**Rutin**

Gäller för: Södra Älvsborgs Sjukhus
Innehållsansvar: Johan Aneljung, (johan16), Säkerhetssamordnare
Granskad av: Johan Aneljung, (johan16), Säkerhetssamordnare
Godkänd av: Gunnar Helgesson, (gunhe2), Enhetschef

Giltig från: 2026-07-03
Giltig till: 2028-06-25

# Personuppgiftsbehandling inom SÄS – register, behandlings- och registerförteckning

## Förändringar sedan föregående version

Detta är ett nytt dokument.

## Sammanfattning

Rutinen beskriver hur SÄS personal ska förhålla sig till personuppgifter, personuppgiftsbehandlingar, behandlingsregister och tillika myndighetens registerförteckning som förekommer inom olika hägn, oavsett om det handlar om känsliga eller icke-känsliga personuppgifter.

## Bakgrund och syfte

Personuppgiftsansvariga ska enligt GDPR föra ett register över sina personuppgiftsbehandlingar. Detta dokument beskriver även ansvar och arbetssätt för att underhålla registerförteckning i SharePoint.

## Utförande

## Personuppgifter

Södra Älvsborg Sjukhus (SÄS) anses som en myndighet och har skyldighet att ha spårbarhet på de behandlingar av personuppgifter som myndigheten bedriver, samt vilka register vi har.

All information som kan knytas till en levande fysisk person är personuppgifter. Vanliga personuppgifter är exempelvis namn, adress, klädstorlek, IP-adresser, fotografier, familjeförhållanden, ljudinspelning, skatt eller hårfärg.

Känsliga personuppgifter är exempelvis hälsa, sexualliv, religiös eller filosofisk övertygelse eller facklig tillhörighet.

En stor mängd icke-känsliga personuppgifter om en person som kombineras kan i den sammanfattande formen även anses vara mer känsligt än de enskilda personuppgifterna som utgör den totala ansamlingen av personuppgifter.

## Personuppgiftsbehandlingar

Behandling är en åtgärd eller en kombination av åtgärder såsom insamling, lagring, läsning, användning, registrering, spridning, sammanförande med mera.

Det innebär exempelvis att ett register kan utgöras av ett Word-dokument i vilket namn, ålder och medicinering finns, och att en behandling är att läsa eller vidarebefordra det dokumentet.

## SOFIA - SharePoint

SharePoint/SOFIA ska undvikas för behandling av personuppgifter. Behandling av personuppgift ska alltid i första hand hanteras i patientadministrativa system. Systemet kan även, i undantagsfall, användas för behandling av personuppgifter kopplat till patienter, i syfte att följa upp verksamhetens kvalitet. Det kan även, i undantagsfall, användas för att verksamhetens grundläggande syften och behov för att utföra sina uppdrag endast kan tillgodoses och uppnås genom att lagra patient- eller journaluppgifter utanför patientadministrativa systemet. Detta ska alltid ske på uppdrag av verksamhetsområdets verksamhetschef.

## Forskning

En samarbetsyta i SharePoint/SOFIA får även användas för att bedriva forskning. Detta ska alltid ske koordinerat med och sanktionerat av Stab för Forskning, Utbildning och Innovation.

En del typer av behandlingar eller bevarande av uppgifter som till exempel känsliga personuppgifter måste äga rum på enskilda ytor. Ytan skapas för att endast innehålla det specifika registret eller behandlingen.

## Känsliga personuppgifter

Patientuppgifter som i undantagsfall förvaras och bearbetas utanför våra patientadministrativa system är exempel på känsliga uppgifter.

De filer som ska arbetas med som innehåller känsliga personuppgifter och som ingår i ett registers helhet får en egen, dedikerad samarbetsyta. Samma person som är ansvarig för registret kan med fördel vara ägare av samarbetsytan. Det är viktigt att den som är ansvarig för registret och ägare av samarbetsytan håller efter uppgifterna som anges.

Ägaren är ansvarig för att endast de som ska arbeta med uppdraget och ta del av ytans innehåll blir medlemmar av samarbetsytan.

De samarbetsytor som innehåller känsliga personuppgifter ska således ha en ytterst begränsad åtkomst, och endast den personal som har i uppdrag att bearbeta de känsliga personuppgifterna får ha tillgång till samarbetsytan. Delning av dokument innehållande känsliga personuppgifter utanför samarbetsytan eller till obehöriga får inte äga rum.

När arbetet är färdigt och registrets syfte är så hanteras filen i enlighet med SÄS informationshanteringsplan tillsammans med uppdragsbeskrivningen och övriga relevanta dokument som har tillkommit som ska bli en allmän handling, och samarbetsytan tas därefter bort.

