
ELEKTRONISK LÅSESYSTEM

Arbejdsgangsbeskrivelse for eksterne leverandørs
brug af borgers elektroniske låsesystem i eget hjem

Indhold

1	Indledning	3
2	Samtykkeerklæring	3
3	Oprettelse af eksterne leverandør	4
3.1	Leder ved ekstern leverandør sender oplysninger til Aarhus Kommune	4
3.2	Aktivering af EXT-bruger	4
3.3	Adgangsgivende tilknytning i Microsoft Azure	4
3.4	Opsætning af to-faktor-godkendelse	4
3.5	Opsætning af Phonirol	5
4	Ophør af eksterne ydelser og sletning af adgang	5

1 Indledning

Arbejdsgangsbeskrivelsen for eksterne leverandørs brug af borgers elektroniske låsesystem i eget hjem (herefter arbejdsgangsbeskrivelsen) beskriver, hvilke processer, der skal følges, for at sikre borgerens databeskyttelse, når eksterne leverandører ønsker at benytte sig af borgerens elektroniske låsesystem i forbindelse med levering af varer eller ydelser.

Arbejdsgangsbeskrivelsen er kun gældende ved de elektroniske låsesystemer, der er installeret af Sundhed og Omsorg (MSO).

Adgang til opgangsdøre kræver ikke en samtykkeerklæring fra borgeren, da det udelukkende er bygningens fælles areal, der gives adgang til.

Eksterne leverandør anses som værende leverandører, der leverer følgende ydelser til borgeren:

- Dagligvarer
- Medicin
- Tøjvask
- Madservice

2 Samtykkeerklæring

Samtykkeerklæringen skal kun bruges, hvis en ekstern leverandør ønsker at benytte det elektroniske låsesystem til at levere de aftalte varer og/eller tjenesteydelser i borgerens bopæl uafhængigt af Aarhus Kommunes hjemmepleje. Adgang til opgangsdøre kræver ikke en samtykkeerklæring fra borgeren.

Samtykkeerklæringen beskriver borgerens reelle valg og giver dem kontrol over, hvordan dennes oplysninger bruges.

Borgeren eller dennes stedfortræder skal underskrive side et på samtykkeerklæringen. Side to skal borgeren beholde. Hvis borgeren ønsker en kopi af side et, sikres dette imødekommet af den, der har indhentet underskriften.

Samtykkeerklæringen kan indhentes af den eksterne leverandør eller udekørende medarbejdere fra Sundhed & Forebyggelse eller Pleje og Rehabilitering. MSO indhenter kun samtykket for de eksterne leverandører, hvis det vurderes relevant og ikke medfører en væsentlig tidskrævende ekstraopgave for MSO.

Når borgeren eller dennes stedfortræder har underskrevet, scannes/tages et billede af samtykkeerklæringen, der sendes som sikker/digital mail til Systemejerskab-datasikkerhed@mso.aarhus.dk og Hasse Eriksen (he@ostbv.dk) ved Østjyllands Brandvæsen (ØJB).

- Der kan først gives adgang til eksterne leverandører, når samtykkeerklæringen er modtaget ved Østjyllands Brandvæsen. Samtykkeerklæring til underskrift kan downloades på <https://aarhus.dk/elaas>
- Samtykket kan også indhentes digitalt, og automatisk sendes til systemejer og Østjyllands Brandvæsen, hvis borger logger ind på følgende link med sit MitID: <https://selvbetjening.aarhuskommune.dk/da/content/samtykkeerklæring-phoniro>
Det er afgørende at det er borgeren MitID der logges ind med.

3 Oprettelse af eksterne leverandør

Det elektroniske låsesystem køres via app på Android og iOS enheder. Det er den eksterne leverandørs eget ansvar at anskaffe og vedligeholde det nødvendige udstyr, hvis de vil benytte sig af det elektroniske låsesystem.

Alle eksterne medarbejdere, der skal anvende løsningen, skal tilgå systemet gennem Aarhus Kommunes loginløsning, der autentificerer den enkelte bruger. Nedenfor beskrives processen for oprettelse af en ny ekstern bruger.

