Konsekvens-bedömning avseende dataskydd enligt art. 35 GDPR

Tillhandahålla och bedriva undervisning för elever som inte kan delta i den ordinarie undervisningen på grund av dokumenterad medicinsk, psykisk eller social problematik *(AV1 – Personlig skolrobot)*

Alingsås kommun

[Logo]

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. Om det finns frågor eller synpunkter tas dessa gärna emot i Kompetenscenter välfärdsteknik helpdesk info@skr.se. Uppge ”Mall dataskyddsbedömning” i ärendemeningen.

Versionshistorik mall

Vers.	Datum	Revision och ändringar	Författare	God-kännare

Versionshistorik konsekvensbedömning

Vers.	Datum	Revision och ändringar	Författare	God-kännare
1.0	2022-12-30		Cecilia Jägevall	

Innehåll

1 Sammanfattande bedömning – Färdigställs efter beslut av nämnden

Inför den sammanfattande bedömningen från avsnitt 9.3 här.

2 Varför en konsekvensbedömning?

2.1 Vad är en konsekvensbedömning?

Av artikel 35.1 i dataskyddsförordningen (GDPR) följer att den personuppgiftsansvarige ska utföra en dataskyddskonsekvensbedömning om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. 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 Integritetsskyddsmyndigheten eller avstå från behandlingen.

Ytterligare information om dataskyddsförordningen finns på Integritetsskyddsmyndighetens 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:

a) 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.

b) 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.

c) 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 konsekvensbedömning. 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 konsekvensbedömningen, 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

Barn- och ungdomsnämnden, Alingsås kommun

3.2 Kontaktuppgifter till dataskyddsombud

Namn: Malin Ericsson
E-post: malin.ericsson@goteborgsregionen.se
Tfn: 031-355 52 54

Namn: Johan Bergström
E-post: johan.bergstrom@goteborgsregionen.se
Tfn: 031-335 52 53

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.

Cecilia Jägevall

E-post: cecilia.jagevall@alingsas.se

Tfn: 0322-61 67 60

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.

Cecilia Jägevall

E-post: cecilia.jagevall@alingsas.se

Tfn: 0322-61 67 60

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.

AV1 (skolrobot)

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.

Personuppgiftsbehandlingen syftar till att i enlighet med 24 kapitlet 20§ i Skollagen kunna tillhandahålla och bedriva särskild undervisning för elever som på grund av sjukdom eller liknande skäl inte kan delta i vanligt skolarbete under längre tid. Sådan undervisning ska så långt det är möjligt motsvara den undervisning som eleven inte kan delta i.

Genom att använda en skolrobot kan en elev som inte har möjlighet att närvara fysiskt i klassrummet delta i undervisningen och interagera med klasskamrater och lärare i realtid.

Skolroboten placeras i klassrummet och eleven deltar från annan plats via en applikation på surfplatta eller mobil. Skolroboten är utrustad med inbyggd kamera, mikrofon och högtalare som gör att eleven kan se, höra och prata med sin omgivning. Ingen kan se eleven. Med hjälp appen kan eleven vrida på roboten, interagera med klassen och delta i undervisningen.

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 i ett regionalt eller nationellt perspektiv.

Elever som på grund av sjukdom eller liknande skäl inte kan delta i vanligt skolarbete under längre tid ges möjlighet att digitalt delta i den ordinarie skolundervisningen.

Det främjar och möjliggör lärande samt skapar möjlighet att hålla kontakt med klasskamrater. Elever får förutsättningar att delta i det sociala sammanhanget kring lärande, vilket minskar risken att elever upplever ensamhet och social isolering.

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		X
Behandling i stor omfattning av känsliga personuppgifter		X
Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser		X
Systematisk övervakning av en allmän plats i stor omfattning		X

4.1.2 KONTROLLFRÅGOR FÖR SANNOLIK HÖG RISK[2]

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

[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 personer att analyseras, utvärderas, profileras eller poängsättas på något sätt?		X
Kommer det fattas automatiserade beslut med rättsliga eller liknande betydande följder för den registrerade?		X
Personuppgiftsbehandlingen innefattar att systematisk övervakning används för att observera, övervaka eller kontrollera den registrerade?		X
Omfattar personuppgiftsbehandlingen känsliga personuppgifter eller personuppgifter av mycket personlig karaktär?		X
Kommer personuppgifter att behandlas i stor omfattning?		
Kommer olika register att samköras?		X
Rör personuppgifterna sårbara personer, till exempel barn, anställda, asylsökande, äldre och patienter?	X	
Kommer teknik användas på ett nytt och innovativt sätt eller kommer nya organisatoriska lösningar användas?	X	
Är det risk för att personuppgiftsbehandlingen i sig hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal?		X

