



Konsekvensbedömning

För hantering av personuppgifter

Granskningen gäller avtal:

Avtal Psykoterapi

Diarienummer i Tendsign:

IN-IN25-0045.

Avtalstecknare:

Lars Almroth

Ärende:

**Köpt vård psykoterapi för patienter inom
BUP, VUP och tandvård**

Diarienummer i regionens diarieföringssystem:

RV250028

Underskrift

Rådfrågan och granskning

Utifrån konsekvensbedömningens komplexitet kan dataskyddsombudet vara tvungen att delta i granskningen.

	Ja	Nej
Har dataskyddsombudet deltagit i granskningen	☒	☐

Informationssäkerhetsfunktionen utlåtande

Om krav på en konsekvensbedömning föreligger enligt avsnitt 2 i denna mall (om det sannolikt föreligger en hög risk för den registrerades rättigheter och friheter) ska Region Västmanlands informationssäkerhetsfunktion rådfrågas om konsekvensbedömningen (art. 35.2 DSF), vilket ska dokumenteras i denna ruta.

Henrik Nilsson Drott har deltagit i konsekvensbedömningen och anser att dokumentet Förtydligande av förhållanden kring personuppgiftsansvar och behandling av personuppgifter ska användas.

Ifyllt av: Tina Bergman

Datum: 2024-04-11

Verksamhetens utlåtande

Verksamhetens beskrivning av varför personuppgiftsbehandlingen är nödvändig och vilka konsekvenser utebliven behandling kan få.

Personuppgiftsbehandling är nödvändig vid köp av vårdtjänst. Personuppgifter hanteras gällande patienter (remiss och Privera) inom den köpta vårdtjänsten.

Ifyllt av: Tina Bergman

Datum: 2025-04-11

Innehållsförteckning

Rådfrågan och granskning	1
1. Övergripande information	3
2. Krav på att konsekvensbedömning ska genomföras	5
3. Systematisk beskrivning av personuppgifter	7
4. Uppfyllnad av grundläggande dataskyddsprinciper och laglig grund	13
5. Åtgärder som stärker den registrerades rättigheter	16
6. Tredjelandsoverföring (Kap. 5 DSF)	18
7. Beskrivning av skyddsåtgärder	19
8. Risker och minimerande åtgärder	20



= Stycke med förklarande text för aktuellt avsnitt.



= Symbol för att markera att aktuellt avsnitt ska beskrivas i bilaga 1 i PuB-avtalet

1. Övergripande information

1.1. Personuppgiftsansvarig(a) för personuppgiftsbehandlingen

Region Västmanland, organisationsnummer: 232100-0172
HSN

1.2. Kontaktuppgift till dataskyddsombud

Telefon:	021-173000
E-post:	dataskyddsombudet@regionvastmanland.se

1.3. Deltagare för konsekvensbedömning

Genomförande

Namn och e-post till den/de som ansvarar för konsekvensbedömningens genomförande och kan fungera som kontaktperson i ärendet om någon del behöver förtydligas eller följas upp. Markera vem som ansvarar för att förvalta denna konsekvensbedömning.

Namn	E-post	Yrkesroll	Ansvarig
Tina Bergman	tina.bergman@regionvastmanland.se	Verksamhetscontroller	☒
Klara Wretlund	Klara.wretlund@regionvastmanland.se	Systemförvaltare	☐
			☐

1.4. Generell eller övergripande konsekvensbedömning

Om konsekvensbedömningen ska genomföras inom ramen för ett större projekt eller ett program ska Region Västmanlands dataskyddsombud rådfrågas avseende genomförande, resurssättning och behov av externa resurser.

Dataskyddsombudet har rådfrågats	☒
Frågan är ej tillämplig för denna konsekvensbedömning	☐

1.5. Projekt/objekt, IT-komponenter och utrustningsinformation

Beskriv nedan om inom vilket kontext personuppgiftsbehandlingen hanteras. Är det inom ett givet projekt? Kommer det att ske inom en IT-komponent och/eller i en medicinteknisk utrustning?

