Forberedelser forud for EU's databeskyttelses-forordning

12 spørgsmål som dataansvarlige allerede nu med fordel kan forholde sig til

Indledning[1]

Dette dokument indeholder 12 spørgsmål, som I, der er dataansvarlige, med fordel kan forholde jer til allerede nu for at forberede jer på den nye databeskyttelsesforordning, som finder anvendelse fra den 25. maj 2018.

Databeskyttelsesforordningen vil have direkte virkning i Danmark, hvilket betyder, at der som udgangspunkt ikke må være anden dansk lovgivning, der regulerer behandling af personoplysninger, i det omfang dette er reguleret i forordningen.

Danmark er dermed forpligtet til at indrette dansk lovgivning i overensstemmelse med databeskyttelsesforordningens bestemmelser. Justitsministeriet har derfor i samarbejde med Datatilsynet, Erhvervsstyrelsen og Digitaliseringsstyrelsen påbegyndt et projekt med en styregruppe og projektgrupper, som skal stå for at sikre ovennævnte overensstemmelse. I kan læse mere herom her
http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2016/Databeskyttelsesforordning.pdf

Mange af databeskyttelsesforordningens begreber og principper er kendt fra den nuværende persondatalov. Hvis I således allerede i dag har de fornødne foranstaltninger og rutiner på plads for at sikre efterlevelse af persondataloven og eventuel særlovgivning, har I også et godt udgangspunkt for at efterleve forordningens bestemmelser. Det er dog vigtigt at pointere, at der med databeskyttelsesforordningen også indføres en række helt nye bestemmelser, som det påhviler jer som dataansvarlige at få styr på og efterleve.

Det er derfor vigtigt, at I allerede nu begynder at overveje, hvordan I vil sikre, at jeres organisation efterlever databeskyttelsesforordningens bestemmelser, så I bl.a. kan nå at få involveret og få støtte fra relevante beslutningstagere og nøglepersoner mv. ’

Dette dokument kan anvendes som en tjekliste, når I skal have styr på hovedforskellene mellem den nuværende lovgivning og den nye databeskyttelsesforordning og på, hvordan de påvirker jeres organisation.

Datatilsynet vil på forskellig vis løbende informere om den kommende databeskyttelsesforordning. Herudover vil den såkaldte Artikel 29-gruppe, der består af samtlige datatilsyn i EU, løbende komme med vejledninger på europæisk niveau. Der vil endvidere i regi af Justitsministeriet løbende blive afholdt stormøder med interessenterne mv.

[1] Ved udarbejdelsen af denne vejledning har Datatilsynet ladet sig inspirere af en publikation, som det engelske datatilsyn (Information Commissioner’s Office) har lavet om samme emne. Information Commissioner’s Office’s (ICO) publikation kan findes på denne hjemmeside: https://ico.org.uk/

1. Har jeres organisation kendskab til den nye databeskyttelsesforordning?

I bør sikre, at beslutningstagere og nøglepersoner i jeres organisation er bevidste om, at persondataloven vil blive erstattet af databeskyttelsesforordningen. I bør også undersøge, hvordan jeres organisation vil blive påvirket af forordningen og identificere de områder, som I bliver nødt til at arbejde særskilt med.

Der kan være behov for, at I afsætter en del ressourcer for at nå at tilpasse jeres organisation til de nye krav, inden databeskyttelsesforordningen finder anvendelse fra den 25. maj 2018. Indledningsvist bør I fokusere på at øge bevidstheden om de kommende forandringer. Det kan nemlig blive vanskeligt at opfylde reglerne i forordningen, hvis I først går i gang med forberedelserne i sidste øjeblik.

2. Hvilke personoplysninger behandler I?

I bør undersøge dokumentere, hvilke personoplysninger I behandler, hvor oplysninger kommer fra, og hvem I deler dem med. Der kan endvidere være behov for at lave en bred gennemgang af jeres organisation med henblik på at finde ud af, hvilke oplysninger, der behandles i hvilke dele af organisationen.

