Upprättad: 2024-06-12
Diarienummer: BOUN.2024.53

Barn- och utbildningsnämnden

Användning av närvarorobotar i grundskolan under provperiod

Förslag till beslut

1. Användningen av AV1 Robot som inkluderingsverktyg för ökad närvaro i skolan godkänns under en provperiod läsåret 2024-25.
2. I samband med provperiodens slut uppdras förvaltningen att redovisa en utvärdering av arbetssättet, som underlag för nämndens fortsatta ställningstagande.
3. Konsekvensbedömning av personuppgiftsbehandlingar vid användning av AV1 Robot enligt Dataskyddsförordningens Artikel 35 godkänns.
4. Förvaltningschef uppdras att teckna hyresavtal för provperioden.

Ärendebeskrivning

Barn- och utbildningsnämnden har i verksamhetsplanen 2024-2026 gett förvaltningen ett prioriterat uppdrag att *Ta fram ett nytt arbetssätt kring ökad elevnärvaro*. Under våren har därför grundskolorna testat ett arbetssätt för att nå elever som inte kommer till skolan ("hemmasittare") genom en AV1 Robot. Roboten gör det möjligt för elever att delta i undervisning och sociala sammanhang när de inte kan vara på plats, med syfte att underlätta återgång när det dags att komma tillbaka. Under testperioden har fyra robotar funnits centralt på förvaltningen för skolorna att låna till utvalda elever.

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.

Det är för tidigt och för få elever som hittills använt sig av närvarorobotarna för att kunna dra större slutsatser av effekterna. Skolorna ser däremot robotarna har hjälpt individer som fått testa arbetssättet. De uppger att den skapar en samhörighet som i bästa fall genererar en nyfikenhet och vilja att ta steget tillbaka till skolan. Exempelvis har roboten kunnat följa med under större delar av skoldagen än bara under lektioner, såsom under rastaktiviteter och i skolmatsalen. Skolorna är nöjda med hur robotarna fungerar och ser vinster i att fortsätta med arbetssättet. Den första testperioden löper ut

till sommaren och då erbjuds möjligheten att köpa ut eller hyra robotar för fortsatt användning.

Ekonomiska konsekvenser

Finansiering sker inom befintlig ram.

Juridiska konsekvenser

Konsekvensbedömning i enlighet med artikel 35 dataskyddsförordningen

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

Nämndens GDPR-samordnare bedömer att det finns tillräckliga organisatoriska och tekniska säkerhetsåtgärder för personuppgiftsbehandlingen. Behandlingen är nödvändig för uppfyllandet av skolplikt enligt skollag för en mindre kategori elever med särskild problematik. 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 mellan elevens enhet och roboten ("peer-to-peer"). 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.

Nämnden föreslås därför att godkänna konsekvensbedömning av personuppgiftsbehandlingar vid användning av AV1 Robot enligt dataskyddsförordningens Artikel 35.

Lagutrymme skollagen

När det gäller elever med problematisk skolfrånvaro är det sällan samma lagrum kommer till användning. Det är också ofta i relation till elever med problematisk skolfrånvaro frågan om distansundervisning kommer upp och farhågor kring att etablera ett varaktigt alternativ till närundervisning. Men att använda AV1 kan utifrån hur skollagen definierar distansundervisning och fjärrundervisning inte betraktas som någotdera. Istället är Skollagens 3 kap. 9-10§ om särskilt stöd det mest tillämpliga.

Inom ramen för särskilt stöd och i ett åtgärdsprogram beslutar rektor om användningen av AV1 (3 kap. 9§). Målet är att stödja eleven på det sätt och i den

omfattningen som behövs för att eleven ska ha möjlighet att uppfylla de betygskriterier eller bedömning av kunskaper som ska uppnås (3 kap. 10§). AV1 används alltid som ett hjälpmedel för att kunna komma tillbaka till skolan, inte för att ersätta ordinarie undervisning på lång sikt. Varje AV1-insats som särskilt stöd utvärderas med korta intervaller.

Bedömning

AV1 Robot används i dag i drygt 120 svenska kommuner såsom Göteborg, Linköping och Eskilstuna. Digitala kommunikationshjälpmedel som AV1 under en planerad och begränsad tid har visat sig vara en framgångsfaktor i att vända långvarig och problematisk frånvaro. Utifrån utvärdering av grundskolorna och genomförd konsekvensbedömning ser förvaltningen positivt på att ha ett antal robotar centralt som kan användas som ytterligare ett verktyg i det åtgärdande arbetet för att få tillbaka elever till skolgång. En provperiod kan användas för att identifiera för- och nackdelar med användningen av AV1 Robot, för eventuell fortsatt användning.

Beslutsunderlag

1. Tjänsteskrivelse 2024-06-12
2. Konsekvensbedömning AV1 Robot

Sändlista

~ Chef för elevhälsa och kvalitet

Johan Skeppstedt
Förvaltningschef

Jenny Karlsson
Strateg

Risk- och sårbarhetsanalys samt konsekvensbedömning av AV1-robot

Innehållsförteckning

1. Bakgrund

1.1 Syfte och avgränsningar

AV1-robotar är ett digitalt hjälpmedel för undervisning och inkludering i skolan som gör att ingen behöver missa lektioner, raster och samtal med vänner. AV1 placeras i klassrummet och eleven deltar från annan plats via surfplatta eller mobil. AV1 är utrustad med inbyggd kamera, mikrofon och högtalare som gör att eleven kan se, höra och prata med sin omgivning. Med hjälp av en app kan eleven vrida på roboten, interagera med klassen och delta i undervisningen ungefär som om hen vore där fysiskt. Syftet med riskanalysen och konsekvensbedömningen är att undersöka vilka risker och konsekvenser det innebär att använda AV1-robotar samt ta fram åtgärdsplan.

1.2 Definitioner

Autentisering: Innebär kontroll av uppgiven identitet, t.ex. vid inloggning, vid kommunikation mellan två system eller vid utväxling av meddelande mellan användare.

Behandling av personuppgifter: Åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Behörighetsstyrning: Innebär möjligheten att styra någons rätt att få tillgång till och behandla information i ett system och kan även omfatta rättigheten att ändra hela strukturen i verktyget.

Dataskyddsförordningen (GDPR): Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG

Dataskyddsombud (DSO): Den som behandlar personuppgifter måste i vissa fall utse ett dataskyddsombud. Ombudets roll är att kontrollera att dataskyddsförordningen (GDPR) följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser.

Inre risk: Risk som förekommer inom organisationen.

Integritetsskyddsmyndigheten (IMY): Inom EU har respektive land sin egen nationella dataskyddsmyndighet. I Sverige är det Integritetsskyddsmyndigheten, i Danmark Datatilsynet, i Finland Dataombudsmannens byrå och så vidare. På engelska brukar dessa kallas för DPA:s, Data Protection Authorities. I Sverige ska tillsynsmyndigheten se till att myndigheter, kommuner, företag och andra organisationer följer dataskyddsförordningen, den svenska kompletterande dataskyddslagen, brottsdatalagen och kamerabevakningslagen. Den svenska tillsynsmyndigheten ska dessutom kunna begära hjälp av systermyndigheter i andra EU-länder vid granskningar av gränsöverskridande verksamheter.

Konsekvensbedömning avseende dataskydd: Konsekvensbedömning ska göras om en ny eller ändrad personuppgiftsbehandling kan komma att medföra en hög risk för fysiska personers rättigheter och friheter. Särskilda risker för fysiska personers rättigheter och friheter kan exempelvis förekomma i samband med behandling av känsliga uppgifter, behandling i särskilt stor omfattning eller vid användning av ny teknik.

Kryptering: Metod för att skydda information med hjälp av en nyckel och en algoritm (algoritm – Systematisk procedur som beskriver hur man via ett begränsat antal steg utför en beräkning eller löser ett problem, dvs texten blir oläsbar för

obehöriga som inte har fått rätt nyckel, kod för att låsa upp texten till läsbart format).

Loggning: Ett kontinuerligt insamlande av sådana elektroniska spår som innehåller information om aktiviteter vid användning av teknisk (dator-) utrustning.

Personuppgiftsansvarig: Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Varje kommunstyrelse och varje nämnd är personuppgiftsansvariga inom den kommunala verksamheten.

Personuppgiftsbiträde: Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsansvariga ska upprätta personuppgiftsbiträdesavtal med personuppgiftsbiträdet.

Personuppgifter: Varje upplysning som avser en identifierad eller identifierbar fysisk person (registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Registrerad: En fysisk levande person som personuppgifterna avser.

Risk: En sammanvägning av sannolikheten för att en händelse ska inträffa och de konsekvenser händelsen kan leda till.

Sårbarhet: De egenskaper eller förhållanden som gör ett samhälle, ett system, eller egendom mottagligt för de skadliga effekterna av en händelse.

Tredje land: En stat som inte ingår i Europeiska unionen (EU) eller är ansluten till Europeiska ekonomiska samarbetsområdet (EES).

Överföring till tredje land: Överföring av personuppgifter till länder utanför EU/ESS är en så kallad tredjelandsöverföring det kan till exempel handla om online IT-tjänster, molnbaserade tjänster, tjänster för extern åtkomst eller globala databaser. Tredjelandsöverföring får endast ske under särskilda förutsättningar.

Underbiträde: Ett personuppgiftsbiträde som anlitas av det personuppgiftsbiträdet som har ett personuppgiftsbiträdesavtal med den personuppgiftsansvarige och som också behandlar personuppgifter för personuppgiftsansvariges räkning. Underbiträdet har samma skyldigheter gällande behandling av personuppgifter som personuppgiftsbiträdet.

Yttre risk: Risk som ligger utanför organisationen.

2.1 Dataskyddsförordningen

Dataskyddsförordningen (även kallad GDPR) reglerar hur personuppgifter ska behandlas med syftet att skydda den enskildes (den registrerades) rättigheter. Följer personuppgiftsansvarige inte dataskyddsförordningen finns det en risk att de registrerades personliga integritet kränks och att kommunens eller bolagets anseende skadas. Tillsynsmyndigheten kan också föreskriva höga sanktionsavgifter och den registrerade kan ha rätt till skadestånd om personuppgiftsansvarige behandlar personuppgifter i strid med bestämmelserna i dataskyddsförordningen.

2.1.1 Grundläggande principer

I dataskyddsförordningen artikel 5 finns de grundläggande principer som alla behandlingar av personuppgifter behöver uppfylla för att vara lagliga. Om någon av dem inte uppfylls bryter behandlingen mot dataskyddsförordningen. Det gäller alla behandlingar av personuppgifter, från e-postmeddelanden till stora verksamhetssystem. Nedan följer en kort beskrivning av dessa principer.

Laglighet, öppenhet och korrekthet: Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Det behöver finnas en rättslig grund, behandlingen ska vara rimlig och de registrerade ska informeras om behandlingen.

Ändamålsbegränsning: Uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas för andra ändamål. Ändamålet beskrivs tydligt och avgränsat.

Uppgiftsminimering: Fler personuppgifter än de som verkligen måste finnas med får inte behandlas. Identifiera nödvändiga direkta och indirekta personuppgifter.

Riktighet: Personuppgifterna ska vara riktiga och om nödvändigt uppdaterade. Rutiner behövs för korrigering och radering.

