

FörRätt - Utveckling av kommunala digitala tjänster för registrering och ändring av livsmedelsverksamheter
Version 1.0 uppdaterad 2023-04-26
Dnr 2021/05358

API-dokumentation för registrering och ändring av livsmedelsverksamhet med
e-tjänsten FörRätt

Versionshistorik

|  |  |  |
| --- | --- | --- |
| Version | Datum | Ändrat/Kommentar |
| 1.0 | 2023-04-26 | Version 1.0 publicerad på projektsidan av API-dokumentation och API-specifikation |

Innehåll

[1 Om projektet FörRätt 4](#_Toc133361384)

[2 Beskrivning av dokumentets syfte och upplägg 4](#_Toc133361385)

[2.1 REST API-profil 4](#_Toc133361386)

[3 Säkerhet 5](#_Toc133361387)

[3.1 Autentisering 5](#_Toc133361388)

[3.2 Känsliga uppgifter 5](#_Toc133361389)

[4 Sekvensdiagram 6](#_Toc133361390)

[5 API-specifikation 7](#_Toc133361391)

[5.1 Metoder 7](#_Toc133361392)

[5.1.1 Hämta anläggningar 7](#_Toc133361393)

[5.1.2 Hämta kontaktuppgifter och plats för vald anläggning 8](#_Toc133361394)

[5.1.3 Hämta verksamhetsuppgifter för vald anläggning 8](#_Toc133361395)

[5.1.4 Hämta fakturamottagare för vald anläggning 8](#_Toc133361396)

[5.1.5 Spara ett registreringsärende 9](#_Toc133361397)

[5.1.6 Spara ett ändringsärende 9](#_Toc133361398)

[5.1.7 Spara ett upphörandeärende 10](#_Toc133361399)

[6 Felhantering 10](#_Toc133361400)

[6.1 Schema för att beskriva feldetaljer 10](#_Toc133361401)

[7 Kodverk för riskklassning 12](#_Toc133361402)

[8 Informationsmodell 13](#_Toc133361403)

# Om projektet FörRätt

Den nya modellen för riskklassning av livsmedelsverksamheter införs 2024. Detta innebär att ca 90 000 anläggningar måste klassas om av kontrollmyndigheterna (kommunerna) under 2023 samt att ca 10 000 nya anläggningar fortsättningsvis kommer att behöva registreras varje år enligt den nya modellen. Dessutom behöver alla anläggningar kontinuerligt ha möjlighet att meddela ändringar om sin befintliga verksamhet från och med 2024.

För att underlätta omklassning, anmälan om registrering, ändring och upphörande av verksamhet har projektet FörRätt tagit fram kravspecifikationer för en e-tjänst, varav detta dokument är ett av sex dokument. Dokumenten har tagits fram gemensamt i projektet av Livsmedelsverket i samarbete med ett 50-tal kommuner, Tillväxtverket, systemleverantörer och e-tjänsteplattformsleverantörer. De är framtagna för de som arbetar inom verksamhetsutveckling eller digitalisering på kommunen, som stöd vid utveckling och vid implementering av e-tjänsten.

I “Ramdokument för registrering och ändring av livsmedelsverksamhet med e-tjänsten FörRätt” finns mer information om FörRätt, övriga kravspecifikationer, vilka målgrupper de riktar sig till och hur de förhåller sig till varandra, samt hur de uppdateras.

Vid frågor om detta dokument, kravspecifikationerna, ändringshantering eller förvaltningsrutiner, kontakta forratt@slv.se.

# Beskrivning av dokumentets syfte och upplägg

API-dokumentationen och API-specifikationen beskriver det tekniska gränssnittet mellan e-tjänsten och verksamhetssystemet.

API-dokumentationen innehåller bl.a. ett sekvensdiagram med de olika metoderna i FörRätt. Varje metod beskrivs för sig med sitt specifika schema. Det finns även en informationsmodell som omfattar alla uppgifter som hanteras vid registrering, ändring och avslut av livsmedelsverksamhet.

API-specifikationen är dokumenterad enligt OpenAPI 3.0.1.

## REST API-profil

API FörRätt baseras på den REST API-profil[[1]](#footnote-2) som tagits fram av Myndigheten för digital förvaltning (DIGG) som en rekommendation till offentliga organisationer. Profilen gör det möjligt att bygga REST API:er utifrån bästa praxis och en uppsättning identifierade kravformuleringar.

