Grundskolenämnden
Barn- och utbildningsförvaltningen
Kvalitetsenheten
Per Silvervret Boberg 016-710 45 02

Datum
2023-10-17

Diarienummer
GSN/2023:602

Handlingsnummer
2023:3883

Grundskolenämnden

Förslag till beslut - Godkännande av personuppgiftsbehandling - AV1 - Inkluderingsverktyg för ökad närvaro

Förslag till beslut

1. Konsekvensbedömning av personuppgiftsbehandlingar vid användning av AV1 Robot enligt Dataskyddsförordningens Artikel 35 godkänns.
2. Enligt konsekvensbedömning specificerade personuppgiftsbehandlingar som sker vid användning av AV1 Robot godkänns.
3. Enligt konsekvensbedömning specificerade tredjelandsöverföringar, som inte omfattar elevdata, kopplade till användningen av AV1 Robot godkänns.
4. Användningen av AV1 Robot som inkluderingsverktyg för ökad närvaro i skolan godkänns.

Ärendebeskrivning

Barn- och utbildningsförvaltningen har givits möjlighet att göra ett pilotförsök med användning av verktyget AV1 Robot, som kan användas för elever med frånvaroproblematik av hemmasittarkaraktär eller på grund av sjukdom.

Syftet med de personuppgiftsbehandlingar som sker genom tjänsten och enheten AV1 Robot är att tillgodogöra elev som inte kan närvara fysiskt i klassrummet undervisning och delaktighet i skolan genom digital närvaro och inkludering i klassrummet och skolarbetet.

Användningen av verktyget sker via en teknisk utrustning/hårdvara bestående en AV1-robot som befinner sig i klassrummet och en app som eleven har på surfplatta. När eleven kopplar upp till roboten indikerar roboten med ljussignal att den är aktiv och eleven kan interagera med klassen och läraren med ljud och uttryckssignalering från roboten. Eleven ser det roboten ser och deltar genom robotens ögon i klassrummet. Roboten kan indikera om eleven vill och kan vara delaktig, eller om eleven bara lyssnar.

I ett första steg sker ett pilotprojekt för att identifiera för- och nackdelar med användningen av AV1 Robot.

Det finns tydliga säkerhetsåtgärder på plats för att förhindra att obehöriga tar del av strömmen eller att den avbildas. Eleven kan endast få tillgång till enheten med en kod som genereras av administratör. Om eleven försöker ta skärmavbilder eller spela in strömmen bryts kontakten och strömningen avbryts, koden blir då ogiltig och en ny kod måste genereras manuellt av administratör. Sändningen inbegriper ingen lagring (registrering) av personuppgifter. Överföringen sker direkt peer-to-peer mellan elevens enhet och roboten. Denna data överförs inte genom leverantörens servrar eller underbiträdens servrar. Inga digitala spår kommer heller att finnas kvar/lagras efter en sändning i servermiljön. Data överförs med stark kryptering mellan enheterna (enligt standard SRTM med DTLS, TLS 1.2, 256bit). Serviceförvaltningens IT-avdelning har granskat roboten och förutsättningarna för dess funktionalitet i kommunens nät från ett tekniskt perspektiv.

Beslut om att roboten utgör rätt verktyg för en specifik elev föregås av en tydlig bedömningsprocess. En intresseanmälan görs av rektor via säkert webbformulär. Därefter gör utvecklingsenheten ett urval utifrån olika kriterier, exempelvis prioriterad skola, hög skolfrånvaro med mera. Återkoppling av utvecklingsenhetens urval återkopplas till rektor.

När urval har gjorts sker möte mellan utvecklingsenheten, rektor och skolteam för en kartläggning kring eleven och elevens situation. Om beslut att elev/familj och skola är aktuell fortsätter man till nästa steg, där skolans kontaktperson vänder sig till hemmet för att ge relevant information. Om intresse finns från hemmet och eleven bokas ett hembesök med elev och vårdnadshavare, där kontaktpersonen tar med sig AV1 Robot och elevens schema. När elev och vårdnadshavare tackat ja och godtagit användningsvillkoren informerar skolans team elevens klass och visar roboten. Elever och vårdnadshavare ges möjlighet att yttra sig. Introduktionsmaterial finns.

Kontaktpersonen finns som stöd i hemmet vid uppstart av verktyget och har kontinuerlig kontakt och samordning mellan elev/vårdnadshavare och mentor, specialpedagog/speciallärare. Rutiner finns för hur kontaktpersonen ska jobba med eleven under uppstartsdag och genom hela projektet. Efter användningen sker utvärdering med elev, mentor/klasslärare, klasskamrater, vårdnadshavare, kontaktperson och rektor. Under hela projektet finns coachande stöd till skolan att tillgå från utvecklingsenheten.

Nämnden föreslås godkänna konsekvensbedömning av personuppgiftsbehandlingar vid användning av AV1 Robot enligt Dataskyddsförordningens Artikel 35 och enligt konsekvensbedömning specificerade personuppgiftsbehandlingar som sker vid användning av AV1 Robot samt specificerade tredjelandsöverföringar, som inte omfattar elevdata, kopplade till användningen av AV1 Robot. Användningen av AV1 Robot som inkluderingsverktyg för ökad närvaro i skolan föreslås godkännas.

Konsekvensbedömning

Eftersom användningen av AV1 Robot innebär en behandling av känsliga personuppgifter i en stor uppfattning och rör uppgifter om personer som befinner sig i beroendeställning till personuppgiftsansvarig, såsom barn och anställda ska en konsekvensbedömning enligt artikel 35 dataskyddsförordningen ske. Behandlingen

omfattar även ny teknik som kan räknas till Internet of Things (IoT), vilket också motiverar genomförandet av en konsekvensbedömning.

Bedömningen har täckt in tekniska och administrativa aspekter av behandlingen. Dataskyddssamordnare, administratör och koordinator har genomfört en konsekvensbedömning och ser vi inga juridiska, tekniska och administrativa hinder för att påbörja behandlingen. Grundskolenämnden tar ställning innan behandling påbörjas och personuppgiftsbiträdesavtal tecknas med leverantören.

Dataskyddssamordnaren har lämnat utlåtandet att behandlingen kan påbörjas efter nämndens godkännande. Tillräckliga organisatoriska och tekniska säkerhetsåtgärder har vidtagits. Behandlingen är nödvändig för att tillgodose rätten till utbildning enligt grundlag och uppfyllandet av skolplikt enligt skollag för en mindre kategori elever med särskild problematik. Överföring sker med starkt krypterad peer-to-peer-ström vars innehåll inte kan nås av obehörig eller No Isolation (leverantören). Rutiner och riktlinjer finns. Material finns. Kompletteringar och förtydliganden har skett efter dataskyddsombudets initiala bedömning.

Dataskyddsombudets slutliga bedömning för detta skede och rekommendationer

Dataskyddsombudet har inkommit med följande slutliga bedömning för detta skede:

”Konsekvensbedömningen har nu till större delen kompletterats enligt tidigare rekommendation.

Dokumentationen av personuppgifter på fliken Beskrivning behöver dock fortfarande kompletteras.

Ni behöver säkerställa att ni har alla uppgifter som krävs om underbiträdena för att bedöma och ha dokumentation på deras behandling:
• Var de finns (adress och kontaktuppgifter)
• Var de behandlar personuppgifter (land och stad)
• Vad de gör (t ex support, utveckling, serverdrift)
• Vilka typer av personuppgifter de behandlar
• Behandlingstid
• Bevis på vilka skyddsåtgärder som har genomförts (så att PUA kan bedöma att personuppgifterna behandlas lagligt)

Vad gäller inloggningsförfarandet så finns en högre säkerhet än enbart en vanlig enkel inloggning. Skolan har inte en egen lag som talar om hur en inloggning ska fungera men GDPR styr och det behöver därför finnas en stark inloggning utifrån att känsliga uppgifter om barn kommer att behandlas. Det finns inga garantier för att denna typ av inloggningsförfarande bedöms tillräcklig vid en granskning av t.ex. IMY då den inte uppfyller kriterierna för en stark autentisering.

Barn har skolplikt och rätt till skolgång och delaktighet. En robot som ger denna möjlighet ser inte ut att ersätta en mindre integritetskänslig lösning. Risker har identifierats och åtgärder tagits fram. När det gäller digitala lösningar för barn finns en

del utmaningar och det behöver därför få ta sin tid att förbereda för ett användandet av en ny digital tjänst och i det här fallet en IoT-produkt. Även om mycket arbete har gjorts inför en pilot med AV1 och det finns en hel del dokumentation så finns inte alla delar på plats. Det har t.ex. inte gjorts någon klassning av informationen och mer information om biträdenas behandling behöver komma på plats. Eskilstuna Kommun har idag en process där nya behov ska hanteras och även denna bör gå genom processen.

En konsekvensbedömning är ett levande dokument och ett verktyg som används fram till start av pilot/implementering och även fortsättningsvis vid behov eller t ex årligen."

Kommentar till dataskyddsombudets bedömning och rekommendationer

Dataskyddsombudet kommenterar att dokumentationen av personuppgifter på fliken beskrivningar behöver kompletteras. Underbiträden har listats med plats för säte, plats för behandling av personuppgifter, funktion/vilken typ av uppgifter de behandlar. Skyddsåtgärder som vidtagits i form av uppgiftsminimering och styrning av data framgår tydligt av konsekvensbedömningen. Biträdet instrueras vid tecknande av PuB-avtal om när gallring ska ske av uppgifter.

Dataskyddsombudet menar att inloggningsförfarandet inte uppfyller kriterierna för stark autentisering.

Inloggningsförfarandet är säkrat med att enbart den elev som tilldelats en unik kod kan använda en specifik AV1 robot. Endast en administratör kan generera unika koder för användningen av AV1 Robot. Robotens MAC-adress är kopplad mot kommunens nät så att inte annan utrustning kan nyttja samma tillgång. Säkerhetsåtgärder har även vidtagits kring stöd runt eleven för användandet, vilket säkrar upp att inloggning sker korrekt. Stark kryptering genom peer-to-peer-anslutning kopplar roboten mot elevens surfplatta. Dessa aspekter säkrar användningen och måste också vägas mot den lagstadgade skyldigheten att ge eleven grundskoleutbildning.

Dataskyddsombudet menar att även om mycket arbete har gjorts inför en pilot med AV1 och det finns en hel del dokumentation så finns inte alla delar på plats. Det har t.ex. inte gjorts någon klassning av informationen och mer information om biträdenas behandling behöver komma på plats.

Då initialskedet är ett pilotprojekt med AV1 Robot som kommer att utvärderas så tas dataskyddsombudets kommentar om klassning av informationen med inför ett eventuellt bredare införande. Om AV1 Robot införs efter pilotprojektet kommer klassning genomföras innan ett införande.

Dataskyddsombudet hänvisar till att Eskilstuna Kommun har en process där nya behov ska hanteras och att även detta initiativ bör gå genom processen.

Behovsanalys utifrån ett pedagogiskt perspektiv kan endast utföras av nämndens verksamhet. I detta fall är behovet så specifikt att det inte faller under ett

kommungemensamt perspektiv och en gemensam analys och beredning av behovet av digitala tjänster. Denna process behöver vidare fastställas innan barn- och utbildningsförvaltningen kan göra en bedömning av vilka digitaliseringsinitiativ som faller under ett kommungemensamt paraply.

Tredjelandsöverföringar av mindre känsliga data

Tredjelandsöverföringar sker av icke elevkopplad användningsdata specificerad i konsekvensbedömningen, samt administratörens namn och e-postadress. Överföringar sker till Amazon Web Services EMEA SARL med säte i USA och Google Cloud EMEA med amerikanskt ägande och säte i Irland. Risken med detta lindras dock av att EU-US Data Privacy Framework finns på plats, vilket medger tredjelandsöverföringar till USA. Utöver detta sker överföring till Storbritannien till No Isolation Ltd. I linje med kommunfullmäktiges molntjänstbeslut fattat 21 oktober 2021 § 205 (KSKF/2021:98) behöver nämnden fatta beslut om tredjelandsöverföring och bedöms kunna göra det.

Finansiering

Finansiering för pilotprojektet och eventuell fortsättning sker inom befintlig ram.

Konsekvenser för hållbar utveckling och en effektiv organisation

Åtgärden bedöms medföra positiva effekter för elever med en hemmasittarproblematik eller längre sjukfrånvaro och säkrar att fler elevers rätt till utbildning realiseras. Dessutom ger införandet organisationen möjligheter att arbeta med nya pedagogiska metoder och verktyg, vilket som en följd också stärker pedagogernas kompetens.

———

Beslutet skickas till:
Dataskyddsombudet
Grundskolans utvecklingsenhet
Akten

BARN- OCH UTBILDNINGSFÖRVALTNINGEN

Lina Axelsson Kihlblom
Förvaltningschef

Cathrine Olsson
Administrativ chef

Eskilstuna kommun

Konsekvensbedömning

enligt dataskyddsförordningen, artikel 35

Behandlingens namn

Distansdeltagande i skoldagen med hjälp av AV1 Robot

Personuppgiftsansvarig nämnd

(Det kan vara en eller flera nämnder som är personuppgiftsansvariga, och även andra organisationer. Ange även om de är gemensamt personuppgiftsansvariga)

Grundskolenämnden

Dokumentinformation

Dokumentversion	1	**Diarienummer**	GSN/2023:602
Objekt (PM3)	Utbildning	**Revision intervall**	(Årligen/vid förändringar)
Dokumentägare	Cathrine Olsson, administrativ chef	**Informationsklassning**	
Godkänd av		**Datum för godkännande**	

Medverkande i konsekvensbedömningen

Datum	**Organisation**	**Namn**	**Titel/Roll**
2023-10-03	BUF Kvalitetsenheten	Per Silvervret Boberg	DSS
2023-10-03	Grundskolan, utvecklingsenheten	Monika Lindblom	Administratör
2023-10-03	Grundskolan, utvecklingsenheten	Anneli Hedström	Koordinator
2023-10-12	BUF Kvalitetsenheten	Per Silvervret Boberg	DSS
2023-10-12	Grundskolan, utvecklingsenheten	Monika Lindblom	Administratör
2023-10-12	Grundskolan, utvecklingsenheten	Anneli Hedström	Koordinator
2023-10-24	BUF Kvalitetsenheten	Per Silvervret Boberg	DSS
2023-10-24	Grundskolan, utvecklingsenheten	Monika Lindblom	Administratör
2023-10-24	Grundskolan, utvecklingsenheten	Anneli Hedström	Koordinator
2023-10-27	BUF Kvalitetsenheten	Per Silvervret Boberg	DSS
2023-10-27	Grundskolan, utvecklingsenheten	Anneli Hedström	Koordinator
2023-10-27	Grundskolan, utvecklingsenheten	Monika Lindblom	Administratör
2023-10-31	BUF Kvalitetsenheten	Per Silvervret Boberg	DSS

Bedömning av hög risk

(Använd dokumentet Information om konsekvensbedömningar och förhandssamråd i arbetet med konsekvensbedömningen.)

1. Personuppgifter

	Ja	Nej
Omfattar behandlingen personuppgifter	X	

(Använd Checklista för identifiering av personuppgifter)

Om behandlingen omfattar personuppgifter, fortsätt.

Om personuppgifter inte behandlas behöver en konsekvensbedömning inte göras.

2. Kriterier för hög risk, storskalighet

Dataskyddsförordningen ger tre exempel på behandlingar som sannolikt leder till hög risk och alltid kräver att en konsekvensbedömning görs. Om det hamnar på gränsen välj Ja. Om ett av ovanstående kriterier uppfylls så behöver en konsekvensbedömning göras.

	Ja	Nej
När man använder automatiskt beslutsfattande som grundar sig på en systematisk och omfattande bedömning av människors personliga aspekter, till exempel profilering.		**X**
När man behandlar uppgifter om lagöverträdelser eller känsliga personuppgifter, till exempel uppgifter om hälsa, religiös tro, politisk uppfattning eller etniskt ursprung, i stor omfattning.		**X**
När man systematiskt övervakar en allmän plats i stor omfattning, genom till exempel kameraövervakning.		**X**

3. Kriterier för hög risk

Om två eller flera av kriterierna nedan är uppfyllda ska en konsekvensbedömning enligt artikel 35 göras.
I tveksamma fall bör man alltid göra en konsekvensbedömning.