4.1.3 ÖVRIGA FAKTORER SOM LEDER TILL HÖG RISK

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

- Tredjelandsöverföring

4.1.4 UNDANTAG FRÅN ATT GENOMFÖRA EN KONSEKVENSBEDÖMNING (ART. 35.3 GDPR)

i *En konsekvensbedömning behöver inte genomföras om något av följande kriterier uppfylls. Om ”ja” väljs för något av kriterierna ska detta motiveras och en data-skyddssamordnare (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		X	
Behandlingens art, omfattning, sammanhang och ändamål är mycket lika en behandling för vilken en konsekvensbedömning redan har genomförts inom kommunen		X	
Behandlingen är godkänd av antingen ett personuppgiftsombud eller		X	

tillsynsmyndigheten (Datainspektionen) i tiden före GDPR

4.1.5 SAMMANFATTANDE BEDÖMNING

Efter samråd med dataskyddsombudet har bedömningen gjorts att en konsekvensbedömning ska genomföras för den aktuella personuppgiftsbehandlingen. Detta utifrån att personuppgifter om barn behandlas (vilka anses vara extra skyddsvärda personuppgifter) samt att ny teknik används och leverantören anlitar underleverantörer i tredje land.

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

i

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?

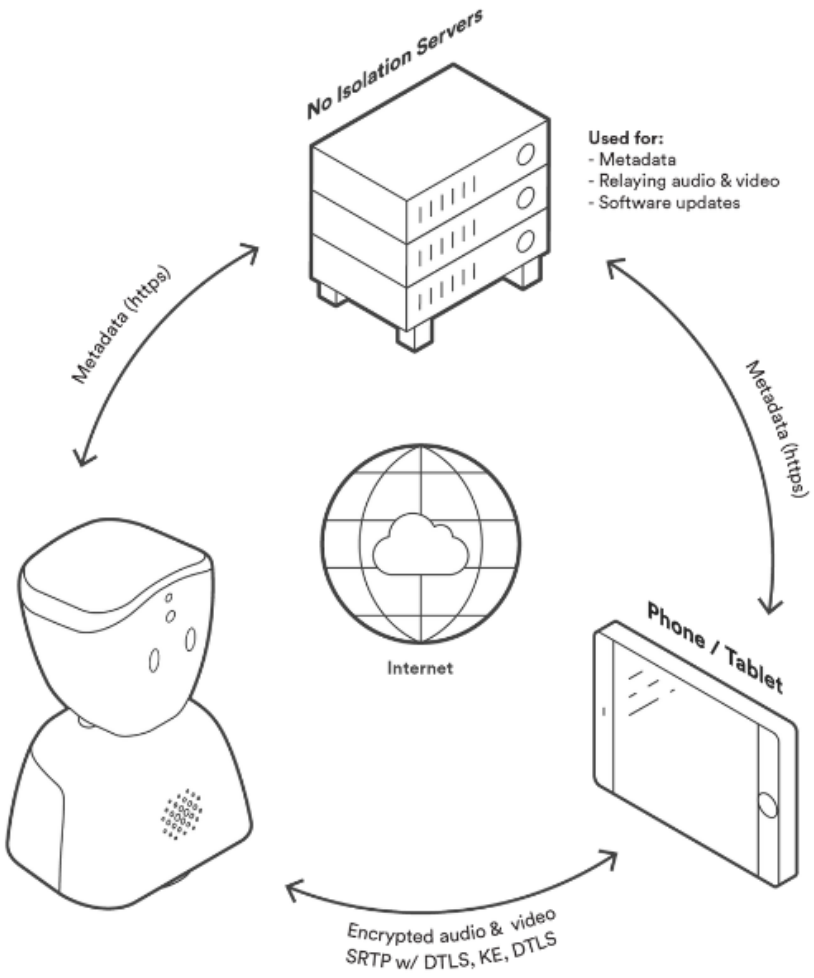
Personuppgifts-behandling (typ av behandlingar)	Ändamål	Personuppgifter	Person-uppgifts-biträde	Kategorier av registrerade	Insamling	Externa mottagare	Lagring/ lagringstid	Radering/ arkivering
Överföring av video- och ljudström	Möjliggöra distribution och användning av AV1.	IP-adress, video- och ljudupptagningar	Amazon Web Services EMEA SARL, 38 Av. John F. Kennedy, 1855, Luxembourg	Personal, elever		Nej	Lagras, cachelagras eller bearbetas inte.	Inget lagras
Lagring av kunduppgifter	Behandla beställning, betalning och leverans.	Namn, e-post, telefonnummer, användar-id (AV1)	HubSpot Ireland Ltd, Ground Floor, Two Dockland Central, Guild Street, Dublin 1, Co. Dublin, Ireland	Personal		Nej	Ja	Max 5 år, raderas av leverantör.
Registrera ansökan och lagring av register över användare (internt register hos Barn- och	Registrera ansökningar om skolrobot och föra register över vem	Namn, användar-id (AV1)		Elever	Ja	Nej	Ja	Radering sker löpande (efter t.ex. beslut om ansökan eller

