Svenska kyrkan
TÄBY FÖRSAMLING

Policy för konsekvensbedömning

ANSVARIG ENHET		DATUM
Täby församling		16 december 2020
MÖTESINSTANS		
Kyrkorådet		
SAMMANTRÄDESDATUM	DAGORDNINGSNUMMER	TYP AV ÄRENDE
16 december 2020	Skriv dagordningsnummer	Beslut
HANDLÄGGARE		ÄRENDENUMMER
Olle Molin		Skriv ärendenummer

☐ Barnkonsekvensanalys genomförd

☒ Dataskyddsombudet har tillstyrkt

Förslag till beslut

Att anta policyn

Att lägga informationen avseende rutin för konsekvensbedömning (GDPR) till handlingarna

Ärendebeskrivning

En konsekvensbedömning är en av de grundläggande kraven för uppfylla ett fullgott GDPR-arbete. En underlåtelse att genomföra en konsekvensbedömning när en sådan ska finnas på plats eller att inte ha en rutin för detta arbete kan leda till en av de högre sanktionsavgifterna (maxbeloppet för detta är 10 miljoner euro eller 2 procent av den globala årsomsättningen).

I arbetet med en konsekvensbedömning ska man rådgöra med dataskyddsombudet och i vissa fall samråda med Datainspektionen. Församlingen behöver vid sidan av riktlinjen och rutinen ha en organisation som kan genomföra hela eller delar av rutinen – likt församlingens organisering för barnkonsekvensanalyser.

Så här skriver Datainspektionen;

”Den personuppgiftsansvarige ska se till att organisationen

- har ett systematiskt förfarande för konsekvensbedömning, så att konsekvensbedömningar genomförs när de ska, och att de genomförs på ett kvalitetssäkrat sätt
- gör konsekvensbedömningen till en integrerad del av organisationens arbetssätt

Täby församling
POSTADRESS: BOX 208 18323 TÄBY
BESÖKSADRESS: Attundavägen 3
TELEFON: +46(8)58003500

- involverar berörda parter och tydligt fastställer deras ansvarsområden i konsekvensbedömningen, till exempel dataskyddsombud, registrerade, organisationens affärsverksamhet och tekniska tjänster.
- när det krävs, ger Datainspektionen tillgång till konsekvensbedömningen
- när det krävs, samråder med Datainspektionen i ett förhandssamråd
- regelbundet ser över konsekvensbedömningar och den behandling som de avser
- dokumenterar de beslut som fattas.

Om den personuppgiftsansvarige beslutar att inte göra en konsekvensbedömning, bör den motivera och dokumentera anledningarna till beslutet."

Bakgrund/överväganden

En konsekvensbedömning är en process avsedd att:

- beskriva en kritisk behandling
- bedöma huruvida den är nödvändig och proportionell
- hjälpa till att hantera risker för fysiska personers rättigheter och friheter som uppkommer genom behandlingen av personuppgifter genom att bedöma dem och bestämma vilka åtgärder som ska vidtas.

I vissa situationer ska församlingar och pastorat göra konsekvensbedömningar. Sådana ska påbörjas innan den kritiska behandlingen påbörjas (men märker man att man har en pågående behandling som uppfyller kraven får man förstås göra den i efterhand). Att göra en konsekvensbedömning när det krävs är ett ska-krav i Dataskyddsförordningen (GDPR). När en konsekvensbedömning är gjord kan man behöva då och då följa upp innehållet för att bedöma om det fortsatt är relevant.

Om man efter en konsekvensbedömning bedömer att det finns kvarvarande risker för de registrerade kan man ibland behöva inleda ett förhandssamråd med Datainspektionen, även detta är ett krav som måste iakttas.

Att underlåta att göra konsekvensbedömningar eller förhandssamråd kan leda till sanktioner (maxbeloppet för detta är 10 miljoner euro eller 2 procent av den globala årsomsättningen).

Datainspektionen kan utkräva sanktionsavgifter till exempel om församlingen;

- inte gör konsekvensbedömning när en planerad behandling sannolikt leder till en hög risk,
- gör konsekvensbedömningar på fel sätt, t.ex. utan att rådfråga dataskyddsombudet eller utan att ta med en beskrivning av behandlingen, dess proportionalitet, risker och åtgärder för att hantera riskerna,
- inte samråder med Datainspektionen före behandlingen när konsekvensbedömningen visar att behandlingen skulle leda till en hög risk om inte åtgärder vidtas för att minska risken.

Barnkonsekvensanalys

Genom att följa dataskyddsförordningens artikel 35 och genomföra en konsekvensbedömning tillvaratas och skyddas barnens intressen vid registrering av personuppgifter.