	Ja	Nej
1. Utvärderar eller poängsätter människor, till exempel ett företag som erbjuder genetiska tester till konsumenter för att bedöma risker för sjukdomar, ett kreditupplysningsföretag eller ett företag som profilerar internetanvändare *(Med profilering menas analys eller förutsägelser av särdrag som i synnerhet gäller arbetsprestationer, den ekonomiska situationen, personliga preferenser, intressen, pålitlighet, beteenden, position eller rörelser.)*		X
2. Behandlar personuppgifter i syfte att fatta automatiska beslut som har rättsliga följder eller liknande betydande följder för den registrerade *(Med automatiska beslut menas att en människa inte deltar i beslutsfattandet utan att beslutet fattas maskinellt utifrån en persons personuppgifter. Detta kan innebära att en person utesluts eller diskrimineras på grund av ett automatiskt beslut. Automatiska beslut kan inhämtas genom enkätformulär etc.* *Exempel: automatiska kreditprövningar, sökande får avslag vid jobbansökan via Internet utan att person varit inblandad, robot fattar automatiserade beslut som avser beslut om ekonomiskt bistånd.)*		X
3. Systematiskt övervakar människor, till exempel genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer *(Det gäller även övervakning av nätverk och övervakning av medarbetares surfbeteenden på arbetsenheter, hur anställda använder internet och e-post)*		X

4. Behandlar känsliga personuppgifter eller uppgifter som är mycket personliga, till exempel ett sjukhus som lagrar patientjournaler, ett företag som samlar in lokaliseringsuppgifter eller en bank som hanterar finansiella uppgifter. *(Känsliga personuppgifter är Uppgifter om ras eller etniskt ursprung, Politiska åsikter, Religiös eller filosofisk övertygelse, Medlemskap i en fackförening, Hälsa, En persons sexualliv eller sexuella läggning, Genetiska uppgifter och Biometriska uppgifter som entydigt identifierar en person via särskild teknik)*	X	
5. Behandlar personuppgifter i stor omfattning *(Gör en bedömning utifrån Antalet registrerade som berörs, antingen som ett särskilt antal eller som en andel av den aktuella populationen, Mängden uppgifter och/eller variationen av hanterade dataelement, Databehandlingens varaktighet eller beständighet, Behandlingens geografiska omfattning.)*	X	
6. Kombinerar personuppgifter från två eller flera behandlingar på ett sätt som den registrerade inte förväntar sig, till exempel när man samkör register *(Samkörning av två databaser som t ex finns hos olika avdelningar men de har olika syften etc.)*		X
7. Behandlar personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, exempelvis barn, anställda, asylsökande, äldre och patienter *(T ex Behandling av Barns personuppgifter i skolverksamhet, Brukare inom socialtjänsten, Elever på KomVux, SFI mm, Personer med skyddade uppgifter)*	X	
8. Använder ny teknik eller nya organisatoriska lösningar, till exempel en sakernas internet-applikation (Internet of things, IoT) *(Ny teknik, nya organisatoriska lösningar, eller gammal teknik som används på ett nytt sätt som omfattar nya former av insamling och användning av personuppgifter.* *Exempel: Internetuppkopplade produkter som kan fjärrstyras, t ex medicintekniska produkter, Teknik som samlar in uppgifter, Verksamheter inom social omsorg som tillhandahåller välfärdsteknik, t.ex. robotar eller kameror/sensorer i människors boende, Smarta elmätare hos elabonnenter för att kunna ta fram, överföra och analysera uppgifter som rör konsumenter på en detaljerad nivå, Fingeravtryck eller ansiktsigenkänning för inpassering.)*	X	
9. Behandlar personuppgifter på ett sätt som hindrar de registrerade från att få tillgång till en tjänst eller ingå ett avtal, till exempel när en bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån *(Exempel: Kreditupplysning, Psykologiska tester som kan ge reservationen hos försäkringsbolag etc.)*		X
	Ja	**Nej**
Summering	**4**	**5**

Om två eller fler av frågorna besvaras med ”ja” krävs det i regel en konsekvensbedömning. Det kan finnas fall där det krävs även om endast en av frågorna besvaras med ”ja”. Om man är osäker bör man göra en, och det är aldrig fel att göra en.

Ska en konsekvensbedömning göras? (Ja/Nej)	**Ja**

Motivering

Ny teknik för elevs distansdeltagande. Innehåller uppgifter om barn och kamera, vilket motiverar genomförande av konsekvensbedömning.

Personuppgiftsbiträden

Ange personuppgiftsbiträden och deras underbiträden nedan. Gå igenom om överföring sker till tredje land, dvs Land utanför EU/EES.

Personuppgiftsbiträden

Biträdets namn	**Land (ägarskap)**	**Var uppgifterna behandlas** (Land+stad)	**Biträdets roll/uppgift**	**Sker överföring?**
No Isolation AS, Trondheimsveien 2, 0560 Oslo, Norway	Norge	Norge	Tillhandahålla tjänsten AV1 Robot Supplier personnel supporting Customer Users and End Users with enquiries regarding the Services.	Nej

Underbiträden

Underbiträdets namn	Land (ägarskap)	Var uppgifterna behandlas (Land+stad)	Underbiträdets roll/uppgift	Sker överföring?
Amazon Web Services EMEA SARL, 38 Av. John F. Kennedy, 1855, Luxembourg	USA.	Frankfurt, Germany. AWS Region: Europe (Frankfurt)	Cloud infrastructure services for Supplier to process and store the data required to provide the Services. AV1, AV1 Assistant App, AV1 Admin, AV1 Dashboard. Amazon: CloudWatch, EC2, EKS, Kinesis, RDS, VPC and Elastic Load Balancing, Amazon DocumentDB	Ja, för vissa uppgifter, loggning och teknisk support samt medarbetares inloggningsinformation. Slutanvändaren kan ej identifieras. USA Transfers: EU-US Adequacy Decision (Data Privacy Framework), adopted July 10th 2023.

Google Cloud EMEA Limited, Velasco, Clanwilliam Place, Dublin 2, Ireland	USA.	Region: Europe.	Email services for Supplier to support Customer Users and End Users with enquiries regarding the Services. AV1, AV1 Assistant App, AV1 Admin, AV1 Dashboard. Google: Google Workspace Gmail	Ja, för vissa uppgifter, leverantörens e-post och support, medarbetarens e-postadress kan förekomma. Slutanvändaren kan ej identifieras. USA Transfers: EU-US Adequacy Decision (Data Privacy Framework), adopted July 10th 2023.
Aircall SAS, 11-15, rue Saint Georges, 75009, Paris, France	Frankrike, region Europa	Frankrike	Telephony services for Supplier to support Customer Users and End Users with enquiries regarding the Services. AV1, AV1 Assistant App, AV1 Admin, AV1 Dashboard	Nej
HubSpot Ireland Ltd, Ground Floor, Two Dockland Central, Guild Street, Dublin 1, Co. Dublin, Ireland	Irland	Europa	Live chat and email services for Supplier to support Customer Users and End Users with enquiries regarding the Services. HubSpot CRM	Nej

Simple Analytics B.V, Jacob van Lennepstraat 78 H, 1053 HM, Amsterdam, Noord-Holland, Netherlands	Nederländerna	Nederländerna. Region Europa	Analysis of Customer metadata providing Supplier with user statistics and reporting anonymized user interactions with the App. AV1 Admin	Nej
Odoo SA, Grand-Rosière-Hottomont, 1367 Ramillies, Belgium	Belgien	Belgien. Region Europa	Billing and accounting services necessary for Supplier to provide the Services to the Customer, documentation of Customer Relationships	Nej
No Isolation Ltd., 239 Old St, London, EC1V 9EY, United Kingdom	Storbritannien	Storbritannien	Tillhandahålla tjänsten AV1 Robot Supplier personnel supporting Customer Users and End Users with enquiries regarding the Services.	Ja, för vissa uppgifter, metadata för en AV1-enhet och kontaktinformation till kontakt på kommunen. Slutanvändaren kan ej identifieras.
No Isolation GmbH., Viktualienmarkt 8, Munich, 80331, Germany	Tyskland	Tyskland	Tillhandahålla tjänsten AV1 Robot Supplier personnel supporting Customer Users and End Users with enquiries regarding the Services.	Nej

Avgränsning

Beskriv avgränsning för konsekvensbedömningen, t ex om det är hela flödet av personuppgifter genom en behandlingsprocess eller om det är en viss del av behandlingsprocessen som avses och i så fall vilken.

Konsekvensbedömningen avser flödet av personuppgifter från AV1 Robot placerad i klassrum till app i elevs surfplatta eller mobiltelefon. Detta är den enda del av hanteringen av AV1 Robot som innehåller elevs personuppgifter. Bedömningen omfattar även administrationen av elevens uppgifter hos personuppgiftsansvarig avseende den här behandlingen.

Informationsflöden

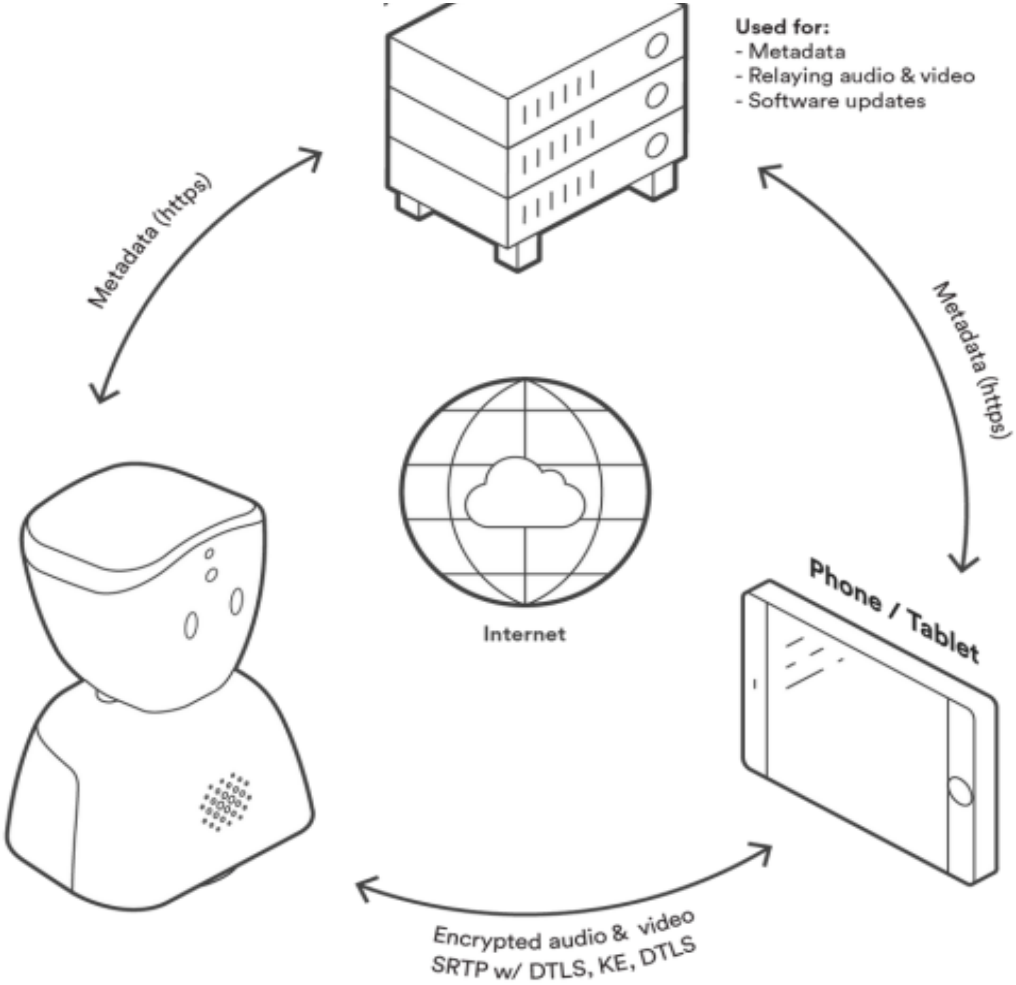
Här redovisas hur informationsflödet ser ut, hela vägen, från början till slut. Gärna både det tekniska flödet, så som en systemskiss, och flödet genom verksamheten, t ex en process.

Tekniskt flöde: Detta ska visa hur systemet eller den tekniska lösningen är uppbyggd så att man får en bild av hur informationen flödar. Det går inte att göra utan att ha fått information från leverantören, så som systemskiss. De behöver även lämna utförlig dokumentation över sin tekniska lösning och dess säkerhet.

Verksamhetens flöde: Visa hur den del av processen för personuppgiftsbehandlingen ser ut som ska konsekvensbedömas. Den kan inkludera t ex hantering av inkomna dokument, hur de förs in i systemet, vilka de delas med osv. (Om en sådan ritad process finns)

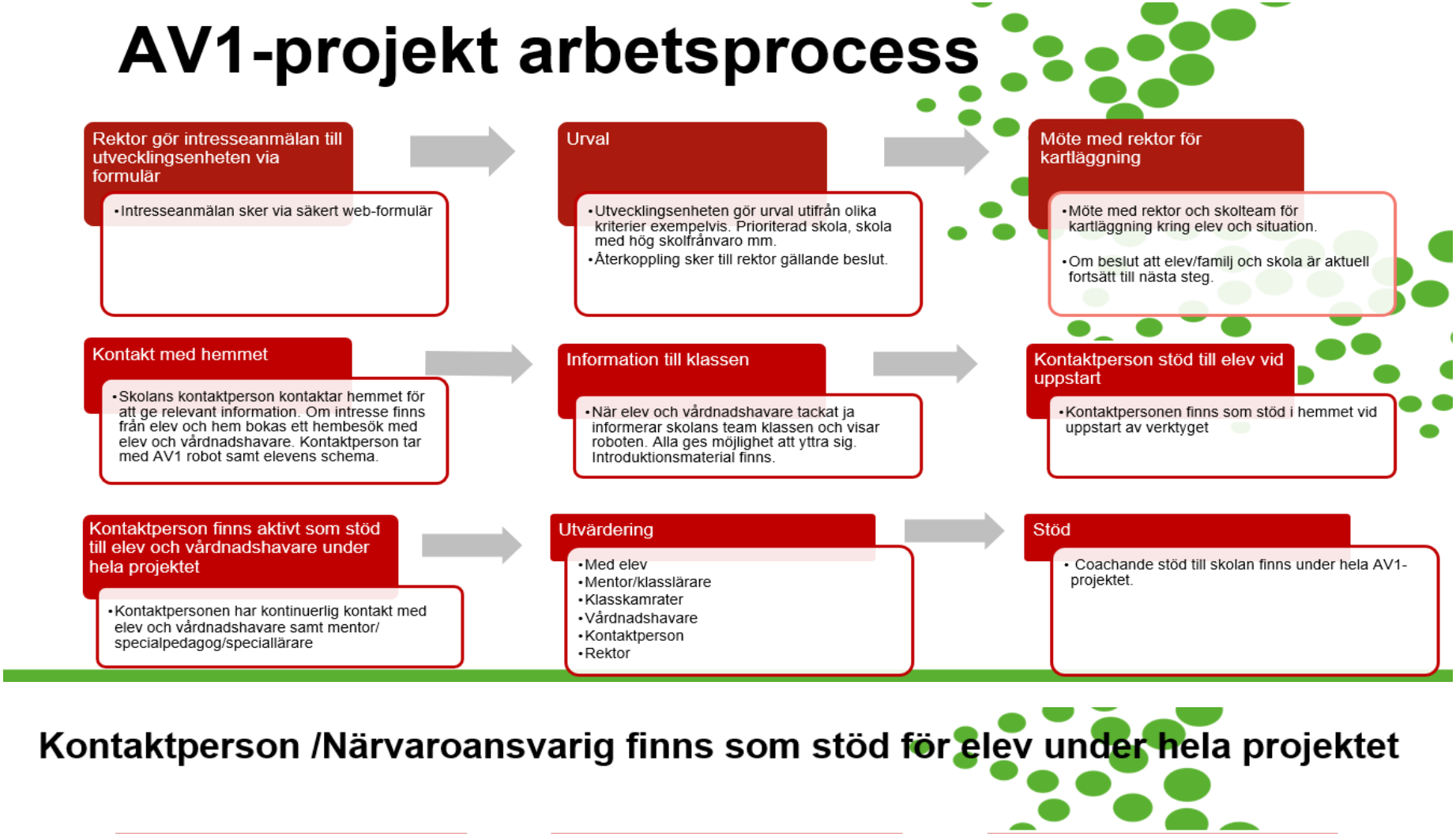
Tekniskt flöde för personuppgifterna

Bild och ljud är starkt krypterade och går via en krypterad stream(TLS 1.2 och AES256 samt sessionsgenererad nyckel med SRTP med DTLS), direkt mellan elevens enhet och roboten (peer-to-peer). I undantagsfall, när P2P inte är möjligt, kan UDP Port 443 användas för att köra streamen via Amazon Web Services (AWS). Även i sådana tillfällen är streamen krypterad, och det är No Isolation som äger krypteringsnycklarna, inte AWS. Eventuell AWS-aktivering kommer att villkoras i Instruktionen till biträdet med att den inte ska ske utan personuppgiftsansvarigs godkännande i förväg. Data som annars passerar AWS i Frankfurt är krypterad metadata (batteristatus på roboten, när användes den senast, wifi, etc och innehåller inga personuppgifter som kan kopplas till eleven). För support och e-post delas med tredje land endast medarbetarens e-postadress/användarnamn och inloggningsuppgifter. Inga elevdata passerar tredje land.



