Sikkerhedsanalyse

Sikkerhedsanalysen har analyseret de strukturelle sikkerhedsudfordringer, som persondata-registreringen står overfor i Danmark. De dele af værdikæden med højest iboende risici findes i distributionen af grunddata. I distributionen af persongrunddata er der en høj iboende risiko for

- at cpr-økosystemet tilgængelighed vil blive begrænset som følge af et DDoS angreb,
- at der vil ske brud på fortroligheden som følge af mange distributionsregistre samt
- at der ligeledes vil ske brud på fortroligheden som følge af fejl i forbindelse med videregivelse af personfølsomme data.

Konsekvenserne ved trusselsbilledet fordeler sig på henholdsvis fortrolighed, integritet og uafviselighed samt tilgængelighed:

- Konsekvenserne ved et brud på fortroligheden af persongrunddata strækker sig fra det uvæsentlige til, ved værst tænkelige scenarie, det uacceptable. Konsekvenserne fordeler sig ligeligt blandt registerejere, anvendere og datasubjekter (borgere)
- Konsekvenserne ved en manglende tilgængelighed af grunddata er begrænsede som følge af persongrunddatas decentrale struktur. Der vil således med stor sandsynlighed være dele af cpr-økosystemet tilgængeligt selvom et af grunddataregistrene er utilgængeligt. Mistet tilgængelighed vurderes derfor kun at være generende og det primært for registerejere og anvendere
- Konsekvenserne ved manglende integritet og uafviselighed varierer kraftigt fra part til part. Registerejere vil potentielt kunne opleve konsekvenser der er uacceptable, ved en ekstrem situation hvor et helt register kompromitteres. For anvendere og datasubjekter vil konsekvenserne typisk ikke overstige generende og i værste fald kritiske.

Et væsentligt behov findes for at udpege en myndighed med ansvar for den strukturelle sikkerhed i cpr-økosystemet, herunder lægge en strategi for det stigende antal distributionsregistre og for hvordan personnumre benyttes i anvenderlaget

Kontekst og struktur for analysen af sikkerhedsudfordringer

Kontekst for analysen

Denne analyse af sikkerhedsudfordringerne ved personregistreringen har fokus på det samlede økosystem for persongrunddata. Analysen beskæftiger sig med risici forbundet med den overordnede struktur og samspillet mellem de enkelte elementer i strukturen, mens det forventes, at de data- og systemansvarlige for hvert enkelt system vurderer og håndterer de risici , der er forbundet med det enkelte system.

Økosystemet er kendetegnet ved, at persongrunddata anvendes i en lang række systemer (mere end 400), af mange brugere (skønnet mere end 100.000), og at data i CPR og CPR-U opdateres af mange brugere og myndigheder.

Som følge af den udbredte anvendelse af cpr-data ligger hovedvægten på dette område, mens data om udlændinge har en mere begrænset anvendelse og dermed ikke har samme fokus i analysen.

Sikkerhedsanalysen anlægger en værdikædebetragtning (jf. værdikædefiguren herunder) med særlige iboende risici for hvert trin i værdikæden. Sikkerhedsanalysen vil analysere hvert trin i værdikæden, men vil have specielt fokus på anvendelses- og distributionstrinnene, idet der distribueres 1,2 mia. poster om året, mens der "kun" sker 3,3 mio. ajourføringer om året.

	Registrering	Registerdrift	Distribution	Anvendelse
Systemer	• Cpr-klient • Myndigheders egne klienter/ applikationer • Borgeradgang	• CPR • CPR-U (CARL2)	• CPR distribuerer ad flere kanaler til mange distributions-registre • CPR-U tilgås af mange systemer	• Cpr-klient • Myndigheders egne applikationer • Borgeradgang

Struktur for analysen

- **Strukturelle sikkerhedsrisici:** Danmark har af historiske årsager valgt den nuværende struktur for grundlæggende personregistrering. Dette valg af struktur medfører nogle iboende risici. På baggrund af en analyse af den danske model udarbejdes et trusselskatalog.

- **Konsekvenser:** På baggrund af trusselskataloget gennemføres en vurdering af udfaldsrummet for konsekvenserne ved at én eller flere risici indtræffer samt hvilke områder, som disse konsekvenser berører.

- **Mulige imødegående tiltag:** Ud fra såvel trusselskataloget og konsekvensvurderingen identificeres række mulige imødegående tiltag, som kan implementeres, hvis de strukturelle risici ved den danske model skal mitigeres.

- **Strukturelle ændringsbehov:** Med udgangspunkt de identificerede imødegående tiltag udvælges en række strukturelle ændringsbehov, som på bedste vis balancerer behovet for risikomitigerende tiltag og gevinsterne ved den nuværende struktur for persongrundregistrering.

De strukturelle ændringsbehov videreføres til projektets fase 2, hvor de vil indgå i designkriterierne for løsningsmodellerne.

Fremgangsmåde for analysen af sikkerhedsudfordringerne

Tilgangen bygger på en tilpasset version af metoden for risikovurdering i Digitaliseringsstyrelsens Styring af informationssikkerhed efter ISO 27001 og gennemgår følgende trin:

- Etablering af kontekst, som i dette projekt omfatter det samlede personregistreringsøkosystem med fire led (jf. værdikædefigur beskrevet tidligere i dette kapitel)
- Udarbejdelse af trusselskatalog:
  - Væsentligste trusler: Særligt trusler der er en følge af økosystemets samlede struktur. Dette suppleres af ENISA, ISF og Deloitte ERS's trusselskatalog og organiseres i henhold til værdikædens fire trin (registrering, registerdrift, distribution og anvendelse).
  - Sårbarheder: For hver trussel vurderes de systemiske sårbarheder. Det vil sige, at analysen har fokus på sårbarheder, der er en følge af økosystemets samlede struktur
  - Iboende risiko: For hver trussel vurderes den iboende risiko (vurderet på en skal fra lav til ekstrem)
- Identifikation af konsekvenser: På baggrund af trusselskataloget og med udgangspunkt i Digitaliseringsstyrelsens vejledning, jf. figur på denne side, vurderes følgende konsekvensdimensioner:
  - Strategisk: Medfører indskrænkninger i råderum
  - Finansielt: Medfører meromkostninger eller tab
  - Administrativ: Medfører administrative belastninger
  - Offentligt omdømme: Påvirker omdømme i uønsket retning
  - Forhold til interessenter: Påvirkninger af forhold til interessenter
  - Konsekvenser for privatlivet (herunder identitetstyveri)
- Risikoevaluering: Evaluering af de identificerede risici og forslag/anbefalinger til mulige imødegående tiltag

