Konsekvensbedömning avseende dataskydd

enligt art. 35 GDPR för vård- och omsorgsverksamhet

Sveriges Kommuner och Regioner

Mallen

Denna mall är framtagen maj 2022 av Kompetenscenter välfärdsteknik, SKR, med syfte att användas vid konsekvensbedömningar av dataskydd inom kommunal vård- och omsorg. Mallen får fritt användas och anpassas till verksamhetens egna rutiner för konsekvensbedömningar.

Ange system, tjänst, program eller art av personuppgiftsbehandling

Versionshistorik mall

Vers.	Datum	Revision och ändringar	Författare	God-kännare

Versionshistorik konsekvensbedömning

Vers.	Datum	Revision och ändringar	Författare	God-kännare

Innehåll

1 Sammanfattande bedömning

Sammanfattande bedömning från avsnitt 9.3

2 Varför en konsekvensbedömning?

2.1 Vad är en konsekvensbedömning?

Av artikel 35.1 i dataskyddsförordningen (GDPR) följer att den personuppgifts-ansvarige ska utföra en dataskyddskonsekvensbedömning om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter (konsekvensbedömning). Syftet med en konsekvensbedömning är att förebygga risker för registrerades personliga integritet innan de uppkommer.

Konsekvensbedömningen är en process för att

- ta reda på vilka risker som finns med att behandla personuppgifter
- ta fram rutiner och åtgärder för att reducera eller eliminera dessa risker och
- visa för registrerade, samverkansparter eller tillsynsmyndighet att man uppfyller GDPR:s krav.

Det är den personuppgiftsansvarige som ansvarar för att genomföra en konsekvensbedömning. Personuppgiftsansvarig är en juridisk eller fysisk person som ensam eller tillsammans med andra bestämmer ändamålen med eller medlen för en viss behandling av personuppgifter.

En dataskyddskonsekvensbedömning går längre än en riskanalys på så sätt att den, förutom en riskanalys också ska beakta åtgärder för att reducera eller eliminera risker samt en sammantagen bedömning om huruvida hög risk för enskildas fri- och rättigheter vid personuppgiftsbehandling kvarstår. Kvarstår en hög risk, trots tekniska och organisatoriska kompensatoriska åtgärder, kan den personuppgiftsansvarig välja att begära förhandssamråd hos Integritetsskydds-myndigheten eller avstå från behandlingen.

Ytterligare information om dataskyddsförordningen finns på Integritetsskydds-myndighetens hemsida
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/

2.2 När krävs en konsekvensbedömning

Det inte obligatoriskt att utföra en konsekvensbedömning för varje behandling av personuppgifter. Av GDPR framgår att en konsekvensbedömning krävs om en viss typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter (artikel 35.1 och skäl 84 GDPR).

En konsekvensbedömning krävs enligt GDPR särskilt i följande fall:

1. Vid en systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.
2. Vid en behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1 (ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.), eller av personuppgifter som rör fällande domar i brottmål och överträdelser.
3. Systematisk övervakning av en allmän plats i stor omfattning.

Enligt artikel 35.4 GDPR ska respektive nationell tillsynsmyndighet upprätta och offentliggöra en förteckning över behandlingar som kräver en konsekvens-bedömning. Integritetsskyddsmyndigheten har, med ledning av riktlinjer från Europeiska dataskyddsstyrelsen, EDPB, publicerat en förteckning över när en konsekvensbedömning ska göras och som kompletterar GDPR:s krav. Förteckningen finns på Integritetsskyddsmyndighetens hemsida, Förteckning enligt artikel 35.4 i Dataskyddsförordningen (imy.se)

Förteckningen är dock inte uttömmande och kan komma att uppdateras och kompletteras med fler exempel framöver. Förteckningen gäller oavsett om det är fråga om personuppgiftsbehandling enbart i Sverige eller behandling av personuppgifter som är att anse som gränsöverskridande enligt definitionen i GDPR, artikel 4.23.

2.3 När ska konsekvensbedömningen göras?

En konsekvensbedömningen ska som huvudregel utföras innan en behandling påbörjas, men kan aktualiseras

- om risken med en pågående behandling ändras eller
- för pågående behandlingar om det inte har gjorts tidigare.