Verksamhetens flöde för personuppgifterna

Flödet är av den information som går mellan eleven och klassrummet via den krypterade anslutningen. I övrigt hanteras behörighetstilldelning av administratör på grundskolans utvecklingsenhet. Administratör är den som kan skapa en kod kopplad till en specifik robot. Denna kod tilldelas den elev som ska använda roboten via appen. Koden kopplas aldrig till eleven i system, varför leverantören ej kan identifiera eleven ens via metadata. Metadata kring användningen av roboten har bara koppling till robotens serienummer. Verksamhetens arbetsprocess anges också.




Vid uppstartsdag bör du som kontaktperson vara hemma hos eleven minst 30 minuter innan lektionsstart så ni hinner stärka tillit och relation samt koppla upp roboten. Ta med elevens schema i fysisk form.
Efter första lektion med roboten tar ni en reflektionstid tillsammans. Hur upplevde eleven lektionen.
Tillsammans med eleven resonerar ni fram vilka lektioner eleven önskar koppla upp sig till.
Säkerhetsställ att eleven känner sig säker på verktyget samt om eleven behöver stöd vid uppstart vid nästa lektionstillfälle.
Meddela mentor/klasslärare kring vad ni kommit överens om så läraren vet vilka lektioner roboten ska vara på.
Boka in stående uppföljningsdagar med elev och vårdnadshavare där ni återkopplar till varandra.

Beskrivning av behandlingen

Systematisk beskrivning av behandlingen	Frågeställning	Beskrivning	Exempel och instruktion
Beskrivning av ändamål och syfte	**Vad är ändamålet med behandlingen?** Flera ändamål kan finnas. Ange samtliga. Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.	Tillgodogöra elev som inte kan närvara fysiskt i klassrummet undervisning och delaktighet i skolan genom digital närvaro och inkludering i klassrummet och skolarbetet. Detta för att möjliggöra elevens rätt till skola samt uppfyllelse av skolplikt, och huvudmannens skyldigheter enligt skollag och grundlag.	*Ni måste ha klart för er varför ni ska behandla personuppgifterna redan när ni börjar samla in dem. Ändamålen sätter ramarna för vad ni får och inte får göra. Det behöver ni för att kunna visa att ni uppfyller principen om ansvarsskyldighet.* *Ändamålen måste vara specifika och konkreta, inte luddiga eller otydliga.* *Ändamålet måste också vara berättigat. Detta innebär att personuppgiftsbehandlingen dels ska ha en rättslig grund i dataskyddsförordningen, dels ska ske i enlighet med övrig tillämplig lagstiftning och allmänna rättsprinciper.*
	Vad är syftet med den planerade behandlingen? Vad vill ni åstadkomma? Vad är den planerade effekten för individer? Vilka fördelar får ni från behandlingen och finns det några bredare fördelar?	Behandlingen syftar till att göra det möjligt för en elev som på grund av fysisk hinder, sjukdom eller annan problematik (exempelvis hemmasittarproblematik) inte kan ta sig till skolan, att kunna tillgodogöra sig och delta i den undervisning och de aktiviteter som sker i klassrummet – trots att eleven och läraren och klasskamraterna är åtskilda i rum. Detta sker via en teknisk utrustning/hårdvara bestående en AV1-robot som befinner sig i klassrummet och en app som eleven kan ha på ipad eller telefon. När eleven kopplar upp till roboten indikerar roboten med ljussignal att den är aktiv och eleven kan interagera med klassen och läraren med ljud och uttryckssignalering från roboten. Eleven ser det roboten ser och deltagande i klassrummet Roboten indikerar om eleven vill och kan vara delaktig, eller om eleven bara lyssnar. Om eleven försöker ta skärmavbilder eller spela in strömmen bryts kontakten och strömningen avbryts. Sändningen inbegriper ingen lagring (registrering) av personuppgifter. Inga digitala spår kommer heller att finnas kvar/lagras efter en sändning i servermiljön.	*Beskriv syftet.* *T ex.* *Effektivisera / Automatisera / Snabbare behandling / Säkra uppgifternas korrekthet / Sänkta kostnader / Bättre service* *Här finns möjlighet att skriva utförligare än ändamålet.*
Beskriv behandlingen	**Kategorier av personuppgifter som ingår i behandlingen**	Bild och ljud (på deltagande i klassrum; klasskamrater och lärare), röst (eleven som styr roboten), namn	*Checklista för identifiering av personuppgifter finns.* *Exempel:* *Data som behandlas är namn, personnummer, adress, kontaktuppgifter i form av telefonnummer och e-postadress, IP-adress, GPS-koordinater.*
	Känsliga personuppgifter. Särskilda kategorier av personuppgifter enligt artikel 9. Ange	Uppgifter delas endast i den mån de skulle delats i en vanlig klassrumssituation. Således kan känsliga personuppgifter förekomma i livesströmningen, men de delas inte med någon utomstående och lagras inte.	*etniskt ursprung* *politiska åsikter* *religiös eller filosofisk övertygelse* *medlemskap i en fackförening* *hälsa* *en persons sexualliv eller sexuella läggning* *genetiska uppgifter* *biometriska uppgifter som används för att entydigt identifiera en person*
	Extra skyddsvärda personuppgifter. Ange	Uppgifter om barn och uppgifter om enskilds sociala situation kan förekomma i livströmmen utifrån att en klassrumssituation föreligger, men de delas inte med utomstående och lagras inte.	*Exempel:* *personnummer, GPS-data, lön eller annan ekonomisk information, uppgifter om enskilds sociala situation, värderande uppgifter, uppgifter om barn (personer under 18 år) mm*

	Innefattar behandlingen uppgifter om brott? Beskriv.	Uppgifter om barn och uppgifter om enskilds sociala situation kan förekomma i livströmmen utifrån att en klassrumssituation föreligger, men de delas inte med utomstående och lagras inte.	*Uppgifter om brott är extra skyddsvärda och behöver ett högre skydd. De omfattas i regel av artikel 10 i GDPR, men vissa omfattas av brottsdatalagen vilket gäller få behandlingar i kommunen. I det fall de omfattas av brottsdatalagen behöver konsekvensbedömning göras utifrån dess kriterier.*
	Innefattar behandlingen sekretessuppgifter? Beskriv.	I den händelse något omfattas av sekretess kan det förekomma i livströmmen utifrån att en klassrumssituation föreligger, men de delas inte med utomstående och lagras inte.	*Sekretess styrs av lag och när personuppgifter omfattas av sekretess behöver de ett högt skydd. Om det är oklart vad som omfattas av sekretess behöver det utredas för att konsekvensbedömningen ska bli korrekt.*
	Innefattar behandlingen skyddade personuppgifter?	Nej. Vid behandling i kontext med elever med skyddade uppgifter säkerställs att dessa elever inte kan identifieras.	*Det finns tre typer av skyddade personuppgifter, eller skyddad identitet som det också kallas:* *- skyddad folkbokföring* *- sekretessmarkering* *- fingerade personuppgifter, som innebär att personen får nytt namn och personnummer.* *Se Skatteverket för information som gäller system för dessa uppgifter.* *https://skatteverket.se/offentligaaktorer/informationsutbyte/folkbokforingsekretessmarkeradepersonuppgifter.4.18e1b10334ebe8bc80002541.html*
	Behandlingar som har identifierats som högriskbehandlingar	Den registrerade står i beroendeställning till personuppgiftsansvarig. Eleven kan vara sårbar utifrån hälsotillstånd och personliga omständigheter med mera. Informationen som hanteras är den information som kan förekomma i en klassrumssituation, och där har läraren ett stort ansvar att se till att eleven inkluderas på rätt sätt. Det är också därför en grundlig bedömning görs innan elev erbjuds möjligheter med AV1. Denna beskrivs i verksamhetens process som illustreras i flik infoflöden.	*Exempel:* *Behandlingen omfattar känsliga personuppgifter* *De registrerade står i beroendeställning till personuppgiftsansvarig* *Oönskad händelse kan leda till hinder eller fördröjning* *Behandlingen omfattar samtliga elever i grundskolan / förskola (stort antal barn)*
	Antal individer som omfattas av behandlingen: Summa:	Vid ett pilotsteg är det 6 robotar och lärare samt klass dessa förekommer i alltså cirka 280 personer om man räknar ihop medarbetare och ett snittantal klasskamrater samt eleven som använder sig av AV1-roboten.	*Ändra text och fyll på med kategorier i de punktade rutorna så att det passar er behandling.* *Antal användare med behörighet?* *Antal individer: personal, brukare, elever, personal utöver användare som finns registrerade, klienter, anhöriga, förtroendevalda, personal inom hemtjänsten, sjuksköterskor, lärare, gymnasieelever.*
	Antal användare	6 elever som använder roboten. Upp till och med 280 personer medräknat lärare och elevers klasskamrater.	
	Antal systemförvaltare/-admin.	1	
	Antal personal	cirka 30	
	Antal brukare		
	...		
	...		
	...		
	Den geografiska omfattningen	Elever som går i skola i Eskilstuna kommun, medarbetare i Eskilstuna kommun.	*Exempel:* *Endast medborgare folkbokförda i Eskilstuna kommun.* *Samtliga elever i grundskolan.* *Alla medarbetare i Eskilstuna kommun.* *Brukare på Vård- och omsorgsboendet XXX, Sverige.*

Beskriv behandlingens kontext	**Den relation organisationen har till de registrerade**	De registrerade är elever och medarbetare.	*De registrerade är Anställda/elever/brukare/prakikanter etc.*
	Uppgifter om barn	Ja, elever i grundskola. Användningen är tänkt att äga rum i årskurs 4-9 efter behovsbedömning.	*Om ja, vad/vilka.* *Barn är alla som inte har fyllt 18 år.* *T ex barn på förskola, Elever i årskurserna 1-3* *Alla uppgifter spm rör barn är extra skyddsvärda.*
	Uppgifter om andra sårbara personer eller personer i beroendeställning	Elever med särskild problematik eller sjukdom. Elever och medarbetare är i beroendeställning.	*Om ja, vad/vilka.* *T ex Elever, brukare, klienter, anställda.*
	De registrerades kontroll över sina uppgifter och hur det säkerställs	Särskild information ges till de registrerade och de registrerades klasskamrater med vårdnadshavare innan behandlingen påbörjas. Rutiner finns på plats för att hantera och behandla de registrerades rättigheter.	*De registrerade har rätt att ha kontroll över sina personuppgifter.* *Information till de registrerade finns på kommunens hemsida. Kommunen har rutiner för att ta emot och behandla de registrerades rättigheter.*
	Förväntar sig de registrerade att personuppgifterna behandlas på detta sätt?	Ja, en behandling initieras inte utan omfattande dialog med elev och vårdnadshavare som berörs.	*Ja/Nej, beskriv om det finns behov*
	Är behandlingen ny på något sätt? Innefattar den ny eller innovativ teknik? Innefattar den gammal teknik som används på ett nytt sätt?	Tekniken är inte helt ny men kan ändå anses vara innovativ och räknas som en del av Internet of Things (IoT).	*T ex IoT, AI, kameror som används på nytt sätt mm.*
	Tidigare oro över denna typ av behandling eller brister i säkerheten	Oron för molnlagring har hanterats genom att strömning ej går genom AWS. Instruktion till personuppgiftsbiträdesavtal kommer att ge att: "All transmission of data over the internet related to AV1 is encrypted to at least the TLS 1.2 standard and covers transmissions required for the services. All signals are encrypted with strong keys and use HTTPS protocol. Databases/servers have encrypted disks/backups/ communications. All media traffic (i.e. audio and video stream) use SRTP (with DTLS for key exchange) or DTLS. Communications are encrypted end-to-end with these keys using SRTP whether communications take place directly between the AV1 to the apps, or through a relay). Metadata (including IP address, end point identifiers and encryption keys) required to establish connections is sent encrypted with TLS between AV1 and No Isolation's servers. The WebRTC standard is used to set up the audio and video stream and WebRTC signals (i.e. metadata) are transmitted (TLS-encrypted) via No Isolation servers." Av instruktionen framgår även att mediatrafiken (ljud/bild) endast får ske peer-to-peer.	*Ja/Nej beskriv ev brister och teknik.* *Exempel:* *Brister i säkerhet gällande …. är vanligt i denna teknik. Det är vanligt att leverantörer av molntjänster har USA-baserade underbiträden vilket leder till över föring till tredjeland.* *Krypteringen håller ofta inte den nivå som krävs för...*
	Oro bland allmänheten som borde tas i beaktande	Ingen känd oro över behandlingen.	*Ja/Nej. Beskriv.* *Har det kanske skrivits i media? Har brukare, vårdnadshavare etc uttryckt oro?*

	Den nuvarande tekniken Om det är relevant.	Det finns ingen lösning idag som kan användas för ändamålet.	*Vid ett skifte till nyare teknik kan det vara relevant att lämna en beskrivning av vad som finns idag. Exempel: utförs idag på papper men ska övergå till digital behandling, systemet finns idag i våra serverhallar men upphandlingen gäller molntjänst, inloggning sker idag med användarnamn och lösenord men vi kommer att gå över till stark autentisering med SITHS-kort.*
	Tekniska tillgångar som behövs för behandlingen	AV1 Robotar tillhandahålls av leverantören för ett pilotförsök. Om detta ger önskat resultat köps roboten in. SEF IT har konstaterat att tekniska förutsättningar för robotarnas anslutning till kommunens nät finns. Internetuppkoppling. Surfplatta. Detta är att betrakta som en IoT-lösning.	*T ex , 50 nya datorer behöver köpas, surfplattor, viss maskinvara, programvara, nätverk, skrivare, annan sorts teknik, RPA, AI, IoT. Molntjänst eller hos kommunen (on prem).* *Behov av integration beskrivs både för att föra in uppgifter i systemet och för att föra ut.*
	Andra tillgångar som behövs för behandlingen	Elev, medverkande lärare, annan personal, vårdnadshavare.	*T ex personer, papper, spridningskanaler för papper.*
	Alternativ till den önskade behandlingen	Det är möjligt med sjukhusundervisning eller undervisning på annan plats, men det medger inte eleven samma möjlighet att känna sig delaktig på sina egna villkor i klassrummet. Behandlingen möjliggör för hemmasittare att närma sig skolan igen på ett mindre krävande sätt än att närvara fysiskt i klassrummet. Behandlingen bedöms också kunna möjliggöra för elever med sjukdom att behålla sin närvaro i klassrummet på ett helt annat sätt än att undervisas separat.	*Finns det flera sätt att genomföra behandlingen? Främst när det gäller mer integritetskänsliga behandlingar.* *Finns det sätt som innebär mindre risk för den registrerade och som är mindre integritetskänslig?* *Redogör för de olika alternativen. Detta är nödvändigt för att en korrekt proportionalitetsbedömning ska kunna göras.*
	Anslutning till någon uppförandekod	No Isolation har en egen code of conduct som tillhandahållls underleverantörer. (Bilaga A)	*De berörda personuppgiftsansvarigas eller personuppgiftsbiträdenas efterlevnad av godkända uppförandekoder enligt artikel 40 ska på lämpligt sätt beaktas vid bedömningen av konsekvenserna av behandlingen. Sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden får utarbeta uppförandekoder, eller ändra eller utöka sådana koder, i syfte att specificera tillämpningen av GDPR.*
	Anslutning till erkänd certifiering som behöver beaktas (när någon blivit godkänd)	Nej.	*Om ja, beskriv*
Beskriv utförandet	**Data för administration av användare**		*Se informationssflödeskartläggning under avgränsning för en visualisering av utförandet.* *Exempel:* *Användares data förs över till systemet via integration med AD,* *Blankett för behörigheter sparas i pärm hos systemförvaltare,*
	Hur data för administration av användare kommer att samlas in	Administratör på utvecklingsenheten får information från rektor/klasslärare om att behov finns för elev att använda AV1 robot. Administratör hanterar skriftlig överenskommelse mellan elev/vh och skola om villkoren för användning - att ingen annan person får finnas i rummet eller avlyssna deltagandet.	
	Hur data för administration av användare kommer att användas	Skriftlig överenskommelse samt information om elev och vilken robot elev är kopplad till via appen.	

