Regelverk för digital hantering av skyddade personuppgifter

Gäller från och med 2019-06-01
Dnr 1-295/2019

Karolinska Institutet

Innehåll

1. Inledning 1
2. Syfte……...1
3. Olika typer av skyddade personuppgifter 1
   3.1 Sekretessmarkering..... 1
   3.2 Kvarskrivning 2
   3.3 Fingerade personuppgifter 2
4. Hantering av begäran om skyddade personuppgifter vid KI 2
5. Begäran om osynlighet på KI: interna och externa webbplats..... 2
6. Generell hantering av skyddade personuppgifter 2
7. Begäran om utlämnande av handlingar som är sekretessmarkerade……3
8. Digitalt flöde av skyddade personuppgifter 4
9. Generell flödesbeskrivning 4
10. Skyddade personuppgifter i förhållande till olika användartyper …….....5
   10.1 Anställda och anknutna 5
      10.1.1 Andringshantering av anställda och anknutna 5
   10.2 Studenter 5
11. Identitets- och behörighetssystem..... 6
   11.1 IDAC 6
   11.2 Active Directory - AD 6
      11.2.1 Attribut för personer i Active Directory..... 6
   11.3 IKAT..... 7
12. Integrationsplattformen KIIP 9
13. Regelverk för konsumerande system..... 10
   13.1 Behörighetsregelverk 10
   13.2 Loggning..... 10
   13.3 Synlighet..... 10
   13.4 Ändringshantering av konsumerande system 10
   13.5 Hantering av studenter/doktorander..... 10

Diarienummer: 1-295/2019	**Dnr för föregående version:**	**Beslutsdatum:** 2019-04-15	**Giltighetstid:** Gäller tillsvidare fr.o.m. 2019-06-01
Beslut: HR-direktör		**Dokumenttyp:** Regler	
Handläggs av avdelning/enhet: HR-avdelningen		**Beredning med:** UFS	
Revidering med avseende på: Finns inga tidigare regler			

1. Inledning

I arbetslivet används personuppgifter i många olika sammanhang, allt från löneregister och adresslistor till behörighetssystem och kompetensdatabaser.

Uppgifter om enskilda personers namn, personnummer, adress, civilstånd, och andra familjeförhållanden används av ett stort antal myndigheter i deras dagliga verksamhet. Den grundläggande insamlingen och registreringen av de personuppgifter som används i samhället sker till stor del inom folkbokföringen hos Skatteverket, varifrån uppgifterna sedan förs vidare på olika sätt.

De uppgifter som registreras i folkbokföringen är som huvudregel offentliga. Det finns dock vissa möjligheter att skydda personuppgifter i folkbokföringsdatabasen genom s.k. sekretessmarkering eller kvarskrivning. Vid särskilt allvarliga hot kan tillstånd att använda s.k. fingerade personuppgifter lämnas.

Förevarande regelverk fokuserar på Karolinska Institutets (KI) digitala användning av uppgifterna. Regelverket berör anställda, anknutna och studenter (även doktorander) samt övriga personer som finns i KI:s identitet- och behörighetssystem.

2. Syfte

Syftet med detta dokument är att förtydliga och klargöra hur KI hanterar digitalt de personuppgifter som förekommer i KI:s databaser.

Personuppgifter aviseras från Skatteverket till andra myndigheter. Mottagande myndighet väljer själv hur den ska hantera skyddade personuppgifter i sina system.

Med enhetliga rutiner kan hanteringen av skyddade personuppgifter underlättas vid KI och minska risken att sekretessmarkerade personuppgifter lämnas ut oavsiktligt. Det är därför viktigt att KI utformar sina rutiner för att förhindra att personuppgifter kommer obehörig person tillhanda.

3. Olika typer av skyddade personuppgifter

Det finns tre olika typer av skyddade personuppgifter med stigande grad av sekretess. Utifrån hanteringen digitalt hanteras *sekretessmarkering* och *kvarskrivning* på likartat sätt. *Fingerade uppgifter* hanteras som en vanlig identitet då man inte kan identifiera dessa som skyddade.

