Identitetsbaserede web services og personlige data

IT- og Telestyrelsen
Ministeriet for Videnskab
Teknologi og Udvikling

>

Identitetsbaserede web services og personlige data

Udgivet af:
IT- & Telestyrelsen

IT- & Telestyrelsen
Holsteinsgade 63
2100 København Ø

Telefon: 3545 0000
Fax: 3545 0010

Nederst foto på forsiden:

Publikationen kan hentes
på IT- & Telestyrelsens
Hjemmeside: http://www.itst.dk
ISBN (internet):

>

Identitetsbaserede web services og personlige data

Version 1.1

IT- & Telestyrelsen
marts 2010

Indhold >

Indledning

>

Identitetsbaserede web services er en særlig slags web services, der kaldes samt opererer på vegne af en bruger. Som eksempler kan nævnes en brugers kalenderservice, der gør det muligt at booke en aftale med brugeren, eller en service, der eksponerer en borgers skatteoplysninger til brug i offentlige myndigheders selvbetjeningsløsninger.

OIO identitetsbaserede web services (herefter OIOIDWS) er et sæt af web service profiler udviklet af IT- og Telestyrelsen, der er målrettet den offentlige sektor. OIOIDWS gør det bl.a. muligt at udbyde services, som eksponerer personlige data fra offentlige registre på en sikker og standardiseret måde, hvilket er nødvendigt for digitalisering af en række tværgående sagsgange.

Et eksempel på en proces, der kræver indhentning af data fra flere myndigheder, er ansøgning om vognmandstilladelse hos Færdselsstyrelsen. Her skal borgeren uden digitalisering igennem en langsommelig, papirbaseret proces med at indhente oplysninger fra SKAT, Politiet, Motorkontoret, Erhvervs- og Selskabsstyrelsen mv. hvorefter disse indsendes til Færdselsstyrelsen, hvor sagsgangen primært består i at kontrollere oplysningerne fra de andre myndigheder, inden tilladelsen kan udstedes. Er der fejl eller mangler i de indsendte formularer, må sagsbehandlingen midlertidigt afbrydes, og borgeren må forsøge igen. Hvis borgerens data kunne indhentes automatisk via services hos de relevante myndighederne, ville det medføre store gevinster både for borgeren og myndighederne.

En forudsætning for, at data kan deles er naturligvis, at det juridiske, tekniske og sikkerhedsmæssige grundlag er i orden. OIOIDWS giver et højt niveau af sikkerhed for både borgere og myndigheder i forhold til mere traditionelle integrationsformer. Eksempelvis kan en service kun kaldes, når borgeren er logget ind hos den applikation, der anmoder om data. Dette giver borgerne en høj grad af tryghed for, at udleveringen af data kun sker, når de har tilgået en selvbetjeningsløsning, der har brug for data. Endvidere giver det den dataansvarlige/udleverende myndighed en tryghed for, at data kun frigives til applikationer, som rent faktisk er i gang med at betjene den pågældende borger.

Med OIO identitetsbaserede webservices bliver det således muligt at lette administration, når myndigheder skal sende/videregive oplysninger om en borger. Arbejdsgange, der tidligere har været udført ved anvendelse af blanketter, kan gøres elektroniske og give en stor administrativ lettelse.

OIOIDWS er et teknisk fundament baseret på interoperable profiler af internationale, åbne standarder. Konceptet og arkitekturen kan realiseres med gængse udviklingsværktøjer og platforme, og der er vide muligheder for tilpasning af konceptet og arkitekturen til den konkrete situation.

Målgruppe

Dette dokument er henvendt til offentlige myndigheder, der ønsker at anvende identitetsbaserede web services baseret på OIOIDWS profilerne til at udveksle data. Dokumentet kan læses af beslutningstagere, projektledere og IT arkitekter med interesse for digitalisering. Der berøres således både forretningsmæssige, juridiske og tekniske problemstillinger i relation til deling af data. Dokumentet er introducerende,

og der henvises til de underliggende profildokumenter for tekniske detaljer for detaljer om juridiske forhold i forhold til persondataloven henvises til www.datatilsynet.dk.

Afgrænsning

Dette dokument tager afsæt i en situation, hvor en myndighed videregiver data til en anden myndighed på vegne af en borger. Det juridiske fokus retter sig imod selve videregivelsen af data fra en myndighed til en anden.

Vejledningen omhandler ikke digital signering af dokumenter og aftalers bindende virkning.

Ved benyttelsen af OIOIDWS forudsættes endvidere, at der ikke sker sammenkøring af data. I stedet anvendes konceptet til at fremsende oplysninger i konkrete tilfælde fra en myndighed til en anden.

Vejledningen er ikke en gennemgang af de i persondataloven gældende behandlingsprincipper i den enkelte myndigheds systemer. Der er således stillet skarpt på det scenarie, som retter sig imod anvendelse af OIOIDWS.

I forhold til videregivelsen vil der blive set på tilfælde, der omfatter fortrolige og følsomme persondata. Videregivelse af almindelige personoplysninger vil ikke blive særskilt behandlet, da reglerne vil kunne opfyldes af samme sikkerhedsniveau som for fortrolige oplysninger.

Definitioner og begreber

>

Videregivende myndighed
Betegnelsen er valgt ud fra persondatalovens begreber (også kendt som personoplysningsloven). Det er den myndighed, der har ansvar og råderet over data, og som giver data til en tredjepart til deres selvstændige brug. Den videregivende myndighed er dataansvarlig.

Modtagende myndighed
Den myndighed, som modtager data. I denne vejledning modtages data til myndighedens eget selvstændige brug, og den modtagende myndighed er derfor også dataansvarlig efter persondatalovens regler.

Den registrerede
Term i persondataloven som henviser til den, der er registreret personoplysninger om. I forhold til de her opstillede scenarier vil den registrerede være den enkelte borger.

Databehandling
I persondatalovens forstand er en behandling læsning, registreringen, opbevaring, brug, videregivelse og sletning af data. Dermed omfattes al anvendelse af data.

Web Service Provider (WSP)
Dette er den tekniske komponent hos den videregivende myndighed, som udstiller data via web services.

Web Service Consumer (WSC)
Dette er den tekniske komponent (typisk en del af en applikation) hos den modtagende myndighed, som henter data via kald til web services.