ungdomsförvaltningen)	som använder vilken skolrobot.							återlämning av skolrobot).
Administrera och tillgängliggöra tjänsten	Skapa och hantera konton, generera lösenord och autentisera kundens användare.	Namn, e-post, användar-id (AV1), IP-adress, serienummer (AV1)	Amazon Web Services EMEA SARL, 38 Av. John F. Kennedy, 1855, Luxembourg	Personal		Nej	Kontouppgifter lagras för personal (AV1 Admin och i AV1 Assistant app om den används). Inga personuppgifter lagras rörande autentisering.	Data kan raderas av kunden vid. Om inte kunden raderar data raderas den av leverantören 60 dagar efter avtalsslut.
Spåra när AV1 aktiveras/avaktiveras samt användning av AV1	Sker vid uppkoppling/anslutning.	IP-adress	Amazon Web Services EMEA SARL, 38 Av. John F. Kennedy, 1855, Luxembourg	Serienummer (AV1). Leverantören och dess underbiträde har inte tillgång till uppgifter om vilken användare (elev) som använder vilket serienummer.		Nej	Lagras, cachelagras eller bearbetas inte.	Inget lagras
Support	Tillhandahålla supporttjänster till kunden och kunna kontakta den som ansvarar för en AV1-robot vid behov av support.	Namn, användar-id (AV1), e-postadress, telefon	Amazon Web Services EMEA SARL, 38 Av. John F. Kennedy, 1855, Luxembourg Google Cloud EMEA Limited	Personal, eventuellt vårdnadshavare (möjligt för vårdnadshavare att ges tillgång till support via e-post/chat,		Ja, eventuellt Amazon och Google som behandlar kontaktuppgifter till personal (och ev. vårdnadshavare), samt information om	Lagras under hanteringen av supportärende.	Raderas efter avslutat supportärende.

			(Google Workspace Gmail)	men de kan också välja support via telefon).		tekniska frågor som krävs i samband med supportärenden		
Implementera säkerhetsåtgärder	Implementera säkerhetsåtgärder och problemlösning	Användar-id (AV1), IP-adress, serienummer (AV1)	Amazon Web Services EMEA SARL, 38 Av. John F. Kennedy, 1855, Luxembourg	Personal		Ja, eventuellt Amazon som ges tillgång till kontaktuppgifter till personal, samt information om tekniska frågor som krävs i samband med supportärenden kopplat till problemlösning och implementering av säkerhetsåtgärder.	Ja	Raderas efter avtalsslut.

5.2 Översiktlig beskrivning av personuppgiftsflödet

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



AV1 (skolroboten) kommunicerar via två kanaler.

- Första kanalen används för signalöverföring där signaler passerar genom leverantörens servrar. Detta används för metadata som t.ex. batterinivå och tillgängligheten för AV1 på internet. Metadata görs tillgänglig för kunden och användare samt leverantörens kundtjänstteam/support.