Hur data för administration av användare kommer att förvaras/ lagras	Förvaras i låst skåp hos administratör på utvecklingsenheten.	
Hur länge data för administration av användare ska sparas	Data sparas bara så länge eleven använder sig av roboten.	
Hur data för administration av användare ska raderas	Administratör makulerar data vid avslutad användning.	
Data som produceras av användarna (för t ex handläggning)		*Exempel:* *Vårdnadshavare fyller i elevens personuppgifter i ett webbformulär, Användares data förs över till systemet via integration med AD, Brukare lämnar uppgifterna vid kontakt med biståndshandläggare, Uppdateras en gång per år, Hämtas automatsikt en gång per dygn, Data samlas in vid registrering av...* *Användarproducerad data kommer att användas för handläggning och beslut om bygglov, Loggdata kommer att användas för regelbunden loggkontroll enligt lagrum…§../vid misstanke om dataintrång.* *Data lagras i molntjänst i leverantörens servrar.* *Personuppgifter får inte sparas längre än vad som är nödvändigt för ändamålet. Därefter ska de raderas, bevaras, anonymiseras eller på annat sätt hanteras så att person inte kan identifieras.* *Det kan styras av lag och i annat fall beslutas. Uppgiften finns ev i informationshanteringsplanen.* *Exempel:* *Användare gallras 6 månader efter avslutad tjänst, Användarproducerad data bevaras / raderas 3 månader efter... / gallras när brukare inte varit aktuell i 5 år.*
Hur data som produceras av användarna (för t ex handläggning) kommer att samlas in	Utgående ljuddata och funktionsinput till robot - streamas i realtid, bevaras inte. Ingående ljud- och videodata streamas och bevaras inte.	
Hur data som produceras av användarna (för t ex handläggning) kommer att användas	Används bara i stunden i livestream.	
Hur data som produceras av användarna (för t ex handläggning) kommer att förvaras/ lagras	Lagras ej, livestream.	
Hur länge data som produceras av användarna (för t ex handläggning) ska sparas	Lagras ej, livestream.	
Hur datasom produceras av användarna (för t ex handläggning) ska raderas	Data som genereras genom liveström sparas ej alls.	
Vad som behöver loggas		*Loggar är viktiga för spårbarheten i ett sytem/tjänst. Där kan man se vem som har gjort vad. Vad som behöver loggas styrs i vissa fall av lagar. I andra fall behöver man tänka igenom vad man behöver kunna se i efterhand. Ju mer skyddsvärd informationen är desto mer detaljerade loggar kan behövas. Loggar ska dock inte visa mer än vad som behövs.* *Det kan finnas krav på loggkontroller i lag, t ex i patientjournaler.*
Hur loggdatan kommer att samlas in	Loggdata av upp och nedkoppling ej kopplad till person, endast robotens användarid.	
Hur loggdatan kommer att användas	Loggdata ska användas för uppföljning av enhetens upp- och nedkoppling vid eventuell incident.	
Hur loggdatan kommer att förvaras/ lagras	Biträdet förvarar loggarna och personuppgiftsansvarig kan få tillgång på begäran.	
Hur länge loggdatan ska sparas	Loggdata bevaras endast så länge en robot är i användning, därefter ska den raderas senast fyra veckor efteråt.	
Bevarande. Ska information föras över till e-arkiv?	Ingen information behöver bevaras. Förs ej över till e-arkiv.	*Om något ska arkiveras kan stadsarkivet behöva kontaktas. Man kan behöva ställa krav så att det går att föra över information digitalt till ett e-arkiv.*

	Vilka informationen ska delas med internt och hur det ska ske	Data delas bara mellan elev och klassrum i realtid.	*Internt: Ska de skickas till någon? Vilka behöver ha behörighet?* *Exempel:* *Informationen förs över till Ekonomiavdelningen via integration med ekonomisystemetx, Informationen lämnas på papper till...*
	Behörighetshantering **Vilka nivåer på behörigheter som behöver finnas.** **Hur ska inloggning ska ske.**	Administratör på utvecklingsenheten får information från rektor/klasslärare om att behov finns för elev att använda AV1 robot. Administratör hanterar skriftlig överenskommelse mellan elev/vh och skola om villkoren för användning. Inloggning sker via unik kod som kopplar elevens app till roboten. Om försök till skärmavbild eller inspelning görs annulleras kopplingen mellan enheten och elevens enhet, och en ny koppling måste göras. Elevens identitet säkerställs vid koppling av enhet till robot samt vid inloggning av elev på enhet som är kopplad till robot.	*Red ut vilka inom organisationen som måste få tillgång till personuppgifterna antingen via behörigheter i systemet eller på annat sätt.* *Titta på hur behörighetsstrukturen behöver se ut så att varje roll bara få tillgång till det den behöver för att utföra sitt arbete.* *Om fler än en nämnd ska använda sett system kan det behöva vara möjligt att skapa parallella organisationer i systemet.* *Ska inloggning ske med anv-ID och lösen eller krävs stark autentisering och i så fall vilken sort?*
	Vilka informationen ska delas med externt och hur det ska ske	Delas ej externt.	*Externt: Ska de skickas till någon, lämnas till myndighet eller ska någon extern ha behörighet, integrationer?* *Exempel:* *Beslut skickas per brev till brukare,* *Information redovisas via webbformulär till…*
	Exit. Hantering av behandlingen när/om avtalet med personuppgiftsbiträdet upphör	Behandlingen upphör. P2P-data överförs ändå inte. Om annat biträde anlitas för liknande behandling finns inga personuppgifter att överföra från biträdet till annat biträde.	*Ett avtal med ett biträde kan avslutas av olika skäl. Avtalstiden kan ta slut och man kan komma att upphandla annan leverantör, leverantören kan gå i konkurs, bli uppköpt, missköta sig, byta till olämpliga underbiträden mm. PUA behöver därför redan under planeringen ha klart för sig vad som ska hända i dessa fall så att de inta förlorar kontrollen över personuppgifterna.*
Konsulteringsprocess	**Frågeställning**	**Beskrivning**	

Konsultering av relevanta intressenter	**Beskriv när och hur ni ska samla in synpunkter från de registrerade eller deras företrädare, eller motivera varför det inte är lämpligt.**	De registrerades företrädare har inte i förväg erbjudits möjligheter att reflektera över idén med en AV1-robot eftersom vi erbjudits att använda den för ett pilotprojekt. Pilotprojektet förutsätter dock en omfattande involveringsprocess. Denna involveringsprocess gäller även om beslut tas om ett bredare införande av AV1 Robot. En involveringsprocess sker i flera led och följer AV1-projektets arbetsprocess: - Rektor gör en intresseanmälan till utvecklingsenheten via formulär. - Utvecklingsenheten gör urval utifrån olika kriterier t.ex.: Prioriterad skola, skola med hög skolfrånvaro, situation i klass m.m., återkoppling sker till rektor med beslut. - Möte sker med rektor och skolteam för kartläggning kring elev och elevens situation. Om beslut att elev/familj och skola är aktuell fortsätter man till nästa steg. - Kontakt sker med hemmet. Skolans kontaktperson kontaktar hemmet för att ge relevant information. Om intresse finns från elev och vårdnadshavare bokas ett hembesök där kontaktperson tar med AV1 Robot samt elevens schema. - Om elev och vårdnadshavare tackar ja informeras klassen och övriga barns vårdnadshavare om intentionen att använda roboten med hjälp av introduktionsmaterial. Förankring kan ske på ett flertal sätt: genom individuella dialoger, på föräldramöte, på klassråd/klassmöte etc. Bedömning om detta tillvägagångssätt görs av rektor beroende på klassens unika förutsättningar. - Kontaktpersonen finns som stöd i hemmet vid första uppstart av verktyget. - Kontaktpersonen har kontinuerlig kontakt med elev och vårdnadshavare samt mentor/specialpedagog/speciallärare. - Utvärdering sker med berörda intressenter efter ett projekt med AV1: elev, mentor/klasslärare, klasskamrater, vårdnadshavare, kontaktperson och rektor bereds möjlighet att utvärdera via enkät. - Under hela projektet finns coachande stöd till skolan från utvecklingsenheten.	*Att involvera de registrerade är ett viktigt led enligt dataskyddsförordningen. Om det inte är lämpligt behöver det motiveras. Fundera ordentligt över möjligheten.*
	Roller från organisationen som behöver vara involverade (exempelvis fackliga representanter, HR) Behöver ni be personuppgiftsbiträden om hjälp? Planerar ni att konsultera säkerhetsexperter, jurister olika kategorier av personer i verksamheten eller andra experter?	Dialog med DSS och utvecklingschef. Nämnd kommer att fatta beslut om behandlingen, därmed lyfts den också till facklig samverkan inför beslut. Dialog har förts med IT-avdelning om tekniska förutsättningar. IT-säkerhetsansvarig har tillfrågats om krypteringens styrka och adekvans. Dataskyddsombud granskar konsekvensbedömning.	*Vilka intressenter har varit med och behöver fler konsuteras. Deltagare från verksamheten med goda kunskaper av processen, de interna arbetssätten och gällande lagkrav.Dataskyddsombud / It / Dataskyddssamordnare / Informationssäkerhetsarkitekt / externa.* *Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter (artikel 38) och rådfråga dataskyddsombudet vid genomförande av en konsekvensbedömning avseende dataskydd (artikel 35).*
Nödvändighet och proportionalitet	**Frågeställning**	**Beskrivning**	
Rättslig grund	**Rättslig grund grund för behandlingen enligt art 6**	1 e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.	*Samtycke* *Avtal* *Rättslig förpliktelse* *Grundläggande intresse* *Uppgift av allmänt intresse eller Myndighetsutövning* *(Det kan vara flera om flera behandlingar ingår i konsekvensbedömningen)*
	Om känsliga personuppgifter behandlas behöver stöd finnas i art 9.	2 g) Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.	*Ange var i artikel 9 stödet finns.*

	Den rättsliga grunden i lag eller författning eller beslut utifrån lag eller författning?	7 kap. 3 § Skollagen: Enligt 2 kap. 18 § första stycket regeringsformen har alla barn som omfattas av den allmänna skolplikten rätt till kostnadsfri grundläggande utbildning i allmän skola. 7 kap 22 § Skollagen: Huvudmannen ska se till att eleverna i huvudmannens förskoleklass, grundskola och anpassad grundskola fullgör sin skolgång.	*Ju känsligare och mer skyddsvärda uppgifter det det gäller desto viktigare är det att visa var stödet finns för behandlingen. T ex vilken lag och paragraf. Om ni har flera rättsliga grunder behöver samtliga uppges.*
Beskriv mått för efterlevnad	**Leder behandlingen till att syftet uppfylls?**	Syftet uppfylls genom att en möjlighet för elever med sjukdom eller problematisk frånvaro får en bättre kontakt med sin klass och skola. Eleven kan vara med fast eleven inte klarar/kan medverka fysiskt på plats. För hemmasittarproblematik har behandlingen visat sig innebära ett närmande till skolan.	*Hur uppfylls syftet? Bättre / Snabbare / Effektivare / Billigare / Annat*
	Hur man kommer att se till att uppgifterna endast behandlas för ändamålet de samlades in för	Rutiner för användning. Information till användare. Information till vårdnadshavare och elev om villkor för användning. PuB-avtal med biträdet.	*Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamå och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.* *Hur kommer ni att göra för att säkerställa att personuppgifterna inte kommer att behandlas för andra ändamål?* *Exempel:* *PUB-avtal med eventuella biträden, Rutiner för användning, Utbildning av användare*
	Hur uppgiftsminimering säkerställs	Tekniken möjliggör kryptering av den data som sänds mellan elev och klassrum. Elev har kontroll över graden av medverkan. Vid försök till filmning eller skärmavbildning stängs anslutningen av och elev behöver kvittera ut ny anslutningskod från administratör för att åter ha åtkomst till roboten.	*Redogör för både tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna är adekvata, relevanta och inte för omfattande i förhållande till det specificerade ändamålet* *Exempel:* *Inte använda fritextfält,* *Endast data som krävs för ändamålet samlas in*
	Hur lagringsminimering säkerställs	Inga data utöver metadata samlas in av biträdet. Stream mellan klassrum och elev sparas ej.	*Redogör för tekniska och organisatoriska åtgärder för att säkerställs att personuppgifter endast lagras så länge de behövs.*
	Hur datans korrekthet säkerställs	Data överförs endast mellan en AV1-enhet vars mac-adress är knuten till kommunens nät och den enhet som kopplats till AV1-enheten med en kod. Eleven måste därutöver logga in i läsplatta för att komma åt applikationen.	*Exempel:* *Data hämtas från folkbokföringen för att säkerställa korrekthet.*
	Vad som görs för att se till att eventuella personuppgiftsbiträden rättar sig efter era beslut	PuB-avtal med tydliga instruktioner. Regelbunden uppföljning och dialog med leverantören.	*PUB-avtal med tydliga och detaljerade instruktioner, kravställan, revisioner.*
	Inbyggt dataskydd **De åtgärder som kommer att vidtas för att säkerställa att kravet på inbyggt dataskydd efterlevs**	Roboten är konstruerad för att inte samla in data utöver det som är nödvändigt. Kryptering av den ström som innehåller elevdata och medarbetardata. Rutiner och instruktioner för att tydliggöra användningsvillkor. Se krav på peer-to-peer-strömmen ovan.	*Hänsyn till kravet på inbyggt dataskydd måste tas under hela behandlingens livslängd, dvs under förstudie, kravställan, utveckling, användning, avveckling och bevarande.* *Åtgärderna behöver vara både tekniska och organisatoriska. Tekniska åtgärder kan vara pseudonymisering, kryptering, minimering av antalet personuppgifter och begränsning i tid. Organisatoriska åtgärder kan vara rutiner och instruktioner.*

