JUSTITSMINISTERIET

Vejledning om lokationskravet i databeskyttelsesloven

Juli 2020

Indhold

1 Forord

Databeskyttelsesforordningen og databeskyttelsesloven
Den generelle forordning nr. 2016/679 om beskyttelse af personoplysninger (databeskyttelsesforordningen) fandt anvendelse fra den 25. maj 2018. Samtidig trådte lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven) i kraft. Databeskyttelsesloven indeholder en bestemmelse om, at justitsministeren efter forhandling med vedkommende minister kan fastsætte regler om, at personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning, helt eller delvis alene må *opbevares* her i landet. Denne bestemmelse indeholder således et lokationskrav, jf. lovens § 3, stk. 9.

Formålet med lokationskravet er at sikre, at de it-systemer, der er omfattet af reglen, er underlagt dansk jurisdiktion. Det sikrer, at danske myndigheder har adgang til de pågældende it-systemer og dermed mulighed for inden for lovgivningens rammer bl.a. at modvirke uretmæssig udnyttelse eller påvirkning af personoplysningerne i systemet ved at overvåge de personer, der arbejder i systemet, eller sikre at visse personer ikke får adgang til systemet. Formålet er også, at det er dansk ret – og dermed ikke andre landes lovgivning – der regulerer adgangen til it-systemerne.

Det er vigtigt at understrege, at lokationskravet alene har til formål at sikre, at personoplysninger i visse it-systemer, som føres for det offentlige, fysisk opbevares i datacentre mv., som er lokaliseret i Danmark (jurisdiktionshensynet). Denne vejledning skal alene læses i dette lys. Lokationskravet finder således ikke anvendelse i forhold til it-systemer, der ikke behandler personoplysninger, eller it-systemer, der føres for private. Det skal desuden understreges, at det ikke er hensigten at anvende lokationskravet for at imødekomme hensyn, der vedrører it-sikkerheden, idet dette hensyn i tilstrækkelig grad må forventes tilgodeset i bestemmelserne i forordningen, herunder databeskyttelsesforordningens artikel 32 om behandlingssikkerhed – uafhængigt af om det pågældende it-system føres her i landet eller i et andet EU-land.

Det fremgår af afsnit 2.1.3.3. i de almindelige bemærkninger til lovforslaget til databeskyttelsesloven, at det forudsættes, at Justitsministeriet kan udarbejde nærmere retningslinjer, som skal følges, når vedkommende minister overvejer at indkøbe et it-system, der helt eller delvis kan være omfattet af anvendelsesområdet for lokationskravet i databeskyttelsesloven. Denne vejledning indeholder sådanne retningslinjer og er hovedsageligt skrevet til offentlige myndigheder, der i forbindelse med indkøb af et it-system eller i forbindelse med genudbud af et eksisterende it-system el. lign. skal undersøge, om it-systemet af hensyn til statens sikkerhed helt eller delvis alene må føres (personoplysninger opbevares) i Danmark. Retningslinjerne vil inddrage de tværgående erfaringer, der er gjort i forbindelse med de it-systemer, som allerede *er* blevet vurderet efter lokationskravet i databeskyttelsesloven.

Lov om retshåndhævende myndigheders behandling af personoplysninger
Ved lov nr. 503 af 23. maj 2018 blev bl.a. § 27 i retshåndhævelsesloven (lov om retshåndhævende myndigheders behandling af personoplysninger) ændret. Bestemmelsen i retshåndhævelsesloven er herefter identisk med lokationskravet i databeskyttelsesloven.

Retshåndhævelsesloven gælder for politiets, anklagemyndighedens, herunder den militære anklagemyndigheds, kriminalforsorgens, Den Uafhængige Politiklagemyndigheds og domstolenes behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og for anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register, når behandlingen foretages med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder for at beskytte mod eller forebygge trusler mod den offentlige sikkerhed.

Vurderingen af, hvornår et it-system skal føres her i landet efter databeskyttelseslovens § 3, stk. 9, og retshåndhævelseslovens § 27, stk. 3, er derfor den samme. Denne vejledning omtaler for overblikkets skyld alene lokationskravet i databeskyttelsesloven, men lokationskravet i retshåndhævelsesloven skal fortolkes i overensstemmelse hermed.

2 Baggrund for lokationskravet

2.1 Den tidligere ”krigsregel” i persondatalovens § 41, stk. 4

Det fremgik af persondatalovens § 41, stk. 4, at der for oplysninger, som behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, skulle træffes foranstaltninger, der muliggjorde bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold. Det var således hensigten, at et it-system omfattet af reglen skulle have en ”rød knap”, der sikrede, at det var muligt at destruere hele systemet ved ét tryk.

Bestemmelsen indebar i praksis, at visse større landsdækkende administrative systemer og specialregistre ikke måtte føres i udlandet. Det var som det klare udgangspunkt den offentlige myndighed, der selv vurderede, om et it-system var omfattet af bestemmelsen.

Der er sket en betydelig teknologisk udvikling siden vedtagelsen af persondataloven i 2000, hvorefter den fysiske driftsafvikling af et it-system inden for Danmarks grænser ikke nødvendigvis længere er en garanti for at sikre bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold. Et krav om at sikre bortskaffelse eller tilintetgørelse af oplysninger vil kunne ske ved at anvende en anden sikkerhedsmodel.

