Stockholms stad

Stadsledningskontoret
Avdelningen för it och digitalisering

Remissutgåva

2021

Konsekvensbedömning enligt GDPR artikel 35

Ansvarig verksamhet (PuA):

Klicka eller tryck här för att ange text.

Personuppgiftsbehandlingens namn:

Klicka eller tryck här för att ange text.

Fastställd datum: Klicka eller tryck här för att ange datum.

Konsekvensbedömning för personuppgiftsbehandling enligt dataskyddsförordningen

Vägledningen utgör ett ramverk för att genomföra godkända konsekvensbedömningar enligt dataskyddsförordningens artikel 35

Innehåll

1. BAKGRUND TILL KONSEKVENSBEDÖMNING

Om en personuppgiftsbehandling sannolikt leder till en hög risk för personers rättigheter och friheter ska en konsekvensbedömning genomföras.

GDPR Artikel 35 – Konsekvensbedömning avseende dataskydd

1. Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppigfter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.
2. Den personuppigftsansvarige ska rådfråga dataskyddsombudet, om ett sådant utsetts, vid genomförande av en konsekvensbedömning avseende dataskydd.

Vid bedömning av risk för personuppgifter är det god sed att genomföra konsekvensbedömningar för att skapa förutsättningar för ett starkt dataskydd för en verksamhets personuppgifter, den specifika personuppgifts-behandlingen. Konsekvensbedömningar ska ses som en integrerad del av den ansvariga organisationens systematiska risk- och säkerhetsarbete och även stödja sig på och som ett gränssnitt mot organisationens etablerade informationssäkerhetsramverk och metodik.

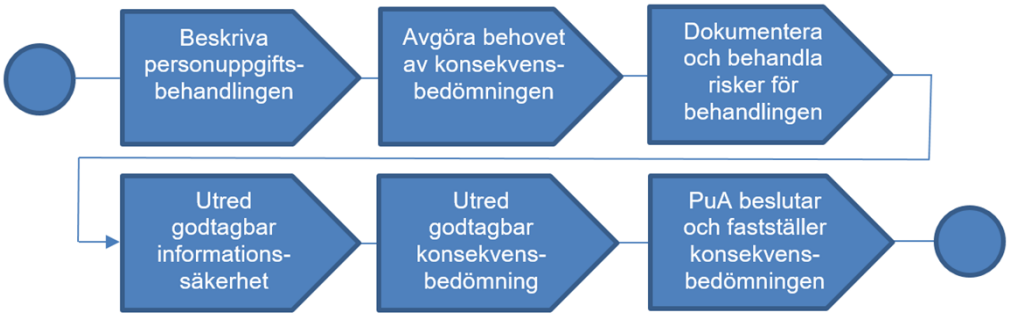
2. PROCESS OCH BESTÅNDSDELAR FÖR KONSEKVENSBEDÖMNINGEN

En konsekvensbedömning ska innehålla följande fyra grundläggande delar vilka är minikriterier enligt EU:s dataskyddsförordning (artikel 35.7 och skälen 84 och 90):

- en systematisk beskrivning av den planerade behandlingen och behandlingens syfte,
- en bedömning behovet av och proportionaliteten hos behandlingen,
- en bedömning av riskerna för de registrerades rättigheter och friheter
- De åtgärder som planeras
    - för att hantera riskerna och
    - för att visa att dataskyddsförordningen efterlevs

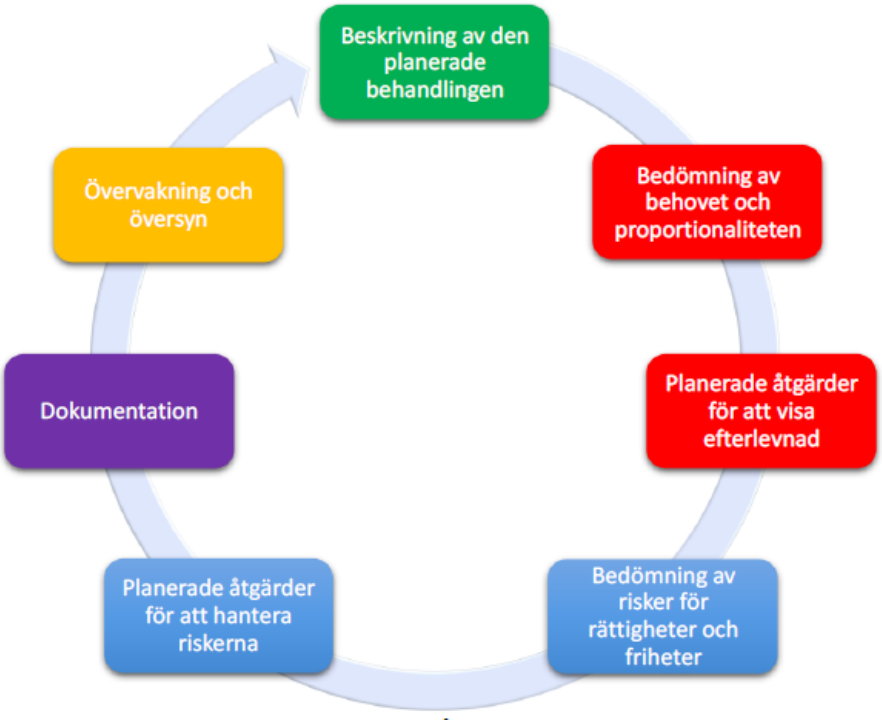
PROCESS FÖR KONSEKVENSBEDÖMNINGEN

På grund av den känsliga natur då höga risker sannolikt förekommer i en personuppgiftsbehandling är mycket viktigt att säkerställa att konsekvensbedömningar genomförs med hög kvalitet.



Figuren visar processen för konsekvensbedömning

Följande figur illustrerar det generella återkommande förfarandet för att genomföra en konsekvensbedömning



Bildtext: generellt återkommande förfarande för att genomföra en konsekvensbedömning (EU:s artikel 29-gruppens riktlinjer för konsekvensbedömningar).

Förfarandet som avbildas här är återkommande: praktiken är det sannolikt att varje steg upprepas flera gånger innan konsekvensbedömningen kan slutföras.