	Dataskydd som standard **De åtgärder som kommer att vidtas för att säkerställa att kravet på dataskydd som standard efterlevs**	Användningen är minimerad genom att strömdata är krypterad Peer-to-peer med stark kryptering TLS 1.2 och 256bit AES, med SRTP med DTLS, KE, DTLS och inte lagras.	*Dataskydd som standard kan vara att man tillämpar inställningar i ett system så att det ger bästa skydd för personuppgifterna. Åtgärderna ska t ex leda till minsta möjliga behandling av personuppgifter, kortaste behandlingstiden, och att inte fler personer än nödvändigt kan komma åt dem.*
Överföring till tredje land	**Kommer överföring att ske till tredje land?** Dvs land utanför EU/EES	Ej för strömmande data peer-to-peer. AWS-molnströmning finns som ett möjligt alternativ men godkänns ej för elevdata. Överföring EU-USA sker för att lagra loggdata som inte är kopplad till de registrerade, samt för administrativa ärenden där medarbetares e-post och inloggningsinformation till tjänsten kan komma att förekomma, samt av tjänstens support.	*Obs att möjlighet till åtkomst från landet räknas som överföring. T ex om utvecklare eller support kan få åtkomst.* *Se beslut i KF 2021 om lagring av information i molntjänster. I första hand inom eruropeinska tjänster. Om sådan inte finns hanteras det enligt EDPB:s riktlijer. En överföringsanalys (Transfer Impact Assessment, TIA) behöver göras om överföring kan bli aktuellt till ett icke godkänt land. Det är en objektiv analys av landets lagar och dess påverkan i det aktuella fallet och riskerna för de registrerade. Det är i praktigen mycket svårt att göra detta så att det uppfyller dataskyddslagarna.*
	Länder som överföring kommer att ske till	USA, Storbritannien	*Ange land eller länder. Noggrann analys kan krävas för att fastställa länderna för vissa molntjänster då det kan finnas underbiträden och tredjepartstjänster som för över personuppgifter till flera länder. En komplett redovisning från biträdet behövs*
	Beskrivning av vad överföringen består av	Loggdata. Data som behövs för att tillhandahålla tjänsterna. E-posttjänster för support till kunds förfrågningar avseende tjänsterna. Administratörens e-postadress och inloggingsinformation (kan ej generera åtkomst till en enskild ström peer-to-peer på något sätt).	*Personuppgifter kan föras över/nås från tredje land på olika sätt och i olika situationer. Exempel:* *vid support, utveckling, lagring, lastbalansering, marknadsföring, diagnostiska data, telemetridata, säkerhetsdata, pga regulatoriska krav, vid internationella faderskapsutredningar mm.*
	Har EU-kommissionen fattat beslut om adekvat skyddsnivå för landet/länderna?	Ja, adekvansbeslut via EU-US Data Privacy Framework.	https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/adekvat-skyddsniva/

	Den överföringsmekanism (skyddsåtgärd) som kommer att användas för överföringen när beslut om adekvat skyddsnivå saknas.	Leverantörens information om att EU-US Data Privacy framework tillämpas. Innan dess har leverantören använt sig av standardavtalsklausuler: * To increase the stability and security of our infrastructure, the Processor uses certain services of companies (and respectively its parent company) that are either located in the USA, or who have engaged subprocessors who are located in the USA. This may result in the transfer of personal data to the USA. Such transfers are based on the adequacy decision of the European Commission (Art. 45 (1) GDPR) as the service provider is registered under the EU-US Data Privacy Framework (DPF). Even in the event that changes are made to this decision or the decision will be revoked, the transfer is secured and legitimated by contractual, technical and organizational measures according to Art. 44 et seqq. GDPR. Prior to the adequacy decision of July 10th 2023 establishing the EU-US Data Privacy Framework (DPF), No Isolation entered with every sub-processor into signed contracts according to current EU standards (EU SCC). All sub-processors have, regardless of the DPF and the SCCs, defined additional guarantees to minimize the impact of possible data transfer to US authorities, such as the utilization of the legal process in the case of inquiries. Other examples of measures and safeguards may be encryption and/or pseudonomysation of the personal data. Transfers to third countries outside the USA will otherwise be relevant in cases where the data processor in question uses data processors who process, transfer or store personal data in third countries. The legal basis for such transfers would be the EU Commission's Standard Privacy Agreements (SCCs), or an EU Adequacy Decision when applicable. Both No Isolation, the company’s data processors and their data processors in turn are bound by these clauses. In cases where our data processors transfer or store personal data in third countries that are not considered to provide an adequate level of protection, the standard agreements are supplemented by additional measures and guarantees that are intended to minimise the risk of a breach of privacy.	*Standardavtalsklausuler, särskilda fall enligt art 49, godkända uppförandekoder eller certifieringar, rättsligt bindande instrument mellan myndigheter*
	Överföringsanalys är gjord	Överföringsanalsy behöver inte göras.	*En överföringsanalys (Transfer Impact Assessment, TIA) behöver göras om överföring kan bli aktuellt till ett icke godkänt land. Det är en objektiv analys av landets lagar och dess påverkan i det aktuella fallet och riskerna för de registrerade samt framtagande av åtgärder för att avvärja riskerna. Se riktlijer från EDPB för genomförande. En överföringsanalys är i praktiken svår och tidskrävande att göra.*
	Indentifierade risker för de registrerade	De registrerades uppgifter, med undantag för namn och e-post för medarbetare som hanterar behandlingen, överförs ej till tredje land alls.	*Frågan ska besvaras utifrån GDPR:s principer avseende personuppgiftsbehandlingar, den enskildes rättigheter, dataskydd och informationssäkerhet enligt GDPR.*
	De extra skyddsåtgärder som kommer att användas	Informationsminimering. Inga data som kan identifiera de registrerade utöver administratör/medarbetare överförs via molntjänst med bas i USA.	*Vid överföring till tredje land behöver en överföringsanalys göras, om inte adekvansbeslut finns för landet. Då analyseras landets lagar och man tittar på om den grund man använder ger tillräckligt skydd eller om det krävs extra skyddsåtgärder. Beskriv skyddsåtgärderna om lämpligt. Exempel på åtgärder kan vara en tillräckligt hög nivå på krypering och att krypteringsnycklarna endast finns hos utsedda personer i kommunen, pseudonymisering mm. Ange inte sekretessuppgifter här utan hänvisa i så fall till bilaga.*

De registrerades rättigheter

Den registrerade, det vill säga den vars personuppgifter behandlas, har ett antal rättigheter enligt dataskyddsförordningen. Som personuppgiftsansvariga har ni ett ansvar för att ha rutiner på plats för att hantera begäranden om att utöva dessa rättigheter när någon begär det. Rättigheterna går inte alltid att tillämpa t ex pga lagar. Ange nedan om och hur rättigheterna kommer att säkerställas.

Rättighet		Hantering för behandlingen
Förfarande kring rättigheterna Enligt art 12 Allmänt förfarande som gäller samtliga rättigheter nedan.	Identifiering av den registrerade (ID)	Begäran avseende rättigheter i förordningen görs enligt kommunens rutin.
	Hur begäran besvaras, t ex kontaktkanal	Begäran avseende rättigheter i förordningen görs enligt kommunens rutin.
	Hur mottagarna informeras om rättelse, radering eller begränsning av uppgifter	Användare, elever och vårdnadshavare informeras inför användning. Användaren får särskild instruktion.
Rätt till information Enligt art 13-14 De registrerade har rätt till information när deras personuppgifter behandlas. De ska lämas av PUA senast vi insamlandet, både när uppgifterna kommer från den registrerade själv (art 13) och när de kommer från någon annan (art 14).	Är rättigheten tillämpbar på den aktuella behandlingen? Finns undantag från rätten till information?	Ja, de registrerade får information skriftligen och muntligen.
	Inhämtas personuppgifterna från den registrerade själv, från någon annan eller båda delar?	Inhämtas från båda delar.
	Hur informationen kommer att ges till de registrerade	Skriftligen till klasskamrater och vårdnadshavare, skriftligen och muntligen till användaren samt användarens vårdnadshavare.
Rätt till tillgång Enligt art 15 Kallas även registerutdrag. När den registterade efterfrågar information om vilka personuppgifter som behandlas och hur de behandlas ska information lämnas till den registrerade enligt art 15.	Är rättigheten tillämpbar på den aktuella behandlingen?	Ja.
	Från vilka källor uppgifterna sammanställs	Från administratörs register över användare.
	Hur uppgifterna skickas till de registrerade	Per rekommenderad post eller utlämning i reception i Värjan.
	Finns det några begränsningar i lag för utlämnande av uppgifterna? T ex enligt om uppgifterna har sekretess gentemot den registrerade själv enligt OSL?	Nej.

	Finns det möjlighet att enkelt hitta information relaterad till en individ och finns det möjlighet att ta ut registerutdrag? Beskriv. Krav kan behöva ställas vid anskaffning.	Ja, eftersom det handlar om ett fåtal administreras detta manuellt.
Rätt till rättelse Enligt art 16. Den registrerade har rätt att vända sig till PUA och be att få felaktiga uppgifter rättade. Den registrerade har även rätt att komplettera med sådana personuppgifter som saknas och som är relevanta för ändamålet behandlingen**.**	Är rättigheten tillämpbar på den aktuella behandlingen?	Nej, eftersom uppgifterna strömmas i realtid och inte kan rättas. Tekniska data kan inte heller rättas.
	Hur en begäran om rättelse hanteras	
	Hur man går tillväga när det finns meningsskiljaktigheter kring rättelser	
	Finns det möjlighet att enkelt hitta information relaterad till en individ och finns det möjlighet att rätta, om tillämpbart? Beskriv. Krav kan behöva ställas vid anskaffning.	
Rätt till radering Enligt art 17. Ni behöver veta vad som kan raderas. Den registrerade har rätt att vända sig till PUA och be om att få sina personuppgifter raderade vilket är möjligt i vissa fall. Om uppgifter raderas på den registrerades begäran måste PUA även informera dem som de har lämnat ut uppgifter till. Det gäller dock inte om det skulle visa sig omöjligt eller innebär en alltför betungande insats.	Är rättigheten tillämpbar på den aktuella behandlingen?	Nej, inget sparas.
	Hur en begäran om radering hanteras	Den registrerade ges besked att inget sparas.
	Finns det möjlighet att enkelt hitta information relaterad till en individ och finns det möjlighet att radera, om tillämpbart? Beskriv. Krav kan behöva ställas vid anskaffning.	Nej.
Rätt till begränsning av behandling Enligt art 18. Med begränsning menas att uppgifterna	Är rättigheten tillämpbar på den aktuella behandlingen?	Nej, behandlingen är redan begränsad. Går att avstå från behandlingen.

Med begränsning menas att uppgifterna markeras så att de i framtiden endast får behandlas för vissa avgränsade syften. Rätten gäller bland annat när den registrerade anser att uppgifterna är felaktiga och har begärt rättelse. Den registrerade kan då även begära att behandlingen av uppgifterna begränsas under tiden uppgifternas korrekthet utreds. När begränsningen upphör ska ni som personuppgiftsansvariga informera den registrerade om detta.	Hur beränsning av behandling utförs i praktiken	
	Tekniska metoder för att säkerställa begränsningen av behandlingen	
	Hur den registrerade informeras om att begränsningen lyfts	
Anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling Enligt art 19. PUA ska underrätta varje mottagare som personuppgifterna har lämnats ut till om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som skett i enlighet med artiklarna 16, 17.1 och 18, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. PUA ska informera den registrerade om dessa mottagare på den registrerades begäran.	Är rättigheten tillämpbar på den aktuella behandlingen?	Nej.
	Mottagare som ska informeras	
	Hur mottagare ska informeras	
Rätt till dataportabilitet Enligt art 20. Den registrerade har i rätt att få ut och använda sina personuppgifter på annat håll. PUA är skyldiga att underlätta en sådan överflyttning av personuppgifter. En förutsättning är att PUA behandlar personuppgifterna med stöd av ett samtycke från den registrerade eller för att uppfylla ett	Är rättigheten tillämpbar på den aktuella behandlingen?	Nej, inget sparas.
	Hur rätten till dataportabilitet genomförs i praktiken	

från den registrerade eller för att uppfylla ett avtal. Det gäller bara sådana personuppgifter som den registrerade själv har lämnat.	Tekniska förutsättningar för överföring och mottagande av uppgifter	
Rätt att göra invändningar Enligt art 21. Den registrerade har rätt att invända mot PUA:s behandling av hans eller hennes personuppgifter. Rätten att invända gäller när personuppgifter behandlas för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning. Om den registrerade invänder mot behandlingen i sådana fall får PUA endast fortsätta att behandla uppgifterna om det går att visa att det finns avgörande berättigade skäl till att uppgifterna måste behandlas som väger tyngre än den registrerades intressen, rättigheter och friheter eller om behandlingen sker för att fastställa, utöva eller försvara rättsliga anspråk.	Är rättigheten tillämpbar på den aktuella behandlingen?	Ja, den registrerade har rätt att göra sådan begäran.
	Hur rätten att göra invändningar ska genomföras	Enligt rutin för registerutdrag/begäran enligt GDPR.
Rätt att slippa automatiserat beslutsfattande, inbegripet profilering Enligt art 22. Automatiserat beslutsfattande innebär att ett system fattar beslutet utan inblandning av en människa. Automatiserat beslutsfattande kan vara tillåtet om det är nödvändigt för att ingå eller fullgöra ett avtal mellan den registrerade och den personuppgiftsansvariga eller om den registrerade har gett sitt uttryckliga samtycke. Det kan även vara tillåtet enligt särskild	Ingår automatiserat beslutsfattande och profilering i behandlingen?	Nej.
	Grunder för automatiserat beslutsfattande	
	Skyddsåtgärder som aka användas (t ex att person deltar, bestridande av beslut mm)	
	Hur det säkerställs att dataskyddspårinciperna följs i samband med automatiserat beslutsfattande	

Det kan även vara tillåtet enligt särskild lagstiftning. Idag stöds det inte av kommunallagen.	Hur den registrerade informeras om att de är föremål för automatiserat beslutsfattande	

Kriterier vid konsekvensbedömning

Sannolikhet	
Mycket hög sannolikhet	Risken kommer att inträffa dagligen om inga speciella åtgärder vidtas
Hög sannolikhet	Risken uppstår varje månad om inga särskilda åtgärder vidtas omedelbart
Låg sannolikhet	Risken kan inträffa årligen om inga särskilda åtgärder vidtas
Osannolik	Det är osannolikt att denna risk kommer att inträffa en gång var 1-3 år

Instruktion

1. Bedöm hur sannolikt det är att händelsen uppstår
2. Bedöm hur allvarlig konsekvensen kan vara för den registrerade. Utgå från den allvarligaste konsekvensen.

Ta med i beräkningen vilken kategori av registrerad det gäller, om det finns lagar som avgör allvarlighetsgrad. Ha en samlad bild av vad situationen inbegriper. Det är t ex allvarligare om uppgifter om en brukare inom socialtjänsten kommer i orätta händer än om det gäller någon som inte är sårbar och inte omfattas av sekretess.

Sannolikhet och konsekvens följs inte åt. Det kan vara 1 på den ena och 4 på den andra.
Även om åtgärd i normalfallet inte anses krävas om det blir grönt behöver man göra en värdering av om det ändå behövs. Risk som innebär att dataskyddsförordningen inte efterlevs accepteras inte.

Oavsett nivå på risk måste dataskyddslagarna efterlevas.

Låg risk	Ej krav på åtgärd, riskvärdet är acceptabelt, förutsatt att dataskyddsförordningen efterlevs. Bedömning görs dock i varje enskilt fall om åtgärd ändå bör vidtas.
Medelhög risk	Åtgärder tas fram och risken bevakas, riskvärdet får ej stiga.
Hög risk	Kan ej accepteras. Skall åtgärdas och värdet sänkas. Förhandssamråd från tillsynsmyndigheten kan övervägas.

Försumbar konsekvens	**Måttlig konsekvens**	**Betydande konsekvens**	**Allvarlig konsekvens**
- Låg eller ingen påverkan på den registrerades integritet - Den registrerade har inga svårigheter att utöva sina fri- och rättigheter - Ingen eller endast försumbar ekonomisk eller social påverkan - Juridiskt lagligt Individen kommer inte beröras eller kommer endast få mindre besvär som de kan hantera med relativt små åtgärder. Till exempel: individen får lägga tid på att fylla i sina uppgifter igen, irritation ect	- Den registrerades fri- och rättigheter kan inte garanteras - Den registrerade uppleva lindriga besvär - Måttlig ekonomisk eller social påverkan - Oklart juridiskt läge / utredning krävs Individen kan få större, men överkomliga, besvär Till exempel: extra kostnader, rädsla, stress och oförstående, mindre fysiska krämpor	- Den registrerade hindras utöva kontroll över sina personuppgifter - Trolig risk för ekonomisk eller social påverkan hos den registrerade om åtgärder inte vidtas - Oklart juridiskt läge/praxis saknas Individen kan få större konsekvenser, som bör vara överkomliga men med betydande ansträngning. Till exempel: betalningsanmärkningar, förlust av jobb, rättsliga följder och lagbrott, fel information till myndigheter, risk för försämrad hälsa	- Skapar stora besvär för den registrerade genom exempelvis diskriminering, identitetsstöld eller integritetsbedrägeri - Stor ekonomisk förlust - Skadat anseende eller annan betydande ekonomiskt eller social nackdel - Kan även innebära fara för liv och hälsa - Olagligt Individen kan få betydande och oåterkalleliga konsekvenser Till exempel: ekonomisk skuld, långsiktiga psykiska och fysiska problem, död

Konsekvens

Exempel på konsekvenser för den registrerade.
- Den registrerade förlorar kontrollen över de egna personuppgifterna - Begränsning av rättigheter - Diskriminering - Identitetsstöld - Bedrägeri - Ekonomisk förlust - Obehörigt hävande av pseudunymisering - Skadat anseende - Förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt - Annan ekonomisk nackdel - Annan social nackdel - Förlust av hälsa - Förlust av liv

Konsekvensbedömning

Identifiera alla risker för personer och deras integritet som ni kan komma på. Tänk inte på om de är sannolika eller inte. Det tar ni ställning till senare. Klumpa inte ihop liknande risker på en rad utan separera dem, dels för att visa att ni förstår skillnaden mellan dem och dels för att de inte sällan har olika värden för risk och/eller konsekvens samt att det kan krävas olika åtgärder.