Databeskyttelsesforordningen indeholder rettigheder, som er tilpasset informationssamfundet. Hvis I for eksempel berigtiger forkerte oplysninger om en person, og I tidligere har delt disse oplysninger med andre, vil I være forpligtet til at informere disse modtagere om berigtigelsen, så de også kan berigtige oplysningerne i deres system. I vil ikke være i stand til at efterleve denne forpligtelse, hvis I ikke ved, hvilke personoplysninger I behandler, hvor oplysningerne kommer fra, og hvem I har delt dem med.

Hvis I får styr på ovennævnte, vil det også kunne hjælpe jer til at efterleve databeskyttelsesforordningens krav om, at I skal have en fortegnelse over jeres behandlingsaktiviteter, således at I kan dokumentere, at forordningens bestemmelser efterleves.

3. Hvilken information giver I de registrerede?

I bør gennemgå den information, som I giver til de registrerede og tænke over, hvilke ændringer af informationen, som databeskyttelsesforordningen måtte nødvendiggøre.

Når I indsamler personoplysninger, skal I efter persondataloven give de registrerede en række oplysninger i forbindelse med indsamlingen, herunder oplysninger om jeres identitet samt formålet med behandlingen.

Databeskyttelsesforordningen indeholder øgede krav til, hvilke oplysninger I skal give de registrerede. Bl.a. indeholder forordningen krav om, at I skal oplyse de registrerede om jeres behandlingsgrundlag, hvor længe oplysningerne behandles og om muligheden for at klage til tilsynsmyndigheden (som i Danmark er Datatilsynet), hvis de registrerede mener, at I behandler

deres oplysninger i strid med forordningen. Det er i den sammenhæng vigtigt at være opmærksom på, at databeskyttelsesforordningen også stiller krav om, at den information I giver de registrerede skal være kortfattet, letforståelig og udformet i et tydeligt og enkelt sprog.

4. Hvordan opfylder I de registreredes rettigheder?

I bør gennemgå jeres procedurer for at sikre, at I kan opfylde alle de rettigheder, som de registrerede er tillagt efter databeskyttelsesforordningen.

De registreredes vigtigste rettigheder efter databeskyttelsesforordningen er:

- Retten til at modtage oplysning om en behandling af sine personoplysninger (oplysningspligt)
- Retten til at indsigt i sine personoplysninger
- Retten til at få urigtige personoplysninger berigtiget
- Retten til at få sine personoplysninger slettet
- Retten til at gøre indsigelse mod at personoplysninger anvendes til direkte markedsføring
- Retten til at gøre indsigelse mod automatiske individuelle afgørelser, herunder profilering
- Retten til at flytte sine personoplysninger (dataportabilitet)

I det store hele kommer de registrerede til at have de samme rettigheder som i dag, men rettighederne styrkes eller skærpes med databeskyttelsesforordningen. Hvis I allerede i dag har styr på de registreredes rettigheder, bør overgangen til den nye forordning være relativ smidig.

Det er derfor en god idé allerede nu at gennemgå jeres rutiner og tænke over, hvordan I vil håndtere en anmodning om for eksempel sletning fra en registreret. Kan jeres system hjælpe jer til at finde og eventuelt slette oplysningerne? Hvem i jeres organisation kan træffe beslutning om sletning?

Databeskyttelsesforordningens ret til dataportabilitet er en nyskabelse. Denne rettighed vil gøre det lettere for de registrerede at flytte deres personoplysninger fra en organisation eller leverandør til en anden, herunder for eksempel fra et socialt netværk til et andet. For jeres organisation indebærer retten til dataportabilitet, at I mange tilfælde skal kunne tilvejebringe oplysningerne i et alment anvendt og maskinlæsbart format. I bør derfor overveje, om I er i besiddelse af de fornødne tekniske løsninger mv. Det skal bemærkes, at retten til dataportabilitet ikke finder anvendelse i situationer, hvor en behandling er nødvendig for udførelse af en opgave i samfundets interesse, eller hvor behandlingen henhører under offentlig myndighedsudøvelse,

5. På hvilket retligt grundlag behandler I personoplysninger?

I bør undersøge, hvilke kategorier af personoplysninger I behandler, og på hvilket retligt grundlag I gør det. I bør samtidig dokumentere jeres konklusioner.