Persondataloven blev ophævet den 25. maj 2018 med lov nr. 502 af 23. maj 2018 (databeskyttelsesloven). Særligt på grund af den teknologiske udvikling indeholder databeskyttelsesloven en nyskabelse af dette lokationskrav, som dermed afløser den tidligere ”krigsregel”.

2.2 Det moderniserede lokationskrav i databeskyttelseslovens § 3, stk. 9

Efter databeskyttelseslovens § 3, stk. 9, bemyndiges justitsministeren til efter forhandling med vedkommende minister at kunne fastsætte regler om, at personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning, helt eller delvis alene må opbevares her i landet. Bestemmelsen afløser – for indkøb af it-systemer efter den 25. maj 2018, herunder (gen)udbud og outsourcing af eksisterende it-systemer – den tidligere ”krigsregel” efter persondatalovens § 41, stk. 4.

Det moderniserede lokationskrav indeholder i modsætning til den tidligere ”krigsregel” ikke en forudsætning om, at et it-system, der er omfattet af bestemmelsen, skal kunne destrueres med en ”rød knap”. Dermed er lokationskravet med databeskyttelseslovens § 3, stk. 9, en regel, der skal sikre, at de it-systemer, som er omfattet af reglen, er underlagt jurisdiktion for danske myndigheder (og den dataansvarlige selv) og således ikke en regel, der skal sikre, at it-systemer kan destrueres.

Efter den nye udformning af lokationskravet skal it-systemer, der er omfattet af bestemmelsen – før de tages i brug – af justitsministeren efter forhandling med vedkommende minister, sættes på den liste, der optages som bilag til en bekendtgørelse efter lovens § 3, stk. 9.[1]

At forhandlingen sker med vedkommende minister betyder i praksis, at det er vedkommende ressortministerium, der – når ressortministeriet vurderer, at det er relevant – *skal* rette henvendelse til Justitsministeriet med henblik på en vurdering af, om it-systemet er omfattet af lokationskravet. Underliggende myndigheder, kommuner, regioner mv. skal således rette henvendelse til Justitsministeriet gennem det ressortministerium, der har lovgivningskompetence inden for det dataområde, som det pågældende it-system vedrører.

Vurderingen af, om it-systemet er omfattet af lokationskravet, vil således – i modsætning til den tidligere gældende "krigsregel" – ligge hos samme myndighed (Justitsministeriet), hvilket vil bidrage til en mere ensartet praksis.

It-systemer sættes alene på listen, hvis det vurderes, at det er af hensyn til statens sikkerhed, at det pågældende it-system fysisk skal føres her i landet. I en sådan situation vil *opbevaringen* af personoplysninger i det pågældende it-system falde uden for EU-retten og dermed databeskyttelsesforordningen, jf. databeskyttelsesforordningens artikel 2, stk. 2, litra a, og EU-traktatens artikel 4, stk. 2, 3. pkt. For nærmere herom henvises til betænkning nr. 1565/2017 om databeskyttelsesforordningen, side 544-550. For *behandling* i øvrigt af personoplysninger i it-systemet (indsamling, videregivelse mv.), vil de almindelige databeskyttelsesretlige regler finde anvendelse.

Forordning 2018/1807 om en ramme for fri udveksling af andre data end personoplysninger i EU (forordningen om frie datastrømme) indeholder et forbud mod dataplaceringskrav for andre data end persondata. Et dataplaceringskrav kan dog fastsættes af hensyn til den offentlige sikkerhed, forudsat det overholder proportionalitetsprincippet. Lokationskravet i databeskyttelseslovens § 3, stk. 9, er således i overensstemmelse med forbuddet mod dataplaceringskrav for andre data end persondata.

Af anden relevant lovgivning kan nævnes § 25, nr. 5, i bekendtgørelse nr. 567 af 1. juni 2016 om informationssikkerhed og beredskab i net og tjenester, hvorefter Center for Cybersikkerhed, såfremt det er af væsentlig samfundsmæssig betydning, efter en konkret vurdering kan påbyde erhvervsmæssige udbydere af offentligt tilgængelige net og tjenester, at udstyr, der benyttes til at foretage indgreb i meddelelseshemmeligheden, skal opsættes i og drives fra Danmark.

Derudover vil det efter omstændighederne i særlige tilfælde kunne være foreneligt med EU-retten at stille lokationskrav i forbindelse med udbud af et it-system, hvis lokationskravet er begrundet i statens sikkerhed.

2.2.1. Hvad gælder for eksisterende it-systemer?

Den tidligere gældende "krigsregel" efter persondataloven skulle bl.a. sikre, at der lovligt kunne træffes beslutning om destruktion mv., hvis det skulle vise sig nødvendigt. Det moderniserede

[1] Bekendtgørelse nr. 1104 af 30. juni 2020 om helt eller delvis opbevaring her i landet af personoplysninger, der behandles i nærmere bestemte it-systemer, og som føres for den offentlige forvaltning (Lokationskravsbekendtgørelsen).

lokationskrav i databeskyttelsesloven indeholder ikke en forudsætning om, at et it-system, der er omfattet af bestemmelsen, skal kunne destrueres med en "rød knap". Der henvises til afsnit 2.1. og 2.2 ovenfor.

