REFERENSKONSEKVENSBEDÖMNING
Trafikanalys med multisensorer
VERSION 1.0

Tillväxt och Samhällsbyggnad
Bo Baudin

Certezza AB
Andreas Dahlqvist
Thomas Nilsson

Referenskonsekvensbedömning – trafikanalys med multisensorer

Revisionshistorik

Revisions-nummer	Kapitel	Orsak till revidering	Sakgranskad av

Innehåll

Ordlista

Här följer en kort ordlista över begrepp såsom de används i denna referenskonsekvensbedömning.

Anonymisering	Behandling som innebär att personuppgifter i rådata med avidentifieringsmetoder förstörs eller förvanskas på ett sätt att det inte går att härleda till en viss fysisk person.
Avidentifiering	Metod för att anonymisera personuppgifter så att enskilda inte längre kan identifieras.
Gallra	Att radera eller på annat sätt förstöra personuppgifter så att de inte kan återskapas.
Informationsägare	Den enhet eller funktion som har nytta av och använder registrerade data för de angivna ändamålen.
Multisensor	En enhet som innehåller flera sensorer som kan mäta flera olika parametrar. I denna framställning ingår även kamerafunktionalitet.
Multisensorsytem	Multisensorer och till dessa anslutande analysverktyg, kommunikationsprotokoll, gränssnitt och fysiska anslutningar.
Personuppgiftsansvarig	Kommunal nämnd eller annat kommunalt organ som bestämmer ändamålen med behandlingen
Registrerad	En fysisk person vars personuppgifter behandlas i ett multisensorsystem.
Rådata	Oredigerad och oförvanskad film eller annan data som kan innehålla personuppgifter

Läs detta först!

Detta dokument är en referenskonsekvensbedömning som är tänkt att användas inför användning av multifunktionssensorer med kamerabevakningsfunktion (multisensorer). Dokumentet kan bland annat användas som stöd vid ansökningar om kamerabevakningstillstånd.

I varje enskilt fall måste en personuppgiftsansvarig granska sin egen planerade behandling och bedöma om innehållet i denna referenskonsekvensbedömning kan appliceras på dessa behandlingar och att de ingående värdena är relevanta för den nyttjande parten.

Om den planerade behandlingen inte helt stämmer överens med vad som omfattas av denna referenskonsekvensbedömning kan du som personuppgiftsansvarig behöva ta fram en kompletterande konsekvensbedömning och göra andra nödvändiga justeringar.

Organisationens dataskyddsombud ska alltid vara med i processen inför och vid genomförande av konsekvensbedömningar.

Den som hänvisar till denna referenskonsekvensbedömning ska se till att de åtgärder som anges häri också genomförs.

Inledning

Den tekniska utvecklingen har lett till att trafiken i den offentliga miljön kan analyseras med ny avancerad teknik i form av exempelvis multifunktionssensorer med kamerabevakningsfunktion (multisensor). Dessa sensorer kan skapa stora nyttor för kommuner och regioner, men innebär samtidigt risker för fysiska personers rättigheter och friheter.

Denna referenskonsekvensbedömning är tänkt att utgöra ett stöd för kommuner och regioner som vill använda multisensorer för att analysera och använda uppgifter om trafikflöden till samhällets nytta.

En konsekvensbedömning är en process

En konsekvensbedömning är en process avsedd att beskriva en behandling, bedöma om den är nödvändig och proportionell och hjälpa till att hantera risker för fysiska personers rättigheter och friheter som uppkommer genom behandlingen av personuppgifter. Detta görs genom att bedöma riskerna och bestämma vilka åtgärder som ska vidtas, dokumentering, samt kontinuerlig övervakning och översyn.

Konsekvensbedömningen är ett viktigt verktyg för utkrävande av ansvar, eftersom den inte bara hjälper personuppgiftsansvariga att uppfylla kraven i dataskyddsförordningen, utan även visar på lämpliga åtgärder som ska vidtas för att säkerställa efterlevnaden av förordningen.

Med andra ord är en konsekvensbedömning en process för att skapa och påvisa efterlevnad. Processen kan beskrivas med följande figur.