Process/objekt:	Vårdavtal för upphandlad vårdtjänst inom psykoterapi
IT-komponent:	Privera
Utrustning:	

1.6. Kortfattade beskrivning av ändamål för personuppgiftsbehandlingen
 Beskriv kortfattat vad behandlingen omfattar. Denna information tydliggöra vad syftet är och vad som behandlas. Beskriv även avgränsningen för denna konsekvensbedömning.



Leverantör ska erbjuda vård enligt vårdavtalets uppdrag och utifrån de patienter som förmedlas via remiss.

Betalningsunderlag för den utförda vården hanteras i Privera.

Leverantören ansvarar för kontakten med patienter samt utförande av vården.

Leverantören ansvarar för remissmottagande, kallande av patient, remissvarande samt att en öppenvårdsfil inkommer till Privera med korrekt underlag för ersättning. Öppenvårdsfil till Privera innehåller information om samtliga patienter, behandlade enligt uppdraget. Det innebär att det inte endast är personer folkbokförda i Västmanland.

1.7. Personuppgiftsbehandlingens effektmål

Beskriv vilka förväntade effekter personuppgiftsbehandlingen kommer att få för den registrerade och vilka förväntade effekter behandlingen kommer att få för verksamheten eller i ett bredare perspektiv, exempelvis för sjukvården lokalt eller nationellt.

För att säkra resurser som utför insatser på uppdrag inom upphandlad vårdtjänst psykoterapi.

1.8. Medverkan från berörda parter

Redogör för eventuella personuppgiftsbiträden

Personuppgiftsbehandling	Biträdets namn	Kommentar

2. Krav på att konsekvensbedömning ska genomföras

2.1. Om personuppgiftsbehandlingen sannolikt innebär en hög risk



Genom att svara på frågorna i avsnitt 2.1.1. och 2.1.2 kan man avgöra om behandlingen sannolikt innebär en hög risk för den registrerades rättigheter och friheter och därför kräver en konsekvensbedömning. Vid bedömningen om behandlingen sannolikt innebär en hög risk är det lämpligt att ta hjälp av en dataskyddssamordnare

2.1.1. Kriterier för hög risk (Art.35 DSF)¹

Om en eller fler av frågorna i detta avsnitt besvaras med "ja" krävs en konsekvensbedömning.

	Kriterium	Ja	Nej
1	Systematisk och omfattande profilering som har rättsliga följder för individer eller på liknande sätt i betydande grad påverkar individer	☐	☒
2	Behandling i stor omfattning av känsliga personuppgifter	☒	☐
3	Behandling av personuppgifter som rör fällande domar i brottmål och överträdelse	☐	☒
4	Systematisk övervakning av en allmän plats i stor omfattning	☐	☒
5	Kommer personer att analyseras, utvärderas, profileras eller poängsättas på något sätt?	☐	☒
6	Kommer det fattas automatiserade beslut med rättsliga eller liknande betydande följder för den registrerade?	☐	☒
7	Kommer personer att övervakas på ett systematiskt sätt?	☐	☒
8	Omfattar personuppgiftsbehandlingen känsliga personuppgifter eller personuppgifter av mycket personlig karaktär?	☒	☐
9	Kommer personuppgifter att behandlas i stor omfattning?	☒	☐
10	Kommer olika register att samköras?	☐	☒
11	Rör personuppgifterna sårbara personer, till exempel barn, anställda, asylsökande, äldre och patienter?	☒	☐
12	Kommer teknik användas på ett nytt och innovativt sätt eller kommer nya organisatoriska lösningar användas?	☐	☒
13	Är det risk för att personuppgiftsbehandlingen i sig hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal?	☐	☒



Det kan även framgå att behandlingen innebär en hög risk för den registrerade utifrån en riskanalys, exempelvis genom att man identifierar tidigare oidentifierade personuppgiftsbehandlingar såsom till exempel tredjelandsöverföringar.

Beskriv övriga faktorer som leder till att personuppgiftsbehandlingen kan innebära en hög risk

¹ Rättslig grund för behandling av personuppgifter | IMY

2.1.2. Undantag från att genomföra en konsekvensbedömning (Art. 35.3 DSF)



En konsekvensbedömning behöver inte genomföras om något av följande kriterier uppfylls. Om "ja" väljs för något av kriterierna ska informationssäkerhetsfunktionen i regionen skriva ett utlåtande på sidan 1.