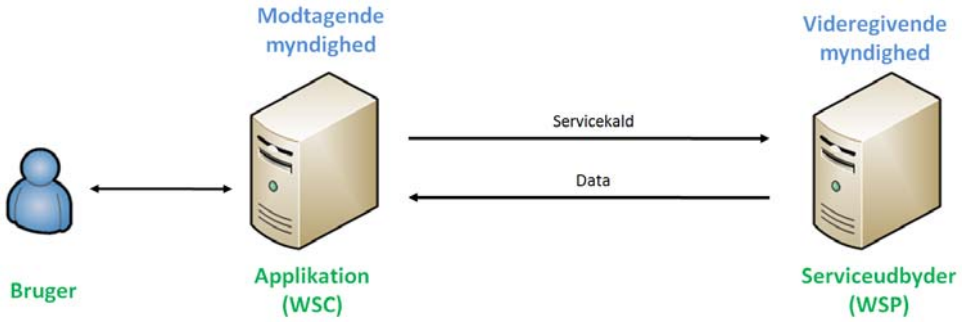
Applikation
Applikationen stiller funktionalitet til rådighed for brugeren, som kan anvendes efter login. Applikationen har brug for at kalde en identitetsbaseret web service hos en fremmed myndighed på vegne af brugeren – eksempelvis med det formål at hente data om brugeren. Typiske eksempler på applikationer er web applikationer / portaler, som tilgås via en browser, eller tykke klienter, der er installeret på brugerens PC.

Bruger
Brugeren er en fysisk person (f.eks. borger eller sagsbehandler), som anvender en applikation. Brugeren har akkreditiver i form af eksempelvis en digital signatur, som anvendes til at logge på applikationen. Når borgeren, som bruger, tilgår egne data betragtes myndigheden som databehandler, og der er her ikke en videregivelse af data, da det er borgeren selv, som styrer dette (som egen access). Dette scenarie falder udenfor vejledningen.

Udtrykkeligt samtykke
Med udtrykkeligt samtykke menes en frivillig, specifik og informeret viljestilkendegivelse, hvor borgeren indvilger i behandling af egne oplysninger.

Der gælder ikke noget formkrav til samtykket, men bevisbyrden påhviler den dataansvarlige og det anbefales, at samtykke afgives skriftligt, evt. via de muligheder den elektroniske løsning giver herfor.

Samtykket skal være konkretiseret så det klart og utvetydigt fremgår, hvad det er, der meddeles samtykke til, herunder, hvilke typer af oplysninger, der må behandles, hvem der kan foretage behandling af oplysningerne og til hvilke formål.



Figur 1: De vigtigste elementer i OIOIDWS

Logintjeneste (Identity Provider)
Dette er en ekstern tjeneste, som forestår autentificering af brugeren for applikationer. Et eksempel er NemLog-in.

Security Token Service (STS)
En Security Token Service er en tjeneste, der kontaktes af applikationer for at få udstedt ”adgangsbilletter” (security tokens) til brug for kald til eksterne web services. Et security token identificerer brugeren, hvilken applikation der må anvende tokenet, samt hvilken service, det er udstedt til.

Scenarier

>

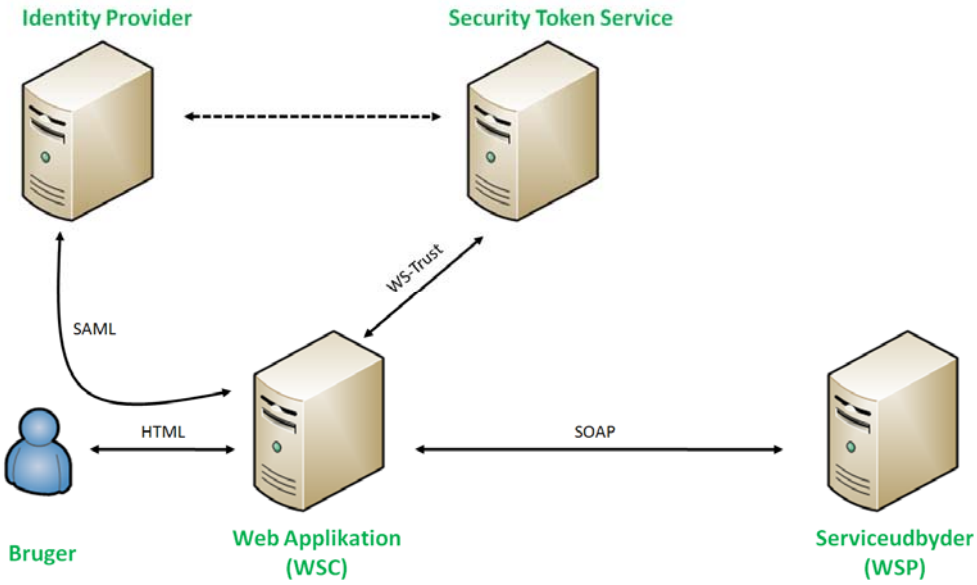
I dette kapitel beskrives en række scenarier, der illustrerer brugen af OIOIDWS konceptet. Scenarierne er valgt, så de viser typiske brugsmønstre i den offentlige sektor indenfor digital forvaltning. Beskrivelsen er overordnet, og der henvises til OIOIDWS profilerne for tekniske detaljer.

Scenarie med browser og ekstern logintjeneste

Nedenstående figur viser et scenarie med en borger, der anvender en browser mod en web-baseret selvbetjeningsapplikation (eller portal) hos en offentlig myndighed. Borgeren autentificerer sig med en digital signatur via en ekstern logintjeneste (som f.eks. NemLog-in). Applikationen får brug for at hente data om borgeren hos en fremmed myndighed via en identitetsbaseret web service, og anvender herefter disse data til betjeningen af borgeren – et eksempel kunne være indhentning af oplysninger som anvendes til behandling af en ansøgning fra borgeren. Til det formål kontakter applikationen en STS for at få udstedt en ”adgangsbillet” (security token) til servicen. Trinene i scenariet er som følger:

1. Borgeren tilgår en selvbetjeningsapplikation via sin browser.
2. Applikationen kræver autentifikation af borgeren og videresender derfor browseren til en ekstern logintjeneste (f.eks. NemLog-in).
3. Logintjenesten autentificerer borgeren via dennes digitale signatur[1] og udsteder herefter en SAML assertion, der identificerer borgeren overfor applikationen. Den udstedte SAML assertion indeholder endvidere et såkaldt ”bootstrap token”, der kan anvendes i det videre forløb (se næste trin).
4. Applikationen får på et senere tidspunkt brug for at kalde en fremmed identitetsbaseret web service på vegne af borgeren – f.eks. med det formål at hente dennes personlige data. Applikationen anmoder derfor en såkaldt Security Token Service (STS) om at få udstedt en ”adgangsbillet” (security token) til den fremmede web service. Applikationen angiver hvilken web service, der ønskes kaldt, og medsender borgerens bootstrap token for at indikere, hvem kaldet skal ske på vegne af.
5. STS’en validerer requestet samt bootstrap tokenet og foretager evt. en autorisationsbeslutning samt evt. et opkald til logintjenesten for at sikre, at brugeren stadig har en aktiv session. Hvis alt går godt udstedes og returneres et nyt token til applikationen, der kan anvendes mod den ønskede web service.
6. Applikationen kalder den fremmede identitetsbaserede web service på vegne af borgeren; kaldet signeres og tokenet udstedt af STS’en medsendes.
7. Web servicen validerer tokenet og udfører servicekaldet på vegne af borgeren. Svaret signeres inden det returneres.
8. Applikationen anvender data i svaret fra serviceudbyderen i det videre forløb.

