



Guide til brugeroprettelse på Datafordeler Administration

Drift og modernisering af Datafordeleren

Januar 2025

Version 1.2 – [24-01-2025](#)



Indholdsfortegnelse

1	Introduktion.....	3
2	Login.....	3
2.1	Login/oprettelse med e-mailadresse.....	3
2.2	Login/oprettelse med MitID.....	5
2.2.1	Yderligere NemLog-in roller	6
3	Brugerinformationer.....	6
3.1	Brugeroplysninger	6
3.2	Deaktivering af bruger	7
3.3	Automatisk deaktivering af brugerkonti.....	7
4	IT-system.....	7
4.1	Begrænsninger	7
4.2	Deling af IT-system.....	7
4.3	Ansøgning om adgang til beskyttede registerdata.....	9
4.3.1	Oprettelse/ansøgning af dataadgang	9
4.3.2	Visning, forlængelse og nedlæggelse af dataadgang	10
5	Autentificerings-metoder på Datafordeler Administration.....	11
5.1	Shared Secrets.....	11
5.2	Certifikater	13
5.3	API-Keys	14
6	IP-allowlist.....	16
7	Revisionslogs	16
7.1	Brugerlogs	16
7.2	IT-system logs	17



1 Introduktion

Denne guide henvender sig til alle anvendere, der skal hente data fra den moderniserede Datafordeler, hvor både brugerstyring og sikkerhedsmodellen er udviklet fra nyt. I den nye portal Datafordeler Administration er der nye arbejdsgange, hvorved anvendere kan oprette og vedligeholde adgang til data, med minimal kontakt til registre og Datafordelerens support.

2 Login

Bemærk, at der ikke er lavet brugermigrering fra den gamle administrationsportal til den nye Datafordeler Administration, så der er behov for at oprette nye brugere ved login.

Datafordeler Administration tilbyder login via e-mailadresse/adgangskode og login via MitID (erhverv og privat), som vises i Figur 1.

Kom godt i gang

Log ind på Datafordeleren ved at bruge dit brugernavn og password. Denne loginmetode giver dig hurtig adgang til platformens data og tjenester. Hvis du allerede har en konto, kan du indtaste dine loginoplysninger nedenfor. Hvis ikke, kan du nemt oprette en ny konto ved at registrere dig.

Du kan også logge ind med MitID for en sikker og nem adgang til Datafordeler.dk. MitID bekræfter din identitet på en pålidelig måde, så du slipper for at huske et separat brugernavn og password. Hvis du ikke har en konto endnu, kan du registrere dig med MitID og få adgang med det samme.

Log ind med Email/Password

Log ind med MitID

Figur 1: Login via e-mailadresse/adgangskode og MitID.

2.1 Login/oprettelse med e-mailadresse

Vælges der at logge ind med e-mailadresse/adgangskode bliver man viderestillet til loginsiden som fremgår af Figur 2.

Figur 2: Loginsiden for e-mailadresse/adgangskode.

Her kan der logges ind med en eksisterende bruger, som er oprettet på Datafordeler Administration, eller også kan man vælge at oprette en ny.

Klikkes der på "Opret Bruger" viderestilles der til en oprettelse side, som det ses i Figur 3.



Dansk v

* Nødvendige felter

Opret ny bruger

E-mail *


Adgangskode *

Bekræft adgangskode *

Fornavn *

Efternavn *

Telefon *

 +45 34 41 23 45

Organisation

Vilkår og betingelser

[Link til Privatlivspolitik](#)

[Link til Brugervilkår](#)

Jeg accepterer vilkår og betingelser

[« Tilbage til log ind](#)


Opret Bruger

Figur 3: Opret ny bruger siden.

Efter at have udfyldt de nødvendige oplysninger og klikket "Opret Bruger", vil der blive sendt en bekræftelse til den indtastede e-mailadresse. Der vises information om at verificering afventes, som vist i Figur 4.

Dansk v

Email verificering

 **Du skal verificere din email adresse for at kunne aktivere din konto.**

En email med instruktioner til, hvordan du verificerer din mail adresse er blevet sendt til dig.

Har du ikke modtaget en verificerings kode i din inbox?
[Klik her](#) for at gensende emailen.

Figur 4: E-mail verifikation.