2.4 När behövs inte en konsekvensbedömning?

- Om det redan har gjorts en konsekvensbedömning för en behandling som är mycket lik den planerade behandlingen; resultatet från den tidigare konsekvensbedömningen kan användas.
- Om den planerade personuppgiftsbehandlingen inte sannolikt leder till en hög risk för enskildas fri- och rättigheter.
- Behandlingar som har kontrollerats av en tillsynsmyndighet eller ett dataskyddsombud i enlighet med artikel 20 i direktiv 95/46/EG (dataskyddsdirektivet, dvs. före GDPR:s ikraftträdande) och vars genomförande inte har ändrats sedan föregående kontroll.

2.5 Vad ska en konsekvensbedömning innehålla?

Det finns fyra grundläggande krav i GDPR på vad en konsekvensbedömning ska innehålla.

1. En systematisk beskrivning av den planerade behandlingen och behandlingens syfte.
2. En bedömning av om behandlingen är nödvändig och proportionerlig i förhållande till syftet med den.
3. En bedömning av riskerna för de registrerades rättigheter och friheter.
4. De åtgärder som planeras för att hantera riskerna och för att visa att GDPR efterlevs.

Därutöver bör en sammantagen bedömning redovisas i konsekvens-bedömningen, bl.a. om hög risk för enskildas fri och rättigheter kvarstår eller inte efter att kompensatoriska åtgärder planeras.

Dessutom ska man dokumentera att man

- rådgjort med dataskyddsombudet (om sådan finns) och
- inhämtat synpunkter från de registrerade eller deras företrädare när det är lämpligt.

För mer information, se Integritetsskyddsmyndighetens hemsida.

3 Övergripande information om behandlingen

3.1 Personuppgiftsansvarig(a) för personuppgiftsbehandlingen

Ange personuppgiftsansvarig(a) för personuppgiftsbehandlingen

3.2 Kontaktuppgifter till dataskyddsombud

Ange kontaktuppgifter till dataskyddsombud

3.3 Ansvarig(a) för konsekvensbedömningen

3.3.1 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

3.3.2 Förvaltning

Namn och e-post till den/de som ansvarar för att förvalta konsekvensbedömningen, vilket innebär att se till att den är aktuell och att åtgärderna är fortsatt effektiva om behandlingen, omständigheter eller risker ändras

3.4 Projektinformation

Om personuppgiftsbehandlingen planeras inom ett projekt, ange projektnamn och eventuellt projekt-ID

3.5 Systeminformation

Om personuppgiftsbehandlingen sker eller kommer att ske inom ett it-system, ange systemnamn och system-ID

3.6 Kortfattad beskrivning av personuppgiftsbehandlingen

Beskriv kortfattat projektet, it-systemet, den nya funktionen i it-systemet etc. som behandlingen omfattar. Denna information kan exempelvis finnas i en projektplan. Beskriv även avgränsningen för denna konsekvensbedömning

3.7 Personuppgiftsbehandlingens effektmål

Beskriv vilka förväntade effekter personuppgiftsbehandlingen kommer att få för den registrerade

Beskriv vilka förväntade effekter behandlingen kommer att få för verksamheten och i ett bredare perspektiv, exempelvis för vård- och omsorg i ett regionalt eller nationellt perspektiv

3.8 Extern samverkan

Om konsekvensbedömningen ska genomföras inom ramen för ett större projekt eller ett program ska ansvarig förvaltningschef (motsvarande) rådfrågas avseende genomförande, resurssättning och behov av externa resurser.

☐	Förvaltningschef (motsvarande) har rådfrågats
☐	Ej tillämplig för denna konsekvensbedömning

4 Identifiering av att en konsekvensbedömning ska genomföras (högriskutvärdering)

4.1 Om personuppgiftsbehandlingen sannolikt innebär en hög risk

I IMY:s förteckning över ”när en konsekvensbedömning ska göras” räknas ett flertal kriterier upp. Enligt anvisningarna ska en konsekvensbedömning genomföras om minst två kriterier i förteckningen är uppfyllda.