[1] Hvis borgeren allerede har en session med logintjenesten overspringes autentifikationen og der kan udstedes en SAML assertion direkte (dvs. brugeren oplever single sign-on).



Figur 2: Scenarie med browserklient

Forudsætningerne for ovenstående scenarie er bl.a.:

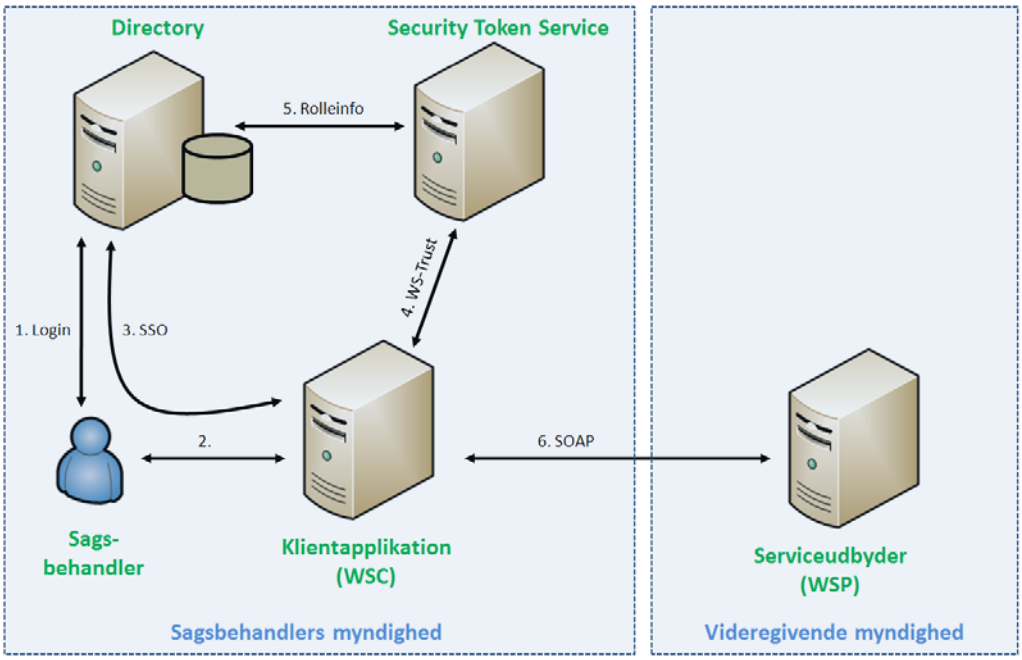
- Borgeren er i besiddelse af akkreditiver (f.eks. en OCES digital signatur), hvormed han kan autentificere sig overfor logintjenesten (Identity Provider).
- Logintjenesten udsteder en SAML assertion indeholdende et bootstrap token, som STS'en kan forstå.
- Web applikationen er i besiddelse af en digital signatur (f.eks. OCES virksomhedssignatur), hvormed den kan autentificere sig overfor STS og WSP.
- STS'en er i besiddelse af en digital signatur hvormed den kan signere tokens.
- Serviceudbyderen (WSP) er i besiddelse af en digital signatur, hvormed svar kan signeres.
- Applikation (WSC) og Serviceudbyder (WSP) stoler begge på STS'en og kan validere de tokens, den udsteder.

Det er *ikke* en forudsætning, at applikation (WSC) og serviceudbyder (WSP) stoler på hinanden og kender hinandens certifikater på forhånd.

>

Scenarie med rig klient og lokal STS

I det næste scenarie er brugeren en sagsbehandler i en offentlig myndighed, der fra en desktop applikation installeret på hans computer har brug for at tilgå data i en anden offentlig myndighed. Brugeren logger på applikationen via netværkslogin på hans arbejdsplads, og en Security Token Service internt hos myndigheden udsteder et security token, der indeholder information om de roller, brugeren er tildelt. Med dette token kan en applikation tilgå den eksterne web service.



Figur 3: Scenarie med rig klient

Trinene i scenariet er som følger:

1. Brugeren logger på det lokale netværk / directory (f.eks. Active Directory) hos myndigheden, når arbejdsdagen begynder.
2. Brugeren starter en klientapplikation på sin PC.
3. Klientapplikationen logger automatisk brugeren på (single sign-on).
4. Klientapplikationen har brug for at kalde en identitetsbaseret web service hos en anden myndighed og anmoder derfor STS'en om et security token.
5. STS'en slår op i directory'et og undersøger hvilke roller/rettigheder/grupper, brugeren er associeret med. STS'en foretager evt. en oversættelse af disse roller i forhold de applikationsroller, som den aktuelle web service forventer.
6. Applikationen foretager kaldet til den ønskede service og medsender det udstedte token. Web servicen validerer tokenet og udfører servicekaldet med de roller/rettigheder, der fremgår af tokenet. Svaret signeres inden det returneres. Applikationen anvender data i svaret fra serviceudbyderen i det videre forløb.

Forudsætningerne for ovenstående scenarie er bl.a.:

- Brugeren er i besiddelse af akkreditiver (f.eks. brugerid/password eller OCES medarbejdersignatur), hvormed han kan autentificere sig på det lokale netværk.

- Applikationen er i besiddelse af en digital signatur (f.eks. OCES virksomhedscertifikat eller funktionscertifikat), hvormed den kan autentificere sig overfor web servicen.
- STS'en er i besiddelse af en digital signatur, hvormed den kan signere tokens.
- Serviceudbyderen (WSP) er i besiddelse af en digital signatur, hvormed svar kan signeres.
- Serviceudbyderen stoler på myndighedens STS – herunder at de medsendte roller er korrekte i forhold til sagsbehandlerens arbejdsfunktion, og at sagsbehandleren er blevet korrekt autentificeret på det lokale netværk.
- STS'en har viden om hvilke applikationsroller, web servicen forventer at modtage, og kan evt. oversætte interne brugerroller fra directory'et til disse.
- Brugeren er tildelt brugerroller i directory'et – f.eks. af myndighedens brugeradministratorer.

Sikkerhedsmæssige og juridiske egenskaber

>

I dette kapitel beskrives en række sikkerhedsmæssige egenskaber, der opnås ved at anvende OIOIDWS - herunder en række af de fordele IDWS giver sammenlignet med mere traditionelle integrationsformer. Egenskaberne sættes i relation til relevante juridiske forhold ved dataudveksling.

Egenskab 1: Den kaldende applikation er autentificeret, og integriteten af kaldet er sikret
Den myndighed, der henter data, skal signere web service kaldet med et certifikat. Anvendes OCES virksomhedscertifikater eller -funktionscertifikater opnår den videregivende myndighed en høj grad af sikkerhed for, hvem den kaldende myndighed er. Desuden sikrer den digitale signatur, at kaldet ikke kan modificeres dvs. integriteten er sikret.

