Länsgemensam kravkatalog för dataåtkomst och informationsutbyte

Kravkatalogen är ett stöd vid upphandling av digitala system och tjänster. Den hjälper organisationer att ställa relevanta krav på dataåtkomst, integration, export, arkivering, gallring och avveckling.

Vad kraven går ut på
Kravkatalogen sätter ord på en gemensam lägstanivå för de krav offentlig sektor behöver kunna ställa på digitala system och tjänster.
Den handlar om rådighet över data – att kommunen har kontroll över den information som skapas, lagras och används i systemen. I praktiken innebär det att data ska kunna nås, användas, delas, exporteras, arkiveras, gallras och avvecklas på ett kontrollerat sätt. Systembyte eller leverantörsbyte ska inte innebära att viktig information blir inlåst.
Kraven fokuserar därför på dataåtkomst, API:er, integrationer, export, arkivering, gallring och avveckling. Syftet är inte att göra upphandlingar mer komplicerade, utan att tydliggöra vilka grundläggande krav som behöver ställas för att kommunen ska behålla rådighet över sin data.

Om katalogen
Kravkatalogen är en första version av en gemensam katalog med konkreta krav som kan användas vid upphandling. Syftet är att ge stöd i att formulera tydliga och användbara krav inom ett avgränsat område.

Den här versionen är främst avgränsad till API:er och andra sätt att ta ut data. Det finns i nuläget inget beslut om att bygga vidare katalogen till fler områden. Nästa steg är att utvärdera om katalogen ger det värde som avsetts.

Viktigt att veta
Kraven är länsgemensamt framtagna av IT-chefsnätverket i Jönköpings län och kan användas i urval. Varje organisation ansvarar för att bedöma relevans, anpassa kraven vid behov och dokumentera eventuella avsteg eller tillägg.

Instruktion vid användning
När krav från katalogen används i länets upphandlingar bör det framgå att de kommer från **Länsgemensam kravkatalog för dataåtkomst och informationsutbyte**.
Det synliggör den länsgemensamma kravställningen och skapar tydlighet kring kravens ursprung.

Målgrupp
Katalogen riktar sig till upphandlare, verksamhetsföreträdare, IT, informationssäkerhet, arkiv och andra roller som deltar i kravställning.

Versionshantering

Version	Beskrivning	Datum
1.0	Första version av länsgemensam kravkatalog, avgränsad till krav som syftar till att säkerställa länets dataåtkomst och informationsutbyte.	2026-05-06

Kravkatalog

Nr	Ska / Bör	Kategori	Krav	Specificera eller utöka kravet	Vägledning
1.1	Ska	Äga data	Köparen ska ha full äganderätt till data som uppstår i systemets användning.		Används när äganderätten till data inte regleras i upphandlingens allmänna villkor, annars kan kravet utgå.
1.2	Ska	API	Systemets API ska vara standardiserat, väldokumenterat och öppet tillgängligt. Det ska vara fullt specificerat enligt vedertagen standard och kunna användas av tredje part utan krav på leverantörsspecifik teknik.		Använd som grundkrav när systemet ska kunna integreras med andra system eller användas av tredje part, för att undvika leverantörsspecifik teknik.
1.3	Ska	API	Systemets API ska stödja etablerade protokoll eller designprinciper och etablerade och moderna dataformat.	Specificera med exempel om det är känt och viktigt, exempelvis: Protokoll (HTTPS, OAuth 2.0, JWT) Designprinciper(GraphQL, RESTful) Dataformat(JSON, XML)	Använd som förtydligande av krav 1.2.
1.4	Ska	API	Systemets API ska ingå i sin helhet så att samtliga funktioner som är relevanta för Köparens avsedda användning av systemet omfattas.	Lägg till efter bedömning: *Exempelvis:* *Inga extra licenskostnader för API:et ska tillkomma vid utökad användning under avtalsperioden.*	Använd för att säkerställa att relevanta API ingår för minst den kravställda funktionalitet som omfattas av upphandlingen. Bedöm om kravet ska utökas så att all användningar av systemets APIer ingår, även sådan användning som inte explicit ingår i upphandlingstillfället. Var medveten om att utökning kan vara kostnadsdrivande och/eller förändra konkurrenssituationen. Extra: Om ni har identifierat/kan

