Vejledning om GDPR til dig, der driver en mindre virksomhed

7 trin, der flytter dig tættere på GDPR-compliance

DATATILSYNET

Overblik

Grundlæggende om GDPR

Hvad er GDPR?

Når du som virksomhed i Danmark bruger personoplysninger, skal du overholde GDPR.

GDPR står for ”General Data Protection Regulation” og er på dansk også kendt som databeskyttelsesforordningen. GDPR er EU-reglerne for databeskyttelse og gælder bl.a., når private virksomheder behandler oplysninger om personer (personoplysninger).

Alle danskere har som EU-borgere en række rettigheder i GDPR. Det betyder konkret, at når du som en privat virksomhed ”behandler personoplysninger” om andre – dvs. indsamler, registrerer, videregiver eller sletter personoplysninger om f.eks. dine kunder eller ansatte – skal du overholde GDPR.

Hvorfor GDPR?

Reglerne har skabt et øget fokus på den enkelte borgers ret til at have kontrol over sine egne data – det gælder også dine oplysninger, når du som privatperson bliver registreret af en virksomhed eller myndighed. Med GDPR har vi som EU-borgere de samme databeskyttelsesrettigheder inden for EU – uanset hvilket EU-land, vores data bruges i.

For virksomheder skal GDPR skabe nogle klarere regler for brug af personoplysninger som forretningsdrivende. Som en fælles EU-lov gør GDPR de forskellige EU-landes håndtering af databeskyttelsesreglerne ensartet og fjerner unødvendig administration på tværs af landene.

GDPR er fleksible regler

Du kender bedst din egen virksomhed, og det er derfor også dig, der er den bedste til at vurdere, hvilke personoplysninger, du har behov for at behandle for at kunne drive din forretning. Derfor er det også dig, der skal vurdere, til hvilke formål du behandler personoplysninger, og hvor længe det er nødvendigt at gemme oplysningerne.

Formålet med at udforme databeskyttelsesreglerne som fleksible regler, hvor du selv skal vurdere og sikre, at du lever op til reglerne er ikke at skabe usikkerhed eller bekymring for dig som virksomhed, men derimod at sikre, at reglerne har den nødvendige fleksibilitet til at favne de mange forskellige brancher og virksomheder.

Heldigvis har du altid mulighed for at få vejledning af Datatilsynet, og typisk vil din brancheorganisation også kunne være behjælpelig med at besvare konkrete spørgsmål til netop din virksomheds håndtering af GDPR.

1

Skab overblik

Reglerne om databeskyttelse gælder også for dig som en lille virksomhed, hvis du bruger eller opbevarer oplysninger om andre personer.

For at du kan overholde reglerne, er det vigtigt, at du får skabt et overblik over:

- hvor du har personoplysninger
- hvem du håndterer personoplysninger om
- hvilke personoplysninger du håndterer

Find ud af, hvor du har personoplysninger

Du vil sandsynligvis have personoplysninger gemt på din telefon, tablet, computer eller it-systemer, f.eks. i e-mails og SMS'er. Det kan også være, at du har printede dokumenter med personoplysninger på. Det kunne være navne og kontaktoplysninger på kunder eller ansatte, men også information om kommende bookinger, aftaler, ordrebøger eller andre bestillinger. Husk, at hvis du kan identificere en person ud fra noget, du har gemt, så er der tale om personoplysninger.

Find ud af, hvem du håndterer oplysninger om

Når du har fundet ud af, hvor du opbevarer personoplysninger, bør du notere dig, hvem oplysningerne handler om. Du kan med fordel inddele disse personer i samlede grupper, herunder:

- Kunder
- Ansatte
- Leverandører

Find ud af, hvilke oplysninger du håndterer

Når du har fundet ud af, hvor der kan være personoplysninger, og hvem du håndterer oplysninger om, bør du starte med at lave en oversigt over, hvilke typer af oplysninger du har om de forskellige grupper, f.eks. "kunders telefonnumre".

Håndterer andre personoplysninger på dine vegne?

Det ovenstående overblik, som du skal skabe, gælder også, hvis du har fået andre til at håndtere oplysningerne på vegne af dig.

Fortegnelse

En fortegnelse er et andet ord for en ordnet oversigt. Begrebet bruges i GDPR til at beskrive den oversigt, man skal lave, når man håndterer personoplysninger om andre.

