KOMBIT
Kommunernes it-fællesskab

NOTAT

SAPA
SAPA & Privacy by Design og Default - dataminimering

1. Indledning

KOMBIT modtager jævnligt spørgsmål til SAPAs overholdelse af Databeskyttelsesforordningen, herunder dataminimering og privacy by design og default, og generelt til forordningens artikel 25 og 32.

De mere tekniske sikkerhedsforanstaltninger i SAPA er beskrevet i databehandleraftalernes bilag 1, men KOMBIT vil med dette notat nærmere beskrive de overordnede principper for de mere funktionelle foranstaltninger, vi har foretaget i SAPA i forhold til databeskyttelse gennem design og standardindstillinger for at understøtte kommunerne i at sikre dataminimering.

2. Baggrund

SAPAs standardindstillinger og designvalg skal bl.a. bidrage til at sikre, at personoplysninger ikke kommer til uvedkommendes kendskab, og at der generelt praktiseres dataminimering for at beskytte de registreredes rettigheder. Kravet følger nu af Databeskyttelsesforordningen artikel 25, men beskyttelse af personoplysninger og fleksibel mulighed for dataafgrænsning har i hele processen omkring specificering og udvikling af SAPA været i fokus.

KOMBIT udarbejdede allerede i 2012 et notat omkring det påtænkte setup for adgangsstyring og beskyttelse af personoplysninger i SAPA, som indgik i en dialog med Datatilsynet om SAPA. Notatet blev udarbejdet på konceptniveau, og før SAPA blev kravspecificeret, udbudt og udviklet.

En række antagelser og forudsætninger fra notatet er fortsat relevante, en række er ændret og andre igen er løst på en anden måde teknisk.

Med dette notat samler KOMBIT op på den etablerede SAPA-løsning i forhold til principper for databeskyttelse gennem design og standardindstillinger for at understøtte dataafgrænsning og -minimering.

3. Kommunens rolle

Pligten til at sikre databeskyttelse gennem design og standardindstillinger påhviler de dataansvarlige, hvilket i forhold til SAPA er kommunerne.

KOMBIT ser det som sin opgave at sikre, at løsningen fra start er bygget til, at kommunen under hensyn til de kriterier der fremgår af Databeskyttelsesforordningen, kan iagttage databeskyttelse gennem design og standardindstillinger i forhold til dataminimering.

Det er derimod kommunens opgave konkret at udmønte det skøn over dataafgrænsning for de enkelte medarbejdere, som opsætningsmulighederne i SAPA giver mulighed for.

4. Principper for databeskyttelse gennem design og standardindstillinger i SAPA i forhold til dataminimering

KOMBIT bidrager til at sikre databeskyttelse gennem design og standardindstillinger i SAPA ved at følge disse principper:

PRINCIP 1: Restriktive standardindstillinger

KOMBIT arbejder i SAPA med udgangspunkt om at gøre standardindstillinger for data i SAPA så restriktive/dataminimerende som muligt, naturligvis under hensyn til de forretningsmæssige behov. Ved standardindstillinger forstås de indstillinger for adgang til data, der er i SAPA, når kommunen eller brugeren tager løsningen i brug, hvis ikke kommunen eller brugeren aktivt ændrer dem. Dette princip er både anvendt i den eksisterende funktionalitet og anvendes ved videreudvikling.

- Som et generelt eksempel på dette kan nævnes, at en bruger ikke kan se andet end basisoplysninger fra CPR (primært navn og adresse), når brugeren tilgår SAPA, hvis ikke brugeren særskilt er blevet tildelt rettigheder til sager på et eller flere KLE-numre.

- Et andet eksempel er, at SAPA, selvom brugeren har rettigheder til at se tværgående bemærkninger, først viser indholdet af en tværgående bemærkning om borgeren, når brugeren aktivt klikker på den tværgående bemærkning. Herved sikres, at denne type data om borgeren kun vises, hvis sagsbehandleren har vurderet, at der er behov for det i den konkrete situation.

Standardindstillingerne er ikke udtryk for, at kommunerne generelt bør undlade at udvide rettighederne, men blot et sikkerhedsnet sådan, at udvidede rettigheder kræver en aktiv handling, og man ikke ”kommer til ” at give en medarbejder for brede rettigheder. Det er meningen, at kommunerne skal udvide rettighederne, så de passer til den enkelte medarbejders opgaver.