- Den andra kanalen skapar en direkt kanal mellan AV1 och appen för att göra det möjligt för användaren att ansluta till och använda AV1 (streama ljud och video). En unik nyckelkod (sifferkod) används för att para ihop användarens app med AV1.

5.3 Ny, innovativ eller kontroversiell personuppgiftsbehandling

i

Exempel på nya eller kontroversiella behandlingar är innovativ användning eller tillämpning av tekniska eller organisatoriska lösningar som innefattar person-uppgiftsbehandling såsom användning av artificiell intelligens (AI) i hälso- och sjukvården, ansiktsigenkänning och ”internet of things”, det vill säga apparater, maskiner, mätutrustning och fordon som har inbyggd teknik och internet-uppkoppling, men typiskt sett inte ses som datorer.

Om det inte finns känd problematik med liknande behandlingar så kan exempelvis Integritetsskyddsmyndigheten ha tagit upp kända risker och utmaningar för liknande behandlingar i publikationer eller tillsynsbeslut.

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

Skolroboten/AV1 används enligt leverantören i över 100 svenska kommuner idag och använder inte AI (artificiell intelligens) i någon form.

Utmaningen med personuppgiftsbehandlingen ligger i att leverantören använder amerikanska underleverantörer. Integritetsskyddsmyndigheten beskriver problematiken med behandling av personuppgifter i molntjänster i rapporten Integritetsskyddsrapport 2020[3].

> ”För att få överföra personuppgifter till länder utanför EU krävs att det är tillåtet enligt dataskyddsförordningens regler om tredjelandsöverföring. Det är en utmaning för den personuppgiftsansvarige att i användning av moln-tjänster ha kontroll både på om personuppgifter överförs till tredje land och om det i så fall är tillåtet. Marknaden för molntjänster har, i vart fall hittills, dominerats av amerikanska aktörer, vilket kan medföra att lagringen efter EU-domstolens avgörande i det så kallade Schrems II-ärendet inte längre är laglig.”

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.

[3] Integritetsskyddsrapport 2020, Integritetsskyddsmyndigheten, 28 januari 2021

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.[4]

Inga känsliga uppgifter behandlas, men personuppgifter om barn behandlas i form av video- och ljudupptagning. Personuppgifter om barn anses vara särskilt skyddsvärda personuppgifter.

5.4.2 MÄNGD REGISTRERADE

Uppskatta hur många registrerade som kommer att påverkas av personuppgiftsbehandlingen.

Skolrobotar kommer när det är lämpligt användas för att tillhandahålla och bedriva särskild undervisning för elever som på grund av sjukdom eller liknande skäl inte kan delta i vanligt skolarbete under längre tid.

Det kommer därmed vara en begränsad mängd registrerade som omfattas av behandlingen.

Initialt ska upp till tre stycken skolrobotar användas och utvärderas.

Antal registrerade som påverkas av behandlingen är:

- Elever som är användare av skolrobotar: 3st
- Eventuellt vårdnadshavare till barn som är användare av skolrobotar: 6st
- Personal: lärare/personal i skolan 12st (ca 2-4st/klass), systemförvaltare/ administratörer av skolrobotar 3-4st
- Elever i berörda klasser (ca 25st/klass): 75st

Totalt: ca 100st

5.4.3 MÄNGD PERSONUPPGIFTER

i *För att räkna ut mängd personuppgifter kan man överslagsräkna genom att ta mängden registrerade som uppskattas bli påverkade av behandlingen gånger hur många olika typer av personuppgifter som behandlas.*

Ange hur många personuppgifter som uppskattningsvis kommer att behandlas.

- Namn (elev/användare av skolrobot, personal och eventuellt vårdnadshavare)
- E-post (personal och eventuellt vårdnadshavare)

[4] 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.

- Telefon (personal och eventuellt vårdnadshavare)
- IP-adress (elev/användare av skolrobot, indirekt personuppgift)
- Serienummer (skolrobot, indirekt personuppgift)
- Användar-id (skolrobot, indirekt personuppgift)
- Ljudupptagning (elev/användare av skolrobot)
- Bild- och ljudupptagningar (elever och personal i berörda klasser)

Elev/användare av skolrobot: 15st

Lärare/personal i skola: 48st

Systemförvaltare/administratör av skolrobotar: 12st

Vårdnadshavare: 18st

Elever i berörda klasser: 75st

Totalt: ca 170st personuppgifter

Beräknat utifrån antalet personuppgifter som behandlas per kategori av registrerade multiplicerat med antalet registrerade.