Skatteverket handlägger ärenden om sekretessmarkering och handlägger även ärende som berör kvarskrivning. Kravet för att få bli kvarskriven är att personen av särskilda skäl kan antas bli utsatt för brott, förföljelse eller andra allvarliga trakasserier. Omständigheterna ska i princip motsvara de som gäller för meddelande av kontaktförbud enligt lagen (1988:688) om kontaktförbud.

Ansökan om fingerade personuppgifter görs hos Polismyndigheten, hänvisning ska göras till personens lokala polis.

3.1 Sekretessmarkering

Uppgifterna som registreras i folkbokföringen är som huvudregel offentliga. Om någon är hotad eller förföljd kan ett utlämnande skada personen. Skatteverket kan då föra in en markering för särskild sekretessprövning, en s.k. sekretessmarkering, i folkbokföringsdatabasen för den personen.

Den legala innebörden av sekretessmarkeringen är att uppgifter om personen enligt folkbokföringens bedömning inte bör lämnas ut utan en särskild sekretessprövning.

Sekretessmarkeringen innebär inte en absolut sekretess. En omprövning av sekretessmarkeringen sker i regel varje år av Skatteverket.

3.2 Kvarskrivning

Om det finns särskilda skäl kan en person även få bli ”kvarskriven” på den gamla adressen vid en flytt. Den nya faktiska adressen förvaras manuellt på Skatteverket. Fördelen är då att den nya adressen inte registreras och därmed inte heller sprids. Den gamla adressen tas bort och personen registreras som ”på kommunen skriven” i den gamla folkbokföringsorten.

Kvarskrivning på den gamla folkbokföringsorten gäller högst tre år i taget efter flytt. Personens post går till ett regionalt skattekontor där särskilda handläggare har den nya adressen manuellt förvarad och kan vidarebefordra personens post.

3.3 Fingerade personuppgifter

Om någon är utsatt för särskilt allvarlig brottslighet och hotas till liv, hälsa eller frihet kan denne erhålla fingerade personuppgifter eller s.k. ny identitet. Detta innebär att man får nya identitetsuppgifter.

Ansökan görs hos Polismyndigheten, som fattar beslut om att en person ska erhålla fingerade personuppgifter. Om en person ska erhålla fingerade personuppgifter tas den gamla identiteten bort ur folkbokföringsregistret, även personnummer. Det innebär även att personen måste flytta till en ny, hemlig ort.

4. Hantering av begäran om skyddade personuppgifter vid KI

Om en person kontaktar KI med önskemål om skyddade personuppgifter ska någon form av relevant intyg (exempelvis från Skatteverket, polisen, socialtjänst eller annan utredning som styrker personens förhållanden) finnas som underlag för bedömningen. Det ska röra sig om ett konkret hot. Det är den som erhållit skyddade personuppgifter som själv ansvarar för att upplysa KI om sin situation.

Informationen eller beslutet om skyddade personuppgifter lämnas till personens närmaste chef som beslutar om erhållande av skyddade personuppgifter.

5. Begäran om osynlighet på KIs interna och externa webbplats

I systemet för identitets- och behörighetshantering (IDAC) finns det möjlighet att som person verksam vid KI, under anställning eller som anknuten, begära att ens uppgifter inte ska vara synliga på KI:s olika webbplatser. En begäran skickas till en administratör som ska godkänna begäran.

Det kan förekomma situationer när beslut om skyddade personuppgifter ännu inte meddelats av annan myndighet men att det ändå är berättigat att KI godkänner en persons begäran om skyddade personuppgifter. Det kan exempelvis handla om att utredningen är pågående men ännu inte avslutad och det finns risk för personens säkerhet, eller personal vid KI som arbetar med djurförsök. Bedömningen får göras i det individuella fallet av administratören i samarbete med personens närmaste chef.

6. Generell hantering av skyddade personuppgifter

Sekretessmarkering är mer vanligt förekommande än de andra skyddstyperna. Det framgår inte av själva sekretessmarkeringen vilken uppgift om personen som är skyddsvärd. Adress är i regel den uppgift som är mest skyddsvärd, men det finns även andra uppgifter inom folkbokföringen som kan behöva skyddas.