Ta även med sådana risker som ni redan har koll på, annars kan ni inte visa att ni har hanterat dem och uppfyller därmed inte ansvarsskyldigheten i artikel 5. Risker tas fram utifrån att inga åtgärder har vidtagits. Om åtgärder har vidtagits skrivs de in under Nuvarande åtgärd.

På fliken Kriterier finner ni stöd vid genomförandet av bedömningen.

Identifiera risk			Konsekvens	Värdera risk				Åtgärder				
Riskområde Inom vilket område finns risken? Se exempel s 8 i Information om konsekvensbedömningar och förhandssamråd. T ex: Bristande teknisk säkerhet, Bristande organisatorisk säkerhet, Överföring till tredjeland (Överföringsanalys behöver göras om landet inte är ett godkänt land), Externa intrång, Interna intrång, Juridiska risker, Inlåsningseffekter, Registrerades rättigheter, Personuppgiftsbiträden. **Beskrivning av risk** Beskriv en händelse eller företeelse som kan leda till risk för den registrerade. Tänk inte på sannolikheten när risker identifieras. Ta med allt ni kommer på. Risker tas fram utifrån att inga åtgärder har vidtagits. **Tips:** 5-10 minuters enskild brainstorming kan vara ett bra sätt att börja ta fram risker.			**Exempel på konsekvenser:** Den registrerade förlorar kontrollen över de egna personuppgifterna, Begränsning av rättigheter, Diskriminering, Identitetsstöld eller bedrägeri, Ekonomisk förlust, Obehörigt hävande av pseudunymisering, Skadat anseende, Förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, Annan ekonomisk nackdel, Annan social nackdel, Förlust av hälsa, Förlust av liv Konsekvenser tas fram utifrån att inga åtgärder har vidtagits.	**Konse-kvens (1-4)**	**Sannolik-het (1-4)**	**Risk-värde** Beräknas auto-matiskt	**Motivera värdena för Sannolikhet och Konsekvens** Riskvärdet kan visa att ingen åtgärd krävs, men bedöm om det är rimligt. Åtgärder kan ändå vara lämpliga att vidta.	**Vilka åtgärder finns idag** Tekniska och organisatoriska skyddsåtgärder. Om åtgärder redan har vidtagits uppge dem här. Exempel på åtgärder: Skriftlig rutin Pseudonymisering Ltark autentisering Kryptering (vilken nivå krävs?) Utbilda personal PUB-avtal, instruktion till biträde Behörighetsstyrning Brandvägg Loggning mm	**Vilka åtgärder planerar ni att vidta för att minska risken för de registrerade** Tekniska och organisatoriska skyddsåtgärder. Exempel på åtgärder: Skriftlig rutin Pseudonymisering Ltark autentisering Kryptering (vilken nivå krävs?) Utbilda personal PUB-avtal, instruktion till biträde Behörighetsstyrning Brandvägg Loggning mm	**Kommentar av bedömning av återstående överenskommet riskvärde** Hur ser risk och konsekvens ut efter vidtagna åtgärder?	**Nästa steg** **Hantera risk genom att:** - Acceptera - Minska, fler åtgärder - Överföra - Undvika - Förhandssamråd med IMY Obs att risk som innebär att man bryter mot dataskyddsförordningen Inte accepteras.	**Riskägare** Ansvarig person och roll. Även tidpunkt för när det ska vara klart kan anges.
Risk-ID	**Riskområde**	**Beskrivning av Risk**	**Konsekvens för den registrerade**	**Konse-kvens**	**Sanno-likhet**	**Riskvärde**	**Kommentar Riskvärde**	**Nuvarande åtgärd**	**Åtgärd**	**Kommentar återstående riskvärde**	**Hantering/riskåtgärd**	**Ansvarig**
1	**Risker hos biträdet**	Risk för att (obehörig) personal tar del av personuppgifterna	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, förlust av konfidentialitet, annan social nackdel.	2	1	8	Risken är låg eftersom få medarbetare har tillgång till de personuppgifter som behandlas och ingen har tillgång till livesträmmad data förutom elev och klassrum.		Regler och rutiner, utbildning av personal, säkerhetsfunktioner, kryptering			
2		Risk för att biträdet behandlar personuppgifterna för egna ändamål	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, annan social nackdel.	2	1	8	Biträdet har ingen möjlighet till åtkomst till uppgifterna rörande elev och klass. Biträdet har ej åtkomst till strömmen då den är P2P.		PUB-avtal, instruktion			
3		Risk för att biträdet gör personuppgifterna tillgängliga för icke godkända personuppgiftsbiträden	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, förlust av konfidentialitet, annan social nackdel.	2	1	8	Biträdet har ingen möjlighet till åtkomst till uppgifterna rörande elev och klass. Biträdet har ej åtkomst till strömmen då den är P2P.		PUB-avtal, instruktion, kryptering			
4		Risk för okända underbiträden pga att biträdet inte redovisar eller inte förstår vad som räknas som underbiträden	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, förlust av konfidentialitet, annan social nackdel.	2	1	8	Biträdet redogör noga för alla aspekter som efterfrågas. Biträdet bedöms ha kunskap kring underbiträden och hanteringen av data. Underbiträden har inte heller åtkomst till elevdata.		PuB-avtal, instruktion, biträdesbilaga			
5		~~Risk för att biträdet använder eget personuppgiftsbiträdesavtal som inte gör det möjligt att efterleva dataskyddslagarna~~				0	Kommunens avtal används.		PuB-avtal, instruktion, biträdesbilaga			
6		Risk för att tjänsten har långa nertider t ex pga problem eller långa/frekventa servicefönster	Skadat anseende, annan social nackdel.	2	1	8	Eleven får inte tillgång till undervisningen.		PuB-avtal, instruktion			
7		Risk för att personuppgifterna kommer i orätta händer pga för låg nivå på inloggningen för biträdets personal	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, förlust av konfidentialitet, annan social nackdel.	3	1	16	Biträdet har ingen möjlighet till åtkomst till uppgifterna rörande elev och klass. Biträdet har ej åtkomst till strömmen då den är P2P.		Rutiner, peer-to-peer-ström med stark kryptering, sessionsgenererade nycklar och SRTP med DTLS som bryts om någon annan ansluter till strömmen.			
8		Risk för att systemet blir onåbart i samband med konkurs	Skadat anseende, annan social nackdel.	2	1	8	Eleven får inte tillgång till undervisningen.		Acceptera risken och söka annan lösning.			
9		Inspelningar av läraren eller andra elever i klassen som publiceras på nätet. Foton/videor på studenter och lärare delas online utan samtycke.	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, förlust av konfidentialitet, annan social nackdel.	3	1	16	Tydliga regler och rutiner finns. Säkerhetsfunktioner finns som hindrar skärmavbildning och inspelning.		Regler och rutiner, säkerhetsfunktioner.			

10		Användaren ser eller hör saker via AV1 som den inte borde ha hört eller sett.	AV1-användaren hör ett privat samtal eller är påkopplad på opassande platser (t.ex. i lärarrummet).	3	1	16	Roboten signalerar tydligt när den är aktiverad. Regler och rutiner för användning finns.		Användningsregler och rutiner för roboten. Arbete för trygghet och mot kränkningar. Utbildning av medarbetare. Överenskommelse med elev och vårdnadshavare. Information till elev och vårdnadshavare. Säkerhetsfunktioner.			
11		AV1-användaren blir mobbad av andra på skolan.	Andra elever kan säga sårande saker som användaren kan höra.	3	1	16	Arbete för trygghet och mot kränkningar gäller på samma sätt med AV1.		Användningsregler och rutiner för roboten. Arbete för trygghet och mot kränkningar. En faktor i bedömningen kring vilka elever AV1-roboten lämpar sig för.			
12		Klassen hör någonting från hemmet eller från sjukhuset som de inte borde ha hört.	Barnen i klassen eller läraren hör ett läkarsamtal eller ett privat samtal mellan föräldrar och barn.	3	2	32	Arbete för trygghet och mot kränkningar gäller på samma sätt med AV1. Medarbetare stänger av roboten enligt rutin.		Användningsregler och rutiner för roboten. Arbete för trygghet och mot kränkningar. Utbildning av medarbetare. Överenskommelse med elev och vårdnadshavare. Information till elev och vårdnadshavare.	Med dessa åtgärder reduceras sannolikheten från nivå 2 till nivå 1.		
13		AV1 används av någon annan än den dedikerade användaren, eller andra befinner sig i rummet och lyssnar.	Föräldrar, syskon, kompisar eller någon annan loggar in på AV1-appen och klassen känner inte denna person.	3	1	16	Användningsregler och rutiner för roboten. Arbete för trygghet och mot kränkningar. Överenskommelse om användning.		Användningsregler och rutiner för roboten. Arbete för trygghet och mot kränkningar. Överenskommelse med elev och vårdnadshavare. Information till elev och vårdnadshavare. Stöd av utvecklingsenheten vid införande hos elev.			
14						0						
15						0						
16						0						
17	**Externa risker**	Risk för att behandlingen görs oåtkomlig av hackare	Skadat anseende, annan social nackdel.	2	1	8	Livesträmmen bryts. Eleven får ej tillgång till undervisningen.		Ingen åtgärd förutom att strömmen bryts. Undervisning återupptas när risken avvärjts.			
18		Risk för att personuppgifterna stjäls av hackare	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, förlust av konfidentialitet, annan social nackdel.	3	1	16	Strömmen är P2P med kryptering och därför är risken liten. Biträdet har inte tillgång till elevernas uppgifter.		Elevens personuppgifter skyddas av MAC-koppling av roboten till kommunens nät och elevens enhet kopplas med säkerhetskod och elevens inloggning till den egna enheten.			
19		Risk för att systemet utsätts för en överbelastningsattack	Skadat anseende, annan social nackdel.	2	1	8	Livesträmmen bryts. Eleven får ej tillgång till undervisningen.		Ingen åtgärd förutom att strömmen bryts. Undervisning återupptas när			
20		AV1s krypterade live-sändning hackas av externa personer.	Live-sändningen ses eller spelas in av en annan enhet utan att klassen eller läraren är medvetna om det.	3	1	16	Strömmen är P2P med kryptering och därför är risken liten. Robotens MAC-adress kopplas till kommunens nät.		Tekniska säkerhetsfunktioner.			
21						0						
22						0						
23						0						
24						0						
25						0						
26						0						
27	**Interna risker**	Obehörig personal får åtkomst till personuppgifterna	Skadat anseende, annan social nackdel.	2	1	8	Administratör har inte heller åtkomst till annat än vem som har enheten. Ingen åtkomst till livesträmmen.		Tekniska säkerhetsfunktioner.			
28		Risk för att personal registrerar fler personuppgifter än nödvändigt för ändamålet	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, annan social nackdel.	2	1	8	Tydliga regler och rutiner finns.		Regler och rutiner följs.			
29		Risk för att personal kan få åtkomst till personuppgifterna utanför arbetstid	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, annan social nackdel.	2	1	8	Tydliga regler och rutiner finns. Uppgifter förvaras på enhet. Livestrøm går ej att komma åt av administratör.		Uppgifter förvaras fysiskt på enhet i låst skåp. Fysisk säkerhet samt att regler och rutiner följs.			
30		Informationen blir inte komplett pga av att personal inte använder systemet i den utsträckning de förväntas, orsakat av osäkerhet/bristande kunskaper/svåranvänt system	Skadat anseende, annan social nackdel.	2	1	8	Tydliga regler och rutiner finns. Användningen är optimerad för att vara enkel. Lathundar och rutiner finns.		Den bedömning som föregår användning av en enhet säkerställer också att användningen sker korrekt.			

31		Uppgifterna i sytemet är inte korrekta	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, annan social nackdel.	2	1	8	Osannolikt då omfattningen inte är ett större antal. Liveström kan stängas av från båda håll.		Få uppgifter behandlas i systemet. Regler och rutiner följs och tekniska säkerhetsfunktioner säkerställer korrekthet.			
32		Enheten lämnas över till obehörig person.	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, annan social nackdel.	2	1	8	Osannolikt då omfattningen inte är ett större antal. Liveström kan stängas av från båda håll.		Rutiner och regler följs. Strömmen stängs av om felaktig hantering sker/om enheten blir stulen. MAC-adressen spärras i kommunens nät om så krävs.			
33						0						
34						0						
35						0						
36						0						
37	**Tekniska risker**	Risk för att tjänsten har långa nertider t ex pga tekniska problem	Skadat anseende, annan social nackdel.	2	1	8	Eleven får inte tillgång till undervisningen.		Ingen åtgärd förutom att strömmen bryts. Undervisning återupptas när risken avvärjts. Annan lösning övervägs.			
38						0						
39						0						
40						0						
41						0						
42						0						
43						0						
44						0						
45						0						
46						0						
47	**Juridiska risker**	Risk för att biträdet för över elevens personuppgifter till tredje land	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, annan social nackdel.	3	1	16	Strömmen är P2P och går ej över tredjeland.		Strömmen är P2P och tillåts ej gå via tredje land. Krypterad.			
48		Risk för att biträdet för över medarbetarnas personuppgifter till tredje land.	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter.	2	4	40	Uppgifter som behandlas är minimerade till namn, e-postadress, inloggning avseende medarbetare. Ingen överföring av elevdata genom starkt krypterad peer-to-peer liveström sker via tredje land.		Behandlingen sker med stöd av EU-US Privacy framework och med exitstrategi till standardavtalsklausuler om rättsläget skulle förändras.	Med denna åtgärd reduceras sannolikheten för otillåten behandling i tredje land från 4 till 1.		
49		Risk för att personuppgifterna förs över till tredje land pga att biträdet inte redovisar eller inte förstår vad som räknas som överföring till tredje land	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, förlust av konfidentialitet, annan social nackdel.	3	1	16	Biträdet redogör noga för alla aspekter som efterfrågas. Biträdet bedöms ha kunskap kring underbiträden och hanteringen av data.	Biträdet har noga redovisat sina underbiträden.	Godkännande av underbiträden i bilaga till PuB-avtal.			
50		Personuppgifter som omfattas av sekretess röjs till obehöriga	Den registrerade förlorar kontroll över personuppgifterna, skadat anseende, begränsning av rättigheter, förlust av konfidentialitet, annan social nackdel.	3	1	16	Strömmen är P2P och går ej att åtkommas externt. Ett fåtal personers data behandlas av administratör.		Strömmen mellan elev och klassrum är P2P och tillåts ej gå via tredje land. Krypterad. Användningsregler och information till eleven samt vårdnadshavare.			
51						0						
52						0						
53						0						
54						0						
55						0						
56						0						

57	**Grundläggande rättigheter**					0							
58	Risk för negativ påverkan på yttrandefriheten	Nej.				0							
59	Risk för negativ påverkan på tankefriheten	Nej.				0							
60	Risk för negativ påverkan på den fria rörligheten	Nej.				0							
61	Risk för diskriminering	Risk för kränkande behandling finns i all skolverksamhet och ett lagstadgat ansvar finns att arbeta mot detta.				0							
62	Risk för negativ påverkan på rätten till frihet, samvete och religion	Nej.				0							

Proportionalitetsbedömning

Proportionalitetsbedömning
En proportionalitetsbedömning kan i vissa fall göras tidig men i andra fall behöver hela konsekvensbedömningen vara klar för att slutsater ska kunna dras. Det ska vara en analys där perspektivet är den registrerades integritet och skydd av personuppgifter och inte verksamhetens behov. Det är en objektiv bedömning där man sammanfattar konsekvensbedömningen för att bedöma lagligheten.