Svenska kyrkan
TÄBY FÖRSAMLING

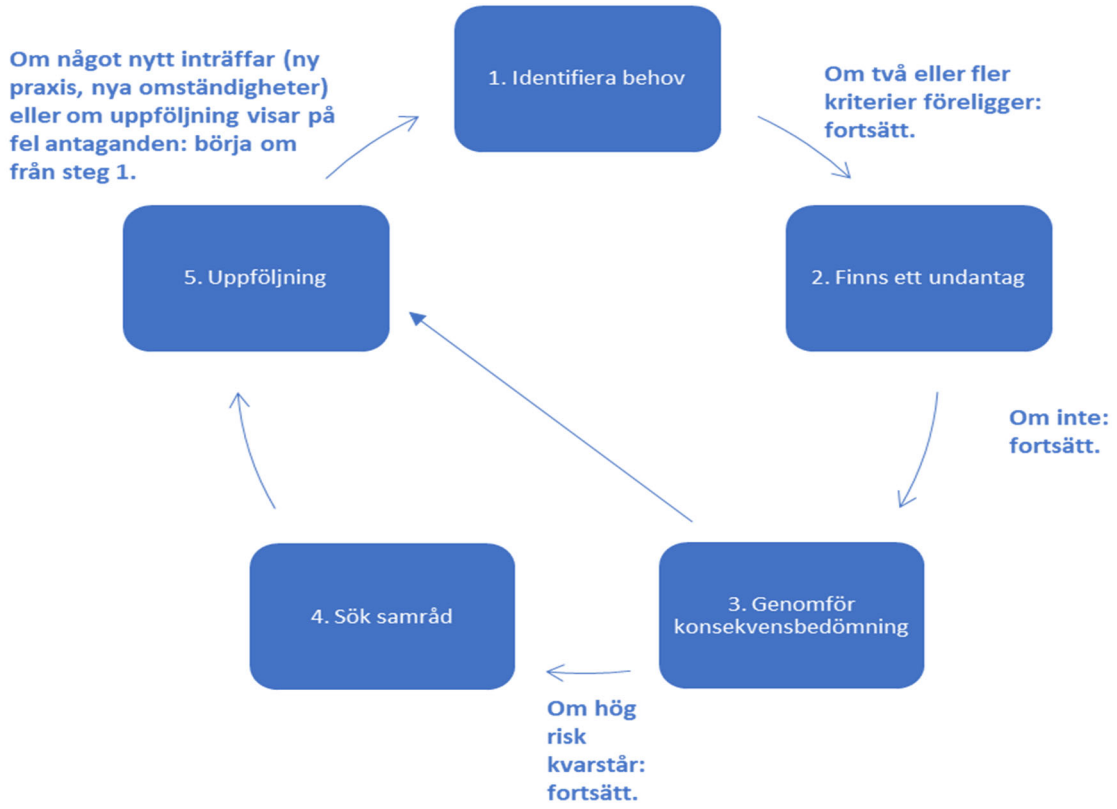
Policy för konsekvensbedömning

Beslutad av kyrkoråd 2020-12-16 § xx

Vid varje behandling, och särskilt vid en ny behandling, av personuppgifter måste det göras en konsekvensbedömning avseende dataskydd, en så kallad ”PIA - Privacy Impact Assessment”.

Enligt dataskyddsförordningens artikel 35 ska en konsekvensbedömning göras och dokumenteras för behandling av personuppgifter som kan leda till en hög risk för de registrerade. I korthet handlar det om att vara förutseende, förebygga risker och därmed skydda människors fri- och rättigheter. Målet är att minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk.

En konsekvensbedömning innehåller flera stega där steg 1 (identifiera behovet av en PIA) alltid ska göras. Varje steg ska dokumenteras och diarieföras.



Stegen ovan finns ingående beskrivna i den rutin för konsekvensbedömning (GDPR) som kyrkoherden utfärdar.

Täby församling
POSTADRESS: BOX 208 18323 TÄBY
BESÖKSADRESS: Attundavägen 3
TELEFON: +46(8)58003500

Svenska kyrkan
TÄBY FÖRSAMLING

Rutin för konsekvensbedömning (GDPR)

Utfärdad av Kyrkoherden 2020-12-16.

Fyll i gemensamma uppgifter

Innan arbetet påbörjas, fyll i följande gemensamma uppgifter för steg 2 och 3 nedan.

Representant från verksamheten (den som gör bedömningen – kan vara en eller flera personer)	
Ansvarig chef (beslutsfattare)	
Dataskyddsombud (man bör involvera dataskyddsombudet från början – inte minst för stöd)	
Övriga (om tillämpligt – ange också roll)	
Inledd den (datum för när steg 2 är inledd)	
Beslut att gå vidare till nästa steg (steg 3 och frmåt ange datum – kan vara flera)	
Beslut att avsluta bedömningen (ange datum)	
Diarienummer (Alla 3 stegen bör ha ett huvuddiarienummer och varje steg + eventuella ytterligare dokument undernummer)	

1. Identifiera behovet av en konsekvensbedömning

Detta steg ska genomföras och dokumenteras av alla som planerar att inleda en behandling av personuppgifter. Datainspektionen har fastställt kriterier för när organisationer, om vissa kriterier är uppfyllda och inga undantag föreligger, är tvungna att genomföra en konsekvensbedömning i en förteckning. En konsekvensbedömning ska enligt förteckningen oftast göras om den planerade behandlingen uppfyller två eller fler av följande nio kriterier (av dessa föreligger kriterium nr 4 och 7 i stor utsträckning för församlingar och pastorat inom Svenska kyrkan):

Täby församling
POSTADRESS: BOX 208 18323 TÄBY
BESÖKSADRESS: Attundavägen 3
TELEFON: +46(8)58003500

1. **Kryssa i vilka kriterier som föreligger;**

Kriterium	Ja	Nej	Kommentar
1. Utvärdering eller poängsättning av människor (Datainspektionen ger här exemplet ett företag som profilerar internetanvändare. Tänk på att plattformsföretag som Google (sökmotorer) och sociala medieföretag som Facebook/Instagram använder profilering som affärsmetod).			
2. Automatiserade beslut med effekt för människor (Kan bli aktuellt om man anlitar någon för att testa personer inför en eventuell anställning).			
3. Systematisk övervakning (t.ex. genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer. Här finns också en särskild lagstiftning att följa som Datainspektionen har tillsyn över).			
4. Känsliga eller integritets-känsliga personuppgifter (En kritisk punkt eftersom det är mycket vanligt i kärnverksamheten. Förutom uppgifter som kan avslöja religiös tillhörighet finns mängder av hälsorelaterade personuppgifter. Utöver de känsliga personuppgifterna förekommer också andra uppgifter av mycket personlig karaktär inte sällan i verksamheten. På Datainspektionens hemsida finns olika exempel).			
5. Stor omfattning (En exakt beskrivning av begreppet finns inte men här kan det vara bra att ha i åtanke att system som Kbok och Kyrksam innehåller väldigt många människors personuppgifter)			
6. Samkör register eller annan kombination av behandlingar (När en organisation kombinerar 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.)			
7. Utsatta registrerade (personer som av något skäl befinner sig i ett underläge eller i beroendeställning			