For de eksisterende it-systemer, der er blevet vurderet efter den tidligere "krigsregel", er der ikke længere krav om, at der lovligt skal kunne træffes beslutning om destruktion mv. Eksisterende it-systemer vil kun skulle vurderes efter det nugældende lokationskrav, hvis – og først på det tidspunkt – it-systemet eller dele heraf (gen)udbydes, outsources eller ændres på en sådan måde, at der er risiko for, at systemets kritikalitet ændres. Vurderingen af, om en outsourcing eller ændring er så væsentlig, at den skal vurderes efter lokationskravet, beror på, om der sker ændringer i opbevaringen af personoplysninger i it-systemet. Skal en driftsleverandør eksempelvis flytte servere til et andet EU-land, skal man som myndighed overveje, om det vil indebære, at it-systemet bliver omfattet af det nugældende lokationskrav.

I det tilfælde, hvor en myndighed påtænker at indkøbe et nyt it-system, skal det ligeledes overvejes, om dette kan medføre væsentlige ændringer i opbevaringen af personoplysningerne i et eksisterende it-system, således at der eventuelt skal ske en samlet vurdering af it-systemerne. Der henvises til afsnit 3.4.2. nedenfor.

Sammenfattende er det dermed alene i forbindelse med indkøb af et nyt it-system eller i ovennævnte situationer, at Justitsministeriet skal kontaktes, jf. afsnit 3 nedenfor.

2.2.2. Behandlingssikkerhed eller statens sikkerhed

Lokationskravet efter databeskyttelsesloven er ikke en regel om *behandlingssikkerhed* (it-sikkerhed), men derimod en regel om, at visse it-systemer, der indeholder personoplysninger, af hensyn til *statens sikkerhed* skal føres i Danmark med det formål at sikre, at det er de danske myndigheder, der er kompetente til at håndhæve lov og ret på det sted, hvor personoplysningerne fysisk opbevares.

Krav til behandlingssikkerheden ved behandling af personoplysninger reguleres af databeskyttelsesforordningens artikel 32 sammen med databeskyttelsesloven (for de retshåndhævende myndigheder gælder retshåndhævelseslovens § 27). Den dataansvarlige og databehandleren skal ifølge bestemmelsen i artikel 32 gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger. Dette skal ske under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Databeskyttelsesforordningen gælder for hele EU og har bl.a. et hovedformål om fri bevægelighed af personoplysninger. En vurdering af, om den dataansvarlige eller databehandleren lever op til kravene om behandlingssikkerhed i artikel 32, er således uafhængig af, i hvilket EU-land vedkommendes driftsleverandør af f.eks. en hosting-ydelse er etableret.

Denne vejledning indeholder således ikke vejledning om, hvad der er tilstrækkelig sikkerhed efter databeskyttelsesforordningens artikel 32. For nærmere herom se vejledning om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger, der er tilgængelig på Datatilsynets hjemmeside www.datatilsynet.dk.

2.2.3. Nærmere om statens sikkerhed

Det er som nævnt hensynet til statens sikkerhed, der kan begrunde, at et it-system skal føres her i landet. Der findes ikke en entydig beskrivelse af begrebet ”statens sikkerhed” i EU-retten eller i praksis fra EU-Domstolen. Domstolen har dog – i forskellige sammenhænge – udtalt sig om et tilstødende begreb ”offentlig sikkerhed”. Der kan f.eks. henvises til sag C-145/09, Tsakouridis, hvorefter den offentlige sikkerhed bl.a. dækker over ”både en medlemsstats indre og ydre sikkerhed” og ”en trussel mod de grundlæggende offentlige institutioners og tjenesters funktionsmåde eller befolkningens overlevelse samt risikoen for en alvorlig forstyrrelse af de internationale relationer eller af nationernes fredelige sameksistens eller en trussel mod militære interesser”, jf. præmis 43 og 44. Endvidere har EU-Domstolen udtalt, at det tilkommer medlemsstaterne nærmere at bestemme, hvad hensynene til den offentlige orden og den offentlige sikkerhed kræver, dog under kontrol af Domstolen, jf. sag C-348/09, P.I., præmis 23.

Begrebet ”statens sikkerhed” skal først og fremmest fastlægges funktionelt ud fra et skøn over, om der er tale om statens sikkerhed.

Andre steder i den nationale lovgivning findes der eksempler på, at hensynet til statens sikkerhed begrunder særlige krav, betingelser, undtagelser mv., som kan tjene til inspiration. Det gælder bl.a. forvaltningslovens § 15 og offentlighedslovens § 31, hvor hensynet til statens sikkerhed kan begrunde, at oplysninger er undtaget fra aktindsigt. Som eksempel kan nævnes oplysninger, der kan bringe statsministerens personlige sikkerhed i fare eller være til fare for sikkerheden for udsendt ambassadepersonale eller operationssikkerheden for udsendte militære styrker. Endvidere kan hensynet til statens sikkerhed i visse tilfælde begrunde, at identiteten på visse personer skal undtages fra aktindsigt. Det kan f.eks. være navne på ansatte i Politiets Efterretningstjeneste (PET) og Forsvarets Efterretningstjeneste (FE), ligesom også oplysninger om f.eks. PET’s konkrete operative sager kan være undtaget.