Lagringsminimering: De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. T ex anonymisering, radering, gallring och arkivering.

Integritet och konfidentialitet: Den personuppgiftsansvarige ska säkerställa att tillräckliga tekniska och organisatoriska säkerhetsåtgärder finns så att uppgifterna inte kommer i orätta händer, går förlorade eller förstörs. Tekniska åtgärder kan vara kryptering, stark autentisering mm och organisatoriska åtgärder kan vara rutiner, instruktioner mm för hur personuppgifterna får behandlas. Personalen ska endast ha behörighet att komma åt de uppgifter de behöver för sitt arbete.

Ansvarsskyldighet: Den personuppgiftsansvarige ska ansvara för och kunna visa att punkterna ovan efterlevs genom dokumentation. Det är bl a registerförteckning över alla behandlingar av personuppgifter, information som lämnats till registrerade, dokumentation över teknisk säkerhet, rutiner och instruktioner, riskanalyser, konsekvensbedömningar, informationsklassningar, beslut och överväganden mm.

2.1.2 Säkerhetsåtgärder

Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning (artikel 24 i dataskyddsförordningen). Dessa åtgärder ska ses över och uppdateras vid behov.

Enligt artikel 32 i dataskyddsförordningen är den personuppgiftsansvarige ansvarig för att personuppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna med användning av tekniska och organisatoriska åtgärder.

Enligt artikel 25 i dataskyddsförordningen ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas.

Den personuppgiftsansvarige ska även beakta säkerheten i relationer med personuppgiftsbiträden. Det framgår av artikel 28 i dataskyddsförordningen följande: "Om en behandling ska genomföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas."

Tekniska säkerhetsåtgärder: Exempel på tekniska åtgärder som måste kontrolleras är:

- Tillräckliga back-up rutiner
- Tillräckliga brandväggar
- Lösenordsskyddade trådlösa nätverk
- Uppdaterat virusskydd
- Lösenordsskydd för mobila enheter såsom mobiltelefoner och surfplattor
- Skydd mot obehörig intern åtkomst
- Lösenordskrav
- Kryptering vid behov
- Loggning av, åtkomst till och användning av IT-system mm

Organisatoriska säkerhetsåtgärder kan innebära att behörighetskontroll används för de system som innehåller personuppgifter, loggning av åtkomst till personuppgifter eller att datorer och dylikt som innehåller personuppgifter ska förvaras så att obehörig åtkomst försvåras och inte lämnas framme.

Personuppgifter får inte bevaras längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Genom att i gallringsbeslut, informationshanteringsplaner eller dokumenthanteringsplaner ange lagringstid för personuppgifterna säkerställer man att personuppgifter gallras när de inte längre behövs. Även personuppgifter i så kallat ostrukturerat material såsom i dokument på servrar, i en enkel lista, på webbplatser etc. behöver raderas när ändamålet med behandlingen är uppfyllt.

2.1.3 Överföring av personuppgifter till tredje land

Enligt dataskyddsförordningen är det förbjudet att överföra personuppgifter till länder som ligger utanför EU/EES (så kallade tredje länder). Det finns dock undantag som framgår av art. 44-49 i dataskyddsförordningen.

2.1.3.1 Exempel på överföring av personuppgifter till tredje land

- När ett dokument som innehåller personuppgifter skickas till någon i ett land utanför EU/EE via e-post
- När ett personuppgiftsbiträde anlitas i ett land utanför EU/EES
- När någon utanför EU/EES får tillgång, exempelvis läsbehörighet, till personuppgifter som finns lagrade inom EU/EES
- När personuppgifter lagras i en molntjänst som är baserad utanför EU/EES
- När personuppgifter lagras, till exempel på en server, i ett land utanför EU/EES.

Att publicera något på internet är *inte* tredjelandsöverföring om webbplatsen lagras hos en internetleverantör som är etablerad inom EU.

2.1.3.2 Undantag när överföringen till tredjeland är tillåten

Det är som huvudregel förbjudet att överföra personuppgifter till tredje länder, men det finns sex undantag, såsom:

- Adekvat skyddsnivå - EU-kommissionen kan fatta beslut om att ett land har en tillräckligt hög skyddsnivå. En lista med länder med adekvat skyddsnivå finns tillgänglig på IMYs hemsida
- Bindande företagsbestämmelser (Binding Corporate Rules, BCR) är regler som en företagskoncern med bolag i flera olika länder kan ta fram för att reglera sin behandling av personuppgifter (ej aktuella för kommuner eller kommunala bolag)
- Standardavtalsklausuler som EU-kommissionen har beslutat om
- Godkända uppförandekoder eller certifieringsmekanismer
- Rättsligt bindande instrument mellan myndigheter
- Tillstånd från tillsynsmyndigheten

Förutom de ovan nämnda undantagen kan personuppgifter överföras till tredje land med stöd av tryckfrihetsförordningen eller yttrandefrihetsgrundlagen eller vid behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande enligt 1 kap. 7 § dataskyddslagen.

2.1.3.3 Adekvat skyddsnivå

EU-kommissionen kan fatta beslut om att ett land har en tillräckligt hög skyddsnivå. I dataskyddsförordningen kallas det för adekvat skyddsnivå. Det kan även gälla ett visst territorium, en internationell organisation eller en eller flera områden i ett tredje land.

När EU-kommissionen fattar beslut om adekvat skyddsnivå tittar de bland annat på landets lagar och internationella åtaganden, vilka möjligheter den registrerade har att få rättslig prövning och om landet respekterar de mänskliga rättigheterna och de grundläggande friheterna. EU-kommissionen kontrollerar också att det finns oberoende tillsynsmyndigheter som ansvarar för att dataskyddsreglerna följs och som kan hjälpa den registrerade.

2.1.3.4 Länder med adekvat skyddsnivå

EU-kommissionen har fattat beslut om att skyddsnivån i till exempel dessa länder är adekvat, det vill säga tillräckligt hög enligt dataskyddsförordningen.
Listan uppdateras regelbundet och finns tillgänglig på IMYs internetsida.

2.1.3.5 Bindande företagsbestämmelser

Bindande företagsbestämmelser (Binding Corporate Rules, BCR) är regler som en företagskoncern med bolag i flera olika länder kan ta fram för att reglera sin behandling av personuppgifter. Bindande företagsbestämmelser måste godkännas av tillsynsmyndigheten i Sverige eller någon annan tillsynsmyndighet i EU.
Bindande företagsbestämmelser är inte aktuella för kommuner och kommunala bolag.

2.1.3.6 Standardavtalsklausuler (SCC)

EU-kommissionen har godkänt vissa standardavtalsklausuler som handlar om dataskydd (Standard Contractual Clauses, SCC). Standardavtalsklausulerna innehåller skyldigheter dels för personuppgiftsansvariga som vill föra över personuppgifter till länder utanför EU/EES, dels för personuppgiftsansvariga eller personuppgiftsbiträden som tar emot sådana uppgifter.
EU-domstolen har i sitt beslut den 16 juli 2020 (så kallat Schrems II) bedömt standardavtalsklausulerna som giltiga med vissa förutsättningar, bland annat krävs det att personuppgiftsansvarige ska vidta ytterligare skyddsåtgärder. EDPB har tagit fram rekommendationer 1/2020 om ytterligare åtgärder för att tillförsäkra att EU:s nivå av skydd för personuppgifter upprätthålls.
Rekommendationerna innefattar också kriterier som tydliggör under vilka tänkbara omständigheter som en överföring inte är möjlig. Bedömningen av vilka åtgärder som ska användas och i vilken utsträckning det är tillräckligt för att uppnå en godtagbar skyddsnivå ska göras i varje enskilt fall och av personuppgiftsansvarige.
Personuppgiftsansvarig skall därför bland annat säkerställa:

1. Väsentligt likvärdig skyddsnivå för uppgifterna som inom EU och EES genom analys av landets lagar och internationella åtaganden
2. Vilka möjligheter den registrerade har att få rättslig prövning
3. Om landet respekterar de mänskliga rättigheterna och de grundläggande friheterna
4. Om det finns oberoende tillsynsmyndigheter som ansvarar för att dataskyddsreglerna följs och som kan hjälpa den registrerade.

2.1.3.7 Uppförandekoder och certifieringsmekanism

Om personuppgiftsansvarig ansluter sig till en godkänd uppförandekod eller godkänd certifieringsmekanism kan det vara tillåtet att överföra personuppgifter till länder utanför EU/EES. Detta gäller under förutsättning att dessa medför rättsligt bindande och verkställbara skyldigheter även för mottagaren av personuppgifterna.

2.1.3.8 Rättsligt bindande instrument mellan myndigheter

Det är tillåtet att grunda en överföring av personuppgifter till ett land utanför EU/EES på ett så kallat rättsligt bindande och verkställbart instrument, om överföringen sker mellan myndigheter. Ett sådant instrument mellan myndigheter kan vara ett samförståndsavtal eller ett informationsutbytesavtal inom till exempel skatteområdet.

2.1.3.9 Tillstånd från tillsynsmyndigheten

Myndigheter får överföra personuppgifter till ett land utanför EU/EES om de har fått tillstånd från tillsynsmyndigheten. Ett sådant tillstånd kan lämnas om överföringen grundar sig på avtalsklausuler mellan den som för över personuppgifter och mottagaren av dessa. Om det gäller överföring av personuppgifter mellan myndigheter kan tillstånd även lämnas om överföringen grundar sig på bestämmelser i administrativa överenskommelser som innehåller verkställbara och faktiska rättigheter för de registrerade. Innan tillsynsmyndigheten beslutar om

särskilt tillstånd ska ett yttrande inhämtas från den Europeiska dataskyddsstyrelsen, där företrädare för alla EU/EES-länders tillsynsmyndigheter är med.

2.1.3.10 Undantag i särskilda situationer

Om det inte föreligger något beslut om adekvat skyddsnivå enligt artikel 45.3 i dataskyddsförordningen, eller om lämpliga skyddsåtgärder enligt artikel 46, inbegripet bindande företagsbestämmelser, får en överföring eller uppsättning av överföringar av personuppgifter till ett tredjeland eller en internationell organisation endast ske om något av följande villkor är uppfyllt:

- Den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den registrerade när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder
- Överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvarige eller för att genomföra åtgärder som föregår ett sådant avtal på den registrerades begäran
- Överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den personuppgiftsansvarige och en annan fysisk eller juridisk person i den registrerades intresse
- Överföringen är nödvändig av viktiga skäl som rör allmänintresset
- Överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk
- Överföringen är nödvändig för att skydda den registrerades eller andra personers grundläggande intressen, när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke
- Överföringen görs från ett register som enligt unionsrätten eller medlemsstaternas nationella rätt är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, men endast i den utsträckning som de i

unionsrätten eller i medlemsstaternas nationella rätt angivna villkoren för tillgänglighet uppfylls i det enskilda fallet.

4. Risk-och sårbarhetsanalys

Enligt artikel 25 i dataskyddsförordningen ska den personuppgiftsanvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

För att säkerställa att den personuppgiftsansvarige vidtar tillräckliga säkerhetsåtgärder krävs ett kontinuerligt informationssäkerhetsarbete för att hantera och minimera risker på det bästa sätt. Den personuppgiftsansvarige kan använda sig av olika åtgärder och teknik men det måste finnas ett implementerat informationssäkerhetsarbete för att uppfylla syftet med dataskyddsförordningen att skydda enskildas grundläggande rättigheter och friheter.