Kriterium	Ja	Nej	Motivering
Behandlingen leder sannolikt <i>inte</i> till höga risker	☐	☒	-
Behandlingens art, omfattning, sammanhang och ändamål är mycket lika en behandling för vilken en konsekvensbedömning redan har genomförts inom Region Västmanland	☐	☒	-
Konsekvensbedömning är redan genomförd som en del av upprättandet av en lag som reglerar behandlingen	☐	☒	-

3. Systematisk beskrivning av personuppgifter

Detta avsnitt ska ge en tydlig överblick över de aktuella personuppgiftsbehandlingarna (Art. 35.7 i DSF).

3.1. Beskrivning av behandling



I tabellen nedan ska det inventeras vilka personuppgiftsbehandlingar som är aktuella, vad de innehåller och hur de utförs. Om konsekvensbedömningen omfattar mer än en personuppgiftsbehandling med mer än ett ändamål, beskriv dessa behandlingar och deras olika ändamål. En IT-komponent kan innehålla flera behandlingar med olika ändamål som "loggning för uppföljning av att interna regler följs" och "drift och support i enlighet med huvudavtalet".

Personuppgifts-behandling	Ändamål	Personuppgifter	Person-uppgifts-biträde	Kategorier av registrerade	Insamling	Externa mottagare	Lagring/lagringstid	Radering/arkivering
Förmedling av aktuellt uppdrag via remiss	Information om patient och diagnos/behandlingsbehov överförs via remiss från Region Västmanland till leverantör med vårdavtal inom psykoterapi.	Patientnamn Personnummer Pat.address/tel. Remittentens namn	Från Region Västmanland till leverantör.	Patienter remitterade av regionen och remittentens namn.	Från Region Västmanlands journalsystem via post till leverantör med vårdavtal inom psykoterapi.	Leverantör	-	-
Begäran ersättning	Information om åtgärd utförd vid besök hos leverantör med vårdavtal inom psykoterapi.	Personnummer Pat.address Besöksdatum Utförd åtgärd Behandlarens namn	Från leverantör till Region Västmanland.	Patienter behandlade av leverantör och leverantörens medarbetare.	Från leverantörens journalsystem via öppenvårdsfil till Privera. Manuell inmatning.	-	-	-

Utföra vård enligt avtalat uppdrag.	Utföra psykoterapeutisk behandling efter remiss från Region Västmanland	Personnummer Namn Adress Information om utförd behandling Behandlarens namn.	Från leverantör till Region Västmanland.	Patienter och behandlare	Överföring av remissvar på pappersremiss från leverantör till Region Västmanland	Avtalad leverantör	Beroende på hantering av pappersremiss hos leverantören. Lagringstid enligt Journalagen	Enligt Journalagen

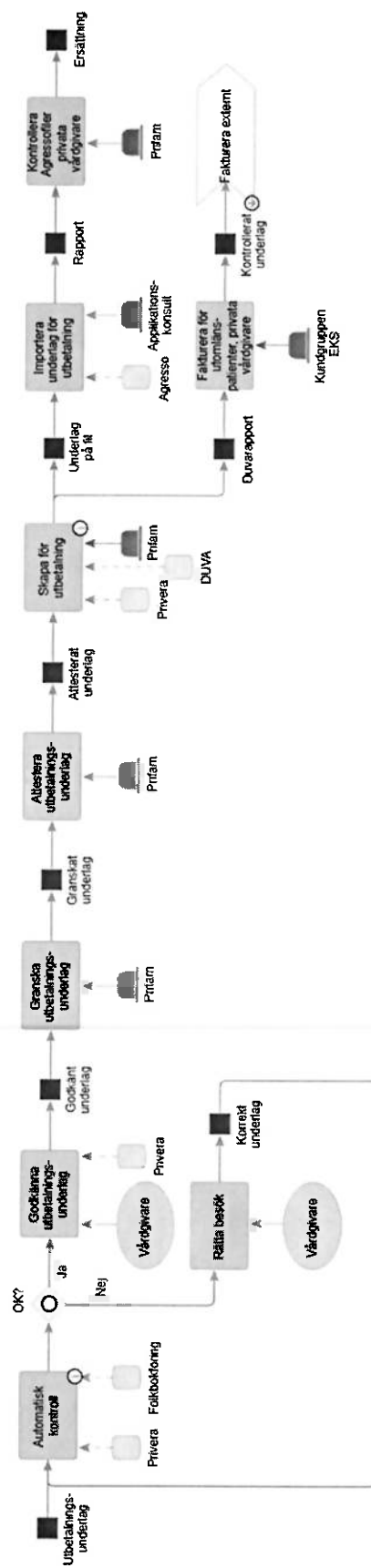
3.2. Översiktlig flödesskiss över informationsvägar för personuppgifter