Mange organisationer har ikke tydeligt udpeget på hvilket retligt grundlag, de behandler personoplysninger. Det er heller ikke usædvanligt, at organisationer kan have flere forskellige retlige grundlag at basere en behandling af personoplysninger på.

Med databeskyttelsesforordningen indføres krav om, at I skal informere de registrerede om jeres retlige grundlag, allerede når oplysningerne indsamles. Det er derfor vigtigt, at I med det samme gør jer klart, hvad der er jeres retlige grundlag for at behandle oplysningerne.

Herudover kan de registreredes rettigheder efter forordningen have forskelligt indhold afhængigt af det retlige grundlag for behandlingen. Et eksempel på dette er, at de registrerede vil have et stærkere krav på sletning af deres oplysninger, hvis I benytter samtykke som behandlingshjemmel.

Helt overordnet svarer databeskyttelsesforordningens behandlingsregler i vidt omgang til reglerne i persondataloven. Efter forordningen vil man således fortsat kunne behandle relevante personoplysninger til saglige formål bl.a. på baggrund af et udtrykkeligt samtykke fra den person, oplysningerne vedrører, eller når det er nødvendigt at behandle oplysningerne med henblik på myndighedsudøvelse. I kan derfor allerede nu kortlægge, hvilke behandlinger I foretager og på hvilket grundlag, I gør det.

Når I har foretaget denne analyse, bør I dokumentere jeres konklusioner, så I også kan vise, at I efterlever forordningens bestemmelser.

Vær opmærksom på, at offentlige myndigheder fremover ikke vil kunne støtte sin behandling på en interesseafvejning.

6. Hvordan indhenter I samtykke?

I bør undersøge, hvordan I indhenter, opbevarer og dokumenterer samtykke, og om I bør foretage nogen ændringer.

Et gyldigt samtykke efter databeskyttelsesforordningen skal ligesom efter persondataloven være en frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling.

Herudover skal et samtykke efter databeskyttelsesforordningen også være ”utvetydigt” og ske ved erklæring eller klar bekræftelse. Efter databeskyttelsesforordningen vil et samtykke således for eksempel ikke kunne være stiltiende. Hvis samtykke gives i en skriftlig erklæring, der også vedrører andre forhold, skal samtykket også klart kunne skelnes fra de andre forhold.

Hvis I benytter samtykke som det retlige grundlag for jeres behandling, bør I sikre jer, at jeres samtykke lever op til de krav, der følger af forordningen. Viser dette sig ikke at være tilfældet, bør I ændre jeres samtykkerutiner eller finde et andet behandlingsgrundlag.

Databeskyttelsesforordningen stiller i øvrigt et tydeligt krav om, at I, som dataansvarlige, skal være i stand til at dokumentere, at samtykke er givet. I bør derfor også overveje, hvordan I sikrer, at jeres procedurer og systemer kan leve op til dette krav.

7. Behandler I personoplysninger om børn?

I bør allerede nu overveje, hvordan I fremadrettet vil kontrollere en persons alder, og hvordan I vil indhente samtykke fra forældremyndighedsindehavere, når I i visse situationer behandler oplysninger om børn.

Med databeskyttelsesforordningen indføres en særlig beskyttelse af personoplysninger om børn, navnlig hvis der er tale om informationssamfundstjenester som for eksempel sociale netværk.

Kort fortalt, hvis I udbyder denne type af tjenester til børn, skal I indhente samtykke fra forældremyndighedsindehaverne, hvis I ønsker at behandle oplysninger om deres børn. Efter databeskyttelsesforordningen gælder den særlige beskyttelse som udgangspunkt for børn under 16 år, men de enkelte medlemsstater har mulighed for at fastsætte en lavere aldersgrænse til børn, dog ikke under 13 år.