Kriterium	Ja	Nej	Kommentar
och därför är sårbara. Till denna grupp räknas bland annat barn, anställda, sjuka, asylsökande och äldre.)			
8. Ny teknik/ny organisatorisk lösning (t.ex. fingeravtryck, ansiktsigenkänning för åtkomstkontroll, personliga tillträdesbrickor, anordningar för automatisering smarta bilar, mätare m.m.)			
9. Hindra registrerade från att få tillgång till en tjänst eller ingå ett avtal. (De exempel som Datainspektionen ger är när en bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån eller inte).			

2. **Dataskyddsombudets bedömning och rekommendation:**
   Klicka eller tryck här för att ange text.

3. **Om dataskyddsombudets bedömning/rekommendation inte följs, motivering:**
   Klicka eller tryck här för att ange text.

4. **Förklara utifrån tabellen ovan i stora drag vad den aktuella verksamheten syftar till att åstadkomma:**
   Klicka eller tryck här för att ange text.

5. **Har två eller fler kriterier markerats med ”Ja” i punkt 1 ovan – fortsätt till steg 2.**
   Detta kan även vara nödvändigt om dataskyddsombudet gör en tolkning som är visar på högre risker för den registrerade än den personuppgiftsansvariga gjort.

2. Föreligger något undantag

Det räcker dock inte att sätta sig in i de nio punkterna o van. Att utföra en konsekvensbedömning enligt punkterna är obligatoriskt endast om behandlingen sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Detta är givetvis en svår avvägning att göra så vid osäkerhet är det bättre att göra en än att låta bli. Dataskyddsombudet kan tillfrågas rörande detta.

1. **Gör en bedömning av om det föreligger ett undantag.**

Undantag	Ja	Nej	Motivering till ställningstagandet
1. Behandlingen kommer sannolikt inte leda till en hög			

Undantag	Ja	Nej	Motivering till ställningstagandet
risk för fysiska personers rättigheter och friheter[1].			
2. Behandlingens art, omfattning, sammanhang och ändamål är mycket lika en behandling för vilken en konsekvensbedömning har utförts. I sådana situationer kan resultat från konsekvens-bedömningar för liknande behandlingar användas.			
3. Behandlingen grundas tydligt på någon av de lagliga grunderna ”rättslig förpliktelse” eller ”allmänt intresse” och lagstiftaren har gjort en konsekvensbedömning när den lagliga grunden (till exempel den svenska lagen där den rättsliga förpliktelsen finns) fastställdes[2].			
4. Behandlingen har kontrollerats av en tillsynsmyndighet som Datainspektionen före maj 2018 under särskilda villkor som inte har ändrats[3].			

2. Dataskyddsombudets bedömning och rekommendation[4]:
Klicka eller tryck här för att ange text.

3. Om dataskyddsombudets bedömning/rekommendation inte följs, motivera varför:
Klicka eller tryck här för att ange text.

5. Om inget undantag finns, gå vidare till steg 3.

[1] Hur riskbedömningen kan ske beskrivs i steg 3, där begreppet hög risk klargörs. Notera att risken inte enbart rör dataskydd utan också hög risk för andra rättigheter och friheter.
[2] Sådana lär inte finnas i äldre lagstiftning som trätt ikraft innan maj 2018, eftersom konsekvensbedömningar infördes genom dataskyddsförordningen.
[3] Torde inte vara aktuell då Sverige inte hade ett sådant system tidigare.
[4] Är i detta steg inte obligatorisk men innebär ett bra inbyggt dataskydd.

3. Genomför en konsekvensbedömning

Genomför konsekvensbedömningen enligt nedan. Den är tänkt för behandlingar som inte påbörjats (där steg 1-2 ovan gåtts igenom), men upptäcker man att man har en pågående behandling som kräver hantering kan man göra en konsekvensbedömning i efterskott (samma mall fungerar). Tänk på att syftet med konsekvensbedömningen är att minska riskerna för registrerade och se till att väga olika intressen mot varandra. Det krävs en omfattande utredning för detta. Från och med detta steg ska dataskyddsombudet delta.

Deltagare i utredningen:

Representant från verksamheten (den som gör bedömningen – kan vara en eller flera personer)	
Ansvarig chef (beslutsfattare)	
Dataskyddsombud (ska delta i detta steg)	
Representant för de registrerade[5]	
Övriga (om tillämpligt – ange också roll)	

När genomfördes utredningen av steg 3:

Inledd den (datum för när steg 3 är inledd)	
Beslut att gå fattat den (ange datum)	
Beslut att avsluta bedömningen (ange datum)	
Diarienummer (Alla 3 stegen bör ha ett huvuddiarienummer och varje steg + eventuella ytterligare dokument undernummer)	

[5] Om de registrerade är anställda kan frågorna möjligen hanteras tillsammans med fackliga företrädare.

