Indenrigs- og Sundhedsministeriet

Dato: 1. februar 2023
Kontor: CPR-kontoret
J.nr.: 2023 - 597

Standardvilkår for offentlige myndigheders adgang til CPR på Datafordeleren

Datafordeleren er databehandler for Indenrigs- og Sundhedsministeriet ved ministeriets videregivelse af oplysninger fra CPR via Datafordeleren.

1 Indledning

Efter § 32, stk. 1, i lov om Det Centrale Personregister kan en offentlig myndighed, der har brug for oplysninger, som er registreret i CPR, indhente oplysningerne i CPR.

Efter § 32, stk. 2, fastsætter ministeriet vilkårene, herunder om sikkerhedsforanstaltninger og betalingen, for videregivelse af oplysninger efter stk. 1.

Det er en betingelse for levering af personoplysninger, at myndigheden efter databeskyttelsesforordningen og databeskyttelsesloven er berettiget til at behandle oplysningerne.

Den, der forsætligt eller ved grov uagtsomhed overtræder nærværende vilkår, straffes med bøde, medmindre højere straf er forskyldt efter den øvrige lovgivning, jf. CPR-lovens § 57, stk. 1, nr. 4.

I øvrigt reguleres forhold vedrørende behandlingen af oplysninger fra CPR, som ikke er reguleret af nærværende vilkår, af CPR-loven, databeskyttelsesforordningen og databeskyttelsesloven og bestemmelser fastsat i medfør heraf.

Ændringer i nærværende vilkår samt løbende information om driftsforhold offentliggøres alene via nyhedsabonnement på www.datafordeler.dk.

2 Oprettelse og ændring af kundeforhold

Anmodning om adgang til CPR på Datafordeleren inden for rammerne af disse vilkår sker ved henvendelse fra myndigheden (Kunden) til Datafordeleren, via Datafordeler.dk.

Ved behandlingen af en sådan henvendelse tager CPR-kontoret stilling til, hvilke data i CPR myndigheden vil blive givet adgang til. Dette sker for at sikre, at leverancen fra CPR ikke vil omfatte flere personer eller flere oplysninger om disse end nødvendigt for den konkrete opgave, og at leverancen er i overensstemmelse med CPR-loven og databeskyttelsesforordningen og databeskyttelsesloven. Leveringstiden afhænger af det valgte produkt og opgavens omfang.

3 Regler for autorisation og adgangskontrol

Myndigheden skal udpege en sikkerhedsansvarlig, der er ansvarlig for overholdelse af nærværende vilkår, samt for:

- at der lokalt er fastsat nærmere interne bestemmelser om sikkerhedsforanstaltninger
- at kun de medarbejdere, for hvem det er nødvendigt at benytte adgangen til CPR i forbindelse med udførelsen af deres arbejde, autoriseres hertil, og at medarbejderne ikke autoriseres til anvendelser, som de ikke har behov for,
- at medarbejderne er oplært i anvendelsen af adgangen til CPR, og
- at medarbejderne har kendskab til de interne bestemmelser om sikkerhedsforanstaltninger samt nærværende vilkår.

Ved online adgang til CPR via Datafordeleren udstedes en autorisation af CPR-kontoret, der effektueres af Datafordeler-operatøren, i form af godkendelse af en eller flere af myndighedens tilknyttede medarbejdersignaturer.

Ved system til system adgang til Datafordeleren benyttes den autoriserede medarbejdersignatur til anvendelse i myndighedens program. Den sikkerhedsansvarlige skal sikre, at de anvendte signaturer til enhver tid tilhører en medarbejder, der har ansættelse i myndigheden. Den enkelte medarbejder anvender den autorisation, som medarbejderen er tildelt af myndigheden til brug i det myndighedssystem, der benytter system til system adgang til CPR-oplysninger fra Datafordeleren.

