JUSTITSMINISTERIET

Vejledning om krigsreglen

Juni 2019

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 delvist alene må *opbevares* her i landet. Denne bestemmelse er den såkaldte »krigsregel«, jf. lovens § 3, stk. 9.

Formålet med krigsreglen er at sikre, at personoplysninger i visse it-systemer opbevares på servere i Danmark af hensyn til statens sikkerhed. Krigsreglen regulerer ikke den behandling af personoplysninger (indsamling, videregivelse mv.), der i øvrigt foretages i et it-system, der er omfattet af reglen.

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 delvist kan være omfattet af anvendelsesområdet for krigsreglen. 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 delvist alene må opbevares i Danmark. Retningslinjerne vil inddrage de tværgående erfaringer, der er gjort i forbindelse med de it-systemer, der allerede *er* blevet vurderet efter krigsreglen.

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 krigsreglen 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 opbevares her i landet efter databeskyttelseslovens § 3, stk. 9, og retshåndhævelseslovens § 27, stk. 3, er derfor den samme. Denne vejledning omtaler for overblikkets skyld alene reglen i databeskyttelsesloven, men krigsreglen i retshåndhævelsesloven skal fortolkes i overensstemmelse hermed.

2. Baggrund om krigsreglen

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 muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

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 selv, der 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 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 krigsreglen.

2.2 Den moderniserede krigsregel 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 delvist 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 gamle krigsregel efter persondatalovens § 41, stk. 4.

Efter den nye udformning af krigsreglen, 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 krigsregelbekendtgørelsen.[1] Det betyder i praksis, at vedkommende ministerium, hvor det er relevant, *skal* rette henvendelse til Justitsministeriet med henblik på en vurdering af myndighedens it-system. Vurderingen vil således – i modsætning til den tidligere gældende krigsregel – ligge hos samme myndighed (Justitsministeriet), hvilket vil bidrage til en mere ensartet praksis.

[1] Bekendtgørelse nr. xx af xx 2019 om helt eller delvis opbevaring her i landet af personoplysninger, der behandles i visse it-systemer, og som føres for den offentlige forvaltning (Krigsregelbekendtgørelsen).

It-systemer sættes alene på listen, hvis det er vurderet, at det er af hensyn til statens sikkerhed, at det pågældende system fysisk skal føres på servere her i landet. I en sådan situation vil *opbevaringen* af de pågældende personoplysninger i it-systemet 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.

2.2.1 Ikke længere krav om mulighed for destruktion – den »røde knap«

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 påhvilede den dataansvarlige at træffe de foranstaltninger, som muliggjorde destruktion mv. Der var således en tankegang om, 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.

Den moderniserede krigsregel i databeskyttelsesloven indeholder ikke en forudsætning om, at et it-system, der er omfattet af bestemmelsen, skal kunne destrueres med en "rød knap". Krigsreglen er fremover i højere grad en regel, der skal sikre tilgængelighed og jurisdiktion for danske myndigheder (og den dataansvarlige selv) end en regel, der skal sikre, at it-systemet kan destrueres.

2.2.2 Behandlingssikkerhed eller statens sikkerhed?

Databeskyttelsesforordningens artikel 32 regulerer – sammen med databeskyttelsesloven – behandlingssikkerheden ved behandling af personoplysninger (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.

Databeskyttelsesforordningens artikel 32 stiller krav til behandlingssikkerheden, som den dataansvarlige skal overholde. Forordningen 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 leverandør af f.eks. en hosting-ydelse er etableret.

Den danske krigsregel er ikke en regel om *behandlingssikkerhed* (it-sikkerhed), men derimod en regel om, at visse personoplysninger af hensyn til *statens sikkerhed* skal opbevares 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.

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.

Formålet med krigsreglen er i videst muligt omfang at sikre de personoplysninger og de offentlige it-systemer, som fremmede magter kunne have en interesse i. Krigsreglen skal sikre, at konkrete it-systemer opbevares i Danmark, så danske myndigheder har adgang til de pågældende systemer og de pågældende servere. Danske myndigheder skal således – uden at skulle være afhængige af f.eks. en samarbejdsvillig leverandør fra et andet land – have adgang til bl.a. at blokere og bevogte stedet, slukke for strømmen, overvåge de personer, der arbejder i systemet eller sørge for, at visse personer ikke har adgang til systemet.