Genom att svara på frågorna i avsnitt 4.1.1. och 4.1.2 kan man avgöra om behandlingen sannolikt innebär en hög risk för den registrerades rättigheter och friheter och därför kräver en konsekvensbedömning. Frågorna är baserade på IMY:s förteckning. Vid bedömningen om behandlingen sannolikt innebär en hög risk är det lämpligt att ta hjälp av dataskyddsombudet.

4.1.1 Kriterier för hög risk (art. 35.3 GDPR)[1]

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

Kriterium	Ja	Nej
Systematisk och omfattande profilering som har rättsliga följder för individer eller på liknande sätt i betydande grad påverkar individer	☐	☐
Behandling i stor omfattning av känsliga personuppgifter	☐	☐
Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser	☐	☐
Systematisk övervakning av en allmän plats i stor omfattning	☐	☐

4.1.2 Kontrollfrågor för sannolik hög risk[2]

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

Kriterium	Ja	Nej
Kommer personer att analyseras, utvärderas, profileras eller poängsättas på något sätt?	☐	☐
Kommer det fattas automatiserade beslut med rättsliga eller liknande betydande följder för den registrerade?	☐	☐
Personuppgiftsbehandlingen innefattar att systematisk övervakning används för att observera, övervaka eller kontrollera den registrerade?	☐	☐
Omfattar personuppgiftsbehandlingen känsliga personuppgifter eller personuppgifter av mycket personlig karaktär?	☐	☐

[1] Kriterierna definieras i GDPR art. 35.3.

[2] Kontrollfrågorna utgår från Integritetsskyddsmyndighetens publicerade lista över när konsekvensbedömningar behöver göras: https://www.imy.se/lagar--regler/dataskyddsforordningen/konsekvensbedomningar-och-forhandssamrad/forteckning-konsekvensbedomning/

Kriterium	Ja	Nej
Kommer personuppgifter att behandlas i stor omfattning?	☐	☐
Kommer olika register att samköras?	☐	☐
Rör personuppgifterna sårbara personer, till exempel barn, anställda, asylsökande, äldre och patienter?	☐	☐
Kommer teknik användas på ett nytt och innovativt sätt eller kommer nya organisatoriska lösningar användas?	☐	☐
Är det risk för att personuppgiftsbehandlingen i sig hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal?	☐	☐

4.1.3 Övriga faktorer som leder till hög risk

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

[Exempel:

- Tjänsteleverantören omfattas av extraterritoriell lagstiftning oavsett var denne bedriver sin verksamhet i världen
- Tredjelandsöverföring
- Komplexa molntjänstavtal
- Leverantören anlitar ett flertal samarbetspartners med vilka denne delar registrerades uppgifter avseende olika ändamål, såsom marknadsföring, support, felsökning, forskning m.m.
- En stor mängd personuppgiftsbiträden och underbiträden i Sverige och utomlands
- Stor förekomst av kakor (cookies) i leverantörens appar och websida som har andra funktioner än att bara vara nödvändiga för tjänstens funktionalitet, t.ex. marknadsföring och analys]

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

4.1.4 Undantag från att genomföra en konsekvensbedömning (art. 35.3 GDPR)

En konsekvensbedömning behöver inte genomföras om något av följande kriterier uppfylls. Om ”ja” väljs för något av kriterierna ska detta motiveras och en dataskyddssamordnare (motsvarande) ska skriva ett utlåtande i avsnitt 9.2 och i sammanfattande bedömning (avsnitt 1).

Kriterium	Ja	Nej	Motivering
Behandlingen leder sannolikt inte till höga risker	☐	☐	
Behandlingens art, omfattning, sammanhang och ändamål är mycket lika en behandling för vilken en konsekvensbedömning redan har genomförts inom kommunen	☐	☐	
Behandlingen är godkänd av antingen ett personuppgiftsombud eller tillsynsmyndigheten (Datainspektionen) i tiden före GDPR	☐	☐	

5 Systematisk beskrivning av personuppgiftsbehandlingen

Detta avsnitt ska ge en tydlig överblick över de aktuella personuppgiftsbehandlingarna (art. 35.7 a GDPR).

