version 1
18. december 2018

SikkerhedsBranchen
Information Viden Kvalitet

GDPR – databeskyttelse

Ofte stillede spørgsmål

Gå til

Definitioner, statistik mv.

1. *Hvor gælder GDPR?*

   Forordningen gælder jf. GDPR artikel 2 ”for behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og for ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.”

   Der er dog en række undtagelser, som er oplistet i GDPR artikel 2.

2. *Hvornår træder forordningen i kraft?*

   Forordningen skal være implementeret i hele EU fra 25. maj 2018.

3. *Hvem er omfattet af forordningen?*

   Alle virksomheder, der behandler persondata - uanset om de er dataansvarlige eller alene behandler data på vegne af andre (databehandlere) – er omfattet af forordningen. Virksomheder uden for EU vil også være omfattet, hvis de tilbyder tjenester i EU og dermed behandler persondata om EU borgere.

4. *Hvad skal jeg som dataansvarlig/databehandler gøre?*

   SikkerhedsBranchen har beskrevet processen med at implementere forordningens

SikkerhedsBranchen
Information Viden Kvalitet

krav i et hjælpeværktøj, der er tilgængeligt for vores medlemmer når de er logget ind på SikkerhedsBranchen.dk.

Dataansvarlige, der ikke er medlem af SikkerhedsBranchen, kan hente hjælp i Datatilsynet og Justitsministeriets vejledninger. De findes på www.datatilsynet.dk og www.dbreform.dk.

5. *Hvad betyder forordningen for kontakten mellem virksomhederne og myndighederne?*

   Der kommer en one-stop-shop mekanisme, hvor virksomhederne alene skal have kontakt med én enkelt tilsynsmyndighed. Til gengæld skal tilsynsmyndighederne inden for EU samarbejde i væsentlig højere grad, og dette vil blive afspejlet i afgørelserne, som forventes at blive mere ensartede.

   Som udgangspunkt bliver krav om anmeldelse og underretning vedrørende behandling af persondata til myndighederne fjernet helt. På visse områder har medlemsstaterne dog mulighed for at fastsætte lokale regler og dermed vælge at fastholde kravet herom, som f.eks. kan være tilfældet for anmeldelse af behandling af persondata som led i personaleadministration i Danmark. Der er dog en række bestemmelser, hvor den konkrete udformning er overladt til medlemsstaterne. Dermed finder total harmonisering ikke sted (alligevel).

6. *Hvordan straffes brud på forordningen?*

   Forordningen medfører mulighed for høje bødestraffe til erhvervsdrivende, der bryder reglerne. I de fleste lande vil det blive det nationale datatilsyn, der udsteder bøderne, men Justitsministeriet har afgjort, at det ikke kan lade sig gøre i Danmark. Derfor skal Datatilsynet også fremover lave politianmeldelser med anmodning om at udstede en bøde.

   Der kan udstedes bøder for overtrædelse af forordningen, som for virksomheder svarer til op til 4 % af den globale årlige koncernomsætning og for øvrige op til 20.000.000 euro. Der er tale om fælles ansvar hos dataansvarlig og databehandler for evt. overtrædelser.

7. *Gælder GDPR kun elektroniske registre?*

   Nej, GDPR omfatter personoplysninger i alle former for registre.

   Under "Hvad er databeskyttelse" Datatilsynets hjemmeside kan du læse:

SikkerhedsBranchen
Information Viden Kvalitet

Enhver behandling af andres personoplysninger, der ikke sker i en rent privat sammenhæng, skal ske i overensstemmelse med reglerne på databeskyttelsesområdet.

Desuden står der i GDPR's artikel 2 stk. 1: "Denne forordning finder anvendelse på……. Ikkeautomatisk behandling af personoplysninger, der vil blive indeholdt i et register."

8. *Er oplysninger om en enkeltmandsvirksomhed personoplysninger?*

   Ja, det er de, og personoplysningerne er således omfattet af GDPR.