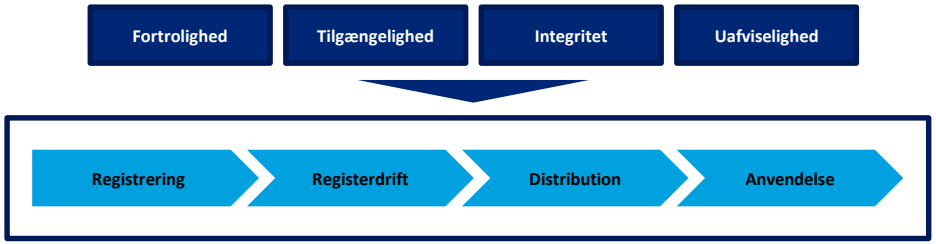
Konsekvenstype	Konsekvens-beskrivelse	Konsekvensniveau			
		Uacceptabelt	Kritisk	Generende	Uvæsentligt
Strategisk	Medfører indskrænkninger i evnen til at handle i en periode	Bliver ude af stand til at gennemføre vigtige aktiviteter, som er planlagt i en periode fremover	Medfører revurdering af vigtige aktiviteter på kort sigt	Planlagte aktiviteter kan gennemføres med mindre justeringer	Ingen særlig påvirkning
Finansiel	Medfører meromkostninger eller tab	Væsentlige økonomiske tab/bliver sat under administration *Beløb:* *> x mio. kr.*	Store økonomiske tab med risiko for at blive sat under administration *Beløb:* *< x mio. kr.*	Meromkostninger og tab i begrænset niveau, som kan kræve mindre budgetændringer *Beløb:* *< x t.kr.*	Ingen særlig finansiel påvirkning *Beløb:* *< x kr.*
Administrativ	Medfører administrative belastninger	Administrative ressourcer må udvides urealistisk	Der må trækkes væsentligt på eksisterende og nye administrative ressourcer	Håndteres inden for rimeligt ekstra administrativt ressourcetræk	Håndteres uden særligt ressourcetræk i de administrative funktioner
Offentligt omdømme (image), Politiske forhold	Påvirker omdømme i uønsket retning	Væsentlig skade på omdømme. Sag behandles på ministerplan	Offentligheden fatter generel negativ interesse, medfører reprimande ("næse") til departementschef(er) og/eller direktører	Forbigående opmærksomhed fra enkelte grupper, påvirker kun dele af ministerium (fx en styrelse)	Påvirkes ikke
Forhold til interessenter	Påvirkninger af forhold til interessenter	Væsentligt nedbrud i det generelle samarbejde med interessenter	Generelt forringet samarbejde mellem interessenter	Forringet samarbejde med interessenter i enkeltsager	Påvirkes ikke

Kilde: Digitaliseringsstyrelsens Vejledning i it-risikostyring og -vurdering bilag 3

Scenarier

På denne side er skitseret en række scenarier for sikkerhedshændelser, som kan påvirke persondataøkosystemet. Formålet med scenarierne er at konkretisere sikkerhedsudfordringerne på personregistreringsområdet

Scenarierne er inddelt i fire områder:



Fortrolighed

Fortrolighed af data (privacy) vil sige, at kun autoriserede brugere (medarbejdere, borgere, andre) med et specifikt og godkendt behov har adgang til data. Manglende fortrolighed kan skade organisationens omdømme og give mulighed for misbrug.

- Scenarie A: En fil med ca. 100 personregistreringer fra CPR bliver ved en fejl tilgængelige på en kommunes hjemmeside i forbindelse med en høringsproces
- Scenarie B: Et komplet kopi-register hackes af Anonymous og gøres fuldt tilgængeligt på gruppens hjemmeside – flere tusinde downloader filen
- Scenarie C: Ukendte gerningsmænd benytter bl.a. navn og cpr-nummer til at tilgå et stort antal borgeres bankoplysninger via en storbanks call center. Disse informationer benyttes efterfølgende til at stjæle større pengebeløb

Tilgængelighed

Tilgængelighed og driftsstabilitet af it-systemer vil sige, at organisationens medarbejdere og slutbrugere skal kunne tilgå data og systemer, når der er behov for det. Manglende tilgængelighed kan medføre, at myndigheder ikke kan udføre deres opgaver, og at virksomheder kan lide økonomiske tab, fx på grund af mistet salg.

- Scenarie D: En fejl i forbindelse med opgraderingen af en server gør CPR utilgængeligt i 12 timer – hverken batch-kørsler eller online adgang er mulig
- Scenarie E: CPR udsættes for et massivt DDOS angreb, der gør registeret utilgængeligt for online søgninger i mere end en uge
- Scenarie F: Et kopi-register hackes og gerningsmændene lykkedes at slette store dele af kopi-registeret inden sikkerhedshullet identificeres og lukkes

Integritet

Pålidelighed eller integritet af data vil sige, at data har den rette kvalitet og ikke er forkerte. Forkerte data kan betyde manglende overholdelse af lovgivningsmæssige eller aftalemæssige krav.

- Scenarie G: En programmeringsfejl i forbindelse med en patch på CPR betyder at et ukendt antal filer er fejlbehæftede
- Scenarie H: En myndighed har igennem flere år systematisk udfyldt et felt forkert i forbindelse med persongrundregistreringen
- Scenarie I: En eller flere medarbejdere i en offentlig institution har registreret ikke validerede persongrunddata

Uafviselighed

Uafviselighed og autenticitet vil sige, at det er muligt entydigt at fastlægge identiteten på den person, der foretager dataændringer eller – transaktioner og at disse ændringer og transaktioner er forsynet med tidsstempel og identifikation, som indebærer, at de ikke efterfølgende kan benægtes af de involverede parter.

- Scenarie J: Der opdages forskelle mellem data i et lokalt fagsystem og CPR-U – det viser sig, at hackere igennem længere tid har ændret data, der kan have indflydelse på grundlaget for familiesammenføring
- Scenarie K: Medarbejdere i et borgerservicecenter er blevet trætte af at logge på en fælles pc hver gang de skal bruge systemet og har derfor ændret skærmlåsningsindstillingerne, så pc'en ikke låses og oprettet et fælles login til systemerne.