Figur 1 Process för konsekvensbedömning

Syftet med konsekvensbedömningen

Syftet med konsekvensbedömningen är dels att skapa förtroende för personuppgiftsansvarigas behandlingar, visa ansvar och transparens. Dels att systematiskt studera användning av multisensorer i trafikmiljö som kan medföra en hög risk för personers rättigheter och friheter. Dels att uppmärksamma dessa risker samt hantera riskerna så att risken minimeras, säkerställa personuppgiftsskyddet och att dataskyddsförordningen efterlevs.

För att skapa förtroende för bedömningarna är syftet också att göra konsekvensbedömningen i sin helhet allmänt tillgänglig och offentlig så att enskilda registrerade kan ta del av den och för SKR:S medlemmar att använda.

En enda referenskonsekvensbedömning

Det är möjligt att en enda konsekvensbedömning kan användas för att bedöma flera behandlingar som liknar varandra vad gäller art, omfattning, innehåll, ändamål och risker. Det finns inget behov av att utföra en konsekvensbedömning i situationer som redan har studerats. Så kan vara fallet när liknande teknik används för att samla in samma slags uppgifter för samma ändamål. Detta kan också göras för liknande

behandlingar som planeras av olika personuppgiftsansvariga. I dessa fall bör en referenskonsekvensbedömning delas eller göras allmänt tillgänglig.[1]

Denna referenskonsekvensbedömning ska göras allmänt tillgänglig och studerar de behandlingar som en enskild kommun eller kommunal nämnd kan komma att göra när den använder multifunktionssensorer med kamerabevakningsfunktion (multisensorer) på allmänna platser för att analysera trafik, miljö och miljöpåverkan till allmänhetens nytta. Eftersom behandlingarna använder liknande teknik och behandlar samma slags uppgifter för samma ändamål är det lämpligt att ta fram endast en enda konsekvensbedömning för behandlingarna. Om personuppgiftsansvarig med användning av sådan teknik planerar att behandla personuppgifter för ett syfte och ändamål som ligger utanför denna referenskonsekvensbedömnings avgränsning måste den personuppgiftsansvariga göra en kompletterande konsekvensbedömning.

Avgränsning

Denna referenskonsekvensbedömning hanterar risker för de registrerade och tar således dessas perspektiv. Det är alltså inte en fullständig riskhanteringsmodell för andra områden inom organisationen, exempelvis informationssäkerhet för verksamhetens behov.

Denna referenskonsekvensbedömning är generell och inte inriktad på teknik från en viss leverantör. Den uppställer således grundläggande krav på all utrustning som en personuppgiftsansvarig måste ställa på leverantörer. Utrustning som inte kan leva upp till kraven enligt denna referenskonsekvensbedömning kan således inte användas med stöd av denna referenskonsekvensbedömning. Den teknik som beskrivs tar sikte på företeelsen multisensorer.

Det är inte lämpligt att peka ut viss teknik från viss eller vissa leverantörer. Dels eftersom tekniken är föremål för intensiv utveckling. Dels eftersom det inte av upphandlingsskäl är lämpligt att inrikta sig på viss eller vissa leverantörer i konsekvensbedömningsarbetet. I många fall kan varje leverantör av utrustning tillhandahålla en särskild konsekvensbedömning som analyserar just den utrustning som leverantören säljer.

Metod

Denna referenskonsekvensbedömning har tagits fram i enlighet med de krav som framgår av artikel 35 dataskyddsförordningen[2] och artikel 29-gruppens riktlinjer för

[1] Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, WP 248 rev. 01 antagna den 4 april 2017 av Arbetsgruppen för skydd av enskilda med avseende på behandling av personuppgifter (artikel 29-gruppen) numera EU:s Dataskyddsstyrelse, (Riktlinjer om konsekvensbedömning).

[2] 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 (allmän dataskyddsförordning).

konsekvensbedömningar[3] samt Integritetsskyddsmyndighetens förteckning enligt artikel 35.4 i dataskyddsförordningen.[4]

Arbetet har i tillämpliga delar bedrivits i enlighet med CNILs metod för konsekvensbedömningar,[5] Svensk standard, SS-ISO/IEC 29134:2020 Informationsteknik – Säkerhetstekniker – Riktlinjer för konsekvensbedömning avseende personlig integritet och ISO 31000:2018(E) riktlinjer för riskhantering samt MSB:s vägledning för risk- och sårbarhetsanalyser (MSB245 2011).