Det finns ett ansvar hos den enskilde att själv upplysa om eventuell sekretessmarkering eftersom det inte åligger KI att utan anledning kontrollera om en person har sekretessmarkering i folkbokföringen.

Kvarskrivning innebär i praktiken att den nya adressen inte framgår av folkbokföringsregistret och därmed inte heller förekommer i KI:s register. En markering görs i folkbokföringsregistret om att personen har skyddade personuppgifter tillsammans med ett utskick av adressen till skattekontoret dit posten går. KI behöver inte göra någon sekretessprövning eller ta ställning till ett eventuellt utlämnande.

Detsamma gäller för fingerade personuppgifter. Den nya identiteten registreras på ett sådant sätt att det inte framgår att det rör sig om fingerade personuppgifter. Kopplingen mellan den nya och den gamla identiteten finns endast hos Polismyndigheten.

Vid framtagande av olika rutiner och arbetssätt bör KI ta hänsyn till nedanstående.

- KI bör inte i onödan ta med överflödig formaliainformation i handlingar.
- KI ska särskilt beakta hanteringen av sekretessmarkerade personuppgifter vid utveckling av IT-stöd.
- IT-stödet ska utformas så att endast ett fåtal personer med särskild behörighet har tillgång till sekretessmarkerade personuppgifter.
- För en handläggare som har behörighet att ta del av sekretessmarkerade personuppgifter bör det på ett tydligt och enhetligt sätt framgå att uppgifterna är sekretessmarkerade.
- Det ska finnas enhetliga och säkra rutiner för att kommunicera med och om personer med sekretessmarkerade personuppgifter. Kommunikation via e-post ska inte användas i fråga om uppgifter som omfattas av sekretess, vare sig av KI eller mellan andra myndigheter och KI. För utskick till en person med sekretessmarkerade personuppgifter kan KI använda den adress som vi förfogar över eller använda Skatteverkets förmedlingstjänst för post.
- KI ska se till att personal som hanterar sekretessmarkerade personuppgifter har goda kunskaper om systemet med sekretessmarkerade personuppgifter.
- Det bör vara möjligt att kontrollera vilka handläggare som har tagit del av sekretessmarkerade personuppgifter.
- KI bör regelbundet följa upp att regler och rutiner kring sekretessmarkerade personuppgifter efterlevs.

7. Begäran om utlämnande av handlingar som är sekretessmarkerade

Bestämmelsen i 21 kap, 3 § offentlighets- och sekretesslagen (2009:400) talar om att uppgifter om enskilds personliga förhållanden, såsom adress, telefon m.m., kan sekretessbeläggas. Syftet med bestämmelsen är att en person som är hotad eller förföljd ska kunna lämna sina personliga uppgifter till sin arbetsgivare utan att riskera att dessa uppgifter lämnas ut.

En sekretessmarkering innebär inte någon absolut sekretess för skyddade uppgifter. Vid en begäran om utlämnande av personuppgifter ska KI själv göra en sekretessbedömning. Vid bedömningen kan KI komma fram att uppgifterna ska lämnas ut. Det är därför lämpligt att prövningen ska göras av en begränsad krets av personer vid KI. Risken för att sekretessmarkerade personuppgifter lämnas ut av misstag ökar med antalet handläggare som kan ta del av uppgifterna.

KI kan vägra lämna ut uppgifter om en anställd som vi kan anta kommer utsättas för hot eller våld eller annat allvarligt men, om uppgiften röjs. Ett beslut om att inte lämna ut sekretessmarkerade handlingar ska göras skyndsamt och skriftligt samt beslutas av universitetsdirektören efter samråd med jurist.

8. Digitalt flöde av skyddade personuppgifter

Vid utveckling av KI:s olika IT-system ska det finnas enhetliga rutiner och med små möjligheter till avvikelser. För att kunna följa upp personer med sekretessmarkerade personuppgifter bör behandlingen av dessa särskilt beaktas vid systemutvecklingen.

Det viktigt att en sekretessmarkering ser likadan ut i alla system samt att den följer med från källsystemen till konsumerande system, där uppgifter eventuellt kan bli synliga för en bredare massa.