3. ARBETSFORMER OCH KOMPETENSER FÖR ATT GENOMFÖRA KONSEKVENSBEDÖMNINGEN

Det är viktigt att en väl sammansättning grupp får möjlighet att stödja och ge synpunkter vid genomförande av konsekvensbedömningen. Likaså bör lämpliga arbetsformer stödja processen, där ansvarig handläggare kallar till arbetsmöten och diskussion om vägval I frågor om riskbedömning och hantering för den aktuella behandlingen.

För att även tekniska risker ska kunna bedömas och hanteras behöver lämpliga tekniska kompetenser knytas till konsekvensbedömningen, t.ex. teknisk förvaltningsledare och objektspecialist.

Verksamhetens informationssäkerhetssamordnare bör delta och ge synpunkter och stöd. Det är obligatoriskt (styrs av lag) att verksamhetens utsedda dataskyddsombud (DSO) får insyn och möjlighet att ge synpunkter i varje genomförd konsekvensbedömning.

Det är önskvärt att följande roller/kompetenser medverkar vid konsekvensbedömningen:

- Verksamhetskunnig/ansvarig
- Processansvarig för den aktuella verksamheten och behandlingen som berörs
- Tekniska roller inom infrastruktur, kommunikation, it-säkerhet
- Verksamhetens informationssäkerhetssamordnare (samordnaren är inte operativt ansvarig utan stödjer de ansvariga rollerna i verksamhetens linje)
- Verksamhetens dataskyddssamordnare (DSO ska erbjudas full insyn och möjlig medverkan men är inte operativt ansvarig utan tillser rådgivning och kontroll)
- Leverantörer i form av biträden till verksamheten, både för övergripande verksamhetsprocesser och för teknisk säkerhet

4. FÖRBEREDELSER – INHÄMTA BEFINTLIGA UPPGIFTER

Förutsättningar:

Information från följande områden kan utgöra underlag till svar för delar av konsekvensbedömningen, t.ex. systematisk beskrivning av behandlingen och riskbedömningar.

- GDPR-registerförteckning DRAFTIT:
    - Om behandlingen inte finns dokumenterad i registerförteckningen (eller är dokumenterad med it/system-perspektiv i stället för i verksamhetsfokus med informations- och processperspektiv) *färdigställ detta först* innan ytterligare steg i konsekvensbedömningen
- KLASSA underlag
    - Verksamhetens/PUAs handlingsplaner tillsammans med leverantörs/PUBs handlingsplaner och samlade riskhantering. Om klassning ej har utförts så behöver detta färdigställas som en del i att konsekvensbedömningen ska kunna fastställas, i del 2, efter tröskelanalysen.
- Riskanalyser, incident- och/eller granskningsrapporter
    - Andra granskningar och dokumentation om kända brister är relevanta i genomförande av konsekvensbedömningen, t.ex. protokoll och rapport från penetrationstester

➔ Den ansvariga handläggaren sammanställer en lista över de befintliga dokumenten för att hjälpa arbetsgruppen att genomföra konsekvensbedömningen.

5. PERSONUPPGIFTSBEHANDLINGEN

5.1 Beskrivning av den planerade (eller befintliga) behandlingen och dess syfte

En systematisk beskrivning av den planerade behandlingen och behandlingens syfte framgår nedan.

En konsekvensbedömning kan också utföras på en *kategori eller grupp av behandlingar* med liknande personuppgifter och ändamål. Det kan ses som ett sätt för verksamheterna att hushålla med resurser men som ändå resulterar i en ändamålsenlig och adekvat skyddsnivå för dess personuppgifter.

5.1 Fakta om personuppgiftsbehandlingen
Personuppgiftsbehandlingens namn: Klicka eller tryck här för att ange text.
Tillhör klassificeringsstruktur: Klicka eller tryck här för att ange text.
Ansvarig verksamhetschef: Klicka eller tryck här för att ange text.
Ansvarig processägare: Klicka eller tryck här för att ange text.

5.2 Beskriv förhållandena för personuppgiftsbehandlingen:
- Hur kommer ni att behandla personuppgifter (innebär bl.a. att samla in, använda, lagra, kommunicera och radera personuppgifter)?
Svar: Klicka här för att ange text.
- Vilka är källorna för personuppgifterna, dvs var kommer de ifrån?
Svar: Klicka här för att ange text.
- Kommer ni att dela personuppgifter med någon annan part, t.ex. en samverkande part eller ett biträde/leverantör?
Svar: Klicka här för att ange text.
- Vilka typer av behandlingar identifieras som sannolikt leder till en hög risk ingår? (kan kräva underlag från steg 5.2 nedan)
Svar: Klicka här för att ange text.

5.2 Typer av personuppgifter i behandlingen:

Nedan indikeras vilka olika typer av personuppgifter som förekommer i behandlingen:

5.2 a Personuppgifter enligt GDPR Artikel 6	5.2 b Skyddsvärda personuppgifter enligt övriga GDPR artiklar	5.2 c Känsliga personuppgifter enligt GDPR Artikel 9	5.2 d Skyddade personuppgifter (”skyddad identitet”)
Namn Adress Mejladress Telefon/ mobilnummer Foto Anställning	Person-/samordningsnr Betalningsinfo Lön Uppgift om ekonomiskt förhållande Rekryteringsunderlag Uppgifter om barn Uppgifter om person i beroendeställning (t.ex. anställda, elever, patienter)	Ras eller etniskt ursprung Politiska åsikter eller tillhörighet Religiös eller filosofisk övertygelse Medlemskap i fackförening Behandling av genetiskt uppgifter Biometriska uppgifter för att entydigt identifiera en fysisk person	Person-/samordningsnr Namn Adress Telefon/ mobilnummer Foto Anställning

	☐Utvärderingar eller bedömningar om persons prestation	☐Uppgifter om hälsa ☐Uppgifter om fysisk persons sexualliv eller sexuella läggning	
Övrigt – andra personuppgifter (t.ex. ip-adress, registreringsnummer):Klicka eller tryck här för att ange text.			