Samråd

I arbetet med referenskonsekvensbedömningen har ett antal experter, sakkunniga, dataskyddsombud och leverantörer av multisensorutrustning konsulterats och getts möjlighet att lämna synpunkter på underlaget. Dataskyddsombud Anette Bengtsson, Stockholms stad; Regionchef Björn Gustavsson Trafikia AB; Stadsadvokat Oscar Jacobsson, Stockholms stad; Focus Area Manager, The Connected Individual Kristina Knaving, RISE; VD Stuart Moffat, Roadinfo Nordic AB; Dataskyddsombud Charlotte Nilsson, Eskilstuna kommun; Managementkonsult Carl Sandström, Governo AB; VD Amritpal Singh, Viscando AB; Arkivarie Patrik Stensson, Trafikkontoret Stockholms stad; Key Account Manager Jonas Stiebar Bang, Milestone; Jurist Susanne Svanholm, Sveriges Kommuner och Regioner samt informationssäkerhetsexpert Greger Westberg Certezza AB.

De platser som kan bli föremål för övervakning med multisensorer kan utgöra arbetsplats för personer som arbetar inom eller med transportnäring, renhållning, bevakning, vägbyggen, elinstallationer, teleinstallationer, postnäring, polisverksamhet, räddningstjänst och kollektivtrafik. Dessa arbetstagare kan komma att vara skyldiga att utföra arbeten på platser där dessa sensorer registrerar arbetstagare i sin yrkesutövning. Därför har dataskyddsombud för Transportarbetareförbundet, Service- och kommunikationsfacket (SEKO), Svenska Byggnadsarbetareförbundet ochg Svenska Elektrikerförbundet, Tjänstemännens centralorganisation (TCO), Polisförbundet och fackföreningen Kommunal getts tillfälle att lämna synpunkter på referenskonsekvensbedömningen.

Givet denna referenskonsekvensbedömnings generella natur och eftersom Integritetskyddsmyndigheten i varje enskilt fall beviljar tillstånd för användning av sensorerna har det inte i detta arbete ansetts lämpligt och praktiskt genomförbart att inhämta synpunkter på referenskonsekvensbedömningen från allmänheten. Centrum för Rättvisa – som är en ideell och oberoende aktör med uppdrag att värna enskildas fri- och rättigheter – har dock fått möjlighet att kommentera underlaget och inkommit med allmänna synpunkter.

[3] Riktlinjer om konsekvensbedömning.
[4] Datainspektionens beslut den 16 januari 2019, dnr. DI-2018-13200.
[5] Privacy Impact Assessment (PIA) Methodology, February 2018 edition.

De synpunkter som framförts av ovan nämnda experter, sakkunniga, dataskyddsombud, jurister, leverantörer och representanter för registrerade har beaktats i detta dokument.

Del I

Behandling av personuppgifter i multisensorer med kamerabevakningsfunktion

1.1 Behandlingens art

Behandlingen avser rörliga bilder på registrerade som registreras av en multisensor. Multisensorns kamerabilder kan bestå av högupplösta upptagningar i det visuella elektromagnetiska spektrumet, dvs. vanliga kamerabilder, men också genom registrering av värmeavtryck.

De personuppgifter som registreras är rörliga bilder på alla fysiska personer som rör sig i kamerans upptagningsområde samt registreringsnummer på fordon.

En multisensor kan även registrera annan data som inte är relevant i dataskyddshänseende, som till exempel luftkvalité, partikelhalt, pollenhalt, lufttryck, luft- eller vägtemperatur och annan väder- eller miljödata.

1.2 Behandlingens omfattning och sammanhang

Användningen av multisensorer syftar till att analysera trafikantslag[6], trafikvolymer, trafikbeteenden, trafikflöden, trafikvariation, fordonsmodell, att registrera behov av exempelvis vägunderhåll och renhållning på vissa givna platser samt till att detektera trafikanter för att styra trafiksignaler (trafikljus). Tekniken kan också användas för att upptäcka trafikolyckor och identifiera och motverka trafikfarliga situationer samt vid behov dirigera trafik. Samtidigt mäts andra uppgifter om miljön i området där sensorn är placerad som till exempel, temperatur, vägtemperatur, väglag, pollenhalt, lufttryck, partikelhalt m.m..