Der kan som nævnt ikke siges noget entydigt om, hvordan statens sikkerhed skal defineres, men det ligger klart, at der skal meget til, før man kan tale om statens sikkerhed. Det vil altså ikke være statens sikkerhed, hvis risikoen ved it-systemets nedbrud er, at det eksempelvis vil være til gene for borgere eller det offentlige, eller hvis det vil skade en myndigheds renommé at opleve et stort sikkerhedsbrud. Den omstændighed, at it-systemet behandler personoplysninger, som stiller store krav til behandlingssikkerheden, vil endvidere ikke være et hensyn til statens sikkerhed. Se desuden afsnit 2.2.2. ovenfor. Der vil omvendt kunne være tale om statens sikkerhed, hvis der med manglende adgang til personoplysningerne i it-systemet vil være tale om *en trussel mod de grundlæggende offentlige institutioners funktionsmåde*, eller hvis den manglende adgang kan siges at *have en ødelæggende effekt på væsentlige funktioner i det danske samfund*.

2.2.4. Justitsministeren foretager vurderingen af, hvilke it-systemer der er omfattet af lokationskravet

I Danmark er det justitsministeren, der varetager opgaver vedrørende det samlede justitsvæsen, herunder politi- og anklagemyndighed, retsvæsen og kriminalforsorg. På den baggrund er det med databeskyttelsesloven vedtaget, at det er justitsministeren, der efter forhandling med vedkommende minister vurderer, hvilke it-systemer der er omfattet af databeskyttelseslovens § 3, stk. 9.

Justitsministeren foretager således i relevante situationer en vurdering af, hvilke it-systemer der er omfattet af bestemmelsen af hensyn til statens sikkerhed. Vurderingen foretages efter inddragelse af PET, som til brug herfor indhenter bidrag fra FE.

3 Hvornår skal man rette henvendelse til Justitsministeriet, og hvilke overvejelser skal en myndighed gøre sig?

3.1 Hvornår skal en offentlig myndighed gennem sit ressortministerium rette henvendelse til Justitsministeriet?

Denne vejledning skal følges, når en offentlig myndighed overvejer at indkøbe et nyt it-system. Vejledningen skal endvidere følges ved (gen)udbud eller outsourcing af eksisterende it-systemer eller dele heraf. Det kan ikke udelukkes, at det også vil være nødvendigt at følge vejledningen, hvis der sker gennemgribende eller væsentlige ændringer i eksisterende it-systemer eller it-infrastrukturer, og hvis sådanne ændringer indebærer en risiko for, at systemets kritikalitet væsentligt forøges eller formindskes. Der henvises til afsnit 2.2.1. for yderligere oplysninger om eksisterende systemer.

Idet lokationskravet gælder for it-systemer, der føres for det offentlige, finder vejledningen ikke anvendelse i forhold til it-systemer, der føres for private.

Lokationskravet i databeskyttelsesloven er en regel om, at it-systemer, der behandler *personoplysninger*, skal føres her i landet. Da lokationskravet endvidere alene gælder for it-systemer, der behandler *personoplysninger*, er det afgørende indledningsvis at få klarlagt, om systemet overhovedet behandler personoplysninger.

3.2 Den indledende visitation hos ressortmyndigheden

Det er den pågældende myndighed, der påtænker at indkøbe et it-system, der vil kunne være omfattet af lokationskravet i databeskyttelsesloven, som er ansvarlig for at rette henvendelse herom til Justitsministeriet. Forhandlingen med Justitsministeriet om, hvorvidt det pågældende it-system er omfattet af lokationskravet, sker med vedkommende minister, hvilket i praksis betyder, at det er vedkommende ressortministerium, der – når ressortministeriet vurderer, at det er relevant – skal rette henvendelse til Justitsministeriet. Underliggende myndigheder, kommuner, regioner mv. skal dermed rette henvendelse til Justitsministeriet gennem det ressortministerium, der har lovgivningskompetence inden for det dataområde, som det pågældende it-system vedrører.

Inden en offentlig myndighed gennem sit ressortministerium retter henvendelse til Justitsministeriet, skal myndigheden selv – på baggrund af denne vejledning – gøre sig en række overvejelser om, hvorvidt it-systemet vil være omfattet af lokationskravet. Det er altså op til den relevante offentlige myndighed at foretage den indledende visitation af myndighedens it-system. Den efterfølgende dialog med Justitsministeriet vil basere sig på de overvejelser, som vedkommende myndighed har gjort sig forinden.

Hvis visitationen viser, at myndigheden gennem sit ressortministerium skal rette henvendelse til Justitsministeriet, er det væsentligt, at der rettes henvendelse i god tid, eksempelvis i god tid inden it-systemet skal tages i brug eller sendes i (gen)udbud. Fra det tidspunkt, hvor Justitsministeriet har fået sagen fuldt oplyst, skal Justitsministeriet som hovedregel bruge 1-2 måneder på – i samråd med PET og FE – at vurdere et it-system. Ved komplekse it-systemer kan det være nødvendigt at bruge længere tid på at vurdere, om it-systemet er omfattet af lokationskravet i databeskyttelsesloven. Det skyldes, at det ikke mindst i forhold til komplekse it-systemer kan være en tidskrævende opgave for Justitsministeriet og relevante parter, der skal inddrages i vurderingen.

3.3 Inddeling af it-systemer i den "grønne" og den "røde" kategori

Ved myndighedens visitation af it-systemet kan systemet med fordel inddeles i to kategorier – en grøn kategori og en rød kategori – set i forhold til personoplysningernes og systemets kritikalitet for statens sikkerhed.