Klargör omständigheter kring behandlingen

1. Hur genomförs behandlingen:

a) Hur kommer vi samla in, använda, lagra och arkivera eller radera uppgifterna?
Klicka eller tryck här för att ange text.

b) Vad är uppgifternas ursprung?
Klicka eller tryck här för att ange text.

c) Kommer vi att dela uppgifterna med någon?
Klicka eller tryck här för att ange text.

d) Kommer vi genomföra behandlingen själva (ha ett eget personuppgiftsansvar)?
Klicka eller tryck här för att ange text.

e) Kommer ett personuppgiftsbiträde att anlitas? Vem i så fall? Finns ett korrekt biträdesavtal?

Personuppgiftsbiträdets namn	Biträdesavtalets datum samt uppgift om relevanta dokumenterade instruktioner

f) Kommer vi samarbeta med annan personuppgiftsansvarig? Vem i så fall? Finns korrekt inbördes arrangemang?

Personuppgiftsansvariges namn	Datum för inbördes arrangemang samt hur vi kommer beskriva den aktuella behandlingen i det

g) Vilka IT-system berörs? Hur ser de ut säkerhetsmässigt – svara på frågorna i kolumnen.

Systemets namn	Behörighetsstyrning?[6]	Logguppföljning?[7]	Kryptering?[8]	Övrig säkerhet[9]

[6] Beskriv hur den säkrats.
[7] Beskriv hur den genomförs.
[8] Ja/Nej. Vid ja, beskriv hur.
[9] Om systemet finns hos ett personuppgiftsbiträde kan dokumenterade instruktioner beskrivas i kolumnen övrig säkerhet.

h) Vilken övrig teknisk utrustning kommer att användas?

Typ av utrustning[10]	Inloggning krävs?[11]	Går att stänga ner centralt vid förlust?[12]	Kryptering?[13]	Övrig säkerhet[14]

i) Om hanteringen sker med hjälp av icke-digitala handlingar, beskriv dessa?

Typ av icke-digital handling[15]	Hur förvaras den?	Övrig säkerhet[16]

Beskriv behandlingens omfattning och varaktighet:

a) Vad är det för kategorier av personuppgifter?
Klicka eller tryck här för att ange text.

b) Inkluderar behandlingen känsliga uppgifter, uppgifter om lagöverträdelser eller andra integritetskänsliga personuppgifter? Om ja, beskriv även omfattning:
Klicka eller tryck här för att ange text.

c) Hur mycket personuppgifter kommer vi att samla in och behandla?
Klicka eller tryck här för att ange text.

d) Hur ofta kommer vi behandla personuppgifterna?
Klicka eller tryck här för att ange text.

e) Hur länge kommer vi att spara uppgifterna?[17]
Klicka eller tryck här för att ange text.

f) Hur många individer berörs?
Klicka eller tryck här för att ange text.

[10] Ange typ som fast dator, laptop, mobil, padda etc.
[11] Ange hur den går till.
[12] Ja/Nej. Vid ja, beskriv hur
[13] Ja/Nej. Vid ja, beskriv hur.
[14] Om systemet finns hos ett biträde kan dokumenterade instruktioner beskrivas i kolumnen övrig säkerhet.
[15] Ange typ som pärm, pappersbilder etc.
[16] T.ex. om handlingen förvaras inlåst eller vilka instruktioner ett biträde kan ha fått.
[17] Jämför här de föreskrifter som finns i SvKB 2016:6, 2017:1 och 2019:1.

g) Vilket geografiskt område omfattas?[18]
Klicka eller tryck här för att ange text.

3. Beskriv behandlingens kontext:

a) Vad är vår relation till berörda individer?
Klicka eller tryck här för att ange text.

b) Hur mycket kontroll kommer enskilda individer själva att ha över behandlingen?
Klicka eller tryck här för att ange text.

c) Kan de rimligen förvänta sig att vi kommer att behandla deras uppgifter på det här sättet?
Klicka eller tryck här för att ange text.

d) Inkluderas barn, äldre, anställda eller andra utsatta registrerade i gruppen registrerade?
Klicka eller tryck här för att ange text.

e) Finns det sedan tidigare betänkligheter kring den här typen av behandling eller säkerhetsrisker? Vad anser Datainspektionen[19]**? Finns det rättsfall som är relevanta?**
Klicka eller tryck här för att ange text.

f) Är det vi tänker göra nytt/innovativt på något sätt?
Klicka eller tryck här för att ange text.

g) Vilken teknik kommer att användas?
Klicka eller tryck här för att ange text.

h) Finns det en allmän oro eller förväntan i samhället för den här typen av behandlingar som vi bör beakta?
Klicka eller tryck här för att ange text.

i) Finns det ett intresse hos vissa registrerade för den här typen av behandling? Vad kan de se för värde i behandlingen? Kan det finnas motstridiga intressen mellan olika registrerade?
Klicka eller tryck här för att ange text.

j) Genomför vi en kameraövervakning eller annan storskalig övervakning?
Klicka eller tryck här för att ange text.

k) Genomför vi en profilering?
Klicka eller tryck här för att ange text.

l) Innefattar behandlingen automatiserat beslutsfattande?
Klicka eller tryck här för att ange text.

4. Beskriv ändamålet (syftet) med behandlingen:

a) Varför vill vi behandla personuppgifterna (vad är det ändamål vi skulle ange för de registrerade)?
Klicka eller tryck här för att ange text.

b) Vad vill vi uppnå?
Klicka eller tryck här för att ange text.

5. Bedöm effekterna av behandlingen?

a) Vad är den avsedda effekten för de registrerade? Nackdelar/fördelar?
Klicka eller tryck här för att ange text.

b) Vad är fördelarna med behandlingen för oss?
Klicka eller tryck här för att ange text.