6. DE REGISTRERADES RÄTTIGHETER

Dokumentera hur de registrerades rättigheter hanteras och tillhandahålls.

Som möjlighet till fördjupad instruktion och definitioner hänvisas till Integritetsmyndighetens hemsida om de registrerades rättigheter.
https://www.imy.se/lagar--regler/dataskyddsforordningen/de-registrerades-rattigheter/

6.1) Beskriv när och hur de som ingår i behandlingen har informerats om att de är registrerade. Notera att informationen behöver vara avgränsad och specifik för den aktuella behandlingen och inte övergripande för verksamheten
Svar: Klicka här för att ange text.

6.2) Beskriv hur, om tillämpligt, samtycke har inhämtats från de registrerade som ingår i behandlingen.
Svar: Klicka här för att ange text. ☐Ej tillämpligt, samtycke används inte

6.3) Beskriv hur de registrerade personerna som ingår i behandlingen kan utöva sina rättigheter till tillgång och dataportabilitet.
Svar: Klicka här för att ange text.

6.4) Beskriv hur de registrerade personerna som ingår i behandlingen kan utöva sina rättigheter till rättelse och radering.
Svar: Klicka här för att ange text.

6.5) Beskriv hur de registrerade kan utöva sina rättigheter till begränsning och invändning.
Svar: Klicka här för att ange text.

6.6) Vid tredjelandsöverföring, dvs. en överföring av personuppgifter ut ur EES, beskriv hur adekvat skyddanivå säkerställs. (annars ange ’förekommer ej’)
Svar: Klicka här för att ange text.

7. NÖDVÄNDIGHET OCH PROPORTIONALITET

En bedömning ska utföras av om behandlingen är *nödvändig* och *proportionerlig* i förhållande till syftet med den.

Beskriv efterlevnad och de proportioneliga åtgärderna specifikt nedan i punkten 7.1.

7.1 Proportionalitet för behandlingen

Bedöm om behandlingens intrång i de registrerades personliga sfär kan anses vara *proportionellt* och *befogat* i förhållande till syftet och omfattningen av den planerade behandlingen?	Ja	Nej
7.1 a) Är den planerade behandlingen av de registrerades personuppgifter *proportionell* i förhållande till tillvägagångssätt, det berättigade syftet och nyttan för de registrerade?	○	○
7.1 b) Är den planerade behandlingen av de registrerades personuppgifter proportionell i förhållande till tillvägagångssätt, det berättigade syftet och nyttan för de registrerade? Är det tydligt att nyttan för de registrerade överväger de intrång som behandlingen medför integritetsmässigt i deras personlig sfär?	○	○
7.1 c) Är syftet *berättigat*, dvs. nödvändigt och passar väl in med verksamhetens uppdrag och syften?	○	○
Eventuell kommentar: Klicka här för att ange text.		

7.2 Laglig grund för behandlingen

7.2 a) Vilken är den lagliga grunden för behandlingen?
Svar: Välj ett objekt.
7.2 b) Hur har den personuppgiftsansvarige uppfyllt informationsplikten?
Svar: Klicka här för att ange text.

Notis: Den lagliga grunden enligt artikel 6.1 a) **samtycke** bör väljas i sista hand och särskild hänsyn behöver tas till att den registrerades samtycke både är frivilligt och lika lätt kan dras tillbaka som när det lämnades. Det är även nödvändigt att den personuppgiftsansvarige har uppfyllt informationsplikten till de registrerade, dvs. att tydlig och specifik information har lämnats om den avsedda behandlingen.

7.3 Berättigat ändamål för behandlingen

Det berättigade syftet anger att det beskrivna syftet även behöver överensstämma med verksamhetens art och uppdrag.

7.3 a) Vad är ändamålet med behandlingen? Svar: Klicka här för att ange text.	Ja	Nej
7.3 b) Är ändamålet berättigat, dvs. nödvändigt och passar väl in med verksamhetens uppdrag och syften?	○	○
7.3 c) Åstadkommer behandlingen sitt avsedda syfte?	○	○
Eventuell kommentar: Klicka här för att ange text.		

8. TRÖSKELANALYS – AVGÖR OM EN KONSEKVENSBEDÖMNING BEHÖVER GENOMFÖRAS

I en förstadium till konsekvensbedömningen ska nio frågor analyseras. Om en eller frågor stämmer på den aktuella behandlingen så är det möjligt att en konsekvensbedömning behöver genomföras. Dock påpekar Integritetsskyddsmyndigheten i överensstämmelse med den europeiska Dataskyddsstyrelsen (f.d. Artikel 29-gruppen) att *även ett kriterium* kan tyda på att en konsekvensbedömning behöver genomföras, beroende på hur riskerna för de registrerades fri- och rättigheter avseende personuppgifternas behandling.

Vid beslut att ej genomföra en konsekvensbedömning ska motiveras och dokumenteras anledningarna till detta, och inkludera dataskyddsombudets synpunkter.

8.1 Nio kriterier för att genomföra en konsekvensbedömning

Enligt dataskyddsförodningens artikel 35.3 a anges nio kriterier för att bedöma om en konsekvensbedömning behöver genomföras.

Som möjlighet till fördjupad information hänvisas till Integritetsskyddsmyndighetens hemsida om när en konsekvensbedömning ska göras: https://www.imy.se/lagar--regler/dataskyddsforordningen/konsekvensbedomningar-och-forhandssamrad/forteckning-konsekvensbedomning/

Kriterium 1:	**Ja**	**Nej**
Kommer personer att utvärderas eller poängsättas?	○	○
Förekommer profilering och förutsägelser?	○	○

Kommentar: Klicka här för att ange text.

Vägledning

Har personuppgifterna att göra med personers beteende, arbetsprestation, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, vistelseort eller förflyttningar?

Exempel:

- Företag/organisationer som utvecklar profiler för beteende eller marknadsföring som grundas på användning av eller navigering på dess webbplats.
- Finansinstitut som granskar sina kunder mot en databas för kreditupplysning eller mot en databas för bekämpning av penningtvätt och finansiering av terrorism.
- Bioteknikföretag som erbjuder genetiska tester direkt till konsumenter för att bedöma och förutse risker för sjukdomar/hälsorisker.

