Vejledning til

GDPR – General Data Protection Regulation

GDPR - General Data Protection Regulation

I maj 2018 træder EU's nye forordning om beskyttelse af personoplysninger i kraft. Det hedder General Data Protection Regulation og forkortes som regel GDPR. Forordningen benævnes også Persondataforordningen, og det er en afløser for persondataloven.

JMA A/S er ikke ekspert på området, men vi har sat os ind i reglerne herom for selv at kunne leve op til disse. Denne information må derfor ikke tages som den fuldstændige sandhed omkring det omfattende regulativ, men som en orientering, som I kan bruge til jeres forberedelser. Desuden beskriver den i hvilket omfang JMA som hosting-center er involveret i jeres ansvar for behandling af personoplysninger.

Alle virksomheder har en opgave i at leve op til GDPR. Kravene er så omfattende, at der næppe er nogen almindelige virksomheder i Danmark, der er klar, uden at det kræver nye tiltag.

GDPR stiller nye krav til jeres virksomheds indsamling og håndtering af data om EU-borgere. GDPR gælder, uanset hvor jeres virksomhed hører hjemme, hvis I håndterer data om EU-borgere.

Hvad betyder GDPR så for jeres virksomhed? Hvad skal I gøre?

GDPR stiller højere krav til jeres virksomhed om beskyttelse af kundernes data, end I har været vant til tidligere. Det stiller grundlæggende 3 krav til jeres virksomhed:

- I skal have skarp kontrol med, hvor personoplysninger gemmes og hvor de anvendes.
- I skal have et sæt processer, der sikrer, at der skabes transparens i data, at der logges ændringer og at der kan rapporteres på håndteringen af data.
- I skal have data-politikker og -processer, der kan give personerne, som I gemmer data om, kontrol over egne data.

JMA A/S | Engelsholmvej 26 | DK-8900 | Randers SV | Tel.: +45 8711 0000 | info@jma.dk

Vejledning til

GDPR – General Data Protection Regulation

Dokumentet er inddelt i følgende afsnit:

Indhold

JMA A/S | Engelsholmvej 26 | DK-8900 | Randers SV | Tel.: +45 8711 0000 | info@jma.dk

Vigtig skelnen: Forskel på almindelige og følsomme personoplysninger

Personoplysninger er omdrejningspunktet i GDPR.

Men hvad er personoplysninger helt præcist?

Personoplysninger forstås som enhver information om en identificeret eller identificerbar fysisk person. Det vil sige oplysninger om alt fra navn og bopæl til etnisk oprindelse og seksuel orientering. Der skelnes ikke mellem personens private, offentlige eller arbejdsmæssige rolle, så det er ikke nogen undskyldning, at: "Jamen, de er jo bare kunde hos os".

Personoplysninger skal beskyttes, så de ikke bliver offentligt tilgængelige. Det er I som virksomhed forpligtet til at sørge for. For at kunne leve op til jeres ansvar skal I være bevidst om karakteren af de personoplysninger, I håndterer. GDPR skelner mellem almindelige og følsomme personoplysninger.

Eksempler på almindelige personoplysninger:

- Navn
- Adresse
- Telefonnummer
- Familie
- Fødselsdato
- Uddannelse, Eksamener og beskæftigelse
- Bolig
- Bil
- Løn, Bank-informationer og skat
- Email-adresse
- Data fra sociale medier
- Kulturel identitet
- Lokation
- IP-adresse og Cookies

Eksempler på følsomme personoplysninger:

- CPR-nummer
- Race
- Etnisk oprindelse
- Politisk, religiøs eller filosofisk overbevisning
- Fagforeningsmæssigt tilhørsforhold
- Genetiske og biometriske data
- Helbredsoplysninger
- Væsentlige sociale problemer
- Seksuelle forhold og seksuel orientering

Som I kan se, så fortolkes " personoplysninger" endog meget bredt.

For at blive klar til GDPR er det vigtigt, at I afsætter den nødvendige tid til at kortlægge, hvilke personoplysninger, I behandler i dag.