2.2.3 Nærmere om statens sikkerhed

Det er som nævnt hensynet til statens sikkerhed, der kan begrunde, at et it-system skal opbevares på servere 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 udtalt sig om begrebet i forskellige sammenhænge. Der kan f.eks. henvises til sag C-145/09, Tsakouridis, hvorefter statens 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 der i det pågældende land skal falde ind under »statens sikkerhed«, 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., og 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 navnene på ansatte i PET og 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 indeholder oplysninger, som stiller store krav til behandlingssikkerheden, vil endvidere ikke være statens sikkerhed. Se endvidere afsnit 2.2.2. Der vil omvendt kunne være tale om statens sikkerhed, hvis der er tale om *en trussel mod de grundlæggende offentlige institutioners funktionsmåde*, eller hvis manglende adgang til systemet *vil 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 statens sikkerhed

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 rådgivning fra efterretningstjenesterne. I henhold til sikkerhedscirkulæret er PET national sikkerhedsmyndighed, dog varetager Forsvarets Efterretningstjeneste (FE) funktionen inden for Forsvarsministeriets område, ligesom Forsvarets Efterretningstjeneste (FE) varetager funktionen som national IT-sikkerhedsmyndighed.

3. Hvornår skal man rette henvendelse til Justitsministeriet, og hvilke overvejelser skal myndigheden gøre sig?

3.1 Hvornår skal en offentlig myndighed rette henvendelse til Justitsministeriet?

Denne vejledning skal følges, når vedkommende minister overvejer at indkøbe et nyt it-system, en ny it-infrastruktur eller lign. 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.

Omvendt skal vejledningen ikke benyttes til at vurdere et eksisterende it-system (eller en eksisterende it-infrastruktur), som myndigheden allerede har vurderet efter persondatalovens § 41, stk. 4. Et sådant system eller infrastruktur vil først skulle vurderes efter den »nye« krigsregel i databeskyttelsesloven i de ovennævnte situationer. Det vil sige, hvis systemet eller dele heraf (gen)udbydes, outsources eller ændres på en sådan måde, at der er risiko for, at systemets kritikalitet ændres.

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

3.2 Den indledende visitation hos ressortmyndigheden

Det er den pågældende myndighed, der påtænker at indkøbe et it-system, der kan være omfattet af krigsreglen, som er ansvarlig for at rette henvendelse herom til Justitsministeriet. Forhandlingen sker med vedkommende minister, hvilket betyder, at det er vedkommende ressortministerium, der skal rette henvendelse til Justitsministeriet. Underliggende myndigheder, kommuner, regioner mv. skal således rette henvendelse til Justitsministeriet via det ressortministerium, der har lovgivningskompetence inden for det dataområde, som det pågældende it-system vedrører.

Inden en offentlig myndighed retter henvendelse til Justitsministeriet, bør myndigheden dog selv – på baggrund af denne vejledning – gøre sig en række overvejelser om, hvorvidt it-systemet vil være omfattet af krigsreglen. Det er altså den enkelte offentlige myndighed, der skal foretage den indledende visitation af myndighedens it-system. Den efterfølgende dialog med Justitsministeriet vil basere sig på de overvejelser, som ressortmyndigheden har gjort sig forinden. Et forløb uden unødvendige forsinkelser forudsætter, at Justitsministeriet bliver bekendt med alle relevante oplysninger, som kun den myndighed, som påtænker at indkøbe eller (gen)udbyde it-systemet, kan tilvejebringe.

Hvis visitationen viser, at myndigheden skal rette henvendelse til Justitsministeriet, er det væsentligt, at myndigheden retter henvendelse til Justitsministeriet i god tid, eksempelvis i god tid inden systemet skal tages i brug eller sendes i (gen)udbud. Justitsministeriet skal som hovedregel bruge 1-2 måneder på – i samråd med PET og eventuelt FE – at vurdere et system eller en infrastruktur. Ved komplekse systemer kan det være nødvendigt at bruge længere tid på at vurdere, om systemet er omfattet af krigsreglen. Det skyldes, at det ikke mindst i forhold til komplekse 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

Det bemærkes, at efter krigsreglen skal der foretages en vurdering af, om selve de (1) personoplysninger, der opbevares i et it-system, kan føre til en aktivering af krigsreglen. Som konsekvens heraf skal der efter forarbejderne også foretages en (selvstændig) vurdering af om (2) it-systemet/it-infrastrukturen (systemets kritikalitet i form af funktioner i systemet, som er samfundsvigtige) kan føre til en aktivering af krigsreglen.