Reglerne kan få konsekvenser for jeres organisation, hvis I lever af at udbyde ovennævnte tjenester til børn. Husk i den forbindelse på, at I også skal kunne dokumentere, at I har indhentet samtykke fra forældremyndighedsindehaverne.

Da børn som sagt ifølge forordningen fortjener særlig beskyttelse må al den information, som retter sig mod børn, i øvrigt også være skrevet på en tydelig og enkel måde, som børn forstår. Der skal også lægges vægt på børns beskyttelsesværdige stilling i forbindelse med interesseafvejning.

8. Hvad skal I gøre ved brud på persondatasikkerheden?

I bør sikre jer, at I har de fornødne procedurer på plads til at opdage, rapportere og undersøge brud på persondatasikkerheden.

Databeskyttelsesforordningen indeholder nye bestemmelser om, hvad I som organisation skal gøre, hvis I bliver udsat for et hackerangreb eller på anden måde mister kontrollen over de personoplysninger, I behandler.

I skal efter forordningen dokumentere alle sådanne brud på persondatasikkerheden. Med mindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, skal I endvidere anmelde bruddet til den relevante tilsynsmyndighed inden for 72 timer.

Hvis bruddet på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder eller frihedsrettigheder, herunder for eksempel en risiko for diskrimination, identitetstyveri eller bedrageri, vil I tillige, uden unødig forsinkelse, skulle underrette de registrerede om bruddet.

For at I kan efterleve databeskyttelsesforordningens krav i forbindelse med brud på persondatasikkerheden, er det vigtigt, at I har de fornødne procedurer på plads til at opdage, rapportere og undersøge brud på sikkerheden. Det er også vigtigt, at I hurtigt kan vurdere alvorligheden af et eventuelt brud på persondatasikkerheden, da der som nævnt er korte frister for

underretning af tilsynsmyndighederne og de registrerede. I kan formentlig med fordel allerede nu begynde at overveje, hvor ansvaret for behandling af brud på persondatasikkerheden skal ligge i jeres organisation.

9. Er jeres behandlinger forbundet med særlige risici?

I bør overveje, om jeres behandling af personoplysninger er forbundet med særlige risici for den registreredes grundlæggende rettigheder, og om I i så fald skal udarbejde en konsekvensanalyse vedrørende databeskyttelse i overensstemmelse med forordningen.

Databeskyttelsesforordningen stiller som noget nyt krav om, at I i visse situationer skal foretage en konsekvensanalyse, hvis I foretager en type behandling der, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

En konsekvensanalyse vedrørende databeskyttelse vil navnlig være påkrævet, hvis I behandler følsomme oplysninger i stort omfang eller beskæftiger jer med profilering og systematisk overvågning af offentligt tilgængelige områder.

Konsekvensanalysen skal bl.a. omfatte en systematisk beskrivelse af de planlagte behandlingsaktiviteter, en vurdering af behandlingsaktiviteternes nødvendighed og rimelige forhold til formålene, en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder og en beskrivelse af de foranstaltninger, der påtænkes med henblik på at imødegå de konstaterede risici.

Viser en konsekvensanalyse, at der vil være en høj risiko for den registrerede skal tilsynsmyndigheden høres, inden I iværksætter behandlingen.

Vær endvidere opmærksom på kravet om at udpege en databeskyttelsesrådgiver ved bl.a. risikofyldte behandlinger, jf. pkt. 11 nedenfor.

10. Har I indtænkt databeskyttelse i jeres it-systemer?

I kan med fordel allerede nu begynde at tage hensyn til databeskyttelsesforordningens regler, når I tager et nyt it-system i brug eller ændrer et eksisterende. Det vil gøre det lettere for jer at efterleve af reglerne og højne sikkerheden.

Det er grundlæggende principper inden for databeskyttelse, at I ikke indsamler flere personoplysninger end nødvendigt, at I ikke opbevarer oplysningerne længere end nødvendigt, og at I ikke anvender oplysningerne til andre formål, end de formål, som oplysningerne oprindeligt blev indsamlet til.