JMA A/S | Engelsholmvej 26 | DK-8900 | Randers SV | Tel.: +45 8711 0000 | info@jma.dk

Personoplysninger kan være registreret mange andre steder end i DSM-systemet. Af eksempler på kilder med personoplysninger kan vi nævne:

- Ansøgninger
- E-mails
- CRM system
- Web-shop
- Ledelsesrapportering
- Excel filer
- Word dokumenter
- etc.

Et eksempel:

I trækker lige en liste over debitorer over i Excel og gemmer listen på fællesdrevet.

Nej, det gør I ikke bare, når GDPR træder i kraft. Det kræver en procedure for, hvordan data overføres, gemmes sikkert, slettes på et bestemt tidspunkt, og hvordan det sikres, at hver enkelt person i denne Excel-fil kan få indsigt i sine data.
I skal altså have styr på, hvad I har gemt, hvor I har gemt det, og hvor længe I af personen har fået samtykke til, at I må gemme oplysningerne. I skal således også have en procedure for sletning af disse oplysninger.

Det kan hurtigt blive en tidskrævende opgave, da det typisk indebærer, at medarbejdere fra alle dele af organisationen inddrages, så I er sikre på, at behandlingen af personoplysninger i praksis lever op til jeres ønskede standard. Det gælder ikke mindst medarbejdere, der til dagligt er udførende på opgaver som involverer personoplysninger.

Kortlægningen skal give svar på:

- Hvilke typer personoplysninger indsamler I?
- Hvorfra indsamler I jeres personoplysninger?
- Hvordan indsamler I jeres personoplysninger?
- Videregiver I jeres personoplysninger og i givet fald til hvem?
- Hvor og hvordan gemmer (og sikrer) I jeres indsamlede personoplysninger?
- Hvordan bruger I jeres personoplysninger? Og hvad har I af fremtidige planer for brug af dem?
- Har I styr på, hvordan og evt. hvornår I sletter personoplysningerne?

Få afklaret din rolle: Er du dataansvarlig eller databehandler?

Stort set alle virksomheder, organisationer, foreninger og offentlige myndigheder håndterer personoplysninger af den ene eller anden art. Det kan være informationer om ansatte, kunder, medlemmer eller borgere. Når I håndterer personoplysninger, er I ansvarlige herfor. Men jeres ansvarsgrad afhænger af, om I optræder som dataansvarlig eller databehandler.

Hvad er forskellen?

Den dataansvarlige afgør til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger.

Databehandleren derimod behandler personlige oplysninger på vegne af den dataansvarlige.

Hvor ligger ansvaret?

Den dataansvarlige er altid den ansvarshavende part i sidste ende. Man kan sammenligne det med forholdet mellem arbejdsgiveren og dennes ansatte. En arbejdsgiver står altid til regnskab for sine medarbejderes gøren og laden – også selvom medarbejderen på egen hånd handler i strid med loven (bevidst eller ubevidst).
Sådan forholder det sig også i samarbejdet mellem den dataansvarlige og databehandleren, når det kommer til at overholde reglerne for behandling af personoplysninger. I praksis kan en databehandler eksempelvis være en virksomhed, der varetager it-systemet for en anden virksomhed, eller det kan være et bureau, der står for e-mail markedsføringen på vegne af en virksomhed.

Forholdet mellem dataansvarlig og databehandler kan dog hurtigt blive yderligere kompliceret, da databehandleren selv kan benytte sig af databehandlere – i dette tilfælde underdatabehandlere – i forbindelse med opgaverne, de udfører for den dataansvarlige.

Eksempler på databehandlere, I benytter:

- JMA behandler jeres data i DSM systemet i vort hosting-center
- I anvender måske et bureau til at stå for e-mail markedsføring
- I har måske en aftale med en ekstern backup udbyder
- I har evt. jeres hjemmeside hostet eksternt

Vigtigt: Få styr på dine databehandleraftaler

Det er vigtigt, at I går jeres aftaler igennem og eventuelt får opdateret dem, så de lever op til reglerne i GDPR. Som dataansvarlig er I i sidste ende hovedansvarlig for jeres databehandlers omgang med jeres indsamlede personoplysninger. Det gælder også, hvis fejlen er placeret hos en underdatabehandler.