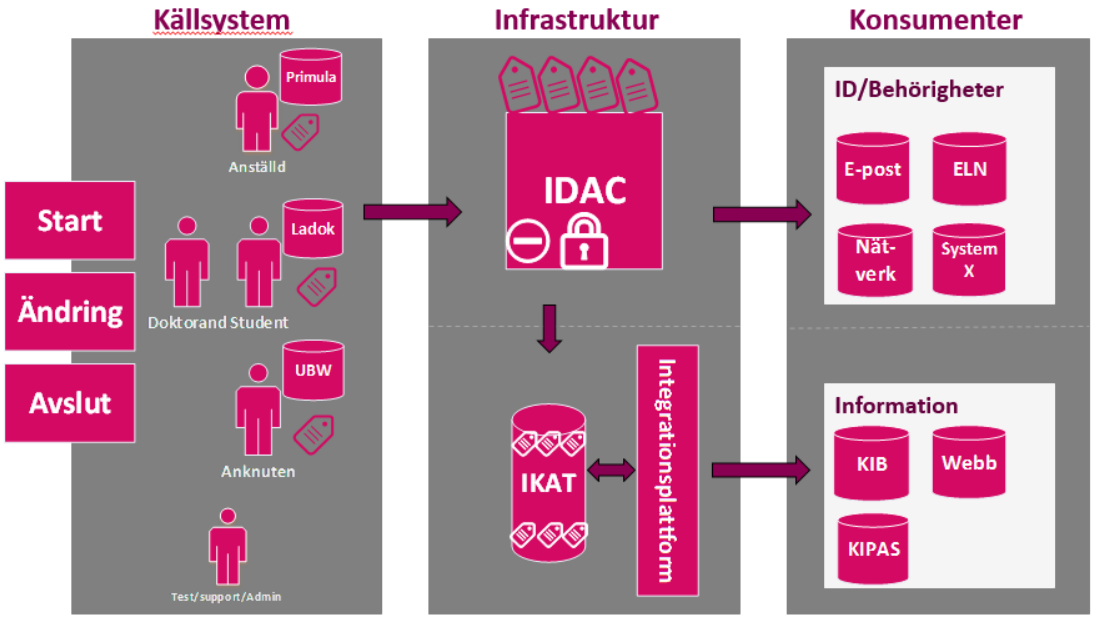
Det finns flera aspekter att ta hänsyn i samband med digital hantering av skyddade personuppgifter.

- Synlighet för administratörer
- Synlighet i andra system
- Vidarebefordran till konsumerande system
- Loggning
- Ändring och borttagning av personobjekt

Det är viktigt att förstå hur flödet av uppgifter går från källsystem, via infrastruktur till konsumerande system samt vilka begränsningar det ska finnas för informationen. Det ska framgå om informationen får eller ska skickas vidare samt huruvida det ska finnas tillgängligt för administratörer.

9. Generell flödesbeskrivning

På KI föds man som digital identitet i ett av källsystemen i enlighet med nedanstående bild.



De olika användartyperna är följande:

- För anställda är det gällande startprocess för anställning som gäller.

- För anknutna är det anknytningsprocessen

- För studenterna är det normalt studentantagningsflödet

- Övriga externa användare som t.ex. studenter, som inte är kopplade i Ladok till KI, följer anknytningsflödet.

När användartyperna har respektive process godkänd kommer personuppgifter och organisationstillhörighet över till IDAC om skapar ett KI-ID och en e-postadress. Personuppgifter inklusive e-postadress och KI-ID skickas sedan över till konsumerande system i syfte att få behörigheter till andra system, fysisk behörighet till lokaler och även bli synliga på t.ex. KI:s medarbetarportal.

Vid ändringar i källssystemet överförs ändringen till infrastruktur och vidare till konsumerande system.

10. Skyddade personuppgifter i förhållande till olika användartyper

10.1 Anställda och anknutna

Hanteringen av personuppgifter i KI:s olika källsystem är kopplade till processerna för start, ändring och avslut för respektive användartyp. I respektive källsystem läggs en markering om skyddade personuppgifter för det fall personen har visat upp ett underlag för erhållande skyddade personuppgifter.