Den sikkerhedsansvarlige skal føre en fortegnelse over de medarbejdere og eventuelle system til system programmer, der har fået autorisation, med angivelse af tidspunkt for autorisationens påbegyndelse og senere ophør.

Medarbejderne må, ved adgang til CPR's tjenester samt øvrige produkter fra Datafordeleren, og anvendelsen af oplysningerne herfra i afledte systemer, kun skaffe sig adgang til oplysninger, som er nødvendige for at kunne udføre pålagte funktioner og opgaver, dvs. oplysninger, som naturligt indgår i sagsbehandlingen.

Enhver anvendelse af CPR til privat brug er strengt forbudt.

Medarbejdere må ikke forlade deres arbejdsstation eller lokalet uden at logge sig ud af Datafordeleren, CPR- systemet eller af det system, der har adgang til CPR oplysninger. Medarbejderne kan dog i stedet låse arbejdsstationen på en måde, hvor genåbning kræver indtastning af et personligt kendeord.

4 Myndighedens kontrol af autorisationer til CPR og opslag i CPR

Myndigheden skal tilrettelægge interne bestemmelser for en løbende og passende kontrol af Myn-

dighedens modtagende autorisationer til CPR samt myndighedens søgninger og opslag via CPR's produkter på Datafordeleren. Myndighedens bestemmelser skal afspejle de faktiske forhold og skal løbende opdateres, dog mindst en gang årligt.

Myndigheden skal på CPR-kontorets anmodning kunne fremsende kopi af de interne bestemmelser samt dokumentation for de gennemførte kontroller.

Myndighedens interne bestemmelser for den løbende kontrol skal tage højde for, at myndigheden skal gennemføre en kontrol med myndighedens autorisationer til CPR mindst hver tredje måned.

Alle søgninger og opslag registreres hos Datafordeleren. Registreringen sker i Datafordelerens log-point løsning og indeholder oplysning om anvender (VID, MID, VOCES og MOCES), transaktionstype (tjeneste, fildownload, etc.), tidspunkt samt hvilke oplysninger, der er forespurgt på eller søgt på hos Datafordeleren. Hvis myndigheden anvender en system til system adgang, skal myndigheden foretage en registrering af den enkelte brugers transaktioner i myndighedens system.

Via Datafordeleren har de af myndigheden udpegede brugere adgang til henholdsvis 1) en logsøgning, der muliggør generering af en udskrift med udvalgte eller alle søgninger og opslag foretaget af myndighedens egne brugere (logsøgning), samt 2) en udskrift indeholdende statistik over anvendelsen (transaktionsstatistik). Statistikken angiver for hver bruger, hvilke transaktionstyper den pågældende bruger har anvendt, samt antallet af gange den enkelte transaktionstype har været anvendt.

Myndighedens interne bestemmelser for den løbende kontrol skal omfatte en kontrol baseret på hhv. logsøgningen og transaktionsstatistikken. Kontrollen skal kunne afdække om myndighedens medarbejdere anvender autorisationer på Datafordeleren i overensstemmelse med nærværende vilkår samt databeskyttelsesforordningen og databeskyttelsesloven. Kontrollen skal gennemføres med højst tre måneders mellemrum.

Ved anvendelse af system til system adgang, skal myndigheden selv udarbejde tilsvarende udskrifter og gennemføre en tilsvarende løbende kontrol.

Hvis myndigheden har mistanke om misbrug af adgangen til CPR, skal myndigheden foretage kontrol heraf. En sådan kontrol kan ikke træde i stedet for den løbende kontrol.

5 Krav til datakommunikationsadgang

Her henvises til Datafordelerens vilkår, der bl.a. omhandler krav til data-adgange, krav til krypteringsteknologier, sikre filoverførsler, forbindelsesteknologier, mv.

Der må ved oprettelse påregnes tid til, at myndighedens IP-adresser skal whitelistes af Datafordeleroperatøren.