Som dataansvarlig risikerer I sagsanlæg.

Som databehandler er man dog ikke fri for ansvar. Er en databehandler eksempelvis til stor skade for en dataansvarlig virksomhed, kan denne virksomhed fremsætte krav mod databehandleren. Det gælder også, hvis fejlen er begået af en underdatabehandler. Derfor skal man som databehandler sikre, at eventuelle underdatabehandlere forpligter sig til at leve op til de samme krav, som gælder i forholdet til den dataansvarlige – som kan være jer.

JMA er i færd med at udarbejde en skabelon til en sådan databehandler-aftale. Den stiller vi gerne til rådighed, når vi har fået den godkendt.

JMA A/S | Engelsholmvej 26 | DK-8900 | Randers SV | Tel.: +45 8711 0000 | info@jma.dk

Kontrol og advisering

Virksomheder skal:

- Beskytte personoplysninger med passende sikkerhedsforanstaltninger
- Advisere myndighederne ved brud på sikkerheden
- Indhente passende samtykke til at behandle data
- Have sporbarhed i databehandlingen

Her hjælper Microsoft Dynamics NAV dig et godt stykke på vej. Microsoft gør meget ud af sikkerheden i de systemer, de udvikler, og Microsoft forpligter sig kontraktligt til at leve op til lovgivningen.

Men det stiller også krav til jeres processer. I skal kunne dokumentere, hvordan og hvornår I har modtaget eksplicit samtykke til at behandle data, og I skal have styr på, om (eller hvordan) data flyder ud af DSM-systemet. I skal ligeledes tage stilling til rettigheder i DSM-systemet: hvem kan se hvilke data, og hvem kan ændre og slette personoplysninger.

Det er ikke tilstrækkeligt at have processerne på plads. I er også forpligtet til at overvåge, at processerne følges. Ellers kan I ikke advisere myndighederne om brud på sikkerheden.

Særligt omkring advisering af myndighederne ved brud på sikkerheden

GDPR stiller krav om, at der ved brud på sikkerheden skal ske henvendelse til den nationale persondatamyndighed (Datatilsynet) OG de personer, hvis data er involveret i bruddet, inden for 72 timer efter sikkerhedsbruddet.

Med den eksplosive stigning i it-kriminalitet er der i sagens natur meget fokus på dette. Og det kan betyde tab af anseelse, hvis man som virksomhed har været medvirkende til en lækage af personoplysninger.

Sådan sker brud på sikkerheden oftest

- Organisatoriske fejl: Manglende stillingtagen til opfyldelse af GDPR's krav.
- Menneskelige fejl: Offentliggørelse af personoplysninger som følge af manglende viden hos de ansatte.
- Fejl i IT-løsningen: Manglende kryptering af formularer i forbindelse med indsendelse af personoplysninger.
- IT-kriminalitet: Datatyveri, hackerangreb og lignende.

Skrappere sanktioner

Et af de mest markante tiltag i GDPR er den massive stigning i størrelsen på bødestraffen ved overtrædelse af forordningens bestemmelser. I dag ligger sanktionerne i størrelsesordenen 5-10.000 kr. Fra den 28. maj 2018, hvor GDPR træder i kraft, kan bøderne udgøre op til 4% af virksomhedens omsætning, dog maksimalt 20 mio. euro.

JMA A/S | Engelsholmvej 26 | DK-8900 | Randers SV | Tel.: +45 8711 0000 | info@jma.dk

Så store bødestraffe er det nok de færreste virksomheder, der vil blive udsat for. De gives i tilfælde af grov uagtsomhed. Men det giver en indikation af, at det generelle bødeniveau vil stige markant.

Rettigheder til data

Personer har ret til følgende vedrørende de oplysninger, som I gemmer om dem:

- At få dem udleveret
- At få rettet fejl i oplysningerne
- At få dem slettet
- At gøre indsigelse mod behandling af deres personoplysninger
- Ret til at "blive glemt" – altså at få sikkerhed for, at de slettes efter den periode, hvor der er givet samtykke til at de anvendes.