Juridisk har dette betydning for, at myndigheden der videregiver data kan stole på, at data sendes frem til den rigtige myndighed. Dermed giver konceptet den videregivende myndighed sikkerhed for, at data kan afsendes til modtager myndigheden.

Egenskab 2: En betroet tredjepart står inde for, at brugeren er logget på
Brugerens identitet fremgår af et såkaldt sikkerhedstoken, der er udstedt af en betroet tredjepart, og som medsendes i web service kaldet. Dette token kan kun udstedes såfremt borgeren, som bruger, er logget på, og da det er signeret med en betroet tredjeparts signatur, kan det ikke forfalskes eller modificeres.

I brugerens token findes en attribut (assurancelevel), der fortæller hvor sikkert brugeren loggede på Identity Provideren. Værdien er et tal i intervallet 1-4, hvor den nuværende OCES signatur indplaceres på niveau 3; se mere i [AUTH-LEV]. På den måde kan myndigheden, der videregiver data, vurdere hvor stærkt brugeren er autentificeret, og lade dette indgå i beslutningen om, hvorvidt data frigives.

Juridisk giver denne egenskab sikkerhed for, at borgeren, som er den registrerede efter persondataloven, er korrekt identificeret og at myndigheden har ret til at tilgå den service, som kaldes på vegne af borgeren. Der gøres opmærksom på, at de videregivende myndigheder altid bør overveje nøje, hvilke services de vil lade modtagende myndigheder tilgå. Desuden bør det overvejes, hvordan det styres, at sagsbehandleren hos modtagende myndighed kun kan tilgå de sager, som er af arbejdsmæssig relevans. Denne egenskab kan fremgå af det udstedte token (via et såkaldt *claim*), således at den modtagende myndighed (via sin STS) overfor den videregivende myndighed står inde for, at sagsbehandleren er tilknyttet den pågældende sag.

Egenskab 3: Data er krypterede under transport
OIOIDWS anvender sikre transportkanaler (SSL / TLS) med stærk kryptering, så data kan ikke aflyttes af uvedkommende under transport. Dermed opnås konfidentialitet af kommunikationen.

Da både SSL og TLS protokollerne kan anvendes med forskellige krypteringsalgoritmer, hashalgoritmer og forskellige nøglelængder, er det vigtigt, at man ikke anvender svage algoritmer eller nøgler. Dette opnås konkret ved at

konfigurere web servere til at kun at anvende stærk kryptering med anerkendte algoritmer (eksempelvis AES med 128 bit nøgler eller bedre).

Når der anvendes stærk kryptering, som bygger på anerkendte algoritmer, opfyldes persondatalovens krav til kryptering af data, der sendes over Internet, og dette er tilstrækkeligt til både fortrolige og følsomme personoplysninger.

Egenskab 4: OIOIDWS Tokens sikrer at adgang gives begrænset
Et token udstedt af en betroet tredjepart er indrettet, så det kun kan anvendes i et kort tidsrum af den applikation, det er udstedt til[2], og kun til den service, det er beregnet til. Der kan implementeres en adgangspolitik, der begrænser hvem der kan få tokens til hvilke services.

Persondataloven stiller krav om, at kun de data, som er nødvendige, behandles. OIOIDWS kan hjælpe med at begrænse adgangen til data på serviceniveau. Det betyder, at den videregivende myndighed kan definere, hvilke services den modtagende myndighed kan tilgå og derved undgå, at der gives adgang til andre services, som kan indeholde oplysninger om borgeren (den registrerede), som den modtagende myndighed ikke har behov for.

Egenskab 5: Web servicen er autentificeret og integriteten af svaret er sikret
Svaret fra web servicen hos den videregivende myndighed er signeret med et certifikat. Anvendes OCES virksomhedscertifikater eller -funktionscertifikater opnås en høj grad af sikkerhed for, hvem den videregivende myndighed er, herunder at de sendte data er korrekte. Endvidere betyder signaturen, at svaret ikke kan modificeres, hvilket sikrer integriteten.

Egenskab 6: Kald til web service kan logges som bevis
Web servicen kan logge kald til den som et kryptografisk sikret bevis på, at den har udleveret data (og hvilke) på baggrund af en legitim anmodning fra en fremmed myndighed; for detaljer om signaturbeviser henvises til [SIG-BEV].

Det er muligt for de dataansvarlige myndigheder at opsætte logning på deres webservices. Behandles fortrolige eller følsomme personoplysninger, stilles der i sikkerhedsbekendtgørelsen krav om, at tilgang og behandling af personoplysningerne logges. Behovet for logning af kald til webservicen bør vurderes op imod den logning, som myndigheden i øvrigt foretager og det it-sikkerhedsniveau, som løsningen skal imødekomme. I forbindelse med logning er det vigtigt at huske, at logningen i sig selv er en behandling af persondata, hvor det skal overvejes hvilke oplysninger der er nødvendige og logge.

Egenskab 7: Svar fra web service kan logges som bevis
Applikationen kan logge svaret fra web servicen som et kryptografisk sikret bevis på, hvilke data den modtog – dette kan eksempelvis være relevant, når afgørelser træffes

[2] Tokenet er bundet til applikationens signatur via ”holder-of-key” mekanismen i SAML.

på baggrund af data modtaget fra fremmede myndigheder; for detaljer om signaturbeviser henvises til [SIG-BEV].

Det er muligt for de dataansvarlige myndigheder at opsætte logning på deres web services. Behandles fortrolige eller følsomme personoplysninger, stilles der i sikkerhedsbekendtgørelsen krav om, at tilgang og behandling af personoplysningerne logges. Behovet for logning af svaret fra webservicen bør vurderes op imod den logning, som myndigheden i øvrigt foretager og det it-sikkerhedsniveau, som løsningen skal imødekomme. I forbindelse med logning er det vigtigt at huske, at logningen i sig selv er en behandling af persondata, hvor det skal overvejes hvilke oplysninger der er nødvendige og logge.

Egenskab 8: Samtykke fra borger
Når der er behov for udtrykkeligt samtykke fra borgeren (som den registrerede) til at videregive data, er det muligt at benytte protokollen ”Request to interact”, som er beskrevet i OIOIDWS. I praksis betyder dette, at den videregivende myndighed beder den kaldende applikation om at sende brugerens browser over til en bestemt adresse, hvor et samtykke fra borgeren kan indhentes, inden web service kaldet udføres, og data frigives til applikationen. Efter indhentet samtykke sender den videregivende myndighed browseren tilbage til applikationen.

Ved udveksling af følsomme personoplysninger uden direkte lovhjemmel, skal udtrykkeligt samtykke indhentes. I ”request to interact” protokollen sker dette ved, at borgeren sendes hen til den videregivende myndigheds applikation, hvor samtykke til at netop de udbedte oplysninger gives. OIOIDWS giver altså en teknisk viderestillingsmekanisme, men det er op til myndigheden selv at udforme, indhente og lagre samtykker, så det giver mening i den konkrete sammenhæng.

