Udvikling af administrativ funktionalitet til versionsstyring af samtykker

Peter Enevoldsen
21. december 2017

Afrapportering af projektet ”Etablering af fundamentet for Big Data i landbruget”, arbejdspakke 1.1. ”Sikring af personfølsomme data”

SEGES
Landbrug & Fødevarer F.m.b.A.
Agro Food Park 15, DK 8200 Aarhus N
+45 8740 5000 info@seges.dk
seges.dk CVR 25529529

Indholdsfortegnelse

Resume 3
Begreber 3
- Consentor 3
- Subject 3
- DPO - Data Protection Officer 3

Oversigt over funktionsændringer i SEGES Aftalesystem 3
- Nyt navn 3
- Fleksibel aftaleskabelon 3
- Styrke dokumentation af indgåede aftaler 3
- Web interface til administration af aftaler 5
- Option: "Overgang uden invalidering" 5

Designprincipper og krav til fagsystemerne 5
Forslag til øvrige aktiviteter i projektet 6

Udvikling af administrativ funktionalitet til versionsstyring af samtykker

Resume

I forbindelse med indførelse af den kommende EU-forordning stilles der skærpede krav i forbindelse med indhentning og dokumentation af samtykker, når disse indhentes til brug for behandling af personoplysninger. For at imødekomme disse krav er der tilføjet ny funktionalitet til den "aftaleløsning" som SEGES tidligere har udviklet til indhentelse af samtykker fra brugere af de landbrugsfaglige løsninger og databaser som SEGES driver. Med ændringerne bliver det nu muligt at validere brugerens tilknytning til en given landbrugsvirksomhed – og dermed sikre at brugeren har en legitim ret til at indgå samtykket for virksomheden - via CVR-nummeret. Ligeledes bliver det muligt at håndtere og dokumentere forskellige versioneringer samtykketekster.

Begreber

Consentor
Den der accepterer aftalen (f.eks. en indlogget bruger)

Subject
Den som aftalen gælder for (f.eks. et CVR nummer).

DPO - Data Protection Officer
Rolle i SEGES specielt udpeget til at kunne vurdere og afgøre aftale- og persondataspørgsmål.

Oversigt over funktionsændringer i SEGES Aftalesystem

Nyt navn
Systemet skifter navn fra "SEGES Samtykkesystem" til "SEGES Aftalesystem". Systemet omhandler brugeres godkendelse af aftaletekster og er ikke snævert målrettet aftaleformen "Samtykker". For at minimere udgiften og sikre fortsat konsistens retter vi ikke dette i koden, hvor "consent" begrebet fortsat anvendes som udtryk for en aftale.

Fleksibel aftaleskabelon
Aftaleskabelonen er i dag hårdt bundet til "Samtykker". I stedet for fast definerede felter og faste overskrifter, ændres templaten til at være ét stort indholdsfelt. Hermed bliver systemet fleksibelt overfor forskellige aftaleformers layout og indhold. Titel, godkendelsesstatus og funktionsknapper er fortsat faste.

Styrke dokumentation af indgåede aftaler
Med udvidelsen af aftaleskabelonen som beskrevet ovenfor gemmes hele aftaleteksten fremover (i dag gemmes kun den rå tekst eksklusiv de fast definerede overskrifter). Desuden vil denne fremover blive dato signeret, så det kan dokumenteres, at teksten ikke er ændret efter afgivelsen.

Nye valideringstyper for aftaler
En aftale kan i dag have valideringstypen ”DLI”.

Valideringstype	”DLI”
Consentor	DLI BrugerID
Subject	DLI BrugerID
Aftalesystemet sikrer	Aftalen kan kun accepteres/afvises af den indloggede bruger. Den indloggede bruger = den DLI BrugerID, der er anført som ønsket Consentor.
Fagsystemet sikrer	At valideringstype ”DLI” er juridisk dækkende til formålet

Denne valideringstype er tænkt til at understøtte aftaler om brugsvilkår – eksempelvis accept af, at der gemmes adfærdstracking på brugerprofilen.

Fremover kan en given aftale også valideres med følgende typer:

Valideringstype	”CVR” – CVR via brugerID
Consentor	DLI BrugerID
Subject	CVR nummer
Aftalesystemet sikrer	Aftalen kan kun accepteres/afvises af den indloggede bruger. Den indloggede bruger = den DLI BrugerID, der er anført som ønsket Consentor. DLI BrugerID er valideret med det CVR nummer, der er anført som ønsket Subject. Ved efterfølgende afvalidering bliver aftalen ugyldig.
Fagsystemet sikrer	At valideringstype ”CVR” er juridisk dækkende til formålet

Valideringstype	”NemID” – CVR via Penneo
Consentor	NemID
Subject	CVR nummer
Aftalesystemet sikrer	Uafklaret
Fagsystemet sikrer	At valideringstype ”NemID” er juridisk dækkende til formålet

Fælles for disse to nye valideringstyper er at aftalen gælder for et CVR nummer. Dette er tænkt til situationer, hvor der arbejdes med virksomhedsinformationer, der kan være omfattet af persondataloven og derfor kræver et specielt samtykke og validering.