Bifoga en schematisk bild över hur personuppgifterna flödar som inkluderar externa mottagare för uppgifterna. Om uppgifter överförs till andra länder ska detta framgå av bilden.

REMISS



PRIVERA



3.3. Ny, innovativ eller kontroversiell personuppgiftsbehandling



Utifrån en snabb teknisk utveckling hanteras stora mängder data med hjälp av smart funktioner och det som i dagligt tal kallas för artificiell intelligens (AI). Detta kan medföra kontroversiella behandlingar där apparater, maskiner, mätutrustning har inbyggd teknik och internet-uppkoppling och hanterar uppgifter utan att de typiskt sett ses som datorer. Detta behöver beaktas då detta inte alltid är uppenbart för användaren.

Finns det känd problematik med liknande personuppgiftsbehandlingar? Kan personuppgiftsbehandlingen anses vara ny, innovativ eller kontroversiell på något sätt?

Nej, inte i dagsläget.

3.4. Behandlingens omfattning



I detta avsnitt beskrivs behandlingens omfattning genom att specificera vilka typer av personuppgifter som behandlas, hur många registrerade som påverkas av personuppgiftsbehandlingen, hur många personuppgifter som behandlas samt vilken geografisk räckvidd personuppgiftsbehandlingen har. Utgå från kartläggningen i avsnitt 3.1 för att svara på frågorna nedan.

3.4.1. Typ av personuppgifter och registrerade

Sammanfatta antalet personuppgifter som behandlas och om det finns känsliga personuppgifter (Art. 9 DSF) eller andra integritetskänsliga eller särskilt skyddsvärda personuppgifter (Art. 10 och 87 DSF) som behandlas².



Typ av personuppgifter:	Personnummer Pat. Adress diagnos/behandlingsbehov Besöksdatum Utförd åtgärd
Varav känsliga personuppgifter:	-
Typ av registrerade:	Personer som behandlas av leverantörer på uppdrag enligt upphandlat vårdavtal inom psykoterapi.

3.4.2. Behandlingens geografiska räckvidd



Med geografisk räckvidd avses om de registrerade vars personuppgifter behandlas exempelvis bara finns i en avgränsad del av Västmanland, hela Västmanland, andra delar av Sverige eller i andra länder.

Beskriv personuppgiftsbehandlingens geografiska räckvidd

Samtliga patienter som behandlas hos vårdgivaren oavsett var de är folkbokförda.

² I art. 9 DSF definieras känsliga personuppgifter som följande: ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometrisk uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Med integritetskänsliga och särskilt skyddsvärda personuppgifter avses bland annat personnummer eller andra nationella identifikationsnummer, uppgifter om lagöverträdelser och uppgifter om någons privatliv.

3.4.3. Nödvändiga informationsbärare



Informationsbärare är det hanterar personuppgifter. Exempel på informationsbärare är maskinvara, programvara, nätverk, personer, papper eller spridningskanaler för papper. Om en informations-klassificering har genomförts kan nödvändiga informationstillgångar ha dokumenterats i samband med denna.

Specificera de informationsbärare som är nödvändiga för att personuppgiftsbehandlingen ska gå att genomföra.

Privera, öppenvårdsfil enligt följande instruktioner i ledningssystemet: -
Filspecifikation för öppen vård Privera 57896
Lathund filspeifikation öppenvårdsfil Privera 57898

3.5. Den registrerades kontroll över sina personuppgifter (Kap 3, DSF)



Med kontroll avses om den registrerade själv kan påverka hur och om personuppgifterna behandlas. Exempelvis har den registrerade kontroll om hen själv kan återkalla ett samtycke genom digitala funktioner som finns tillgängliga för den registrerade, eller om hen själv kan ladda ner alla sina personuppgifter från den personuppgiftsansvarige i ett strukturerat, elektroniskt format.