Rent praktisk kan man overveje at give den registrerede en mulighed for at underskrive den udtrykkelige samtykkeerklæring med sin digitale signatur. I den forbindelse er det vigtigt at kommunikere tydeligt, hvilke data, samtykket giver ret til videregivelse af.

Egenskab 9: Det er muligt at sætte et sikkerhedsniveau, der matcher det konkrete behov
Flere elementer i arkitekturen er åbne og kan indstilles efter det konkrete behov. Det gælder f.eks. timeout perioder, tilladte akkreditiver, adgangspolitikker, granularitet af adgange, certifikatpolitikker mv. Med udgangspunkt i den konkrete situation defineres de acceptable værdier, som er afstemt med det ønskede sikkerhedsniveau alt efter den konkrete anvendelse, herunder om der udveksles almindelige, fortrolige eller følsomme personoplysninger, se definitionen herfor under afsnittet Juridiske forhold.

Det er op til den enkelte myndighed at definere et niveau, som passer med de personoplysninger der udveksles, og så det hele tiden følger den praksis, der er for sikkerhedsopsætninger. Kravene til sikkerhed kan udvikle sig over tid, og af denne grund er persondatalovens krav beskrevet teknik-neutralt. Den sikkerhed, som vil give tilstrækkelig beskyttelse af oplysningerne afhænger af, hvad der til enhver tid kan anses for god it-sikkerhed set i forhold til, hvor følsomme oplysninger der udveksles.

Profiler i OIOIDWS

OIOIDWS består af en række profiler af en række internationale standarder bl.a. fra OASIS og Liberty Alliance. Nedenfor findes en oversigt over disse profiler, og deres roller forklares. Der henvises til profildokumenterne for tekniske detaljer.

Profil	Anvendelse
Liberty Basic SOAP Binding [LIB-BAS]	Denne profil af standarden ”Liberty ID WSF 2.0 SOAP Binding” beskriver hvad et web service kald fra en Web Service Consumer til Web Service Provider skal indeholde samt regler for behandling. Profilen detaljerer udseendet af SOAP meddelelsen med særlig vægt på SOAP headere, foreskriver transportniveau, kryptering, signering af meddelelsen og medsendelse af security tokens. Profilen kan udvides med ”Request to Interact” protokollen fra den overliggende Liberty standard, som gør det muligt for web servicen at bede applikationen om at sende brugerens browser til en specifik URL – hvor brugerens samtykke til frigivelse af data så kan indhentes.
OIO WS-Trust Profile [OIO-WST]	Denne profil af ”OASIS WS-Trust 1.3” standarden beskriver hvorledes en applikation kan anmode om at få udstedt et security token med henblik på et efterfølgende web service kald for en bruger. Profilen beskriver alene beskedformatet for de meddelelser, der udveksles (ligesom WS-Trust standarden).
OIO WS-Trust Deployment Profile [OIO-WST-DEP]	Denne profil specificerer en række tekniske detaljer i forbindelse med deployment af OIO WS-Trust profilen i en dansk kontekst. Bl.a. beskrives en konkret ”binding” til SOAP via ”Liberty Basic SOAP Binding”, der refereres til danske profiler vedr. indhold af tokens samt brug af danske attributter defineret i OIOSAML, og endelig anbefales brug af OCES certifikater.
OIO Identity Token Profile [OIO-IDT]	Denne profil beskriver indholdet af de security tokens (i form af SAML 2.0 assertions) som udstedes af en STS til brug for et efterfølgende servicekald.
OIO Bootstrap Token Profile [OIO-BOOT]	Denne profil beskriver en særlig attribut, der kan indlejres i en SAML assertion opnået via en browser fra en Identity Provider (se næste profil). Attributten rummer et såkaldt ”bootstrap token”, der kan anvendes til at identificere brugeren overfor en STS, når der anmodes om et security token. Boostrap tokenet udtrækkes konkret af applikationen og anvendes i WS-Trust kaldet mod STS’en.
OIOSAML Web SSO Profile [OIO-SAML-SSO]	Denne profil af SAML 2.0 standarden beskriver web SSO scenariet, hvor brugeren via sin browser logger på en applikation (Service Provider) ved brug af en logintjeneste (Identity Provider) udbudt af en tredjepart (f.eks. NemLog-

>

	in). Profilen beskriver bl.a. hvorledes en række danske attributter, som befindes sig i brugerens OCES certifikat, kan repræsenteres i den udstedte SAML assertion.

Kontrol af aktiv brugersession

I dette kapitel dykkes ned i en af de tekniske detaljer omkring udstedelsen af security tokens fra STS'en i OIOIDWS, der har betydning for sikkerhed og arkitektur.

Ideelt set skal en STS kun udstede et security token til en kaldende applikation, hvis brugeren er logget ind hos den applikation, der anmoder om tokenet, og hos den Identity Provider, der gav adgang til applikationen. Derfor vil det være optimalt, hvis STS'en kan kalde Identity Provideren og forespørge, om brugeren (stadig) har en aktiv session. Imidlertid er der ikke nogen standardiseret protokol til dette, og kontrollen kan derfor ikke realiseres uden mere eller mindre proprietære integrationer mellem STS og IdP.

Det overlades derfor til de enkelte dataansvarlige myndigheder at foretage en risikovurdering som afdækker, hvorvidt der er behov for real-time information om brugerens session. På den måde kan integrationen udelades, når den ikke er absolut nødvendig. Endvidere opfordres fællesoffentlige Identity Providere til at udbyde en grænseflade, hvormed STS'er kan forespørge om sessionsstatus for en bruger.

I nogle sammenhænge stilles en Identity Provider og en STS op ved siden af hinanden i samme organisation (f.eks. som to dele af et fælles softwareprodukt), og i den forbindelse kan det være lettere at foretage integrationen. Her anvendes betegnelsen at IdP og STS er ko-lokerede.

I tilfælde hvor STS'en ikke har adgang til at forespørge Identity Provideren om brugerens aktuelle sessionsstatus, må der tages en beslutning om hvorvidt tokenet kan udstedes ud fra informationerne i bootstrap tokenet. Her vil være angivet et tidspunkt for, hvornår brugeren loggede på Identity Provideren (Assertion/AuthnStatement@AuthnInstant), samt hvornår brugeren fik udstedt den SAML assertion, som gav adgang til applikationen (Assertion@IssueInstant). Med disse informationer kan STS'en definere en timeoutpolitik, der begrænser hvor længe efter disse tidspunkter applikationen kan hente security tokens og dermed tilgå services på brugerens vegne. I princippet kunne brugeren jo have logget ud på Identity Provideren efter at have tilgået applikationen. Jo kortere denne timeout periode sættes, jo tættere mindre bliver vinduet, hvor services kan kaldes uden sikkerhed, for at brugeren ikke har logget ud. Omvendt vil en for kort periode medføre byrder for applikationen om hyppigt at forny (web SSO) tokens hos Identity Provideren (og dermed forny bootstrap tokens).