För att dra nytta av dessa uppgifter kan det finnas behov av att installera ett stort antal sensorer på flera platser såväl inom tätbebyggt, som glesbefolkat område dit allmänheten normalt har obehindrat tillträde. Antalet multisensorer kan variera efter den personuppgiftsansvarigas storlek, behov och resurser. Det kan röra sig om allt mellan en och tusen sensorer. Det kan också finnas behov av att sensorerna ska vara aktiva under långa perioder för att, över tid, mäta trafikflöden uppdelat på trafikantgrupper och trafikslag, köbildning och väderförhållanden.

Det finns inget behov av att identifiera särskilt utpekade personer utan behovet är endast att analysera trafik och miljö för ovan nämnda syften. Vid normal användning ska därför personuppgifter som behandlas gallras omgående efter registrering och kategorisering i trafikslag, trafiktyp eller fordonsmodell. Närmare om ungefärlig tid för lagring och behandling av personuppgifter framgår av avsnitt 2.4.

[6] Fotgängare, cyklist, fordonsslag (t.ex. personbil, buss, lastbil, tunga fordon).

1.3 Ändamål med behandlingen

Personuppgifter i form av upptagning av rörliga bild behandlas för att identifiera ett visst trafikslag i trafikmiljön. Personuppgifter i form av registreringsnummer på fordon används för att identifiera fordonsmodell.

Genom uppgift om trafikslag, trafikvariation, rörelsemönster, hastighet och fordonsmodell i kombination med andra sensoruppgifter kan följande mål uppnås:

- Förbättring av miljö och klimat,
- förbättring av trafikflöden och minskad trängsel,
- förbättrad framkomlighet för kollektivtrafik,
- förbättrat underlag för stadsplanering och detaljplanering,
- förbättring och effektivisering av renhållning och väghållning, samt
- ökad säkerhet för trafikanter.

Dessa förbättringar förväntas leda till stora samhällsekonomiska vinster som är kopplade till resurs- och energieffektiviseringsvinster, miljö- och klimatvinster samt hälsovinster för enskilda. Användning och implementering av sensorsystem kan på olika sätt leda i samma riktning som FN:s globala mål.[7] De mål som man arbetar mot i samband med användning av multisensorer är huvudsakligen följande:

Behandlingen görs också för att samla statistik och för forskningsändamål.

De anonymiserade uppgifterna kan därutöver komma allmänheten till del så att de kan vidareutnyttjas för kommersiella eller icke-kommersiella ändamål i enlighet med Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn samt Kommissionens delegerade förordning (EU) 2015/962 av den 18 december 2014 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande realtidstrafikinformationstjänster.

Utöver dessa ändamål finns också behov av att använda uppgifter för kalibrering och verifiering av sensorerna som ska användas.

1.4 Mottagare och period för lagring av personuppgifter

För de huvudsakliga syftena och ändamålen med behandlingen finns inget behov att lagra personuppgifter. Personuppgifterna ska inte tas emot av någon fysisk person för att hanteras. Personuppgifterna behandlas således under en mycket kort tidsperiod. Det vill säga endast för den tid som behövs för att analysera kameraströmmen och/eller skicka fråga till fordonsregistret och därefter anonymisera uppgifterna.

[7] FN:s utvecklingsprogram (UNDP), Globala målen http://www.globalamalen.se, hämtad 2021-03-03.

När utrustning kalibreras och verifieras kan personuppgifter komma att behandlas av en utrustningstekniker. Dessa uppgifter används i sådant fall enbart för kalibrering och verifiering av utrustning. När kalibrering och verifiering genomförts förstörs de bilder som använts för förfarandet.

Närmare uppgift om tid för lagring och behandling framgår av avsnitt 2.4.