6 Krav til myndighedens tekniske installationer

Ved internet (TCP/IP) opkoblinger skal myndigheden sikre sig, at Myndighedens udgående IP-

adresse/r til brug for TCP/IP trafik til og fra CPR's produkter på Datafordeleren kun anvendes af den pågældende myndighed eller af andre myndigheder med en tilsvarende adgang til CPR.

Det er i øvrigt myndighedens ansvar, at følgende krav overholdes:

- Det administrative lokalnet er sikret mod uønsket indtrængning udefra.
- Der ikke kan ske snifning (aflytning af data) på det administrative lokalnet fra pc'er, der ikke hører til administrationen.
- Det administrative lokalnet skal netværksmæssigt være afgrænset til øvrige lokalnet, herunder lokalnet til eksempelvis publikums- eller skoleelevterminaler.
- Administrative terminaler og servere, der har TCP/IP opkobling til CPR/Datafordeleren, må ikke anvende samme IP-adresse til udgående TCP/IP trafik som ikke administrative terminaler, herunder eksempelvis publikums- eller skoleelevterminaler.

7 Krav til hjemmearbejdspladser (adgang fra terminal i hjemmet eller tilsvarende til myndighedens lokalnet)

Det er den sikkerhedsansvarliges ansvar, at følgende retningslinjer overholdes:

- Der skal være særlige retningslinjer for etablering af hjemmearbejdspladser, således at det sikres, at bestemmelserne om sikkerhedsforanstaltninger iagttages.
- Lokaler, der benyttes i forbindelse med hjemmearbejdspladser, skal være indrettet med henblik på at forhindre uvedkommendes adgang til oplysningerne.
- Adgangen fra hjemmearbejdspladsen til myndighedens lokalnet skal ske som beskrevet i det forrige afsnit om datakommunikationsadgang.
- Oplysninger fra CPR må ikke lagres på hjemmearbejdspladsen, medmindre oplysningerne krypteres.
- Hvis der tillades anden anvendelse af hjemmearbejdspladsen, f.eks. til privat brug, skal der fastsættes retningslinjer for denne anvendelse og etableres de nødvendige sikkerhedsforanstaltninger hermed.
- Hvis der udskrives oplysninger på hjemmearbejdspladsen, skal der findes regler, der sikrer forsvarlig opbevaring, så uvedkommende ikke får fat i dem, herunder også regler om betryggende destruktion.
- Der skal være retningslinjer for, hvordan hjemmearbejdspladsen beskyttes mod virus eller andet misbrug.
- Der skal være time out, hvis hjemmearbejdspladsen ikke er brugt i 10 minutter, dvs. at der enten spærres, således at den kun kan åbnes med et kendeord, eller således at forbindelsen til eget fagsystem med CPR-oplysninger, eller den direkte adgang til CPR's tjenester på Datafordeleren, afbrydes.
- Den sikkerhedsansvarlige skal udføre kontrol af de særlige retningslinjer med henblik på sikring af, at bestemmelserne om sikkerhedsforanstaltninger overholdes.

8 Regler for myndighedens behandling af personnummer

I kapitel 13 i CPR-loven er der fastsat følgende regler for offentlige myndigheders behandling af

personnummer:

"**§ 52.** Hvis en offentlig myndighed i overensstemmelse med Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og databeskyttelsesloven anvender personnummer som identifikation eller journalnummer, skal det være personnummeret for den person, sagen vedrører.

Stk. 2. Bestemmelsen i stk. 1 gælder dog ikke, hvis det følger af lov eller bestemmelser fastsat i henhold til lov, at det under et forvaltningsområde er nødvendigt at henføre flere personer til samme sag. I sådanne tilfælde afgør forvaltningen selv, hvorledes den interne sagsregistrering tilrettelægges mest hensigtsmæssigt. Ved denne tilrettelæggelse skal der bl.a. tages ligestillingsmæssige hensyn.