Analys ska göras om behandlingen är skälig, rimlig och proportionerlig. Man behöver analysera om behandlingen är lämplig att utföra på det tänkta sättet med utgångspunkt i ändamål, vilka personuppgifter som ska behandlas och vilka de registrerade är. Det kan t ex inte anses lämpligt att utföra en behandling på ett mer integritetskänsligt sätt än nödvändigt. Det kan innebära att gamla rutiner kan behöva fortsätta användas i stället för en digital behandling om den är mer integritetskänslig än vad som kan anses rimligt. Även om ni har identifierat rättsliga grunder ovan kan rättslig grund för behandlingen saknas om den utförs på ett sätt som är onödigt integritetskänsligt.

Bedömningen kräver mycket goda kunskaper om GDPR och om innebörden av frågeställningarna. Dataskyddsombudet bör bedöma efteråt om bedömningen är korrekt.

Förhandssamråd med IMY
Om en hög risk för de registrerades friheter och rättigheter fortfarande finns efter att man har gjort en konsekvensbedömning och den risken inte går att begränsa med framtagna åtgärder ska man samråda med Integritetsskyddsmyndigheten för att få råd om hur man ska göra. Hög risk kan uppstå i olika situationer som t ex tredjelandsöverföring, användande av ny teknik mm. Särskild blankett ska användas.
Förhandssamråd går inte att välja bort i de fall där det är obligatoriskt. Det måste vara klart innan behandlingen får påbörjas.
Dataskyddsombudet är behjälpligt med bedömning och samråd.

Proportionalitets-bedömning	**Är ändamålet för den planerade personuppgiftsbehandlingen berättigat och tillräckligt avgränsat?**	Ja, ändamålet är preciserat och avgränsat.

Är behandlingen nödvändig?	Ja, behandlingen är nödvändig för att möjliggöra skolgång och inkludering för vissa elever med sjukdom och frånvaroproblematik för att uppfylla kraven enligt skollag om skolplikt och rätten till utbildning enligt grundlag.
Går ändamålet att uppfylla på ett sätt som är mindre ingripande? Beskriv alternativen.	Nej. Åtgärden når elever som annars skulle bli utan vissa undervisningsmoment.
Är personuppgifterna som behandlas nödvändiga för ändamålet?	Ja, begränsning och avgränsning är gjord.
Finns rättslig grund?	Ja, allmänt intresse.
Håller den rättsliga grunden även när behandlingen utförs på det planerade sättet?	Ja.
Finns juridiska hinder för den planerade personuppgiftsbehandlingen?	Nej.
Finns det grund för överföringen av personuppgifter till tredje land, om sådan planeras?	Ej tillämpbart på överföringen peer-to-peer. Viss medarbetardata enligt redovisning kan komma att överföras till tredje land med stöd av EU-US Privacy framework och med extistrategi till standardavtalsklausuler om detta skulle ogiltigförklaras i domstol.

	Eliminerar eller minimerar de föreslagna skyddsåtgärderna identifierade risker som identifierats kopplat till den planerade personuppgiftsbehandlingen tillräckligt?	Ja.
	Uppfylls de grundläggande principerna i artikel 5?	Ja, laglighet, korrekthet, öppenhet, ändamålsbegränsning, uppgiftsminimering, integritet och konfidentialitet samt ansvarsskyldighet är uppfyllda.
	Återstår höga risker för de registrerades friheter och rättigheter? Vilka?	Nej.
	Slutsats: Är den planerade personuppgiftsbehandlingen adekvat och proportionerlig i relation till ändamålet och inte mer omfattande än nödvändigt, och är den laglig?	Ja, behandlingen är nödvändig för att möjliggöra skolgång för vissa elever med sjukdom och frånvaroproblematik för att uppfylla kraven enligt skollag om skolplikt och rätten till utbildning enligt grundlag. Detta gör den med vidtagna skyddsåtgärder proportionerlig till ändamålet, inte mer omfattande än ändamålet och laglig.
Förhandssamråd med IMY	**Behöver förhandssamråd med IMY göras?** Om hög risk kvarstår när åtgärder tagits fram är det lagkrav på att förhandssamråd med IMY ska göras (artikel 36). Förhandssamråd hanteras av DSO i samarbete med lämpliga roller.	Nej.

Dokumentation

Sammanfattning av konsekvensbedömningen

(Skriv en sammanfattninga av er bedömning och vad ni har kommit fram till)

Bedömningen har täckt in tekniska och administrativa aspekter av behandlingen. Sammanfattningsvis ser vi inga juridiska, tekniska och administrativa hinder för att påbörja behandlingen. Personuppgiftsansvarig, grundskolenämnden, kommer också att ta ställning innan PuB-avtal tecknas och behandlingen påbörjas.

Dataskyddssamordnarens bedömning

(Fylls endast i av dataskyddssamordnaren.)

Behandlingen kan påbörjas efter godkännande. Tillräckliga organisatoriska och tekniska säkerhetsåtgärder har vidtagits. Behandlingen är nödvändig för att tillgodose rätten till utbildning enligt grundlag och uppfyllandet av skolplikt enligt skollag för en mindre kategori elever med särskild problematik. Överföring sker med starkt kpypterad peer-to-peerström vars innehåll inte kan nås av obehörig eller No Isolation. Rutiner och riktlinjer finns. Material finns. Kompletteringar och förtydliganden har skett efter DSO:s initiala bedömning.

Överlämning

Dataskyddsombudet ska rådfrågas vid konsekvensbedömning, t ex om rättsliga krav, åtgärder som minskar risker och om behandlingen är tillåten och laglig utifrån dataskyddslagarna. Dataskyddsombudets synpunkter ska alltid ges tillbörlig vikt och om de inte följs dokumenteras orsaken.

DPIA överlämnad till dataskyddsombudet av: (Ange namn/sign och datum)

Per Silvervret Boberg, DSS, 2023-10-17; Kompletteringar enligt efterfrågan inlämnade av Per Silvervret Boberg, DSS, 2023-10-27.

Dataskyddsombudets bedömning och rekommendationer

(Fylls endast i av dataskyddsombudet. Bilaga kan vara aktuellt om kommentarerna är omfattande)

231020

Behandlingen har beskrivits till större delen väl. Det finns dock några saker som behöver förtydligas och hanteras innan min slutliga bedömning kan göras. Detta är en första bedömning.

Det beskrivs på ett ställe att t ex personalens e-postadress förs över till tredje land men på andra platser står det att ingen överföring sker. Detta blir motsägelsefullt. Om personuppgifter förs över, t ex genom att det finns åtkomst till uppgifterna så behöver det framgå. Dessa uppgifter finns inte med inom avgränsningen för bedömningen men det behöver de göra.

Kommer de att användas i samtliga årskurser i grundskolan? Förtydliga detta så att det blir tydligt vilket åldersspann det gäller.

När det gäller insamlande av synpunkter från registrerade så är detta en behandling där det bör göras. Här skulle det vara möjligt att ta in synpunkter från föräldrar till andra barn och förankra innan det är ett faktum. Finns det t ex någon föräldraorganisation, eller organisation för de äldre eleverna att samla in synpunkter från? Detta ser jag som ett fall där man inte bör avvika från kravet att samla in synpunkter innan. Det finns mycket att vinna på sådan förankring och minska risken för att det blir protester i samband med implementeringen och då också besvikna elever som får vänta på sin robot.

En sak som är svår ur ett integritetsperspektiv är att jag uppfattar det som att det inte finns stark autentisering och det blir svårt att få lagligt utan samtidigt som det är svårt att hantera när det gäller barn. När känsliga personuppgifter behandlas över öppna nät (Internet) krävs stark autentisering, eller minimum tvåfaktorsautentisering. Att styra vad som talas om lär inte vara möjligt. Utveckla beskrivningen kring detta så att det blir tydlig hur autentiseringen fungerar och ta fram risker kopplat till det.

I riskbedömningen är det lämpligt att ta upp fler risker som kan uppstå i elevernas hem, t ex risk för att vårdnadshavare, syskon med flera hör eller ser vad som sker på skärmen, risk för att någon tar kort t ex med en mobil. Barnen kan ha svårt att avvärja detta. Bilder kan spridas eller lagras i molntjänster kopplade till telefonen. Risker kopplade till vad kameran tar upp/upptagningsområdet bör hanteras. Hur viktigt är det att se klasskamraterna? Om det är viktigt beskriv och motivera. Kan klasskamraterna känna obehag över roboten och kameran? Hur har resonamanget gått kring det? Kameror är ett känsligt område där motivering krävs. De åtgärder som inte finns på plats bör flyttas till kolumnen Åtgärder och det finns också ett värde i att skriva in när de ska vara klara och vilken roll som ansvarar.

Barn har rätt till skolgång och delaktighet. När det gäller digitala lösningar för barn finns en del utmaningar och det behöver därför få ta sin tid att förbereda för ett införande. Det finns saker att titta vidare på och förtydliga samt finna lösning på. Risker behöver framgå tydligt och åtgärder behöver vara konkreta för att visa att de avvärjer risken. Därför är min rekommendation att arbetet med DPIA:n fortsätter.

231101 Slutlig bedömning för detta skede
Konsekvensbedömningen har nu till större delen kompletterats enligt tidigare rekommendation.

Dokumentationen av personuppgifter på fliken Beskrivning behöver dock fortfarande kompletteras.

Ni behöver säkerställa att ni har alla uppgifter som krävs om underbiträdena för att bedöma och ha dokumentation på deras behandling:
• Var de finns (adress och kontaktuppgifter)
• Var de behandlar personuppgifter (land och stad)
• Vad de gör (t ex support, utveckling, serverdrift)
• Vilka typer av personuppgifter de behandlar
• Behandlingstid
• Bevis på vilka skyddsåtgärder som har genomförts (så att PUA kan bedöma att personuppgifterna behandlas lagligt)

Vad gäller inloggningsförfarandet så finns en högre säkerhet än enbart en vanlig enkel inloggning. Skolan har inte en egen lag som talar om hur en inloggning ska fungera men GDPR styr och det behöver därför finnas en stark inloggning utifrån att känsliga uppgifter om barn kommer att behandlas. Det finns inga garantier för att denna typ av inloggningsförfarande bedöms tillräcklig vid en granskning av t ex IMY då den inte uppfyller kriterierna för en stark autentisering.

Barn har skolplikt och rätt till skolgång och delaktighet. En robot som ger denna möjlighet ser inte ut att ersätta en mindre integritetskänslig lösning. Risker har identifierats och åtgärder tagits fram. När det gäller digitala lösningar för barn finns en del utmaningar och det behöver därför få ta sin tid att förbereda för ett användandet av en ny digital tjänst och i det här fallet en IoT-produkt. Även om mycket arbete har gjorts inför en pilot med AV1 och det finns en hel del dokumentation så finns inte alla delar på plats. Det har t ex inte gjorts någon klassning av informationen och mer information om biträdenas behandling behöver komma på plats. Eskilstuna Kommun har idag en process där nya behov ska hanteras och även denna bör gå genom processen.

En konsekvensbedömning är ett levande dokument och ett verktyg som används fram till start av pilot/implementering och även fortsättningsvis vid behov eller t ex årligen.

Nästa steg

DPIA avslutad	
Samråd med [komplettera]	
Samråd med IMY	
Annat	231020: Gå igenom kommentarer i dokumentet och synpunkterna ovan. Komplettera och utveckla vissa delar innan slutgranskning. 231101: Det är lämpligt att konsultera någon angående att skicka behovet genom processen för anskaffning och göra de steg som ingår. Däribland klassning av informationen.

Bedömning genomförd av DSO:	Charlotte Nilsson, 2023-10-20 Charlotte Nilsson, 2023-11-01

DSO:s rekommendation godkändes av:	Ange namn/sign och datum

eller

DSO:s rekommendation godkändes inte av:	Ange namn/sign och datum

Motivera om DSO:s rekommendation inte följs

Andra intressenter

om andra intressenters synpunkter inte har beaktats dokumenteras detta nedan.

Andra intressenters synpunkter godkändes inte av:	Ange namn/sign och datum

Beskriv och motivera varför

Dokumentation av nästa steg

(Beskriv hur ni kommer att gå vidare i arbetet)

Nästa steg efter att DSO har lämnat rekommendation är nämndbeslut om konsekvensbedömning, behandling och tredjelandsöverföring av viss data om anställda.

Beslut om att gå vidare med behandlingen eller avsluta

Går vidare med behandlingen	Ange namn/sign och datum

eller

Går ej vidare med behandlingen	Ange namn/sign och datum

Beskriv och motivera varför

Förhandssamråd

Om en konsekvensbedömning visar att det kvarstår en hög risk för de registrerade finns en skyldighet att göra förhandssamråd med IMY, enligt dataskyddsförordningen art 36.

Förhandssamråd med IMY kommer att göras	Nej.

Om IMY begär komplettering för att kunna bedöma behandlingen behöver komplettering göras eller så avstår PUA från att påbörja behandlingen.

Ev anteckningar

Resultat av förhandssamråd med IMY

När förhandssamråd med IMY har gjorts måste organisationen följa deras rekommendation eller avstå från att påbörja behandlingen, annars blir den inte laglig. Att ändå fortsätta kan leda till t ex sanktionsavgifter.

Sammanfattning

Vad som beslutades utifrån förhandssamrådet

Kommentarer till DSO:s initiala bedömning 231020

Det stämmer att medarbetarens e-postadress överförs till tredje land. Detta har också förtydligats så att det tydligt framgår. Nämnden kommer föreslås godkänna denna tredjelandsöverföring som endast sker för info i klass 0 och 1.

Robotarna används i åk 4-9.

Synpunkter från registrerade kommer att samlas in innan införande i varje enskilt fall enligt beskrivning på den punkten.

Avseende stark autentisering så är kontrollen av tillgång till strömmen i vilket fall en tvåfaktorslösning, där kod specifikt tilldelas en enhet och elevens enhet kopplas ihop med AV1-enheten under överinseende från ansvanig administratör. Detta reducerar risken. Vi utvecklar beskrivningen kring detta.

Vi utvecklar riskerna enligt önskemål avseende risker i elevernas hem. Vi flyttar det som inte finns på plats till åtgärder.

Arbetet med DPIA:n fullgörs utifrån DSO:s rekommendationer.

Versioner och förändringar

Revisionshistorik

Författare	Version	Datum	Förändringshistorik

Förändringar i konsekvensbedömningen

Datum	Risk ID #	Namn, Titel	Kommentarer

Instruktioner för konsekvensbedömning

Alla personuppgiftsbehandlingar måste leva upp till dataskyddsförordningen och dess grundläggande principer i artikel 5. De innebär bland annat att personuppgiftsansvariga:

* måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter
* bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål
* inte ska behandla fler personuppgifter än vad som behövs för ändamålen
* ska se till att personuppgifterna är riktiga
* ska radera personuppgifterna när de inte längre behövs
* ska skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs
* ska kunna visa att de lever upp till dataskyddsförordningen och hur det görs, genom dokumentation.

Ett led i detta är att göra en konsekvensbedömning om behandlingen innebär en hög risk för de registrerade.

Vad är en konsekvensbedömning?

Konsekvensbedömningen är ett verktyg för att hantera dataskyddslagarnas krav på den aktuella behandlingen.

Konsekvensbedömningen är en process för att:
* ta reda på vilka risker som finns med en personuppgiftsbehandling
* ta fram rutiner och åtgärder för att bemöta dessa risker
* visa att man uppfyller dataskyddsförordningens krav

En konsekvensbedömning är en pågående process som påbörjas tidigt inför en ny eller ändrad behandling eller organisationsförändring och ska vara klar innan behandlingen påbörjas men den behöver också vara ett levande dokument och omprövas samt vid behov uppdateras kontinuerligt även under pågående behandling.

Det är viktigt att konsekvensbedömningen är tillräckligt omfattande och grundligt gjord så att den fyller sin funktion och lever upp till dataskyddsförordningen. Den kan även komma att begäras ut av IMY vid tillsyn. Eftersom utomstående kan komma att da del av den behöver den vara så tydligt skriven att även de förstår innehållet. Använd t ex inte interna förkortningar.