Det overlades til de enkelte myndigheder at definere en passende timeout periode, som afvejer følsomheden af konkrete data mod byrderne ved hyppige fornyelser af tokens.

Juridiske forhold

>

Regulering

Den regulering, der er i forhold til selve persondataloven er relevant for videregivelsen af borgerens data, er listet i nedenstående tabel. Listen har til formål og give et overblik over de krav som stilles i persondataloven og som uddybes i underliggende retskilder og standarder. På specialområder er der ofte særregler for persondatabeskyttelse, og de skal naturligvis overholdes på de enkelte områder. Når disse giver bedre beskyttelse end persondataloven, er det specialreglerne der skal følges.

Det er vigtigt, at der inddrages jurister i de enkelte projekter, da retsområdet er komplekst. Dette afsnit repræsenterer udelukkende et kortfattet og generelt overblik.

Den tungeste kilde er loven, som gælder for alle myndigheder og private virksomheder. Den næste kilde, der er angivet, er sikkerhedsbekendtgørelsen, som er direkte gældende for den offentlige forvaltning, og som uddyber sikkerhedskravene i persondataloven. De efterfølgende kilder er vejledninger og standarder for sikkerhed, der har vejledende karakter og er med til at fastsætte god praksis for behandling af personoplysninger.

Regulering og standarder	Hvornår
Persondatalov: Lov om behandling af personoplysninger Nr. 429 af 31/5 - 2000	Når der udveksles persondata. Der er forskellige krav til behandlingen alt efter om det drejer sig om eksempelvis et navn eller om det er udveksling af eksempelvis straffeattest eller sygdomsoplysninger. Forkortes som PDL og omtales persondataloven.
Sikkerhedsbekendtgørelsen Nr. 528 af 15/6-2000.	Når der udveksles persondata indenfor det offentlige. Bekendtgørelsen uddyber tekniske og administrative krav til persondataloven.
Vejledning til bekendtgørelse nr. 528 af 15. juni 2000	Vejledning omkring sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.
Datatilsynets afgørelser og publikationer	Datatilsynet har tilsynet med Persondataloven. Derfor skal den praksis og de udtalelser, som Datatilsynet fremkommer med tages med, når kravene i persondataloven skal overholdes. Se mere på: www.datatilsynet.dk
DS484:2005	It-sikkerhedsstandard, som efter statslig beslutning skal følges indenfor staten. Her omhandler afsnit 15 privacy og er relevant i forhold til de identitetsbaserede webservices
ISO/IEC CD 29100 – under udarbejdelse	Information technology -- Security techniques -- A privacy framework. Standarden er under udarbejdelse, men er relevant I forhold til dens indgangsvinkel på identity management.

Persondataloven

Der stilles krav til, hvordan personoplysninger behandles, og groft opdelt kan det siges, at der arbejdes indenfor følgende 4 hovedområder:

- Administrative/organisatoriske krav til behandlingssikkerhed.
- Den registreredes rettigheder.

- Anmeldelse til Datatilsynet.
- Teknisk sikkerhed.

Kravene retter sig imod al behandling af data, fordi en databehandling i persondatalovens forstand vedrører al brug af data. Det betyder, at læsning, registreringen, opbevaring, brug, videregivelse og sletning alt sammen er databehandlinger. Ingen behandlinger går derfor fri, men kravene til procedurer og sikkerhed bliver større eller mindre alt efter datas klassifikation, dvs. alt efter om data er almindelige, fortrolige eller følsomme.

Internettet er et åbent netværk, og det er hverken sikkert eller lovligt i forhold til persondataloven at sende fortrolige eller følsomme personoplysninger uden ekstra sikkerhedsforanstaltninger over Internet.

OIOIDWS kan give den tekniske sikkerhed, når myndighed skal sende oplysninger sikkert over Internet. Den enkelte myndighed skal dog stadig sikre, at anvendelse af personoplysningerne internt i myndigheden opfylder persondatalovens ikke tekniske krav.

I det følgende fokuseres på de krav i persondataloven og sikkerhedsbekendtgørelsen, som retter sig specifikt mod de scenarier, som OIOIDWS understøtter, nemlig videregivelse af oplysninger fra en myndighed til en anden via web services over internettet.

Omdrejningspunktet vil være it-sikkerheden og dermed persondatalovens § 41, stk. 3 som lyder:

*"Stk. 3. Den dataansvarlige skal træffe de fornødne **tekniske** og **organisatoriske** sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt **tilintetgøres, fortabes** eller **forringes**, samt mod, at de kommer til **uvedkommendes kendskab**, **misbruges** eller i øvrigt **behandles i strid med loven**. Tilsvarende gælder for databehandlere."*

Kravene til sikkerheden skærpes alt efter datas klassifikation, og generelt kan data i forhold til persondataloven klassificeres i følgende 3 kategorier:

Følsom		**Almindelig -Fortrolig**		**Almindelig – ikke fortrolig**
PDL § 7	**PDL § 8**	**PDL § 11**	**PDL§ 6**	**PDL§ 6**
Racemæssig / etnisk baggrund, politisk, religiøs, eller filosofisk overbevisning, fagforeningsforhold, seksuelle forhold, helbredsmæssige forhold. Eksempel hvis der er angivet registreret partnerskab.	Strafbare forhold, væsentlige sociale problemer, andre rent private forhold. Eksempel herpå er selvmordsforsøg, bortvisning fra job.	CPR-nummer.	Private oplysninger om eks. økonomi, hemmelig adresse, skatteforhold, gæld, sygedage, tjenestelige forhold og familieforhold	Bolig, bil, eksamen, ansøgning, ansættelsesdato, stilling, arbejdsområde, arbejdstelefon, stamoplysninger. Eksempler er Navn, adresse og fødselsdato.

>

Klassificeringen af oplysningerne er ikke et lovkrav men et nyttigt praktisk redskab, når man skal lave en risikovurdering der klarlægger, hvor høj et niveau af it-sikkerhed, der er nødvendigt.

Når myndigheden skal klassificere personoplysningerne, vil der altid være tale om en konkret vurdering, som det påhviler den dataansvarlige myndighed at foretage. For eksempel vil oplysninger om en borgers adresse kunne være en fortrolig oplysning, hvis borgeren har navne- og adressebeskyttelse efter CPR-loven. Et CV kan indeholde fortrolige eller følsomme oplysninger om f.eks. den registreredes karakterer eller personnummer eller andet. Det er derfor vigtig at tage aktivt stilling til de oplysninger myndigheden behandler og kun anvende nedenstående skema som hjælp til klassificeringen.

Når data er blevet inddelt i en af de 3 kategorier – følsom, almindelig-fortrolig og almindelig – ikke fortrolig - kan man ud fra klassifikationen se, hvilken tyngde der skal ligge på it-sikkerheden og kontrollerne med behandlingen af data.