Ved at tage hensyn til disse principper, når I udvikler nye, eller ændrer eksisterende, it-systemer, bliver det lettere for jer at efterleve reglerne i databeskyttelsesforordningen. At indtænke databeskyttelse i it-systemer kaldes databeskyttelse gennem design (privacy by design), og et sådan krav følger nu direkte af databeskyttelsesforordningen.

Når I behandler personoplysninger, skal I – ligesom i dag – træffe passende tekniske og organisatoriske foranstaltninger for at opfylde kravene i databeskyttelsesforordningen, både når I træffer beslutning om, hvordan behandlingen skal foretages og under hele den fortsatte behandling. Hvilke foranstaltninger, som er nødvendige, beror på oplysningernes karakter, mængden af oplysninger, formålet med behandlingen, og hvilke risici en behandling kan indebære for de registreredes rettigheder og frihedsrettigheder. Foranstaltningerne kan for eksempel bestå i pseudonymisering, som indebærer, at en oplysning ikke kan henføres til en bestemt person uden en "nøgle", som holdes adskilt fra oplysningerne, eller dataminimering, hvilket vil sige kun at behandle de oplysninger, der nødvendige for hvert enkelt formål.

11. Hvem er ansvarlig for databeskyttelsesspørgsmål i jeres organisation?

I bør beslutte, hvor i jeres organisation ansvaret for databeskyttelsesspørgsmål skal ligge. I visse situationer indeholder databeskyttelsesforordningen også krav om, at I formelt skal udpege en databeskyttelsesrådgiver (DPO).

Databeskyttelsesforordningen stiller krav om, at visse organisationer skal udpege en databeskyttelsesrådgiver. Det gælder for eksempel alle offentlige myndigheder og organisationer, hvor kerneaktiviteterne består af behandling i stort omfang af følsomme oplysninger mv.

En databeskyttelsesrådgiver skal udpeges på grundlag af sine faglige kvalifikationer, navnlig ekspertise inden for databeskyttelsesret og –praksis samt evne til at udføre de opgaver, som rådgiveren er pålagt efter databeskyttelsesforordningen.

I bør allerede nu overveje, om jeres organisation vil blive underlagt databeskyttelsesforordningens krav om at have en databeskyttelsesrådgiver, ligesom I allerede nu bør overveje, om I har en person med de fornødne evner i jeres organisation, eller om der er behov for efteruddannelse af en medarbejder eller ansættelse af en ny.

12. Driver I virksomhed i flere lande?

Hvis jeres organisation driver virksomhed i flere EU-lande, bør I finde ud af, hvilken tilsynsmyndighed, som har ansvaret for at føre tilsyn med de behandlinger af personoplysninger, som I foretager jer.

Hovedreglen i den nye databeskyttelsesforordning er, at I kun behøver at kommunikere med én tilsynsmyndighed inden for EU, når I foretager grænseoverskridende behandlinger.

Hvis I driver virksomhed i flere EU-lande er det derfor vigtigt, at I finder ud af, hvilken tilsynsmyndighed, som har ansvaret for at føre tilsyn med de behandlinger af personoplysninger, som I foretager jer.

Databeskyttelsesforordningens regler om, hvilken tilsynsmyndighed, der er kompetent ved grænseoverskridende behandlinger, er komplicerede, men forenklet sagt er den kompetente tilsynsmyndighed den, der er placeret i det EU-land, hvor I har jeres centrale organisation eller hvor

der træffes beslutninger om behandling af personoplysninger. I organisationer med en traditionel opbygning, hvor hovedkontoret træffer alle vigtige beslutninger, vil de nye kompetenceregler næppe skabe store problemer. Det kan dog være mere vanskeligt i organisationer med spredte ansvarsområder, hvor beslutninger om behandling af personoplysninger ofte tages forskellige steder. I sådanne situationer kan forskellige behandlinger falde under forskellige tilsynsmyndigheders kompetence.

Det kan altså være nødvendigt, at I foretager en kortlægning af, hvor i jeres organisation de mest betydningsfulde beslutninger om behandling af personoplysninger træffes.