3.1 Leder ved ekstern leverandør sender oplysninger til Aarhus Kommune

- Der sendes en mail til Systemejerskab-datasikkerhed@mso.aarhus.dk med medarbejderens
 - Fornavn
 - Efternavn
 - Arbejdsmail (ekstern) (til at modtage invitationsmail)
 - Firmanavn
 - CVR-nummer.
- Hvis medarbejderen ikke har en arbejdsmail, kan lederens mail anvendes i den videre proces.

3.2 Aktivering af EXT-bruger

- Aarhus Kommune klagør en ny ekstern bruger på baggrund af fremsendte oplysninger, hvorefter medarbejderen modtager en mail med emnebeskrivelsen "**Du er inviteret som ekstern i Aarhus Kommune**". Hvis leders mail er anvendt til modtagelse, skal man være opmærksom på, at mailen er rettet mod medarbejderen, og at det **kun** er denne, der må igangsætte den videre proces.
- I ovenstående mail skal medarbejderen kopiere aktiveringskoden og dernæst trykke på "**Klik her for at starte**".
- Der åbnes en side hvorpå medarbejderen skal indsætte sin aktiveringskode og trykke "**Videre**".
- Medarbejderen modtager en ny mail med emnebeskrivelsen "**Du er oprettet som ekstern i Aarhus Kommune**". I mailen står medarbejderens brugernavn (mailadresse) og et link til opsætning af to-faktor-godkendelse.

3.3 Adgangsgivende tilknytning i Microsoft Azure

- Leder og/eller medarbejder sender ovenstående brugernavn (mailadresse) til Systemejerskab-datasikkerhed@mso.aarhus.dk, hvorefter Aarhus Kommune bestiller medlemskab i adgangsgivende gruppe.
- Mailadresse vil f.eks. se således ud: ext34481@aarhus.dk

3.4 Opsætning af to-faktor-godkendelse

- Medarbejderen trykker på linket i mail med brugernavn for at starte opsætning af to-faktor-godkendelse.
- Man kan alternativt tilgå denne side [Vendor - Aarhus Kommune \(service-now.com\)](https://vendor.aarhuskommune.com/service-now) til opsætning af to-faktor-godkendelse. "**Nulstil dit kodeord**" og "**Spær din brugerkonto**" skal/kan **kun** bruges på et

senere tidspunkt, hvis man til en fungerende bruger glemmer koden eller mistænker kompromittering.

- Medarbejderen skal nu følge vejledningen. Der skal være adgang til en computer, ens MitID og til en personlig arbejdstelefon – hvis medarbejderen ikke har dette, kan en privattelefon anvendes.

Det er vigtigt, at to-faktor-godkendelse opsættes på en **personlig telefon**, uanset om det er en arbejds- eller privattelefon, da man ikke kan koble flere brugere på Microsoft Authenticator app'en, der bruges til at godkende login.

3.5 Opsætning af Phoniro

- Leder og/eller medarbejder kontakter Hasse fra Østjyllands Brandvæsen mhp. opsætning af bruger og app. Østjyllands Brandvæsen sikrer korrekt brugeroprettelse, tilknytning samt registrering af enheden.
- Hasse kontaktes på telefonnummer 29685691 i hverdage i tidsrummet kl. 07.00-15.00.

4 Ophør af eksterne ydelser og sletning af adgang

Den eksterne leverandør er ansvarlig for at sikre at adgange er vedligeholdt løbende og bør gennemgå behovet for adgange årligt.

I tilfælde af at der er en adgang der ikke længere skal anvendes, skal leverandøren sende en mail til Systemejerskab-datasikkerhed@mso.aarhus.dk og Hasse Eriksen (he@ostbv.dk) ved Østjyllands Brandvæsen (ØJB). I mailen skal oplyses:

- Fornavn
- Efternavn
- Brugernavn/ext-mailadresse
- Firmanavn
- CVR-nummer