

Rutin för personuppgifter i Jira Cloud

SISAB, Skolfastigheter i Stockholm AB

Postadress:
Box 5010
121 05 Johanneshov

Besöksadress:
Palmfeltsvägen 5, våning 5
121 62 Johanneshov

Tel: 08-508 460 00
e-post: diarie@sisab.se
webbadress: www.sisab.se

Org.nr: 556034-8970
Styrelsens säte: Stockholm
En del av Stockholms stad

1 Övergång från Jira on-prem till molnlösning

SISAB har av leverantören Atlassian informerats om att de uteslutande fokuserar på sitt molntjänstutbud. Den fristående lokalt installerade Data Center-versionen av Jira, som hittills använts, kommer inte längre finnas kvar i Atlassians utbud av tjänster. I och med detta har SISAB tillsammans med Stadens personuppgiftsbiträde Tieto, Atlassian samt dataskyddsombuden genomfört en tredjelandsoverföringsbedömning för att identifiera potentiella risker och hantera risk för tredjelandsoverföring i molnlösningen.

Risk för tredjelandsoverföring finns, men då SISAB arbetar med aktiv uppgiftsminimering och övrig implementering av juridiska, organisatoriska och tekniska skyddsåtgärder kommer ett byte av plattform till Atlassians molntjänst Jira Cloud att ske.

Av Atlassians tjänsteutbud använder SISAB endast ett begränsat antal av tjänster som är nödvändiga för att SISAB effektivt ska kunna utföra sin verksamhet kopplad till ärendehantering, projektledning, förvaltning av system och för att kommunicera. Detta innebär att SISAB inte använder produkter såsom AI-funktioner då det ökar tredjelandsoverföring av personuppgifter.

2 Dataskyddsombudens rekommendationer

SISAB:s dataskyddsombud har lämnat följande rekommendationer i samband med tredjelandsoverföringsbedömningen avseende personuppgiftsbehandling i Jira.

- Tydligt kommunicerade rutiner för vilka uppgifter som får läggas in i Jira
- Information till samtliga användare om innebörden av att Jira inte längre kommer att användas on-prem
- Tydlig kravställning till leverantören att kontinuerligt uppdatera sin säkerhet och kryptering samt att regelbundet utföra penetrationstester
- Tydliga behörighetstilldelningar utifrån uppdelning mellan projekt eller processer
- Begränsad behörighet beroende på om det är interna eller externa användare/konton.
- För externa användare kan det finnas skäl att i större utsträckning begränsa antalet behöriga användare.
- Hanteringen av visningsnamn (namn på anställda och konsulter), profilbild och e-postadress (pseudonymisering)
- Löpande säkerställa att Jiras AI-funktion hålls stängd för användarna
- Säkerställa principen om lagringsminimering, kravet om nödvändighet och uppgiftsminimering.

Föreliggande rutin avser att behandla vilka personuppgifter som får läggas in i Jira Cloud och behörighetsstyrning kopplat till personuppgiftsbehandling.

3 Personuppgiftsbehandling i Jira Cloud

För interna användare (SISAB:s anställda och konsulter) behandlas alltid ditt namn, e-postadress, profilbild (valfritt), gruppaccesser och produktaccesser i Jira.

För externa användare, såsom exempelvis externa leverantörer och samarbetspartners, behandlas endast e-postadress om det är den enda information som läggs in av SISAB för att användaren ska få begränsad tillgång till tjänsten.

För att interna användare ska få tillgång till Jira Cloud behöver följande personuppgifter behandlas.

- Visningsnamn, namn
- E-postadress (unik identifierare för inloggning)
- Atlassian Account ID
- Profilbild/Foto/Avatar (valfritt)
- Authentiseringsdata (SSO)
- Group Memberships (vilka Atlassian grupper en användare tillhör)
- Produktaccess (vilka Atlassian Cloud produkter en användare har tillgång till)

Vid användning av Jira Cloud kan följande personuppgifter komma att behandlas.

Information innehållande personuppgifter finns i ärendefält/formulär och som är kopplade till syftet med ett enskilt utrymme (fd projekt) i Jira Cloud. Det kan innehålla:

- Personuppgifter som kopplar till ett specifikt ärende
- Telefonnummer
- Personnummer i enskilda fall för beställning av konsult/eller leverantörskonton inom Stockholms stad för att utföra uppdrag åt SISAB. Personnummer definieras såsom extra skyddsvärd personuppgift, även kallad integritetskänslig personuppgift.¹
- Information om avslut/förändring av anställd
- Dokument/bilagor som biläggs i ärende

Indirekta personuppgifter förekommer också, såsom ärende-nummer, AD-nummer, IP-adress.

I tjänsten Jira Cloud har det via ett pinn-system säkerställts att information tillhörande ett ärende lagras inom EU/EES. Uppgifter avseende ett användarkonto kan vid denna rutins upprättande inte pinnas till EU/EES, vilket innebär att dessa uppgifter kan komma att tredjelandsöverföras i större utsträckning än personuppgifter kopplade till ärende- och projekthantering.