Hvis en myndighed vurderer, at myndighedens it-system er i den grønne kategori (se nærmere nedenfor under afsnit 3.4), vil det ikke være nødvendigt at rette henvendelse til Justitsministeriet for at få vurderet, om systemet er omfattet af lokationskravet. Myndigheden vil således kunne (men skal ikke) anvende et it-system, der ikke føres i Danmark. Myndigheden skal dog være opmærksom på at overholde krav til behandlingssikkerheden i systemet i medfør af bl.a. databeskyttelsesforordningens artikel 32, ligesom reglerne i databeskyttelsesforordningens kapitel V vil skulle overholdes ved overførsel af personoplysninger til tredjelande.

Hvis en myndighed derimod vurderer, at myndighedens it-system er i den røde kategori (se nærmere nedenfor under afsnit 3.4), skal myndigheden gennem sit ressortministerium rette henvendelse til Justitsministeriet med anmodning om, at Justitsministeriet efter forhandling med det relevante ressortministerium foretager en vurdering af, om it-systemet vil være omfattet af lokationskravet og dermed skal føres her i landet. Vurderes it-systemet at være omfattet af lokationskravet, vil it-systemet blive tilføjet til listen over it-systemer, der skal føres her i landet (jf. bilag 1 til lokationskravsbekendtgørelsen).

3.4 Spørgsmål

Når myndigheden skal vurdere, om it-systemet kan være omfattet af lokationskravet, skal følgende spørgsmål indgå i myndighedens overvejelser:

1. Kan det have alvorlige negative konsekvenser, at personoplysninger opbevares uden for dansk jurisdiktion? Det skal i den forbindelse overvejes, hvilke konsekvenser det vil have, hvis det fremmede land anvender oplysningerne mod Danmark, f.eks. offentliggør eller ændrer dem. (Se nærmere herom under afsnit 3.4.1.)

2. Hvad er konsekvenserne ved, at der ikke er adgang til personoplysningerne i it-systemet? Det skal i den forbindelse overvejes, hvor lang tid det vil tage at genskabe adgangen til oplysningerne i it-systemet, herunder om dette kan ske, inden et kritisk tidspunkt indtræder. (Se nærmere herom under afsnit 3.4.2.)

Nedenfor følger en nærmere beskrivelse af ovennævnte punkter, som myndigheden således bør overveje i forbindelse med køb, (gen)udbud el. lign. af offentlige it-systemer.

Hvis myndigheden vurderer, at besvarelsen af ét af spørgsmålene nedenfor fører til, at it-systemet er i den røde kategori, skal myndigheden gennem sit ressortministerium kontakte Justitsministeriet med henblik på at få foretaget en endelig vurdering af, om it-systemet er omfattet af lokationskravet i databeskyttelsesloven.

3.4.1 Konsekvenserne ved at personoplysningerne i it-systemet kommer i et fremmed lands varetægt og eksempelvis offentliggøres eller ændres

Under dette punkt skal myndigheden foretage en vurdering af, hvilken betydning det vil have, hvis personoplysningerne i it-systemet eksempelvis kommer i et andet lands varetægt eller mister deres integritet.

Det vil kunne pege i retning af, at et it-system er i den grønne kategori, hvis systemet kun behandler almindelige personoplysninger, herunder oplysninger om navn, adresse, alder eller indkomst. Derudover vil et it-system også være omfattet af den grønne kategori, selvom systemet indeholder en kopi af CPR-registret, medmindre der er andre forhold, der taler for, at systemet alligevel er omfattet af den røde kategori.

Det vil endvidere tale for, at et it-system som det klare udgangspunkt vil være i den grønne kategori, hvis der eksempelvis er tale om personoplysninger, der skal bruges i statistisk øjemed, selvom oplysningerne vil blive ubrugelige, hvis de mister deres integritet.

Omvendt vil det tale for, at it-systemet er i den røde kategori, hvis der i systemet behandles personoplysninger om medarbejdere, der besidder højt profilerede eller særligt betroede stillinger, eksempelvis visse sikkerhedsgodkendte ansatte i efterretningstjenesterne.

Det vil også kunne have betydning, hvor mange forskellige personoplysninger der behandles i it-systemet. Hvis der eksempelvis både behandles oplysninger om helbred (fra sundhedsplatformen), adresse (fra CPR-registret), strafbare forhold (fra Kriminalregistret) og identifikationsoplysninger (fra Skatteforvaltningens systemer), vil dette i højere grad tale for, at it-systemet kan være omfattet af den røde kategori, end hvis der i systemet udelukkende behandles oplysninger om indkomst fra eksempelvis Skatteforvaltningen.

Under dette punkt skal myndigheden endvidere vurdere, om der i it-systemet behandles personoplysninger, der kan påvirke ledende personers holdninger, eksempelvis oplysninger, der vil kunne bruges til at afpresse ministre. I så fald vil it-systemet være omfattet af den røde kategori.

Endvidere vil it-systemet være omfattet af den røde kategori, hvis der i systemet er personoplysninger, der vil kunne udnyttes på en måde, der kan vanskeliggøre afholdelse af et retmæssigt demokratisk valg.

3.4.2 Konsekvenserne ved manglende adgang til personoplysninger i it-systemet

Under dette punkt skal myndigheden foretage en vurdering af, hvilken betydning det potentielt vil have for borgere, private virksomheder og offentlige myndigheder, hvis der ikke er adgang til personoplysningerne i it-systemet, herunder hvor stor betydning tidsperioden, hvor der ikke er

adgang til oplysningerne i systemet, har. Myndigheden vil i den forbindelse bl.a. skulle vurdere nødvendigheden af, at adgangen til personoplysningerne er underlagt dansk jurisdiktion.