Markeringen om skyddade personuppgifter följer sedan med övrig information till Identitets och behörighetssystemet IDAC.

Personobjektet inklusive markering om skyddade personuppgifter skickas sedan vidare till Active Directory (AD - kontohanteringsverktyg) samt databasen för informationsförsörjning (databas för personinformation). Markeringen om skyddade personuppgifter betyder standardmässigt att informationen sedan inte får konsumeras av några andra system, via webbservice, filer eller andra former av informationsöverföring.

I de fall konsumerande system (t.ex. nyckel/fysiskt access-system, KIPAS) behöver informationen för att medarbetare ska kunna arbeta på KI ställs det krav på det systemet att kunna hantera skyddade personuppgifter (se Generell hantering av skyddade personuppgifter). Syftet med att överföra skyddade personuppgifter ska vara kopplat till möjligheten för den skyddade personen att genomföra sitt arbete.

Integrationsplattformen tillsammans med källsystemet har i sina processer ansvar för att säkerställa att konsumerande system uppfyller kraven innan skyddade personuppgifter överförs.

10.1.1. Ändringshantering av anställda och anknutna

I de fall ett redan existerande personobjekt får en markering för skyddade personuppgifter ska den följa med till Identitet- och behörighetssystemet IDAC, i nästkommande informationsuppdatering.

Personobjektet ska sedan endast vara synlig för administratör med rätt behörigheter. Personobjektet får också en markering för skyddade personuppgifter i databasen för informationsförsörjning, som hindrar att det skickas vidare. Det innebär att integrationsplattformen inte tar med personobjektet från databasen för informationsförsörjning till de system som prenumerera på personobjektet.

10.2 Studenter

Ladok, som är studenthanterigskällsystem, hämtar sin information direkt från folkbokföringen och sekretessmarkeringen överförs till Ladok. Det genererar en manuell hantering i Ladok av personobjektet.

I KI:s integration mellan Ladok och lokal databas överförs ingen sekretessmarkering. I Identitets- och behörighetssystemet sker inga särskilda åtgärder med hänsyn till studenterna. Informationen hanteras såsom den kommer från Ladok, dvs. utan

sekretessmarkering. Det kan eventuellt finnas uppdaterad personuppgifter för att dölja den ursprungliga identiteten.

11. Identitets- och behörighetssystem

I identitets- och behörighetssystemet hanteras personuppgifterna, avsett skyddsnivå, på samma sätt när de passerar vidare i informationsflödet mellan system. Det ställs därför krav på konsumerande system att dessa ska uppfylla vissa skyddskrav för att uppgifterna ska kunna skickas över till respektive system.

Utgångspunkten är att inga personuppgifter som är skyddade, och är obehövliga för tilldelning av behörigheter skickas vidare till andra konsumerande system där dessa är synliga.

11.1. IDAC

IDAC består av två komponenter; MIM synkroniseringsmotor och Omada som hanterar gränssnitt och affärslogik. MIM är tillgängligt för en begränsad mängd systemadministratörer och utvecklare.

I gränssnittet för IDAC finns i princip fyra behörighetsnivåer.

- Mina sidor – där jag endast ser information om mig själv
- Chef/Resursägare – Ser information i sin grupp/personer med tillgång till resurs
- Administratör på Institution – Ser information om personer kopplade till institutionen
- IT-support – Ser information om alla på KI
- Systemadministratör – Ser information om alla på KI

Systemadministratörer, utvecklare, administratörer på institution, chefer och IT-support har tillgång till information om skyddade identiteter. Som chef över dessa befattningar ska man säkerställa att dessa individer har fått adekvat utbildning utifrån detta regelverk.

11.2. Active Directory - AD

Personuppgifter skickas över till AD- user.ki.se för att kunna skapa behörigheter samt tilldela behörigheter till olika digitala informationssystem.

Då AD är en öppen katalog minimeras information som IDAC skickar vidare till ett absolut minimum för att kunna leverera de tjänster som används.