Strukturelle risici ved registrering af persongrunddata

Trussel	Iboende risiko	Beskrivelse af truslen og sårbarhed	Truslen vedrører	Eksempler på mulige imødegående tiltag
Fejl i registrering af data	Middel	Fejl under datafangst/registrering kan vise sig at være kilde til upålidelige data. Fejl kan fx skyldes menneskelige fejl under indtastning eller fejl i integrationer med tilstødende systemer. Den store stigning i selvbetjeningsløsninger giver desuden mulighed for snyd med registreringen (jf. Effektiv sagsbehandling og kontrol) *Sårbarhed:* Vurdering af sårbarhed kræver nærmere indsigt i, hvorledes data kan fødes samt i workflows i den forbindelse. Dog er der indikationer om at digital selvbetjening ifm. flytninger åbner op for en potentiel fejlkilde i CPR. Registrering i CPR-U er potentielt en større kilde til fejl, da der er ikke er fyldestgørende datavalideringsmekanismer og der er flere inddateringsmuligheder og flere aktører, som ikke nødvendigvis inddaterer efter samme praksis.	Integritet	a. Implementer datavalideringer i registre, registreringssystemerne og særligt selvbetjeningssystemerne *Forretningsmæssige konsekvenser:* • Omkostninger til definering af valideringsregler og implementering af disse
Cpr-nummerets opbygning tolkes og eftergøres; og udnyttes efterfølgende til misbrug	Lav	Anvendelse af et betydningsbærende nummer kan indebære nogle risikomomenter, idet betydningen gør det lettere for misbrugere at konstruere et nummer *Sårbarhed:* De fleste cpr-numre dannes ved anvendelse af et modulo-11-princip. Visse fødselsdatoer er opbrugt, og i så fald anvendes et andet princip, der fejler ved en modulo-11-validering. Det må ikke desto mindre anses for nemt at generere et falsk cpr-nummer. Dog skal det bemærkes, at det også er nemt at skaffe sig et gyldigt og tildelt cpr-nummer ad andre veje. Et betydningsbærende nummer udgør ikke i sig selv en høj sikkerhedsrisiko, men derimod den omfattende og udvidede anvendelse af nummeret i situationer, som det ikke beregnet til (fx autentificering ved henvendelser). I forbindelse med selvbetjening, så reducerer brugen af NemID konsekvenserne ved denne risiko	Integritet og uafviselighed	a. Erstat cpr-nummeret med nyt personnummer uden betydning *Forretningsmæssige konsekvenser:* • Kan ikke benyttes til umiddelbar verificering (alder, køn) • Datasubjekter har sværere ved at huske nummeret • 400+ systemer skal tilpasses b. Begræns cpr-nummerets brug som eneste middel til autentifikation ved henvendelser til myndigheder og private (finansielle) virksomheder *Forretningsmæssige konsekvenser:* • NemID eller en anden mekanisme skal benyttes som autentifikation. c. Begræns antallet af forsøg på inddatering af cpr-nummer som selvbetjenings-løsninger tillader uden indledende login med NemID for dermed at reducere automatiserede gæt *Forretningsmæssige konsekvenser:* • Begrænsede konsekvenser for både offentlige og private aktører

Strukturelle risici ved registerdrift (styringsmæssige trusler)

Trussel	Iboende risiko	Beskrivelse af truslen og sårbarhed	Truslen vedrører	Eksempler på mulige imødegående tiltag
Tab af styring af registerdrift og det samlede persongrunddata -økosystem	Lav	Grunddata-økosystemets distribuerede opbygning kræver en høj grad af koordineret styring af sikringsforanstaltninger med henblik på at forebygge hændelser med brud på fortrolighed, integritet og tilgængelighed. *Sårbarhed:* Økosystemet er i dag fragmenteret og fordelt på flere dataejere, hvoraf nogle dataejerskaber er opstået i forbindelse med oprettelsen af distributionsregistre. Det skaber en risiko for et uens beskyttelsesniveau og besværliggør revisions- og erklæringsarbejde i relation til grunddata-systemer og -datasæt. Anvendere kan potentielt have vanskeligt ved at opnå konsistente SLA'er for alle grunddata. Kopiregistre oprettes, uden at der stilles krav til sikringsforanstaltninger fra den oprindelige dataejer. Der er ingen periodisk uafhængig kontrol med distributionsregistre. Flere dataejere har endvidere outsourcet driften af grunddata-systemerne, hvilket yderligere bidrager til styringens kompleksitet. Fragmentering og distributionsregistre vanskeliggør opretholdelsen af en høj datakvalitet i alle led af anvenderkæden.	Fortrolighed og integritet	a. Reduceret mulighed for at oprette distributionsregistre *Forretningsmæssige konsekvenser:* • Større belastning af CPRs webservices og de autoriserede distributionsregistre b. Skærpet tilsyn med dataejerskab og databehandling *Forretningsmæssige konsekvenser:* • Øget ressourcetræk hos dataejere og databehandlere til dokumentation, it-kontroller og audits c. Yderligere reduktion i antallet af felter, som er tilgængelige for private anvendere *Forretningsmæssige konsekvenser:* • Øgede omkostninger til private aktører, der skal genskabe eksisterende data

Strukturelle risici ved registerdrift (procesmæssige trusler)

Trussel	Iboende risiko	Beskrivelse af truslen og sårbarhed	Truslen vedrører	Eksempler på mulige imødegående tiltag
Misbrug af administrative adgangs-rettigheder	Middel	Truslen består i, at 40-50.000 administrativt personale hos dataejere (inkl. kopidataejere) og driftsleverandører har adgang til CPR og potentielt kan misbruge deres administrative adgangsrettigheder til at skaffe sig adgang til grunddata, uden at der foreligger et driftsmæssigt hensyn. *Sårbarhed:* Sårbarheden afhænger af: • Udmeldte retningslinjer for administrative medarbejderes omgang med grunddata • Den tekniske tilrettelæggelse af rolle-rettigheder i applikationer og databaser • Tilrettelæggelsen af den periodiske kontrol med rettigheder • Tilrettelæggelsen af logning og sporbarhed af forespørgsler.	Fortrolighed og uafviselighed	a. Implementering af mere restriktive adgangsrettigheder og it-kontroller i hele økosystemet *Forretningsmæssige konsekvenser:* • Omkostninger til kontrol med adgangsrettigheder b. Flere audit af it-kontroller og adgangsrettigheder i systemer og registre *Forretningsmæssige konsekvenser:* • Omkostninger til audit
Mangelfuld logning	Middel	Mangelfulde opfølgningslogs eller sikkerhedslogs vanskeliggør efterforskningen af sikkerhedshændelser og kan efter omstændighederne være i strid med gældende lovgivning om databeskyttelse. Dette forværres i situationer, hvor brud på sikkerheden involverer flere aktører i økosystemet. *Sårbarhed:* Logning er implementeret i persongrunddataregistrene, men den er ikke universel. Det vil sige, at der fx ikke er krav om logning af adresseoplysninger og der ikke nødvendigvis er logning i distributionsregistre. Vurdering kræver nærmere indsigt i opsætning af logs for anvendelse af master-grunddata. Truslen er også relevant for anvendere	Tilgængelighed og uafviselighed	a. Øgede krav til logning af alle ændringer i persongrunddataregistre og i distributionsregistre *Forretningsmæssige konsekvenser:* • Øgede omkostninger