På Datatilsynets hjemmeside, kan du hente en skabelon til en fortegnelse over oplysninger om kunder.

2

Spørg dig selv "hvorfor"

Når du har oplysninger om andre, f.eks. kunder eller ansatte, skal du først og fremmest finde ud af, om du har en god grund til at have personoplysningerne.

Her kan du med fordel spørge dig selv "Hvorfor har jeg oplysningerne?". Hvis du kan besvare dette spørgsmål på en fornuftig måde, f.eks. at du har oplysninger om en kunde for at kunne levere vedkommendes bestilling, eller fordi loven siger, at du skal opbevare oplysningerne, vil du som udgangspunkt have en god grund til at have oplysningerne.

Lovlige grundlag

Selvom du selv synes, du har en god grund til at have oplysninger om andre, er det også nødvendigt, at du opfylder en eller flere betingelser i loven for at have oplysningerne. Du må håndtere personoplysninger, hvis en af følgende betingelser er opfyldt:

- Du har samtykke fra den, som du håndterer oplysninger om
- Du har behov for personoplysninger for at opfylde en aftale, som du har indgået med den, som du håndterer oplysninger om
- Du udfører en opgave for en offentlig myndighed
- Du er forpligtet af en anden lovgivning til at håndtere oplysningerne
- Du forfølger din gode grund, samtidig med at din brug af oplysningerne ikke medfører særlige gener eller konsekvenser for den, som du håndterer oplysninger om
- Du skal vælge det grundlag, som passer bedst til den enkelte situation. Du skal således ikke indhente samtykke, hvis du har et andet lovligt grundlag.

Du skal f.eks. ikke have samtykke fra kunder eller leverandører, hvis du har oplysninger om dem, fordi du skal levere eller modtage en bestilling. Det skyldes, at du skal bruge oplysningerne for at kunne opfylde din aftale med kunden eller leverandøren.

Ønsker du derimod at gøre brug af de samme oplysninger til at sende markedsføring (nyhedsbrev) skal du have samtykke til det. Dette samtykke kan du udforme på følgende måde:
"Jeg giver samtykke til, at virksomhed X må bruge min e-mailadresse til at sende mig markedsføring inden for virksomhedens produktsortiment. Jeg kan til enhver tid tilbagekalde mit samtykke"

Du skal heller ikke have samtykke fra dine ansatte, medmindre du ønsker at håndtere oplysninger om dem i forbindelse med noget, der ikke som sådan har noget med ansættelsesforholdet at gøre.

Husk

Du skal i øvrigt altid være opmærksom på, at du ikke må håndtere flere oplysninger end dem, du skal bruge.

3

Husk at slette

Du skal slette personoplysninger, når du ikke længere har behov at have dem, dvs. når det ikke længere er nødvendigt at håndtere oplysningerne for at opfylde din gode grund (se trin 2: Spørg dig selv ”hvorfor”).

Hvis det følger af andre regler, at du skal gemme personoplysninger, hvilket f.eks. er tilfældet i bogføringsloven, skal du ikke slette oplysningerne, så længe du er forpligtet til at opbevare oplysningerne. Bogføringsloven siger nemlig, at du skal opbevare regnskabsmateriale i 5 år fra udgangen af det regnskabsår, materialet vedrører.

Hvis du ikke på baggrund af anden lovgivning skal gemme personoplysninger, så er det reglerne i GDPR, der afgør, hvor længe du må gemme oplysningerne. I de tilfælde er det ikke altid let at fastlægge, hvor længe du må opbevare personoplysninger, idet databeskyttelsesreglerne ikke indeholder faste grænser for opbevaring.

Du ved bedst, hvornår det er nødvendigt at slette

At databeskyttelsesreglerne ikke specifikt angiver, hvor længe du må håndtere personoplysninger, skyldes, at det er dig, der kender din virksomhed bedst, og derfor bedst kan vurdere, hvor længe du har brug for oplysningerne.

Du har således et vist råderum til at vurdere, hvor længe det er nødvendigt for dig at opbevare personoplysninger for at opfylde dit/dine formål. I praksis kan du spørge dig selv ”Hvorfor har jeg stadig brug for oplysningerne?”. Så længe du kan besvare dette spørgsmål på en fornuftig måde, kan du opbevare oplysningerne.

Så længe du har rutiner, der sikrer, at du løbende sletter personoplysninger, har du ikke pligt til løbende at gennemgå samtlige dokumenter mv. for at overveje, om enkeltstående oplysninger er nødvendige at gemme.