5.4.4 BEHANDLINGENS GEOGRAFISKA RÄCKVIDD

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

Beskriv personuppgiftbehandlingens geografiska räckvidd.

Alingsås kommun

5.4.5 NÖDVÄNDIGA INFORMATIONSTILLGÅNGAR

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

Nätverk

Surfplatta/mobiltelefon

AV1 (skolrobot)

Programvara

5.5 Finns uppförandekoder

Olika branscher kommer att kunna ta fram särskilda uppförandekoder för personuppgiftsbehandling. Ännu finns dock inga sådana uppförandekoder.

Ange om behandlingen är ansluten till en av Integritetsskyddsmyndighetens godkända uppförandekoder som reglerar personuppgiftsbehandlingen.

Nej

5.6 Den registrerades kontroll över sina personuppgifter

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

- Det är valfritt för barn/vårdnadshavare att ansöka om att använda en skolrobot.
- Berörda barn, personal och vårdnadshavare informeras om personuppgiftsbehandlingen. Detta sker inför varje enskilt beslut där en skolrobot ska användas.
- Begäran om exempelvis registerutdrag, rättelse och radering är möjlig att göra via kommunens e-tjänster.
- Användaren av skolroboten (barnet) kan välja att vid behov stänga av sin mikrofon.
- Det finns möjlighet att välja om vårdnadshavare ska kunna registrera personuppgifter och använda leverantörens app för support via chat eller e-post, alternativt enbart använda telefonsupport (utan att några personuppgifter registreras).

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).[5] 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
Se avsnitt 5.1, Beskrivning av behandlingar	Uppgift av allmänt intresse och myndighetsutövning (art. 6 e)	Personuppgiftsbehandlingen syftar till att i enlighet med 24 kapitlet 20§ i Skollagen kunna tillhandahålla och bedriva särskild undervisning för elever som på grund av sjukdom eller liknande skäl inte kan delta i vanligt skolarbete under längre tid. Sådan undervisning ska så långt det är möjligt motsvara den undervisning som eleven inte kan delta i.	Klicka här: Välj undantag från rullgardinslistan

6.2 Ändamål

6.2.1 ANDRA LÄMPLIGA SÄTT ATT UPPNÅ ÄNDAMÅLET

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

Nej, det finns inte några kända alternativa leverantörer inom EU/EES eller alternativa digitala lösningar som på ett likvärdigt sätt skyddar elevens integritet.

Att exempelvis använda en digital tjänst för videokonferens som Google Meet skulle uppfylla ändamålet att bedriva undervisning på distans och skapa möjligheter för eleven att delta i undervisningen och interagera med sina klasskamrater.

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

Google Meet bedömer vi dock inte ha samma inbyggda skydd för elevens integritet som AV1/skolroboten. Till exempel kan barnets kamerafunktion slås på i Google Meet som visar barnet och potentiellt andra personer som befinner sig i samma rum (i hemmet eller på sjukhuset). Det går också att ta skärmdumpar och spela in video/ljud samt koppla till en extern skärm från Google Meet, vilket inte går att göra med AV1.

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.

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.

Behandlingen är nödvändig för att skapa möjlighet för elever som på grund av sjukdom eller liknande skäl inte kan delta i vanligt skolarbete under längre tid att ta del av skolundervisning och hålla kontakten med klasskamrater och delta i det sociala sammanhanget kring lärande. Detta för att minska risken för utanförskap och rätten till att vara delaktig.

I enlighet med 24 kapitlet 20§ i Skollagen ska särskild undervisning för elever som på grund av sjukdom eller liknande skäl inte kan delta i vanligt skolarbete under längre tid så långt det är möjligt motsvara den undervisning som eleven inte kan delta i. Genom användning av skolrobotar kan elever delta i den ordinarie undervisningen i realtid.

6.2.3 ÄNDAMÅLSGLIDNING

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

Beskriv hur ändamålsglidning motverkas.

- Kriterier tas fram för bedömning och beslut när en skolrobot ska användas och inte.
- Rutiner och användarinstruktioner tas fram för användning av skolroboten.
- Inför varje enskild situation och beslut där en skolrobot ska användas görs en utredning och en handlingsplan tas fram för hur skolroboten ska användas.