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 oplysningernes 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 krigsreglen. Myndigheden vil således kunne (men skal ikke) opbevare personoplysninger i et it-system, der ikke ligger i Danmark. Myndigheden skal dog være opmærksom på de øvrige krav til behandlingssikkerheden i systemet, som skal overholdes, jf. 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 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 krigsreglen og dermed skal opbevares her i landet. Vurderes it-systemet at være omfattet af krigsreglen, vil it-systemet blive tilføjet til listen over it-systemer, der helt eller delvist alene må opbevares her i landet (jf. bilag 1 til krigsregelbekendtgørelsen).

3.4 Spørgsmål til myndigheden

Når myndigheden skal vurdere, om it-systemet kan være omfattet af krigsreglen, skal myndigheden gøre sig følgende overvejelser i forhold til både 1) borgere, 2) private virksomheder og 3) offentlige myndigheder:

1. Tværgående spørgsmål: Hvilke personoplysninger behandles i it-systemet?
2. Tværgående spørgsmål: Omfanget af personoplysninger i it-systemet.

3. Hvad er konsekvenserne ved, at it-systemet er utilgængeligt (gerne opdelt i tid og kritikalitet)?
4. Hvad er konsekvenserne ved, at personoplysninger kompromitteres, f.eks. offentliggøres eller kommer i et fremmed lands varetægt?
5. Hvad er konsekvenserne ved, at personoplysninger mister deres integritet, f.eks. ved, at der sker ændringer eller tilføjelser?
6. Hvad er konsekvenserne, hvis myndigheden ikke har styring med løsningens funktionalitet, f.eks. ved, at andre tilføjer/fjerner funktionalitet eller opdateringer forhindres?
7. Hvor lang tid vil det tage at flytte driften af it-systemet til ny driftsleverandør? *Både* hvis leverandøren er samarbejdsvillig, *og* hvis leverandøren ikke er tilgængelig/samarbejdsvillig?
8. Kan myndigheden forestille sig scenarier, hvor kompromittering/udnyttelse af løsningerne kan bruges til at påvirke holdninger/meninger eksempelvis i forbindelse med valg?

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. I forhold til punkt 1 (se afsnit 3.4.1) og punkt 2 (se afsnit 3.4.2) er der tale om tværgående spørgsmål. Det vil sige, at karakteren og omfanget af de personoplysninger, der findes i systemet, i sig selv kan begrunde en aktivering af krigsreglen, men karakteren og omfanget af oplysningerne kan også have betydning for vurderingen af de øvrige punkter.

Myndigheden kan med fordel besvare de enkelte punkter i et samlet notat eller ved at fremsende en Privacy Impact Assessment (PIA), hvis en sådan foreligger.

3.4.1 Tværgående spørgsmål: Hvilke personoplysninger behandles i it-systemet? (pkt. 1)
Krigsreglen er en regel om, at it-systemer, der indeholder *personoplysninger*, skal opbevares på servere her i landet. Da krigsreglen alene gælder for it-systemer, der indeholder personoplysninger, er det afgørende at få klarlagt, om systemet overhovedet indeholder personoplysninger. Når det er slået fast, at it-systemet indeholder personoplysninger, kan selve karakteren af personoplysningerne i systemet medføre aktivering af krigsreglen. Under dette punkt skal myndigheden derfor foretage en vurdering af, hvor følsomme de personoplysninger, som myndigheden behandler i it-systemet, er.

Det vil kunne pege i retning af, at et it-system er i den grønne kategori, hvis systemet kun behandler almindelige personoplysninger som eksempelvis oplysninger om navn, adresse, alder eller indkomst. Derudover vil et 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.

Omvendt vil det tale for, at systemet er i den røde kategori, hvis der behandles oplysninger af følsom karakter eksempelvis om medarbejdere, der besidder højt profilerede og sikkerhedsstemplede stillinger. Ligeledes vil det tale for, at systemet er i den røde kategori, hvis oplysningernes karakter er væsentlige for grundlæggende offentlige institutioners funktionsmåde eksempelvis følsomme oplysninger, der – i de forkerte hænder – vil ødelægge det danske hospitalsvæsen og bringe liv i fare.