Risk-och sårbarhetsanalys är därför ett viktigt verktyg för att identifiera och bedöma risker som kan leda till negativa konsekvenser för den personuppgiftsansvarige och de registrerade för att information kan vara värdefull för både organisationen och för den enskilda individen. Det gäller allt från fastighetsförteckningar, patientjournaler, forskningsresultat till saldot på ett bankkonto. Det kan handla om styrsystem till vatten-och avlopp eller värmeverk. Om informationen förloras, eller om den felaktigt ändras kan det få katastrofala följder. Skydd av information ska vara behovsanpassat och det ska vara tillräckligt bra och inte för svagt eller allt för krångligt eller dyrt. Brister i hantering av information riskerar att leda till försämrat förtroende för tjänsten och sker upprepade störningar kan det leda till förtroendekriser.

Vid arbete med informationssäkerhet ingår det att införa och förvalta administrativa regelverk till exempel policys och riktlinjer. Det behöver finnas tekniskt skydd som till exempel brandväggar och kryptering samt fysiskt skal-och brandskydd.

Informationssäkerhetsarbetet har sin grund i standarderna i ISO 27000-serien som har beteckningen "ledningssystem för informationssäkerhet". ISO-27000 serien bildar grunden för att bedriva ett systematiskt informationssäkerhetsarbete i en organisation.

4.1 Information skall alltid skyddas så att den är

- Tillgänglig (informationen ska alltid finnas nåbar när den behövs).
- Riktig (informationen ska gå att lita på, den ska vara korrekt och spårbar inte manipulerad eller förstörd).
- Konfidentiell (behörighetsstyrd, endast behöriga personer har rätt att ta del av informationen).

4.2 ISO-standard SS-EN ISO/IEC 27001 kräver kortfattat

- Att informationsäkerhetsrelaterade risker analyseras
- Att riskanalysens resultat ligger till grund för val och utformning av säkerhetsåtgärder och det systematiska informationssäkerhetsarbetet.

4.3 Frågor som en riskanalys ska besvara

En riskanalys ska underlätta att identifiera, klassificera och formulera risker samt att finna åtgärder som kan minimera riskerna. Det är bra att ställa sig följande frågor

- Vad kan hända?
- Hur sannolikt är det att det inträffar?
- Vad blir konsekvenserna om det inträffar

4.4 Exempel på skyddsåtgärder som kan vidtas:

4.4.1 Krypteringslösningar och nyckelhantering

Krypteringslösningar och nyckelhantering utgör en viktig del av skyddsåtgärderna kring ett it-system eller en it-tjänst. Området är omfattande och förutsättningarna förändras ständigt.

- **Kryptering:** Metod för att skydda information med hjälp av en nyckel och en algoritm (algoritm – Systematisk procedur som beskriver hur man via ett begränsat antal steg utför en beräkning eller löser ett problem, dvs texten blir oläsbar för obehöriga som inte har fått rätt nyckel, kod för att låsa upp texten till läsbart format)
- **Kryptografisk funktion**: Metoder och principer för skydd av information mot insyn vid överföring och lagring med hjälp av kryptering
- **Nyckelansvarig:** Entitet som administrativt och operativt ansvarar för en viss kryptonyckel eller serie av kryptonycklar

Krypteringslösningar är en förutsättning för att kunna skydda information i dagens it- system. Genom att använda kryptolösningar, både i när information är i rörelse och i vila, minskas risken för att obehöriga kan ta del av känsliga data. Kryptering av data innebär att verksamheten till en viss nivå kan lita på att informationen inte kan läsas av utan betydliga resurser, även när kommunikationskanalen som bär informationen är avlyssnat eller att USB- minnet som lagrar informationen är borttappad. Den skyddsnivå som kryptolösningen ger är inte enbart baserat på den tekniska lösningen. Krav på hur kryptonycklar hanteras, åtkomst till kryptolösningar och val av kryptolösningar är mycket viktiga i sammanhanget. Kryptering är således inte enbart en it-säkerhetsåtgärd, utan mycket beroende av andra

säkerhetsåtgärder som vidtas i samband med hanteringen av krypto- lösningen. Informationen måste skyddas mot angrepp mot både konfidentialitet och riktighet. När kryptering ska användas inom och mellan verksamheter måste de också iaktta behovet att kunna upptäcka ”illasinnad” trafik. Skyddet som kryptering erbjuder måste alltså upprättas på sådant sätt att möjliggöra trafikinspektion i vissa fall.

4.4.2 Autentisering

Autentisering innebär kontroll av uppgiven identitet, t.ex. vid inloggning, vid kommunikation mellan två system eller vid utväxling av meddelande mellan användare. Det vanligaste sättet att autentisera sig är fortfarande genom att använda ett användarnamn och ett lösenord. Dessvärre är metoden osäker och många använder samma kombination av användarnamn och lösenord på flera plattformar. Detta gör det relativt enkelt för en antagonist att få åtkomst till flera system på samma gång om ett konto skulle kompromettеras. Av denna anledning är “stark autentisering” att föredra nu för tiden då den likställs med flerfaktorsautentisering under en viss tillitsnivå.

4.4.3 Stark autentisering

I detta sammanhang att likställa med flerfaktorsautentisering under en viss tillitsnivå (Tillförlitlighet – Mått på i vilken grad ett system levererar information av den kvalitet det säger sig leverera och inloggningen sker med hjälp av flera olika steg.

4.4.4 Loggning

Loggning innebär att man samlar loggar för händelser som kan bidra till att upptäcka, förstå och återställa efter ett angrepp. Händelser bör registreras så att säkerhetsöverträdelser kan upptäckas så tidigt som möjligt, om inte förhindras. Vid incidenter kan loggar bidra till att identifiera skadans karaktär och omfattning och att skadan kan åtgärdas. Loggar bidrar också till att kartlägga omfattningen av ett

angrepp, tidslinje för angreppet och kan utgöra en grund för eventuella rättsliga påföljder. Oönskad aktivitet i eget nätverk kan vara svårt att upptäcka, och om en angripare får fotfäste kommer det mesta av trafiken internt i det egna nätverket att maskeras som legitim trafik. Bristande eller felaktig konfiguration av loggning och logganalys kan medföra att angripare oupptäckt kan gömma både sin närvaro, skadlig programvara och aktiviteter i verksamhetens it-system. Loggar användas för att skapa en översikt över normaltillståndet så att avvikelser kan upptäckas. Detta, i kombination med större användning av ändpunkt-till-ändpunkts-kryptering, gör att loggning vid slutpunkter och mellan nätverkssegment bör prioriteras framför loggning av generell nätverkstrafik. Att ta fram ett normaltillstånd måste göras med beaktandet att en angripare redan kan vara i nätverket och på så sätt påverka vad som uppfattas vara normaltillstånd. Att aktivera loggning på all utrustning för att logga allt kommer generera stora mängder data som kan vara svårt att hantera och att bearbeta detta för hand är inte praktiskt möjligt. Konfigurera så att varningar ges för vissa identifierade händelser för att urskilja dessa i bruset. Detaljerade loggar kan fortfarande vara bra att ha tillgängliga för att undersöka dessa händelser. Loggar är viktiga för incidenthantering och effektiv drift av it-system, men de ska också användas med varsamhet och därför skyddas väl. Loggar kan innehålla känslig information om enskilda medarbetare och behovet av loggning måste alltid vägas mot behovet för skydd av personlig integritet.

4.4.5 Behörighetsstyrning

Behörighetsstyrning innebär möjligheten att styra någons rätt att få tillgång till och behandla information i ett system och kan även omfatta rättigheten att ändra hela strukturen i verktyget. En behörighet kan även ge någon rätt att utföra ett uppdrag(till exempel genomföra en betalning). Behörigheter kan sättas på olika nivåer, till exempel kan du som användare på en Sharepoint-webbplats ha behörighet att läsa och ladda ner, men inte ändra information (låg behörighet), medan den som skapade webbplatsen (administratören) kan förutom att läsa, lägga

till och ändra information samt även ändra hela strukturen i verktyget (hög behörighet). Kort sagt handlar behörighetshantering om att ge rätt person tillgång till rätt information vid rätt tillfälle.

5. Konsekvensbedömning

Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter (artikel 35 dataskyddsförordningen). Artikel 29 gruppen har antagit riktlinjer för hur konsekvensbedömningen ska göras.

Personuppgiftsansvarig, ska påbörja konsekvensbedömningen så tidigt som möjligt och börja även om vissa delar av behandlingen fortfarande är okända. Även personuppgiftsbehandlingar som har påbörjats innan dataskyddsförordningen började gälla, omfattas av kravet att en konsekvensbedömning ska genomföras vid behov. Den personuppgiftsansvarige ska rådfråga dataskyddsombudet om konsekvensbedömningen. Dataskyddsombudet bör även övervaka genomförandet av konsekvensbedömningen. Det är dock alltid den personuppgiftsansvarige som är ansvarig för att konsekvensbedömningen utförs. Konsekvensbedömningen kan utföras av någon annan, inom eller utanför organisationen, men den personuppgiftsansvarige har det yttersta ansvaret. Dataskyddsombudets råd och de beslut som den personuppgiftsansvarige fattar bör dokumenteras i konsekvensbedömningen.

En konsekvensbedömning har som syfte att förebygga risker när det kommer till dataskydd (Data Protection Impact Assessment - DPIA) för den enskildes fri-och

rättigheter[1]. Det är en process som hjälper till att identifiera och minimera dataskyddsrisker i samband med en personuppgiftsbehandling.

Det är viktigt att konsekvensbedömningen är tillräckligt omfattande och grundligt gjord så att den fyller sin funktion och uppfyller dataskyddsförordningen. Den kan även komma att begäras ut av IMY vid tillsyn.

5.1 Prövningen av om konsekvensbedömning ska göras

En konsekvensbedömning ska göras om en viss personuppgiftsbehandling ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter". Risken ska i första hand bedömas utifrån dataskydd och integritet, men även utifrån andra grundläggande rättigheter som yttrandefrihet, tankefrihet, fri rörlighet, förbud mot diskriminering, rätt till frihet, samvete och religion (artikel 35 punkt 1 dataskyddsförordningen).

5.2 När ska en konsekvensbedömning göras?

Enligt artikel 35.3 ska en bedömning särskilt krävas vid:

1. En systematisk och omfattande bedömning av fysiska personers personliga förhållanden som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.

[1]Skäl 75, GDPR Risken för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av personuppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering eller annan betydande ekonomisk eller social nackdel, om registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter, om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter, uppgifter om hälsa eller sexualliv eller fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder behandlas, om personliga aspekter bedöms, framför allt analyser eller förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

2. Behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller av personuppgifter som rör fällande domar i brottmål och överträdelser som avses i artikel 10.

3. Systematisk övervakning av en allmän plats i stor omfattning.

Om behandlingen inte ingår i de tre kategorier som framgår av artikel 35.3, ska man göra en bedömning för att komma fram till om en behandling ”sannolikt leder till en hög risk” och om det behövs därför en konsekvensbedömning.