Beskriv hur mycket och på vilket sätt den registrerade kommer ha kontroll över sina personuppgifter.

Genom att kontakta personuppgiftsansvarig i regionen och dennes dataskyddsombud

4. Uppfyllnad av grundläggande dataskyddsprinciper och laglig grund
I detta avsnitt dokumenteras laglig grund (art. 6, DSF) för behandling och hur de grundläggande dataskyddsprinciperna (art. 5, DSF) uppfylls. Minst en verksamhetsrepresentant ska alltid delta i laglighetsbedömningen. Vid osäkerhet om vilken rättslig grund som är tillämplig för de aktuella behandlingarna, kontakta informationssäkerhetsfunktionen.

4.1. Laglighet och laglig grund



För verksamheter inom region Västmanland är det ytterst ovanligt att samtycke (A) väljs som laglig grund. Om detta anses vara aktuellt kontrollera med informationssäkerhetsfunktionen och motivera på vilket sätt samtycket uppfyller kraven i DSF (exempelvis genom att bifoga en kopia av samtyckesblanketten). Laglig grund, fullgöra avtal (B), används om det föreligger ett "köp och sälj" förhållande mellan region Västmanland och privatperson.

Inom Region Västmanland bedrivs verksamhet som bland annat utgår från Hälso- och Sjukvårdslagen. Många uppdrag utgår från att vi har en rättslig förpliktelse (C) och en del av dessa uppdrag kan vara av allmänt intresse eller utföras som myndighetsutövning (E).

Om allmänt intresse eller rättslig förpliktelse väljs nedan, hänvisa till vilket lagrum som avses, exempelvis kommunallag (2017:725) eller hälso- och sjukvårdslag (2017:30).

Val (D) och (F) används ytterst sällan för regionens verksamheter.

	Laglig grund	
A	Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.	☐
B	Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.	☐
C	Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.	☐
D	Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.	☐
E	Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.	☒
F	Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.	☐

4.2. Känsliga personuppgifter får endast behandlas om något av undantagen i artikel 9.2 uppfylls.

Ange vilken rättslig grund som behandlingen stödjer sig på (art. 6 DSF)³.
Förekommer flera behandlingar med olika rättsliga grunder behöver det framgå tydligt vilken rättslig grund som gäller för respektive personuppgiftsbehandling.

Om känsliga personuppgifter (art. 9 DSF) behandlas, ange vilket undantag som möjliggör behandlingen (art. 9.2 DSF)⁴ och fyll sedan i typ av personuppgift samt motivering.

	Laglig grund	
A	Den registrerade har uttryckt sitt samtycke samtidigt som det inte finns ett förbud mot behandlingen.	☐
B	Nödvändigt för att den registrerades ska kunna fullgöra sina skyldigheter samt utöva sina särskilda rättigheter. (Arbetsrätt, Social trygghet och skydd, nationell rätt och kollektivavtal)	☐
C	Behandlingen är nödvändig för skydda den registrerades intressen när denna är fysiskt eller rättsligt förhindrad.	☐
D	Behandlingen är berättigad utifrån arbetsgivaransvaret under förutsättning att adekvata skyddsåtgärder vidtagits.	☐
E	Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.	☐
F	Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet.	☐
G	Behandlingen proportionerlig och nödvändig utifrån till exempel ett viktigt allmänt intresse. Adekvata åtgärder ska säkerställa den registrerades rättigheter.	☒
H	Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser etc.	☐
I	Behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan.	☐
J	Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1	☐

Typ av känslig Personuppgift	Motivering

³ Vägledning om de rättsliga grunderna finns på IMY:s webbplats: <https://www.imy.se/lagar--regler/dataskyddsförordningen/rattslig-grund/>

⁴ Läs dom olika lagliga grunderna i sin helhet på IMYs webbplats: [Dataskyddsförordningen i fulltext](#) | IMY