# Säkerhet

Den nivå på säkerhetslösning som väljs för e-tjänst och verksamhetssystem är upp till respektive kontroll­myndighet att besluta om, baserat på den informationssäkerhetsklassning som gjorts eller bör göras av respektive informationsägare.

Några generella rekommendationer är:

* Alla accesser till API:er ska vara krypterade.
* Klienter bör använda nyckelbaserad autentisering eller OAuth.
* Validera alla in-parametrar i ett API-anrop (schema-validering), för att förhindra SQL-injektion och liknande.

## Autentisering

I API-specifikationen för FörRätt finns exempel på metoder för autentisering. På adress <https://swagger.io/docs/specification/authentication> finns beskrivningar på de olika autentiserings- och auktoriseringsmetoder som kan användas. OpenAPI stödjer fyra olika autentiseringsscheman; API key, http, OAuth 2.0 och Open ID Connect.

De säkerhetsmetoder som är definierade i specifikationen är API-key och Oauth2. Vid implementation ska de exemplen ersättas med relevant konfiguration för respektive integration.

## Känsliga uppgifter

API FörRätt har valt att göra avsteg från den korrekta semantiska betydelsen vid val av HTTP-operation. Detta för att undvika att exponera potentiellt känsliga personuppgifter (personnummer) i header-delen i en GET-operation. Även om RFC 7231 inte förbjuder att man skickar med information i body-delen i GET saknar body-delen semantisk betydelse och ignoreras av många ramverk och verktyg och bör därför inte användas. I dessa fall brukar man i stället använda POST-operationen.

FörRätt har valt att göra avsteget i operationen som med parametern organisationsnummer hämtar anläggningar som drivs av företaget med angivet organisationsnummer.

# Sekvensdiagram

Sekvensdiagrammet i Figur 1 beskriver flödet mellan e-tjänst och verksamhetssystem för registrering och ändring av livsmedelsverksamhet. Den inramade delen överst i diagrammet visar översiktligt användningen av den sammansatta bastjänsten för företagsuppgifter[[2]](#footnote-3).

I Bolagsverkets Infrastrukturen för vidareförmedling av grundläggande uppgifter om företag*[[3]](#footnote-4)* finns regelverk och beskrivningar av samspelet mellan konsument, förmedlare och producent.



Figur 1. Sekvensdiagram FörRätt API

Beroende på om postningen avser en registrering, en ändring eller ett upphörande så är det olika anrop. Hanteringen föreslås vara synkron, i första hand eftersom hela modellen bygger på synkron hantering. Om inte anrop fungerar övergår interaktionen till en asynkron hantering med kvittens i e-tjänsteplattformen.

Kvittens på registrerade uppgifter

I respektive metod för att spara uppgifter returnerar e-tjänsten ett ärendenummer/id till användaren tillsammans med en PDF med registrerade uppgifter.

När verksamhetssystemet erhållit uppgifterna returneras ett OK eller felmeddelande, eventuellt tillsammans med diarienummer eller motsvarande, till e-tjänsten och användaren. Det är upp till varje kontrollmyndighet att bestämma hur detta sista steg ska visas upp i e-tjänsten för användaren.

# API-specifikation

FörRätts API är dokumenterat baserat på OpenAPI 3.0.1. Med t.ex. open source-programvaran Swagger[[4]](#footnote-5) kan specifikationen öppnas för att få en visuell vy över API:et eller för att ha ett gränssnitt för redigering av API:et.

Uppgifter att ändra i API-specifikationen vid implementation är:

* + Kontaktuppgifter
	+ URL till API
	+ Inställningar för säkerhet

I API-specifikationen finns enbart ID:n med för de aktiviteter som inte kräver godkännande. De aktiviteter, verksamhetstyper och omfattningar som kräver godkännande finns i kodverket för riskklassning, och kan hämtas till API-specifikationen därifrån.

Webbtjänsten som ansluter till Bolagsverkets sammansatta bastjänst ska använda namnet LivsmedelForratt.

## Metoder

### Hämta anläggningar

Hämta aktiva anläggningar med angivet organisationsnummer. Enbart aktiva anläggningar returneras från verksamhetssystemet, d.v.s. livsmedelsanläggningar som inte upphört. Anläggningsnamn kan, beroende på system, vara en kombination av namn på anläggning, objekt och verksamhet.