## Informationshanteringsplan

Register som inte längre är aktuella och ändamålsenliga ska hanteras i enlighet med SÄS informationshanteringsplan, och beroende på syfte och innehåll så bevaras de eller gallras efter en viss tid. Vid frågor om detta kontaktas registerförteckningsansvarig eller informationssäkerhetsteamet på SÄS via sas@vgregion.se. I de fall ett register ska slängas ska även samarbetsytan för register i VGR uppdateras. Även detta ska göras av utsedd funktion/person på enheten/verksamhetsområdet. I de fall ett register ska arkiveras ska gällande rutiner för arkivering följas.

## Personuppgiftsbiträden

SÄS kan emellanåt lämna ut personuppgifter till en annan part, utanför myndighetens väggar. När SÄS överlämnar personuppgifter till en annan part för behandling å våra vägnar så ska ett personuppgiftsbiträdesavtal (PUB-avtal) med stor sannolikhet tecknas mellan SÄS och behandlande part.

## PUB-avtal

Ett PUB-avtal upprättas för att diktera syfte, krav, begränsningar och villkor för behandlingen som äger rum. Ett PUB-avtal behövs även när personuppgiftsbiträdet anlitar ett underbiträde som ska utföra en specifik behandling på den personuppgiftsansvarigas vägnar.

Ett PUB-avtal behöver däremot inte registreras när en part inte behandlar en personuppgift å SÄS vägnar, och behöver uppgifter för att utföra sina uppdrag. Ett exempel är när en namnlista på kursdeltagare ges ut till en annan part som genomför en utbildning.

Behörig undertecknade av PUB-avtal är sjukhusdirektören. Om det är aktuellt att upprätta ett PUB-avtal eller om det finns frågor om ett sådant avtal är nödvändigt, kontaktas alltid i god tid ledningsstödet via sas@vgregion.se eller tfn. 033-616 49 93.

## Register och behandlingsregistret

Södra Älvsborgs Sjukhus har konsoliderat den regiongemensamma förteckningen över register med kravet på att ha ett behandlingsregister.

I SÄS behandlingsregister, tillika registerförteckning, redovisas därför samtliga IT-system som innehåller allmänna handlingar eller personuppgifter, övriga register samt behandlingar av personuppgifter.

Detta inkluderar känsliga personuppgifter såsom patientuppgifter.

I Registerförteckningen så ska även samtliga (PUB-avtal) ingå, och varje nytt PUB-avtal som tecknas ska anmälas till registeransvarig.

## Genomförande i behandlingsregistret

Anmälan av ett nytt register eller annan information som ska inkluderas i SÄS behandlingsregister ska innehålla namn på registrets ägare, e-postadress till ägaren, namn på registret och en kort beskrivning av syftet med personuppgiftsbehandlingen och registret.

När en ny post i behandlingsregistret registrerats så kommer den dedikerade ägaren att kontaktas via e-post. Ägaren av registerposten förväntas följa den länk som delas och som leder till SÄS behandlingsregister. Därefter kompletteras den registerpost som ägaren är ansvarig för med ytterligare information där det är möjligt. Ägaren av en registerpost förväntas kontakta behandlingsregisteransvarig eller informationssäkerhetsteamet på SÄS via sas@vgregion.se om frågor uppstår, om en registerpost anses ska avslutas eller om dess syfte ändrats.

## Länk till behandlingsanmälan:

Anmälan ny behandling av personuppgifter - Södra Älvsborgs Sjukhus (vgregion.se) alternativt e-post till sas@vgregion.se

## Uppföljning och kvalitetsarbete

Behandlingsregisteransvarig på SÄS eller Dataskyddsombud (DSO) utför ett löpande kvalitetsarbete för att hålla registerförteckningen uppdaterad.

Enskilda ansvariga för ett register kan komma att bli kontaktade och ombedda att uppdatera ett register som konverteras från en enkel registrering till en fullständig.

Enskild registeransvarig är ansvarig för att löpande uppdatera informationen i de registerposter de är ansvariga för, och samtidigt ta kontakt med behandlingsregisteransvarig eller DSO för att informera om ändringar i information om register. Detta för att säkerställa att syftet med behandling eller register kvarstår. Enskild registeransvarig ska även kontakta behandlingsregisteransvarig eller DSO för att informera om ett registers önskade avslut.

Om du anser att ett register eller behandling vars syfte måste ändras så är det bättre att avsluta behandlingen eller registret och i stället bilda ett nytt.