[18] Kommer det t.ex. att ske någon överföring av personuppgifter till land utanför EU/EES eller till en internationell organisation?
[19] Gå in på Datainspektionens hemsida för att se vad senaste läget är. Jämför gärna med pågående tillsyner och avslutade tillsynsärenden hos inspektionen.

c) Vad är nackdelarna om vi inte genomför behandlingen för oss?
Klicka eller tryck här för att ange text.
d) Finns det några fördelar/nackdelar för andra individer?
Klicka eller tryck här för att ange text.
e) Finns det några fördelar/nackdelar för samhället eller andra organisationer?
Klicka eller tryck här för att ange text.

6. Vad i behandlingen som den beskrivs i punkterna ovan skulle kunna innebära en hög risk för registrerade?
Klicka eller tryck här för att ange text.

7. Dataskyddsombudets bedömning och rekommendation av punkterna ovan:
Klicka eller tryck här för att ange text.

8. Om dataskyddsombudets bedömning/rekommendation inte följs, motivering:
Klicka eller tryck här för att ange text.

9. Finns dokument, så som rekommendationer från dataskyddsombudet, eller annat som är relevanta i bedömningen. Det kan underlätta att referera till ett flödesdiagram eller på något annat sätt beskriva flödet av personuppgifter visuellt för att visa hur bedömningarna enligt ovan gjorts.

Dokumentets namn	Kommentar

Beskrivning hur vi hanterar de grundläggande principerna för behandling (artikel 5)

1. Vilka ändamål använder vi de berörda personuppgifterna för idag?
Klicka eller tryck här för att ange text.
2. Vilka tillkommande ändamål har vi för personuppgifterna (jämför punkt 4 i föregående avsnitt)?
Klicka eller tryck här för att ange text.
3. Vad har vi för laglig grund för de personuppgifter vi redan har idag som vi vill använda i den aktuella behandlingen (även laglig grund för lagring)?

Laglig grund	Ändamål enligt punkt 1	Omfattar följande kategorier personuppgifter

4. Om vi åberopat berättigat intresse i tabellen ovan, beskriv intresseavvägningen[20]:

a) den registrerades intresse[21]:

Klicka eller tryck här för att ange text.

b) vårt intresse:

Klicka eller tryck här för att ange text.

c) andras intresse (andra individers, samhällets etcetera):

Klicka eller tryck här för att ange text.

5. Vilken laglig grund kommer vi att ha för personuppgifterna i den nya behandlingen (inklusive lagring av uppgifterna)? För de vi redan har måste vi också motivera hur vi får en tillåten vidarebehandling.

Laglig grund	Tillkommande ändamål	Omfattar följande kategorier personuppgifter

6. Om vi åberopat berättigat intresse i tabellen ovan, beskriv intresseavvägningen[22]:

a) den registrerades intresse[23]:

Klicka eller tryck här för att ange text.

b) vårt intresse:

Klicka eller tryck här för att ange text.

c) andras intresse (andra individers, samhällets etc):

Klicka eller tryck här för att ange text.

7. Om behandlingen (se punkt 1) omfattar tidigare insamlade personuppgifter, hur säkerställer vi att den tänkta vidarebehandlingen (se punkt 2) får en laglig grund? Observera att det inte alltid kommer vara samma lagliga grund. Hur ser vår analys ut?

Klicka eller tryck här för att ange text.

8. Motivera varför den tänkta behandlingen är nödvändig? Går det göra på mindre ingripande sätt? Varför/varför inte?

Klicka eller tryck här för att ange text.

9. Hur kommer vi hantera öppenhetsprincipen (hur informerar vi den registrerade och hur lättillgängligt kommer detta att vara)?

Klicka eller tryck här för att ange text.

---

[20] Observera att bedömningen inte får göras slentrianmässigt utan vi måste ordentligt beakta den registrerades tankar (se även avsnittet Utredning av registrerades intressen). I den bedömningen kan vi utgå ifrån de fakta vi hämtade in i föregående avsnitt. Ju mer integritetskänslig behandling desto starkare måste våra eller andras intresse vara.

[21] Gör en realistisk bedömning av vad registrerade kan tycka, se frågan från deras perspektiv.

[22] Observera att bedömningen inte får göras slentrianmässigt utan vi måste ordentligt beakta den registrerades tankar (se även avsnittet Utredning av registrerades intressen). I den bedömningen kan vi utgå ifrån de fakta vi hämtade in i föregående avsnitt. Ju mer integritetskänslig behandling desto starkare måste våra eller andras intresse vara.

[23] Gör en realistisk bedömning utifrån vad registrerade kan tycka, utgå ifrån deras perspektiv.

10. Hur säkerställer vi korrekthet, det vill säga att den registrerade upplever att hens personuppgifter behandlas korrekt (känns rättvisande och ”schysst”):
Klicka eller tryck här för att ange text.

11. Hur säkerställer vi riktighet, det vill säga att vi enbart behandlar uppgifter för ändamål vi har berättat om och har laglig grund för och att de är riktiga/uppdaterade?
Klicka eller tryck här för att ange text.

12. Hur ser vi till att personuppgifter som behandlas är adekvata, relevanta och inte för omfattande (hur säkrar vi behörighetsstyrning, att medarbetare är utbildade i ändamålet, att vi inte tar in för många uppgifter i förhållande till ändamålet etc.)?
Klicka eller tryck här för att ange text.

13. Vilka åtgärder har vi vidtagit för att säkra konfidentialitet (säkerhetsåtgärder som pseudonymisering, kryptering[24] etc, logguppföljning, brandväggar, centrala styrdokument etc)?
Klicka eller tryck här för att ange text.