For valideringstypen ”CVR” afgives samtykket af den indloggede DLI bruger og aftalesystemet kontrollerer, at CVR nummeret er valideret af brugeren – og sikrer at aftalen annulleres ved efterfølgende afvalidering.

Valideringstypen ”NemID” er tænkt til situationer, hvor samtykker indhentes af DLBR virksomhederne via Penneo med NemID signatur, og efterfølgende indlæses i SEGES Aftalesystemet. Her er den krævede underskriver (consentor) for CVR nummeret identificeret af DLBR virksomheden.

Web interface til administration af aftaler
Hidtil har retningslinjen for SEGES Aftalesystemet været, at selv den mindste rettelse i aftaleteksten krævede genindhentelse af alle indgåede aftaler. SEGES Ansvar & Skade vurderer, at såfremt ændringer er uden juridisk betydning, kan teksten rettes uden

Vi anbefaler at der udvikles et web interface til dette, for at sikre

- At ændringer i aftaler kun kan foretages af bemyndigede personer (DPO'er) der er garanter for, at rettelsen er uden juridisk betydning og reelt kan ske uden genindhentelse
- At ændringer versioneres og logges
- At oprettelse af en ny aftale kun kan udføres af en DPO, og at denne er garant for at aftalen juridisk er dækkende for anvendelsen i fagsystemet, herunder at fagsystemet anvender valideringstyperne korrekt.

Option: "Overgang uden invalidering"
Ovenævnte funktionsrettelser vil kræve, at alle aftaler for alle fagsystemer skal indhentes igen. Det må forventes, at dette vil ske ind i mellem, når der er "breaking changes" i systemet. En option kunne være at lave et setup, hvor dette kan undgås: Vi opretter en backup database med en kopi af alle samtykkeafgivelser og historikken på disse. Den nye database, der understøtter de nye funktioner, vil alene have "autoriteten" på de historiske samtykker gemt (peger på backup databasen). Hermed kan systemet udvides uden genindhentelse, men udtræk af dokumentation/historik på historisk afgivne samtykker, vil i forbindelse med en tvist til gengæld skulle slås op i den gamle kopi database (en udvikleropgave).

Designprincipper og krav til fagsystemerne

Det centrale designprincip i SEGES Aftalesystemet er, at den juridiske og forretningsmæssige vurdering af hvilke aftaler der skal indhentes, samt hvornår dette skal ske og med hvilken valideringstype, ligger i fagsystemerne. Aftalesystemet kan ikke vurdere, om en given valideringstype for en aftale er tilstrækkelig til den anvendelse fagsystemet påtænker. Indhenter fagsystemet aftalen med en utilstrækkelig valideringstype, er der ikke noget teknisk, der eksploderer, hvorfor fejlen nemt kan gå under radaren.

Det samme hvis flere systemer deles om en aftale. Aftalen kan være indhentet af System X med valideringstype "DLI", men System Y kræver juridisk valideringstypen "CVR". Spørger System Y om brugeren har accepteret med valideringstype "CVR" vil aftalesystemet svare nej. Men hvis System Y spørger om brugeren har accepteret med valideringstype "DLI" vil aftalesystemet svare ja. System Y skal her selv konstatere, at dette ikke er tilstrækkeligt, og efterfølgende indhente aftalen med den rette valideringstype.

Korrekt håndtering af aftaler stiller derfor store krav til den tekniske og juridiske viden hos bemandingen på fagsystemerne og fagområdernes DPO.

Forslag til øvrige aktiviteter i projektet

- ”Brandøvelse”
  Opstille konflikt/tvist scenarier og prøve disse af mod aftalesystemet. Juridisk kyndig udfordrer systemet og vi fremlægger dokumentation.

- Backup/restore øvelse

- Udarbejdelse af vejledning til aftagende systemer
  Vores forslag er at DPO’erne er tovholdere på implementering eller ændring af aftaler i fagsystemerne. Valideringstyperne stiller som nævnt ovenfor skærpede krav til fagsystemernes anvendelse af aftalesystemet. Vi anbefaler derfor, at der bliver udarbejdet en juridisk og teknisk vejledning i af SEGES aftalesystemet.

- Review af CVR valideringsprocessen
  - Er den tilstrækkelig i forhold til persondataforordningen?