4.2.1. Andra lämpliga sätt att uppnå ändamålet

i *Med annat lämpligt sätt avses om det finns andra, mindre riskfyllda sätt att uppnå ändamålet med personuppgiftsbehandlingen. Det kan till exempel finnas andra tekniska lösningar, möjlighet att använda andra, färre eller mindre känsliga uppgifter eller möjligheter att använda anonyma och aggregerade data. Denna fråga besvaras lämpligen av projektledaren med stöd av beställaren av tjänsten och en verksamhetsrepresentant.*

Ange om det finns något annat lämpligt sätt än den planerade personuppgiftsbehandlingen för att uppnå samma ändamål.

Inte aktuellt

4.2.2. Nödvändighet och proportionalitet

I dataskyddsförordningen står det att personuppgiftsbehandlingen ska vara "nödvändig" och proportionerlig i förhållande till riskerna för den registrerades rättigheter och integritet.

Ange varför behandlingen är nödvändig och proportionerligt utifrån verksamhetsnyttan och dom risker som uppstår för den registrerade

För att kunna få ersättning för det uppdrag som finns avtalat med RV. Samt möjliggöra för Region Västmanland att följa upp det uppdrag som utförs av avtalad privat vårdgivare.

4.2.3. Ändamålsglidning

i *Ändamålsglidning är att uppgifterna behandlas för ett specifikt ändamål men att man sedan börjar behandla dem för ett annat, otillåtet ändamål. Exempelvis att ett system upphandlas för att behandla personuppgifter för ett visst syfte, men att personuppgifterna utan analys och bedömning börjar användas för andra ändamål eftersom det är tekniskt möjligt i systemet.*

Beskriv hur ändamålsglidning motverkas.

Avtalsuppföljning gentemot leverantör och vid behov utökad uppföljning.

4.3. Uppgiftsminimering

i *Endast personuppgifter som är nödvändiga för ändamålet får behandlas. Ett exempel på uppgiftsminimering är att inte "för säkerhets skull" även samla in personnummer när endast namn och födelsedatum behövs för att uppnå ändamålet.*

Redogör för hur personuppgifterna i behandlingen är relevanta i förhållande till det specificerade ändamålet.

Alla personuppgifter är relevanta för att kunna utföra uppdraget.

4.4. Lagringsminimering

i *Personuppgifter får inte sparas längre än vad som behövs för att uppnå ändamålen med behandlingen. När ändamålen som angetts i avsnitt 3.1 har uppnåtts ska gallring eller avidentifiering alltid övervägas om personuppgifterna inte ska arkiveras eller behövs för forskning eller statistik. Se till att all lagring av personuppgifter, inklusive mellanlagring eller tillfällig lagring, tas höjd för när denna fråga besvaras.*

Eftersom leverantörer ofta har standardinställningar för hur länge information sparas behöver Region Västmanland i egenskap av personuppgiftsansvarig göra ett aktivt val och informera leverantörer om vilka lagringstider som är aktuella.

☰ *Detta bör anges i utkastet för det PuB-avtal som ska bifogas förfrågningsunderlag i en upphandling.*

Redogör för hur länge personuppgifterna behöver lagras/sparas av biträdet.

Gallring kommer att ske i enlighet med Region Västmanlands rutiner för detta.

5. Åtgärder som stärker den registrerades rättigheter

I detta avsnitt ska effektiva åtgärder som vidtagits för att stärka den registrerades rättigheter dokumenteras (art. 12–23 och art. 34 DSF). Åtgärderna kan vara organisatoriska, som framtagande av en rutin för handläggning och att utse ansvariga och/eller tekniska som att till exempel alla personuppgifter i ett system går att utsöka. För att åtgärderna ska kunna anses vara effektiva ska de utgå från behandlingen och dess ändamål (art. 35.7 b DSF).

5.1. Information till den registrerade

i *Informationen till den registrerade ska uppfylla de krav som ställs i dataskyddsförordningen. Mer information och vägledning har du i instruktioner och vägledning som finns i ledningssystemet: Ifyllnadsguide till informationsplikt, Informationsplikt som ska fyllas i som en del av konsekvensbedömningen.*

Beskriv hur information om behandlingen utformats och hur den på olika sätt kommer att lämnas eller delges den registrerade.

