UDVIKLINGS OG FORENKLINGS STYRELSEN

Notat

19. juni 2020
J.nr. 2020-299

Opfølgning på sag om utilsigtet afsendelse af cpr-numre

Dette notat er en opfølgning på Udviklings- og Forenklingsstyrelsens redegørelse af 7. februar 2020 om en konkret sag om utilsigtet afsendelse af cpr-numre.

På baggrund af den konkrete sag om en it-leverandørs utilsigtede afsendelse af cpr-numre til de amerikanske virksomheder Google, Adobe og MaxCDN iværksatte Udviklings- og Forenklingsstyrelsen en række undersøgelser og initiativer for at afdække omfanget af sagen og for at få rettet den fejl i "TastSelv Borger", som var årsag til den utilsigtede afsendelse.

I den nævnte redegørelse blev hændelsernes karakter, omfang og konsekvenser nærmere beskrevet, for så vidt angik Google og Adobe, ligesom det blev beskrevet, at der ikke længere blev afsendt cpr-numre, idet fejlen var blevet rettet.

Udviklings- og Forenklingsstyrelsen oplyste, at man ville følge op på redegørelsen, når den del, der vedrørte MaxCDN, var fuldt udredt. Samtidig ville styrelsen redegøre for en gennemgang af styrelsens øvrige relevante systemer for at sikre, at der ikke var fejl af samme karakter dér.

Nedenfor gives en status på de yderligere undersøgelser og initiativer, som styrelsen har iværksat i relation til MaxCDN og i forhold til styrelsens øvrige relevante systemer siden afgivelsen af redegørelsen.

Den nærmere udredning i forhold til MaxCDN
Der er siden redegørelsen indhentet yderligere oplysninger om videregivelsen af cpr-numre til MaxCDN, herunder bl.a. om hændelsens tidsmæssige udstrækning, antallet af berørte borgere samt om sletning af oplysningerne.

Indledningsvis bemærkes, at MaxCDNs software anvendes til at forbedre Skatteforvaltningens websites og indberetningsløsninger.

Den utilsigtede videregivelse til MaxCDN blev opdaget af leverandøren den 29. januar 2020 i forbindelse med analyser foranlediget af den tilsvarende Google problematik. På

dette tidspunkt var den grundlæggende fejl med personnumre i URL allerede under udbedring. Det er oplyst, at videregivelsen var sket mellem den 2. februar 2015 og den 2. februar 2020, hvor fejlen blev rettet, og videregivelsen blev stoppet.

Leverandørens undersøgelser viste indledningsvist, at 4.735 cpr-numre utilsigtet var videregivet til MaxCDN, jf. redegørelsen af 7. februar 2020. En fintælling har imidlertid vist, at der er videregivet cpr-numre til MaxCDN vedrørende 3.315 borgere. Dette er således en nedjustering på ca. 1.000 borgere i forhold til det tal, der fremgår af redegørelsen.

MaxCDN har videre oplyst, at cpr-numrene blev modtaget og slettet efter syv dage i henhold til MaxCDNs interne procedure.

Det er endelig oplyst fra MaxCDNs side, at det – for så vidt angår personoplysninger – alene er cpr-nummeret, som blev videregivet til MaxCDN. Der blev således ikke videregivet andre personoplysninger som navn, adresse, løn, skatteforhold eller lignende i samme tekstfelt som cpr-nummeret til MaxCDN. IP-oplysninger er dog fulgt med.

Det er Udviklings- og Forenklingsstyrelsens vurdering, at der ikke er behov for at orientere den enkelte borger direkte, da videregivelsen af cpr-numre til MaxCDN på baggrund af de nu foreliggende oplysninger ikke har medført høj risiko for misbrug af borgernes cpr-numre.

Styrelsen har dog fundet grundlag for at informere om hændelsen i sin pressemeddelelse af 7. februar 2020 med mulighed for, at borgerne kan kontakte styrelsen og få yderligere information om, hvorvidt de er berørt.

Gennemgang af andre leverandørers systemer
Udviklings- og Forenklingsstyrelsen har på baggrund af sagen fundet anledning til at få gennemført undersøgelser af alle andre relevante borger- og virksomhedsrettede it-systemer hos sine it-leverandører med henblik på at sikre, at samme type fejl ikke også optræder i disse systemer.

De pågældende leverandører har derfor gennemgået de relevante systemer, og på baggrund af de hidtil gennemførte undersøgelser har leverandørerne oplyst skriftligt, at der ikke er noget, som peger på, at der skulle være yderligere tilsvarende fejl.

Helt konkret har følgende seks leverandører gennemgået i alt 24 borger- og virksomhedsrettede systemer, som de drifter og vedligeholder på vegne af Udviklings- og Forenklingsstyrelsen. Det er tale om internet-vendte systemer, dvs. systemer, der kan tilgås af borgere og virksomheder. Disse systemer fremgår af nedenstående tabel 1.

Tabel 1 – Gennemgåede it-systemer, der kan tilgås af borgere og virksomheder

Leverandør	System
CGI	Eksport
	e-Moms
	Import
	ICS
	Manifest
DXC	DCS
	DCS-Login Gateway
	DKvies
	e-Kapital
	e-Skat data
	OSM
	TastSelv-Erhverv
	TastSelv- Årsopgørelse
European Dynamics	EMCS
IBM	e-indkomst
	LetLøn
KMD	AogD
	Forskud
	Skattekontoen
	TastSelv
Netcompany	BBR
	DIAS
	DMR
	PSRM

Yderligere tiltag fra Udviklings- og Forenklingsstyrelsens side
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.