9. *Har Sikkerhedsbranchen overvejet at udarbejde et adfærdskodeks/ en certificeringsordning baseret på Datatilsynets "Vejledning om adfærdskodekser og certificeringsordninger", som medlemmerne kan tilslutte sig?*

   SikkerhedsBranchen overvejer løbende muligheden, men indtil nu har medlemsinteressen været så begrænset, at vi ikke mener det kan forsvare arbejdsindsatsen.

   SikkerhedsBranchen stiller til gengæld en række værktøjer til rådighed til medlemmerne, der kan hjælpe med overholdelse af GDPR. De kan ses på den lukkede del af hjemmesiden under menupunktet "Filer" og mappen "Databeskyttelsesforordningen."

10. *Stiller GDPR krav om logning af alt, herunder hvad den enkelte bruger laver på systemet, hvad han ser mv.?*

    SikkerhedsBranchens opfattelse er at det er nok at logge hvem der er logget ind i systemet i hvilket tidsrum. Princippet i den gamle persondatalovs § 41 stk. 3 er ført videre i GDPR, og praksis derfra understøtter vores opfattelse.

Shared services og deling med tredjelande

11. *Hvilke forbehold skal jeg tage, hvis jeg ikke ved, hvor mine data befinder sig?*

    Der altid skal være en databehandleraftale, når man lader andre opbevare sine data. Hvis det overhovedet er muligt, at data kan risikere at ryge udenfor EU, eller et såkaldt sikkert tredjeland, skal der stilles de fornødne garatier for beskyttelse af personoplysninger. Det kan blandt andet ske ved at anvende EU-kommissionens standardbestemmelser om databeskyttelse. Nedenstående er en kort oplistning (ikke udtømmende) af overførselsgrundlag i den forbindelse:

SikkerhedsBranchen
Information Viden Kvalitet

- Overførsler baseret på en afgørelse om tilstrækkeligheden af beskyttelsesniveauet (sikre tredjelande) (artikel 45)
- Overførsler omfattet af fornødne garantier (artikel 46)
- Bindende virksomhedsregler – Binding Corporate Rules (ofte blot kaldet BCR) (artikel 47)
- EU-Kommissionens standardkontraktbestemmelser (https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en)
- EU-U.S. Privacy Shield

12. *Skal jeg kende til alle mine databehandlere?*

    Erhvervskunder skal sikre sig at de har navne på alle deres databehandlere, hvilke data de behandler og meget mere (GDPR artikel 30). Der kan med moderne teknologi være tale om en lang kæde af virksomheder, idet der ofte anvendes underleverandører til nogle opgaver, herunder fx backup (se GDPR artikel 28).

13. *Under hvilke forhold kan man overføre persondata til et tredjeland?*

    Det kræver enten en tilladelse fra Datatilsynet eller at man benytter sig af standardkontrakten fra EU-kommissionen: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

    Man bør dog sikre sig, at standardbestemmelserne er rigtigt indgået, og at man i øvrigt er i stand til at leve op til de forpligtelser, der følger med brugen af standardbestemmelserne. Det er derfor vigtigt, at man sætter sig grundigt ind i indholdet af standardbestemmelserne. Det er muligt at lade standardbestemmelserne være en del af en bredere kontrakt mellem to parter, ligesom det også er muligt at medtage andre bestemmelser eller yderligere garantier. Man bør imidlertid ikke foretage ændringer i standardbestemmelsernes indhold eller medtage andre bestemmelser, der direkte eller indirekte har betydning for standardbestemmelsernes indhold. Gør man dette, vil der ikke længere være tale om standardbestemmelser, der uden videre kan benyttes ved en overførsel.

Databehandling og databehandleraftaler

14. *Hvad er en databehandleraftale?*

SikkerhedsBranchen
Information Viden Kvalitet

Den dataansvarlige kan lade andre opbevare eller på anden vis behandle indsamlet data. Hvis det sker, skal der foreligge en skriftlig databehandleraftale mellem de to parter (GDPR artikel 28).

Det er den dataansvarliges ansvar at have en databehandleraftale med alle, der behandler vedkommendes data. Indholdet skal blot være, at databehandleren kun arbejder efter instruks fra den dataansvarlige og at han aldrig må mere end sin opdragsgiver.

