksomhed ikke falder ind under en af disse kategorier, behøver du ikke at udpege en DPO.