Strukturelle risici ved registerdrift (tekniske trusler)

Trussel	Iboende risiko	Beskrivelse af truslen og sårbarhed	Truslen vedrører	Eksempler på mulige imødegående tiltag
Kapacitets-mangel	Middel	Manglende kapacitet til at lagre grunddata eller besvare anvenderes forespørgsler kan udgøre en trussel i forhold til grunddatas tilgængelighed. *Sårbarhed:* Den almindelige driftsmæssige belastning på grunddata-systemerne vurderes som stabil over tid og er tilmed rimeligt forudsigelig. Dog kan der forekomme særlige tidspunkter på året eller måneder, hvor der er brug for særlig kapacitet (fx ved lånkonverteringsbølger), men overordnet udvikler kapacitetsbehovene sig forudsigeligt.	Tilgængelighed	a. Cloudløsning med "uendelig" skalering af registre *Forretningsmæssige konsekvenser:* • Vil sandsynligvis kræve kraftig tilpasning af registerløsning b. Opbygning af en lokal kapacitetsbuffer i registrene *Forretningsmæssige konsekvenser:* • Øgede omkostninger til drift af registrene
Mangelfuld opdatering af masterdata eller sletning af kopier	Middel	Grunddatas livscyklus håndteres ikke fyldestgørende og korrekt på det tekniske plan. Der kan dels være tale om, at stamoplysninger ikke opdateres i masterdatabasen eller kopier ikke slettes, når de er uaktuelle, eller formålet med deres indsamling er ophørt. *Sårbarhed:* Persondata stiller krav til dette, men en konkret vurdering kræver nærmere indsigt i det praktiske workflow for opdatering samt i evt. kriterier for datas sletning.	Integritet	a. Samlet ansvar for personregistreringen i hele dets livscyklus samles i en styrelse eller enhed *Forretningsmæssige konsekvenser:* • Omkostninger til en myndighed med mandat til tværgående styring på persondataområdet • Indskrænkning af råderummet for registrerende myndigheder og for anvendere

Strukturelle risici ved registerdrift (fysiske trusler)

Trussel	Iboende risiko	Beskrivelse af truslen og sårbarhed	Truslen vedrører	Eksempler på mulige imødegående tiltag
Mangelfuld fysisk sikkerhed	Lav	Uautoriseret fysisk adgang til udstyr, hvorpå grunddata lagres og behandles, kan resultere i alle typer af sikkerhedsbrud fordi udstyr modificeres, ødelægges eller stjæles. *Sårbarhed:* Vurdering kræver nærmere indsigt i tilrettelæggelsen af den fysiske sikkerhed omkring grunddatainfrastrukturen, men den fysiske adgang er styret kontraktmæssigt. Truslen er også relevant for distributionsregistre og anvendere.	Fortrolighed, Tilgængelighed, integritet og uafviselighed	a. Øget fysisk sikring af centrale persongrunddataregistre og krav til øget fysisk sikring af distributionsregistre *Forretningsmæssige konsekvenser:* • Omkostninger til sikring af centrale registre • Omkostning til fysisk sikring og audit af fysisk sikring i distributionsregistre
Naturkatastrofe	Lav	Naturkatastrofer, der berører det udstyr, hvorpå grunddata lagres og behandles, kan resultere i alle typer af sikkerheds-brud. *Sårbarhed:* Vurdering kræver nærmere indsigt i tilrettelæggelsen af den fysiske sikkerhed omkring grunddata-infrastrukturen, herunder dublering af serverrum	Fortrolighed, tilgængelighed og integritet	a. Yderligere investering i dubleret / spejlede serverrum og netværksadgange *Forretningsmæssige konsekvenser:* • Øgede omkostninger b. Fuld transfer af data fra persongrund-dataregistre til udvalgte distributionsregistre for derved at have back-up på det fulde persongrunddataregister *Forretningsmæssige konsekvenser:* • Øgede omkostninger til de udvalgte distributionsregistre • Potentielt øget sårbarhed i form af fuld adgang til persongrunddata i de udvalgte distributionsregistre c. Landets beredskabsplan skal inkludere udførelsen af en fuld persongrund-dataregistre kopi *Forretningsmæssige konsekvenser:* • Øgede omkostninger

Strukturelle risici ved distribution (overførsel af data)

Trussel	Iboende risiko	Beskrivelse af truslen og sårbarhed	Truslen vedrører	Eksempler på mulige imødegående tiltag
Distribution af grunddata udsættes for DDOS-angreb.	Høj	Et Distributed Denial of Service (Distribueret Service Nægtelse) angreb kan primært ramme internetvendte tjenester, hvorfra grunddata kan udtrækkes på forespørgsel. *Sårbarhed:* En konkret vurdering kræver en nærmere indsigt i antallet af potentielt berørte tjenester samt i tilrettelæggelsen af sikringsforanstaltninger mod DDOS. Eksistensen af distributionsregistre bidrager alt andet lige til at imødegå denne trussel.	Tilgængelighed	a. Øget investering i kapacitet til behandling af internetvendte forespørgsler *Forretningsmæssige konsekvenser:* • Omkostning til overkapacitet b. Investering i alternative online søgefunktioner hos udvalgte distributionsregistre *Forretningsmæssige konsekvenser:* • Omkostninger til udvikling og drift af nye søgefunktioner
Opsnapning af data under transmission	Middel	Sniffing, spoofing og man-in-the-middle er alle teknikker, der kan anvendes til at opsnappe data, der transmitteres over netværket. I en distribueret driftsmodel, som den der anvendes i forbindelse med grunddata, er truslen særligt relevant. *Sårbarhed:* En konkret vurdering af sårbarheden kræver en nærmere indsigt i tilrettelæggelsen af de tekniske foranstaltninger i forbindelse med transmission af data (kryptering, mv.).	Fortrolighed og integritet	a. Implementering af stærkere autentifikationsløsninger, accesslister, IP-adresseverifikation, krypteringsløsninger, etc. *Forretningsmæssige konsekvenser:* • Omkostninger til implementering af sikkerhedsløsninger hos anvendere og registrerende systemer
Nedbrud i netværks-forbindelserne	Lav	Nedbrud i netværksforbindelser kan skyldes mekaniske fejl (overrivning af kabler) eller konfigurationsmæssige fejl (routningsfejl mv.). Truslen har alt andet lige mindre betydning i en distribueret arkitektur men kan dog have betydning for distributionsregistres korrekthed. *Sårbarhed:* Vurderingen af sårbarheden kræver nærmere indsigt i det samlede økosystems netværksmæssige setup	Tilgængelighed	a. Investering i yderligere redundans i netværksforbindelser til persongrunddataregistre *Forretningsmæssige konsekvenser:* • Omkostninger til redundante netværksforbindelser