5.1 Beskrivning av behandlingar

Att tänka på: Hur samlas personuppgifter in, används, lagras och raderas? Vad är källan till personuppgifterna? Är det ”personuppgifter” per definition enligt GDPR? Kommer personuppgifterna att delas med någon? Finns personuppgiftsbiträden? Är det en molntjänst? Det kan vara användbart att referera till ett flödesdiagram eller annat sätt att beskriva dataflöden (se nedan). Ändamål: Vad ska uppnås med behandlingen?

Person-uppgifts-behandling (typ av behandlingar)	**Ändamål**	**Person-uppgifter**	**Person-uppgifts-biträde**	**Kategorier av registrerade**	**Insamling**	**Externa mottagare**	**Lagring/ lagringstid**	**Radering/ arkivering**

5.2 Översiktlig beskrivning av personuppgiftsflödet

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

Kommentar till den schematiska bilden som bifogas som en separat bilaga

5.3 Ny, innovativ eller kontroversiell personuppgiftsbehandling

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

Ange om det finns känd problematik med liknande personuppgiftsbehandlingar samt om personuppgiftsbehandlingen anses vara ny, innovativ eller kontroversiell på något sätt

5.4 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.

5.4.1 Känsliga personuppgifter

Utgå från svaren i avsnitt 5.1 och sammanfatta vilka känsliga personuppgifter (art. 9 GDPR) eller andra integritetskänsliga eller särskilt skyddsvärda personuppgifter (art. 10 och 87 GDPR) som behandlas.[3]

Sammanfatta vilka känsliga personuppgifter eller andra integritetskänsliga eller särskilt skyddsvärda personuppgifter som behandlas

5.4.2 Mängd registrerade

Uppskatta hur många registrerade som kommer att påverkas av personuppgiftsbehandlingen

5.4.3 Mängd personuppgifter

Ange hur många personuppgifter som uppskattningsvis kommer att behandlas

5.4.4 Behandlingens geografiska räckvidd

Beskriv personuppgiftbehandlingens geografiska räckvidd

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

5.4.5 Nödvändiga informationstillgångar

Specificera de informationstillgångar som är nödvändiga för att personuppgiftsbehandlingen ska gå att genomföra

5.5 Finns uppförandekoder

Ange om uppförandekod finns

5.6 Den registrerades kontroll över sina personuppgifter

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

6 Uppfyllnad av grundläggande dataskyddsprinciper

I detta avsnitt dokumenteras hur de grundläggande dataskyddsprinciperna (art. 5 GDPR) uppfylls. Bedömningen innefattar en behovs- och proportionalitetsbedömning enligt följande: Vilken är den rättsliga grunden för behandlingen? Uppnår behandlingen faktiskt syftet? Finns det ett annat sätt att uppnå samma resultat? Hur undviks ”ändamålsglidningar”? Hur säkerställs datakvalitet och uppgiftsminimering.

6.1 Laglighet

Ange vilken rättslig grund som behandlingen stödjer sig på (art. 6 GDPR).[4] Förekommer flera behandlingar med olika rättsliga grunder behöver det framgå tydligt vilken rättslig grund som gäller för respektive personuppgiftsbehandling.

Om känsliga personuppgifter (art. 9 GDPR) behandlas, ange vilket undantag som möjliggör behandlingen (art. 9.2 GDPR).

Personuppgifts-behandling	Rättslig grund	Motivering	Undantag som möjliggör behandling av känsliga personuppgifter
	Klicka här. Välj rätt		Klicka här. Välj un

6.2 Ändamål

6.2.1 Andra lämpliga sätt att uppnå ändamålet

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

6.2.2 Nödvändighet

Om behandlingen bygger på en annan rättslig grund än samtycke, beskriv varför den planerade behandlingen är *nödvändig* för att uppnå ändamålet samt varför man valt detta sätt att uppnå ändamålet snarare än något av de andra lämpliga sätten som beskrivits i 6.2.1.

Beskriv varför den planerade behandlingen är nödvändig för att uppnå ändamålet samt varför man valt detta sätt att uppnå ändamålet

[4] Vägledning om de rättsliga grunderna finns på IMY:s webbplats: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/

Om den planerade behandlingen bygger på den rättsliga grunden samtycke, beskriv varför den planerade personuppgiftsbehandlingen har valts samt varför man valt detta sätt att uppnå ändamålet snarare än något av de andra lämpliga sätten som beskrivits i 6.2.1.