6.3 Uppgiftsminimering

i *Endast personuppgifter som är nödvändiga för ändamålet får behandlas..*

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

Bedömningen är att det enbart är nödvändiga personuppgifter som behandlas i relation till ändamålet att tillhandahålla och bedriva distansundervisning som särskilt stöd för elever som inte kan delta i den ordinarie undervisningen på grund av dokumenterad medicinsk, psykisk eller social problematik.

Tekniska åtgärder som vidtagits för att begränsa behandling av personuppgifter:

- Barnet visas inte på bild för de elever och lärare som befinner sig i klassrummet.
- Det är inte möjligt att spela in eller spara video- ljudström från skolroboten.
- Det är inte möjligt att ta skärmdumpar från skolroboten. Om eleven försöker göra det på en iOs-enhet får eleven ett meddelande och enheten stängs av.

Organisatoriska åtgärder som vidtagits för att begränsa behandlingen av personuppgifter:

- Inga personuppgifter om barnet (användaren av skolroboten) samlas in eller behandlas av leverantören. Det finns inget register hos leverantören över vilka barn/vårdnadshavare som ansökt om att använda en skolrobot, vilka barn som är användare av skolrobotar eller vilket barn som har vilken skolrobot.
- Vårdnadshavare till barn som använder en skolrobot måste skriva under på att det endast är barnet som ska använda skolroboten. Om någon annan än barnet skulle logga in är det ett kontraktsbrott med leverantören.
- Instruktioner och riktlinjer för personal i skolan tas fram för användning av skolroboten och hur den ska hanteras för att begränsa behandlingen av personuppgifter.
- Vårdnadshavare kan kontakta leverantörens support via telefon. Då registreras inga personuppgifter. Det är valbart för vårdnadshavare om de önskar registrera namn och kontaktuppgifter i syfte att ta kontakt med leverantörens support via e-post/chat.
- I supportärenden behandlas inga personuppgifter om barn.

6.4 Lagringsminimering

i

Personuppgifter får inte sparas längre än vad som behövs för att uppnå ändamålen med behandlingen. När ändamålen som angetts i avsnitt 3.1 har uppnåtts ska gallring eller avidentifiering alltid övervägas om personuppgifterna inte ska arkiveras eller behövs för forskning eller statistik.

Ange hur det tekniskt och organisatoriskt säkerställs att personuppgifter endast lagras så länge de behövs.[6]

De personuppgifter leverantören lagrar är den kundinformation som behövs för att behandla beställning, betalning, leverans och i förekommande fall supportärenden. Kundinformation lagras max i 5 år och raderas därefter av leverantören.

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

Personuppgifter relaterade till supportärenden raderas efter avslutat ärende av leverantören.

Register över ansökningar om skolrobot samt vilket barn/användare som har vilken skolrobot hanteras inom Barn- och ungdomsförvaltningen och raderas av ansvarig administratör löpande efter till exempel beslut om ansökan eller återlämning av skolrobot.

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.

Information om personuppgiftsbehandlingen kommer att ges skriftligt till personal, elever och vårdnadshavare inför varje enskilt införande av skolrobot.

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

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

Den registrerade begär registerutdrag via kommunens befintliga e-tjänst. Inkommen begäran om registerutdrag samordnas av Barn- och ungdomsförvaltningens GDPR-samordnare med berörda funktioner inom förvaltningen t.ex. systemförvaltare och eventuella leverantörer.

7.3 Rätt till dataportabilitet (art. 20 GDPR)

Om applicerbart, ange hur den registrerades rätt till dataportabilitet säkerställs.

Inte aktuellt eftersom rättslig grund för behandlingen inte är samtycke eller avtal.

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

Ange hur den registrerades rätt till rättelse säkerställs.

Den registrerade begär rättelse via kommunens befintliga e-tjänst. Inkommen begäran om rättelse samordnas av Barn- och ungdomsförvaltningens GDPR-samordnare med berörda funktioner inom förvaltningen t.ex. systemförvaltare och eventuella leverantörer.

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.