Her er der mulighed for at gensende mailen, skulle der opstå problemer med f.eks. firewall eller andre sikkerhedsrelaterede blokeringer.

Bemærk, at det først er muligt at logge på når ens e-mailadresse er verificeret via linket der modtages.



2.2 Login/oprettelse med MitID

Vælges der at logge ind med MitID i form af MitID privat eller MitID erhverv er processen for login den samme.

Hvis brugeren allerede eksisterer i Datafordeler Administration fra tidligere login vil man automatisk blive logget ind efter at have indtastet sine MitID oplysninger via MitID integrationen.

I tilfælde af at brugeren ikke allerede eksisterer, vil man blive viderestillet til en oprettelse side, hvor de oplysninger MitID har, vil blive udfyldt automatisk og derfor ikke vises. Se Figur 5.

Dansk v

* Nødvendige felter

Update Account Information

Email *

Telefon *

+45 34 41 23 45

Indsend

Figur 5: Opret ny bruger MitID.

Når de ikke-automatiske felter er udfyldt kan der klikkes "Indsend" og der vil blive sendt en bekræftelse til den indtastede e-mailadresse. På samme måde som for e-mailadresse/adgangskode, skal man verificere den oprettede bruger før der kan logges ind. Indtil dette er gjort, vil information om verificering af e-mailadresse vises, se Figur 6.

Dansk v

Email verificering

⚠ Du skal verificere din email adresse for at kunne aktivere din konto.

En email med instruktioner til, hvordan du verificerer din mail adresse er blevet sendt til dig.

Har du ikke modtaget en verificerings kode i din inbox?
[Klik her](#) for at gensende emailen.

Figur 6: E-mail verifikation.

Her er der mulighed for at gensende mailen, skulle der opstå problemer med f.eks. firewall eller andre sikkerhedsrelateret blokeringer.

Bemærk, at det først er muligt at logge ind når ens e-mailadresse er verificeret via linket der modtages.



2.2.1 Yderligere NemLog-in roller

I forbindelse med IT-system-begrebet der bliver introduceret i næste sektion, så er der åbnet op for, at man som anvender kan få tildelt en NemLog-in rolle, der giver adgang til alle IT-systemer oprettet inden for ens organisation samt adgang til en oversigt over brugerne i organisationen og dertil mulighed for at deaktivere dem.

Denne rolle er tildelt og administreret igennem NemLog-ins eget system og derved noget en NemLog-in administrator for hver enkelt organisation kan styre.

Privilegie	Type	Funktion
Organisationsadministrator	NemLog-in Administrationssystem	Mulighed for at se alle IT-systemer inden for en organisation og videregive ejerskab, samt mulighed for at se alle brugerne inden for organisationen og deaktivere dem.

3 Brugerinformationer

3.1 Brugeroplysninger

Ens brugeroplysninger findes under menupunktet "Brugeroplysninger", som illustreret i Figur 7.

Brugeroplysninger

Brugeroplysninger

Vis revisionslog

E-mail* test2@test.dk Opdater E-mail

Fornavn* Thilde

Efternavn* Schmidt

Telefon* 11223344

Organisation

Gem Deaktiver bruger

Vis Bruger ID

Figur 7: Siden "Brugeroplysninger" viser brugeroplysninger på den bruger du er logget ind som.

På denne side er det muligt at opdatere kontaktoplysninger, se sit Bruger ID, samt at se en log over de handlinger man som bruger har udført.



3.2 Deaktivering af bruger

Skulle man som anvender ikke længere ønske at bruge sin bruger, kan man via siden "Brugeroplysninger" deaktivere sin bruger.

Dette gøres ved at klikke på "Deaktiver konto" knappen og derefter bekræfte at man ønsker at deaktivere brugeren. Det skal bemærkes, at der ved deaktivering ikke er mulighed for selv at aktivere brugeren.

Hvis der efter en deaktivering er et ønske om en genaktivering, skal det ske igennem Datafordelerens support.

3.3 Automatisk deaktivering af brugerkonti

Har man oprettet en bruger, men aldrig verificeret den, tilknyttet et IT-system eller pålogget, vil brugerkontoen blive deaktiveret efter 3 måneder og fysisk slettet efter 2 år.