Leverantören ansvar för att informera patient om deras rättigheter samt behandling enligt upphandlat vårdavtals uppdrag.

5.2. Rätt till tillgång (registerutdrag) (Art. 15 DSF)



Det behöver både finnas teknisk möjlighet att tillgodose rätten till tillgång och en rutin för hur en begäran ska handläggas.

Beskriv hur den registrerades rätt till tillgång (registerutdrag) säkerställs.

Det sker genom kontakt med regionens informationssäkerhetsfunktion för t verksamhet inom PUA's ansvar, men finns inte automatiserat.

5.3. Rätt till rättelse (Art. 16 och 19 DSF)



Felaktiga eller ofullständiga personuppgifter ska gå att rätta eller komplettera. Offentliga handlingar och handlingar inom hälso- och sjukvård kan inte ändras utan måste rättas genom tjänsteanteckning där information fortfarande finns kvar. (Vid rättelser som innebär radering av en hälso eller sjukvårdsuppgift kan detta bara beslutas av IVO).

Ange hur den registrerades rätt till rättelse säkerställs.

En inskickad men inte utbetald ersättning i en öppenvårdsfil går att rätta.

5.4. Rätt till radering (Art 17 och 19 DSF)



Region Västmanland har en rättslig skyldighet att registrera och bevara allmänna handlingar i enlighet bestämmelserna i offentlighets- och sekretesslagen (2009:400) och arkivlagen (1990:782). Rätten till radering är därför inte aktuell för personuppgifter i handlingar som inkommit till, upprättats vid, och/eller finns förvarade hos Region Västmanland eftersom dessa utgör allmänna handlingar vid myndigheten. (Vid radering av en hälso eller sjukvårdsuppgift kan detta bara beslutas av IVO).

I de fall den är tillämplig, ange hur den registrerades rätt till radering säkerställs samt hur det säkerställs att personuppgifterna som raderas inte går att återskapa.

Inkomna personuppgifter i öppenvårdsfil till Privera som är felaktiga kan inte raderas men rättas.

5.5. Rätten att göra invändningar och rätten till begränsning av personuppgiftsbehandling (Art. 18, 19 och 21 DSF)



Den registrerade har i vissa fall rätt att kräva att behandlingen av personuppgifter begränsas. Detta måste vägas utifrån behandlingens lagliga grund. Exempelvis kan en patient önska att vissa personuppgifter inte dokumenteras i samband med vård, vilket behöver beaktas utifrån nödvändigheten.

Ange hur den registrerades rätt att göra invändningar och rätt till begränsning av personuppgiftsbehandlingen säkerställs.

I Privera finns möjlighet till kodning för bland annat smittskydd och j skyddade personuppgifter som säkerställer möjlighet till begränsning av personuppgiftsbehandling.

6. Tredjelandsoverföring (Kap. 5 DSF)



Med tredjeland avses ett land utanför EU/EES. Begreppet "överföring" som det definieras i dataskyddsförordningen innefattar all form av åtkomst (innefattar även tillgängliggörande) till personuppgifter. Även överföringar av Region Västmanlands uppgifter utanför EU/EES som görs av Region Västmanlands personuppgiftsbiträden och deras underbiträden är tredjelandsoverföringar som vi ansvarar för eftersom det är våra uppgifter som överförs.

Ett exempel på överföring till tredjeland är att ett av Region Västmanlands personuppgiftsbiträden inom EU/EES har anlitat ett underbiträde i Indien som sköter Region Västmanlands supportärenden och i samband med detta ges åtkomst till personuppgifter i klartext.



Vid tredjelandsoverföring måste den personuppgiftsansvarige (Region Västmanland) säkerställa att rättspraxis och administrativa metoder/rutiner hos myndigheter och domstolar i mottagarlandet möjliggör en väsentligen likvärdig skyddsnivå med den som garanteras inom EU.

	Ja	Nej
Överförs personuppgifter till tredjeland i samband med behandlingen?	☐	☒

7. Beskrivning av skyddsåtgärder

Beskriv vilka skyddsåtgärder som vidtas vid personuppgiftsbehandlingen. Om personuppgifter behandlas av tredje part något sätt, ange vilka skyddsåtgärder som vidtas och vilka överföringsmekanismer som används vid tredjelandsoverföring (land med adekvat skyddsnivå eller lämpliga skyddsåtgärder).