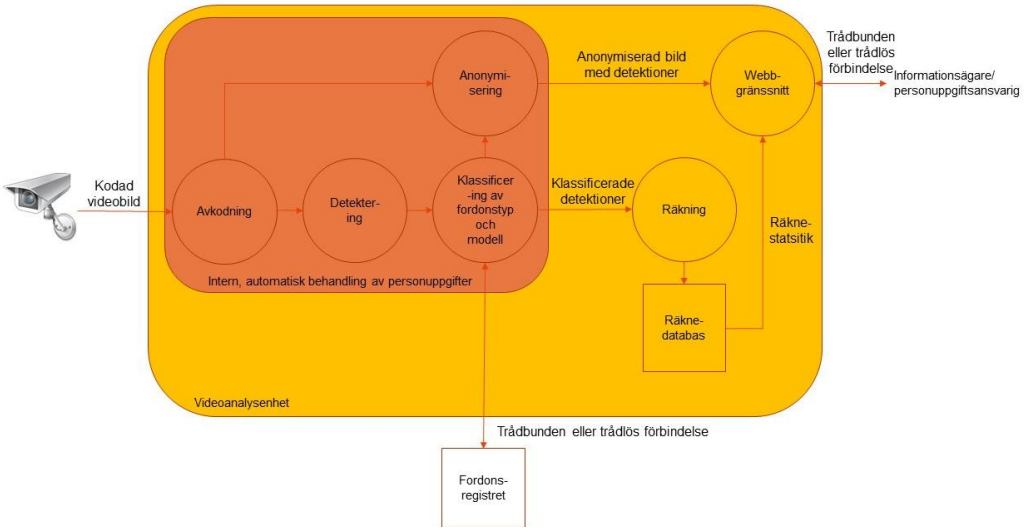
1.5 Funktionell beskrivning av behandlingen

En kamerasensor tar video eller värmeregistrerande filmer (rådata) av ett särskilt utpekat område där det förekommer allmän trafik. Kamerans upptagningsområde och brännvidd ställs in så att upptagningsområdet tar upp de delar av området som är av relevans för ändamålen. Husfasader med ingångar maskeras antingen mekaniskt eller elektroniskt.

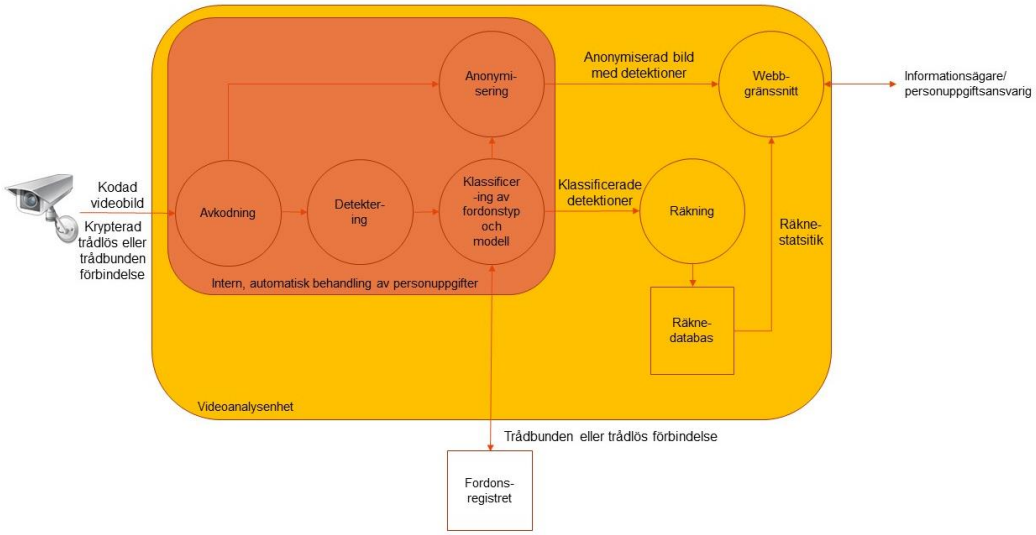
Kamerasensorns videoanalysenhet avkodar bilden och detekterar fordonstyp m.m.. En kontroll av registreringsnummer kan göras för att få uppgift om fordonsmodell. Filmen anonymiseras och slagningen mot fordonsregistret raderas. Det innebär att personuppgifterna förstörs av systemet och endast anonyma uppgifter som inte kan härledas till någon fysisk person därefter hanteras av den personuppgiftsansvarige.

Detta kan fungera på två sätt.