Artikel 29 gruppen har sammanställt nio steg, som bedömningen ska göras i, som beskrivs här.

1. Utvärdering eller poängsättning, som inbegriper profilering och förutsägelse, särskilt ”aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar” (skälen 71 och 91).

2. Automatiskt beslutsfattande med rättsliga eller liknande betydande följder.

3. Systematisk övervakning.

4. Känsliga uppgifter eller uppgifter av mycket personlig karaktär.

5. Uppgifter som behandlas i stor omfattning. I förordningen definieras inte vad som avses med stor omfattning, även om viss vägledning ges i skäl 91. Arbetsgruppen rekommenderar i vart fall att följande faktorer beaktas särskilt vid bedömningen av huruvida behandlingen utförs i stor omfattning:

- 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.

6. Matchande eller kombinerande uppgiftsserier.

7. Uppgifter som rör sårbara registrerade (skäl 75).

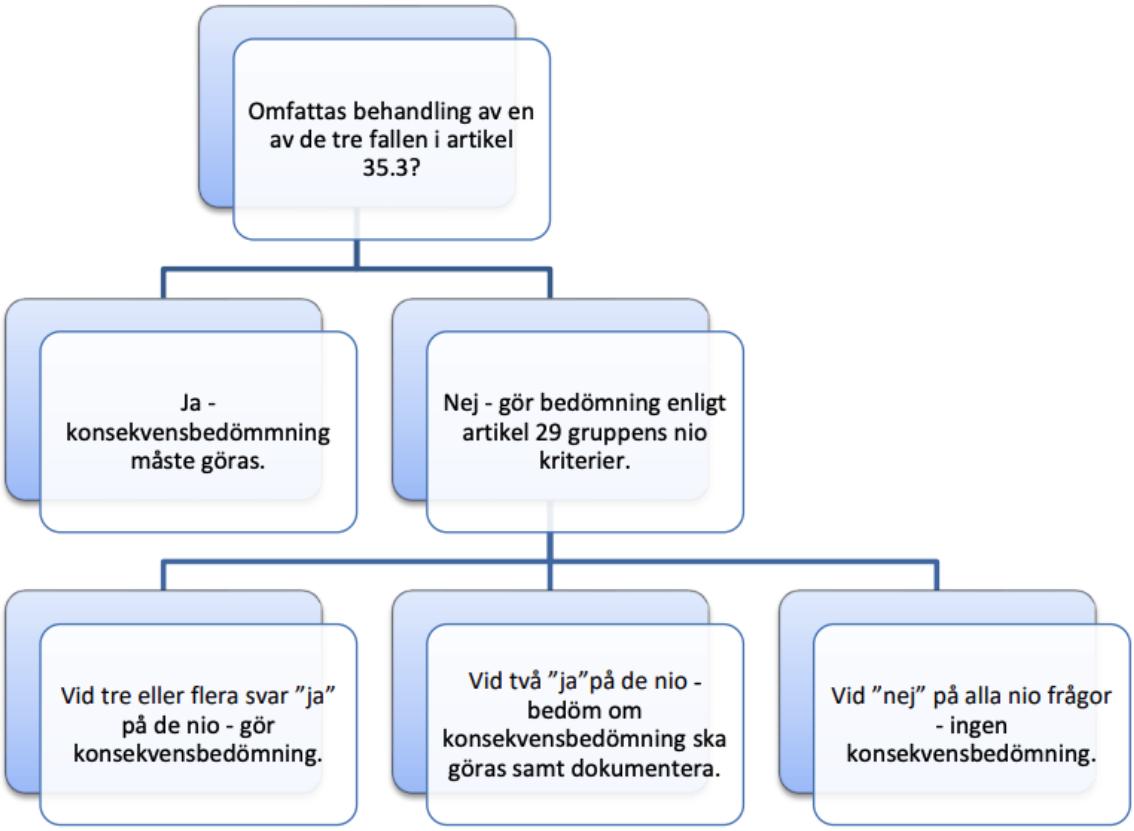
8. Innovativ användning eller tillämpning av nya tekniska eller organisatoriska lösningar: Behandling som en kombination av fingeravtryck och ansiktsigenkänning för förbättrad fysisk åtkomstkontroll osv. I förordningen klargörs (artikel 35.1 och skälen 89 och 91) att användningen av ny teknik definierad i skäl 91.

9. Om behandlingen i sig ”hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal (artikel 22 och skäl 91).

I artikel 29-gruppens riktlinjer tilläggs sedan att i de flesta situationer kan en personuppgiftsansvarig anse att en konsekvensbedömning ska utföras om två av dessa kriterier är uppfyllda. Generellt sett anser arbetsgruppen att ju fler kriterier behandlingen uppfyller, desto mer sannolikt är det att det föreligger en hög risk för de registrerades rättigheter och friheter, och att det därför krävs en konsekvensbedömning, oberoende av vilka åtgärder som den personuppgiftsansvarige planerar att vidta.

Om man får två eller flera svar ” ja” de nio frågorna ska en konsekvensbedömning göras!

Nedan följer en bild som visar de olika stegen vid prövningen.



En konsekvensbedömning skall alltid genomföras om:

- En behandling av personuppgifter kan utgöra en hög risk för enskilda personers fri- och rättigheter
- Personuppgifter ska användas i nya sammanhang, i nya system dvs. innan nya personuppgiftsbehandlingar ska påbörjas
- Risken med en pågående personuppgiftsbehandling ändras
- Det inte finns någon gjord sedan tidigare på pågående personuppgiftsbehandling.

5.3 När ska en konsekvensbedömning inte göras?

Det krävs inte en konsekvensbedömning om personuppgiftsbehandlingen: Sannolikt inte leder till en hög risk för fysiska personers rättigheter och friheter. Är mycket lik en annan personuppgiftsbehandling där det redan finns en konsekvensbedömning. Har sin rättsliga grund i en lag eller förordning, och en konsekvensbedömning redan har genomförts när lagen eller förordningen fastställdes. En konsekvensbedömning behöver inte göras om den tilltänkta behandlingen inte innefattar någon av de kriterier som artikel 29 gruppen har tagit fram som bedömningsmall.

5.4 En eller flera behandlingar?

En konsekvensbedömning kan gälla för en eller för flera liknande behandlingar. En enda konsekvensbedömning kan till exempel användas för att bedöma flera behandlingar som liknar varandra vad gäller art, omfattning, innehåll, ändamål och risker, såsom ett antal matvarubutiker ska var och en införa liknande övervakningssystem på likartade platser. De kan göra en enda konsekvensbedömning. En organisation vill införa en personuppgiftsbehandling som liknar en annan personuppgiftsbehandling där det redan finns en konsekvensbedömning. Då kan de använda den första bedömningen som referens i sin nya konsekvensbedömning. Den som gör en gemensam konsekvensbedömning för flera personuppgiftsbehandlingar ska motivera varför en enda konsekvensbedömning har utförts. Motiveringen ska dokumenteras.

5.5 Konsekvensbedömningens innehåll

En konsekvensbedömning ska enligt artikel 29 gruppen innehålla följande:

1. En systematisk beskrivning av behandlingen

Den systematiska beskrivningen ska innefatta beskrivning av behandlingens art, omfattning, sammanhang och ändamål. Den ska också innehålla beskrivning av vilka personuppgifter som registrerats, vilka mottagare de överförs till och vilken period de kommer att lagras. Det ska finnas en funktionell beskrivning av behandlingen. De tillgångar som är nödvändiga för behandlingen ska beskrivas (maskinvara, programvara, nätverk, personer, papper eller spridningskanaler för papper). Efterlevnad av eventuella godkända uppförandekoder ska beaktas (artikel 35.8).

2. Bedömning av behovet av och proportionaliteten hos behandlingen (artikel 35.7 b)

De planerade åtgärderna för att visa att förordningen följs som har fastställts (artikel 35.7 d och skäl 90), ska beskrivas. Det ska visas hur åtgärder som bidrar till att behandlingen är proportionell och nödvändiga på grundval av:

- särskilda, uttryckligt angivna och berättigade ändamål (artikel 5.1 b),
- laglig behandling (artikel 6),
- adekvata, relevanta och inte för omfattande uppgifter (artikel 5.1 c),
- begränsad lagringstid (artikel 5.1 e).

Det ska tas upp vilka åtgärder som stärker de registrerades rättigheter som är tillgängliga med beaktande av:

- Information till den registrerade (artiklarna 12, 13 och 14).
- Rätt till tillgång och till dataportabilitet (artiklarna 15 och 20). Rätt till rättelse och radering (artiklarna 16, 17 och 19).
- Rätt att göra invändningar och till begränsning av behandling (artiklarna 18, 19 och 21).
- Förhållandet till personuppgiftsbiträden (artikel 28).

- Skyddsåtgärder som vidtagits för internationella överföringar och det ska beskrivas om förhandssamråd skett (artikel 36).

3. Hantering av risker för de registrerades rättigheter och friheter (artikel 35.7 c)

Det ska göras en uppskattning av riskens ursprung, art, särdrag och allvar (se skäl 84). Mer specifikt, för varje risk ur de registrerades perspektiv:

- Beaktande av riskens ursprung (skäl 90).
- Identifiering av möjliga konsekvenser för de registrerades rättigheter och friheter vid händelser, däribland obehörig åtkomst, oönskad ändring och förlust av uppgifter.
- Identifiering av hot som kan leda till obehörig åtkomst, oönskad ändring och förlust av uppgifter.
- Uppskattning av sannolikhetsgrad och allvar (skäl 90).
- Fastställande av planerade åtgärder för att hantera dessa risker (artikel 35.7 d och skäl 90).

Exempel på risker är obehörig åtkomst, oönskad ändring och att uppgifter försvinner.

4. Medverkan från berörda parter

Medverkan från berörda parter ska dokumenteran, här märks:

- Rådfrågan av dataskyddsombudet (artikel 35.2).
- När så är lämpligt, inhämtning av synpunkter från de registrerade eller deras företrädare (artikel 35.9).

5.6 Inhämta synpunkter från de registrerade?

Den personuppgiftsansvarige ska, när det är lämpligt, inhämta synpunkter från de registrerade eller deras företrädare om den avsedda behandlingen, utan att det påverkar skyddet av kommersiella eller allmänna intressen eller behandlingens säkerhet. Beroende på hur personuppgiftsbehandlingen är planerad att fungera kan man fråga på olika sätt. I vissa fall är det lämpligt med en enkät till allmänheten, ibland kan det vara bra att rådgöra med fackliga företrädare. För en skola kan det vara lämpligt att rådgöra med elevernas vårdnadshavare. Om den personuppgiftsansvarige och de registrerade inte har samma syn på behandlingen, ska det dokumenteras. Det är särskilt viktigt om man väljer att gå vidare med personuppgiftsbehandlingen. Om den personuppgiftsansvarige väljer att inte inhämta synpunkter från de registrerade, ska man dokumentera även det. Kanske är det inte lämpligt för att det skulle äventyra företagets affärsplaner, innebära oproportionerligt mycket arbete vara eller ogenomförbart av andra skäl.

