Økonomi- og Indenrigsministeriet

Dato: 25. maj 2018
Kontor: CPR-kontoret
J.nr: 2018-321

Standardvilkår for offentlige myndigheders adgang til CPR.

(herunder grønlandske myndigheder)

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 oplysninger fra CPR, 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 databeskyttelsesforordningen og databeskyttelsesloven og bestemmelser fastsat i medfør heraf.

Ændringer i nærværende vilkår samt løbende information om driftsforhold offentliggøres alene via nyhedsabonnement på www.cpr.dk samt lysaviser i CPR-systemet.

2 Oprettelse og ændring af kundeforhold.

Anmodning om adgang til CPR inden for rammerne af disse vilkår sker ved skriftlig henvendelse fra myndigheden (kunden) til CPR-kontoret, kc@cpr.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 sikkerhedsforanstaltningerne overholdes,
- 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 kun de medarbejdere, der varetager indberetning til CPR, autoriseres hertil (gælder for bl.a. kommunerne, folkekirkens ministerialbogsførere, personregisterførerne i Sønderjylland, Statsforvaltningen, domstolene, Integrationsministeriets Indfødsretskontor, sygehuse og SKAT),
- at det er den rette person, der foretager anmeldelse, f.eks. af flytning, med henblik på ajourføring af CPR via en selvbetjeningsserver,
- 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 udsteder CPR-kontoret en eller flere administrationskoder (personkode og kendeord) til den sikkerhedsansvarlige, som herefter i CPR-systemet rekvirerer de nødvendige personkoder til relevante medarbejdere. Hver medarbejder skal have sin egen personkode, som tildeles et hemmeligt kendeord. Dette kendeord skal udskiftes ved den enkelte medarbejders første adgang til CPR til et personligt og fortroligt kendeord, der kun kendes af den pågældende medarbejder. Ved tilbagelevering af autorisationen skal den sikkerhedsansvarlige sikre, at kendeordet ændres til et fortroligt kendeord, der kun kendes af den sikkerhedsansvarlige.

Ved system til system adgang til CPR udstedes dog normalt kun en systembrugerkode til anvendelse i myndighedens program. Den sikkerhedsansvarlige skal sikre, at kendeordet ændres til et fortroligt kendeord, første gang programmet anvendes som adgang til CPR. Den enkelte medarbejder anvender den autorisationskode, som medarbejderen er tildelt af myndigheden til brug i det system, der benytter system til system adgang til CPR.

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. Fortegnelsen over medarbejdere kan føres i CPR-systemet i de dertil indrettede faciliteter.

Ved online adgang til CPR skal den enkelte medarbejder overholde følgende regler vedrørende kendeord (password):

- kendeordet skal være personligt,
- kendeordet må ikke deles med, lånes ud eller oplyses til andre,
- kendeordet skal udskiftes efter højst 90 dages brug,
- kendeordet må ikke genbruges,

- kendeordet skal følge de til enhver tid gældende regler for gyldige tegn,
- kendeordet må ikke indeholde løbenummer (f.eks. peter001, peter002, etc.),
- kendeordet må ikke bestå af eget eller familiens navn, initialer, fødselsdato, personnummer, bilnummer, bilmærke eller andet, der er nemt at gætte for andre, og
- kendeordet skal ændres, hvis det er eller kunne være blevet kendt af andre.

Brugeren (personkoden) vil blive spærret efter 5 mislykkede forsøg på at indtaste det rigtige kendeord (password). Personkoder, der er blevet spærret, skal genåbnes af den sikkerhedsansvarlige eller den eller de personer, som den sikkerhedsansvarlige har bemyndiget hertil. CPR-kontoret vil kun i særlige tilfælde være behjælpelig med at genåbne personkoder.

Medarbejderne må i CPR 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 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 myndighedens autorisationer til CPR samt myndighedens søgninger, opslag og ajourføringer i CPR. 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, opslag og ajourføringer registreres i CPR. Registreringen sker i CPR-systemet og indeholder oplysning om personkode (brugernavn), transaktionstype, tidspunkt samt hvilke oplysninger, der er forespurgt på, søgt på eller ajourført i CPR. Hvis myndigheden anvender en system til system adgang, skal myndigheden foretage en registrering af den enkelte brugers transaktioner i myndighedens system.

Via CPR-systemet (CPRWeb) har de af myndigheden udpegede brugere adgang til henholdsvis 1) en logsøgning, der muliggør generering af en udskrift med udvalgte eller alle søgninger, opslag og ajourføringer 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 til CPR i overensstemmelse med nærværende vilkår samt lov om behandling af personoplysninger. 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.

Batchleverancer sker udelukkende via filoverførsel.

Dataoverførsel skal ske, så data ikke kompromitteres. CPR-kontoret fastsætter reglerne herfor. Reglerne omfatter bl.a. brug af kryptering og kontrol af IP-adresse.

Anmodning om åbning for nye IP-adresser vil på hverdage normalt ske inden for 24 timer, såfremt anmodningen er modtaget inden kl. 12.00 på hverdage.

Adgang til CPR via system til system løsninger må ikke anvendes som transaktionskanon (online batch) uden forudgående godkendelse fra CPR-kontoret.

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 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, 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 CPR 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.

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

Oplysninger, som myndigheden har modtaget fra CPR, 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 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, 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.

Omkostningerne i forbindelse med adgangen til CPR 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 på mail kc@cpr.dk. 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.

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

12 Driftsforhold.

CPR-systemet er til rådighed 24 timer i døgnet, 7 dage om ugen. Med henblik på service og vedligeholdelse m.v. kan der forekomme nedlukninger - normalt i weekenden - på nogle timers varighed. Tidspunkter for nedlukninger offentliggøres på www.cpr.dk og på CPR-systemets lysavis.

Batch-leverancer afvikles på hverdage mandag til fredag i tidsrummet efter kl. 18.00, undtagen 5/6, 24/12 og 31/12. Derudover kan særlige batch-opgaver afvikles efter aftale.

Specielt for så vidt angår CPR-produkter, der anvendes til system til system løsninger, tilpasses disse løbende, så de lever op til omverdenens krav. Eventuelle ændringer i de enkelte produkter meddeles med mindst 3 måneders varsel. Udgifter, som myndigheden i den forbindelse måtte have til nødvendige omlægninger, afholdes af myndigheden.

En eventuel flytning af CPR's drift til en anden IT-leverandør meddeles med mindst 3 måneders varsel. Udgifter, som myndigheden i den forbindelse måtte have til nødvendige omlægninger, afholdes af myndigheden.

13 Fejl og mangler.

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

Hvis CPR-kontoret 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 hæf-

telse 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-systemet er vital, hvorfor CPR-kontoret vil træffe alle hensigtsmæssige foranstaltninger med henblik på at sikre systemets fortsatte driftsafvikling, når force majeure situationen foreligger, herunder ved strejke og lockout.

16 Tvister.

Enhver tvist, der udspringer af dataleverancer fra CPR-kontoret 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, herunder reglerne i databeskyttelsesforordningen og databeskyttelsesloven.

17 Opsigelse.

Aftale om adgang til CPR 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 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.