
GDPR
25 MAY 2018

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.

Hos REEFT A/S har sat os ind i reglerne herom for selv at kunne leve op til disse. Vi vil her forsøge at beskrive den og i hvilket omfang REEFT A/S som program og hosting-leverandør er involveret i jeres ansvar for behandling af personoplysninger. Alle virksomheder har en opgave i at leve op til GDPR.

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.

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 vist, 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.

Personoplysninger kan være lagret mange steder, men her vil vi koncentrere os om Hvilke der findes i REEFT samt hvor de er lagret og ikke mindst hvordan de håndteres

For at komme frem til dette kan man spørge de næste spg.

Hvilke typer personoplysninger indsamles?

• Hvorfra indsamles personoplysninger?

• Hvordan indsamles personoplysninger?

• Videregives personoplysninger og i givet fald til hvem?

• Hvor og hvordan gemmes (og sikre) indsamlede personoplysninger?

• Hvordan bruges personoplysninger?

• Er der styr på, hvordan og evt. hvornår personoplysningerne slettes?

Dataansvarlig eller -Behandler

Her er det også vigtigt at skelne, er du Dataansvarlig eller Databehandler.

Men 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.

Vi hos REEFT A/S har defineret vores rolle som værende Databehandler, dvs. vi behandler jeres data på jeres foranledning. Dette stiller krav til, at vi indgår en såkaldt databehandler aftale.

Aftalen definerer hvor ansvaret for behandlingen ligger. 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.

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. REEFT A/S 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.

Konsekvens ved brud

Konsekvenserne hvis der sker brud på sikkerheden kan være uoverskuelige, der uddelses ved grov uagtsom nogle særdeles høje bøder, et omfang som der ikke tidligere har været præcedens for.

Den personlige ret

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 ”Persondataportal”, hvor alle kan logge ind for at se, ændre, slette og eksportere data, eller klage. Dette har REEFT fravalgt.

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 tilbehandling af personoplysninger.

Hvilken type oplysninger findes i REEFT

Udfra GDPR artikel 6, regnes følgende oplysninger fra REEFT systemet som værende omfattet. Vi har defineret det til at vi i REEFT overholder forordningen til kun at gemme den type data der betegnes som almindelige data.

Medarbejderdata

-
    - Navn
    - Telefon
    - Mobiltelefon
    - Email

Kundedata

-
    - Kundenummer
    - Kontaktperson
    - Navn
    - Adresse
    - Telefon
    - Mobiltelefon
    - Email
    - EAN

Kontaktperson

-
    - Navn
    - Adresse
    - Telefon
    - Mobiltelefon
    - Fax
    - Email

Leveringsadresse

-
    - Navn
    - Kontaktperson
    - Adresse
    - Telefon
    - Mobiltelefon
    - Email
    - EAN

Disse data er omdrejningspunktet for Databehandler kontrakten. REEFT vil med udfyldelse af sagte kontrakt, vedgå sig at overholde forordningens artikel 5, der omhandler God Databehandlingsskik. I selvsagt kontrakt beskriver REEFT compliance til Artikel 30, hvor der omtales Fortegnelse over behandlingsaktiviteter.

I nedenstående skelnes der mellem om Databehandler er Hostet hos REEFT eller hos 3. part.

Kunden er hostet hos REEFT

I dette tilfælde er REEFT ansvarligt for sikkerheden både i systemet samt i Hosting

Kunden Hoster selv eller hos Tredjepart

Her er REEFT ansvarlig for sikkerheden i selve REEFT systemet, men kan ikke holdes ansvarlig for brud på sikkerheden, der direkte relateres til at Persondata kan resultere i Identifikation af individuelle personer. Se ovenstående beskrivelse af tredjepart.

Behandling ifbm. Sletning eller anonymisering af data

GDPR forordningen giver mulighed for enten at slette data der kan identificere med en privatperson, eller anonymisere selvsamme data. I REEFT arbejder vi mod anonymisering

Det betyder, at nævnte data ved henvendelse, eller et herefter angivet tidsinterval, anonymiseres ved at overskrive de nævnte data med ordet ”Anonymiseret” i felter med Alfa kode samt i numeriske felter med cifret ”0”, alt efter typen af data.

Som udgangspunkt, skal data automatisk anonymiseres når der ikke længere er et relevant grundlag for at beholde dem, dette er beskrevet i Artikel 5 Grundlæggende regler.

Data vil dog være i fortsat brug, hvis der indenfor fastlagt tid opdateres på data, dette kan i REEFT gøres ved at der sendes nye ordrer ud til selvsamme kunde, hvorpå Personoplysninger er registreret, det er dog iflg. Artikel 5 nødvendigt at selvsagte data skal opdateres og ajourføres. Dette gøre via Dataansvarlig og kan på foranledning af samme, ske i REEFT systemet af REEFT. Der er dog visse oplysninger der ikke er omfattet af GDPR, men umyndiggøres af lokal lovgivning. I sammenhæng med REEFT er dette omhandlende

Skemaer & Kvalitetssikring
Er der oprettet skemaer og/eller kvalitetssikring på en sag, skal denne type data opbevares i ti (10) år

Fordningen giver mulighed for at data skal være relevante, så længe data er relevante er det ikke nødvendigt at anonymisere disse ej heller slette dem. Dog skal de opbevares efter god dataskik, samt ikke mindst der sikrer tilstrækkelig sikkerhed for selvsamme personoplysninger.

Sådan anonymiserer du dine data i REEFT

PT har REEFT ikke en funktion der kan ”anonymisere” data automatisk, derfor er det nødvendigt at i kontakter REEFT på support@reeft.dk for at få dette til at ske. Der kan dog via Systemadministrator (via Management Konsol eller WebPlanner) ske en anonymisering af stamdata for at sikre fremtidig anonymisering, da det pt. ikke er muligt at slette stamdata. Selve overskrivningen kan også ske via Integration fra Databehandlers ERP system, ex. Navision eller C5 – ved at udfylde felter der skal anonymiseres som ovenstående, og herefter overføre data via Integrationen.

REEFT arbejder fremadrettet på en funktion, der muliggør at en total sletning af data kan finde sted.

Risikovurdering

Det er REEFTS opfattelse, at der er en meget lav Risiko for at en brist i sikkerheden, kan lede til afsløring af Personfølsomme data, som beskrevet i artikel 9 & 10.

Hvis du har spg. er du selvfølgelig altid velkommen til at kontakte os på info@reeft.dk. Når REEFT er klar med Databehandler erklæringen, vil den blive sendt til samtlige vores kunder.