5.7 Ska konsekvensbedömningen offentliggöras?

Det är inte ett rättsligt krav enligt förordningen att offentliggöra en konsekvensbedömning, utan detta är den personuppgiftsansvariges beslut. En upprättad konsekvensbedömning blir dock offentlig hos en kommun om det inte finns skäl att sekretessbelägga delar. Detta enligt reglerna i tryckfrihetsförordningen och offentlighets- och sekretesslagen.

5.8 Hur ska konsekvensbedömning följas upp?

Den personuppgiftsansvarige ska vid behov genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen avseende dataskydd åtminstone när den risk som behandlingen medför förändras. Personuppgiftsansvarige bör regelbundet och kontinuerligt se över och omvärdera

sina personuppgiftsbehandlingar för att bedöma om det bör genomföras en ytterligare konsekvensbedömning i fall om förhållanden har ändrats. Till exempel kan riskerna ha ändrats så att behandlingen nu sannolikt leder till en hög risk fast den inte gjorde det tidigare. Konsekvensbedömningen är en pågående process.

Konsekvensbedömning

En konsekvensbedömning har som syfte att förebygga risker när det kommer till dataskydd (Data Protection Impact Assessment - DPIA) för den enskildes fri-och rättigheter[2]. Det är en process som hjälper till att identifiera och minimera dataskyddsrisker i samband med en personuppgiftsbehandling.

Det är viktigt att konsekvensbedömningen är tillräckligt omfattande och grundligt gjord så att den fyller sin funktion och uppfyller dataskyddsförordningen. Den kan även komma att begäras ut av IMY vid tillsyn.

En konsekvensbedömning skall alltid genomföras om:

- En behandling av personuppgifter kan utgöra en hög risk för enskilda personers fri- och rättigheter
- Personuppgifter ska användas i nya sammanhang, i nya system dvs. innan nya personuppgiftsbehandlingar ska påbörjas
- Risken med en pågående personuppgiftsbehandling ändras
- Det inte finns någon gjord sedan tidigare på pågående personuppgiftsbehandlingar.

[2]Skäl 75, GDPR Risken för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av personuppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering eller annan betydande ekonomisk eller social nackdel, om registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter, om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter, uppgifter om hälsa eller sexualliv eller fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder behandlas, om personliga aspekter bedöms, framför allt analyser eller förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

Del I: Förhandsbedömning

En förhandsbedömning skall alltid genomföras för synliggöra om behandlingen sannolikt leder till en hög risk för de registrerades fri-och rättigheter. Vid hög risk skall en fullständig konsekvensbedömning genomföras.

Behandling

Datum	2024-01-31
Deltagare	Jenny Karlsson, GDPR-samordnare
Vilken personuppgiftsbehandling avses? *(Rubrik på den behandling som ska utföras)*	AV1 robotar
Ange den personuppgiftsansvarige	Barn- och utbildningsnämnden

Personuppgifter

Fråga	Ja	Nej
Omfattas behandlingen av några personuppgifter?	X	

Om du svarade ”ja”, fortsätt till nästa fråga.

Om du svarade ”nej” är en konsekvensbedömning inte nödvändig. Fortsätt till ”Attest”.

Kriterier för hög risk (storskalighet)

Kontrollera om behandlingen av personuppgifterna uppfyller någon av följande kriterier enligt artikel 35.3 samt skäl 71,72 och 91. Bedömning skall göras för att säkerhetsställa om personuppgiftsbehandlingarna sker i stor omfattning.

Kriterium	**Ja**	**Nej**
Sker storskalig behandling av känsliga personuppgifter eller lagöverträdelser (ex. domstolsbeslut)? Exempel: Med storskalig behandling menas mängden (1000-tals) registrerade samt mängden personuppgifter samt behandlingens varaktighet och geografiska omfattning. Det kan variera från fall till fall vad som betraktas storskaligt (exempelvis är storskaligt en kommuns samtliga elever eller anställda). 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. Uppgifter om lagöverträdelser är personuppgifter som rör någon som har begått ett brott, blivit fälld i domstol i ett brottmål, blivit föremål för så kallade straffprocessuella tvångsmedel till exempel häktning, reseförbud eller beslag etc.).		X
Sker systematisk och omfattande profilering av individer med betydande effekter (bedömning eller kategorisering av personer baserad på de registrerades personuppgifter, av individer med betydande effekter)? Exempel: Med ”profilering” menas i dataskyddsförordningen kategorisering eller skiktning (digitalt urval) av personer baserad på de registrerades personuppgifter. Varje form av automatisk behandling av personuppgifter används för att bedöma personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga dennes fysiska personens arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteenden, vistelseort eller förflyttningar (GPS-positionering) etc.		X

Sker systematisk övervakning av en allmän plats i stor omfattning? Exempel: kameraövervakning, internetövervakning, Wifi (samlar in uppgifter från enheter) etc.		X

Om en eller fler av frågorna besvaras med ”ja” krävs det en konsekvensbedömning. Om det är svårt att bestämma ja eller nej, välj heller ja.

Om behandlingen inte uppfyller någon av kriterierna är det fortfarande möjligt att det krävs en konsekvensbedömning (beroende på svaren i punkt 3 “Kriterium för hög risk (övrigt)”).

Kriterium för hög risk (övrigt)

Kontrollera om behandlingen av personuppgifterna uppfyller någon av följande kriterier enligt artikel 35.1 samt skäl 84,89,90 och 92. Bedömning skall göras för att säkerhetsställa om personuppgiftsbehandlingarna leder till en hög risk för den enskilde individen.

Svara på följande frågor.

Fråga	**Ja**	**Nej**
1. Kommer personer att analyseras, utvärderas, profileras eller poängsättas på något sätt? *Med profilering menas analys eller förutsägelser av särdrag som i synnerhet gäller arbetsprestationer, den ekonomiska situationen, personliga preferenser, intressen, pålitlighet, beteenden, position eller rörelser.* *Exempel: En profilering kan ske om en bank behandlar kreditklassuppgifter om lånesökanden för att fatta lånebeslut och en fysisk person avsevärt deltar i beslutsprocessen innan det slutliga lånebeslutet ges, DNA-analys hos biotechföretag som tjänst, beteendebaserad marknadsföring som analyserar beteenden och vad någon gör, personlighetstester inför anställning, psykologtester, positioneringsuppgifter med mobilapp, gps i tjänstebil etc.).*		**X**
2. Kommer det fattas automatiska beslut med rättsliga eller liknande betydande följder för personer? *Med automatiska beslut menas att en människa inte deltar i beslutsfattandet utan att beslutet fattas maskinellt utifrån en persons personuppgifter såsom automatiska kreditprövningar. Detta kan innebära*		**X**

att en person utesluts eller diskrimineras på grund av ett automatiskt beslut. Automatiska beslut kan inhämtas genom enkätformulär etc. *Exempel: robot fattar automatiserade beslut som avser beslut om ekonomiskt bistånd.*		
3. Kommer personer att övervakas på ett systematiskt sätt? *Exempel:* • *systematisk kameraövervakning* • *övervakning av nätverk,* • *övervakning av medarbetares surfbeteenden på arbetsenheter, hur anställda använder internet och e-post,,* • *en arbetsgivare inför ett inpasseringssystem för anställda som innefattar behandling av biometriska uppgifter i syfte att identifiera en viss fysisk person, t.ex. fingeravtrycksavläsning,* • *ett företag använder kundens lokaliseringsuppgifter, som till exempel inhämtas via en mobilapp, i syfte att rikta marknadsföring till kunden eller planera sina marknadsföringsstrategier,* • *en kommun samlar in personuppgifter innefattande bland annat lokaliseringsuppgifter i syfte att använda dessa vid exempelvis stads och trafikplanering*		**X**
4. Omfattar personuppgiftsbehandlingen känsliga personuppgifter eller extra skyddsvärda personuppgifter? *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 etc.* *Exempel på extra skyddsvärda personuppgifter är:* • *Personnummer* • *Samordningsnummer* • *Uppgifter om skyddade personer*		**X**

• *Uppgifter om ekonomisk situation* • *Uppgifter om civiltillstånd* • *Uppgifter om brott eller misstanke om brott* • *Uppgifter om social situation* • *Information om omfattas av sekretess/tystnadsplikt* • *Inkomst* • *Skulder* • *Omdömen och bedömningar* • *Prestationsmätningar* *Exempel: En kommun som behandlar personuppgifter i social omsorg.*		
5. Kommer personuppgifter att behandlas i stor omfattning? I förordningen definieras inte vad som avses med stor omfattning, även om viss vägledning ges i skäl 91. Artikel 29 arbetsgruppen rekommenderar i vart fall att följande faktorer beaktas särskilt vid bedömningen av huruvida behandlingen utförs i stor omfattning: • 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. Exempel: • Behandling av barns personuppgifter i skolverksamhet, om det är ett större antal registrerade. • En myndighet som, enskilt eller tillsammans med andra personuppgiftsansvariga, genom digitala plattformar ger service till befolkningen, vilket leder till storskalig personuppgiftsbehandling. • Vårdgivares behandling av personuppgifter om patienter i annat än ringa omfattning. Exempel på ringa omfattning är när en läkare är ensam verksamhetsutövare och behandlar uppgifter om sina 5 (6) patienter. Exempel på behandlingar av personuppgifter som INTE att anse som en behandling i "en stor omfattning": enstaka brukare, patienter till en läkare är inte storskaligt, inte heller enstaka besök hos andra yrkesverksamma inom hälsoområdet eller juridiskt ombud.		**X**

6. Kommer olika register att samköras (till exempel samkörning av två eller fler databaser)? Samkörning av två databaser som finns hos olika avdelningar men de har olika syften etc. Personuppgiftsansvarig kombinerar personuppgifter från två eller flera behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig, till exempel när man samkör register. Exempel: Verksamheter som utför bakgrundskontroller inför rekryteringar.		**X**
7. Behandlas personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara? Sårbara personer: ● Barn ● Anställda ● Psykiskt sjuka personer ● Asylsökande ● Äldre personer ● Patienter ● Personer med skyddad identitet Exempel: ● En organisation inför ett gemensamt system i vilket det är möjligt för anställda att anmäla missförhållanden på arbetsplatsen – ett s.k. visselblåsarsystem ● Behandling av barns personuppgifter i skolverksamhet	**X**	
8. Kommer ny teknik, nya organisatoriska lösningar, eller gammal teknik användas på ett nytt sätt som omfattar nya former av insamling och användning av personuppgifter? *Användningen av sådan teknik kan omfatta nya former av insamling och användning av uppgifter, eventuellt med hög risk för enskildas rättigheter och friheter. De personliga och sociala konsekvenserna av användningen av ny teknik kan vara okända.* *En konsekvensbedömning hjälper den personuppgiftsansvarige att förstå och hantera sådana risker. Till exempel kan vissa "internet of things (IoT)"-*	**X**	

applikationer få betydande konsekvenser för enskildas dagliga liv och integritet och således kräva en konsekvensbedömning.. *Exempel:* *Ett företag som tillhandahåller internetuppkopplade produkter för konsumenters bostäder (smarta hem-produkter), till exempel för att kunna fjärrstyra uppvärmning, belysning eller ljuduppspelning, samlar in detaljerade uppgifter om hur kunderna använder tjänsterna.* *Verksamheter inom social omsorg som använder välfärdsteknik, t.ex. robotar eller kamerabevakning i människors boende.* *Installation av smarta elmätare hos elabonnenter för att kunna ta fram, överföra och analysera uppgifter som rör konsumenter på en detaljerad nivå.* *Fingeravtryck med ansiktsigenkänning för inpassering.*		
9. Är det risk för att personuppgiftsbehandlingen i sig hindrar de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal? Detta omfattar behandlingar som syftar till att medge, ändra eller neka registrerade tillgång till en tjänst eller att ingå ett avtal. Ett exempel på detta är 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**

Krävs det en konsekvensbedömning?