					specificera explicita integrationer skriv även krav för det. Skicka eventuellt med en övergripande skiss
1.5	Ska	API	Systemets API ska vara versionshanterat och bakåtkompatibelt med minst föregående version. Versionsuppdatering ska dokumenteras och kommuniceras på ett sätt som är tydligt för Köparen och tredje part. Leverantören ska lämna information om hur versionsuppdateringar kommuniceras.	Om det är känt och viktigt, specificera hur många tidigare versioner som ska vara bakåtkompatibla.	Använd när API:et ska kunna användas stabilt över tid av köparen och andra parter.
1.6	Ska	API	Systemets API ska för REST-APIer följa Diggs allmänna krav på REST APIer (https://dev.dataportal.se/rest-api-profil).	Komplettera vid behov med organisationens krav på säkerhet, dokumentation eller integration.	Använd för REST-API:er för att utgå från Diggs REST API-profil i stället för att formulera egna detaljkrav.
1.7	Ska	API	Köparen ska ha rätt att integrera med API via egen anvisad integrationsplattform för informationsutbyte med andra system.	Om organisationen har principer för informationsdelning kan de läggas till i kravet. (exempelvis: Standardisering, Masterdata Interoperabilitet, Lösa kopplingar, Dataminimering, Säkerhet, Spårbarhet, Masterdata)	Används för att säkerställa er rätt att integrera via organisationens egna integrationsplattform, för att ta ägarskap över att organisationens principer följs och upprätthålls.
1.8	Ska	API	API:et ska skyddas av moderna säkerhetsprotokoll som är godkända enligt aktuell cybersäkerhetspraxis. Leverantören ska kontinuerligt följa upp och fasa ut protokoll som blir föråldrade (t.ex. äldre TLS-versioner).	Komplettera med mer konkreta krav om säkerheten behöver gå att utvärdera mer exakt.	Använd som övergripande säkerhetskrav för API:et. Kravet anger säkerhetsnivå utan att specificera tekniska detaljer. Se krav 1.9 och 1.10 som är specificering.
1.9	Ska	API	All transport av data via API:et ska skyddas genom kryptering under överföring med TLS 1.2 eller högre. Okrypterad kommunikation (t.ex. HTTP) får inte tillåtas.	Specificera om ni har lokal krav på exempelvis TLS-version, certifikat eller andra	Använd för att detaljera krav 1.8.

			Säkerhetskrav kopplade till transportskydd ska framgå av API-specifikationen och tillhörande dokumentation.	säkerhetsnivåer utifrån er infrastruktur.	
1.10	Ska	API	API:et ska stödja säker autentisering och auktorisation enligt etablerade och standardiserade protokoll (t.ex. OAuth 2.0 och OpenID Connect). Basic Authentication och Digest Authentication får inte användas. Autentisering och auktorisation ska i tillämpliga delar uppfylla de krav som anges i Diggs REST API-profil avseende säkerhet. Vald autentiserings- och auktorisationsmekanism ska framgå av API-specifikationen och tillhörande dokumentation.	Ange konkreta protokoll om det är känt och viktigt. För att ge leverantören större frihet är det möjligt att istället begära att lösningen beskrivs och utvärdera om den motsvarar behovet. *Exempelvis:* *Beskriv vilka protokoll och mekanismer som används, Köparen kommer att utvärdera om lösningen uppfyller kravet.*	Använd för att detaljera krav 1.8. Använd när API:et ska skydda åtkomst till data och funktioner med säker autentisering och auktorisation.
1.11	Ska	API - Skolverksamhet	Systemets API ska följa relevanta standarder, för system avsedda för utbildningsverksamheten ska standarden SS 12000 stödjas. Leverantören ska på Köparens begäran kunna visa att API är validerat, t.ex. med Skolverkets valideringstjänst.		Använd när upphandlingar avser skolverksamhet och systemet behöver stödja informationsutbyte enligt standarden SS 12000.
1.12	Ska	API	Systemets API ska kunna definierina loggningsnivåer samt möjliggöra att dessa används som grund för att generera konfigurerbara varningar och larm. Om loggningsnivåer inte ingår i Systemet API ska leverantören istället föreslå hur relevanta varningar och larm kan uppnås på annat sätt. Leverantören ska tillhandahålla beskrivning av loggningsnivåer. Om kravet uppfylls på annat sätt, kommer Köparen utvärdera om kravet uppfylls.	Ändra till Bör när behovet är mindre kritiskt eller det är känt att det kan lösas på annat sätt. *Exempelvis:* *Systemets API bör kunna definierina loggningsnivåer samt möjliggöra att dessa används som grund för att generera konfigurerbara varningar och larm.* *Leverantören ska tillhandahålla beskrivning av hur relevanta loggningsnivåer uppnås.*	Använd när loggning och larm är viktiga för drift, felsökning eller informationssäkerhet.

