UDVIKLINGS OG FORENKLINGS STYRELSEN

**Notat**

7. februar 2020

# Redegørelse om utilsigtet afsendelse af cpr-nr.

Som led i Udviklings- og Forenklingsstyrelsens løbende styrings- og tilsynsaktiviteter over for Skatteforvaltningens it-leverandører har styrelsen identificeret, at der utilsigtet er afsendt cpr-numre fra 'TastSelv Borger' i 2015-2020. I forbindelse med styrelsens undersøgelse af denne hændelse hos it-virksomheden DXC Technology, der varetager drift og vedligeholdelse af det pågældende system, er yderligere utilsigtede overførsler konstateret. Hændelserne skyldes samme tekniske fejl.

Udviklings- og Forenklingsstyrelsen har anmodet Kammeradvokaten vurdere, hvorvidt der er grundlag for at rejse krav mod DXC med henblik på at sikre staten erstatning for de udgifter, der måtte følge af databruddet, samt med henblik på at kræve et forholdsmæssigt afslag på Skatteforvaltningens betaling for ydelser relateret til systemet.

*Hændelsernes karakter og omfang*
DXC har oplyst over for Udviklings- og Forenklingsstyrelsen, at den første hændelse, som blev konstateret den 21. januar 2020, er sket, når en borger har logget på 'TastSelv Borger' og klikket på "Ret kontaktoplysninger" for at checke eller rette sine kontaktoplysninger. Hermed har borgerens browser kaldt en standardfunktion hos 'Google Hosted Libraries', som hjælper med at øge hastigheden på websiden, så brugeroplevelsen bliver bedre. Kaldet har i sig selv kun taget få millisekunder.

Når funktionen er blevet kaldt, er borgerens cpr-nummer ved en fejl blevet sendt med som en del af URL'en til Google. Der er i perioden fra den 2. februar 2015 til den 24. januar 2020 samlet set afsendt cpr-numre for ca. 1,26 mio. borgere, der en eller flere gange har rettet deres kontaktinformation.

URL'en er afsendt via en krypteret forbindelse, og som en integreret del af modtagerprocessen slettes al identificerbar information af Google og er således hverken blevet logget eller lagret hos Google. Dette er skriftligt bekræftet af Google. Det vurderes på den baggrund, at der ikke har været en fare for misbrug af borgernes cpr-numre. DXC har desuden bekræftet over for Udviklings- og Forenklingsstyrelsen, at der ikke længere utilsigtet afsendes cpr-numre til Google.

Hændelsen relaterer sig til udformningen af systemet bag 'TastSelv Borger', som har gjort, at cpr-nummeret indgik i URL´en ved kald af "Ret kontaktoplysninger". Udformningen

er sket tilbage i tiden – formentlig helt fra 'TastSelv Borger' blev udviklet, hvor det ikke var unormalt at anvende cpr-nummeret i URL'er. Over årene er denne udformning af systemerne ændret, men ved en fejl er det ikke ændret i "Ret kontaktoplysninger".

En utilsigtet konsekvens af den identificerede fejl er, at såfremt en borger har anvendt en delecomputer, så vil browserhistorikken være tilgængelig for den næste bruger af computeren, hvis browserhistorikken ikke er slettet, inden computeren forlades.

Der er iværksat en afdækning af afledte konsekvenser af den konstaterede fejl. Det er i den forbindelse konstateret, at der tillige er overført cpr-numre til it-virksomheden Adobe samt til it-virksomheden MaxCDN, hvis software anvendes til at forbedre Skatteforvaltningens websites og indberetningsløsninger. Også i disse tilfælde er det sket utilsigtet, når borgeren har kaldt "Ret kontaktoplysninger" på 'TastSelv Borger'. DXC har oplyst, at oplysningerne er sendt krypteret til de to virksomheder.

DXC har oplyst, at der én eller flere gange er overført cpr-numre for 1.334 borgere til Adobe i perioden 29. januar 2020 til 1. februar 2020. Adobe har modtaget oplysningerne på et sikret datalager og har over for Udviklings- og Forenklingsstyrelsen bekræftet, at de overførte cpr-numre er blevet slettet. DXC har ligeledes bekræftet over for Udviklings- og Forenklingsstyrelsen, at der ikke længere overføres cpr-numre til Adobe.

DXC har ligeledes oplyst, at der én eller flere gange er overført cpr-numre for 4.735 borgere til MaxCDN – hovedsageligt i perioden 2015-2016. Denne fejl er konstateret den 6. februar 2020 og er fortsat under kortlægning. Udviklings- og Forenklingsstyrelsen vil, når kortlægningen er tilendebragt, træffe de nødvendige foranstaltninger.

Det er endvidere oplyst, at der i de konstaterede hændelser ikke er overført andre personoplysninger som løn, skatteforhold eller lignende til it-leverandører, som ikke er omfattet af en databehandleraftale.

Udviklings- og Forenklingsstyrelsen har bedt DXC undersøge og bekræfte, at der ikke i andre systemer og applikationer, som DXC varetager driften af for Skatteforvaltningen, fortsat foretages utilsigtet afsendelse af cpr-numre. Dette har DXC bekræftet.