¹ [Känsliga personuppgifter | IMY](#) (2026-07-02)

4 Behörighetsstyrning

SISAB kommer att använda produkten Atlassian Guard Premium som är ett avancerat molnsäkerhetstillägg som ett säkerhetsverktyg för organisationer som använder Atlassians molnprodukter. Tjänsten ger SISAB en centraliserad kontroll över användarhantering, åtkomst och säkerhetspolicyer, vilket inkluderar funktioner som enkel inloggning (SSO), tvåfaktor autentisering, dataetikettering, hotdetektering och detaljerade revisionsloggar för att upptäcka hot och förhindra dataförlust.

Alla SISAB-anställda med AD-konto kommer att logga in via SSO/ID-portalen för autentisering. Produkt- och gruppaccesser hanteras av SISAB per specifik användare för att säkerställa korrekt behörighet.

Externa användare kommer att logga in via e-postadress och eventuella produkt- och gruppaccesser hanteras av SISAB per specifik användare för att säkerställa korrekt behörighet.

Jira Cloud är uppbyggt på utrymmen (fd projekt) där varje utrymme har en utrymmesansvarig. Behörighetstilldelningar till utrymmen i SISAB:s Jira Cloud behöver alltid beställas av den som är ansvarig för utrymmet till Jira-administratörer för att få access. Därefter är det den utrymmes-ansvariges ansvar att lägga till personen i sitt utrymme samt kontinuerligt se över och ta bort användare vid avslut.

Endast de medarbetare, konsulter och samarbetspartners som behöver ha tillgång till Jira har ett användarkonto och inga personer med skyddade personuppgifter exponeras i tjänsten. SISAB genomför även behörighetsrevisioner för att säkerställa att användarna har rätt behörighet och att obehöriga samt inaktiva användare inte har åtkomst till Jira.

5 Hur personuppgifter får hanteras i Jira Cloud

Nedan beskrivs hur personuppgifter får behandlas i Jira Cloud för att stödja verksamheten, begränsa tredjelandsoverföring och säkerställa regelefterlevnad. Nedan beskrivs även kort regelverket för dataskydd som bedöms ha relevans vid personuppgiftsbehandlingen för att begränsa de eventuella risker som en tredjelandsoverföring kan medföra vid användande av Jira Cloud.

Dataskyddsförordningen uppställer grundläggande principer för all personuppgiftsbehandling. Dessa är laglighet, korrekthet, öppenhet, ändamålsbegränsning, uppgifts- och lagringsminimering, riktighet, integritet och konfidentialitet samt ansvarsskyldighet.

Vid användande av Jira Cloud är det som beskrivits ovan olika kategorier av personuppgifter som behandlas. Till ett användarkonto behöver visa personuppgifter läggas in i Jira för att tjänsten ska kunna användas och behörighetsstyras. Dessa är absolut nödvändiga att behandla.

Profilbild är däremot inte en nödvändig uppgift och det är frivilligt för användaren att lägga in i tjänsten. Användaren styr således helt själv om denne önskar lägga in en

profilbild i tjänsten. Det är i detta sammanhang emellertid viktigt att kommunicera att uppgiften kan komma att tredjelandsoverföras, då den inte går att pinna till EU/EES.

Vid användning av tjänsten kan användare även komma att lägga in personuppgifter vid kommunikering och vid ärende- och projekthantering. Tjänsten har fritextfält, där uppgifter kan läggas in av behöriga användare i samband med kommunikation och i arbetet med projekt och ärendehantering. Användarområdet för fritextfälten är fastställda till att hantera information kopplade till förvaltning och utveckling av fastigheterna, samt interna verksamhetsfrågor.

Vid fria textinmatningar är det alltid av vikt att förtydliga att inmatning ska vara korrekt, relevant och objektivt formulerad. Formuleringar som indirekt eller direkt kan identifiera en fysisk person är en personuppgift.

Känsliga och integritetskänsliga personuppgifter ska som huvudregel inte läggas in i Jira Cloud.

Känsliga personuppgifter är, enligt dataskyddsförordningen, behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Integritetskänsliga personuppgifter är löneuppgifter, uppgifter om lagöverträdelser, värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler, information som rör någons privata sfär, skyddade personuppgifter (skyddad identitet), personnummer och samordningsnummer.

Inför att personuppgifter ska matas in i Jira Cloud ska interna och externa användare vara informerade om och beakta följande.

- att information som indirekt eller direkt kopplar till en levande fysisk person är en personuppgift.
- att endast relevanta och absolut nödvändiga personuppgifter ska skrivas in i tjänsten.
- att personuppgifter som skrivs in ska uppgiftsminimeras, där så är möjligt.
- att hänvisning görs till roll/titel där så är möjligt, pseudonymisering.
- att inte dokumentera integritetskänsliga och känsliga personuppgifter om det inte är absolut nödvändigt.
- att uppmärksamma personuppgiftsbehandling i tjänsten och befintligt gallringsbeslut för att säkerställa att personuppgifter inte lagras längre än möjligt.
- att faktisk gallring genomförs enligt befintligt gallringsbeslut.

Ovan åtgärder bidrar till att begränsa integritetsrisker i tjänsten överlag och säkerställer även att begränsa personuppgifter som behandlas och som kan exponeras för en potentiell eller faktisk tredjelandsoverföring.

Rutin accepterad av dataskyddsombud
2026-08-04

Nils Lundborg

Dataskyddsombud
Stockholms stad

Peter Sundström

Dataskyddsombud
Stockholms stad