§ 53. Anvender en offentlig myndighed personnummer ved henvendelse til en person om dennes forhold, skal myndigheden anvende vedkommendes eget personnummer. En person kan tilsvarende kun blive afkrævet sit eget personnummer ved henvendelser til offentlige myndigheder i situationer omfattet af § 52.

§ 54. Offentlige myndigheder skal sørge for, at personnummer ikke kommer uvedkommende i hænde. Personnumre må ikke påføres fuldt læseligt uden på breve, i rudekuverter eller ved andre forsendelser til vedkommende. Er det nødvendigt i sådanne tilfælde at angive en identifikation, skal personnummeret sløres, således at det ikke er umiddelbart genkendeligt.

Stk. 2. Personnummer kan angives fuldt læseligt på giroindbetalingskort, såfremt dette fremsendes i lukket kuvert til vedkommende.

Stk. 3. Personnummer må ikke offentliggøres, herunder i Statstidende, bortset fra ved proklamaer i dødsboer, medmindre det følger af lov eller bestemmelser fastsat i henhold til lov."

9 Regler for myndighedens behandling og videregivelse af oplysninger modtaget fra CPR's produkter via Datafordeleren

Myndigheden er dataansvarlig for de oplysninger, som myndigheden har modtaget fra CPR.

CPR-oplysninger, som myndigheden har modtaget fra Datafordeleren, må kun anvendes til det forudsatte formål.

Myndigheden må kun videregive oplysninger, herunder beskyttede navne og adresser, til andre offentlige myndigheder eller private, hvis videregivelsen følger af lov eller bestemmelser fastsat i henhold til lov.

Myndighedens overladelse af data, som er modtaget fra CPR, til behandling på et servicebureau eller lign., betragtes ikke som videregivelse til private, såfremt databehandlerens behandling af oplysningerne er i overensstemmelse med databeskyttelsesforordningen og databeskyttelsesloven.

En person kan i CPR være registreret med navne- og adressebeskyttelse, således at vedkommendes navn og adresse ikke må videregives til private.

Myndigheden skal sørge for, at beskyttede navne og adresser ikke bliver tilgængelige for private. Myndigheden skal i alle tilfælde i forbindelse med navn og adresse registrere oplysning om beskyttelsen. Denne oplysning skal endvidere altid meddeles i forbindelse med eventuel videregivelse af navn og adresse til andre. Dette afsnit gælder ikke, hvis andet følger af lov eller bestemmelser fastsat i henhold til lov.

Myndigheden har ansvaret for, at uvedkommende ikke kan få adgang til CPR's data. Anvendes adgangen til CPR's produkter på Datafordeleren i forbindelse med en selvbetjeningsservice på en offentlig tilgængelig hjemmeside, skal myndigheden sikre, at brugere af denne selvbetjeningsservice kun kan initiere opslag i CPR efter at være blevet autentificeret med NemID eller MitID, ligesom pågældendes personnummer skal være verificeret via Nets.

10 Regler for myndighedens benyttelse af CPR's oplysninger i statistisk eller videnskabeligt øjemed

Der henvises til Sundhedsdatastyrelsen, som varetager videregivelse af CPR-oplysninger til brug i statistisk eller videnskabeligt øjemed.

11 Betaling

For hovedparten af de offentlige anvendere er CPR-data på datafordeleren frikøbt gennem en aftale indgået mellem staten, regionerne og kommunerne. Frikøbet gælder også evt. underleverandører til egne it-løsninger.

Visse offentlige virksomheder er dog ikke omfattet af frikøbet. Det vil typisk være særlige virksomhedskonstruktioner og statsvirksomheder, der enten fører indtægtsdækket virksomhed, eller som tilbyder løsninger på markedsvilkår (f.eks. Danmarks Radio, ATP, DSB, Ørsted (tidl. DONG), m.fl.).

Omkostningerne i forbindelse med adgangen til CPR's produkter på Datafordeleren skal afholdes af den modtagende myndighed. Betalingen sker direkte til Statens Administration, som på CPR-kontorets vegne forestår faktureringen.