1. Multisensorn har i eller i nära anslutning till sensorn den analys- och anonymiseringskapacitet som krävs och att den data som skickas från sensorn till informationsägaren och centrala funktionerna för analys endast utgörs av anonymiserad metadata.
2. Videoanalysenheten finns centralt hos informationsägaren, rådatan sänds krypterad till den hårdvara i centrala funktioner hos informationsägaren som gör analys och anonymisering.



Figur 2 Funktionell beskrivning av en multisensor enligt punkten 1 ovan.



Figur 3 Funktionell beskrivning av en multisensor enligt punkten 2 ovan.

För att kalibrera och verifiera anonymisering och upptagningsområde hos varje enskild sensor kan en utrustningstekniker komma göra enstaka uttag av bilder eller kortare filmsekvenser som inte anonymiserats. Dessa uppgifter ska förstöras när de inte längre behövs för kalibrering eller verifiering. Arbetet ska också genomföras vid tidpunkter med lite trafik på platserna.

1.6 Tillgångar som är nödvändiga för personuppgifterna

De tillgångar som är nödvändiga för behandlingen av personuppgifterna är i första hand kamerasensor, kablage till videosensor eller krypteringsenhet, överföringsfunktionalitet antingen trådlös via WiFi, över mobilnätet eller trådbundet genom nätverkskabel eller fiberoptik samt analysenhet med anonymiseringsfunktion. Även fordonsregistret och förbindelsen till detta är i viss utsträckning nödvändig för behandling av personuppgifterna.

1.7 Uppförandekoder

Det saknas av Integritetsskyddsmyndigheten godkända uppförandekoder för denna typ av behandling för dessa ändamål i denna typ av verksamhet.

Del II

Behov och proportionalitet

2.1 Ändamål med behandlingen och samhällsekonomisk nytta

Ändamålen med behandlingen framgår av avsnitt 1.3. Bakgrunden till ändamålen är att det genom ny teknik och nya tillämpningar finns möjlighet att insamla uppgifter som kan vara till stor nytta för såväl samhället i stort, för enskilda kommuner och regioner och för enskilda medborgare.

De samhällsekonomiska konsekvenserna kan sammanfattas i bättre miljö och klimat i form av minskade koldioxidutsläpp och partikelhalter i trafikmiljön. Detta kan i sin tur förväntas leda till bättre möjlighet att uppnå miljömål och minska personligt lidande för enskilda genom att dessa i lägre grad utsätts för skadliga partiklar och risker för sjukdomar därmed minskar. Förbättrade trafikflöden och minskad trängsel kan leda till positiva effekter för framkomligheten och minskade restider vilket i sig kan medföra minskade utsläpp, lägre stress i trafiken och ökad produktiv tid. Minskad trängsel på gator och torg kan därtill leda till minskad smittspridning i samhället av såväl vanligt förekommande virala sjukdomar som i händelse av pandemier vilket i sin tur kan leda till lägre belastning på vården och mindre lidande för enskilda. Ökad framkomlighet för kollektivtrafik innebär bättre arbetsmiljö för yrkeschaufförer, säkrare tidtabeller i kollektivtrafiken, minskad stress och bättre miljö. Förbättrat underlag för stads- och detaljplanering hjälper kommuner och regioner att planera för och bygga bort sådana saker som utgör störningsmoment i trafikmiljön för en säkrare och tryggare trafikmiljö. Genom att kommunen i realtid kan uppmärksammas på vägförhållanden och andra förhållanden som t.ex. fyllnadsgrad på offentliga soptunnor kan väghållnings- och renhållningsåtgärder vidtas mer effektivt vilket i sin tur kan leda till minskad trängsel, ökad framkomlighet samt säkrare trafikförhållanden och färre olyckor. Uppgifter om trafikincidenter kan också medföra att problematiska trafikmiljöer identifieras och därmed kan modifieras på lämpligt för att minska riskera för olyckor i framtiden.

Data och statistikuppgifter kan komma att användas för forskning och utveckling som i sin tur kan leda till ytterligare åtgärder för säkrare och bättre trafikmiljö. Dessa uppgifter kan också komma att användas för att kontrollera att de önskade samhällsekonomiska effekterna av användningen av mulitsensorerna uppnås.

Anonymiserade trafikuppgifter från intelligenta trafiksystem kan därtill komma till nytta för näringsliv och enskilda genom utvecklingen av nya innovativa tjänster som kan skapa ytterligare nyttor för samhället.