Kravene, der skal opfyldes er styret af, hvorvidt det er anmeldelsespligtigt at behandle disse, se mere herom på www.datatilsynet.dk. Helt overordnet kan følgende generelle tommelfingerregler opstilles for de enkelte klassifikationer:

Generelle krav		
Følsom	**Almindelig –fortrolig**	**Almindelig – ikke fortrolig**
Der er et generelt forbud mod at dele data medmindre der er lovhjemmel eller udtrykkeligt samtykke fra borger. Med udtrykkeligt menes, at samtykkes skal gives af en borger, der er tydeligt oplyst om data der skal behandles, formål hvem der kan behandle og anvendelse. Desuden bør det udtrykkelige samtykke være givet skriftligt, så der ingen tvivl er om omfanget og det efterfølgende kan dokumenteres. Der stilles store krav til såvel administrativ som teknisk sikkerhed. Der skal ske anmeldelse til Datatilsynet og borgerens ret til eksempelvis at se og rette data skal sikres.	Der stilles krav til sikkerheden såvel teknisk som administrativt. Ikke alle behandlinger af fortrolige data skal anmeldes til Datatilsynet, men forholdet skal undersøges. Borgerens ret til eksempelvis at se og rette data skal sikres.	Der stilles ikke så store sikkerhedskrav til almindelige persondata, men husk, at kun nødvendige oplysninger må behandles. Behandlingen er omfattet af persondataloven. Behandlingen skal generelt ikke anmeldes til Datatilsynet. Borgerens ret til eksempelvis at se og rette data skal sikres.

For at stille skarpt på de forhold, der er væsentlige når internettet anvendes til at videregive data, er kravene uddybet i listen nedenfor, der tager udgangspunkt i persondatalovens behandlingsregler i kapitel 4 samt det generelle sikkerhedskrav i persondatalovens § 41. Listen fokuserer særligt på de krav som OIOIDWS løsningen kan hjælpe med at opfylde.

Gennemgangen er således ikke en fuldstændig liste over krav til sikkerheden og behandlingen af personoplysninger, det anbefales derfor at der inddrages juridisk assistance tidligt i projektforløbet, for at få opstillet de konkrete krav den enkelte

myndighed i det enkelte tilfælde skal overholde.

OIOIDWS kan således bidrage med tekniske egenskaber, der hjælper med overholdelsen af personoplysningsloven, men det er den enkelte myndigheds ansvar at sikre, at opsætning sker korrekt og at behandlingen af personoplysningerne også sikres igennem organisatoriske tiltag.

Krav der vedrører den enkelte myndigheds interne administration af data såsom relevans og saglighedskriterier efter PDL § 5 medtages overordnet, borgerens rettigheder såsom indsigelse og indsigt, og den enkelte myndigheds anmeldelse til Datatilsynet er **ikke medtaget,** da det ikke har sammenhæng med anvendelsen af OIOIDWS til videregivelse af data.

I kolonnen til højre kommenteres kravet i forhold til OIOIDWS.

Krav	OIOIDWS
A. Behandlingshjemmel	
PDL § 5	PDL § 5 kræver overholdelse af god databehandlingsskik. De principper der ligger bag og som videregivende og modtagende myndighed skal have i mente er: *Et sagligt formål med behandlingen *Kun relevante og proportionale data behandles * Data opdateres *Data opbevares kun så længe det er nødvendigt, derefter skal ske anonymisering/arkivering/sletning. I øvrigt henvises til Datatilsynets praksis herom.
Databehandling og videregivelse er lovlig (PDL §§ 5, 6,7,8 og 11)	Videregivende myndighed skal sikre hjemmel til videregivelsen ved udtrykkeligt samtykke fra borgeren eller ved tilladelse i lov. For følsomme og fortrolige data, der videregives på baggrund af udtrykkeligt samtykke, skal det være, så vidt muligt specificeres, hvilke oplysninger der videregives, hvem data videregives til. Kravene til uafviselighed vil være mest tungtvejende ved følsomme data. Bevisbyrden for samtykket påhviler den dataansvarlige.
Retsinformationssystemer PDL § 9	Følsomme personoplysninger kan behandles, hvis dette sker med henblik på at føre retsinformationssystemer af væsentlig samfundsmæssig betydning.

>

Krav	OIOIDWS
	Dette vil navnlig være systemer, som er til rådighed for en bredere kreds af abonnenter for at sikre en ensartet retsanvendelse. Det kan blandt andet være en myndigheds offentliggørelse af afgørelser på myndighedens hjemmeside eller i **Retsinformation** eller offentliggørelse af domme i et tidsskrift. Behandlingen skal samtidig være nødvendig for førelsen af systemerne.
Statistiske og videnskabelige undersøgelser PDL §10	Bestemmelsen giver en udvidet mulighed for at behandle følsomme personoplysninger, hvis dette sker til statistiske eller videnskabelige formål af samfundsmæssig betydning.
Adresserings- og kuverteringsbureauer § 12	Ikke relevant i forhold til IOIIDWS løsningen, da denne vedrører offentlige myndigheder. Adresserings- og kuverteringsbureauer er særligt reguleret i bestemmelsen, som nævnes for at medtage hele kap 4 i persondataloven
Registrering af telefonnumre PDL § 13	Ikke relevant i forhold til OIOIDWS løsningen, men nævnes for at medtage hele kap 4 i persondataloven.
Arkivering PDL § 14	Bestemmelsen giver hjemmel til at overføre data til arkivering.
Data behandles sikkert PDL § 41, stk. 3	OIOIDWS krypterer data ved afsendelsen og sikrer, at afsenderen kan have tillid til modtagermyndighedens og borgerens identitet. Niveauet af sikkerhed kan justeres i konceptet alt efter hvordan opsætning sker af eksempelvis timeout, adgangspolitiker, certifikatpolitiker mv.
Logning af adgang og behandling af fortrolige personoplysninger (sikkerhedsbekendtgørelsen §§ 15, 18 og 19)	Pligten til logning af adgang og behandling af personoplysninger omfatter de oplysninger der er omfattet af anmeldelsespligten til Datatilsynet – groft sagt fortrolige oplysninger. Se evt. nærmere om anmeldelsespligten i Datatilsynets vejledning nr. 125 af 10. juli 2000. **Servicekald** kan logges ved brug af IDWS konceptet. Det er den enkelte dataansvarlige myndighed der skal sikre, at egne webservices sættes op, så den nødvendige logning af tilgang og brug af fortrolige og følsomme