Evt. spørgsmål og korrespondance i forbindelse med faktureringen rettes til CPR-kontorets kundecenter via CPR Servicedesk. Betalingen for benyttelse af CPR sker efter de til enhver tid gældende enhedspriser. Der betales fra det tidspunkt, hvor CPR-kontoret har etableret adgangen til CPR's produkter på Datafordeleren.

Enhedspriserne kan oplyses ved henvendelse til CPR-kontoret.

CPR-kontoret kan forlange forudbetaling, eventuelt i form af en aconto betaling.

Såfremt Myndigheden videregiver oplysninger, som er modtaget fra CPR, i kommerciel henseen-

de, forbeholder CPR-kontoret sig ret til at modtage et beløb (royalty), der fastsættes af CPR-kontoret, fra Myndigheden.

12 Driftsforhold

CPR produkter fra Datafordeleren er til rådighed 24 timer i døgnet, 7 dage om ugen. Med henblik på service og vedligeholdelse m.v. kan der forekomme servicevinduer og nedlukninger - normalt i weekenden - på nogle timers varighed. Tidspunkter for nedlukninger offentliggøres på www.datafordeler.dk - der henvises i øvrigt til Datafordeler-operatøren for alle henvendelser vedrørende driftsforhold.

13 Fejl og mangler

Såfremt en dataleverance fra Datafordeleren er fejlbehæftet eller mangelfuld, og dette udelukkende skyldes forhold, der kan tillægges Datafordeleren, vil Datafordeleren uden ugrundet ophold foretage afhjælpning.

Hvis Datafordeleren gennemfører behørig afhjælpning, kan CPR's kunde ikke gøre andre krav gældende i anledning af fejl og mangler.

14 Ansvar

CPR-kontoret hæfter ikke for driftstab, avancetab eller andet indirekte tab. CPR-kontorets hæftelse kan ikke overstige det beløb, der er betalt i forbindelse med adgangen til CPR.

15 Force Majeure

Såfremt CPR-kontoret eller CPR's kunde forhindres i at opfylde sine forpligtelser som følge af omstændigheder opstået efter aftalens indgåelse, er parten berettiget til at træde tilbage fra aftalen. Det er en forudsætning for anvendelse af denne tilbagetrædelsesret, at parten ikke ved aftalens indgåelse burde have taget de omstændigheder, der umuliggør aftalens opfyldelse, i betragtning.

CPR-kontoret er indforstået med, at driften af CPR's produkter på Datafordeleren er vital, hvorfor Datafordeler-operatøren vil træffe alle hensigtsmæssige foranstaltninger med henblik på at sikre tjenesternes fortsatte driftsafvikling, når force majeure situationen foreligger, herunder ved strejke og lockout.

16 Tvister

Enhver tvist, der udspringer af dataleverancer fra Datafordeleren til CPR's kunder, afgøres af en af Det Danske Voldgiftsinstitut nedsat voldgift i overensstemmelse med reglerne for behandling af sager ved Den Almindelige Voldgiftsret i Danmark.

Ved sagens afgørelse skal gældende dansk ret lægges til grund.

17 Opsigelse

Aftale om adgang til CPR's produkter på Datafordeleren med CPR-kontoret kan af Myndigheden skriftligt opsiges med 1 måneds varsel til udgangen af en måned – dog tidligst tre måneder efter, at adgangen er oprettet.

CPR-kontoret kan opsige aftalen om adgangen til CPR's tjenester på Datafordeleren med øjeblikkelig varsel i tilfælde af overtrædelse af de fastsatte vilkår samt ved manglende betaling.

CPR-kontoret kan i forbindelse med lovændringer, den tekniske udvikling, effektiviseringsbestræbelser m.v. foretage ændringer i CPR's dataleverancer og -former eller udfase serviceprodukter, uddatamedier m.v. med rimelige varsler.