2.2 Laglig grund för behandlingen

2.2.1 Uppgift av allmänt intresse, artikel 6.1.e. dataskyddsförordningen

Behandling av personuppgifter är laglig enligt artikel 6.1.e. 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 (dataskyddsförordningen) om:

> *Behandlingen är nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning;*

I detta fall är det endast det första ledet som kan tillämpas eftersom användning av multisensorer inte är ett led i myndighetsutövning.

I 2 kap. 2 § 1 lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning anges att en uppgift av allmänt intresse ska följa av lag eller annan författning eller av beslut som meddelats med stöd av lag eller annan författning.

Den verksamhet som en kommunal myndighet bedriver, inom ramen för sin befogenhet, är av allmänt intresse. Det är därmed den rättsliga grunden i artikel 6.1 e i dataskyddsförordningen som vanligen bör tillämpas av myndigheter, även utanför området för myndighetsutövning. De kommunala myndigheternas obligatoriska uppgifter följer av åligganden som fastställts i lag eller förordning. Även frivilliga åtaganden som en kommun gör inom ramen för sin allmänna befogenhet ska framgå av gällande rätt, nämligen av det reglemente som fullmäktige utfärdar för den ansvariga nämnden.[8]

2.2.2. Väglagen

Utöver detta är kommuner i vissa fall väghållare inom kommunen. När en kommun är väghållare är den kommunala nämnd som kommunfullmäktige utser väghållningsmyndighet, (5 och 6 §§ väglagen (1971:948). Väghållning omfattar byggande av väg och drift av väg. Vid väghållning ska tillbörlig hänsyn tas till enskilda intressen och till allmänna intressen såsom trafiksäkerhet, miljöskydd, naturvård och kulturmiljö, (4 § väglagen). Av 26 § väglagen ska väg hållas i ett för samfärdseln tillfredsställande skick genom underhåll, reparation och andra åtgärder. Genom renhållning ska vägområdet hållas i ett sådant skick att olägenheter för människors hälsa förebyggs eller avhjälps och så att skäliga trevnadshänsyn blir tillgodosedda. Till drift av väg räknas också serviceåtgärder och förbättringsåtgärder. Av 5 kap 1 § vägförordningen (2012:707) framgår att drift av väg innefattar åtgärder som

1. säkerställer att trafiken kan komma fram, såsom snöplogning, halkbekämpning, reparation av mindre skador samt hyvling och dammbindning på grusvägar (servicearbeten),

[8] Ny Dataskyddslag, prop. 2017/18:105 s. 57 f.

2. vidmakthåller vägens standard, såsom förnyelse av slitlager och vägmarkeringar samt dikning (underhållsarbeten),
3. förbättrar vägens standard genom smärre åtgärder, såsom beläggning av grusväg, förstärkning av bärigheten och punktåtgärder för att öka trafiksäkerheten (förbättringsarbeten),
4. håller vägen ren, såsom sopning, borttagande av skräp och smuts samt ogräsbekämpning (renhållning), eller
5. på annat sätt håller vägen i ett för samfärdseln tillfredställande skick.

2.3 Adekvata, relevanta och inte för omfattande uppgifter

De personuppgifter som behandlas är bilder på alla fysiska personer som rör sig i kamerans upptagningsområde, registreringsnummer på fordon. Varje kameraplacering ska vara inriktad så att den begränsar upptagningsområdet så att relevant trafik registreras.

Fasader till byggnader ska maskeras logiskt eller fysiskt så att arbetsplatser, restauranger, uteserveringar samt trafikanters rörelser till och från byggnader i möjligaste mån inte registreras. Vid byggnader där verksamhet som skulle kunna avslöja känsliga personuppgifter förekommer, som till exempel politisk, facklig eller religiös verksamhet eller om det skulle kunna avslöja uppgifter om enskildas hälsa, sexualliv eller sexuella läggning är det av särskild vikt att dessa byggnader maskeras så att besökare till och från dessa verksamheter inte registreras.