Den registrerade begär radering via kommunens befintliga e-tjänst. Inkommen begäran om radering samordnas av Barn- och ungdomsförvaltningens GDPR-samordnare med berörda funktioner inom förvaltningen t.ex. systemförvaltare och eventuella leverantörer. I de fall radering inte får lov att utföras på grund av att det strider mot annan lagstiftning (t.ex. Arkivlagen) informeras den registrerade om det.

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.

Invändningar och ärenden rörande begränsning av personuppgiftsbehandling samordnas av Barn- och ungdomsförvaltningens GDPR-samordnare med berörda funktioner inom förvaltningen t.ex. systemförvaltare och eventuella leverantörer.

7.7 Tredjelandsöverföring (kap. 5 GDPR)

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

7.7.1 BESKRIVNING OCH SKYDDSÅTGÄRDER

Om personuppgifter överförs till tredjeland, beskriv vilka tredjelandsöverföringar 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.

Kommentar: En kompletterande beskrivning av de skyddsåtgärder som leverantören vidtagit finns beskrivet i Bilaga 1 - AV1 Technical and organisational security measures.

Personuppgifts-behandling	Beskrivning av tredjelandsöverföring	Överförings-mekanism	Motivering av skyddsåtgärd(er) och tillämplighet[7]
Överföring av video- och ljudström	Underbiträde Amazon Web Services EMEA SARL är ett amerikanskägt företag och lyder under amerikansk lagstiftning, vilket innebär att uppgifter kan samlas in/ begäras ut av amerikanska myndigheter	Standardavtalsklausuler	All överföring av data över internet relaterad till AV1 är krypterad minst TLS 1.2. AV1 streamar med WebRTC, vilket innebär att all data skickas genom en end-to-end-krypterad tunnel (med nycklar i båda ändarna). All mediatrafik använder SRTP (med DTLS för nyckelutbyte). När den end-to-end-krypterade livesträmmen är etablerad, utbyts IP-adresserna för AV1 och användaren via AWS i Frankfurt för att initiera livestreamen mellan dem. Vid streamning av video/ljud sker ingen behandling utanför EU/EES.

[7] 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

			Leverantören använder regionen Frankfurt, Tyskland från AWS/Amazon som värd för sina tjänster. Streaminganslutningen kommer att ta den kortaste möjliga nätverksvägen och kommer endast att korsa AWS i Frankfurt vid streaming om en direkt anslutning mellan AV1 och appen inte är möjlig. I båda fallen, när streaming-anslutningen väl har upprättats, krypteras ljud och video från ände till ände med nycklar som är unika för strömningssessionen och kan därför inte dekrypteras av någon underprocessor i liveströmmens väg. Ingen lagring, cachelagring eller bearbetning av video- och ljudström sker. Ytterligare skyddsåtgärder som leverantören har vidtagit finns beskrivna i Bilaga 1 - AV1 Technical and organisational security measures.
Lagring av kunduppgifter	HubSpot är ett amerikanskägt företag och lyder under amerikansk lagstiftning, vilket innebär att kan samlas in/ begäras ut av amerikanska myndigheter.	Standardavtalsklausuler	Lagring och behandling sker i ett europeiskt datacenter. Personuppgifter som HubSpot behandlar är begränsade till kundinformation (personalens namn och kontaktinformation). Hubspot har ingen information om de enskilda robotarna eller uppgifter om elever.

			Ytterligare skyddsåtgärder som leverantören har vidtagit finns beskrivna i Bilaga 1 - AV1 Technical and organisational security measures.
Administrera och tillgängliggöra tjänsten	Underbiträde Amazon Web Services EMEA SARL är ett amerikanskägt företag och lyder under amerikansk lagstiftning, vilket innebär att uppgifter kan samlas in/ begäras ut av amerikanska myndigheter.	Standardavtalsklausuler	All överföring av data över internet relaterad till AV1 är krypterad enligt ovanstående beskrivning. Lagring och behandling av personalens konton sker inom EU/EES. Leverantören eller leverantörens underbiträde har inte tillgång till några personuppgifter om användaren (eleven). Ytterligare skyddsåtgärder som leverantören har vidtagit finns beskrivna i Bilaga 1 - AV1 Technical and organisational security measures.
Spåra när AV1 aktiveras/avaktiveras samt användning av AV1	Underbiträde Amazon Web Services EMEA SARL är ett amerikanskägt företag och lyder under amerikansk lagstiftning, vilket innebär att uppgifter kan samlas in/ begäras ut av amerikanska myndigheter.	Standardavtalsklausuler	All överföring av data över internet relaterad till AV1 är krypterad enligt ovanstående beskrivning. Behandling sker inom EU/EES. Leverantören och dess underbiträde har inte tillgång till uppgifter om vilken användare (elev) som använder vilket serienummer. Ytterligare skyddsåtgärder som leverantören har vidtagit finns beskrivna i Bilaga 1 - AV1 Technical and organisational security measures.
Support	Underbiträde Amazon Web Services EMEA SARL och Google Cloud EMEA Limited är	Standardavtalsklausuler	All överföring av data över internet relaterad till AV1 är krypterad