Dette gøres for at minimere antallet af brugere, der ikke er aktive i systemet.

4 IT-system

For at få adgang til data skal du tilknytte et IT-system til din bruger. Det er IT-system, der holder rettigheder og autentifikation. Et IT-system fungerer også som en gruppe man kan blive medlem af. Ejeren af gruppen har ansvaret for handlingerne i gruppen, men har mulighed for at give administrator rettigheder til andre.

IT-systemet vil ofte være tilknyttet en organisation, men det er muligt at oprette et IT-system som privat person.

Når en anvender opretter et IT-system, defineres anvenderen som ejeren og IT-systemet oprettes med organisation svarende til anvenderens.

IT-systemer kan oprettes af en given person som er logget på Datafordeler Administration ved brug af følgende muligheder:

- E-mailadresse og adgangskode
- MitID privat
- MitID erhverv

Alt efter hvilken type login der benyttes ved oprettelse af et IT-system, vil IT-systemet have en række begrænsninger af, hvad der kan gives adgang til.

4.1 Begrænsninger

IT-systemet er begrænset af det medlem der har den laveste adgangstype, det vil sige at hvis et IT-system har en bruger der benytter e-mailadresse til login tilknyttet kan IT-systemet ikke få adgang til beskyttet data. Ligeledes kan brugere der logger ind med e-mailadresse ikke blive tilføjet til et IT-system, der har adgang til beskyttet data.

4.2 Deling af IT-system

Der er til et IT-system tilknyttet tre rettigheder, som er beskrevet i nedenstående tabel.

Rettighedsnavn	Beskrivelse
----------------	-------------



Ejer	Brugeren som har det fulde ejerskab over IT-systemet og som vil være ansvarlig for dens brug. IT-systemet vil altid være oprettet i den samme Organisation som ejeren. Kun Ejer kan videre give ejerskab inden for samme organisation og udpege Administratorer samt Læser for IT-systemet uafhængig af organisation.
Administrator	En bruger som kan udføre ændringer på IT-systemet. Anvenderen kan administrere selve IT-systemet men kan ikke slette det. Administrator kan godt være fra en ekstern organisation. Administrator kan dele rettigheder indenfor egen organisation.
Læser	En bruger der kan se data som IT-systemet giver adgang til, samt information om IT-systemet, men ikke ændre oplysninger. Læser kan ikke dele med andre.

På overblikssiden for IT-systemet ses listen af de brugere med adgang til det pågældende IT-system samt tilknyttet rettighed. Det er illustreret på Figur 8 **Fejl! Henvissningskilde ikke fundet.**

Oversigt over delinger af IT-system

Listen viser, hvilke anvendere på Datafordeleren IT-systemet er delt med. Opret ny for at dele IT-systemet med interne eller eksterne anvendere (for eksempel IT-leverandører). Bemærk, at du kun kan dele IT-systemer med anvendere, der er oprettet med MitID Erhverv. Du kan kun dele IT-systemer med andre, hvis du har en rettighed som Ejer eller Administrator.

Navn	Organisation	Rolle	Handling
Tonni Christiansen	Styrelsen for Dataforsyning og Infrastruktur	Ejer	<input type="button" value="Slet"/>
Trina Østergaard	Styrelsen for Dataforsyning og Infrastruktur	Administrator	<input type="button" value="Slet"/>
Tasha Berthelsen	Styrelsen for Dataforsyning og Infrastruktur	Læser	<input type="button" value="Slet"/>
			<input type="button" value="Opret"/>

Figur 8: Overblik over brugere som har adgang til et IT-system.

Ved hjælp af overblikket har man som anvender, med Administrator- eller Ejersrolle, mulighed for at fjerne de brugere som ikke skal have adgang. For at dele IT-systemet med en anden vælges "Opret" under tabellen, som vist på Figur 10.

Del IT-system

For at oprette en deling skal du have modtaget Brugernøgle fra anvender. Anvender henter Brugernøgle under Brugeroplysninger på egen konto. Vær opmærksom på, hvilken rettighed til IT-systemet du giver anvender, når du deler.

Bruger ID*

Brugerrolle*

Figur 9: Opret ny deling af IT-system.