Det är viktigt att SÄS har en möjlighet att blicka tillbaka på behandlingshistorik. Genom att skapa ett nytt register så bevarar vi rätt information och håller samtidigt isär separata syften med behandlingar.

Enskild registeransvarig ska också kontakta behandlingsregisteransvarig eller DSO för att informera om ett registers önskade avslut. Det är viktigt att inte ta bort några register ut SÄS behandlingsregister då dessa ska arkiveras.

## Relaterad information

Anmälan ny behandling av personuppgifter - Södra Älvsborgs Sjukhus (vgregion.se)

Rutin för hantering av forskningsstudier Södra Älvsborgs Sjukhus (SÄS) (vgregion.se)

# Bilaga 1 – SOFIA/SharePoint lagring

Vad som får lagras på SOFIA-ytor beror på vilken säkerhetsnivå ytan har.


Ytan **får inte** innehålla information som är skyddad enligt sekretess eller känslig personinformation.


Ytan **får inte** innehålla information som anses vara känslig personinformation. Informationsklass 1-2


Ytan **får** lagra information som anses vara av känslig karaktär, inklusive information som lyder under sekretess/GDPR. Observera att de samarbetsytor som innehåller känsliga personuppgifter ska ha en ytterst begränsad åtkomst. Informationsklass 1-3. Dock ej uppgifter som faller under Patientdatalagen.

# Informationsklasser

Informationsklasser är olika nivåer av säkerhet som används för att bedöma och värdera skyddsbehovet för information inom en organisation.

## Informationsklass 1

Informationsklass 1 innebär, *ingen* eller *obetydlig skada* eller *kränkning* för verksamheten, annan myndighet eller enskild fysisk- eller juridisk person om konsekvens inträffar. Ingen eller obetydlig förtroendeskada för verksamheten. Här är några exempel på vad som kan ingå i informationsklass 1:

**Allmän information**: Information som är avsedd för offentligheten och inte kräver särskilt skydd, till exempel broschyrer, allmänna nyhetsbrev och marknadsföringsmaterial.

**Interna meddelanden**: Icke-känsliga interna meddelanden och e-post som inte innehåller konfidentiell eller känslig information.

**Publika rapporter**: Rapporter och dokument som är avsedda att delas med externa parter och inte innehåller känslig information.

**Allmänna riktlinjer och policydokument**: Dokument som beskriver allmänna arbetsrutiner och riktlinjer som inte innehåller känslig information.

## Informationsklass 2

Informationsklass 2 innebär, *begränsad* skada eller kränkning för verksamheten, annan myndighet eller enskild fysisk- eller juridisk person om konsekvens inträffar. Begränsad förtroendeskada för verksamheten. Uppgifterna inom informationsklass två kan ligga inom ramen för sekretesslagen.

Kan anses vara intern information som kan hanteras i det löpande arbetet. Som exempelvis personuppgifter och uppgifter om verksamheten som anses vara skyddsvärda till exempel:

**Interna uppgifter**: Information som används internt inom organisationen och som inte är avsedd för offentligheten, men som inte heller är kritisk eller mycket känslig.

**Schema på avdelningen**: Scheman och tidsplaner för avdelningar som innehåller information om arbetsfördelning och tidtabeller, men som inte innehåller känsliga personuppgifter.

**Vissa personuppgifter som anses som mindre känsliga**: Personuppgifter som inte omfattas av strikta sekretesskrav, till exempel namn och kontaktuppgifter som används internt.

**Enklare ekonomiska uppgifter**: Finansiell information som inte är kritisk, såsom budgetutkast och preliminära ekonomiska rapporter.

**Leverantörsvillkor:** Villkor och avtal med leverantörer som inte innehåller affärskritisk eller konfidentiell information.

## Informationsklass 3

Informationsklass 3 innebär *allvarlig* skada eller kränkning för verksamheten, annan myndighet eller enskild fysisk eller juridisk person om konsekvens inträffar. Till exempel:

**Inloggningsuppgifter**: Användarnamn och lösenord som används för att logga in på system och applikationer.

**Kunskaps- och psykologiska prov/tester**: Resultat från tester som innehåller känslig information om individers kunskaper och psykologiska tillstånd.

**Känsliga personuppgifter**: Information om individer som omfattas av strikta sekretesskrav, inklusive:

Etniskt ursprung

Politiska åsikter

Religiös eller filosofisk övertygelse

Medlemskap i en fackförening

Hälsa

En persons sexualliv eller sexuella läggning

Genetiska uppgifter

Biometriska uppgifter som används för att entydigt identifiera en person.