Kriterium 2:	Ja	Nej
Omfattar personuppgiftsbehandlingen automatiskt beslutsfattande med rättsliga eller liknande betydande följder för enskilda?	○	○

Kommentar: Klicka här för att ange text.

Vägledning
Skulle personuppgiftsbehandlingen till exempel kunna leda till att personer utesluts eller diskrimineras?

Kriterium 3:	Ja	Nej
Innebär personuppgiftsbehandlingen systematisk övervakning?	○	○

Kommentar: Klicka här för att ange text.

Vägledning
Kommer de registrerade att observeras, övervakas eller kontrolleras på allmän plats eller exempelvis elektroniskt inom ett nätverk?

Denna typ av övervakning är ett kriterium eftersom personuppgifter kan samlas in i situationer där de registrerade kanske inte är medvetna om vem som samlar in deras uppgifter eller hur de kommer att användas. Dessutom kan det vara omöjligt för enskilda att undvika att bli föremål för sådan behandling på allmän plats.

Kriterium 4:	Ja	Nej
Behandlas känsliga eller skyddade personuppgifter* enligt artikel 9 eller uppgifter som är av mycket personlig karaktär, till exempel ett sjukhus som lagrar patientjournaler, ett företag som samlar in lokaliseringsuppgifter eller en bank som hanterar finansiella uppgifter?	○	○

(*) Avser skyddade personuppgifter (”skyddad identitet”) i nivåerna sekretessmarkering och kvarskrivning genom Skatteverket

Kommentar: Klicka här för att ange text.

Vägledning
Ska ni till exempel samla information om enskildas politiska åsikter eller personuppgifter om fällande domar i brottmål. Vilka personuppgifter som är känsliga framgår av artikel 9 i dataskyddsförordningen.

Exempel: Ett allmänt sjukhus som lagrar patienternas journaler

Personuppgifter av mycket personlig karaktär kan vara:

- uppgifter om hushållet och privat verksamhet, till exempel elektronisk kommunikation
- uppgifter som påverkar utövandet av en grundläggande rättighet, till exempel lokaliseringsuppgifter som kan göra att den fria rörligheten ifrågasätts

finansiella uppgifter som skulle kunna användas för betalningsbedrägeri
uppgifter såsom personliga dokument, e-postmeddelanden, dagböcker, kommentarer från läsplattor som är utrustade med kommentarfunktioner och mycket personlig information i applikationer som registrerar aktiviteter.

Det kan ha betydelse om uppgifterna redan har offentliggjorts av den registrerade eller av tredje man och om den registrerade kunnat förvänta sig att uppgifterna skulle återanvändas för andra ändamål.

Kriterium 5:	Ja	Nej
Kommer personuppgifter att behandlas i stor omfattning?	○	○

Kommentar: Klicka här för att ange text.

Vägledning

Stor omfattning kan både räknas i antal och i andel av en population. Fundera särskilt på:

- hur många som är registrerade, antingen som ett exakt antal eller som en andel av den berörda gruppen
- hur mycket och vilka typer av personuppgifter som behandlas
- hur länge personuppgifterna behandlas
- inom hur stort geografiskt område de registrerade finns.

Kriterium 6:	Ja	Nej
Kombineras personuppgifter från två eller flera behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig, till exempel när man samkör register?	○	○

Kommentar: Klicka här för att ange text.

Vägledning

Kombinerar ni personuppgifter från två eller flera behandlingar som utförs i olika syften eller av olika personuppgiftsansvariga på ett sätt som den registrerade inte rimligen förväntar sig?

Kriterium 7:	Ja	Nej
Behandlas personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, till exempel barn, anställda, asylsökande, äldre och patienter?	○	○

Kommentar: Klicka här för att ange text.

Vägledning

Om det är obalans i förhållandet mellan de registrerade och den personuppgiftsansvarige behövs särskilda hänsyn. Det kan till exempel vara svårt för de registrerade att lämna ett frivilligt samtycke, att motsätta sig behandling av sina uppgifter eller att utöva sina rättigheter.

Sårbara personer kan till exempel vara

- barn
- anställda hos den personuppgiftsansvarige
- psykiskt sjuka personer
- asylsökande
- äldre personer
- patienter

8) Ska personuppgifterna användas i nya tekniska eller organisatoriska lösningar eller på något nytt och innovativt sätt?

Kriterium 8:	Ja	Nej
Ska personuppgifterna användas i nya tekniska eller organisatoriska lösningar eller på något nytt och innovativt sätt?	○	○

Kommentar: Klicka här för att ange text.

Vägledning

Ny teknik kan innebära att personuppgifter samlas in och används på nya sätt som kan innebära hög risk för enskildas rättigheter och friheter. De personliga och sociala konsekvenserna av användningen av ny teknik kan vara okända.

Exempel:

- Användning av automatiseringar, artificiell intelligens eller så kallade *digitala medarbetare*
- En kombination av fingeravtryck och ansiktsigenkänning för förbättrad fysisk åtkomstkontroll.
- ”Sakernas internet”-applikationer, till exempel smarta mätare, smarta bilar eller anordningar för hemautomatisering kan få betydande konsekvenser för enskildas dagliga liv och integritet.

9) Är det risk för att personuppgiftsbehandlingen i sig hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal?

Kriterium 9:	Ja	Nej
Är det risk för att personuppgiftsbehandlingen i sig hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal?	○	○

Kommentar: Klicka här för att ange text.

Vägledning

Exempel: En bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån.

8.2 Analys av de bedömningskriterierna

Om ett eller flera krierier ovan besvarats jakande så är det rimligt och god sed att genomföra resten av processen med konsekvensbedömningen. Integritetsskyddsmyndigheten (IMY) anger i sina råd om konsekvensbedömningar att om två eller fler kriterier stämmer in på behandlingen så bör det anses tvingande att genomföra en konsekvensbedömning.