For at dele systemet skal man kende Bruger ID'et til den bruger man vil tilføje. Dette ID findes kun på brugerens brugeroplysningsside, og er derfor noget brugeren skal give til personen der skal give adgangen.

Det er kun muligt at dele adgang med en anvender som har været logget ind på Datafordeler Administration tidligere og dermed har en brugerkonto.



Bemærk, at der på et IT-system som er oprettet under en MitID erhverv-organisation, kun kan tildeles adgang til andre MitID erhverv-baserede brugere.

4.3 Ansøgning om adgang til beskyttede registerdata

4.3.1 Oprettelse/ansøgning af dataadgang

Under et IT-system kan man som anvender søge om adgang til beskyttede registerdata. Det gøres ved at oprette en ansøgning i Datafordeler Administration, og med den et bilag, som en registeradministrator herefter godkender.

Dataadgang

Her kan alle oprettede ansøgninger om adgang til beskyttet registerdata ses. Der kan oprettes nye ansøgninger på entitetsniveau per register med beskyttet data.

Register datasæt ▾	Status ▾	Udløbsdato ▾
CVR	Approved	13-12-2026
EJF	New	Ikke sat
SVR	Approved	30-01-2025
SVR	Cancelled	28-02-2025

Opret

Figur 10: Overblik over dataadgange til registre.

Det er kun muligt for IT-systemer som er en del af en virksomhedsorganisation (MitID erhverv) at få tildelt adgange til beskyttet data. Derfor vil et IT-system oprettet af brugere der er oprettet med e-mailadresse eller MitID privat ikke kunne ansøge om adgang til beskyttet registerdata.

En dataadgangsansøgning består af følgende:

- Navn og e-mailadresse på ansøgeren (udfyldes automatisk).
- CVR på ansøgers organisation (udfyldes automatisk).
- Telefonnummer (udfyldes automatisk hvis muligt).
- Bilag til ansøgningen (variere efter behovet for det enkelte register), her understøttes filformaterne .doc, .docx og .pdf.
- Det valgte register.
- De valgte entiteter fra registeret der ansøges om adgang til.

Et eksempel på en dataadgang kan ses i Figur 11.



Dataadgang for KDS

Kontakt

Fornavn*

Trina

Efternavn*

Østergaard

CVR*

19552101

Email*

trina@real-svr.dk

Telefon

34 56 78 90

Dataadgang

Hent og udfyld bilag til ansøgning via link til datafordeler.dk og vedhæft ansøgning om dataadgang. Bemærk at registrene har individuelle krav til ansøgningen, der fremgår af vejledningen.

[Vejledning og bilag til ansøgning](#)

Bilag til ansøgning

Vælg fil

Vedhæft

Register*

EJF

Vælg entiteter og tjenester*

Ejendomsadministrator

AlternativAdresse

Ejendomsadministrator

Figur 11: Dataadgangsansøgning.

4.3.2 Visning, forlængelse og nedlæggelse af dataadgang

Gennem oversigten over dataadgange på et IT-system kan man klikke på en given ansøgning og derved tilgå informationer om det.

Det er, under den enkelte dataadgang, muligt at forlænge adgangen på godkendte ansøgninger med 2 år frem i tiden, dette gøres ved et klik på "Forlæng"-knappen (se Figur 12) hvorefter udløbsdato sættes til 2 år fra dags dato. Skulle det ske at adgangen udløber før den forlænges, skal der laves en ny ansøgning på de ønskede entiteter. En ny ansøgning skal godkendes af registeret igen.

Vil man nedlægge IT-systemets adgang til beskyttet data, kan dette gøres på samme side ved at klikke på "Afmeld"-knappen (se Figur 12).



Dataadgang: SVR

Kontakt

Fornavn	Trina
Efternavn	Østergaard
CVR	19552101
Organisation	Styrelsen for Dataforsyning og Infrastruktur
E-mail	trina@real-svr.dk
Telefon	34 56 78 90

Dataadgang

Se status for dataadgang for IT-System og bilag til ansøgning

Status: Ny

Bilag til ansøgning:Ingen bilag vedhæftet denne ansøgning.

Register:
SVR

Entiteter:

- svr_virksomhedadresse
- svr_virksomheddriftform

Udløbsdato:

Forlæng

Forlæng udløbsdatoen for dataadgangen for it-systemet. Bemærk at perioden bliver forlænget med 2 år. Det kræver ikke en fornyet godkendelse fra registret at forlænge perioden.