Om en behandling av personuppgifter passar in i någon av kategorierna ovan kan det innebära att ni behöver göra en konsekvensbedömning. Om två eller flera av punkterna är uppfyllda ska man i de allra flesta fall göra en konsekvensbedömning. I tveksamma fall bör man alltid göra en konsekvensbedömning.

☒ Ja

☐ Nej

Beskriv och kommentera ditt svar nedan:

I risk- och sårbarhetsanalysen ser GDPR-samordnare att risken inte är hög, men utifrån att barns personuppgifter behandlas och det rör sig om relativt ny teknik bedöms att en konsekvensanalys behöver genomföras.

Del II: Konsekvensbedömning

1. Tidigare konsekvensbedömning (DPIA)

Detta är en:

☒ ny konsekvensbedömning

☐ komplement till en tidigare konsekvensbedömning (DPIA)

Är behandlingens art, omfattning, sammanhang och ändamål mycket lika en behandling för vilken en konsekvensbedömning tidigare har utförts?

☐ Ja

☒ Nej

☐ Inte säker

Beskriv och kommentera ditt svar nedan:

2. Kommer ny teknik, nya organisatoriska lösningar, eller gammal teknik användas på ett nytt sätt som omfattar nya former av insamling och användning av personuppgifter?

Exempel: Ny teknik är teknik som inte är så vanligt förekommande såsom ansiktsigenkänning, ögonavläsning eller automatiserade processer. Att använda molntjänster för lagring av data är inte ny teknik då den oftast baseras på databasregistrering.

☒ Ja

☐ Nej

3. Vad är syftet (ändamål) med behandlingen, varför behandlas personuppgifter

a) Syftet med behandlingen, övergripande bild

Exempel: Syftet med närvarokontrollen är att förenkla för de anställda att registrera sin arbetstid samt använda flextid, ha en bättre kontroll över arbetsbelastning och som resultat förbättra arbetsmiljö.

AV1-robotar är ett digitalt hjälpmedel för undervisning och inkludering i skolan som gör att ingen behöver missa lektioner, raster och samtal med vänner. AV1 placeras i klassrummet och eleven deltar från annan plats via surfplatta eller mobil. AV1 är utrustad med inbyggd kamera, mikrofon och högtalare som gör att eleven kan se, höra och prata med sin omgivning. Med hjälp av en app kan eleven vrida på roboten, interagera med klassen och delta i undervisningen ungefär som om hen vore där fysiskt. Syftet med riskanalysen och konsekvensbedömningen är att undersöka vilka risker och konsekvenser det innebär att använda AV1-robotar samt ta fram åtgärdsplan.

b) Syfte med behandlingen av användardata

Exempel: Effektivt verktyg för närvarokontroll för arbetsgivaren. Samla in statistik över användning för ekonomisk uppföljning.

Inloggning för att enskilda elever ska kunna använda AV-robotarna.

4. Vilka kategorier av personuppgifter omfattas av behandlingen?

Det finns tre kategorier (grupper) av personuppgifter: harmlösa, extra skyddsvärda och känsliga. Här svarar du på frågan om harmlösa (vanliga) personuppgifter.

Vanliga personuppgifter	**Extra skyddsvärda personuppgifter**	**Känsliga personuppgifter eller uppgifter om brott**
❑ **Namn/efternamn** ❑ Telefonnummer ❑ Adress ❑ Födelsedatum ❑ E-postadress ❑ Anställningsnummer ❑ Medlemsnummer ❑ IP-adress ❑ Kontonummer ❑ Fakturanummer ❑ Användar-ID ❑ Passnummer ❑ Bostadsadress ❑ SIM-kortsnummer ❑ Uppgift om anhöriga ❑ Stöldskyddsnummer ❑ Inloggningsuppgifter ❑ Teknisk metadata ❑ Annan	❑ Personnummer ❑ Samordningsnummer ❑ Skyddade personuppgifter ❑ Ekonomisk situation ❑ Civiltillstånd ❑ Uppgifter om brott eller misstanke om brott ❑ Uppgifter om social situation ❑ Information om omfattas av sekretess/tystnadsplikt ❑ Inkomst ❑ Skulder ❑ Omdömen och bedömningar ❑ Prestationsmätningar ❑ **Annan**	❑ 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 ❑ Biometriska uppgifter ❑ Uppgifter om brott är personuppgifter om lagöverträdelser om någon har begått ett brott, blivit fälld i domstol i ett brottsmål, blivit föremål för så kallad straffprocessuella tvångsmedel, till exempel häktning, reseförbud eller beslag etc.)

Motivera om du valt "annan":	Motivera om du valt "annan": **<u>Ljud- och videoupptagning av personal och barn/elever</u>**	X

5. Från vilka källor inhämtas personuppgifterna?

Med källa menas det ställe som uppgifternas insamling ursprunglig kommer hämtas ifrån. Exempel: systemet är källan som uppgifterna hämtas ifrån exempelvis AD-systemet "Active directory och uppgifterna delas vidare till ett antal andra verksamhetssystem.

☒ Den registrerade själv

☐ Annan än den registrerade (Skatteverket, SCB, en annan person osv.)

☐ Annat

6. Omfattas sårbara kategorier av registrerade av behandlingen?

I vissa fall behandlas det personuppgifter gällande extra sårbara kategorier av registrerade som kräver extra skydd. Detta gäller personer som av något skäl befinner sig i underläge eller i beroendeställning gentemot personuppgiftsansvarig. Denna kategori av registrerade anses som sårbara, till exempel barn, anställda, asylsökande, äldre, personer med skyddad identitet, patienter.[3]

☒ Barn

☒ Anställda

☐ Psykiskt sjuka personer

☐ Asylsökande

☐ Äldre personer

☐ Patienter

☐ Personer med skyddad identitet

7. Vilka andra kategorier av registrerade omfattas av behandlingen?

Nu har du svarat på frågan om sårbara kategorier av registrerade men det finns andra kategorier som vi behöver veta om. Ange vilka andra kategorier av registrerade (personer) som omfattas av arbetsprocessen.

[3] Förteckning enligt artikel 35.4 i Dataskyddsförordningen, DI, 2019-01-16, DI-2018-13200, s. 3

☐ Anhöriga

☐ Förtroendevalda

☐ Besökare

☐ Medlemmar

☐ Konsulter

☐ Medborgare

☐ Elever över 18 år gamla

☐ Brukare

☐ Klienter

☐ Fastighetsägare

☐ Boende

☐ Övriga

Beskriv och kommentera ditt svar nedan:

8. Hur många registrerade omfattas av behandlingen?

Uppskatta gärna hur många registrerade som omfattas av behandlingen:

☐ 1- 10

☐ 11 - 100

☒ 101 - 1000

☐ 1001 - 5000

☐ 5001 - 10000

☐ 10001 - 50000

☐ 50001 eller fler

☐ Annat

Beskriv och kommentera ditt svar nedan:

9. Tillgång till personuppgifter (internt inom kommun/bolag)

Vilka tjänstepersoner och andra roller kommer ha tillgång till uppgifterna?

☐ En person

☐ Ett fåtal medarbetare

☐ Personal inom enheten

☒ Personal inom förvaltningen

☐ Personal inom kommunen

☐ IT-administratörer

☐ Annan

Beskriv och kommentera ditt svar nedan:

Inga uppgifter lagras men personal kommer känna till vilka som har en robot.

10. Kommer personuppgifterna att delas med någon (externt)?

Välj alla kategorier som personuppgifterna kan delas med.

☐ Leverantörer (support, lagring, utveckling, metadat, loggar annat)

☐ Myndigheter (Skatteverket, Försäkringskassan, SCB, annat)

☐ Allmänhet

☐ Andra system

☐ Annat

Beskriv och kommentera ditt svar nedan:

Nej

11. Vilka rättsliga grunder finns för behandlingen av personuppgifter?

Det finns sex rättsliga (lagliga) grunder:

Uppgift av allmänt intresse eller som ett led i myndighetsutövning: När en kommun är ansvarig för något område och det framgår av lagar/regler. Kommunen är till exempel ansvarig för att bedriva skolverksamhet enligt skollagen (hantering av klasslistor, hantering av elevernas närvaro osv.). Kommunen är ansvarig för biblioteksverksamhet enligt bibliotekslagen (hantering av lånekort).

Rättslig förpliktelse: En behandling för att uppfylla krav som nationell lagstiftning kräver, exempelvis bokföringslag, skollag och arkivlag. Exempel: Betygssättning enligt bestämmelser i skollagen.

Avtal: Anställningsavtal, hyresavtal där registrerade är en part i avtalet (hantering av anställdas löner).

Samtycke: Kan användas när ingen annan rättslig grund passar. Samtycke kan återkallas när som helst. Samtycke kan ej användas mot de registrerade som befinner sig i beroendeställning gentemot den personuppgiftsansvarige (anställda, elever, patienter, omsorgstagare, brukare osv.).

Skydda intressen som är av grundläggande betydelse: Kan användas i akuta fall, när den registrerade inte kan samtycka till behandlingen till exempel på grund av medvetslöshet.

Berättigat intresse (intresseavvägning): Kan ej användas av myndigheter när de fullgör sina uppgifter.

Ange den rättsliga grunden för varje ändamål (syfte) som tidigare angetts i konsekvensbedömningen ovan. Motivera och argumentera samt ange paragraferna i det nationella lagstödet eller uppge vilka politiska beslut som finns. Har ni nationellt beslut finns det stöd i förordningen nedan, ange rätt grund.

Rättsliga (lagliga) grunder i artikel 6 dataskyddsförordningen:

☐ Uppgift av allmänt intresse eller som ett led i myndighetsutövning

☐ Rättslig förpliktelse

☒ Avtal

☐ Samtycke

☐ Skydda intressen som är av grundläggande betydelse

☐ Berättigat intresse (intresseavvägning)

12. Hur kommer funktions- eller ändamålsglidning förhindras?

Med ändamålsglidning menas att personuppgifterna används till ett annat syfte än vad som var tanken från början. Vilka åtgärder kommer att vidtas för att minska risken för funktions-eller ändamålsglidning?

☒ Interna rutiner,

☐ Utbildning,

☐ Behörighetsstyrning,

☐ Biträdesavtal kring support och uppdateringar,

☐ Granskning av personuppgiftsbiträdet (begära ut loggar över åtkomst till individens data)

☐ Andra

Beskriv vilka andra åtgärder kommer att vidtas.

Båda parter ingår ett avtal, med roboten följer tydliga instruktioner för användare och personal.

13. Hur säkerställs att personuppgifterna är korrekta?

Personuppgifter som behandlas ska vara riktiga och, om nödvändigt, uppdaterade. Om personuppgifterna inte stämmer ska ni rätta eller radera dem. Det är därför viktigt att det finns rutiner på plats för att kunna korrigera och ta bort oriktiga personuppgifter, till exempel om en registrerad begär det.