At det er dig, der bedst kan vurdere, hvor længe du har brug for oplysningerne, indebærer derfor også, at du i langt de fleste tilfælde ikke skal være nervøs for, at Datatilsynet vil være uenig i en slettefrist, du har fastsat.

4

Oplys om, at du behandler personoplysninger

Du har pligt til at oplyse dine kunder eller dine ansatte om, at du har oplysninger om dem. Udover at oplyse dem om, at du har oplysninger om dem, skal du give dem en række andre informationer, f.eks. om hvad du skal bruge oplysningerne til, og hvor længe du gemmer dem. Hvis du får oplysningerne fra personen selv, skal du give informationen på det tidspunkt, du modtager dem. Hvis du får oplysningerne fra andre end personen selv, skal du give oplysningerne hurtigst muligt (senest inden 1 måned).

Du skal give dem information på en måde, der er let for folk at forstå. Du kan med fordel give informationen i en privatlivspolitik, som ligger på din hjemmeside, og som du kan linke til, når kunden afgiver oplysninger om sig selv, f.eks. hver gang du får en ny kunde.

Du skal oplyse om:

Identitet og kontaktoplysninger
Dette er virksomhedens navn og kontaktoplysningerne.

Hvilke personoplysninger
Den type af oplysninger, som du har fundet i forbindelse med trin 1: Skab overblik.

Hvorfor
Her skriver du din gode grund og dit lovlige grundlag fra trin 2: Spørg dig selv hvorfor.

4

Hvem oplysningerne evt. deles med
Hvis du giver folks oplysninger til nogen uden for din virksomhed, skal du oplyse om, at du gør dette, og om hvem der modtager oplysningerne. Det kan f.eks. være et leveringsfirma, som skal levere en pakke, som du sender til din kunde, eller en, som håndterer oplysningerne på dine vegne.

Hvor længe gemmes oplysninger
Her skrives dine overvejelser fra trin 3: Husk at slette.

Rettigheder
Her kan du med fordel skrive følgende:

”Du har efter databeskyttelsesforordningen en række rettigheder i forhold til vores behandling af oplysninger om dig.

Ret til at se oplysninger (indsigtsret)
Ret til berigtigelse (rettelse)
Ret til sletning
Ret til begrænsning af behandling
Ret til indsigelse
Ret til at transmittere oplysninger (dataportabilitet)

Hvis du vil gøre brug af dine rettigheder, skal du kontakte os.

Du har i øvrigt ret til at indgive en klage til Datatilsynet, hvis du er utilfreds med den måde, vi behandler dine personoplysninger på. Du finder Datatilsynets kontaktoplysninger på www.datatilsynet.dk”

5

Sørg for at have gode procedurer

De personer, hvis oplysninger du bruger eller gemmer, har en række rettigheder. De har bl.a. ret til at anmode om at få en kopi af deres oplysninger (ret til indsigt), at få forkerte oplysninger rettet og at få deres oplysninger slettet.

Hvis en person anmoder om at gøre brug af en af disse rettigheder, skal du svare inden for en måned, også selvom du afviser deres anmodning. For at sikre, at du kan svare inden for denne frist, er det en god idé at have gode procedurer for, hvordan du håndterer disse anmodninger.

Tjekliste
Her kan du finde en tjekliste, som du kan bruge, når du modtager en anmodning fra en person, som ønsker at gøre brug af sine rettigheder.

1. Vælg en ansvarlig
Vælg en af dine ansatte (eller dig selv) til at være tovholder på alle opgaver, som handler om databeskyttelse.

2. Vær sikker på, hvem personen er
Du skal tjekke, hvem der anmoder om at gøre brug af sine rettigheder. Du må gerne bede om mere information, men bed kun om at se ID, hvis det er absolut nødvendigt.

3. Tjek, at de har ret til det, som de beder om
Læs mere om de registreredes rettigheder på Datatilsynets hjemmeside.

4. Find ud af, hvad personen vil have
Spørg gerne ind til, hvad det præcist er, personen gerne vil have oplyst, slettet, rettet mv.

5

5. Sæt deadlines
Du skal svare inden for en kalendermåned, uanset om den er 28 eller 31 dage lang. Sæt derfor gerne en deadline på 28 dage, så du er sikker på at nå det. Hvis du modtager en kompliceret anmodning, eller den samme person anmoder hele tiden, kan du forlænge fristen med to måneder. Du skal dog gøre personen opmærksom på, at det kommer til at tage længere tid.