Strukturelle risici ved distribution (principper for distribution)

Trussel	Iboende risiko	Beskrivelse af truslen og sårbarhed	Truslen vedrører	Eksempler på mulige imødegående tiltag
Brug af distributionsregistre medfører brud på fortrolighed og risiko for fejl i data	Høj	Den aktuelle it-arkitektur til levering af grunddata medfører, at anvendere af grunddata, af performancemæssige og finansielle årsager, i vidt omfang opretter lokale distributionsregistre, som der forespørges på. Brugen af distributionsregistre medfører alt andet lige forøget risiko for brud på fortroligheden af grunddata samt forøget risiko for fejl i data *Sårbarhed:* Sårbarheden afhænger i vidt omfang af niveauet af de krav, som dataejer af masterdatabasen stiller som betingelse for at tillade generering af distributionsregistre.	Fortrolighed og integritet	a. Reducer antallet af distributionsregistre *Forretningsmæssige konsekvenser:* • Væsentlig vækst i kapacitetskrav til grunddataregistre b. Fjern det finansielle incitament til at oprette distributionsregistre ved at fjerne indtægter fra datasalg *Forretningsmæssige konsekvenser:* • Reduceret indtægt til persongrunddataregistrene
Manglende overens-stemmelse med lovbundne krav.	Høj	Distribution af grunddata vil efter omstændighederne være videregivelse af personoplysninger i persondatalovens forstand. Videregivelse kræver som udgangspunkt samtykke til videregivelsen fra de registrerede eller en klar hjemmel i persondataloven *Sårbarhed:* Vurdering af sårbarhed kræver nærmere indsigt i de indbyrdes forhold og aftaler mellem registerejere og anvendere af grunddata samt kortlægning af grundlaget for videregivelse	Fortrolighed	a. Udføre informationsseminarer omkring fortrolighed af personoplysninger *Forretningsmæssige konsekvenser:* • Øgede omkostninger til informations seminarer b. Skærpet straf ved videregivelse af persondata uden samtykke *Forretningsmæssige konsekvenser:* • Øgede omkostninger til sagsanlæg
Distribution sker i strid med EU-principper for databeskyttelse	Middel	De EU-fæstnede databeskyttelsesprincipper sætter klare rammer for anvendelsen af persondata. Når adgang til grunddata i stadigt stigende omfang tilbydes private aktører, kan der bl.a. være risiko for, at de oprindelige formål, hvortil grunddata er indsamlet, fordrejes til andre formål, som er vanskelige at styre. Andre relevante databeskyttelsesprincipper er: • Lovlighed i behandlingen • Begrænsning i indsamlingen • Værn om datakvalitet • Åbenhed • Indsigt- og indsigelsesret • Ansvarlighed *Sårbarhed:* Økosystemet er sårbart i det omfang. det ikke står klart for anvendere af grunddata, at de har et selvstændigt ansvar for at behandle data lovligt. Sårbarheden skærpes, såfremt der ikke føres efterfølgende kontrol med anvendelsen af data.	Fortrolighed	a. Skærpet straf ved brud på EU's databeskyttelsesprincipper *Forretningsmæssige konsekvenser:* • Øgede omkostninger til sagsanlæg

Strukturelle risici ved anvendelse

Trussel	Iboende risiko	Beskrivelse af truslen og sårbarhed	Truslen vedrører	Eksempler på mulige imødegående tiltag
ID-tyveri og social engineering	Middel	Idet man i vid udstrækning benytter cpr-nummeret, som middel til autentifikation, både i den offentlige og private sektor, så øger det muligheden for identitetstyveri. Identitetstyveri omfatter alle situationer, hvor en tredjemand stjæler og misbruger registrerede personers grunddata fra et register eller på anden måde med henblik på at begå bedrageri. Bedrageriet består typisk i, at oplysningerne bruges til at indgå retshandler i den besvegnes navn. Social Engineering-teknikker benyttes til at overtale eller lokke personer med en bestemt viden til at afsløre oplysninger, som de normalt ikke ville oplyse til ukendte 3. parter. Også her er cpr-nummerets udbredte brug som middel til autentifikation en forøgende faktor *Sårbarhed:* Et grunddataregisters sårbarhed i forhold til at kunne anvendes som udgangspunkt for ID-tyveri eller social engineering er alt andet lige proportionalt med antallet af enkeltoplysninger, der er registreret om hver person samt disse oplysningers potentiale til at skabe troværdighed om en persons identitet hos tredjeparter (samlet identifikationspotentiale). En konsolidering af flere grunddataregistre i ét større register øger alt andet lige konsekvenserne ved id-tyveri eller social engineering.	Fortrolighed	a. Forbyd brugen af cpr-nummeret som eneste middel til autentifikation – fx ved telefoniske henvendelser til bank eller kommune *Forretningsmæssige konsekvenser:* • Offentlige og private vil skulle ændre procedurer • Potentielt fordyrende, idet der vil være behov for et supplerende middel til autentifikation b. Gennemfør en lovændring, der umuliggør inddrivelse af tilgodehavender, hvis eneste kilde til autentificering ved aftaleindgåelse har været cpr-nummer, navn og adresse. *Forretningsmæssige konsekvenser:* • Ændrede forretningsgange for private virksomheder c. Skærpelse af kontrol med selvbetjeningsløsninger, der foretager cpr-check samt selvbetjeningsklienter, browsere, mobilapps, der opbevarer cpr-numre (ukrypterede) for at øge brugervenligheden. *Forretningsmæssige konsekvenser:* • Øgede omkostninger til design af digitale løsninger til borgere og kunder
Misbrug af adgangs-rettigheder og eskalering af privilegier	Middel	Personale hos anvendere misbruger tildelte adgangsrettigheder til at skaffe sig adgang til grunddata, uden at der foreligger et arbejdsbetinget behov. Personale, som har visse rettigheder til at tilgå grunddata har held til at eskalere (udvide) disse rettigheder med henblik på at tilgå flere oplysninger, end rollen oprindeligt er autoriseret til. *Sårbarhed:* Vurdering af sårbarhed kræver en nærmere indsigt i anvenderes retningslinjer og tekniske setup for anvendelse af grunddata samt deres styring af rolle/rettigheder, men med det store antal anvendelsessystemer er sandsynligheden for en vis sårbarhed tilstede	Fortrolighed og uafviselighed	a. Skærpede krav til it-kontroller og logning for anvendere af persongrunddata *Forretningsmæssige konsekvenser:* • Øgede omkostninger hos anvendere til implementering af it-kontroller og logningsløsninger • Øgede omkostninger til audits af it-kontroller b. Skærpet straf ved brud på persondataloven *Forretningsmæssige konsekvenser:* • Øgede omkostninger til sagsanlæg