11.2.1. Attribut för personer i Active Directory

Attribut i AD user.ki.se	Beskrivning
DisplayName	Visningsnamn
Mobile	Mobiltelefonnummer
GivenName	Förnamn
mail	KI-basserad e-post
extensionAttribute6	PointSharp mobilnummer för VPN
sn	Efternamn
otherPager	Om personen är aktiv för PointSharp
telephoneNumber	Telfonummer KI

userPrincipalName	påloggningsnamn baserat på e-postadress
wWWHomePage	Avdelning
department	Institution
division	Enhet
company	KI
postalCode	Postkod
street	Postadress
l	Postort
sAMAccountName	KIID
manager	Chef
homeDrive	Hemkatalog
homeDirectory	Hemkatalog
proxyAddresses	Samtliga e-postadresser inom KI

11.3. IKAT

IKAT kallas den nuvarande databasen för informationsförsörjning. Här finns konsoliderad personinformation och organisationsinformation som andra system kan hämta på ett standardmässigt sätt, via integrationsplattformen.

Det finns inget grafiskt gränssnitt till databasen utan är endast till för informationsförsörjning. Endast tre system har tillgång direkt till IKAT; KIIP, Schibboleth och Account.ki.se.

Nedan beskrivs de olika objekt som skickas ut till IKAT samt dess funktion.

- **Personer / användare (kiPerson)**
- **Container och RDN**
  DN: uid=<ki-uid>,ou=people,o=ki
  Ex: uid=alfbag,ou=people,o=ki
- **Attribut**

Attribut	**Värde/beskrivning**
cn (person)	Förnamn + ” ” + Efternamn
coordinationNumber (ki.schema)	Samordningsnummer
displayName (inetOrgPerson)	Visningsnamn el. Förnamn + ” ” + Efternamn
eduPersonAffiliation (eduPerson.schema) MULTI	“student”, “member”, “affiliate”, “employee”
eduPersonAssurance (eduPerson.schema)	
eduPersonEntitlement (eduPerson.schema) MULTI	Extra behörigheter i målsystem enligt GMAI-notation.
eduPersonPrimaryOrgUnitDN (eduPerson.schema)	Referens till primär institution

givenName (inetOrgPerson)	Förnamn
hideMobile (ki.schema)	Dölj mobilnummer
manager (inetOrgPerson)	Närmsta chef; kiPerson-referens
mobile (inetOrgPerson)	Mobiltelefonnummer
kiActivationCode (ki.schema)	Aktiveringskod
kiActivationStatus (ki.schema)	Aktiveringsstatus
kiCardNumber (ki.schema)	Passerkortnummer
kiLadokKey (ki.schema)	Ladok3 UID
kiPersonType (ki.schema) MULTI	anställd, anknuten, student, samarb-stud, doktorand
kiPersonIdentifier (ki.schema)	Personidentifierare. T.ex. personnummer, passnummer
kiPrimulaKey (ki.schema)	Primula A_Person_ID
kiProtected (ki.schema)	”TRUE” för personer med skyddade personuppgifter
mail (inetOrgPerson)	E-postadress (endast den primära)
otherMail (ki.schema)	Annan e-post, t.ex. från Ladok eller UBW
passportNumber (ki.schema)	Passnummer
personalIdentityNumber (ki.schema)	Personnummer
postalAddress (inetOrgPerson)	Postadress, ’$’-separerade rader
registeredAddress (inetOrgPerson)	Besöksadress, ’$’-separerade rader
sn (person)	Efternamn
telephoneNumber (inetOrgPerson)	Telefonnummer
uid (inetOrgPerson) RDN	KI-UID
validFromTimestamp (ki.schema)	När personen ska bli/senast blev aktiv(?)
validToTimestamp (ki.schema)	När personen inte längre har någon aktiv KI-koppling
department	Institution
office	Avdelning
ou	Organisatorisk enhet (enhet eller grupp)
IDAC UID (ki.schema)	IDAC UID
kiEducations (ki.schema) MULTI	Utbildningar (kurs-/programkoder) och deras start-/slutdatum