14. Vilka åtgärder har vi vidtagit för att säkra sekretess kring behandlingen (till exempel utbildning, centrala styrdokument)?
Klicka eller tryck här för att ange text.

15. Hur säkerställer vi att gallring sker när laglig grund inte längre föreligger (automatiskt eller genom manuell hantering); beskriv hur:
Klicka eller tryck här för att ange text.

16. Dataskyddsombudets bedömning och rekommendation av punkterna ovan:
Klicka eller tryck här för att ange text.

17. Om dataskyddsombudets bedömning/rekommendation inte följs, motivering:
Klicka eller tryck här för att ange text.

18. Finns dokument, så som rekommendationer från dataskyddsombudet, texter i integritetspolicy, behandlingsregister, dokumenthanteringsplan, avtal eller samtycken med registrerade eller annat som är relevanta i bedömningen?

Dokumentets namn	Kommentar

[24] Kryptering är ett ska-krav om känsliga personuppgifter, personuppgifter om lagöverträdelser eller övrigt integritetskänsliga personuppgifter ingår.

Utredning av registrerades intressen

1. Beskriv hur vi inhämtat de registrerades ståndpunkter? Motivera gärna hur ni tänkt rörande metod.
Klicka eller tryck här för att ange text.

2. Vad anser de registrerade om behandlingen?

a) Vad upplevs positivt?
Klicka eller tryck här för att ange text.

b) Vad upplevs negativt? Vilka risker ser de?
Klicka eller tryck här för att ange text.

c) Finns det delar som varken har en positiv eller negativ inverkan?
Klicka eller tryck här för att ange text.

d) Har de registrerade idéer kring hur vi kan minska risker för dem?
Klicka eller tryck här för att ange text.

3. Om punkt 1-2 inte genomförts, motivera varför/beskriv hur ni på annat sätt beaktar deras intressen.

a) Varför kan de registrerade inte tillfrågas?
Klicka eller tryck här för att ange text.

b) Har vi kunnat hämta information om vad de tycker på ett annat sätt? Svarar detta på frågorna i punkt 2 (fyll i så fall i den punkten)?
Klicka eller tryck här för att ange text.

c) Har andra än registrerade bidragit i bedömningen av deras intressen enligt punkt b, vilka i så fall?
Klicka eller tryck här för att ange text.

4. Dataskyddsombudets bedömning och rekommendation av punkterna ovan:
Klicka eller tryck här för att ange text.

5. Om dataskyddsombudets bedömning/rekommendation inte följs, motivering:
Klicka eller tryck här för att ange text.

6. Finns dokument, såsom rekommendationer från dataskyddsombudet eller dokumentation från enkäter, workshops[25] eller liknande som är relevant i bedömningen.

Dokumentets namn	Kommentar

[25] Om man inte kan efterfråga synpunkter från registrerade direkt kan ett sätt vara att genomföra en bred workshop med deltagare som ofta möter registrerade och som vet vad de kan vilja.

Riskbedömning avseende registrerade

1. Bedöm hur registrerade uppfattar riskerna i behandlingen?

a) Utifrån utredningen ovan: fyll i följande tabell (använd färger och värden som anges i fotnoterna):

Nr	Risken och den effekt den bedöms få	Sannolikheten för skada[26]	Konsekvens[27]	Helhetsrisk[28]

Helhetsriskerna fås fram genom att man multiplicerar värdena för sannolikhet och konsekvens.

- Låg helhetsrisk: 1-2 (grön)
- Medel helhetsrisk: 3-6 (gul)
- Hög helhetsrisk: 7-10 (orange)
- Mycket hög helhetsrisk: 10–16 (röd)

b) Dataskyddsombudets bedömning och rekommendation till tabellen ovan:

Klicka eller tryck här för att ange text.

c) Om dataskyddsombudets bedömning/rekommendation inte följs, motivering:

Klicka eller tryck här för att ange text.

2. Om helhetsriskerna enligt ovan bedöms som höga eller mycket höga, ange vilka åtgärder som planeras att vidtas (använd samma nr som i punkt 1):[29]

Nr[30]	Föreslagen riskminimering och kvarvarande risk därefter	Sannolikheten för skada[31]	Konsekvens[32]	Helhetsrisk[33]

[26] Osannolik (värde 1: grön färg), möjlig (värde 2: gul färg), sannolik (värde 3: orange färg) eller mycket sannolik (värde 4: röd färg)
[27] Liten (värde 1; grön färg), betydande (värde 2: gul färg); allvarlig (värde 3: orange färg) eller mycket allvarlig (värde 4)
[28] Multiplicera värdena i tidigare kolumner och ange det sammanlagda värdet här.
[29] En riskminskning kan göras genom att vidta åtgärder kopplade till de grundläggande principerna eller genom att minska t.ex. omfattning, varaktighet eller annat. På intranätet finns förslag på åtgärder.
[30] Använd nr från tabell i avsnittet Riskbedömning av registrerades intressen.
[31] Osannolik (värde 1: grön färg), möjlig (värde 2: gul färg), sannolik (värde 3: orange färg) eller mycket sannolik (värde 4: röd färg)
[32] Liten (värde 1; grön färg), betydande (värde 2: gul färg); allvarlig (värde 3: orange färg) eller mycket allvarlig (värde 4)
[33] Multiplicera värdena i tidigare kolumner och ange det sammanlagda värdet här.

Nr[30]	Föreslagen riskminimering och kvarvarande risk därefter	Sannolikheten för skada[31]	Konsekvens[32]	Helhetsrisk[33]

Helhetsriskerna fås fram genom att man multiplicerar värdena för sannolikhet och konsekvens.