Man kan finde et udkast til en databehandleraftale på Datatilsynets hjemmeside – klik her. SikkerhedsBranchen stiller en branchetilpasset databehandleraftale til rådighed for sine medlemmer på den lukkede del af hjemmesiden klik på filer/Databeskyttelsesforordningen.

15. *Skal jeg have en databehandleraftale?*

Hvis du er dataansvarlig skal du sørge for at have en databehandleraftale med alle dine databehandlere. Hvis du selv er databehandler, bør du hjælpe den dataansvarlige ved at opfordre til at der udarbejdes en databehandleraftale.

SikkerhedsBranchen stiller en branchetilpasset databehandleraftale til rådighed for sine medlemmer på den lukkede del af hjemmesiden klik på filer/Databeskyttelsesforordningen.

16. *Kræver ydelser som service, installation og konfigurering databehandleraftaler alene fordi teknikeren kan se data når han udfører sit arbejde?*

Nej. Det fremgår klart af justitsministeriets vejledning "Dataansvarlige og databehandlere," punkt 3, at når man kun leverer en håndværks- eller it-mæssig ydelse, hvor aftalen ikke vedrører behandling af selve data, men altså arbejde på systemet, hvorved man kommer til at se persondata, så er man ikke databehandler. Man er ikke noget i relation til GDPR. Hvis kunden ønsker en form for garanti for fortrolighed o.l., kan man udstede en tavshedserklæring eller lignende.

17. *Hvem er ansvarlig for databehandleraftalen?*

Den dataansvarlige er ansvarlig for databehandleraftalen. Hverken databehandleren eller den eventuelle installatør af dataindsamlingsudstyret kan stilles til ansvar for en manglende databehandleraftale. SikkerhedsBranchen opfordrer dog til at alle led i kæden gør deres for at få styr på aftalerne. GDPR

SikkerhedsBranchen
Information Viden Kvalitet

artikel 28 betyder desuden, at databehandleren, som noget nyt er ansvarlig for overholdelse af den dataansvarliges forpligtelser i henhold til GDPR, på linje med den dataansvarlige.

18. *Skal jeg som installatør sikre at min kunde har en databehandleraftale?*

    Det er ikke dit ansvar som installatør at sikre at din kunde har en databehandleraftale med fx den kontrolcentral, tv-overvågningsbilleder sendes til. SikkerhedsBranchen opfordrer dog alle sine medlemmer til at de som en service tilbyder kunden at formidle databehandleraftalen.

19. *Hvordan skal jeg som kontrolcentral forholde mig til databehandleraftaler?*

    Det er ikke dit ansvar som kontrolcentral at sikre, at der er en databehandleraftale. Det er dog ikke alle dataansvarlige, der er opmærksomme på kravet om en databehandleraftale, og derfor bør kontrolcentralen opfordre den dataansvarlige – eventuelt gennem installatøren – til at udarbejde en databehandleraftale.

20. *Jeg leverer blot back up af data - skal jeg have en databehandleraftale?*

    Back up er også databehandling, så der skal være en databehandleraftale mellem dig og den dataansvarlige. Det er den dataansvarliges ansvar, men du bør opfordre til udarbejdelsen af aftalen.

21. *Kan en databehandleraftale undlades, hvis man kan påvise at det kun drejer sig om dataopbevaring? Det vil sige at det firma som opbevarer fx videodata ikke har mulighed for at se data grundet kryptering eller anden beskyttelse.*

    Nej. Opbevaring er også databehandling, jf. GDPR artikel 2 nummer 2.

22. *Må databehandler udlevere kundens tv-overvågningsbilleder?*

    Som databehandler må du ikke udlevere billeder fra tv-overvågning til andre end den dataansvarlige selv. Hvis politiet kræver adgang til billederne, må du udlevere efter aftale med den dataansvarlige eller når der foreligger en dommerkendelse. SikkerhedsBranchen anbefaler at det indskrives i databehandleraftalen at billeder må udleveres til politiet.

    Du skal til enhver tid udlevere billeder til den dataansvarlige, hvis denne ønsker

det. Billederne er den dataansvarliges ejendom, og databehandleraftalen giver dig ingen ret til at tilbageholde billederne for dataansvarlige.