	amerikanskägda företag och lyder under amerikansk lagstiftning, vilket innebär att uppgifter kan samlas in/ begäras ut av amerikanska myndigheter.		enligt ovanstående beskrivning. All lagring och bearbetning sker inom EU/EES. Leverantören och dess underbiträde har inte tillgång till uppgifter om vilken användare (elev) som har vilken robot/vilket användar-id. Ytterligare skyddsåtgärder som leverantören har vidtagit finns beskrivna i Bilaga 1 - AV1 Technical and organisational security measures.
Implementera säkerhetsåtgärder	Underbiträde Amazon Web Services EMEA SARL är ett amerikanskägt företag och lyder under amerikansk lagstiftning, vilket innebär att uppgifter kan samlas in/ begäras ut av amerikanska myndigheter.	Standardavtalsklausuler	All överföring av data över internet relaterad till AV1 är krypterad enligt ovanstående beskrivning. All lagring och bearbetning sker inom EU/EES. Leverantören och dess underbiträde har inte tillgång till uppgifter om vilken användare (elev) som har vilken robot/vilket användar-id eller serienummer. Ytterligare skyddsåtgärder som leverantören har vidtagit finns beskrivna i Bilaga 1 - AV1 Technical and organisational security measures.

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.

Nej.

Bedömningen att inte inhämta synpunkter från registrerade baseras på att huvudmannen ska kunna tillhandahålla och bedriva särskild undervisning för elever som på grund av sjukdom eller liknande skäl inte kan delta i vanligt skolarbete under längre tid. Sådan undervisning ska så långt det är möjligt motsvara den undervisning som eleven inte kan delta i.

Vår bedömning att inte inhämta synpunkter från registrerade grundar sig också i svårigheten att identifiera rätt målgrupp att rådgöra med för att få användbara svar.

7.8.2 PERSONUPPGIFTSBITRÄDEN, SPECIALISTER ETC.

i *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.[8]

Riskbedömningsdelen av en konsekvensbedömning ska innehålla[9]:

- 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 konsekvensbedömningen 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.

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.

Se Bilaga 2 - Riskanalys

[8] Mer information om riskbedömningar avseende informationssäkerhet finns i kommunens ledningssystem för informationssäkerhet. Kontakta informationssäkerhetsansvarig (motsvarande).
[9] 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

8.2 Kvarstående höga risker

Dokumentera de risker från riskbedömningsdelen av konsekvensbedömningen som är fortsatt <u>höga</u> (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	Kommentar
					[Hög alt. 8-10]	

Kommentar: Inga risker har bedömts kvarstå som höga efter att riskreducerande åtgärder vidtagits.

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.

9.2 Dataskyddsombudet 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 konsekvensbedömningen (art. 35.2 GDPR), vilket ska dokumenteras i denna ruta. Rutan får endast fyllas i av dataskyddsombudet.

Se ”Bilaga 3 - Dataskyddsombudets kommentar på konsekvensbedömning rörande skolrobot, Alingsås kommun”.

9.3 Sammantagen bedömning – Färdigställs efter beslut av nämnden

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

[Sammantagen bedömning och rekommendation]

Intressenter/saken	Namn/datum	Anteckningar
Dataskyddsombudet har rådfrågats:	Johan Bergström Malin Ericsson 2023-01-09	Se ”Bilaga 3 - Dataskyddsombudets kommentar på konsekvensbedömning rörande skolrobot, Alingsås kommun”.
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:		
Skäl för beslut som avviker från intressenters synpunkter:		
Gå vidare med personuppgiftsbehandlingen (JA/NEJ), beslutad av:		
Motivering:		