När ska en konsekvensbedömning göras?

När en behandling av personuppgifter kan utgöra en hög risk för enskilda personers fri- och rättigheter ska alltid en konsekvensbedömning göras. Den ska göras innan behandlingen påbörjas och påbörjas så tidigt som möjligt. I de fall där man inte behöver göra en konsekvensbedömning måste man alltid göra en riskanalys. Det är aldrig fel att göra en konsekvensbedömning då den är ett bra verktyg för att arbeta igenom informationen i en behandling.

Vilka kompetenser behövs?

Vilka som är involverade kan variera utifrån typ av behandling men flera roller behövs då det behövs olika perspektiv på behandlingen och olika kompetenser. Alla roller behöver inte vara med på workshoppar utan kan konsulteras vid behov, t ex biträdet. Bedömning görs för varje konsekvensbedömning. Några exempel på kompetenser är:

* Verksamheten (personuppgiftsansvarig): ansvarar för att den blir gjord och har kunskap om verksamheten, de registrerade, arbetssätt, processer mm. Flera roller kan behövas.
* Dataskyddsombudet: ska enligt artikel 35 frågas om råd, samt kan övervaka genomförandet. Det är dataskyddsombudet som ska granska konsekvensbedömningen, bedöma om den lever upp till dataskyddsförordningen och ge råd utifrån resultatet.
* Personuppgiftsbiträdet: hjälper till och bidrar med information (om ett personuppgiftsbiträde finns).
* De registrerade eller deras företrädare: lämnar synpunkter i de fall det är lämpligt.
* Teknisk kompetens från IT-avdelningen.
* Jurist.
* Andra expertroller efter behov. De kan vara både interna och externa.

Hur gör man en konsekvensbedömning?

En konsekvensbedömning behöver påbörjas tidigt inför en ny behandling av personuppgifter eller inför förändring av en befintlig behandling. Den behöver vara utförlig och detaljerad så att den verkligen beskriver behandlingen och riskerna. När åtgärderna tagits fram och genomförts ska konsekvensbedömningen visa att hela dataskyddsförordningen följs. Det räcker därför inte att lyfta ett fåtal risker utan ett omfattande arbete behöver göras. Även sådant som ni anser att ni har hanterat och har koll på behöver inkluderas, annars saknar ni bevis för att ni har hanterat det.

Det finns krav på att den ska innehålla:
* en systematisk beskrivning av den planerade behandlingen och behandlingens syfte.

* en bedömning av om behandlingen är nödvändig och proportionerlig i förhållande till syftet med den.
* en bedömning av riskerna för de registrerades rättigheter och friheter.

* de åtgärder som planeras för att hantera riskerna och för att visa att dataskyddsförordningen efterlevs.

Förutom risken för den enskildes personliga integritet måste man även titta på riskerna för andra grundläggande rättigheter så som:
* Yttrandefrihet
* Tankefrihet
* Fri rörlighet
* Förbud mot diskriminering
* Rätt till frihet, samvete och religion

Man måste också:
* rådgöra med sitt dataskyddsombud.
* inhämta synpunkter från de registrerade eller deras företrädare när det är lämpligt. Om detta inte görs dokumentera orsaken noga.

Beskrivning av behandlingen

Beskriv behandlingen noggrant i mallen. Beskrivningen behöver vara så tydlig att en utomstående förstår vad det innebär. Använd t ex inte interna förkortningar. Alla frågor behöver besvaras. Det brukar kunna bli en givande diskussion om behandlingen när man går igenom den i detalj genom att besvara frågorna. Här händer det att risker börjar identifieras. Skriv gärna in dem i riskanalysen direkt så att de inte glöms bort. Anteckna även annat som kan vara till hjälp t ex inför kravställan på system.

Risker för de registrerade

Identifiera alla risker för personer och deras integritet som ni kan komma på. Tänk inte på om de är sannolika eller inte. Det tar ni ställning till senare. Klumpa inte ihop liknande risker på en rad utan separera dem, dels för att visa att ni förstår skillnaden mellan dem och dels för att de inte sällan har olika värden för risk och/eller konsekvens.

Ta även med sådana risker som ni redan har koll på, annars kan ni inte visa att ni har hanterat dem och uppfyller därmed inte ansvarsskyldigheten.

Under en konsekvensbedömning tittar man på många olika typer av risker. Riskerna kan vara interna eller externa.

Riskområdena nedan kan användas för att identifiera risker. Det kan finnas flera risker inom ett område men det kanske inte finns risker i alla områden för alla behandlingar.
* Bristande teknisk säkerhet
* Bristande organisatorisk säkerhet
* Överföring till tredjeland (Överföringsanalys behöver göras)
* Externa intrång
* Interna läckor
* Intern obehörig användning
* Tekniska fel/brister (buggar)
* Avbrott
* Oönskad förändring/radering mm
* Virusangrepp/annan skadlig kod
* Spioneri/företagsspioneri
* Juridiska risker
* Oönskat utlämnande enligt lag
* Inlåsningseffekter (vid byte av leverantör, om leverantören säljs eller går i konkurs, hinder för byte av leverantör mm)
* Hur man ska hantera om leverantören under avtalstiden vill göra förändringar i tjänsten som inte följer kommunens krav
* Om de registrerades rättigheter inte kan tillgodoses
* Om fler personuppgifter än nödvändigt behandlas
* Om personuppgifter används för fel ändamål i organisationen
* Om biträdet använder personuppgifter för egna ändamål (t ex utveckling av tjänsten)
* M.m.

Konsekvenser för de registrerade

När riskerna är identifierade tittar ni på vilka konsekvenser de kan få för personerna (de registrerade). Exempel på konsekvenser kan vara:
* Den registrerade förlorar kontrollen över de egna personuppgifterna
* Begränsning av rättigheter (Vilka rättigheter?)
* Diskriminering
* Identitetsstöld eller bedrägeri
* Ekonomisk förlust
* Obehörigt hävande av pseudonymisering
* Skadat anseende
* Förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt
* Annan ekonomisk nackdel
* Annan social nackdel

Ange hur hög risken är och hur stor konsekvensen kan bli för personer.

Åtgärder

När risker har identifierats ska åtgärder tas fram och genomföras innan behandlingen får påbörjas. Personer behöver tilldelas ansvar för att åtgärderna blir genomförda.

Exempel på åtgärder kan vara:
* autentisering/stark autentisering
* kryptering (ange nivå)
* rutiner
* tydlig information om säkerhet till systemets användare
* utbilda användare
* logg över vem som använder personuppgifter
* stöd för säkerhetskopiering
* pseudonymisering av personuppgifter
* öppen redovisning av personuppgifternas syfte och behandling
* möjlighet för den registrerade att övervaka uppgiftsbehandlingen
* minska antalet personer som har tillgång till uppgifterna
* begränsa sökbegreppen så att det inte går att söka på känsliga personuppgifter
* införa automatisk borttagning av personuppgifter som inte längre ska behandlas
* utforma it-systemen så att inte fler personuppgifter än nödvändigt behandlas, det vill säga inbyggt dataskydd och dataskydd som standard.

Om det inte går att begränsa riskerna trots åtgärder, så att risken fortfarande är hög, måste ett förhandssamråd med IMY göras.

Konsekvensbedömningen – ett levande dokument

Även om konsekvensbedömningen ska vara klar och åtgärderna genomförda innan behandlingen av personuppgifterna påbörjas så är den inte permanent avslutad. Den är ett levande dokument bör omvärderas regelbundet. Uppdatera den om ni upptäcker risker under pågående behandling och när det görs en förändring, t ex om en ny funktion ska läggas till i ett IT-system.

Är behandlingen laglig och rimlig? (Proportionalitetsbedömning)

Senast i samband med konsekvensbedömningen behöver en bedömning göras av om det är lämpligt att gå vidare med den tänkta behandlingen eller förändringen, dvs en sk proportionalitetsbedömning (rimlighetsbedömning). Finns det mindre integritetskänsliga sätt att uppfylla ett ändamål så saknas i regel rättslig grund för behandlingen. Det mindre integritetskänsliga sättet bör då användas. Bedömning görs av om behandlingen är laglig utifrån dataskyddslagarna.
Bedömningen görs av dataskyddsombudet. Om någon annan gör denna bedömning bedömer dataskyddsombudet om den bedömning som gjorts är korrekt.

Man tittar då på behandlingens skyddsvärde och bedömer om den är rimlig och inte mer integritetskänslig än nödvändigt för ändamålet. Man behöver analysera om behandlingen är lämplig att utföra på det tänkta sättet med utgångspunkt i ändamål, vilka personuppgifter som ska behandlas och vilka de registrerade är. Frågor att ta ställning till kan t ex vara:

* Är den rimlig att genomföra med hänsyn till säkerhet, risker, juridik mm?
* Är det rimligt att lägga ut den till leverantören eller om det behöver vara på egna servrar.

* Har vi tillräcklig kontroll över uppgifterna om de läggs i en molntjänst? Kan vi skydda uppgifterna tillräckligt? Vad kan hända om uppgifterna kommer i orätta händer?
* Finns lagstöd att behandla personuppgifterna på det tilltänkta sättet? T ex när det gäller känsliga personuppgifter. Det räcker inte att det finns lagstöd för att behandla personuppgifterna. Sättet de behandlas på får inte vara mer integritetskänsligt än nödvändigt.

* Går det att utföra behandlingen på ett mindre integritetskänsligt sätt? Då bör det väljas.

Om man ändå vill behandla personuppgifterna på det tilltänkta sättet men det finns risk för att det innebär hög risk måste förhandssamråd med IMY göras, enligt artikel 36 i dataskyddsförordningen.

Grundläggande rättigheter

Dataskyddsförordningen är ett led i att efterleva artikel 8 i Europakonventionen om de mänskliga rättigheterna, dvs rätten till skydd för privat- och familjeliv.
Även andra rättigheter kan påverkas på ett negativt sätt vid behandling av personuppgifter. Bedöm följande på fliken konsekvensmatris:
- vilka av rättigheterna nedan som kan påverkas vid den aktuella behandlinen
- beskriv påverkan
- uppge hur negativ påverkan ska förhindras.

Rättigheterna är:
- Rätten till yttrandefrihet
- Rätten till tankefrihet
- Rätten till fri rörlighet
- Rätten att inte bli diskriminerad
- Rätten till tankefrihet, samvetsfrihet och religionsfrihet

(Exempel vid kamerabevakning i det offentliga rummet: Människors vilja att vistas på platsen kan minska vilket kan leda till att de känner sig hindrade att delta i demonstrationer eller andra aktiviteter kopplade till yttrandefrihet, tankefrihet mm)

CODE OF CONDUCT AND ETHICAL GUIDELINES FOR SUPPLIERS

This code of conduct formalizes the key principles related to expected business practice and conduct of No Isolation's suppliers and other third party contractors (including service providers, agents, sales representatives, consultants and other parties involved in the production of products and components and in the provision of services to No Isolation) (hereinafter referred to as "suppliers"). No Isolation expects its suppliers (and their subcontractors) to be committed to ethical standards and business practices compatible with those of No Isolation when providing products and/or services to No Isolation.

Suppliers are required to comply with this code, and we expect that suppliers ensure their subcontractors adhere to this code.

1 ACT WITH INTEGRITY AND IN COMPLIANCE WITH APPLICABLE RULES, REGULATIONS AND POLICIES

All suppliers to No Isolation commit to conduct its business operations in an ethical manner by maintaining a culture of integrity, transparency, openness and compliance.

All suppliers to No Isolation shall comply with all applicable local and national laws, rules and regulations and requirements in the provision of products and/or services manufactured or provided to No Isolation.

2 LABOUR RIGHTS AND HUMAN RIGHTS

2.1 UNDERAGE LABOUR

Suppliers shall ensure that no underage labour has been used in the production or distribution of goods and services to No Isolation. A child is any person under the minimum employment age according to the laws of the country where the product (or parts of) or services are sourced from, or in the absence of law under the minimum age for completed mandatory education.

2.2 FORCED LABOUR AND RESPECT OF HUMAN RIGHTS

Suppliers will not use or tolerate in their supply chain any form of slavery, servitude, indentured, bonded, involuntary, military or compulsory labour or any form of human trafficking.

All work must be conducted voluntarily and without threat of any penalty or sanctions.

No employee government issued identification, passports or work permits shall be retained by the supplier as a condition of employment.

Workers' rights to leave their workplace after their shift or to terminate their employment after reasonable notice and receive owed salary must be recognized by the supplier. This also applies to local or migrant employees.

Suppliers are asked to report to No Isolation any incidents of slavery or human trafficking found in its business or supply chain.

No Isolation is committed to protect and respect the fundamental human rights of anyone affected by our operations. No Isolation expects its suppliers and, business partners and other parties directly linked to its operations, products or services to be equally committed to respecting internationally recognized human rights.

Further to the above expectation to recognize human rights, suppliers shall respect the rights of workers to associate or not to associate with any group as permitted by and in accordance with all applicable local and national laws and freedom of association and collective bargaining. Suppliers shall not interfere with or discriminate against workers choosing to take part in such free associations and collective bargaining.

Where the right to freedom of association and collective bargaining is restricted under national law suppliers will facilitate, not hinder, alternative means of independent and free association and bargaining.

2.3 WAGES AND BENEFITS

Wages and benefits of the supplier's employees and/or workers must meet legal minimums and industry standards without unauthorized deductions.

2.4 HEALTHY AND SAFE WORKING CONDITIONS

The supplier must provide safe and clean conditions for workers at sites of working and residential facilities. Clear procedures must be in place to ensure regulated occupational health safety and wellbeing standards are adhered to.

2.5 WORKING ENVIRONMENT

No Isolation expects that all suppliers treat everyone with courtesy and respect, regardless of race, gender, national or social origin, disability, sexual orientation, religious belief etc. An inclusive and diverse work environment is encouraged with equal opportunities for all workers.

All employees must be treated fairly and not be discriminated against in any form of employment.

Suppliers must not discriminate against any employee based on age, gender, sexual orientation, race, ethnicity, disability, religion, political affiliation, union membership, national origin, marital or pregnancy status or any other relevant grounds during any hiring or other employment practices.

Suppliers must commit to a workforce free of any harassment or threat of harassment. Any forms or threats of harassment physical, mental, sexual or verbal must be prohibited and not tolerated.

3 CONFLICTS OF INTEREST

A conflict of interest occurs when an individual's personal relationships or interests could influence, or could be perceived to influence, the individual's decision making when acting for the supplier.

The supplier shall ensure that neither the company nor its directors and employees have any external positions or engagements that could represent a conflict of interest in relation to the supplier’s work for No Isolation.

4 ANTI CORRUPTION

All suppliers shall in relation to their activities with No Isolation and generally work against corruption in all its forms. Suppliers shall have a clear policy against all forms of corruption including but not limited to, extortion, solicitation, bribery of public officials, private sector bribery, negligent financing of corruption, facilitation payments, fraud and money laundering.

No Isolation expects its suppliers not to make any facilitation payments, i.e. payments that are made to speed up decisions and approvals that No Isolation is entitled to.

5 ENVIRONMENT

Suppliers are committed to operate in an environmentally responsible and efficient manner and comply with national and international laws and resolutions for the protection of the environment. Suppliers are committed to minimizing pollution, promoting efficient and sustainable use of resources, including energy and water, and minimizing greenhouse gas emissions in production and transport.

6 REPORTING CONCERNS

Suppliers are invited to report any area of concern to No Isolation. If suppliers identify severe adverse impacts that they either cause, contribute or are linked to, suppliers must immediately inform No Isolation and propose a plan to remedy the impact.

7 APPLICABILITY OF AND COMPLIANCE WITH THE CODE

This code applies to all No Isolation’s suppliers.

Suppliers must be able to demonstrate compliance with the No Isolation supplier code of conduct. This includes documented evidence and right of No Isolation or a third party designated by No Isolation to conduct audits. Audits to include facility inspections, reviews of supplier’s records business practices and conducting employee interviews.

In case of breach of this Code of Conduct No Isolation may suspend or terminate the agreement with the supplier.

8 FURTHER INFORMATION

Any questions that suppliers may have regarding this code shall be addressed to the CEO of No Isolation.

The code shall be available on No Isolation’s website and communicated internally to No Isolation personnel and externally to all Suppliers.