Når myndigheden skal vurdere konsekvenserne ved den manglende adgang til personoplysninger i it-systemet, skal de desuden være opmærksom på myndighedens samlede it-arkitektur, herunder om der eventuelt er et eller flere af myndighedens underliggende it-system(er), som har afgørende betydning for adgangen til personoplysningerne i det pågældende it-system.

Det bemærkes, at det forhold, at et it-system er omfattet af lokationskravet, ikke indebærer, at såkaldte "leverandørsystemer" eller underliggende it-systemer, der behandler personoplysninger i det omhandlede it-system, herunder bl.a. leverer, anvender eller opdaterer personoplysninger i systemet, i sig selv bliver omfattet af lokationskravet. Det er det pågældende it-system med de indeholdte personoplysninger, der omfattes af lokationskravet med det formål at sikre, at danske myndigheder har adgang til det pågældende it-system. Der henvises til eksemplerne i pkt. 3.6. om it-systemerne NemLog-in3, MitID samt Digital Post.

Det vil tale for, at it-systemet er i den røde kategori, hvis personoplysningernes karakter er væsentlige for grundlæggende offentlige institutioners funktionsmåde, eksempelvis hvis den manglende adgang til oplysningerne væsentligt vil forstyrre driften af det danske hospitalsvæsen og derved bringe liv i fare. Her vil det kunne have betydning, om myndigheden har mulighed for at fortsætte med sin drift, uanset at der ikke er adgang til personoplysningerne i it-systemet – vil myndigheden eksempelvis stadig kunne udskrive livsvigtig medicin til borgerne. Dette vil en myndighed eventuelt kunne, hvis myndigheden har fysiske dokumenter, der viser den enkelte patients medicinforbrug, eller fordi myndigheden kan finde oplysningerne i et andet it-system. Hvis dette er tilfældet, vil it-systemet som det klare udgangspunkt være omfattet af den grønne kategori. Hvis oplysninger derimod ikke kan fremskaffes andre steder, og hvis den manglende adgang f.eks. truer borgernes sundhed, vil it-systemet kunne være omfattet af den røde kategori.

Endvidere vil et it-system, der vedrører digital kommunikation med borgerne, eksempelvis kunne høre til den grønne kategori, hvis den digitale arbejdsgang i it-systemet kan erstattes af fysiske breve, eventuelt suppleret af mail- og telefonkommunikation. Hvis det omvendt vurderes, at it-systemets kommunikation ikke kan erstattes af anden kommunikationsform, vil det tale for, at systemet er omfattet af den røde kategori.

Derudover vil *tidsperioden* for den manglende adgang til personoplysninger i it-systemet kunne have betydning for vurderingen af, om it-systemet er omfattet af lokationskravet. Nogle it-systemer vil således ikke kunne undværes i blot et par dage, uden at det eksempelvis udgør en trussel mod de grundlæggende offentlige institutioners funktionsmåde, mens en manglende adgang til andre it-systemer kan vare i flere måneder, uden at det udgør en trussel mod statens sikkerhed. For eksempel vil et it-system være omfattet af den røde kategori, hvis den manglende adgang over flere dage vil have en ødelæggende effekt på væsentlige funktioner i det danske samfund.

Hvis der eksempelvis er tale om et it-system, der udelukkende behandler personoplysninger om borgere i en enkelt kommune, vil omfanget af personoplysninger tale for, at systemet er i den grønne kategori. Det forhold, at it-systemet er landsdækkende, vil dog ikke i sig selv være tilstrækkeligt til at fastslå, at systemet hører til i den røde kategori. Der skal altså som det klare udgangspunkt noget "mere til", førend et landsdækkende it-system (eller en samling af systemer, der tilsammen er landsdækkende) falder i den røde kategori.

3.5 Kryptering

Hvis ovenstående vurdering fører til, at it-systemet er omfattet af den røde kategori, f.eks. hvor omfanget af personoplysninger og karakteren af personoplysningerne kan udgøre en risiko for statens sikkerhed, hvis oplysningerne kommer en fremmed stat i hænde, vil systemet dog – efter konsultation af Justitsministeriet – kunne føres uden for Danmarks grænser, hvis der foretages en kryptering af personoplysningerne i systemet, når oplysningerne befinder sig uden for Danmark. Dekrypteringsnøglen/dekrypteringsnøglerne må i så fald alene opbevares i Danmark, og det betyder, at kryptering ikke vil kunne anvendes i alle situationer. I praksis vil det primært være backup af it-systemer, der forventes at kunne udnytte denne mulighed.

Såfremt et it-system skal anvende kryptering for at kunne placeres uden for Danmark, vil kravet til krypteringen blive fastsat i samarbejde med den nationale it-sikkerhedsmyndighed,

Det skal bemærkes, at it-systemet i en sådan situation alligevel vil kunne være omfattet af lokationskravet f.eks. på grund af tidshorisonten for, hvornår personoplysningerne igen vil kunne være tilgængelige for myndigheden, hvis driftsleverandøren i udlandet bliver utilgængelig eller pludselig ikke vil samarbejde.

3.6 Eksempler på it-systemer, der er omfattet af lokationskravet i databeskyttelsesloven

Justitsministeriet har – med bistand fra efterretningstjenesterne og efter forhandling med det relevante ressortministerium – foretaget en række vurderinger af konkrete it-systemer efter lokationskravet i databeskyttelsesloven. De it-systemer, der er vurderet omfattet af lokationskravet, fremgår af bilag 1 til lokationskravsbekendtgørelsen.