6. Søg efter information om personen de relevante steder
Du skal overveje, hvor du kan have oplysninger liggende, og være grundig når du leder. Husk også at tænke på eksterne harddiske, USB-stik, opslag på sociale medier, optagelser fra overvågningskamera mv. Det kan også være hos andre, som håndterer oplysningerne på vegne af dig.

7. Tjek om materialet, du udleverer, indeholder oplysninger om andre
Du må ikke udlevere oplysninger om andre personer end personen selv. Hvis det materiale, som du vil udlevere, indeholder oplysninger om andre, skal du fjerne oplysningerne om disse andre personer. Det kan du f.eks. gøre ved at overstrege oplysningerne eller sløre et billede eller videomateriale. Hvis du bruger en computer til dette, skal du fjerne oplysningerne på en måde, så modtageren ikke kan genskabe informationen

8. Forbered de supplerende oplysninger og dit svar
Udover selve oplysningerne skal personen også have at vide, hvorfor du bruger deres oplysninger, hvordan du har fået dem, hvor længe du planlægger at gemme dem, hvem du deler dem med, og hvordan de kan få deres oplysninger slettet eller forkerte oplysninger rettet. Link eventuelt til din privatlivspolitik, som du har udarbejdet i forbindelse med trin 4: Oplyst om at du behandler personoplysninger.

6

Husk sikkerheden

Hvorfor IT-sikkerhed?

Cyberangreb rammer både små og store virksomheder. Derfor spiller IT-sikkerhed en vigtig rolle, når virksomhedens systemer og personoplysninger skal beskyttes.

Hvis du ikke har tænkt over IT-sikkerhed før, så start med de elektroniske enheder, hvor du håndterer personoplysninger, der kræver særlig beskyttelse fx helbredsoplysninger, CPR-numre og straffeattester. Elektroniske enheder er fx PC, tablets, mobil, USB-stik og ekstern harddisk.

Praktiske råd til bedre behandlingssikkerhed

SikkerDigital har samlet 7 gode råd om it-sikkerhed, som kan hjælpe små og mellemstore virksomheder med at styrke deres basale digitale sikkerhed:

1. Få overblik over vigtige data og systemer
2. Opdater programmer, herunder applikationer, løbende
3. Køb antivirus og firewall
4. Tag backup af data
5. Lær at spotte mistænkelige e-mails
6. Lav stærke adgangskoder
7. Stil sikkerhedskrav til IT-leverandører
8. Læs mere om de 7 gode råd her

Har du outsourcet?

Hvis du har outsourcet IT-driften og IT-sikkerheden, er det dit ansvar at stille de rigtige krav til din leverandør. SikkerDigital har udarbejdet en værktøjskasse med vejledning og et spørgeskema, som kan hjælpe dig med at stille de rigtige spørgsmål og krav til din IT-leverandør.

6

Tænk sikkerhed ind i dine arbejdsprocesser

Nedenunder finder du en række lavpraktiske råd, der giver god sikkerhed i de daglige arbejdsprocesser – også når man arbejder hjemmefra.

Brug sikker WiFi
Så risikerer du ikke, at andre uberettiget får adgang til oplysninger om dine kunder, ansatte eller virksomhedens forhold.

Lås skærmen, når du forlader din plads – uanset hvor længe du er væk
Så risikerer du ikke uberettiget adgang til oplysninger om dine kunder eller ansatte via dine elektroniske enheder med personoplysninger.

Husk sikkerheden, når du arbejder på distancen
Når du arbejder på distancen skal du huske at beskytte dine elektroniske enheder, som hvis du var på arbejdspladsen. Du skal også være opmærksom på dine omgivelser, fx hvis du arbejder i toget eller i bussen, hvor andre personer potentielt kan følge med på din skærm eller lytte til din samtale.

Afskaf elektroniske enheder på en forsvarlig måde
Inden du afskaffer dine elektroniske enheder fx mobil, tv, pc og tablet, skal du sikre dig, at enhederne ikke indeholder personoplysninger. Det kan du gøre ved at nulstille enheden. Alternativt kan du sikre dig, at oplysningerne på ingen måde kan tilgås af andre, f.eks. ved kryptering.