- Låg helhetsrisk: 1-2 (grön)
- Medel helhetsrisk: 3-6 (gul)
- Hög helhetsrisk: 7-10 (orange)
- Mycket hög helhetsrisk: 10-16 (röd)

a) Dataskyddsombudets bedömning och rekommendation till tabellen ovan:
Klicka eller tryck här för att ange text.
b) Om dataskyddsombudets bedömning/rekommendation inte följs, motivera varför:
Klicka eller tryck här för att ange text.

3. Om riskerna fortsatt är höga eller mycket höga efter punkt 2, fortsätt till nästa två avsnitt

Bedömning av egna intressen

1. Bedöm hur viktig den tänkta behandlingen är för den egna verksamheten:

a) Finns det risker för vår verksamhet om vi inte vidtar den behandling som planeras (utgå ifrån utredningen ovan)?

Nr	Risken och den effekt den bedöms få	Sannolikheten för skada[34]	Konsekvens[35]	Helhetsrisk[36]

Helhetsriskerna fås fram genom att man multiplicerar värdena för sannolikhet och konsekvens.

- Låg helhetsrisk: 1-2 (grön)
- Medel helhetsrisk: 3-6 (gul)
- Hög helhetsrisk: 7-10 (orange)
- Mycket hög helhetsrisk: 10-16 (röd)

[34] Osannolik (värde 1: grön färg), möjlig (värde 2: gul färg), sannolik (värde 3: orange färg) eller mycket sannolik (värde 4: röd färg)
[35] Liten (värde 1; grön färg), betydande (värde 2: gul färg); allvarlig (värde 3: orange färg) eller mycket allvarlig (värde 4; röd färg)
[36] Multiplicera värdena i tidigare kolumner och ange det sammanlagda värdet här.

b) Dataskyddsombudets bedömning och rekommendation till tabellen ovan:
Klicka eller tryck här för att ange text.
c) Om dataskyddsombudets bedömning/rekommendation inte följs, motivering:
Klicka eller tryck här för att ange text.

2. Om det kvarstår höga/mycket höga helhetsrisker för den registrerade och vi själva inte får så stora effekter av att avstå från den bör detta (dvs att avstå från den planerade behandlingen) övervägas här. Motivera annars varför vi ändå vill behandla:
Klicka eller tryck här för att ange text.

Bedömning av andras intressen

1. Finns det risker för andras friheter och rättigheter om vi inte genomför den behandling som planeras (utgå ifrån utredningen ovan)? Detta kan avse även andra rättigheter än integritet som yttrandefrihet, religionsfrihet, trygghet och säkerhet etc.

a) Bedöm risker för andra enskilda än de registrerade (kan vara fysiska eller juridiska personer)

Nr	Risken och den effekt den bedöms få	Sannolikheten för skada[37]	Konsekvens[38]	Helhetsrisk[39]

Helhetsriskerna fås fram genom att man multiplicerar värdena för sannolikhet och konsekvens.

- Låg helhetsrisk: 1-2 (grön)
- Medel helhetsrisk: 3-6 (gul)
- Hög helhetsrisk: 7-10 (orange)
- Mycket hög helhetsrisk: 10-16 (röd)

b) Dataskyddsombudets bedömning och rekommendation till tabellen ovan:
Klicka eller tryck här för att ange text.
c) Om dataskyddsombudets bedömning/rekommendation inte följs, motivera varför:
Klicka eller tryck här för att ange text.

[37] Osannolik (värde 1: grön färg), möjlig (värde 2: gul färg), sannolik (värde 3: orange färg) eller mycket sannolik (värde 4: röd färg)
[38] Liten (värde 1; grön färg), betydande (värde 2: gul färg); allvarlig (värde 3: orange färg) eller mycket allvarlig (värde 4: röd färg)
[39] Multiplicera värdena i tidigare kolumner och ange det sammanlagda värdet här.

2. Om det kvarstår höga/mycket höga risker för den registrerade och andra inte får så stora effekter av att vi avstår från behandlingen bör detta (dvs att avstå från den planerade behandlingen) övervägas här. Motivera annars varför vi ändå vill behandla:
Klicka eller tryck här för att ange text.

Förnyad bedömning av risker för den registrerade

1. Sammanfatta riskerna för den registrerade:

a) Hur många mycket höga risker finns för registrerade?
Klicka eller tryck här för att ange text.

b) Hur många mycket höga risker finns för registrerade?
Klicka eller tryck här för att ange text.

2. Sammanfatta riskerna för oss:

a) Hur många mycket höga risker finns för oss?
Klicka eller tryck här för att ange text.

b) Hur många mycket höga risker finns för oss?
Klicka ellre tryck här för att ange text.

3. Sammanfatta riskerna för andra enskilda:

a) Hur många mycket höga risker finns för andra enskilda?
Klicka eller tryck här för att ange text.

b) Hur många mycket höga risker finns för andra enskilda?
Klicka eller tryck här för att ange text.

4. Vilken bedömning görs utifrån 1-3:
Klicka eller tryck här för att ange text.
Om bedömningen är att inte genomföra behandlingen kan ärendet avslutas här. Annars behöver en ny riskbedömning göras i punkt 5.

5. Vill vi fortsätta med behandlingen trots att det kvarstår höga/mycket höga risker för de registrerade behöver vi göra en förnyad riskbedömning.

a) Utred möjligheterna till riskminimering djupare (kryssa i vad som genomförts):

☐ Inhämtat synpunkter från experter för att få fler alternativ på hur frågor kan lösas (ange i förekommande fall vad den utredningen visar):
Klicka eller tryck här för att ange text.