- **Organisationsenhet (kiOrgUnit)**
- **Container och RDN**
  DN: orgid=<org-id>,ou=organizations,o=ki
  Ex: orgid=12345,ou=organizations,o=ki

- **Attribut**

Attribut	Värde/beskrivning
orgid (ki.schema) RDN	org-id
nameEn (ki.schema) nameSv (ki.schema)	Organisationsenhetens namn på engelska Organisationsenhetens namn på svenska
parent (ki.schema)	Parent; kiOrgUnit-referens
manager (inetOrgPerson.schema)	Enhetens chef; kiUser-referens
registeredAddress (organizationalUnit)	Besöksadress
postalAddress (organizationalUnit)	Postadress
orgLevel (ki.schema)	Organisationsnivå (0-6)
departmentShortName	Institutionsförkortning
departmentCode	Institutionskod

- **Organisationskoppling (kiOrgFunction)**

- **Container och RDN**
  DN: cn=<org-id>-<funk-id>,uid=<ki-uid>,ou=people,o=ki
  Ex: cn=12345-54321,uid=alfbag,ou=people,o=ki

- **Attribut**

Attribut	Värde/beskrivning
cn (core.schema) RDN	org-id + ”-” + funk-id
nameEn (ki.schema) nameSv (ki.schema)	Funktionsnamn på engelska Funktionsnamn på svenska
parent (ki.schema)	Organisationsenhet; kiOrgUnit-referens
validFromTimestamp (ki.schema)	Datum när kopplingen börjar/började gälla
validToTimestamp (ki.schema)	Datum när kopplingen slutar gälla
primaryOrg (ki.schema)	Denna koppling personens primära organisation
uid (inetOrgPerson.schema)	KIID som kopplingen tillhör
departmentShortName	Institutionsförkortning
departmentCode	Institutionskod

12. Integrationsplattformen KIIP

Trepartsavtal ska upprättas mellan KIIP och källsystem, i samband med en förfrågan om att få hämta personinformation till andra system/tjänster. Syftet är att källsystem, som äger informationen, får vetskap om och kan godkänna hämtningen av informationen.

I avtalen ställs motsvarande specificerade krav, se nedan ”Regelverk för konsumerande system”. I avtalen ska de konsumerande systemen och tjänsterna beskriva hur de uppfyller kraven i regelverket. De ska kunna påvisa i praktiken att kraven är på begäran uppfyllda.

13. Regelverk för konsumerande system

13.1. Behörighetsregelverk

Behörighetsregelverket för de roller som finns i konsumerande systemet är utformat så att det finns speciell behörighet för att se och hantera skyddade personuppgifter begränsat till de som har behov av att hantera skyddade personuppgifter.

13.2. Loggning

Det ska finnas tillfredsställande loggning i konsumerande system för att i efterhand ta fram uppgifter om vem som har haft tillgång till skyddade personuppgiftsposter.

13.3. Synlighet

Konsumerande system, såsom webben där information om skyddade personer kan bli synliga för allmänheten eller internt på KI, ska inte få hämta information relaterat till en person med skyddade personuppgifter. Det ska säkerställas att endast behöriga administratörer ska ha tillgång till känslig information om skyddade personer och att informationen inte ska föras vidare till obehöriga personer.

13.4. Ändringshantering av konsumerande system

Konsumerande system ska ha en etablerad ändringshantering av personobjekt för befintliga person vid KI som får skyddade personuppgifter. Det innebär att personobjektet ska, beroende på syftet, automatiskt tas bort i det konsumerande systemet. Är det nödvändigt för systemet att bibehålla personobjektet ska synligheten per automatik begränsas till behöriga administratörer. Systemet ska kunna reagera och ha tydliga regelverk för skyddade personuppgifter. Kan inte systemet uppvisa ett regelverk som följer innehållet i detta dokument ska inte information skickas vidare till det systemet.

13.5. Hantering av studenter/doktorander

Motsvarande digital hantering kommer att ske om en student får skyddade personuppgifter i källsystemet Ladok. Hanteringen är densamma för anställda och anknutna. Om ingen tydlig markering görs i Ladok kan inte studenten hanteras som skyddad. Studenters information är inte synliga på KI:s interna eller externa webb.