3.4.2 Tværgående spørgsmål: Omfanget af personoplysninger i it-systemet? (pkt. 2)

Under dette punkt skal myndigheden foretage en vurdering af omfanget af de personoplysninger, som behandles i systemet.

Hvis der er tale om et it-system, der eksempelvis behandler oplysninger udelukkende om borgere i en enkelt kommune, vil omfanget af personoplysninger tale for, at systemet er i den grønne kategori. Dog skal man være opmærksom på den situation, hvor en leverandør drifter for en lang række kommuner og dermed bliver landsdækkende. Det forhold, at systemet er landsdækkende, vil ikke i sig selv være tilstrækkeligt til af fastslå, at systemet hører til den røde kategori. Der skal altså som det klare udgangspunkt noget ekstra til, førend et landsdækkende system (eller en samling af systemer, der tilsammen er landsdækkende) falder i den røde kategori.

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

3.4.3 Konsekvenserne ved, at it-systemet er utilgængeligt, opdelt i tid og kritikalitet (pkt. 3)

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

Her vil det eksempelvis have betydning, om myndigheden har mulighed for at fortsætte med sin drift, uanset at systemet er utilgængeligt. Eksempelvis om myndigheden stadig kan udskrive livsvigtig medicin til borgere. Dette vil en myndighed eventuelt kunne, fordi myndigheden har nogle (måske) fysiske dokumenter, der viser den enkelte patients medicinforbrug, eller fordi myndigheden kan finde oplysningerne i et andet it-system. Hvis dette er tilfældet, vil systemet som det klare udgangspunkt være omfattet af den grønne kategori. Hvis oplysninger derimod ikke kan skaffes andre steder, og hvis den manglende adgang f.eks. truer borgernes sundhed, vil systemet kunne være omfattet af den røde kategori.

Endvidere vil et it-system, der vedrører digital kommunikation med borgerne, eksempelvis høre til den grønne kategori, hvis den digitale arbejdsgang i it-systemet uden store omkostninger kan erstattes af f.eks. fysiske breve, eventuelt suppleret af mail- og telefonkommunikation. Omvendt vil oplysningernes følsomme karakter samt mængden af oplysninger kunne føre til, at den digitale kommunikation ikke kan erstattes med fysiske breve mv., hvilket kan føre til, at systemet af omfattet af den røde kategori.

Derudover vil tidsperioden for it-systemets tilgængelighed kunne have betydning. Nogle 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 andre systemer kan være utilgængelige 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 systemets utilgængelighed over flere dage vil have en ødelæggende effekt på væsentlige funktioner i det danske samfund.

3.4.4 Konsekvenserne ved kompromittering af personoplysningernes fortrolighed, integritet eller tilgængelighed (pkt. 4-6)

Under disse punkter skal myndigheden foretage en vurdering af, hvilken betydning det vil have, hvis personoplysninger eksempelvis kommer i et andet lands varetægt eller mister deres rigtighed, eller hvis myndigheden ikke længere kan opdatere sit it-system.

Det vil tale for, at et it-system er i den røde kategori, hvis der eksempelvis behandles oplysninger om, hvor alle Danmarks militære baser, fly, skibe, ansatte og befalingsmænd mv. er placeret, idet statens sikkerhed vil kunne komme i fare, hvis sådanne oplysninger kommer i et fremmed lands varetægt. Modsat vil det forhold, at et andet EU-land får oplysninger om alle danskeres indkomstoplysninger, ikke være tilstrækkeligt til, at et it-system er i den røde kategori.

Endvidere vil et system som det klare udgangspunkt være i den grønne kategori, hvis der eksempelvis er tale om oplysninger, der skal bruges i statistisk øjemed, selvom oplysningerne vil blive ubrugelige, hvis de mister deres integritet.

3.4.5 Tidshorisont på, hvor lang tid det vil tage at flytte driften af it-systemet til ny driftsleverandør (pkt. 7)

Under dette punkt skal myndigheden foretage en vurdering af, hvor lang tid det vil tage at flytte driften af it-systemet til ny driftsleverandør (både hvis leverandøren er samarbejdsvillig, og hvis leverandøren ikke er tilgængelig/samarbejdsvillig). Alt efter systemets øvrige karakter set i forhold til statens sikkerhed, vil en kort periode tale for, at systemet er i den grønne kategori, mens en lang periode omvendt vil tale for, at systemet kan være i den røde kategori.