1.13	Ska	Dataexport	Systemet ska ha funktion för löpande export av information till datalager via etablerade metoder såsom API, ETL eller säker filöverföring. Exporten ska ske i ett öppet och dokumenterat maskinläsbart format (t.ex. CSV, XML, JSON eller SQL-dump) och bevara dataintegritet samt relationer. Leverantören ska tillhandahålla fullständig teknisk dokumentation. Med löpande export avses dygnsvis om inget annat avtalas.	Ordet löpande gör kravet ospecificerat, ersätt exemplet dygnsvis med en annan tydlig frekvens, till exempel var fjärde timme eller veckovis om behovet är känt och viktigt. Om leverantören får ange avvikelser från önskad frekvens behöver det framgå hur detta ska utvärderas. *Exempelvis Leverantören ska ange med vilken frekvens export är möjligt. Köparen kommer utvärdera om lösningen uppfyller kravet.*	Använd när information behöver exporteras till datalager, BI-plattform eller motsvarande
1.14	Ska	Gallring	Det ska gå att konfigurera bevarande- och gallringsregler i systemet		Använd om det inte ingår på annat sätt i upphandlingen. Som kravet är formulerat har det fokus på systemfunktion, verksamheten kan ha mer specifika bevarande- och gallringsregler som förtydligas av detta IT-nära krav.
1.15	Ska	Arkivering	Systemet ska ha funktion för export i syfte att mellanarkivera eller långtidsarkivera, uttag för arkivering ska kunna genomföras vid avtalsslut men även löpande om behov finns.	Specificera om det är känt och viktigt om uttag ska kunna göras löpande, på begäran eller enligt schema.	Använd när information behöver kunna tas ut både för mellanarkivering eller långtidsarkivering och vid avtalsslut.
1.16	Ska	Arkivering	Export avsett för arkivering ska vara i arkivbeständigt format enligt Arkivlagen vid tidpunkten alternativt exporteras i ett öppet, dokumenterat och allmänt maskinläsbart format (t.ex. CSV, XML, JSON eller SQL-dump) som möjliggör konvertering till arkivbeständigt format i annat system, nödvändiga specifikationer ska		Använd när ni behöver säkerställa att arkivexport kan bevaras över tid och användas i annat system.

			tillhandhållas av Leverantören Export ska säkerställa att dataintegritet inte går förlorad samt innehålla nödvändig metadata, inklusive sekretssmarkeringar och dylikt.		
1.17	Ska	Avveckling av tjänst	Vid avtalets upphörande ska utan dröjsmål Köparens Information/data kunna exporteras i ett öppet, dokumenterat och maskinläsbart format (t.ex. CSV, XML, JSON eller SQL-dump) som möjliggör fortsatt användning i annat system, nödvändiga specifikationer ska tillhandhållas av leverantören. Export ska säkerställa att dataintegritet inte går förlorad samt innehålla nödvändig metadata, inklusive sekretssmarkeringar och dylikt.		Använd i alla upphandlingar där ni vill minska risken för inlåsning vid avtalets slut. Även allmäna villkor kan reglera rätten till sin egen data, detta krav används för att reglera HUR datan görs tillgänglig.
1.18	Ska	Avveckling av tjänst	Leverantören ska efter godkänd export av Köparens information/data radera samtliga kopior av Köparens Information/data (Produktionsmiljö, Testmiljö, Backuper, Datafiler etcetera) Radering ska ske inom 30 kalenderdagar efter godkänd export om inget annat överenskommits och leverantören ska skriftligt intyga att radering genomförs.		Används när äganderätten till data inte regleras i upphandlingens allmänna villkor, annars kan kravet utgå.
1.19	Ska	Dataöverföring	Överföring av information/data i export som sker utanför systemets API ska ske på ett likvärdigt sätt med hänsyn till rådande lagar och annan kravställning, exempelvis via krypterad filöverföring (ex SFTP, HTTPS eller motsvarande enligt överenskommelse).		Använd när data behöver överföras utanför systemets API, till exempel via säker filöverföring.