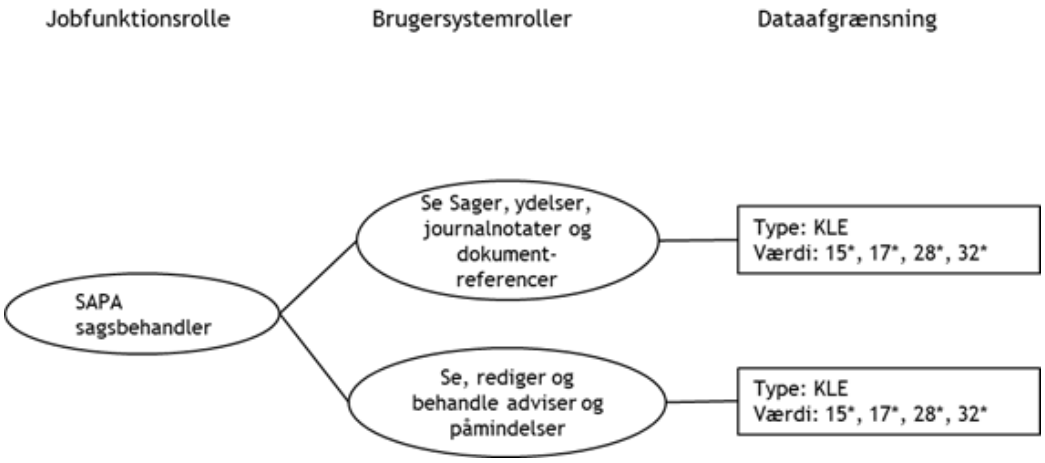
PRINCIP 2: Differentiering

Hvor der er mulighed for det, skal adgangen til SAPAs funktionalitet og data i SAPA kunne differentieres, så kommunerne har mulighed for at praktisere en høj grad af differentiering i dataadgange mellem de forskellige brugere.

Generelt er dataafgræsningen i SAPA bygget op omkring jobfunktionsroller og brugersystemroller.

En jobfunktionsrolle er et sæt af rettigheder, der gør det muligt for en medarbejder at udføre en funktion i SAPA. En jobfunktionsrolle kan fx være 'Administrator', 'Sagsbehandler' eller 'Kontrolmedarbejder'. En jobfunktionsrolle består af et sæt af brugersystemroller, som hver især yderligere kan gradueres ved en dataafgrænsning. En medarbejder kan have flere forskellige jobfunktionsroller. Jobfunktionsrollerne defineres af kommunen selv, mens brugersystemrollerne er defineret af KOMBIT og Netcompany.

Nedenstående figur skitserer sammenhængen mellem jobfunktionsrolle, brugersystemroller og dataafgrænsning.



Eksemplet i figuren er bygget op omkring en jobfunktionsrolle, som er navngivet "SAPA sagsbehandler". Jobfunktionsrollen er defineret ved to brugersystemroller "Se sager, ydelser, journalnotater og dokumentreferencer" og "Se, redigér og behandle adviser og påmindelser". Begge brugersystemroller er yderligere defineret ved en dataafgrænsning af typen KLE med værdien 15*, 17*, 28*, 32*.

Dataafgrænsning er det tredje led af afgrænsningen og det redskab, der kan sikre, at medarbejdere har adgang til netop de data, der er nødvendige for at udføre deres arbejde. Man kan sige, at dataafgrænsning kan anvendes til at tilpasse en brugersystemrolle til individuelle og organisatoriske behov. Dataafgrænsning foregår på brugersystemrolleniveau, og der findes 4 typer af dataafgrænsning, hvoraf KLE-emneområde er den primære:

- KLE-emneområde
- Følsomhed
- IT-system
- Organisatorisk Enhed

PRINCIP 3: Vejledning og videndeling

KOMBITs vejledning til kommuner om brug af jobfunktionsroller, brugersystemroller, dataafgrænsninger og andre databeskyttelsesemner skal sikre, at kommuner hjælpes til at efterleve GDPRs databeskyttelsesprincipper. KOMBIT hjælper desuden kommunerne med at vidensdele omkring dette, så man kan søge inspiration hos nogen, der sidder med de samme opgaver.

KOMBITs vejledning til opsætningen af løsningen suppleres desuden af den generelle vejledning fra KL om informationssikkerhed.

Principperne suppleres af konkret vejledning til kommunerne om,

- Hvordan kommunerne selv kan ændre standardindstillingerne, så der vises flere informationer
- Hvilket ansvar kommunerne har i den forbindelse mht. at sikre, at kun relevante data vises.

PRINCIP 4: Sletning, når behovet er forbi

SAPA sikrer, at data ikke lagres i SAPA længere end det er nødvendigt for brugerens opslag, dvs. at data, der læses fra andre steder, fx registre og indekser, kun gemmes i den tid, det skal bruges til brugerens konkrete søgning.

SAPA indfører desuden automatiske slettepolitikker for det data, som ikke længere anvendes, men som hører til i SAPA og ikke hentes fra andre steder, fx. brugernes gemte søgninger, påmindelser og tværgående bemærkninger, der er udløbet.

5. Principperne i praksis

KOMBIT anvender principperne både ved udvikling af ny funktionalitet på SAPA, men også i en løbende sikkerhedsevaluering af den eksisterende løsning, hvor vi bl.a. vurderer, om der er behov for nye eller ændrede brugersystemroller.

KOMBIT, 8. juli 2019.