8.2 a) Behov av genomföra konsekvensbedömning enligt artikel 35 GDPR:	Ja	Nej
Finns det ett behov, med de nio kriterierna som underlag, och med tanke på personuppgifternas känslighet och omfattning, att genomföra en konsekvensbedömning?	○	○

Notis: Vid osäkerhet i bedömningen rekommenderas att genomföra konsekvensbedömningen, både enligt god sed samt som en försiktighetsprincip, för att tillvarata de registrerades fri- och rättigheter.

8.2 b) Motivera särskilt bedömningen i det fall att att behov inte finns att genomföra en konsekvensbedömning enligt fråga 4.2 a: *(besvaras endast vid NEJ på föregående fråga)*
Svar: Klicka här för att ange text.
Datum och namn på ansvarigt dataskyddsombud då denne har tagit del av underlaget och bedömningen ovan. Datum: Klicka här för att ange text. Dataskyddsombud: Klicka här för att ange text.

9. RISKANALYS FÖR PERSONUPPGIFTSBEHANDLINGEN

9.1 Riskmatrisen för sannolikhet och konsekvens

Riskmatrisen består av en kombination av nivåer för sannolikhet och konsekvens.

Risknivåerna bedöms i allvarlighetsgrad från låg risk, medel risk, hög risk till extrem risk. Riskerna anges i formen A3, C2, D1, dvs bokstaven först för sannolikhetsnivån, sedan i kombination med siffran för nivån av konsekvens.

Sannolikhet				
D	H	H	E	E
C	M	H	H	E
B	L	M	H	H
A	L	L	M	H
	1	**2**	**3**	**4**
	Konsekvens			

9.2 Sannolikhet

Sannolikheten för risker ska bedömas för den aktuella personuppgiftsbehandlingen, dvs. hur troligt det är att den negativa händelsen inträffar.

Sannolikhet		
Nivå	**Sannolikhet**	**Exempel på betydelse**
A	”**Osannolik**” Inträffar mycket sällan	Kan inträffa en gång på 10 år
B	”**Möjlig**” Kan inträffa men inte så ofta	Kan inträffa under ett år
C	”**Trolig**” Kan inträffa återkommande	Kan inträffa fler än en gång per år
D	”**Återkommande**” Kan inträffa ofta	Kan inträffa flera gånger

Sannolikheten bedöms i fyra steg, i nivåerna A till D

Nivåerna i skalan för sannolikhet kan behöva anpassas till verksamhetens kontext.

9.3 Konsekvens

Skadan, dvs konsekvensen av en tänkt negativ händelse ska bedömas i en skala av fyra nivåer.

Konsekvens			
Nivå	**Konsekvens**	**Beskrivning av nivå**	**Potientiell skada**

1	**Låg**	Berörda personer bedöms i låg grad påverkas negativt, materiellt eller immateriellt	Materiella och immaterialla skador (se 10.3)
2	**Begränsad**	Berörda personer bedöms i begränsad omfattning påverkas negativt, materiellt eller immateriellt	Materiella och immaterialla skador (se 10.3)
3	**Betydande**	Berörda personer bedöms i betydande grad påverkas negativt, materiellt eller immateriellt	Materiella och immaterialla skador (se 10.3)
4	**Allvarlig**	Berörda personer bedöms i allvarlig grad påverkas negativt, materiellt eller immateriellt	Materiella och immaterialla skador (se 10.3)

Konsekvensen kännetecknar den möjliga skadan och bedöms i fyra nivåer

Det är viktigt att beakta orsakerna till riskerna för de skador som kan uppkomma, t.ex.

- brister i tekniska skyddsåtgärder,
- organisationsbrister,
- brist på uppföljning,
- brist på incidentförmåga, m.m.

9.4 Skador till följd av risker i hantering av personuppgifter

I en konsekvensbedömning ska risker *inventeras, analyseras, och hanteras* för en tänkta händelser, som i negativt påverkar *de registrerades rättigheter och friheter* eller den personuppgiftsansvariges ansvar att säkert hantera dessa personuppgifter.

Brister i hantering av personuppgifter kan leda till både *materiell* och *immateriell* skada:

a) Materiell skada: påtaglig, fysisk eller ekonomiska skador för individer så som:
   - Kroppslig skada
   - Förlust av frihet eller frihet till rörelse
   - Skada på inkomstförmåga och finansiell skada, och
   - Andra skador på ekonomiska intressen, till exempel följder från identitetsstöld

b) Immateriell skada: t.ex. oro/ångest för individer:
   - Skador som följd av övervakning eller exponering av identitet, egenskaper, aktivitet, samrören eller åsikter
   - Inskränkande påverkan av yttrandefrihet, frihet till organisering, etc
   - Skada för rykte
   - Förlägenhet eller social rädsla som rör personlig, familj, arbetsplats
   - Oacceptabelt intrång i privatlivet
   - Olaglig diskriminering eller stigmatisering
   - Skada på eller förlust av autonomi/självständighet
   - Olämplig begränsning av det personliga fria valet
   - Identitetsstöld
   - Förlust av kontroll över personuppgifter

9.5 Riskkartläggning

Riskerna kartläggs i olika risknivåer enligt matrisen ovan (punkterna 7.1 och 7.2). Varje risk beskrivs och bedöms samt vilken riskreducerande åtgärd som behövs för att hantera risken. De kvarstående riskerna beskrivs och bedöms på samma sätt som den ursprungliga risken. På så sätt kan de verksamhetsansvariga ges en bedömd effekt, som beslutsunderlag, för vilka av de beskrivna riskreducerande åtgärderna som ska genomföras.

9.5.1 Risker för fri- och rättigheter för de registerade

Sök att identifiera risker för fri- och rättigheter för de registrerade i relation med ***principerna för dataskydd*** (GDPR artikel 5) då personuppgifterna kan riskera vara:

a) Felaktiga, otillräckliga eller inte uppdaterade
b) Överflödiga eller irrelevanta
c) Sparas för länge
d) Delges till fel personer eller parter
e) Används på ej godkända sätt eller på sätt som inte kan förutses av de registrerade
f) Lagras eller överförs på ett ej skyddat sätt

9.5.1) Vilka möjliga risker, som rör principerna för dataskydd, kan förekomma för den aktuella behandlingen? (svara i formen ”a, d, e”)
Svar: Klicka här för att ange text.