Strukturelle risici ved anvendelse

Trussel	Iboende risiko	Beskrivelse af truslen og sårbarhed	Truslen vedrører	Eksempler på mulige imødegående tiltag
Manglende instrukser om vilkår for opslag i og anvendelse af grunddata	Lav	Personale hos anvendere har utilstrækkelig viden om vilkår for opslag i grunddata om personer, herunder at der skal være et arbejdsbetinget behov. *Sårbarhed:* Vurdering af sårbarhed kræver en nærmere indsigt i anvenderes retningslinjer for anvendelse af grunddata samt deres styring af rolle/rettigheder.	Fortrolighed	a. Forøget antal af audit af instrukser vedrørende persondata hos anvendere af persongrunddata *Forretningsmæssige konsekvenser:* • Omkostninger til audit b. Begrænsning i mulighederne for at udnytte persondata hos private og offentlige anvendere *Forretningsmæssige konsekvenser:* • Omkostninger til at opbygge alternativer til de centralt distribuerede persongrunddata c. Udføre informations seminarer/kampagner omkring fortrolighed af personoplysninger *Forretningsmæssige konsekvenser:* • Øgede omkostninger til informations seminarer/kampagner d. Skærpet (bøde)straf for virksomheder og myndigheder ved brud på persondataloven *Forretningsmæssige konsekvenser:* • Øgede omkostninger til sagsanlæg

Status på EU-forordningen om persondata og generelle trends vedrørende sikkerhed

Igangværende arbejde med EU-forordning

Europa-Kommissionen har i begyndelsen af 2012 fremlagt et forslag til forordning med nye regler om beskyttelse af personoplysninger i EU.

Forordningsforslaget vil ved dets vedtagelse erstatte det eksisterende direktiv om personoplysninger samt de nationale implementeringer heraf (i Danmark persondataloven), idet forordningen får direkte retskraft i medlemsstaterne.

Forordningen introducerer krav om, at bl.a. offentlige myndigheder tager større ansvar for databeskyttelse ved i praksis at implementere databeskyttelsesfremmende initiativer og udvise ansvarlighed ved behandling af personoplysninger. Som central aktør på persondataområdet vil CPR skulle fungere i lyset af forordningens øgede krav til sikker håndtering af persondata.

Forordningen forventes kun i begrænset omfang at påvirke myndigheders anvendelse af persongrunddata, mens konsekvenserne for privates anvendelse ikke er afklaret på nuværende tidspunkt.

Digitaliseringsstyrelsen følger arbejdet med EU-forordningen, hvor der ikke endnu tegner sig et klart billede af indhold og tidsplaner. Digitaliseringsstyrelsen vurderer, at som det ser ud nu, er der ikke noget, der entydigt peger på, at det ændrer ved de potentielle løsninger, der kan udledes af analysen.

EU-forordningens konsekvenser vil derfor først blive vurderet, når der er et mere konkret og sikkert grundlag.

EU-forordningens væsentligste forslag til ændringer

- One stop shop
- Slut med samtykke i ansættelsesforhold?
- It-systemer (eksisterende og nye) skal understøtte forordningen
- Implementering af sikkerhedsforanstaltninger
- Alle medarbejdere skal følge procedurer
- Data Protection Officer i alle store virksomheder får en aktiv rolle
- Lempelse ved overførsler til tredjelande
- Kontakt til Datatilsynet, når det går galt
- Store bøder ved overtrædelse

Cyber security trends: Nye trusselsbilleder, der potentielt påvirker persongrundregistreringen

Nedenfor beskrives en række fremspirende trusler samlet under overskriften "Cyber security trends", som potentielt kan have væsentlig indflydelse på persongrundregistreringens økosystem:

- *Løbende fremkomst af nye måder, hvormed cyberkriminelle kan udnytte stjålen information:* Der observeres løbende fremkomst af nye teknikker til at udnytte stjålen information, især med henblik på at opnå økonomisk vinding. For dataejere af grunddata-registre har denne udvikling særlig betydning, idet anvendelse af tilsyneladende troværdige grunddata udgør en væsentlig bestanddel i mange angrebsteknikker
- *Hacktivism:* Eksterne angreb med formål at skabe opmærksomhed om enkeltsager ved at gøre tjenester utilgængelige eller ved at blotlægge potentielt kontroversielle oplysninger er mere og mere almindelige
- *Stigende anvendelse af mobile enheder til at tilgå data:* Stigende brug af mobile enheder til at tilgå grunddata, særligt blandt anvendere, gør det vanskeliggere at tilrettelægge og kontrollere sikkerheden.
- *Stigende forekomst af og villighed til at udnytte 0-dags-sårbarheder:* 0-dags-sårbarheder er en samlebetegnelse for sårbarheder, som er offentliggjort, men for hvilke der ikke findes patches eller antimalware-signaturer.
- *Udviklingsprojekter gennemføres, uden at sikkerhedskrav er tilstrækkeligt dokumenteret:* Softwarekomponenter udvikles under tidspres og med forretningsmæssig fokus på at levere ny og forbedret funktionalitet, på bekostning af sikker udvikling og sikkerhedsfokuseret test.
- *Autentificering af brugere er vanskelig at styre i en it-arkitektur, der tillader flere typer endpoint-enheder og flere opslags-kanaler:* Flere kanaler og flere typer udstyr kan medføre en fragmentering af de autentifikationsløsninger, der samlet set er taget i brug