Forlæng

Afmeld

Afmelder du adgangen, vil it-systemet ikke længere have adgang til data. Du skal ansøge igen for at få fornyet adgang.

Afmeld

Figur 12: Oplysninger om dataadgang, med mulighed for forlængelse og afmelding.

5 Autentificerings-metoder på Datafordeler Administration

I Datafordeler Administration er data tilgængeligt via tre autentificerings-metoder:

- Shared Secrets.
- Certifikater.
- API-Keys.

5.1 Shared Secrets

En Shared Secret er en OAuth token, der kan bruges til at kalde alle typer af data hos Datafordeleren, dog med forbehold for at beskyttet data først kan hentes ved godkendt ansøgning. En Shared Secret skal ved alle kald til Datafordelerens tjenester sættes i en header.

Shared Secrets kan oprettes via Datafordeler Administration ved at navigere til et IT-system man er ejer eller administrator for og klikke på "Opret"-knappen under "OAuth Shared Secret"-sektionen som vist på Figur 13.



OAuth Shared Secret

En OAuth shared secret er en privat nøgle, som deles mellem en OAuth-klient (f.eks. en applikation) og OAuth-udbyderen (f.eks. en service som Datafordeleren). Denne nøgle bruges som en del af godkendelsesprocessen, hvor en klient får adgang til ressourcer på vegne af en bruger uden at afsløre brugerens loginoplysninger.

Navn	Client ID	Status	Udløbsdato	Handling
Test	e022c4d1-c94e-4480-bf94-96e302aaa246	Aktiv	26-02-2025	<button>Deaktiver</button>
				<button>Opret</button>

Figur 13: Overblik over OAuth Shared Secrets.

Ved klik på knappen "Opret" navigeres der videre til en "Opret OAuth Shared Secret" side, hvor et navn og en udløbsdato kan sættes. Det er muligt at sætte udløbsdatoen til maks. 2 år frem i tiden.

Opret OAuth Shared Secret

Navn*:

Gyldig i (antal dage)*:

Udløbsdato*:



Figur 14: "Opret OAuth Shared Secret"-siden.

Efter udfyldning af felter kan der klikkes "Opret"-knappen, og der vil blive genereret en Shared Secret, tilsvarende den som fremgår af Figur 15.



Opret OAuth Shared Secret

Navn*:

Gyldig i (antal dage)*:

Udløbsdato*:

Shared Secret er oprettet

Shared Secret:

Kopier ovenstående OAuth Shared Secret. Den bliver kun vist en gang.

Figur 15: En oprettet Shared Secret.

Bemærk, at en Shared Secret kun vises én gang og det vil efterfølgende ikke være muligt at få den vist igen, hvorfor den skal kopieres over i et værktøj af eget valg for at sikre at den ikke går tabt.

Ønskes der en tidlig deaktivering af en Shared Secret kan dette gøres ved at klikke på "Deaktiver" knappen på Shared Secret overbliklisten vist på Figur 13.

5.2 Certifikater

Der er i Datafordeler Administration mulighed for at uploade et OCES 3-certifikat. Denne type kan ligesom shared secrets bruges til at kalde alle typer af data hos Datafordeleren.

Certifikater tilknyttet et IT-system kan ses under sektionen OAuth certifikat via et valgt IT-system.

OAuth certifikat

Klientautentificering med certifikater i OAuth er en sikkerhedsmetode, hvor klienten bruger et digitalt certifikat i stedet for en hemmelig nøgle til at bevise sin identitet over for autorisationsserveren. Processen involverer, at klienten præsenterer sit certifikat under TLS-håndtrykket, hvorefter autorisationsserveren validerer det. Denne metode er særligt velegnet til miljøer med høje sikkerhedskrav eller ved håndtering af følsomme data.

Navn	Client ID	Fingeraftryk	Status	Udløbsdato	Handling
Certifikat test	a5c92020-1d59-42af-a82b-2eaff88c2787	52CAB8C21DC2EA477BC994D0252F5CC8A495555B	Aktiv	24.10.2026, 12.09.27	<input type="button" value="Slet"/>
Test 606 del 2	4a8ac69f-0543-483d-8139-76bc24bc7818	52CAB8C21DC2EA477BC994D0252F5CC8A495555B	Aktiv	24.10.2026, 12.09.27	<input type="button" value="Slet"/>

Figur 16: OAuth certifikat oversigt.