3.4.6 Eventuelle scenarier, hvor kompromittering/udnyttelse af løsningerne kan bruges til at påvirke holdninger/meninger (pkt. 8)

Myndigheden skal under dette punkt bl.a. vurdere, om der i it-systemet behandles oplysninger, der kan påvirke ledende personers holdninger, eksempelvis om et system indeholder oplysninger, der vil kunne bruges til at afpresse ministre. I så fald vil systemet være omfattet af den røde kategori. Endvidere vil systemet være omfattet af den røde kategori, hvis systemet indeholder oplysninger, der vil kunne udnyttes på en måde, der kan vanskeliggøre afholdelse af et retmæssigt demokratisk valg.

3.5 Tilstrækkelig sikker kryptering

Hvis ovenstående vurdering fører til, at it-systemet på visse punkter er omfattet af den røde kategori, f.eks. hvor omfanget af personoplysninger og karakteren af personoplysningerne kan udgøre en risiko for statens sikkerhed, hvis it-systemet placeres uden for Danmarks grænser, vil systemet dog – efter konsultation af Justitsministeriet – kunne placeres uden for Danmarks grænser, hvis der foretages en sikker kryptering af personoplysningerne i systemet, når oplysningerne befinder sig uden for Danmark.

Det skal dog bemærkes, at it-systemet/it-infrastrukturen i en sådan situation alligevel vil kunne være omfattet af krigsreglen 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. Det vil eksempelvis kunne være en trussel mod de

grundlæggende offentlige institutioners funktionsmåde, hvis borgerne ikke kan få adgang til deres sundhedsoplysninger i en længere periode.

3.6 Eksempler på it-systemer, der er omfattet af krigsreglen

Justitsministeriet har – med bistand fra PET og i samarbejde med det relevante ministerium – foretaget en række vurderinger af konkrete it-systemer efter den nye krigsregel. De systemer, der er vurderet omfattet af krigsreglen, fremgår af bilag 1 til krigsregelbekendtgørelsen.

Som eksempel på et system, der af justitsministeren er blevet vurderet som omfattet af krigsreglen (efter retshåndhævelsesloven), kan nævnes Kriminalforsorgens kommende it-system Offender Management System (OMS), som skal indeholde registrering af en række almindelige og følsomme personoplysninger om afsonere i de danske fængsler. Systemet vil være grundlaget for en korrekt varetagelse af myndighedsopgaven med straffuldbyrdelse. Manglende adgang til systemet eller manglende dataintegritet vil have alvorlige konsekvenser for Kriminalforsorgens muligheder for at løse sine myndighedsopgaver og vil kunne påvirke hele Danmarks fængselsvæsen, herunder at man hverken kan indsætte eller løslade dømte personer rettidigt.

Et andet eksempel på systemer, der af justitsministeren er blevet vurderet som omfattet af krigsreglen, er systemerne Nem Log-in, MitID samt Digital Post. Mængden af informationer samt karakteren af informationerne, der behandles i systemerne, kan medføre en risiko for statens sikkerhed, hvis de placeres uden for Danmark. Endvidere vil systemernes utilgængelighed over flere dage kunne have ødelæggende effekt på væsentlige funktioner i det danske samfund, ligesom længden af den periode, som det vil tage at flytte driften til en dansk driftsleverandør, kan udgøre en trussel mod statens sikkerhed.

3.7 Eksempler på it-systemer, der ikke er omfattet af krigsreglen

Som eksempel på et it-system, der af justitsministeren efter forhandling med vedkommende minister er blevet vurderet til *ikke* at være omfattet af krigsreglen, kan nævnes Skatteministeriets e-Indkomst-system. 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 indberetningspligt 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]

Et andet eksempel på et system, der af justitsministeren efter forhandling med vedkommende minister, er blevet vurderet til *ikke* at være omfattet af krigsreglen er Moderniseringsstyrelsens HR-

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

løsning, der indeholder 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.

Endvidere er det blevet vurderet, at det system, der anvendes til behandling af personoplysninger, der behandles af Undersøgelseskommissionen for SKAT, *ikke* er omfattet af krigsreglen. I den forbindelse er der blevet lagt vægt på, at der kun behandles ikke klassificerede personoplysninger, at der anvendes en stærk kryptering, og at arkitekturen i løsningen samt opbevaring af dekrypteringsnøgler vil sikre, at en leverandør 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 leverandør i udlandet.