Som eksempler på it-systemer, der af justitsministeren allerede er blevet vurderet som omfattet af lokationskravet, kan Digitaliseringsstyrelsens it-systemer NemLog-in3, MitID samt Digital Post nævnes. Begrundelsen herfor er, at mængden af personoplysninger samt karakteren af personoplysninger, der behandles i systemerne, kan medføre en risiko for statens sikkerhed, hvis de opbevares uden for Danmark. Det bemærkes, at det forhold, at ovennævnte it-systemer er omfattet af lokationskravet, ikke i sig selv indebærer, at såkaldte "leverandørsystemer" til NemLog-in3, MitID samt Digital Post bliver omfattet af lokationskravet. Det er således det pågældende it-system med de indeholdte personoplysninger, der omfattes af lokationskravet med det formål at sikre, at danske myndigheder har adgang til det pågældende it-system.

Derudover kan Økonomistyrelsens it-system Statens Lønløsning nævnes som eksempel på et system, der er blevet vurderet som omfattet af lokationskravet. Statens Lønløsning beregner og anviser månedligt løn og tjenestemandspension til ca. 375.000 statslige ansatte i Danmark, Grønland og på Færøerne, ansatte i selvejersektoren og tjenestemandspensionister. Da systemet håndterer oplysninger om ansatte hos Politiet og Forsvaret, vil der kunne udledes oplysninger om statens sikkerhed, hvis oplysningerne kommer et fremmed land i hænde.

Et andet eksempel på et it-system, der er vurderet omfattet af lokationskravet, er Forsvarsministeriets it-system DeMars, som behandler oplysninger om ansatte i Forsvaret og logistikoplysninger, der har en kritisk betydning for Forsvaret. Statens sikkerhed vil kunne komme i fare, hvis oplysningerne kommer i et fremmed lands varetægt.

3.7 Eksempler på it-systemer, der ikke er omfattet af lokationskravet i databeskyttelsesloven

Som eksempel på et it-system, der af justitsministeren efter forhandling med vedkommende minister er blevet vurderet til *ikke* at være omfattet af lokationskravet, er det it-system, der opbevarer personoplysninger, som behandles af Undersøgelseskommissionen for SKAT. I den forbindelse er der blevet lagt vægt på, at systemet ikke behandler klassificerede personoplysninger, at der anvendes en stærk kryptering, og at arkitekturen i løsningen samt opbevaring af dekrypteringsnøgler vil sikre, at en driftsleverandør i udlandet ikke vil kunne få adgang til informationer, uden at disse er krypterede. Endelig vil personoplysningerne kunne genfremsendes fra den oprindelige afsender, hvis informationerne skulle være utilgængelige hos en driftsleverandør i udlandet.

Endvidere er det vurderet, at Beskæftigelsesministeriets it-system DFDG (Det fælles it-baserede datagrundlag), ikke er omfattet af lokationskravet. Systemet, der er et landsdækkende it-system, anvendes af staten, arbejdsløshedskasserne og andre aktører til forvaltning af beskæftigelsesindsatsen. Det blev lagt til grund, at det vil være til ulempe for berørte borgere, jobcentre og a-kasser, hvis systemet er utilgængeligt. Dette medførte dog ikke, at systemet var omfattet af lokationskravet i databeskyttelsesloven, da systemet ikke behandler personoplysninger, der kan true statens sikkerhed.

Som endnu et eksempel på et it-system, der af justitsministeren efter forhandling med vedkommende minister er blevet vurderet til ikke at være omfattet af lokationskravet, kan nævnes Skatteministeriets it-system eIndkomst. E-Indkomst er et fællesoffentligt grundregister med indkomstoplysninger på borgere, som løbende opdateres med indberetninger om indkomst og arbejdsomfang. E-Indkomst modtager mere end 10 millioner indberetninger på personniveau hver måned fra virksomheder og offentlige myndigheder. Systemet er essentiel for indberetningspligtige, borgere, offentlige myndigheder og andre, som har ret til at bruge oplysningerne i e-Indkomst. Systemet indeholder bl.a. oplysninger om beløb, som er omfattet af indberetningspligten efter skattekontrollovens § 7, oplysninger om timer for udbetalte sygedagpenge efter lov om sygedagpenge samt oplysninger om CPR-nr. og eventuelle andre oplysninger, der er nødvendige til identifikation af den, oplysningerne vedrører.[2] I forbindelse med vurderingen blev der dog lagt vægt på, at it-systemet ikke behandler personoplysninger, der kan true statens sikkerhed.

Derudover kan Økonomistyrelsens HR-løsning, nævnes som eksempel på et it-system, der ikke er blevet vurderet omfattet af lokationskravet. Systemet behandler oplysninger om en række statsansatte og organisationsoplysninger for de institutioner, der er omfattet af løsningen. Det drejer sig om oplysninger om bl.a. navn, adresse, stillingsbetegnelse, CPR-nr., indkomst- og pensionsforhold og i nogle tilfælde bankforhold og ansættelseskontrakter. Systemet håndterer dog ikke en række større offentlige myndigheder, herunder oplysninger om ansatte hos Politiet, Forsvaret og SKAT. I forbindelse med vurderingen blev der lagt vægt på, at systemet ikke behandler personoplysninger, der kan true statens sikkerhed.