☐ Vägt in om vi kan vidta åtgärder som kräver mer resurser (ange i förekommande fall vad den utredningen visar):
Klicka eller tryck här för att ange text.

☐ Involverat representant för de registrerade ytterligare en gång och låtit den/dem få kommentera bedömningen och ge förslag på alternativa lösningar (ange i förekommande fall vad den utredningen visar):
Klicka eller tryck här för att ange text.

b). Gör riskbedömningen utifrån den fördjupade utredningen:

Nr[40]	Föreslagen riskminimering och kvarvarande risk därefter	Sannolikheten för skada[41]	Konsekvens[42]	Helhetsrisk[43]

Helhetsriskerna fås fram genom att man multiplicerar värdena för sannolikhet och konsekvens.

- Låg helhetsrisk: 1-2 (grön)
- Medel helhetsrisk: 3-6 (gul)
- Hög helhetsrisk: 7-10 (orange)
- Mycket hög helhetsrisk: 10-16 (röd)

c) Dataskyddsombudets bedömning och rekommendation till tabellen ovan:
Klicka eller tryck här för att ange text.
d) Om dataskyddsombudets bedömning/rekommendation inte följs, motivera varför:
Klicka eller tryck här för att ange text.
e) Om vi inte kan genomföra fler riskminimerande åtgärder eller om det alltjämt kvarstår en hög risk, motivera varför vi ändå vill fortsätta med behandlingen?
Klicka eller tryck här för att ange text.

Steg 4 – Samråd med Datainspektionen

Om det kvarstår hög risk för registrerades rättigheter efter steg 3 behöver ett samråd genomföras med Datainspektionen. Om inte kan man gå direkt till steg 5.

Deltagare:

Fyll i de som deltagit i bedömningen.
Representant från verksamheten: Klicka eller tryck här för att ange text.
Ansvarig chef (beslutsfattare): Klicka eller tryck här för att ange text.
Dataskyddsombud[44]: Klicka eller tryck här för att ange text.
Övrig(a) (ange också roll): Klicka eller tryck här för att ange text.

När inleddes arbetet med samråd:

Inledd den Klicka eller tryck här för att ange datum.

1. Precisera den höga/mycket höga risk som kvarstår:
Klicka eller tryck här för att ange text.

[40] Använd nr från tabell i avsnittet Riskbedömning av registrerades intressen.
[41] Osannolik (värde 1: grön färg), möjlig (värde 2: gul färg), sannolik (värde 3: orange färg) eller mycket sannolik (värde 4: röd färg)
[42] Liten (värde 1; grön färg), betydande (värde 2: gul färg); allvarlig (värde 3: orange färg) eller mycket allvarlig (värde 4; röd färg)
[43] Multiplicera värdena i tidigare kolumner och ange det sammanlagda värdet här.
[44] Dataskyddsombudet ska vara involverat och ge råd och rekommendationer.

2. Ange varför vi inte själva kan hantera den:
Klicka eller tryck här för att ange text.

3. Ange vilka andra intressen (egna och andras som vägts in i bedömningen), det vill säga varför det är proportionellt för oss att vilja behandla trots de höga riskerna:
Klicka eller tryck här för att ange text.

4. Fatta beslut om att inleda samråd:
☐ Konsekvensbedömningen är godkänd av ansvarig chef: Klicka eller tryck här för att ange datum.
☐ Beslut att inleda samråd är fattat av kyrkoråd eller ansvarig chef[45]:Klicka eller tryck här för att ange datum.
☐ Samråd inlett: Klicka eller tryck här för att ange datum.
☐ Samråd avslutat: Klicka eller tryck här för att ange datum.

Steg 5 – Följ upp tidigare beslut

Om man beslutar sig för att gå vidare med behandlingen kan man behöva följa upp beslutet och dokumentera detta. Konsekvensbedömning är tänkt att vara en process för lärande och utveckling vilket innebär att man kan behöva göra om tidigare bedömningar. Uppföljningen kan också initieras av dataskyddsombudet när hen övervakar arbetet.

Deltagare:
Fyll i de som deltagit i bedömningen.
Representant från verksamheten: Klicka eller tryck här för att ange text.
Ansvarig chef (beslutsfattare): Klicka eller tryck här för att ange text.
Dataskyddsombud[46]: Klicka eller tryck här för att ange text.
Övrig(a) (ange också roll): Klicka eller tryck här för att ange text.

1. Tidpunkt för uppföljningen: Klicka eller tryck här för att ange datum.
2. Vad är anledningen till uppföljningen:
Klicka eller tryck här för att ange text.
3. Uppföljningens resultat:
☐ Tidigare bedömningar kvarstår:
Klicka eller tryck här för att ange text.
☐ Ny bedömning med ökad risk som innebär att vi inleder ny konsekvensbedömning (beskriv varför och ange även nya diarienumret):
Klicka eller tryck här för att ange text.
☐ Ny bedömning visar lägre risk för den registrerade än vi tidigare antagit:
Klicka eller tryck här för att ange text.

[45] Detta torde kräva att det finns en tydlig delegation för chefen att fatta beslutet.
[46] Dataskyddsombudet ska vara involverat och ge råd och rekommendationer.

Versionshantering

Det är viktigt att diarieföra blanketten, eftersom den innehåller beslutsunderlag. Se även inledningen till detta dokument angående att arbeta med versioner av dokumentet. I det inledande avsnittet Diarieföring anges när det är lämpligt att diarieföra en version.

DATUM	VERSION	FÖRFATTARE	KOMMENTAR
20XX-XX-XX	X.X	[Namn på ansvarig person]	[Ange det som gäller för versionen, t.ex. första utkast, första beslutade version, samråd med Datainspektionen inlett osv.].