Endelig kan nævnes, at systemet borger.dk er blevet vurderet til *ikke* at være omfattet af krigsreglen. Systemet indeholder bl.a. en omfattende kopi af en lange række CPR-oplysninger fra CPR-registeret.

4. Systemudviklere uden for Danmark

4.1 Systemudviklere i EU, når it-systemet *er* omfattet af krigsreglen

Hvis et it-system er omfattet af krigsreglen, 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 sådan support-/kiggefunktion vil eksempelvis kunne være mulig – selvom systemet er omfattet af krigsreglen – hvis det sikres, at den dataansvarlige 1) kan lukke for supporterens (kigge)adgang til systemet og 2) sikrer sig en fintmasket autorisationsmodel for supporterens adgang til systemet, så supporteren ikke får uhindret adgang hertil i forbindelse med support, herunder etablering af en meget specifik søgemulighed, når supporteren skal have adgang, eller ved at overvåge, når supporteren er inde i systemet, så man kan sikre sig, at supporteren alene yder den ønskede konkrete support.

4.2 Systemudviklere uden for EU, når it-systemet *er* omfattet af krigsreglen

Selvom et it-system er omfattet af krigsreglen, kan myndigheden – i forbindelse med konsultationen af Justitsministeriet – potentielt overveje et muligt scenarie om at etablere en support-/kiggefunktion fra et tredjeland (det vil sige et ikke EU-land).

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.

Det er vigtigt for den dataansvarlige at være opmærksom på disse regler, 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 krigsreglen eller ej.

Hvis personoplysningerne kan overføres til tredjelande efter disse regler, vil der derudover være meget strenge krav til, hvordan personoplysningerne i øvrigt sikres i forhold til statens sikkerhed.

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

5. Opsummering

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

1. Tværgående spørgsmål: Hvilke personoplysninger behandles i it-systemet?
2. Tværgående spørgsmål: Omfanget af personoplysninger i it-systemet.
3. Hvad er konsekvenserne ved, at it-systemet er utilgængeligt (gerne opdelt i tid og kritikalitet)?
4. Hvad er konsekvenserne ved, at personoplysninger kompromitteres, f.eks. offentliggøres eller kommer i et fremmed lands varetægt?
5. Hvad er konsekvenserne ved, at personoplysninger mister deres integritet, f.eks. ved, at der sker ændringer eller tilføjelser?
6. Hvad er konsekvenserne, hvis myndigheden ikke har styring med løsningens funktionalitet, f.eks. ved, at andre tilføjer/fjerner funktionalitet eller opdateringer forhindres?
7. Hvor lang tid vil det tage at flytte driften af it-systemet til ny driftsleverandør? *Både* hvis leverandøren er samarbejdsvillig, *og* hvis leverandøren ikke er tilgængelig/samarbejdsvillig?
8. Kan myndigheden forestille sig scenarier, hvor kompromittering/udnyttelse af løsningerne kan bruges til at påvirke holdninger/meninger eksempelvis i forbindelse med valg?

Myndigheden kan med fordel besvare de enkelte punkter i et samlet notat eller ved at fremsende en Privacy Impact Assessment (PIA), hvis en sådan foreligger.

Ved myndighedens visitation af it-systemet på baggrund af 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 kriminalitet for statens sikkerhed. Se endvidere afsnit 3.4 for en nærmere beskrivelse af de enkelte punkter.

Indeholder systemet elementer fra den røde kategori, *kan* systemet være omfattet af krigsreglen. Hvis besvarelsen af et eller flere af ovennævnte punkter er omfattet af den røde kategori, skal myndigheden kontakte Justitsministeriet med henblik på at få foretaget en endelig vurdering af, om it-systemet er omfattet af krigsreglen.

Hvis myndigheden på baggrund af en samlet vurdering af ovennævnte punkter finder, at systemet er omfattet af den grønne kategori, vil det ikke være nødvendigt for myndigheden at rette henvendelse til Justitsministeriet. Myndigheden vil således kunne (men skal ikke) opbevare personoplysninger i et it-system, der ikke er placeret i Danmark.

.

Dato
Juni 2019

Justitsministeriet
Slotsholmsgade 10
1216 København K

Telefon
72 26 84 00

Email
jm@jm.dk

ISBN
978-88-98564-35-7

Foto
Scanpix