Ved brug af oversigten set i Figur 16 kan man som anvender, med rollen administrator eller ejer, slette og oprette certifikater, ved klik på "Opret"-knappen navigeres der til "Upload Certifikat"-siden som vises i Figur 17.

Upload Certifikat

Certifikat skal være et OCES 3 bruger eller organisationscertifikat. For at bestille et OCES 3 certifikat, kontakt venligst OCES 3 udbyder.

Upload Certifikat*:

 No file chosen

Navn*:

Figur 17: "Upload Certifikat"-siden.

Når der via "Upload Certifikat"-siden vælges et certifikat ved brug af knappen "Choose File", vil certifikatet blive valideret. Hvis certifikatet er validt, skal certifikatet navngives, og efterfølgende vil "Opret"-knappen blive aktiv og certifikatet kan da tilføjes ved at klikke på "Opret".

Der er følgende krav til et certifikat:

- Certifikatet skal være et OCES 3 (X.509-certifikat) og i PEM-format.
- Certifikat skal være aktivt og ikke udløbet.
- Certifikatet skal være udstedt af den danske stat.

5.3 API-Keys

API-Keys erstatter det tidligere brugernavn/adgangskode, der indsættes direkte i URL'en ved nogle kald til ikke-beskyttet data.

En API-key er en token der genereres én gang og derefter kan holdes i live så længe man som anvender ønsker at benytte den. Dog har de en gyldighed på 2 år fra oprettelse, men kan inden for de 2 år fornyes, med en ny gyldighed på 2 år.

API-keys vil på samme måde, som med brugernavn/adgangskode, blive anvendt direkte i URL'en og vil kun give adgang til ubeskyttet data (offentlig tilgængelige data).

Under et IT-system findes sektionen API-Keys, kan ses på Figur 18. Denne indeholder en oversigt over alle API-Keys på IT-systemet og giver mulighed for at forlænge, deaktivere og oprette en API-Key.

API-Keys

En API-Key er en privat nøgle, som bruges til at autentificere mod en API. Denne nøgle bruges som en del af godkendelsesprocessen, hvor en klient får adgang til et API uden at afsløre brugerens loginoplysninger.

Navn	Status	Udløbsdato	Handling	
Test 540	Aktiv	02-01-2027	<input type="button" value="Forlæng"/>	<input type="button" value="Deaktiver"/>
Test	Inaktiv	02-01-2027	<input type="button" value="Forlæng"/>	<input type="button" value="Deaktiver"/>

Figur 18: Oversigt over API-Keys.



Klikkes der på "Opret"-knappen navigeres der til "Opret API-Key"-siden som vises i Figur 19.

IT-systemer / IT-system

Opret API-Key

Navn*:

Navn er påkrævet.

Opret

Figur 19: "Opret API-Key"-siden.

Efter at have navngivet API-Key'en skal der klikkes på Opret, og en API-Key vil herefter blive generet, og vises i sektionen "API-Key er oprettet" når den er klar, som vist i Figur 20.

IT-systemer / IT-system

Tilbage til IT-system

Opret API-Key

Navn*:

Opret

API-Key er oprettet

API-Key:

Kopier

Kopier ovenstående token nu. Tokenen vises kun en gang her. OBS: Der kan gå op til 15 minutter før API-key er oprettet.

Figur 20: Oprettet API-Key.

Bemærk, at API-Key'en, ligesom en shared secret, kun vises én gang og det vil efterfølgende ikke være muligt at få den vist igen, hvorfor den skal kopieres over i et værktøj af eget valg for at sikre at den ikke går tabt.

Ved klik på "Kopier"-knappen vil den blive kopieret til clipboard og kan derefter CTRL + V over et andet sted.



6 IP-allowlist

Det er i Datafordeler Administration muligt at sætte et krav til hvilke IP-adresser IT-systemet kan kalde fra. Dette er en måde at yderligere sikre ens IT-system for uautoriseret brug, men også et krav for at kunne tilgå beskyttet data.