Krav	OIOIDWS
	personoplysninger foretages. Der skal som minimum sikres logning af: *Tidspunkt (kan kræve synkronisering af ure på tværs af systemer). *Bruger (den ID som logges, skal kunne hæftes på en person, og må dermed ikke være en "anonym" token). *Anvendelse. *Angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. *Afviste adgangsforsøg desuden skal der ske blokering ved gentagne afviste forsøg
Tildelte adgange er i overensstemmelse med arbejdsmæssigt betingede behov. (sikkerhedsbekendtgørelsen §§12 og 16 autorisation og adgangskontrol).	Hver myndighed skal sikre, at de medarbejdere, der tilgår data, er autoriserede til det. OIOIDWS giver mulighed for at tilknytte roller til medarbejderne, så det sikres, at de må bruge systemet – herunder er autoriserede til kald af web services i fremmede myndigheder. Det er ikke muligt at automatisere det organisatoriske krav, som altid vil gælde uanset hvilken teknisk løsning der vælges.
Tildelte brugeradgange revurderes halvårligt (sikkerhedsbekendtgørelsen § 17)	Hver myndighed skal følge op på medarbejdernes autorisationer.
Procedure for sikring af eksterne kommunikationslinier er udarbejdet og kryptering (Sikkerhedsbekendtgørelsen § 14)	OIOIDWS profilerne foreskriver stærk kryptering.
Medarbejdere instrueres om hvorledes behandling af data skal ske.(PDL § 41, stk. 1)	OIOIDWS sørger for at der er vejledninger tilgængelige, men hver myndighed har pligten til at instruere egne medarbejdere.
B. Den registreredes rettigheder	
Den dataansvarliges har opfyldt sin oplysningspligt.	I scenariet bestiller borgeren videregivelsen af oplysningerne, og der gives et SAML token med som dokumentation for at borgeren bestiller data til en bestemt modtager myndighed. Det er dog vigtig at være sikker på, at borgeren ved hvilke data, der indsamles hos den modtagende myndighed.

Krav	OIOIDWS
	Modtager og afsender myndighed kan aftale, hvem der sikrer, at borgeren modtager oplysninger omkring, hvilke data der er videresendt til hvilken myndighed, og hvem der er ansvarlig i forhold til rettigheder omkring indsigelse, berigtigelse og indsigt.

Bevismæssige forhold

Bevismæssige forhold er væsentlige at have for øje, når en sagsgang omlægges fra papir til et digitalt medie. Det er også tilfældet ved benyttelsen af OIOIDWS.

I scenariet er der en myndighed, der videregiver (afsender) data, og en som modtager.

Logningen af tilgang og brugen af data er en vigtig del af dokumentationen for det sagsforløb, myndigheden har ansvaret for. Det gælder for den myndighed, der afsender data helt frem til det tidspunkt, hvor data videregives, og for den modtagende myndighed fra det tidspunkt, hvor data modtages.

I forhold til den enkelte borger, som er den registrerede efter persondataloven, er det væsentlige at have for øje, at det udtrykkelige samtykke, som borgeren afgiver, efterfølgende skal kunne bevises.

For nærmere information henvises i øvrigt til IT- og Telestyrelsens udgivelse ”Signatur- og systembevis - Teknisk vejledning i sikring af digitale signaturers bevisværdi.” [SIG-BEV].

Ansvar

Såvel videregivende som modtagende myndighed har ansvar og opgaver, når persondataloven skal overholdes.

Ses der på ansvaret i forhold til den afgivende myndighed, som er dataansvarlig for de oplysninger, der videregives, så er det den videregivende myndighed som skal sikre, at der er hjemmel i lov eller via borgerens udtrykkelige samtykke til at videregive oplysningerne.

Da modtagermyndigheden generelt skal anvende data til egne selvstændige formål, vil modtagermyndigheden efter modtagelse af oplysningerne være ansvarlig for den fremadrettede behandling af data.

Formålet med denne anvendelse af OIOIDWS er derfor ikke, at den ene myndighed skal være databehandler på vegne af den anden. Derimod skal data til den videregives til den modtagende myndigheds eget brug.

Det ansvar, som i forbindelse med videregivelsen af data påhviler den videregivende myndighed, er blandt andet, at:

- Sikre klassifikation af data dvs. om det er almindelige, fortrolige eller følsomme persondata.
- Sikre hjemmel til videregivelsen eksempelvis i forbindelse med udtrykkeligt samtykke fra borgeren eller ved tilladelse i lov.
- Sikre at videregivelsen sker til den rigtige myndighed - dette understøtter OIOIDWS.
- Sikre at medarbejdere er korrekt autoriserede til at anvende OIOIDWS konceptet. OIOIDWS konceptet understøtter dette med mulighed for rolletildeling.
- Sikre at modtageren er den rigtige. OIOIDWS konceptet sørger for anvendelse af certifikater, så dette understøttes.
- Sikre at der er historik i forhold til adgangen af data dvs. den enkelte myndighed skal sikre opsætning af logning.
- Sikre at borgeren er orienteret om videregivelse af data, når der er pligt til det.
- Sikre at data er korrekte.

Det ansvar, som påhviler den dataansvarlige myndighed som modtager data, er blandt andet, at:

- Oplyse borgeren om hvilke data, der er behov for at indsamle.
- Sikre at medarbejdere er korrekt autoriserede til at anvende data. OIOIDWS understøtter dette med mulighed for rolletildeling.
- Sikre at der er historik i forhold til adgangen af data dvs. den enkelte myndighed skal sikre opsætning af logning.

Referencer

>

[DTT]	http://www.datatilsynet.dk/offentlig/internettet/udveksling-af-oplysninger-i-portaler/
[OIO-WST]	“OIO WS-Trust Profile V1.0”, Danish IT and Telecom Agency.
[OIO-WSTDEP]	”OIO WS-Trust Deployment Profile V1.0”, Danish IT and Telecom Agency.
[OIO-IDT]	“OIO SAML Profile for Identity Tokens, V1.0”, Danish IT and Telecom Agency.
[OIO-BOOT]	“OIO Bootstrap Token Profile V1.0”, Danish IT and Telecom Agency.
[OIO-SAML-SSO]	“OIO Web SSO Profile V2.0”, Danish IT and Telecom Agency.
[LIB-BAS]	“Liberty Basic SOAP Binding Profile”, version 1.0, Liberty Alliance Project.
[LIB-SOAP]	”Liberty IDWF 2.0 SOAP Binding”, Liberty Alliance Project.
[WST]	”WS-Trust 1.3”, OASIS Standard.
[SIG-BEV]	”Signatur- og Systembevis – teknisk vejledning i sikring af digitale signaturers bevisværdi”, IT- og Telestyrelsen. http://www.itst.dk/arkitektur-og-standarder/infrastruktur-og-felles-losninger/brugerstyring/signatur-og-systembeviser
[SSL]	”SSL 3.0 Specification”: http://www.freesoft.org/CIE/Topics/ssl-draft/3-SPEC.HTM
[TLS]	”The Transport Layer Security (TLS) Protocol Version 1.2”, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc5246.txt
[OCES-CP]	https://www.signatursekretariatet.dk/certifikatpolitikker.html
[AUTH-LEV]	”Vejledning vedrørende niveauer af autenticitetssikring”. http://www.itst.dk/arkitektur-og-standarder/Standardisering/standarder-for-serviceorienteret-infrastruktur/standarder-for-brugerstyring/filer-til-standarder-for-brugerstyring/Horing.B.st.niv.autenticitetssikring.v5.pdf