9.5.2 Faktiska risker kopplade till personuppgifter

De faktiska riskerna mot personuppgifter kan innefatta:

g) It-angrepp/hacking
h) Virus och skadlig kod
i) Läckage eller skada genom intrång
j) Phishing-aktiviteter
k) Otillräckligt utbildad personal
l) Okrypterade laptops utanför arbetsplatsen
m) Brister i behörighetsstyrning
n) Svaga lösenord

9.5.2) Vilka är de möjliga faktiska riskerna mot personuppgifterna i den aktuella behandlingen? (svara i formen ”g, h, m”)
Svar: Klicka här för att ange text.

9.5.3 Tre kategorier av risker

Anpassade risker till området dataskydd kan formuleras i tre olika kategorier.

Risker för:

A) obehörig åtkomst till personuppgifter,
B) oönskade förändringar av personuppgifter,
C) förlust av personuppgifter

Risker i varje kategori (A-C) inventeras självständigt, för att sedan samlat hanteras i steget för riskhantering, då åtgärder föreslås för att behandla de inventerade riskerna.

De identifierade riskkategorierna behöver formuleras i **konkreta riskexempel**. Det sker i de nästföljande avsnitten 9.6-9.8.

9.6 Obehörig åtkomst till personuppgifter

Obehörig åtkomst eller förlust av åtkomst innebär att obehöriga tar del av personuppgifter eller att behöriga personer av någon anledning inte längre kommer åt uppgifter som de behöver i sina uppdrag.

Redogör för riskerna nedan genom att *utgå från de inventerade risktyperna* i stegen:

- 9.4 a-b (materiella och immateriella skador),
- 9.5.1 (risker för fri- och rättigheter) samt
- 9.5.2 (faktiska risker)

Notera att det är viktigt att riskerna formuleras som en konkret skada som kan uppkomma pga en orsak (t.ex. ”A inträffar på grund av B”). *Om riskerna inte formuleras som en konkret skada kommer inte konsekvensen att kunna bedömas.*

Exempel: ”Jag blir påkörd av en bil och bryter ett ben på grund av att jag inte ser mig om vid övergångsstället”.

I exemplet är **skadan** det brutna benet när jag blir påkörd av en bil, men **orsaken** är *riskbeteendet* att jag inte ser mig om vid övergångsstället.

Redogör för riskerna nedan (ta avsnitt 9.4 a-b i beaktande)

Kategori A Risker för obehörig åtkomst till personuppgifter eller förlust av åtkomst	Sannolikhet att skadan inträffar	Konsekvens om skadan inträffar	Risknivå
Risk A1: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk A2: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk A3: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk A4: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk A5: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk A6: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk A7: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk A8: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk A9: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.

Notis: Om fler rader krävs så utöka matrisen

9.7 Obehörig eller oönskad ändring av personuppgifter

Obehörig ändring innebär att personuppgifter ändras av obehöriga parter som inte ska få ta del av uppgifterna. Oönskad ändring innebär att ändring sker på ett sätt som inte är planerat eller avsett, t.ex. genom brister i rutiner och processer.

Redogör för riskerna nedan (ta avsnitt 9.4 a-b i beaktande)

Kategori B Risker för obehörig eller oönskad förändring av personuppgifter	Sannolikhet att skadan inträffar	Konsekvens om skadan inträffar	Risknivå

Risk B1: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk B2: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk B3: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk B4: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk B5: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk B6: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk B7: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk B8: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk B9: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.

Notis: Om fler rader krävs så utöka matrisen

9.8 Förlust av personuppgifter

Förlust av personuppgifter innebär att uppgifter skadats eller raderats så att de inte går att använda.

Redogör för riskerna nedan (ta avsnitt 9.4 a-b i beaktande)

Kategori C Risker för förlust av personuppgifter	Sannolikhet att skadan inträffar	Konsekvens om skadan inträffar	Risknivå
Risk C1: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk C2: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk C3: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk C4: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk C5: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk C6: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk C7: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk C8: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Risk C9: Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.

Notis: Om fler rader krävs så utöka matrisen

10. RISKBEHANDLING

Identifiera åtgärder som kan reducera eller eliminera risker i stegen 10.5 (Å), 10.6 (Ä) och 10.7 (F) som har ***medel- eller hög risknivå*** (låga risker ska inte accepteras, men instrumentet konsekvensbedömning syftar till att stödja verksamheten att behöva hantera sannolika höga risknivåer vid personuppgiftsbehandlingar.

Risk (urval: A1-9, B1-9, C1-9)	Åtgärder för reducera eller eliminera risker	Effekt på risk	Kvarstående risk	Åtgärd godkänd för genomförande
Risk: Klicka här för att ange text.	Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Kommentarer: Klicka eller tryck här för att ange text.				
Risk: Klicka här för att ange text.	Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Kommentarer: Klicka eller tryck här för att ange text.				
Risk: Klicka här för att ange text.	Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.

Kommentarer: Klicka eller tryck här för att ange text.				
Risk: Klicka här för att ange text.	Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Kommentarer: Klicka eller tryck här för att ange text.				
Risk: Klicka här för att ange text.	Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Kommentarer: Klicka eller tryck här för att ange text.				
Risk: Klicka här för att ange text.	Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Kommentarer: Klicka eller tryck här för att ange text.				
Risk: Klicka här för att ange text.	Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Kommentarer: Klicka eller tryck här för att ange text.				
Risk: Klicka här för att ange text.	Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Kommentarer: Klicka eller tryck här för att ange text.				
Risk: Klicka här för att ange text.	Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Kommentarer: Klicka eller tryck här för att ange text.				
Risk: Klicka här för att ange text.	Klicka här för att ange text.	Välj ett objekt.	Välj ett objekt.	Välj ett objekt.
Kommentarer: Klicka eller tryck här för att ange text.				

Notis: Om fler rader krävs så utöka matrisen

10.1 Kvarstående risker

Kvarstående höga risker	
Finns i punkt 10 ovan en eller flera höga risker kvar?	◯ Ja ◯ Nej
Beskriv nedan bedömningen av de kvarvarande höga riskerna: Klicka eller tryck här för att ange text.	