Beskriv varför den planerade personuppgiftsbehandlingen har valts samt varför man valt detta sätt att uppnå ändamålet

6.2.3 Ändamålsglidning

Beskriv hur ändamålsglidning motverkas

6.3 Uppgiftsminimering

Redogör för både tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna är adekvata, relevanta och inte för omfattande i förhållande till det specificerade ändamålet

6.4 Lagringsminimering

Ange hur det tekniskt och organisatoriskt säkerställs att personuppgifter endast lagras så länge de behövs[5]

[5] Se kommunens regelverk för bevarande och gallring eller kontakta arkivarie.

7 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 GDPR). Åtgärderna kan vara organisatoriska, som framtagande av en rutin för handläggning och att utse ansvariga, och tekniska, t. ex. att 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 GDPR). Avsnittet berör följande frågor: Vilken information kommer personuppgiftsansvarig att ge individer? På vilket sätt? Hur ska deras rättigheter främjas? Vilka åtgärder ska vidtas för att säkerställa att personuppgiftsbiträden följer vidtagna åtgärder om dataskydd? Hur ska överföringar av personuppgifter till andra länder skyddas?

7.1 Information till den registrerade (art. 12, 13 och 14 GDPR)

Beskriv hur information om personuppgiftsbehandlingen utformats och kommer att lämnas till den registrerade

7.2 Rätt till tillgång (registerutdrag) (art. 15 GDPR)

Beskriv hur den registrerades rätt till tillgång (registerutdrag) säkerställs

7.3 Rätt till dataportabilitet (art. 20 GDPR)

Om applicerbart, ange hur den registrerades rätt till dataportabilitet säkerställs

7.4 Rätt till rättelse (art. 16 och 19 GDPR)

Ange hur den registrerades rätt till rättelse säkerställs

7.5 Rätt till radering (art. 17 och 19 GDPR)

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

7.6 Rätt att göra invändningar och rätt till begränsning av personuppgiftsbehandling (art. 18, 19 och 21 GDPR)

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

7.7 Tredjelandsöverföring (kap. 5 GDPR)

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

7.7.1 Beskrivning och skyddsåtgärder

Om personuppgifter överförs till tredjeland, beskriv vilka tredjelands-överföringar som görs i och med behandlingen.

Ange även vilka överföringsmekanismer (land med adekvat skyddsnivå eller lämpliga skyddsåtgärder) som har använts för tredjelandsöverföringarna samt motivera varför dessa mekanismer är tillämpliga.

Personuppgifts-behandling [Exempel: support, diagnostiska data, regulatoriska krav, marknads-föring etc.]	**Beskrivning av tredjelands-överföring**	**Överförings-mekanism** [Exempel: adekvansbeslut av kommissionen, standardavtals-klausuler, art. 49.1-undantag]	**Motivering av skydds-åtgärd(er) och tillämplighet**[6]

[6] Se EDPB:s vägledning för val och bedömning av skyddsåtgärder för att uppnå lagenlig tredjelandsöverföring: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

7.8 Medverkan från berörda parter

7.8.1 Synpunkter från registrerade

När så är lämpligt ska synpunkter inhämtas från de registrerade eller deras företrädare (art. 35.9 GDPR).

Har ni rådgjort med registrerade eller deras 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

7.8.2 Personuppgiftsbiträden, specialister etc.

Om utlåtanden från relevanta intressenter finns i annan bifogad dokumentation såsom en riskbedömning kan man hänvisa dit.