Efterlad ikke fysiske dokumenter og elektroniske enheder uden opsyn
Brud på persondatasikkerheden kan opstå, når fysiske dokumenter eller elektroniske udstyr med personoplysninger efterlades uden opsyn på steder, hvor uvedkommende har adgang. Det kan typisk være på hotellet, i bilen eller i toget. Sørg for altid for at opbevare dine dokumenter og enheder et sikkert sted, når de ikke er i brug.

6

Hav styr på, hvem der har adgang til hvad
Du skal altid have styr på, hvem der har adgang til hvilke systemer og bygninger, samt hvorfor de har adgang. Du kan ikke lade enhver have adgang til dine systemer og bygninger, da sikkerheden forringes og risikoen for brud på persondatasikkerheden øges. Du skal derfor begrænse adgangen, så det kun er personer med et arbejdsbetinget behov, der har adgang. Når en medarbejder stopper, skal du sørge for, at den pågældende ikke længere har adgang til systemer og bygninger.

Gem ikke personoplysninger i længere tid end nødvendigt
Du kan begrænse dit ansvar og din risiko ved ikke at opbevare flere personoplysninger end nødvendigt og ved ikke at opbevare dem længere end nødvendigt. Jo færre oplysninger du har, jo mindre risiko er der også for at miste data, f.eks. i forbindelse med et cyberangreb.

Send og modtag sikkert
Du skal være særligt opmærksom på, hvordan du sender/modtager personoplysninger, der kræver særlig beskyttelse, som f.eks. helbredsoplysninger, CPR-numre og straffeattester.

Når du vælger at sende/modtage personoplysninger, er det vigtigste, at du vælger en sikker måde at kommunikere på, så personoplysninger ikke ender i de forkerte hænder.

Du kan som regel godt kommunikere sikkert via e-mail.

Digital Post som f.eks. e-boks er også en sikker måde at kommunikere på. Forsendelse af fysisk brev eller pakke med posten betragtes ligeledes som en sikker kommunikation.

Husk, at hvis du sender elektroniske enheder, f.eks. USB-stik, PC eller ekstern harddisk, som indeholder fortrolige eller følsomme personoplysninger, skal enhederne være krypteret.

7 Du er også ansvarlig, når du deler

Du vil næsten altid have behov for at dele data med andre, enten fordi du gemmer personoplysninger i et IT-system, eller fordi du er forpligtet til at videregive personoplysninger til andre, f.eks. myndigheder. I GDPR skelner man mellem at være 'dataansvarlig' og 'databehandler', da det har en betydning for dit ansvar, når du behandler personoplysninger.

Din virksomhed er dataansvarlig for de personoplysninger, I behandler om jeres medarbejdere og kunder. Det betyder, at det er dit ansvar at sikre, at personoplysninger om dine medarbejdere og kunder bliver behandlet lovligt.

Når du anvender et IT-system

Leverandører af de IT-systemer, du bruger, vil typisk være databehandlere. Det kan være leverandører af software til udsendelse af nyhedsbreve (f.eks. Mailchimp), lønadministrationsprogrammer (f.eks. Bluegarden eller Visma), kundehåndteringssystemer/CRM-system (f.eks. Salesforce eller WebCRM) og mailprogrammer (f.eks. Outlook i MS365, hotmail eller gmail).

Når du anvender en databehandler, skal du have en databehandleraftale. Det er vigtigt, at du har et overblik over de databehandleraftaler, du har med dine leverandører. Du kan med fordel gemme aftalerne i en mappe på din computer.

Når du videregiver personoplysninger til andre dataansvarlige

Nogle gange har du behov for at give personoplysninger om dine kunder eller medarbejdere videre til andre. Det kunne være SKAT, der skal bruge dine medarbejderes lønoplysninger, eller en samarbejdspartner der skal invitere dine kunder til et fælles arrangement.

Du skal tænke over, hvem du giver oplysningerne til, og du skal huske at informere dine medarbejdere eller kunder om, at deres oplysninger bliver delt. Det kan du passende gøre i din persondatapolitik, trin 4: Oplys om, at du behandler personoplysninger.

Har du spørgsmål til GDPR i din virksomhed?
Skriv eller ring til os.

33 19 32 00
dt@datatilsynet.dk
www.datatilsynet.dk/gdpruniver

GDPR-universet for mindre virksomheder er lavet i samarbejde med

Dansk Industri

DANSK ERHVERV

SMVdanmark

DATATILSYNET