11. INFORMATIONSSÄKERHET OCH RISKHANTERING

En konsekvensbedömning ska enligt god sed integrera mot bästa praxis för organisationens risk- och säkerhetsarbete. En central bedömning för informationssäkerhet är att de verksamhetsansvariga informationsklassificerar de processer och information som de ansvarar för.

En informationsklassificering är just en dokumenterad konsekvensbedömning för att, för att möta verksamhetens behov, bestämma nivån av nödvändigt skydd för en process och dess tillhörande information. Därför blir det av stor vikt att en noggrann informationsklassificering genomförs samt att organisationen har en fungerande metodik att koppla verksamhetens krav till relevanta skyddsåtgärder, i detta fall de svenska versionerna av ISO-standarderna för informationssäkerhet (SS-ISO/IEC 27001 kravstandard och 27002 Vägledning till säkerhetsåtgärder).

Riktlinjer för informationssäkerhet styr övergripande i Stockholms stad all hantering av informationssäkerhet och dataskydd. En del i den obligatoriska metodstyrningen är användningen av SKR:s metodstöd KLASSA vilket kontrolleras för den aktuella personuppgiftsbehandlingen i uppföljningsmatrisen nedan.

Informationsklassificering och riskhantering			Ja	Nej
11.1 a) PuA fastställer skyddsnivån genom informationsklassificering Har den personuppgiftsansvarige fastställt en informationsklassificering av personuppgiftsbehandlingens process?			○	○
11.1 b) Ange datum och nivåerna för den fastställda informationsklassificeringen (ÅÅÅÅ-MM-DD): Klicka eller tryck här för att ange text.	**Konfidentialitet:** Välj ett objekt.	**Riktighet:** Välj ett objekt.	**Tillgänglighet:** Välj ett objekt.	
11.2 PuA kontrollerar efterlevnad av skyddsåtgärderna Har den personuppgiftsansvarige genomfört en självskattning hur säkerhetsåtgärderna efterlevs som utgår från den fastställda informationsklassificeringen?			○	○
11.3 PuA kopplar skyddsåtgärderna till ISO-standarden Beskriver självskattningen detaljerade krav i SS-ISO/IEC 27002 (2017), dvs. vägledningarna för de rekommenderade säkerhetsåtgärderna i ISO-standarden för informationssäkerhet?			○	○
11.4 PuA upprättar en handlingsplan för att behandla säkerhetsbristerna Har den personuppgiftsansvarige fastställt en åtgärdslista med prioriteringsordning utifrån bristerna för säkerhetsåtgärderna i punkt 3.2?			○	○
11.5 PuA reducerar säkerhetsbrister Har den personuppgiftsansvarige reducerat riskerna enligt handlingsplanen?			○	○
11.6 PuA bedömer de kvarvarande riskerna Finns det en eller flera högt prioriterade brister i åtgärdslistan som ännu inte har åtgärdats?			○	○
11.7 KRAVSTÄLLNING (PUA): Har personuppgiftsbiträdet delgivits upphandlingskraven som utgår från informationsklassificeringen?			○	○
11.8 EFTERLEVNAD (PUB): Har personuppgiftsbiträdet genomfört en självskattning av hur upphandlingskraven efterlevs?			○	○
11.9 ISO-STANDARD (PUB): Beskriver personuppgiftsbiträdets självskattning detaljerade krav i SS-ISO/IEC 27002 (2017), dvs. vägledningarna för de rekommenderade säkerhetsåtgärderna i ISO-standarden för informationssäkerhet?			○	○

11.10 RISKREDUCERING (PUB): Har personuppgiftsbiträdet, i samverkan med den personuppgiftsansvarige, fastställt en åtgärdslista för att åtgärda de mest prioriterade bristerna?	○	○
11.11 KVARVARANDE RISKER (PUB): Finns det en eller flera högt prioriterade brister som personuppgiftsbiträdet inte efterlever?	○	○
11.12 KONTROLL AV EFTERLEVNAD (PUA): Har den personuppgiftsansvarige genomfört kontroll (t.ex. stickprov) av personuppgiftsbiträdets självskattning?	○	○
11.13 RISKBESLUT (PUA): Har den personuppgiftsansvarige dokumenterat beslutat om hantering av de kvarvarande riskerna?	○	○
Kommentarer till punkterna 11.1-11.13 ovan, t.ex. hur säkerhetskraven kan hanteras: Klicka eller tryck här för att ange text.		

12. CHECKLISTA FÖR EN GODTAGBAR KONSEKVENSBEDÖMNING

Den europeiska dataskyddsstyrelsens arbetsgrupp (Artikel 29-gruppen) har fastslagit följande checklista med kriterier för en godtagbar konsekvensbedömning[1]. Checklistan används här som en *kvalitetskontroll* av den nu genomförda konsekvensbedömningen huruvida den har tillräckligt god kvalitet eller om förbättringar behövs.

Arbetsgruppen föreslår följande kriterier som kan användas av personuppgiftsansvariga för att bedöma huruvida en konsekvensbedömning, eller en metod för att utföra en konsekvensbedömning, är tillräckligt omfattande för att iaktta förordningen.

Uppfyller konsekvensbedömningen följande kravegenskaper enligt riktlinjen från den europeiska dataskyddsstyrelsen?

☐ 12.1 En systematisk beskrivning av behandlingen tillhandahålls (artikel 35.7 a):
- ☐ 12.1.1 Behandlingens art, omfattning, sammanhang och ändamål beaktas (skäl 90).
- ☐ 12.1.2 Registrering av personuppgifter, mottagare och den period under vilken personuppgifterna kommer att lagras.
- ☐ 12.1.3 En funktionell beskrivning av behandlingen tillhandahålls.
- ☐ 12.1.4 De tillgångar som är nödvändiga för personuppgifterna (maskinvara, programvara, nätverk, personer, papper eller spridningskanaler för papper) är identifierade.
- ☐ 12.1.5 Efterlevnad av godkända uppförandekoder beaktas (artikel 35.8).