23. *Kan databehandler nægte dataansvarlig at få udleveret egne billeder?*

Nej. Dataansvarlig må altid få udleveret sine egne billeder.

24. *Er alle jeg videregiver data til min databehandler?*

Nej, man kan sagtens have to selvstændige dataansvarlige som udveksler data. De er så hver især ansvarlige for at behandling af personoplysninger i deres organisationer sker efter reglerne. Det forekommer især hvor en juridisk enhed modtager oplysninger fra en anden, men selvstændigt behandler oplysningerne. Altså, hvor de ikke handler efter instruks fra dig. Det kan være SKAT, forsikring, sundhedsforsikring, inkasso etc.

Her skal man ikke have en databehandleraftale, men sikre sig at man først og fremmest har ret til eller ligefrem pligt til at udlevere oplysningerne.

Når man skal afgøre om man er dataansvarlig mv. er der hjælp at hente i vejledningen om dataansvarlige og databehandlere (se vores hjemmeside under "filer og Databeskyttelsesforordningen". Det er særligt punkt 3.1.3 og følgende.

Et af de afgørende spørgsmål, når man skal afgøre om den anden part, der behandler persondata fra dig, er dataansvarlig eller databehandler, er om den anden part udfører en opgave som du selv kunne have taget dig af. Det andet spørgsmål er om den anden part kan behandle data uden din instruks eller godkendelse og om du fører kontrol med den anden part. Det tredje gode spørgsmål er hvem der træffer beslutning om formål og behandlingsskridt.

25. *Må to virksomheder på samme adresse med deling af fx lager, bogholderi mv. dele data?*

Her er det vigtigt at adskille personoplysninger, som falder under GDPR, og forretningsoplysninger, som ikke gør. Forretningsoplysninger om kunderne er ikke relevante for GDPR, og hvis virksomhederne kun har banale data på kunderne (navn, telefonnummer mv.) er der ingen større udfordringer.

Udfordringen ligger i hvis en kunde tror han handler med den ene virksomhed og den anden så får hans oplysninger. Det skal virksomhederne have kundernes samtykke til uanset GDPR.

SikkerhedsBranchen
Information Viden Kvalitet

I bogholderiet mv. behandler man typisk følsomme personoplysninger når man laver løn, sygemeldinger, billeder af de ansatte mv. Hvis funktionen formelt ligger i den ene virksomhed behandler den jo særlige (følsomme) personoplysninger for den anden, hvilket kræver en databehandleraftale. I forvejen skal virksomheden have medarbejdernes samtykke til disse behandlinger.

Alle medarbejdere der behandler personoplysninger skal underskrive en tavsheds-/fortrolighedserklæring, være instruerede og løbende holdes opdateret.

26. *Skal jeg have en databehandleraftale med kunder på AIA og ADK (uden tv-overvågning)?*

    Ja, men kun hvis opgaven er at behandle personoplysninger. Hvis opgaven er at behandle signaler med almindelige personoplysninger fra anlæggene eller servicere dem, kræves ikke databehandleraftale. Hvis signalbehandlingen omfatter oplysninger som billeder, CPR-nummer o.l. vil det formentlig kræve en databehandleraftale. Det kræver stadig ikke databehandleraftale, hvis man kun servicerer, opdaterer mv. systemet.

27. *I forbindelse med servicering af adgangskontrolinstallationer hos vore kunder, opbevarer vi en sikkerhedskopi af det aktuelle adgangskontrolprogram. Programmet kan indeholde personlige data på kundens brugere. Sikkerhedskopien opbevares, så vore sikringsteknikere har adgang til sikkerhedskopien. Gør det os til databehandler overfor den aktuelle kunde?*

    Hvis det blot er banale oplysninger: Navn, nummer, e-mail og lignende, så nej. Hvis der bliver tale om andre oplysninger som CPR, billeder, løn, fagforening, helbred og andre særlige personoplysninger, så ja. Medmindre, I kan argumentere for, at det er nødvendigt som led i service og vedligeholdelse af kundens anlæg, for så er I ikke databehandler.