Det er ikke simpelt. Der er tale om en udvidet aktindsigt. I de fleste tilfælde vil der skulle gives svar så hurtigt som muligt, i nogle tilfælde inden for en måned, og med begrundelse om, hvorfor I evt. ikke kan imødekomme henvendelsen. Personen skal også oplyses om, at han eller hun kan klage til Datatilsynet over jeres databehandling.

Hvis det skal foregå 100% selvbetjent, så har I behov for en "kundeportal", hvor alle kan logge ind for at se, ændre, slette og eksportere data, eller klage.

Skærpede samtykkekrav

Grundlæggende gælder der de samme krav til samtykke efter at GDPR træder i kraft, som der gør nu. Det vil sige, at et samtykke fra den registrerede skal være udtrykkeligt og ikke stiltiende eller underforstået. Som virksomhed eller offentlig myndighed, der indsamler personoplysninger, skal I derfor gøre det klart:

- Hvilken type data der indsamles
- Hvem der foretager indsamlingen
- Til hvilket formål informationerne indsamles

En ny ting ved GDPR er dog, at de registrerede skal informeres om, at de har ret til at trække deres samtykke tilbage, og at det samtidig skal være let for de registrerede personer at foretage tilbagetrækningen af samtykket.

Andre skærpede krav til samtykke er, at:

- En dataansvarlig skal til enhver tid kunne dokumentere at have modtaget et bestemt samtykke til behandling af personoplysninger.
- Børn under 16 år kan ikke give et gyldigt samtykke, her skal der indhentes samtykke fra en forælder.

- Hvis samtykket indhentes ved hjælp af en skriftlig erklæring, der indeholder anden information – det kunne eksempelvis være en ansættelseskontrakt - skal samtykkeerklæringen være tydeligt adskilt fra resten.

Lever jeres nuværende samtykkeerklæringer op til kravene?

I forbindelse med overgangen GDPR er det vigtigt at have styr på, om de samtykkeerklæringer, I benytter jer af i dag, lever op til de nye krav. Hvis det ikke er tilfældet, kan I nemlig blive nødt til at indhente nye samtykkeerklæringer for at kunne tilpasse jer til de nye krav.

Ny regel: Retten til at blive glemt

Som noget nyt har registrerede ret til at "blive glemt". Det vil sige, at den dataansvarlige er forpligtet til at slette data, hvis:

- Formålet med registreringen er opfyldt
- Et datasubjekt tilbagekalder sit samtykke
- Behandlingen af data er ulovlig
- Sletningen er nødvendig af lovmæssige årsager
- Den registrerede er under 16 år

Skærpede krav for behandling af personlige oplysninger om medarbejdere og ansøgere

Alle virksomheder opbevarer personoplysninger om deres medarbejdere og potentielle medarbejdere. Det er nødvendigt bl.a. for at kunne udbetale løn eller kontakte interessante ansøgere. GDPR får betydning for, hvordan virksomheder må behandle personlige oplysninger om medarbejdere og ansøgere.

Ansøgere

De fleste virksomheder modtager ansøgninger fra potentielle medarbejdere. Det kan enten være opfordrede eller uopfordrede ansøgninger. I disse ansøgninger vil der ofte forekomme personoplysninger som fx navn, adresse, telefonnummer og mailadresse. De informationer må I gerne bruge, eksempelvis til at kontakte en ansøger med henblik på en samtale.

I må dog ikke opbevare ansøgningen til senere brug, med mindre I informerer vedkommende om det og samtidig tilbyder ansøgeren muligheden for at takke nej. Ligeledes skal ansøgeren informeres om hvor længe ansøgningen gemmes.

Ansatte

Nogle oplysninger er I nødt til at være i besiddelse af for f.eks. at kunne udbetale løn.