☐ 12.2 En bedömning av behovet av och proportionaliteten hos behandlingen (artikel 35.7 b):
- ☐ 12.2.1 De planerade åtgärderna för att visa att förordningen efterlevs har fastställts (artikel 35.7 d och skäl 90), med beaktande av följande:
  - ☐ 12.2.1.1 Åtgärder som bidrar till att behandlingen är proportionell och nödvändig på grundval av
    - ☐ 12.2.1.1.1 särskilda, uttryckligt angivna och berättigade ändamål (artikel 5.1 b),
    - ☐ 12.2.1.1.2 laglig behandling (artikel 6),
    - ☐ 12.2.1.1.3 adekvata, relevanta och inte för omfattande uppgifter (artikel 5.1 c),
    - ☐ 12.2.1.1.4 begränsad lagringstid (artikel 5.1 e).

[1] Checklista för kriterier för en godtagbar konsekvensbedömning från den europeiska dataskyddsstyrelsen (f.d. Artikel-29 gruppen) https://www.imy.se/globalassets/dokument/riktlinjer-om-konsekvensbedomning-avseende-dataskydd.pdf

☐ 12.2.1.2 Åtgärder som stärker de registrerades rättigheter:
- ☐ 12.2.1.2.1 Information till den registrerade (artiklarna 12, 13 och 14).
- ☐ 12.2.1.2.2 Rätt till tillgång och till dataportabilitet (artiklarna 15 och 20).
- ☐ 12.2.1.2.3 Rätt till rättelse och radering (artiklarna 16, 17 och 19).
- ☐ 12.2.1.2.4 Rätt att göra invändningar och till begränsning av behandling (artiklarna 18, 19 och 21).
- ☐ 12.2.1.2.5 Förhållandet till personuppgiftsbiträden (artikel 28).
- ☐ 12.2.1.2.6 Skyddsåtgärder för internationella överföringar (kapitel V).
- ☐ 12.2.1.2.7 Förhandssamråd (artikel 36).

☐ 12.3 Hantering av risker för de registrerades rättigheter och friheter (artikel 35.7 c):
- ☐ 12.3.1 Uppskattning av riskens ursprung, art, särdrag och allvar (se skäl 84) eller, mer specifikt, för varje risk (obehörig åtkomst, oönskad ändring och att uppgifter försvinner) ur de registrerades perspektiv:
  - ☐ 12.3.1.1 Beaktande av riskens ursprung (skäl 90).
  - ☐ 12.3.1.2 Identifiering av möjliga konsekvenser för de registrerades rättigheter och friheter vid händelser, däribland obehörig åtkomst, oönskad ändring och förlust av uppgifter.
  - ☐ 12.3.1.3 Identifiering av hot som kan leda till obehörig åtkomst, oönskad ändring och förlust av uppgifter.
  - ☐ 12.3.1.4 Uppskattning av sannolikhetsgrad och allvar (skäl 90).
- ☐ 12.3.2 Fastställande av planerade åtgärder för att hantera dessa risker (artikel 35.7 d och skäl 90).

☐ 12.4 Medverkan från berörda parter:
- ☐ 12.4.1 Rådfrågan av dataskyddsombudet (artikel 35.2).
- ☐ 12.4.2 När så är lämpligt, inhämtning av synpunkter från de registrerade eller deras företrädare (artikel 35.9).

Kommentarer, behöver något förbättras? (referera till ovan numrerade punkter)
Klicka eller tryck här för att ange text.

13. PERSONUPPGIFTSANSVARIG FASTSTÄLLER KONSEKVENSBEDÖMNINGEN

Konsekvensbedömningen fastställs av ansvarig verksamhetsrepresentant för den personuppgiftsansvarige
Beslutsdatum: Klicka eller tryck här för att ange datum. **Beslutsfattare**: Klicka eller tryck här för att ange text. **Befattning/roll:** Klicka eller tryck här för att ange text.
Kvarstående risker: ○ Inga sannolika höga risker för registrerade kvarstår i den aktuella behandlingen eller grupp av behandlingar ○ En eller flera sannolika höga risker kvarstår i den aktuella behandlingen eller grupp av behandlingar *Notera*: Om en eller flera höga risker kvarstår ska ett förhandssamråd ske med Integritetsskyddsmyndigheten (IMY) före den planerade behandlingen får genomföras (länk till IMY:s instruktion)
Dataskyddsombudet bör rådge efterlevnaden med säkerhet och riskhantering samt en bedömning om behandlingen kan genomföras med en adekvat skyddsnivå för behandlingen av personuppgifterna Dataskyddsombud (namn): Klicka här för att ange text. **Dataskyddsombudets råd:**

Klicka här för att ange text.

Sammanfattning av dataskyddsombudets råd:

- ○ DSO råder att behandlingen kan genomföras enligt föreslagen hantering i konsekvensbedömningen
- ○ DSO råder att kompleterande åtgärder behöver ske innan behandlingen kan genomföras (kommenteras)
- ○ DSO avråder från att genomföra den planerade behandlingen på grund av höga risker för de registrerades friheter och rättigheter avseende personuppgifter

Kommentar om kompletterande åtgärder: Klicka här för att ange text.

PuA:s följsamhet till dataskyddsombudets rådgivning

- ○ Rådgivningen accepteras i sin helhet
- ○ Rådgivningen accepteras delvis
- ○ Rådgivningen accepteras ej

Redogör för skälen till att dataskyddsombudets råd avvisas (helt eller delvis):
Klicka här för att ange text.

PuA utser en medarbetare med ett särskilt ansvar för genomförande av behandlingens handlingsplan rörande hantering av eventuella säkerhetsbrister i relation med denna konsekvensbedömning.
Utsedd person: Klicka här för att ange text.

Notera:
Verksamhetens dataskyddsombud ska beredas möjlighet att systematiskt och riskbaserat, *med stöd av verksamhetens informationssäkerhetssamordnare*, granska och följa den pågående efterlevnaden av konsekvensbeskrivningens dokumentation och slutförande av aktiviteterna i handlingplanen samt hanteringen av de kvarvarande riskerna.