Endelig kan nævnes, at Digitaliseringsstyrelsens it-system borger.dk er blevet vurderet til ikke at være omfattet af lokationskravet. Borger.dk er en portal, der opbevarer en kopi af en lang række

[2] For nærmere se § 3 i lov om et indkomstregister, jf. lovbekendtgørelse nr. 49 af 12. januar 2015 (indkomstregisterloven).

CPR-oplysninger fra CPR-registeret. Portalen foretager dog alene en visning af personoplysninger fra forskellige offentlige myndigheders it-systemer, men disse personoplysninger opbevares ikke i systemet. Hvis it-systemet havde været et såkaldt infrastruktursystem, der leverer og opbevarer personoplysninger ud til mange dele af den offentlige sektor, ville vurderingen af systemet kunne have været en anden.

4 Supportmedarbejdere placeret uden for Danmark

4.1 Supportmedarbejdere i EU, når it-systemet *er* omfattet af lokationskravet i databeskyttelsesloven

Hvis et it-system er omfattet af lokationskravet i databeskyttelsesloven, vil det kunne være relevant at overveje et muligt scenarie om at etablere en support-/kiggefunktion fra et andet EU-land. En sådan eventuel overvejelse skal foretages i forbindelse med, at myndigheden drøfter sagen med Justitsministeriet.

En support-/kiggefunktion vil eksempelvis kunne være mulig – selvom it-systemet er omfattet af lokationskravet – hvis det sikres, at den dataansvarlige 1) kan lukke for supportmedarbejderens (kigge)adgang til systemet og 2) sikrer sig en fintmasket autorisationsmodel for supporterens adgang til systemet, så medarbejderen ikke får uhindret adgang hertil i forbindelse med support, herunder etablering af en meget specifik søgemulighed, når supportmedarbejderen skal have adgang, eller ved at overvåge, når medarbejderen er inde i systemet, så det sikres, at medarbejderen alene yder den ønskede konkrete support. De konkrete foranstaltninger, som skal etableres, skal ske med udgangspunkt i baggrunden for, at it-systemet er omfattet af lokationskravet i databeskyttelsesloven.

4.2 Supportmedarbejdere uden for EU, når it-systemet *er* omfattet af lokationskravet i databeskyttelsesloven

Selvom et it-system er omfattet af lokationskravet, kan myndigheden potentielt overveje et muligt scenarie om at etablere en support-/kiggefunktion fra et tredjeland (det vil sige et ikke EU-land). En sådan eventuel overvejelse skal drøftes med Justitsministeriet med udgangspunkt i baggrunden for, at it-systemet er omfattet af lokationskravet i databeskyttelsesloven.

Databeskyttelsesforordningen indeholder i kapitel V regler for overførsler af personoplysninger til tredjelande.[3] Der er efter disse regler krav om, at overførsel af personoplysninger til tredjelande kun må finde sted, hvis betingelserne i dette kapitel er overholdt. Herudover skal de øvrige databeskyttelsesretlige krav iagttages.

Det er vigtigt for den dataansvarlige at være opmærksom på reglerne om tredjelandsoverførsler, idet der ikke kan etableres en support-/kiggefunktion fra et tredjeland, hvis reglerne i forordningens kapitel V ikke er overholdt. Dette gælder uanset, om det pågældende system er omfattet af lokationskravet eller ej.

[3] Afsnit VII i lov om retshåndhævende myndigheders behandling af personoplysninger.

5 Opsummering

Det er en forudsætning for lokationskravet efter databeskyttelsesloven, at it-systemet behandler personoplysninger.

Følgende punkter bør myndigheden overveje, inden myndigheden gennem sit ressortministerium retter henvendelse til Justitsministeriet:

1. Hvad er konsekvenserne ved, at personoplysninger kommer i et fremmed lands varetægt? Det skal i den forbindelse overvejes, hvilke alvorlige konsekvenser det vil have, hvis det fremmede land anvender oplysningerne mod Danmark, f.eks. offentliggør eller ændrer dem.

2. Hvad er konsekvenserne ved, at der ikke er adgang til personoplysningerne i it-systemet? Det skal i den forbindelse overvejes, hvor lang tid det vil tage at genskabe adgangen til personoplysningerne i it-systemet, herunder om dette kan ske, inden et kritisk tidspunkt indtræder.

Ved myndighedens og ressortministeriets visitation af it-systemet med udgangspunkt i ovennævnte punkter kan systemet med fordel inddeles i to kategorier – en grøn kategori og en rød kategori – set i forhold til personoplysningernes karakter og systemets kritikalitet for statens sikkerhed. Se endvidere afsnit 3.4 for en nærmere beskrivelse af de enkelte punkter.

Hvis myndigheden vurderer, at ét af spørgsmålene ovenfor fører til, at it-systemet er i den røde kategori, skal myndigheden gennem sit ressortministerium kontakte Justitsministeriet med henblik på at få foretaget en endelig vurdering af, om systemet er omfattet af lokationskravet i databeskyttelsesloven.

Hvis myndigheden vurderer, at begge spørgsmål fører til, at systemet er i den ”grønne kategori”, vil det ikke være nødvendigt at rette henvendelse til Justitsministeriet. Myndigheden vil således kunne (men skal ikke) anvende et it-system, der ikke føres i Danmark.

Dato
Juli 2020

Justitsministeriet
Slotsholmsgade 10
1216 København K

Telefon
72 26 84 00

E-mail
jm@jm.dk

ISBN
978-88-98564-35-7

Foto
Scanpix