Udviklings- og Forenklingsstyrelsen skærper i forlængelse af sagen herudover tilsynet med alle Skatteforvaltningens it-leverandører på en række områder, herunder stiller 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.

Styrelsen vil som led i sit tilsyn også løbende monitorere eventuelle fejl af anden karakter, som involverer personoplysninger.

Udviklings- og Forenklingsstyrelsens opfølgning over for Datatilsynet
Udviklings- og Forenklingsstyrelsen har indberettet sagen med de utilsigtet afsendte cpr-numre til Datatilsynet, som fører tilsyn med, at de persondataretlige regler overholdes.

I forlængelse heraf har tilsynet den 17. februar 2020 stillet en række opklarende spørgsmål, der primært vedrører sagen om MaxCDN, dog med nogle enkelte spørgsmål vedrørende afsendelsen til Google og Adobe.

Styrelsen har besvaret Datatilsynets spørgsmål ved brev af 25. marts 2020. Brevet er vedlagt som bilag 1.

I det følgende gengives svarerne på tilsynets spørgsmål kort.

Datatilsynets første spørgsmål omhandler, om der er indgået en databehandleraftale med Adobe, og de efterspørger en mail fra Google af 27. januar 2020. Udviklings- og Forenklingsstyrelsen har fremsendt dokumentation for både databehandleraftalen med Adobe og mailen fra Google i svaret til tilsynet.

Det næste spørgsmål handler om, hvorvidt der har været andre oplysninger i URL'en, herunder borgerens IP-adresse eller andet, som indirekte kunne forbinde borgerens personnummer i URL'en med borgeren. Svaret på dette spørgsmål er, at der ikke er blevet videregivet personoplysninger i form af f.eks. adresseoplysninger sammen med personnummeret i URL'en, men at IP-adressen er fulgt med.

De efterfølgende spørgsmål vedrører MaxCDN, herunder startdato for overførslen af personnumre til MaxCDN, hvilke hændelser der skete på starttidspunktet for overførslen af personnumre, om overførslen til MaxCDN var krypteret, og hvilken form for oprydning der skete hos MaxCDN. Det fremgår af besvarelsen, at starttidspunktet for overførslen var den 2. februar 2015, hvor man begyndte at benytte MaxCDNs rutiner i "TastSelv Borger"-systemet, at overførslen af personnumre til MaxCDN er sket via en krypteret forbindelse, en såkaldt https forbindelse, og at oprydningen hos MaxCDN har bestået i, at de modtagne personnumre er blevet slettet efter syv dage i overensstemmelse med deres faste praksis.

Datatilsynet spørger yderligere ind til, om der er indgået en databehandleraftale med MaxCDN, hvortil Udviklings og Forenklingsstyrelsen svarer, at der ikke er indgået en databehandleraftale mellem styrelsen og MaxCDN, idet MaxCDN er underleverandør til leverandøren. Leverandøren har desuden oplyst til Udviklings og Forenklingsstyrelsen, at de ikke vurderer, at der er et behov for en databehandleraftale mellem dem og MaxCDN.

Datatilsynets sidste spørgsmål retter sig mod underretning af de berørte borgere. Svaret til tilsynet er, at de berørte borgere ikke er blevet underrettet enkeltvis, men at der er udsendt en pressemeddelelse med angivelse af, hvor borgeren kan rette henvendelse for at få yderligere information.

Tilsynet har ikke på nuværende tidspunkt oplyst den forventede sagsbehandlingstid, og Udviklings- og Forenklingsstyrelsen afventer således fortsat Datatilsynets afgørelse.

Udviklings- og Forenklingsstyrelsens opfølgning over for leverandøren vedrørende de aftalte ydelser
Det fremgår af redegørelsen af 7. februar 2020, at Udviklings- og Forenklingsstyrelsen har bedt Kammeradvokaten vurdere, hvorvidt der er grundlag for at rejse krav mod leverandøren med henblik på at sikre staten erstatning for de udgifter, der måtte følge af sagen, samt med henblik på at kræve et forholdsmæssigt afslag på Skatteforvaltningens betaling for ydelser relateret til "TastSelv – Borger" systemet.

Kammeradvokaten har den 29. maj 2020 afgivet sin endelige udtalelse om, hvorvidt Udviklings- og Forenklingsstyrelsen kan rejse et krav mod leverandøren som følge af den konstaterede fejl i "TastSelv-Borger" systemet og den utilsigtede overførsel af cpr-numre.

Det er Kammeradvokatens vurdering, at leverandøren som udgangspunkt har handlet ansvarspådragende. Styrelsen vil kunne kræve halvdelen af sagens omkostninger dækket af leverandøren samt evt. et forholdsmæssigt nedslag i den betaling, Skatteforvaltningen har erlagt for driften af "TastSelv-Borger".

På denne baggrund vil Kammeradvokaten nu på styrelsens vegne påbegynde forhandlinger med leverandøren.

Sagens afslutning
Som nærmere beskrevet ovenfor har Udviklings- og Forenklingsstyrelsen nu fået afdækket de relevante aspekter af sagen. De pågældende leverandører har således gennemgået deres borger- og virksomhedsrettede systemer, og på baggrund af de hidtil gennemførte undersøgelser har leverandørerne oplyst, at der ikke er noget, som peger på, at der skulle være yderligere tilsvarende fejl.

Herudover har sagen givet anledning til, at styrelsen skærper sit tilsyn med alle Skatteforvaltningens it-leverandører på en række områder. Dette skærpede tilsyn vil således ligge ud over styrelsens faste praksis med gennemførelse af en række højt prioriterede styrings- og tilsynsaktiviteter over for eksterne it-leverandører.