DATATILSYNET

SAS Scandinavian Airlines System Denmark
Amager Strandvej 392
2770 Kastrup
Danmark

Sendt med Digital Post

14. juni 2022

J.nr. 2022-431-0185
Dok.nr. 485343
Sagsbehandler
Poul Erik Weidick

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Anmeldelse af brud på persondatasikkerheden

Datatilsynet er gennem dagspressen – blandt andet via en artikel på DR.DK den 10. juni 2022 – blevet opmærksom på et muligt brud på persondatasikkerheden hos Scandinavian Airlines System Denmark (herefter SAS).

1. Anmodning om oplysninger

Af artikler i dagspressen, blandt andet på hjemmesiden DR.DK den 10. juni 2022 fremgår, at SAS i slutningen af maj 2022 har været ramt af en teknisk fejl i virksomhedens bookingsystem, hvilket resulterede i, at en række kunders bookinger blev annulleret. Desuagtet har en række af de kunder, hvis bookninger var blevet annulleret, konstateret, at det stadig var muligt at købe billetter til præcis samme afgange.

Af artiklen på hjemmesiden DR.DK af den 10. juni 2022 fremgår, at SAS har oplyst, at:

> *"I forbindelse med at SAS måtte aflyse i omegnen af 4.000 af sommerens flyafgange - og derfor forsøge at finde sæder til en masse passagerer - satte man ved en fejl også systemet til per automatik at fjerne overbookninger på andre fly."*

Datatilsynet kan konstatere, at tilsynet til brug for sin behandling af sagen har brug for yderligere oplysninger vedrørende de faktuelle forhold i forbindelse med hændelsen.

Datatilsynet skal derfor anmode SAS om at give en fyldestgørende beskrivelse af hændelsen, årsagen til hændelsen og hvad konsekvensen var for de registrerede. Beskrivelsen bedes udformet så omstændighederne fremstår klart også for personer, der ikke har kendskab til bookingsystemer og luftfart.

Endvidere bedes SAS besvare følgende spørgsmål enkeltvis.

A. Beskrivelse af hvordan systemet blev kodet til at udføre de pågældende ændringer.
B. Beskrivelse af hvilke test, der blev udført for at sikre, at ændringerne ville blive udført korrekt.
C. Beskrivelse af hvilke test, der blev udført for a sikre, at ændringerne var blevet udført korrekt.
D. Beskrivelse af de foranstaltninger, der var implementeret inden bruddet fandt sted, som havde til formål at hindre denne type hændelse.
E. Beskrivelse af de foranstaltninger, som der er truffet for at begrænse eventuelle skadevirkninger.

F. Om der foretages underretning af de registrerede, jf. forordningens artikel 34, og i bekræftende fald hvordan og hvornår.
G. Hvis der ikke foretages underretning af de registrerede, hvorfor.
H. Kategorier og antal berørte personer.
I. Kategorier og antal berørte registreringer af personoplysninger.
J. Beskrivelse af de konsekvenser bruddet har haft for de registrerede.
K. Beskrivelse af de sandsynlige konsekvenser bruddet vil have for de registrerede.
L. Beskrivelse af de foranstaltninger, som der er truffet eller foreslås truffet for at håndtere bruddet.
M. Hvis den dataansvarlige mangler at indsamle oplysninger om hændelsen skal Datatilsynet anmode om en status på, hvornår disse oplysninger vil være tilgængelige for den dataansvarlige.

Det bemærkes, at Datatilsynet på nuværende tidspunkt ikke kan udelukke, at oplysningerne vil kunne få betydning for bedømmelsen af en mulig overtrædelse af databeskyttelsesforordningen og databeskyttelsesloven, der kan medføre straf. Datatilsynet skal derfor gøre opmærksom på, at SAS ikke er forpligtet til at afgive oplysninger i sagen, idet der i givet fald kan være risiko for, at der afgives oplysninger om et strafbart forhold. Der henvises i den forbindelse til retssikkerhedslovens[1] § 10, der er vedlagt som bilag.

Hvis SAS vælger at besvare Datatilsynets spørgsmål, vil tilsynet betragte dette som et samtykke til at afgive oplysninger til brug for nærværende sag. De oplysninger, som SAS fremkommer med, vil derfor kunne indgå i Datatilsynets vurdering af sagen og en eventuel efterfølgende straffesag.

2. Relevante retsregler

Af databeskyttelsesforordningens artikel 5, stk. 1 fremgår, at personoplysninger skal:

a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«)
[…]
c) være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»rigtighed«)
[…]
f) behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

Stk. 2. fastslår, at den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (»ansvarlighed«).

Det fremgår af databeskyttelsesforordningens artikel 32, stk. 1, at den dataansvarlige og databehandleren, 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, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:

[1] Lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter med senere ændringer.

a) pseudonymisering og kryptering af personoplysninger
b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Ifølge artikel 32, stk. 2, tages der ved vurderingen af, hvilket sikkerhedsniveau der er passende, navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Af præambelbetragtning 75 og 76 fremgår det, at risiciene for fysiske personers rettigheder og frihedsrettigheder, af varierende sandsynlighed og alvor, kan opstå som følge af behandling af personoplysninger, der kan føre til fysisk, materiel eller immateriel skade, navnlig hvis behandlingen kan give anledning til forskelsbehandling, identitetstyveri eller -svig, finansielle tab, skade på omdømme, tab af fortrolighed for personoplysninger, der er omfattet af tavshedspligt, uautoriseret ophævelse af pseudonymisering eller andre betydelige økonomiske eller sociale konsekvenser. […]

Risikoens sandsynlighed og alvor for så vidt angår den registreredes rettigheder og frihedsrettigheder bør bestemmes med henvisning til behandlingens karakter, omfang, sammenhæng og formål. Risikoen bør evalueres på grundlag af en objektiv vurdering, hvorved det fastslås, om databehandlingsaktiviteter indebærer en risiko eller en høj risiko.