*Konsekvenser af sagen*
Udviklings- og Forenklingsstyrelsen har anmeldt persondatahændelserne til Datatilsynet henholdsvis den 24. januar, 31. januar og den 6. februar 2020. Anmeldelserne er sket i overensstemmelse med gældende regler, idet der formelt er tale om brud på persondatasikkerheden. Da bruddene relateret til Google og Adobe ikke har medført risiko for misbrug af borgernes cpr-numre, er det Udviklings- og Forenklingsstyrelsens vurdering på det foreliggende grundlag, at der ikke er behov for at orientere den enkelte borger direkte.

Udviklings- og Forenklingsstyrelsen har anmodet Kammeradvokaten vurdere, hvorvidt der er grundlag for at rejse krav mod DXC med henblik på at sikre staten erstatning for

de udgifter, der måtte følge af databruddet, samt med henblik på at kræve et forholdsmæssigt afslag på Skatteforvaltningens betaling for ydelser relateret til systemet.

Udviklings- og Forenklingsstyrelsen vil i den kommende tid tage initiativ til at gennemgå borger- og virksomhedsrettede it-systemer hos Skatteforvaltningens øvrige it-leverandører med henblik på at sikre, at samme type fejl ikke også optræder i disse systemer.

Udviklings- og Forenklingsstyrelsen vil endvidere skærpe tilsynet med alle Skatteforvaltningens it-leverandører på flere områder, herunder stille krav om øget kode- og softwarekvalitet og strammere opfølgning på og tilsyn med de såkaldte databehandleraftaler, der ligger til grund for, at eksterne it-leverandører må håndtere persondata.

Udviklings- og Forenklingsstyrelsen vil give en status på forholdene senest 1. marts 2020.

*Baggrund om Skatteforvaltningen som dataansvarlig myndighed*
Skatteforvaltningen behandler mange forskellige personoplysninger som led i sine myndighedsopgaver og fastsætter i den forbindelse formål og hjælpemidler ved de forskellige behandlinger. Dermed er Skatteforvaltningen dataansvarlig myndighed, jf. art. 4, nr. 7, i persondataforordningen.

At være dataansvarlig indebærer bl.a., at Skatteforvaltningen skal sikre, at der sker tilstrækkelig beskyttelse af personoplysninger, herunder at personoplysninger behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til borgerne, jf. forordningens art. 5.

Som led i myndighedsopgaver samarbejder Skatteforvaltningen med mange forskellige eksterne leverandører om drift, udvikling og analyse af it-systemer og dataløsninger. I det omfang en leverandør behandler personoplysninger på Skatteforvaltningens vegne, vil leverandøren være databehandler for Skatteforvaltningen. Skatteforvaltningen er dermed forpligtet til at instruere leverandører i, hvordan personoplysninger må behandles, og hvilke krav leverandørerne skal overholde i forhold til bl.a. behandlingssikkerheder, jf. forordningens art. 28.

I Skatteforvaltningen er det Udviklings- og Forenklingsstyrelsen, der forvalter dataansvaret i forbindelse med anvendelse af it-systemer. Udviklings- og Forenklingsstyrelsen indgår skriftlige databehandleraftaler med leverandørerne for at regulere, hvordan leverandøren må behandle oplysninger på Skatteforvaltningens vegne og til hvilke formål, jf. forordningens art. 28. Den seneste databehandleraftale, som Udviklings- og Forenklingsstyrelsen har indgået med DXC, er fra 17. december 2018.

*Baggrund om styring og tilsynsaktiviteter over for it-leverandører*
For at sikre forsvarlig drift af Skatteforvaltningens it-systemer og varetage opgaven som dataansvarlig myndighed gennemfører Udviklings- og Forenklingsstyrelsen en række styrings- og tilsynsaktiviteter over for eksterne it-leverandører. Det har ligeledes gjort sig gældende i forholdet til DXC som databehandler på 'TastSelv Borger'.

Styrings- og tilsynsaktiviteter gennemføres ikke kun med udgangspunkt i databeskyttelsesreglerne, men også med udgangspunkt i andre hensyn, herunder sikring af at leverandøren opfylder kontraktlige bestemmelser.

Konkrete styrings- og tilsynsaktiviteter omfatter blandt andet, at Udviklings- og Forenklingsstyrelsen løbende indhenter sikkerhedsrapportering fra leverandørerne og 3. parts revisorerklæringer samt gennemfører teknisk scanning af it-sikkerhedsmæssige sårbarheder og huller. Dertil afholdes månedlige opfølgningsmøder med leverandørerne med henblik på opfølgning på driftsmæssige og sikkerhedsmæssige forhold.

Den konkrete fejl, der ligger bag alle hændelserne, er identificeret som led i scanning og applikationstest af 'TastSelv Borger', der blev suppleret med manuelle kontroller med henblik på at identificere sårbarheder og sikkerhedssvagheder. Testen er gennemført af et anerkendt eksternt sikkerhedsfirma, der leverer forebyggende sikkerhedsløsninger.