Personuppgiftsbehandling	Beskriv skyddsåtgärder	Beskriv tredjeland eller tredje part.	Beskriv överföringsmekanism

7.1. Medverkan från berörda parter



När så är lämpligt ska synpunkter inhämtas från de registrerade eller deras företrädare (art. 35.9 DSF). Om utlåtanden från relevanta intressenter finns i annan bifogad dokumentation såsom en riskbedömning kan man hänvisa dit. Inom hälso- och sjukvårdens kan det bland annat vara fackförbund.

7.1.1. Synpunkter från registrerade eller biträden

Om det är aktuellt har ni rådgjort med registrerade eller dess företrädare? Om ja: Redogör för dessa synpunkter. Om nej: Motivera varför ni bedömer att det inte är lämpligt att inhämta eller följa synpunkter från de registrerade.

8. Risker och minimerande åtgärder

Målet med en konsekvensbedömning avseende dataskydd är att minimera risker för den registrerades rättigheter och friheter (art. 35.7 c DSF). För att möjliggöra detta ska en riskbedömning där man hanterar risker för kränkningar av den registrerades rättigheter och friheter genomföras i samband med konsekvensbedömningen, det vill säga informationssäkerhetsrisker som kan resultera i negativa konsekvenser för enskilda individer. Konsekvenserna kan vara av materiell, fysisk eller psykisk karaktär.

Endast risker för den registrerade ska vara i fokus under riskbedömningsdelen av konsekvensbedömningen eftersom det bara är den registrerades perspektiv som är av relevans i en konsekvensbedömning. Risker ur ett bredare perspektiv, såsom risker för Region Västmanland som organisation, hanteras i stället i en riskbedömning avseende informationssäkerhet.

Riskbedömningsdelen av en konsekvensbedömning ska innehålla:

- *Riskens ursprung (orsak/sårbarhet) (skäl 90 DSF).*
- *Identifiering av hot som kan leda till obehörig åtkomst, oönskad ändring och förlust av personuppgifter (personuppgiftsincidenter).*
- *Identifiering av möjliga konsekvenser för den registrerades rättigheter och friheter vid händelser, däribland obehörig åtkomst, oönskad ändring och förlust av uppgifter.*
- *Uppskattning av sannolikhetsgrad och konsekvensgrad (värdering av risker) (skäl 90 DSF).*
- *Fastställande av planerade åtgärder för att hantera dessa risker (artikel 35.7 d DSF och skäl 90 DSF)*

Riskbedömningsdelen av en konsekvensbedömning kan av praktiska skäl genomföras samtidigt som en riskbedömning avseende informationssäkerhet. Dokumentationen kan göras i Region Västmanlands riskhanteringsverktyg VIRA eller göras via mallen nedan.

Tillsammans utgör en komplett ifylld mall för konsekvensbedömning samt tillhörande riskhanteringsdokument en komplett konsekvensbedömning

8.1. Riskdokumentation

Hänvisa till aktuellt riskbedömningsdokument (diarienummer eller motsvarande beständigt referensnummer) eller bifoga riskerna och de minimerande åtgärderna i sin helhet till detta dokument.

-

8.2. Riskbedömningsmall för att bedöma den registrerade

Enligt tabellen nedan beskrivs risk och vilken konsekvens det är för den registrerade. Om risken är försumbar behöver inte åtgärder vidtas. Om risken däremot är måttlig till allvarig behöver åtgärder beskrivas och vidtas för att eliminera eller minimera dessa risker. Risktalet ska ses som ett stöd i bedömningen.

riskvärde x sannolikhetsvärde = risktal

Risk och konsekvensbedömning		Handlingsplan								
Beskrivning av risker för den registrerade	Konsekvens	1	2	3	4	1-4	Risktal	Åtgärder – vad behöver göras för att ta bort eller minska risken	Ansvarig	Tid
		Försumbar risk	Måttlig risk	Betydande risk	Allvarig risk	Sannolikhet				