IP-adresserne styres direkte på siden for IT-system under sektionen "IP Allowlist", hvor det er muligt at ændre, slette og oprette nye IP'er på listen, via knapperne vist på Figur 21.

IP Allowlist

PLACEHOLDER TEXT

Navn	IP-Adresse	Handling
TEST	80.198.54.1	Ændre Slet

[Opret](#)

Figur 21: "IP Allowlist"-sektionen.

Ved klik på knappen "Opret" navigeres der til en "Opret IP-adresse"-side som vist på Figur 22, hvor informationen om IP-adresse kan skrives ind. Når der klikkes "Opret" på denne side vil den blive tilføjet listen.

Opret IP-adresse

IP Navn*:

Navnet på IP-adresse er påkrævet.

IP-adresse*:

IP-adresse er påkrævet og skal være en gyldig IPv4-adresse

Range*:

Range er påkrævet

[Opret](#)

Figur 22: "Opret IP-adresse"-siden.

7 Revisionslogs

Der er i Datafordeler Administration lavet en række forskellige revisionslogs som giver et indblik i de operationer, der er foretaget på ens bruger, samt IT-systemer man har en forbindelse til.

7.1 Brugerlogs

Inde på siden "Brugeroplysninger" kan man via knappen "Revisionslog" få vist en log over alle de handlinger man som bruger har foretaget sig, derudover vil handlinger, som fx ændringer i mine roller og rettigheder, udført på ens bruger af andre også logges her.

Et eksempel på en brugers revisionslog illustreres i Figur 23.



Brugers Revisionslog

Dato	Bruger	Beskrivelse
9.1.2025, 14.09.14	Thilde Schmidt	Loggede på med MitID
7.1.2025, 16.10.18	Thilde Schmidt	Loggede på med MitID
7.1.2025, 16.02.29	Thilde Schmidt	Loggede på med MitID
7.1.2025, 14.48.51	Thilde Schmidt	Loggede på med MitID
7.1.2025, 10.07.04	Thilde Schmidt	Ansøgning (ee16e432-60ea-4b78-ae26-08ee704eef22) om adgang til beskyttet data i registeret SVR blev godkendt.
7.1.2025, 10.06.57	Thilde Schmidt	Ansøgning (ff2ed9bf-c285-43ed-a42b-7fcd01d259be) om adgang til beskyttet data i registeret SVR blev afvist.

Figur 23: Eksempel på en "Brugers Revisionslog".

7.2 IT-system logs

Inde under et IT-system vil man via knappen "Revisionslog" få vist en log over alle handlinger der har en relation til IT-systemet, dette kan f.eks. være deling med en anden bruger eller ansøgning om adgang til beskyttet data.

Et eksempel på en IT-system revisionslog illustreres i Figur 24.

IT-systemer / IT-system / Revisionslog

KDS-ITSystem Revisionslog

Dato	Bruger	Beskrivelse	Vedkommende
19.12.2024, 15.51.35	Trina Østergaard	Ansøgning (86783a81-f432-4941-92a4-45cdac147150) om adgang til beskyttede data i registeret CVR blev forlænget for IT-System (a47bfd9b-9ae0-43b2-9385-93df57455b9f). Ny udløbsdato: 12/19/2026 14:51:35	
19.12.2024, 15.27.11	Trina Østergaard	Tilføjede en OAuth Shared Secret SharedSecretTest180	
19.12.2024, 15.07.49	Trina Østergaard	Opdaterede en IP-Adresse fra 80.198.54.1/24 til 80.198.54.1/24	
19.12.2024, 14.43.43	Tami Hansen	Tilføjede en OAuth Shared Secret Gentest af TC	
19.12.2024, 14.15.07	Titte Skov	Nedgraderede rolle fra Ejer til Administrator	Trina Østergaard
19.12.2024, 14.15.07	Titte Skov	Tildelte Ejer rolle	Tami Hansen
19.12.2024, 13.52.52	Trina Østergaard	Ansøgning (7b18f284-4a1a-4ed6-9055-1c3d355ccbf0) om adgang til beskyttede data i registeret SVR blev godkendt for IT-System (540 Test).	

Figur 24: Eksempel på et IT-systems Revisionslog, her navngivet "KDS-ITSystem".