☒ Genom interna rutiner

☐ Korrekta upphandlingskrav vad gäller riktighet

☐ Kontinuerlig kontroll av personuppgifter

☐ På annat sätt.

Beskriv vilka andra åtgärder kommer att vidtas.

Inga personuppgifter lagras förutom namn på avtal. Elevers och vårdnadshavares namn har förvaltningen tillgång till via folkbokföringen. Om en registrerad begär det kan avtalet ändras eller avslutas.

14. Hur kommer uppgiftsminimering säkerställas?

Personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till syftet (ändamålet). Ni ska aldrig behandla fler personuppgifter än vad som behövs, och de personuppgifter som behandlas ska vara tydligt kopplade till syftet (ändamålet). Det är med andra ord inte tillåtet att samla in personuppgifter för obestämda framtida behov, för att de kan vara "bra att ha".

☒ Genom interna rutiner,

☐ Utbildningar för anställda

☐ Tekniska inställningar som förhindrar behandling av onödiga personuppgifter

☐ På annat sätt

Beskriv hur uppgiftsminimering säkerställs?

Inga personuppgifter lagras förutom namn på avtal.

15. Hur kommer lagringsminimering säkerställas?

Ni får bara spara personuppgifter så länge som de behövs för ändamålet med personuppgiftsbehandlingen. När personuppgifterna inte längre behövs för ändamålet ska ni radera eller avidentifiera dem. Ni bör därför införa rutiner för gallring av personuppgifter, till exempel att ni genomför regelbundna kontroller eller raderar efter en viss tid. Det kan också vara tillåtet att lagra personuppgifter, efter att det ursprungliga ändamålet slutar att vara aktuellt, om det endast sker för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål. Ni måste dock alltid se till att vidta lämpliga säkerhetsåtgärder för att skydda personuppgifterna.

☐ Genom att ta fram en dokumenthanteringsplan/gallringsplan/ informationshanteringsplan

☐ Genom att uppdatera dokumenthanteringsplan regelbundet, t. ex. en gång per år

☐ Utbildningar

☐ På annat sätt

Beskriv hur lagringsminimering säkerställs?

Inga personuppgifter lagras förutom namn på avtal. Avtalet gallras vid avslut.

16. Hur länge kommer personuppgifterna sparas (lagras)?

Exempel: Viktigt att hänvisa till dokumenthanteringsplan men informationen ska specificeras nedan. Saknas gallringsbeslut ska detta uppdateras snarast och vara en del av konsekvensbedömningsarbetet.

Beskriv hur länge kommer personuppgifterna kommer att lagras (både användardata och loggdata).

Inga personuppgifter lagras förutom namn på avtal. Avtalet gallras vid avslut.

17. På vilket sätt får de registrerade information om behandlingen av personuppgifter?

De registrerade ska alltid få information om hur och för vilket ändamål uppgifterna används, även om behandlingen inte grundar sig på samtycke. Informationen ska lämnas vid första interaktionen med användaren. Den ska alltid finnas tillgänglig varje gång den registrerade (användaren) använder tjänsten.

Informationen lämnas ut:

☐ På blanketter

☐ På hemsidan

☐ I e-tjänster

☒ På annat sätt

Beskriv och kommentera ditt svar nedan.

I samband med underskrift av avtal.

Bifoga informationstexten som de registrerade ska få/har fått som bilaga till det här dokumentet. Om informationstexten hänvisar till en generell policy eller webbplats ska även den texten infogas nedan.

Om de registrerade inte ska informeras förklara varför.

18. Kan den registrerade förvänta sig att dennes personuppgifter används i andra syften som inte omfattas av huvudbehandlingen?

Exempel : Vid användning av e-post samlas och lagras även loggdata och metadata om den enskilde vilket den enskilde inte kan förvänta sig. Man förväntar sig till exempel inte insamling av information om vilka möte har den enskilde deltagit i, hur länge, vilka tjänster den enskilde använder osv.

☐ Ja

☒ Nej

Beskriv och kommentera ditt svar nedan:

19. Vilka åtgärder vidtar den personuppgiftsansvarige för att se till att eventuella personuppgiftsbiträden uppfyller kraven?

Om en behandling ska genomföras på en personuppgiftsansvariges vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.

☐ Klassning av system i "KLASSA"

☐ Kravställande vid upphandlingen

☒ PUB-avtal

☐ Kontinuerliga granskningar av personuppgiftsbiträde

☐ Granskning av nya underbiträden

☐ Annat

Beskriv och kommentera ditt svar nedan:

20. Har leverantören anmält sig till någon godkänd uppförandekod eller certifiering?

En uppförandekod är ett slags regelbok om behandling av personuppgifter som utarbetats av och frivilligt tillämpas inom till exempel en viss bransch. En certifiering ska göras av ett ackrediterat

certifieringsorgan. I Sverige ansvarar det nationella ackrediteringsorganet Swedac för ackreditering av certifieringsorgan. De kriterier som en ackreditering ska grunda sig på tas fram av den nationella tillsynsmyndigheten, alltså av Integritetsskyddsmyndigheten. Integritetsskyddsmyndigheten ska även godkänna de kriterier som ligger till grund för en certifiering.

☐ Ja

☒ Nej

Beskriv och kommentera ditt svar nedan. Vilken godkänd uppförandekod eller certifieringsordning?

21. Överförs personuppgifter till tredjeland eller internationell organisation?

Det finns strikta regler i dataskyddslagstiftningen för när personuppgifter får lämnas till länder utanför EU/EES, så kallat tredjeland. Detta gäller all överföring, även till personuppgiftsbiträden som inte själva använder personuppgifterna i sin verksamhet utan bara lagrar, driftar, supportar, utvecklar, underhåller eller servar systemet. Observera att ordet överföring även omfattar åtkomst till personuppgifterna i tredjeland, även om de lagras inom EU/EES.

Om du svarar ja på en av de fem frågorna så betyder det att personuppgifter överförs till tredje land:

- När ett dokument som innehåller personuppgifter skickas till någon i ett land utanför EU/EES via e-post
- När ett personuppgiftsbiträde anlitas i ett land utanför EU/EES.
- När någon utanför EU/EES får tillgång, exempelvis läsbehörighet, till personuppgifter som finns lagrade inom EU/EES.
- När personuppgifter lagras i en molntjänst som är baserad utanför EU/EES.
- När personuppgifter lagras, till exempel på en server, i ett land utanför EU/EES.
- När det finns ett ägarintresse i tredje land (exempel: när amerikanskt bolag äger servrar som är placerade inom EU/EES omfattas bolaget (även dotterbolag) fortfarande av amerikansk lagstiftning).

Sker överföring av personuppgifter till tredjeland?

☐ Ja

☒ Nej

Beskriv och kommentera ditt svar nedan:

22. Om personuppgifter överförs till tredjeland eller internationell organisation, vilken mekanism används för tredjelandsöverföringen?

Enligt dataskyddsförordningen är det förbjudet att överföra personuppgifter till länder som ligger utanför EU/EES (så kallade tredje länder). Det finns dock undantag som framgår av art. 44-49 i dataskyddsförordningen.
Exempel: Om personuppgifter ska föras över till ett tredjeland dvs utanför EU/EES måste skyddet för fysiska personer säkerhetsställas genom att personuppgiftsbehandlingen har rätt skyddsnivå. Detta kan gälla sociala medier eller molntjänster som driftas i Europa.

Välj mekanism för tredjelandsöverföringen:

- Adekvat skyddsnivå - EU-kommissionen kan fatta beslut om att ett land har en tillräckligt hög skyddsnivå.

- Standardavtalsklausuler som EU-kommissionen har beslutat om.
- Om ni använder denna överföring svara på fråga 5.2.11

- Godkända uppförandekoder eller certifieringsmekanismer
- Ange uppförandekod/certifieringsmekanism: _____

- Rättsligt bindande instrument mellan myndigheter
- Ange de bindande instrumenten:_____
- Tillstånd från tillsynsmyndigheten
- Överföring sker med stöd av undantagen i artikel 49

Beskriv och motivera vilket undantag i artikel 49 som gäller för

överföringen: _____

Det finns även bindande företagsbestämmelser (*ej aktuella för kommuner eller kommunala bolag, regleras i artikel 47):* Bindande företagsbestämmelser (Binding Corporate Rules, BCR) är regler som en företagskoncern med bolag i flera olika länder kan ta fram för att reglera sin behandling av personuppgifter.

23. Om standardavtalsklausuler används som mekanism för tredjelandsöverföring

Finns det risk att lagarna i det tredje landet hindrar de registrerade från att utöva sina fri-och rättigheter (exempelvis finns inga rättigheter att få sin sak prövad i domstol, landet bryter mot de mänskliga rättigheterna)?

Vilka extra skyddsåtgärder behöver vidtas? *Extra skyddsåtgärder (avtalsåtgärder, organisatoriska och tekniska) länkas här: EDPB rekommendationer*

Beskriv vilka åtgärder som kommer att vidtas för att säkerställa adekvat skyddsnivå. (Exempel: Vilka säkerhetsåtgärder kommer vidtas utifrån EDPB:s rekommendationer för att säkerställa skyddsnivån för personuppgifterna)

24. Finns det några aktuella problem av allmänt intresse som ni borde ta hänsyn till?

Exempel: Förändrat världsläge, oviss lagstiftning ex. nya lagar tillkommer som gör det helt omöjligt att föra över personuppgifter av känslig karaktär som lyder under offentlighets- och sekretesslag eftersom det kan detta leda till sekretessbrott. Aktuellt kan vara att avtal förändras/faller mellan länder, BREXIT, ogiltigförklarandet av Privacy Shield etc.

☐ Ja

☒ Nej

Beskriv och kommentera ditt svar nedan.

25. Finns det tidigare kända problem med denna typ av behandling alternativt säkerhetsbrister?

Exempel: Det handlar om händelser som är kända sedan tidigare, granskningar hos myndigheter, brister hos leverantörer, standardavtal som inte kan omförhandlas av kommun/bolag, hänsyn till lagstiftning ”CLOUD ACT; FISA; Privacy Shield”, att en behandling är under granskning av IMY.

Beskriv och kommentera ditt svar nedan. Ange vilka problem eller säkerhetsbrister som har identifierats.

26. Beskriv flödet av personuppgifter och/eller helst bifoga i bildformat)

Exempel på hur ett flödesschema kan beskrivas:

- AD-system föder uppgifter
- Leverantör och underleverantörer får tillgång
- Behörigheter skapas på IT-avdelning men beställs av chef
- Chef, systemförvaltare, personalkontor, medarbetare får tillgång till konto
- Registreringar görs löpande från olika enheter och platser
- GPS-position samlas in
- Chef kontrollerar/verifierar och attesterar uppgifter
- Rapport sammanställs varje kvartal till chef med loggdata
- Gallring sker automatiskt i systemet

- Uppgifterna överförs till arkiv etc.

Beskriv flödet av personuppgifter och/eller bifoga underlag.