Konsekvensvurdering for fortrolighed

Konsekvensspænd

Konsekvenserne ved et tab af fortrolighed af persongrunddata spænder fra de uvæsentlige til, i yderste konsekvens, uacceptable. Konsekvensspændene er ens for både registerejere, anvendere og datasubjekter.
Størstedelen af persongrunddata ikke er følsomme, men derimod alment kendte oplysninger. Konsekvenserne ved et tab af fortrolighed vil kun være væsentlige, hvis tabet er omfattende (dvs. omfatter både de alment kendte oplysninger og følsomme oplysninger) og hvis de kompromitterede data tilgår personer, som er villige til at gøre en aktiv indsats for at bruge data til skadelig virksomhed.

Part	Konsekvensspændets øvre udfaldsrum	Konsekvenstype
Registerejere	En hændelse, hvor et grunddataregister bliver ramt af systematiske eller omfattende datafejl, f.eks. som følge af en programmeringsfejl, vurderes som uacceptabel. Ud over de politiske og omdømmemæssige konsekvenser som er nævnt ovenfor kan en hændelse betyde, at de administrative ressourcer til at opretholde et nødberedskab og til at få genetableret en acceptabel og tilstrækkelig datakvalitet må udvides urealistisk.	Politisk Omdømme Interessenter
Anvendere	Vurderingen for anvendere, der har etableret et kopiregister, er den samme som for registerejere: tab af fortroligheden til samtlige grunddata i et kopiregister vurderes som uacceptabelt for anvenderen, omdømmemæssigt og i forhold til interessenter. Det politiske aspekt vil, efter omstændighederne, ikke være lige så udtalt som for registerejere, idet datalækket sker et led længere ude i kæden. Et brud på fortroligheden, der kun vedrører en mindre delmængde af et register, vurderes som kritisk. Selv om de omdømmemæssige konsekvenser er alvorlige, vil der kunne argumenteres for, at skaden trods alt er blevet begrænset.	Omdømme Interessenter
Datasubjekter	Konsekvensen for den enkelte borger af tab af fortrolighed til egne grunddata vurderes som uacceptabel ud fra et privacy-perspektiv. Den væsentligste trussel borgere herved udsættes for er identitetstyveri, hvilket kan være en voldsom personlig belastning for den enkelte. Dette gør sig særligt gældende i en kontekst, hvor de lovgivningsmæssige værn mod identitetstyveri ikke er sat i system. Konsekvenserne kan også vedrøre andre aspekter af privatlivsbeskyttelsen af den enkelte borger, og kan, efter omstændighederne, betyde en indskrænkning i den enkeltes handlefrihed (jf. Digitaliseringsstyrelsens privacy-vejledning).	Fortrolighed (Privacy)

Mulige imødegående tiltag

- Implementering af et åbent system, som gør cpr-nummeret alment kendt og derfor ikke brugbart til autentifikation, herunder mulighed for at slå alle, ikke-følsomme informationer op online.
- Implementering af et autentifikation system, som vil låse følsomme oplysninger op. Registrer og fagsystemer skal også videreudvikles for at kunne håndtere forskellige beskyttelsesniveauer af følsomme oplysninger.

Konsekvensvurdering for tilgængelighed

Konsekvensspænd

Konsekvenserne ved manglende tilgængelighed af persongrunddata varierer mellem de enkelte parter i persondataøkosystemet. Det vil primært være anvenderne, som berøres og her vil konsekvenserne variere kraftigt fra anvender til anvender, men vil sjældent være mere end kritisk, idet de fleste anvendere ikke arbejder direkte på persongrunddataregistrene, men enten via distributionsregistre eller via egen database i deres respektive fagsystemer.

Part	Konsekvensspændets øvre udfaldsrum	Konsekvenstype
Registerejere	Tab af tilgængelighed i op til et par dage vurderes som generende. Den udbredte anvendelse af distributionsregistre gør, at de primære interessenter, anvenderne, kun i begrænset omfang vil blive berørt af den manglende tilgængelighed af masterdata-registre, idet distributionsregistrene vil have en tilstrækkelig aktualitet til at kunne bruges.	Omdømme Interessenter Administrativt
Anvendere	Konsekvensen ved tab af tilgængelighed vil, fra en anvender-synsvinkel, afhænge af de forretningsprocesser, der påvirkes af den manglende tilgængelighed. Konsekvensen kan også afhænge af, om der kan trækkes på en nødplan i forhold til de berørte processer. En konkret vurdering må bero på de enkelte anvender-situationer.	Strategisk Omdømme Interessenter Administrativt
Datasubjekter	Mistet tilgængelighed til grunddata vil sjældent få direkte betydning for den enkelte borger. I nogle tilfælde kan det få indirekte betydning, i det omfang borgerne, som følge af den manglende tilgængelighed, påvirkes af langsom eller ineffektiv sagsbehandling hos anvendere.	Administrativt

Mulige imødegående tiltag

- Øget robusthed kan opnås ved at implementere fuld adskillelse mellem persongrunddataregistrene og de registrerings- eller anvendersystemer, som benytter grunddata. Således vil de alle arbejde med kopidata og ikke være afhængige af online adgang til persongrunddataregisteret
- Implementering af end-to-end tilgængelighed, overvågning og måling for at identificere de flaskehalser eller kritiske områder, der skal forbedres

Konsekvensvurdering for integritet og uafviselighed

Konsekvensspæn

Konsekvenserne ved manglende integritet og uafviselighed af persongrunddata varierer mellem de enkelte parter i persondataøkosystemet. For registerejere spænder det fra uvæsentlige konsekvenser til, i yderste konsekvens, uacceptable konsekvenser. For anvender-laget og datasubjekter er kan konsekvenserne være kritiske, men vil oftest mere være af generende karakter.