För att undvika att exponera personnummer när de skickas med som parameter används POST i stället för GET. Se även kapitel 3.2 ovan.



### Hämta kontaktuppgifter och plats för vald anläggning

Hämtar en anläggnings kontaktuppgifter, adresser och plats.



Användare som via SSBTEN/RO bekräftats ha en behörig roll i företaget får se samtliga uppgifter som definieras i anropet. Övriga användare får enbart se namn och adress på anläggningen.

### Hämta verksamhetsuppgifter för vald anläggning

Hämtar uppgifter om en anläggnings livsmedelsverksamhet. Med livsmedelsverksamhet avses bl.a. huvudsaklig inriktning, aktiviteter, produktgrupper och eventuella tredjepartscertifieringar.



Enbart användare som via SSBTEN/RO bekräftats ha en behörig roll i företaget får se uppgifter ur verksamhetssystemet. Övriga användare har inte behörighet att hämta dessa uppgifter.

### Hämta fakturamottagare för vald anläggning

Hämtar fakturamottagare och faktureringsadress för ett företag/en anläggning.



Enbart användare som via SSBTEN/RO bekräftats ha en behörig roll i företaget får se dessa uppgifter ur verksamhetssystemet. Övriga användare har inte behörighet att hämta dessa uppgifter.

### Spara ett registreringsärende

Sparar uppgifter rörande anmälan av en ny livsmedelsverksamhet.



### Spara ett ändringsärende

Sparar uppgifter rörande ändring av uppgifter om en livsmedelsverksamhet.

Vid ändring av uppgifter ska inte besöksadress kunna ändras, eftersom detta innebär att det är en ny livsmedelsverksamhet. Det är e-tjänsten som behöver hantera denna begränsning.



Samtliga uppgifter från e-tjänsten postas, inte enbart ändrade uppgifter.

### Spara ett upphörandeärende

Spara uppgifter rörande upphörande av anläggning. Precis som för registrering och ändring så kan vem som helst med e-legitimation skicka in en anmälan om upphörande av anläggning.

För samtliga flöden så fattas det faktiska beslutet av en handläggare vid kontrollmyndigheten.



# Felhantering

## Schema för att beskriva feldetaljer

Schemat enligt RFC 7807 kan innehålla nedan attribut och kräver att mediatypen application/problem+json eller application/problem+xml används i svaret.

| **Attribut** | **Beskrivning** |
| --- | --- |
| type | En URI som identifierar problemtypen som skall vara mer specialiserad än statuskoden. URI:n skall peka på dokumentation av feltypen om den används. |
| title | En kort beskrivning av problemtypen. Dvs att beskrivningen alltid ska vara identisk för samma typ av fel. Om inte type är angivet skall title reflektera beskrivningen av statuskoden. |
| status | Detsamma som statuskoden för HTTP-svaret om det används. Kan vara lämpligt att använda om svaret behöver vara självförklarande. |
| detail | Kort beskrivning av det faktiska felet, avsedd för läsning av människa. |
| instance | En URI som identifierar den faktiska resursen. |

# Kodverk för riskklassning

Nedanstående diagram beskriver relationerna mellan flikar och kolumner i Excelfilen med kodverket för riskklassning.



Figur 2. Datamodell över Kodverket för riskklassning

# Informationsmodell

Informationsmodellen omfattar uppgifter som hanteras vid registrering av livsmedelsanläggningar. FörRätt ingår som en del i denna informationsmodell. Nycklar som används i relationer mellan objekt finns inte med i informationsmodellen.



1. https://dev.dataportal.se/rest-api-profil [↑](#footnote-ref-2)
2. Grundläggande uppgifter om företag. http://samverkan.bolagsverket.se/gu/DataModelDiagram/69ff0b32-fb0c-414d-be20-d13fe1e5dcfc.html [↑](#footnote-ref-3)
3. https://bolagsverket.se/download/18.46f4138717c599ee403ab285/1675425469042/regelverk-bilaga-a-tekniska-ramverk-ssbt.pdf [↑](#footnote-ref-4)
4. Swagger OpenAPI Guide. https://swagger.io/docs/specification/about [↑](#footnote-ref-5)