Ved brud på persondatasikkerheden anmelder den dataansvarlige ifølge forordningens artikel 33, stk. 1, uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, bruddet på persondatasikkerheden til den tilsynsmyndighed, som er kompetent i overensstemmelse med artikel 55, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Foretages anmeldelsen til tilsynsmyndigheden ikke inden for 72 timer, ledsages den af en begrundelse for forsinkelsen.

Ifølge forordningens artikel 33, stk. 5, skal den dataansvarlige dokumentere alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger. Denne dokumentation skal kunne sætte tilsynsmyndigheden i stand til at kontrollere, at denne artikel er overholdt.

Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter den dataansvarlige uden unødig forsinkelse den registrerede om bruddet på persondatasikkerheden. Det følger af forordningens artikel 34, stk. 1.

Stk. 2 fastlår, at underretningen af den registrerede i henhold til denne artikels stk. 1 skal i et klart og forståeligt sprog beskrive karakteren af bruddet på persondatasikkerheden og mindst indeholde de oplysninger og foranstaltninger, der er omhandlet i artikel 33, stk. 3, litra b), c) og d).

Ifølge stk. 3, kan underretning efter stk. 1, undlades, hvis en af følgende betingelser er opfyldt:

a) den dataansvarlige har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, som f.eks. kryptering
b) den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registreredes rettigheder og frihedsrettigheder som omhandlet i stk. 1 sandsynligvis ikke længere er reel
c) det vil kræve en uforholdsmæssig indsats. I et sådant tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

3. Afsluttende bemærkninger

SAS bedes snarest muligt og **senest den 21. juni 2022** bekræfte modtagelsen af dette brev.

Besvarelsen bedes sendt til Datatilsynet **senest den 28. juni 2022**.

Hvis ovenstående giver anledning til spørgsmål, er SAS velkommen til at kontakte undertegnede telefonisk på 2949 3252 eller via mail på pew@datatilsynet.dk.

Med venlig hilsen

Poul Erik Weidick

Bilag: Lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter (uddrag)

Bilag

Lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter (uddrag).

§ 9. Hvis en enkeltperson eller juridisk person med rimelig grund mistænkes for at have begået en strafbar lovovertrædelse, kan tvangsindgreb over for den mistænkte med henblik på at tilvejebringe oplysninger om det eller de forhold, som mistanken omfatter, alene gennemføres efter reglerne i retsplejeloven om strafferetsplejen.

Stk. 2. Reglen i stk.1 gælder ikke, hvis tvangsindgrebet gennemføres med henblik på at tilvejebringe oplysninger til brug for behandlingen af andre spørgsmål end fastsættelse af straf.

Stk. 3. Reglerne i stk. 1 og 2 finder tilsvarende anvendelse, hvis der i sagen rettes et tvangsindgreb mod andre end den mistænkte.

Stk. 4. Den mistænkte kan meddele samtykke til fravigelse af stk. 1 og 3. Samtykke skal være skriftligt og skal meddeles på et frivilligt, specifikt og informeret grundlag. Et samtykke kan til enhver tid tilbagekaldes. Meddeler den mistænkte samtykke til fravigelse af stk. 1 og 3, finder reglerne i §§ 2-8 tilsvarende anvendelse ved de i § 1, stk. 1, nævnte tvangsindgreb.

§ 10. Hvis der er konkret mistanke om, at en enkeltperson eller juridisk person har begået en lovovertrædelse, der kan medføre straf, gælder bestemmelser i lovgivningen m.v. om pligt til at meddele oplysninger til myndigheden ikke i forhold til den mistænkte, medmindre det kan udelukkes, at de oplysninger, som søges tilvejebragt, kan have betydning for bedømmelsen af den formodede lovovertrædelse.

Stk. 2. I forhold til andre end den mistænkte gælder bestemmelser i lovgivningen m.v. om pligt til at meddele oplysninger, i det omfang oplysningerne søges tilvejebragt til brug for behandlingen af andre spørgsmål end fastsættelse af straf.

Stk. 3. En myndighed skal vejlede den mistænkte om, at vedkommende ikke har pligt til at meddele oplysninger, som kan have betydning for bedømmelsen af den formodede lovovertrædelse. Hvis den mistænkte meddeler samtykke til at afgive oplysninger, finder reglerne i § 9, stk. 4, 2. og 3. pkt., tilsvarende anvendelse.

Stk. 4. Den mistænkte kan meddele samtykke til anvendelse af en oplysningspligt over for andre med henblik på at tilvejebringe oplysninger til brug for en straffesag mod den mistænkte. Reglerne i § 9, stk. 4, 2. og 3. pkt., finder tilsvarende anvendelse.