Part	Konsekvensspændets øvre udfaldsrum	Konsekvenstype
Registerejere	En hændelse, hvor et grunddata-register bliver ramt af systematiske eller omfattende datafejl, fx som følge af en programmeringsfejl, vurderes som uacceptabel. Ud over de politiske og omdømmemæssige konsekvenser som er nævnt ovenfor kan en hændelse betyde, at de administrative ressourcer til at opretholde et nødberedskab og til at få genetableret en acceptabel og tilstrækkelig datakvalitet må udvides urealistisk. En hændelse, hvor grunddata-register ikke har logget ændringer i fx forældremyndighed, som efterfølgende giver den "forkerte" forælder ret til at træffe uoprettelige beslutninger på vegne af barnet er at betragte som havende uacceptable politiske og omdømmemæssige konsekvenser	Politisk Omdømme Interessenter Administrativt
Anvendere	Tab af integritet vil være generende for anvendere, der har etableret eget kopiregister. Integriteten vil i de fleste tilfælde nemt kunne genoprettes ved at forny kopiregisteret via en ny replikering fra en masterkopi. Hvis anvenderen har nået at agere på basis af forkerte data (udføre sagsbehandling, træffe afgørelser, mv.), kan konsekvensen, alt efter omstændighederne, være kritisk. En hændelse, hvor data ændres, men det ikke logges, hvem der har foretaget ændringen er primært af generende karakter, idet anvenderdata for så vidt angår persongrunddata ikke kan betragtes som autoritative og at autenticiteten af data i kopi-registeret kan fastslås ved et opslag i grunddataregisteret	Administrativt
Datasubjekter	Ukorrekte grunddata kan primært få betydning for den enkelte borger i det omfang den manglende datakvalitet medfører, at der træffes forkerte afgørelser. Konsekvensen kan i særlige tilfælde være kritisk for den enkelte borger, men omvendt må det forventes, at evt. fejl i langt de fleste tilfælde vil kunne rettes inden de får alvorlige konsekvenser.	Administrativt

Mulige imødegående tiltag

- Implementering af datafordeleren vil kunne skabe et fuldt, redundant kopi-register af et eller flere persongrunddataregistere
- Implementering af check mellem registre og distributionsregistre for at tjekke integritet og efterfølgende rette op på fejl

Opsummering af væsentligste sikkerhedsudfordringer, mulige imødegående tiltag og afledte strukturelle sikkerhedsbehov

Distributionsregistre

Der er 400+ distributionsregistre og applikationer, der tilgår CPR. Antallet af distributionsregistre for CPR udgør i sig selv en risiko, idet hvert kopi-register er en potentiel kilde til lækage af følsomme persongrunddata.

På nuværende tidspunkt er der ingen central styring eller kontrol med disse distributionsregistre andet end de retningslinjer, som Persondataloven udstikker og evt. kontrol fra Datatilsynet.

Der er behov for at reducere sandsynligheden for at større mængder person-grunddata lækkes. Dette kan gøres ved at reducere antallet af mulige kilder til lækage af følsomme data eller at reducere disse kilders sårbarhed. Det bør derfor overvejes at styrke kontrollen med distributionsregistre eller decideret aktivt arbejde for at reducere antallet. Det skal bemærkes at en hver reduktion af antallet af distributionsregistre vil skulle balanceres med den positive effekt, som distributionsregistrene har på den grundlæggende tilgængelighed af persondata.

Autentificering

Der er i Danmark kutyme for at benytte cpr-nummeret som eneste middel til autentificering og ikke blot som middel til entydig identifikation. Denne praksis benyttes både i den offentlige og private sektor og giver mulighed for både identitetstyveri og social engineering, hvormed følsomme eller private informationer kan tilgås, hvilket videre kan give mulighed for bedrageri.

Der er behov for at reducere konsekvenserne ved at cpr-nummeret falder i de forkerte hænder. Et muligt tiltag kunne være at fjerne muligheden for at benytte cpr-nummeret som autentifikation ved at offentliggøre samtlige cpr-numre online, hvilket bl.a. gøre i Island. Et mindre radikalt tiltag kunne være en lovændring, der umuliggør inddrivelse af tilgodehavender, hvis eneste kilde til autentificering ved aftaleindgåelse har været cpr-nummer, navn og adresse.

Betydningsbærende numre

Cpr-nummeret er betydningsbærende, hvilket gør det nemmere at gætte ved målrettet udnyttelse af eksempelvis selvbetjeningsløsninger. I kombination med den danske kutyme for brug af cpr-nummeret som eneste autentifikation udgør dette en risiko.

Der er dog mange kilder til at få adgang til personers cpr-numre og de fleste påvirkes ikke af om numret er betydningsbærende eller ej.

Der er derfor primært behov for at reducere konsekvenserne ved at cpr-numret opsnappes (jf. afsnittet om autentificering) og reducere muligheden for automatiseret "gæt" af cpr-numre ved at styrke kontrollen med selvbetjeningsløsninger, der foretager cpr-check og ved at reducere muligheden for at selvbetjeningsklienter, browsere, mobilapps og lignende opbevarer cpr-numre (ukrypterede) for at øge brugervenligheden.

Identitetstyveri

Danmarks opbygning af et centralt personnummer med meget bred udbredelse, kutyme for brug som autentificering og valget af et betydningsbærende nummer giver det danske personnummersystem en særlig risikoprofil for identitetstyveri.

Der findes, som nævnt under de tre forudgående afsnit, flere muligheder for at begrænse de enkelte risikoelementer, som dog alle vil have væsentlige forretningsmæssige konsekvenser for anvendere og registranter.

Det skal desuden bemærkes, at erfaringen fra lande som England og USA, der har indrettet personregistreringen med flere adskilte domæner med separate nøgler, at udbredelsen af identitetstyveri er langt større i disse lande end i Danmark. Der er således intet der umiddelbart taler for, at indretningen af det danske personnummer økosystem i sig selv giver risiko for identitetstyveri. Opbygningen af økosystemet tager således højde for de sikkerhedsmæssige udfordringer ved at der er indbygget en række sikkerhedsmæssige tiltag i kraft af Datatilsynets rolle samt NemID og anvendelsen heraf til en række offentlige og private selvbetjeningsløsninger. Disse vil dog med fordel kunne styrkes yderligere.

Behov som følge af sikkerhedsudfordringerne

For at sikre en samordnet indsats for sikkerhed på tværs af hele cpr-økosystemet, så er der behov for en myndighed, der har entydigt ansvar for sikkerheden, herunder ansvar for brugen af personnumre i anvenderlaget og kontrol med distributionsregistre