Redogör för synpunkter från relevanta intressenter, exempelvis personuppgiftsbiträden eller informationssäkerhetsspecialister

8 Risker och riskreducerande åtgärder

Målet med en konsekvensbedömning avseende dataskydd är att minimera risker för den registrerades rättigheter och friheter (art. 35.7 c GDPR). För att möjliggöra detta ska en riskbedömning göras där man hanterar risker för kränkningar av den registrerades rättigheter och friheter i samband med konsekvensbedömningen, det vill säga risker 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 kommunen som organisation, hanteras i stället i en riskbedömning avseende informationssäkerhet.[7]

Riskbedömningsdelen av en konsekvensbedömning ska innehålla[8]:

- Riskens ursprung (orsak/sårbarhet) (skäl 90 GDPR).
- 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 GDPR).
- Fastställande av planerade åtgärder för att minska eller eliminera dessa risker (artikel 35.7 d GDPR och skäl 90 GDPR).

Riskbedömningsdelen av en konsekvensbedömning kan av praktiska skäl genomföras samtidigt som en riskbedömning avseende informationssäkerhet. **Dokumentationen görs i kommunens eget riskhanteringsverktyg**. Det är dock viktigt att värdera och dokumentera de risker som tillhör konsekvens-bedömningen separat. Detta för att konsekvensbedömnings-riskerna endast ska bestå av risker för den registrerade och inte kommunen som organisation.

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

[7] Mer information om riskbedömningar avseende informationssäkerhet finns i kommunens ledningssystem för informationssäkerhet. Kontakta informationssäkerhetsansvarig (motsvarande).
[8] Se den franska dataskyddsmyndigheten CNIL:s vägledning för stöd i riskbedömningen: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

8.1 Riskdokumentation

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

Hänvisning och kommentar

8.2 Kvarstående höga risker

Dokumentera de risker från riskbedömningsdelen av konsekvensbedömningen som är fortsatt *höga* (riskvärde 8 eller högre om en tio-gradig skala används – 5 sannolikhet – 5 konsekvens) efter att riskreducerande åtgärder har vidtagits.

ID	**Riskscenario (hot, aktör och konsekvenser)**	**Riskens ursprung (sårbarhet, orsak)**	**Riskreducerande åtgärder**	**Eventuella krav fastställda av kommunen**	**Riskvärde efter åtgärder** [Hög alt. 8-10]	**Kommentar**

9 Rådfrågan, slutlig bedömning och godkännande

9.1 Dataskyddssamordnarens (motsvarande) utlåtande

Vid behov kan dataskyddssamordnaren (motsvarande) som rådfrågats i denna ruta ge ett samlat utlåtande om konsekvensbedömningen. Rutan får endast fyllas i av dataskyddssamordnaren.

Dataskyddssamordnarens samlade utlåtande om konsekvensbedömningen. Får endast fyllas i av dataskyddssamordnaren

9.2 Dataskyddsombudets bedömning och rekommendationer

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 kommunens dataskyddsombud rådfrågas om konsekvens-bedömningen (art. 35.2 GDPR), vilket ska dokumenteras i denna ruta. Rutan får endast fyllas i av dataskyddsombudet.

Dataskyddsombudets konsekvensbedömning. Får endast fyllas i av dataskyddsombudet

9.3 Sammantagen bedömning

De som genomfört konsekvensbedömningen ska skriva en sammantagen bedömning med rekommendationer (som också sammanfattas under avsnitt 1).

Genomförarnas sammantagna bedömning med rekommendation

Intressenter/saken	**Namn/datum**	**Anteckningar**
Dataskyddsombudet har rådfrågats:		[Dataskyddsombud ska rådfrågas om rättsliga krav, åtgärder som minskar risker och om behandlingen är tillåten.]
Dataskyddsombudets rekommendationer godtogs inte:		[Förklara nedan varför ansvarig chef, nämnd (motsvarande) gått emot dataskyddsombudets rekommendation/er.]
Motivering varför dataskyddsombudets rekommendationer inte godtagits:		
Genomförare (se avsnitt 3.3.1):		
Genomförarnas rekommendationer:		
Samråd med andra intressenter granskade och beaktade av:		[Om ett beslut avviker från t.ex. registrerades synpunkter ska skälen redovisas här.]

Intressenter/saken	**Namn/datum**	**Anteckningar**
Skäl för beslut som avviker från intressenters synpunkter:		
Gå vidare med personuppgiftsbehandlingen (JA/NEJ), beslutad av:		[Om kvarstående sannolika höga risker finns innebär ett JA att begära förhandssamråd hos IMY]
Motivering:		