**Patientuppgifter**: Medicinsk information om patienter, inklusive diagnoser, behandlingar och medicinska historik.

**Känsliga uppgifter som är pseudonymiserade/krypterade**: Information som har bearbetats för att skydda identiteten av individer, men som fortfarande är känslig.

**Säkerhets- och bevakningsåtgärder**: Information om säkerhetsprotokoll och bevakningssystem som används för att skydda organisationens tillgångar.

**Listor med behörigheter**: Listor över vilka individer som har tillgång till specifika system och information.

**Incidentrapporter**: Dokumentation av säkerhetsincidenter och åtgärder som vidtagits för att hantera dem.

**Driftförhållanden av känsliga objekt och utrustning**: Information om driften och underhållet av kritisk utrustning och objekt.

**Projektplaner**: Detaljerade planer för projekt som innehåller känslig information om mål, resurser och tidsplaner.

**Knutpunkter för kommunikation**: Information om viktiga kommunikationsnoder och system som används inom organisationen.

**Vissa försörjningssystem**: Information om system som är kritiska för organisationens försörjning och drift.

**Hantering av annan myndighetsuppgift**: Information som hanteras på uppdrag av andra myndigheter och som är känslig.

## Informationsklass 4

Informationsklass 4 innebär *mycket allvarlig* skada eller kränkning för verksamheten, annan myndighet eller enskild fysisk- eller juridisk person om konsekvens inträffar. Allvarlig förtroendeskada för verksamheten.

Det kan röra sig om uppgifter som:

**Skyddade identiteter:** Information om individer vars identiteter måste skyddas på grund av säkerhetsskäl, till exempel vittnesskydd.

**Information och utredningar om brottsförebyggande åtgärder**: Data och rapporter som rör strategier och åtgärder för att förebygga brott, inklusive känsliga utredningar.

**Information om nyckelpersoner för verksamheten:** Uppgifter om personer som har kritiska roller inom organisationen och vars säkerhet är av yttersta vikt.

**Stora mängder av information kan vara extra skyddsvärd:** Omfattande datamängder som, på grund av sin volym

och innehåll, kräver särskilt skydd för att förhindra obehörig åtkomst och potentiella säkerhetsrisker

**Säkerhetsklassad information**: Uppgifter som omfattas av säkerhetsskyddslagen och är av betydelse för Sveriges säkerhet.

**Känsliga forskningsdata**: Information från forskningsprojekt som innehåller känsliga uppgifter och som kan påverka nationell säkerhet eller konkurrenskraft.

**Strategiska affärsplaner**: Affärsplaner och strategier som innehåller kritisk information om företagets framtida riktning och konkurrensfördelar.

**Kritiska infrastruktursystem**: Information om drift och säkerhet för kritiska infrastruktursystem, såsom energiförsörjning och vattenförsörjning.

**Militära uppgifter**: Information om militära operationer, strategier och utrustning som är av yttersta vikt för nationell säkerhet.

**Diplomatiska kommunikationer**: Känslig information som rör diplomatiska relationer och förhandlingar mellan länder.

**Hantering av känsliga rättsliga ärenden**: Information om rättsliga ärenden som involverar känsliga eller kontroversiella frågor.

## Patientdatalagen

Patientdatalagen (2008:355) reglerar hur personuppgifter ska behandlas inom hälso- och sjukvården för att säkerställa patientsäkerhet och integritet. Här är några exempel på uppgifter som faller under denna lag:

**Patientens identitet**: Namn, personnummer och andra identifierande uppgifter.

**Bakgrund till vården**: Väsentliga uppgifter om patientens medicinska historia och anledningen till vården.

**Diagnos**: Uppgifter om ställd diagnos och anledningen till betydande medicinska åtgärder.

**Vidtagna och planerade åtgärder**: Information om medicinska behandlingar och åtgärder som har utförts eller planeras.

**Patientjournal**: Skyldigheten att föra en patientjournal som innehåller ovanstående uppgifter samt annan relevant medicinsk information.

# Information om handlingen

**Handlingstyp**: Rutin

**Gäller för**: Södra Älvsborgs Sjukhus

**Innehållsansvar**: Johan Aneljung, (johan16), Säkerhetssamordnare

**Granskad av:** Johan Aneljung, (johan16), Säkerhetssamordnare

**Godkänd av:** Gunnar Helgesson, (gunhe2), Enhetschef

**Dokument-ID**: SAS9613-1190749860-150

**Version**: 3.0

**Giltig från:** 2026-07-03

**Giltig till:** 2028-06-25