- AV1 överför en livesändning av ljud och video. Inga personuppgifter lagras.
- Livesändningen som visas genom AV1 är end-to-end-krypterad. Det betyder att innehållet inte kan visas för någon annan än den dedikerade AV1-användaren.
- AV1-appen är skyddad med ett lösenord så att det endast är den dedikerade användaren som kan logga in.
- Endast en enhet (surfplatta/mobil) kan användas med en AV1. Ett nytt nyckelord krävs för att synkronisera en enhet till AV1. Detta nyckelord skickas säkert ut till kunden av oss på No Isolation.
- No Isolation kräver eller lagrar inte information om våra användare (elever) som t.ex. ålder, namn, eller sjukdom.

27. Uppnår behandlingen faktiskt de avsedda syften (ändamålen)?

☒ Ja

☐ Nej

Beskriv och kommentera ditt svar nedan.

28. Är det möjligt att uppnå syftet med behandlingen som innebär ett mindre intrång i den personliga integriteten?

Vid en bedömning av om behandlingen är proportionerlig måste behovet av att genomföra behandlingen vägas mot intrånget i den enskildes personliga integritet. Finns det andra mindre ingripande sätt för personuppgiftsbehandlingen som uppnår samma resultat.

Exempel: Syftet med GPS-positionering är att kontrollera om person varit på rätt plats vid rätt tillfälle. Detta kan kontrolleras genom mindre ingripande åtgärder genom att föra dialog med individen samt utvärdera till exempel arbetsresultat. Syftet kan därmed uppnås med mindre intrång i den enskildes integritet.

Beskriv och kommentera ditt svar nedan.

Nej, personuppgiftshanteringen minimeras redan

29. Samråd med berörda parter

Beskriv när och hur ni kommer att söka personernas åsikter, eller motivera varför det inte är lämpligt att göra det. Vem behöver projektet involvera inom verksamheten? Behöver verksamheten be leverantörer att hjälpa till? Finns det planer på att ta kontakt med informationssäkerhetssamordnare, jurister eller andra experter?

☐ Dataskyddsombud

☐ Personalansvarig

☐ Informationssäkerhetsansvarig

☐ IT-säkerhetsansvarig

☐ Stadsjurist/arbetsrättsjurist

☒ Leverantör

☒ Systemförvaltare

☐ Annat

Beskriv och kommentera ditt svar nedan.

Del III: Bedömningsmodell för konsekvensbedömningen

Riskanalysen är gjort efter den modell som tagits fram av IT-enheten. Det innebär att sannolikhet och konsekvens bedöm enligt de skalor som redovisas i tabellerna nedan:

Mycket osannolikt	**1**	I det närmaste otänkbart att risken inträffar Inträffar mer sällan än var femte år, alt Nästan omöjligt att förverkliga risken genom att utnyttja systemets egenskaper (T ex Stöld av dokument från rum med två-faktors inpasseringssystem)
Osannolikt	**2**	Risken inträffar inte under normala omständigheter Inträffar oftare än var femte år men mer sällan än varje år, alt Svårt att förverkliga risken genom att utnyttja systemets egenskaper (T ex Stöld av dokument från rum med en-faktors inpasseringssystem)
Sannolikt	**3**	Risken kan mycket väl inträffa Inträffar oftare än varje år men mer sällan än varje månad, alt Möjligt att förverkliga risken genom att utnyttja systemets egenskaper (T ex Stöld av dokument från kontor med en- faktors inpasseringssystem)

Mycket sannolik	**4**	Risken är så stor att det närmast är en tidsfråga innan den inträffar Inträffar oftare än varje månad alt. Lätt att förverkliga risken genom att utnyttja systemets egenskaper (T ex Stöld av pappersdokument från en hotellobby)

Del IV: Konsekvensgrader och värde

Ingen eller försumbar skada	**1**	• 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
Måttlig skada	**2**	• Den registrerades fri- och rättigheter kan inte garanteras • Den registrerade uppleva lindriga besvär • Måttlig ekonomisk eller social påverkan • Oklart juridiskt läge / utredning krävs
Betydande skada	**3**	• 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
Allvarlig skada	**4**	• 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

Del V: Sannolikhet och allvarlighetsgrad

Allvarlighetsgrad **Sannolikhet**	**Allvarlig skada (4)**	**Betydande skada (3)**	**Måttlig skada (2)**	**Ingen eller försumbar skada (1)**
Mycket osannolikt (1)	4	3	2	1
Osannolikt (2)	8	6	4	2
Sannolikt (3)	12	9	6	3
Mycket sannolik (4)	16	12	8	4

Del VI: Risknivåer och accepterat riskvärde

Ett accepterat riskvärde är upp till 4. Ett riskvärde över 4 kräver åtgärd. Tabellen nedan visar vilka risknivåer som har använts under denna riskanalys:

Riskvärde	Risknivå	Åtgärd
1-4	Låg risk	Ingen åtgärd, riskvärdet är acceptabelt
5-11	Medelhög risk	Åtgärder tas fram och risken bevakas, riskvärdet får ej stiga
12-16	Hög risk	Kan ej accepteras. Skall åtgärdas och värdet sänkas. Förhandssamråd från tillsynsmyndigheten kan övervägas.

Del VII: Riskanalys DPIA

Nr.	Riskanalys DPIA					Kommentar sannolikhet	Kommentar konsekvens	Åtgärds-förslag	Riskvärde efter åtgärd	Nästa steg/ Beslut inkl. ansvarig samt datum
Nr	Riskformulering	Konsekvenser för den registrerade	Sanno-likhet (1-4)	Konse-kvens (1-4)	Risk-värde SxK=?	Motivera sannolikhet	Motivera konsekvens	Åtgärder för att minska risken för registrerade	Ange nytt riskvärde enligt modell S (1-4) x K (1-4) = ?	Dokumentera bedömningen samt utse ansvarig och datum för utförd åtgärd
Inre risker till exempel inom den egna organisationen										
1	Filmning eller inspelning av video eller ljud.	Inspelningar av läraren eller andra elever i klassen som publiceras på nätet. Foton/videor på elever och lärare delas online utan samtycke.	2	3	6	Det är liten risk för att ett barn i behov av en AV1 kommer att bryta mot användarvillkoren.	Konsekvensen blir att elever eller lärare förlorar kontrollen över sina personuppgifter	AV1s användarvillkor, so användaren eller denne vårdnadshavare måste acceptera innan användning, förbjuder detta beteende. VH och elev informeras om konsekvenserna av att bryta mot dem. Appen tillåter inte skärmdumpar. Inspelning måste göras med en annan enhet, till exempel en smartphone	2	

								Skärmen i appen blir svart om en användare tar en skärmdump. Du måste kontakta No Isolation för att komma åt AV1 igen efter att ha försökt ta en skärmdump. Det är lättare att spela in i klassrummet än via AV1. Om en inspelning/skärmdump laddas upp online kommer en advokat från No Isolation att skicka ett "Cease & Desist"- brev till det sociala medieföretaget och personen som laddade upp materialet. Detta brev hotar med rättsliga åtgärder om inte inlägget raderas. Dessutom ber skolan ansvarig att ta bortinlägget, och/eller anmäla inlägget på sociala medier.		
2	Användaren ser eller hör saker via AV1 som den inte	AV1-användaren hör ett privat	2	2	4	Rutiner för när och hur AV1 ska användas minimerar risken	Konsekvensen blir att elever eller lärare	AV1 stängs av och laddas i slutet av skoldagen.	2	

	borde ha hört eller sett.	samtal eller är påkopplad på opassande platser (t.ex. i lärarrummet).					förlorar kontrollen över sina personuppgifter	AV1 stängs in i en garderob, i ett annat rum, eller är avstängd när den inte används. AV1 används under fasta tider på schema, så att eleven loggar in först när lektionerna eller rasterna startar.		
3	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.	2	3	6	Det är väldigt liten sannolikhet för att barnet kommer att vara uppkopplad på AV1 samtidigt som hen har ett läkarsamtal eller privat samtal.	Konsekvensen blir att eleven förlorar kontrollen över sina personuppgifter	AV1 kan ställas in på "tyst läge". När roboten är i tyst läge kommer inte klassen att höra någonting från hemmet eller användaren. Informera barnet om funktionen "tyst-läge innan hen använder AV1. Se till att uppstartsguiden är läst och förstådd. Användaren och dennes föräldrar informeras om hur AV1 fungerar och hur ljud överförs till klassrummet. Eleven rekommenderas att		

								endast använder AV1 i ett tyst rum där eleven kan vara ensam och arbeta ostört. Om klassen hör någonting de inte borde, stängs AV1 av så snart som möjligt.		
4	AV1 används av någon annan än den dedikerade användaren	Föräldrar, syskon, kompisar eller någon annan loggar in på AV1-appen och klassen känner inte denna person.	2	2	4	Det är liten risk med tanke på inloggningsppgifter och användarvillkor som godkänns.	Konsekvenserna är inte stora då sannolikheten att den obehöriga personen hör känslig information är låg.	För att aktivera AV1 för första gången måste eleven skriva in en unik kod på 8 siffror. Barnet och föräldrarna informeras om användarvillkoren. Denna kod synkroniserar deras surfplatta/ smarttelefon med den dedikerade AV1-roboten. Denna kod ges till kundkontakten (ansvarig lärare eller liknande) som ska se till att AV1 ges till rätt elev. Användarvillkoren för AV1 måste accepteras innan användning och därmed säkerställa att användaren	4	

								endast är det barn som AV1 är ansluten till (dvs den elev som har appen). AV1-appen kan endast öppnas genom att eleven anger en unik PIN-kod som hen själv valt. Denna kod ska hållas hemlig så att det bara är användaren som känner till den. Vid misstanke att någon annan än barnet använder roboten kan frågor ställas till AV1. Om man inte får svar och fortfarande är osäker, kan roboten stängas av. Vid fortsatt osäkerhet kan No Isolation kontaktas för att generera ett nytt lösenord för att synkronisera roboten och surfplatta/smarttelefonen på nytt. Därefter måste eleven välja en ny PIN-kod		
5	AV1s krypterade live-sändning	Live-sändningen ses	1	3	3	AV1 streamar med WebRTC, vilket innebär att all media som	Personuppgifterna som en eventuell hackare	Vid misstänke att någon har hackat	3	

	hackas av externa personer.	eller spelas in av en annan enhet utan att klassen eller läraren är medvetna om det.				skickas är end-to-end-krypterad genom krypteringsprotokollet (SRTP/ DTLS). Streamen sänds då endast mellan användare och robot, och nekar externa personer att ansluta. Amazon/AWS är en säker, branschledande leverantör som säkerställer att att ingen tredje part, inte ens No Isolation, kan ansluta till streamen.	skulle kunna komma åt är eventuellt videoupptagning av elever och lärare. Inga känsliga personuppgifter.	AV1, kontaktas No Isolation. No Isolation övervakar ständigt alla servrar för hackningsförsök och har hittills aldrig blivit hackade. I det mycket osannolika fallet att servrarna hackas, kommer No Isolation att rapportera detta till lämpliga myndigheter inom 72 timmar. De har interna riktlinjer för sådana incidenter, även om det, igen, är mycket osannolikt att det inträffar.		

Del VIII: Godkännande

Bedömning genomförd av:	Jenny Karlsson, GDPR-samordnare barn- och utbildningsförvaltningen Gnesta kommun. 2024-01-31
Godkänd av ansvarig chef:	Ange namn/sign och datum