JMA A/S | Engelsholmvej 26 | DK-8900 | Randers SV | Tel.: +45 8711 0000 | info@jma.dk

Andre oplysninger, det der er i GPDR kaldes følsomme oplysninger, kræver et udtrykkeligt samtykke fra medarbejderen. Det kan være cpr-nr. eller oplysninger om helbred, race, trosforhold, fagforening og politisk overbevisning.

Enkelte følsomme personoplysninger om medarbejderne er jeres virksomhed nødt til at indsamle. Det drejer sig især om registrering af fravær på grund af sygdom. Medarbejdere er ikke forpligtet til at oplyse om karakteren af deres sygdom, selvom de fleste oplyser det frivilligt, særligt i forbindelse med længerevarende sygdomsforløb. Hvis karakteren af sygdom registreres, er der tale om følsomme oplysninger, der kræver et udtrykkeligt samtykke fra medarbejderen.

Tidligere ansatte

Hvad gør I med de personlige oplysninger, I er i besiddelse af, når en medarbejder ophører med at arbejde i virksomheden? GDPR gør det klart, at I kun må gemme personlige oplysninger om tidligere ansatte, hvis der er et klart og sagligt formål med det. Det kan være nødvendigt at opbevare oplysninger om tidligere medarbejdere for at leve op til retslige krav, f. eks. i forbindelse med aflønning efter fritstilling. Men det springende punkt er, at der er et udtrykkeligt formål med opbevaringen.

Nyt krav om en Data Protection Officer – gælder det for jer?

Med indførelsen af GDPR bliver det for visse offentlige instanser og større private virksomheder et krav at udpege en såkaldt Data Protection Officer (DPO), det man på dansk kan kalde en databeskyttelsesrådgiver. Kravet kan gælde både for dataansvarlige og databehandlere.

Den vigtigste opgave for databeskyttelsesrådgiveren er at sikre de registreredes rettigheder.

Da der kun stilles krav om at have en DPO for offentlige virksomheder og større private virksomheder, der systematisk og regelmæssigt indsamler personoplysninger, vil vi her blot orientere jer om, at det kan være et krav til jer – og I bedes indhente yderligere information herom.

Sådan kommer I i gang

Der er ikke lang tid til den 28. maj 2018.

For at komme i gang med de opgaver, I har i den forbindelse, kan I støtte jer til denne disposition:

- Få kortlagt jeres behandling af personoplysninger – i hvilket omfang I håndterer personoplysninger
- Formulere en overordnet datapolitik og definere arbejdsprocesser
- Sikre at IT-systemer lever op til sikkerhed og understøtter jeres processer omkring håndteringen af personoplysninger
- Sikre at I har databehandler-aftaler med alle, som behandler / opbevarer data for jer
- Etablere adgang for personer til egne data
- Uddanne medarbejdere, der har adgang til personoplysninger

- Udarbejde politikker for transparens, kontrakter og betingelser for samtykke
- Overvåge overholdelse af datapolitikker og advisere myndigheder om brud
- Revidere og opdatere datapolitikker
- Ansætte en Data Protection Officer, hvis påkrævet

Det kan virke som en helt uoverskuelig opgave, men der er hjælp at hente.

Hvor er der hjælp at hente?

Der er et utal af virksomheder, der har gjort det til en vigtig del af deres levebrød at hjælpe virksomheder igennem denne opgave.

Hos JMA har vi selv valgt at tage kontakt til en specialist på området, ligesom vi har indkøbt software til at støtte vores etablering af de nye processer – og ikke mindst den efterfølgende overvågning af, om processerne bliver overholdt.

Her er et par gode links til steder, I kan hente inspiration til at komme i gang med jeres arbejde:

- Erhvervsstyrelsen har lavet et udmærket hjælpeværktøj kaldet PrivacyKompasset. Det kan findes her: https://privacykompasset.erhvervsstyrelsen.dk/

- Datatilsynet har en guide: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/12_spoergsmaal_-_GDPR.pdf

- Microsoft har en udmærket "Get started" guide, som I kan benytte jer af. https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/get-started

JMA A/S | Engelsholmvej 26 | DK-8900 | Randers SV | Tel.: +45 8711 0000 | info@jma.dk