Om sensorerna är placerade på platser där demonstrationståg förekommer bör sensorerna – om det inte är absolut nödvändigt – vara avstängda när manifestationer eller demonstrationståg passerar. Så kan till exempel vara fallet när den personuppgiftsansvariga har kännedom om att demonstrationer eller manifestationer passerar platsen vid 1 maj eller Pride parader.

2.4 Begränsad lagringstid

De personuppgifter som behandlas i den löpande driften av multisensorerna ska automatiskt och omgående anonymiseras efter att trafikslag har identifierats. I dessa fall så innebär det att personuppgifter lagras i sekunder eller mindre än sekunder. När slagning görs mot fordonsregistret för att identifiera fordonsmodell behandlas uppgifterna under potentiellt längre tid då detta är beroende av svarstider i förhållande till fordonsregistret. I alla avseenden ska personuppgifterna inte lagras längre än tio minuter innan de gallras genom anonymisering.

I enstaka fall när sensorerna installeras, kalibreras, verifieras och ställs in kan en tekniker behöva behandla bildmaterial under en längre tid för dessa ändamål. Dessa personuppgifter ska dock aldrig behandlas längre absolut nödvändigt för det aktuella syftet.

2.5 Information till registrerade

Information om kamerabevakningen ska lämnas på ett begripligt och lättillgängligt sätt. Information ska lämnas såväl på skyltar på platsen där multisensorer är uppsatta

som på en särskild webbplats och via särskilt telefonnummer dit registrerade kan ringa.

2.5.1 Information på skyltar

Skyltarna ska placeras väl synliga från alla ingångsvägar till varje multisensors upptagningsområde. Skyltarna ska innehålla den viktigaste informationen såsom den personuppgiftsansvariges identitet och kontaktuppgifter, kontaktuppgifter till dataskyddsombud, ändamålet med kamerabevakningen, sådant som är viktigt för de registrerade att känna till om kamerabevakningen samt information om vart den bevakade kan vända sig för att få ytterligare och mer detaljerad information om kamerabevakningen. För fordonstrafikanter kan det vara svårt att uppfatta skyltar med mycket information därför lämnar vi också förslag på utformning av en enklare skylt med mindre information som lättare kan uppfattas av personer som framför fordonstrafik.

Förslag på skylt 1: [9]

Figur 4 Förslag till utformning av skylt vid användning av multisensorer

[9] Enligt modell från Integritetsskyddsmyndighetens hemsida: https://www.imy.se/vagledningar/kamerabevakning/informera/

Förslag på skylt 2:

Figur 5 Förslag till utformning av skylt vid användning av multisensorer, exempelvis för att informera bilister.

2.5.2 Information på annat sätt

Fullständig information om kamerabevakningen ska tillhandahållas på ett öppet, enkelt och transparant sätt. Dels på en webbplats men fullständig information ska även

kunna tillhandahållas fysiskt på begäran, exempelvis genom ett informationsblad eller liknande.

Den information som tillhandahålls på detta sätt ska innehålla kontaktuppgifter till personuppgiftsansvarig och dennas företrädare (i tillämpliga fall), kontaktuppgifter till dataskyddsombud, ändamålet och den rättsliga grunden för kamerabevakningen. Kriterierna för hur länge personuppgifterna ska lagras, vilka rättigheter som registrerade har, till exempel begäran av registerutdrag, att registrerade kan klaga hos integritetsskyddsmyndigheten samt information om att uppgifterna inte kommer att överföras till tredje land, att de inte används för automatiserat beslutsfattande och att personuppgifter endast undantagsvis lagras under en längre tid (dock inte längre än en arbetsdag) för att kalibrera och ställa in utrustningen. Anledningen till att inte denna längre tid anges på skylten är för att detta endast sker vid enstaka tillfällen och inte är förknippat med den normala driften av multisensorn. Beslut om tillstånd för kamerabevakning ska också finnas i anslutning till dessa informationskanaler.

2.6 Andra åtgärder som stärker registrerades rättigheter

2.6.1 Rätt till tillgång, rättelse, radering och att göra invändningar

Enligt dataskyddsförordningen har registrerade rätt till tillgång till personuppgifterna (artikel 15 dataskyddsförordningen). Enskilda har också rätt att utan onödigt dröjsmål få felaktiga personuppgifter rättade, (artikel 16 dataskyddsförordningen) och raderade (artikel 17 dataskyddsförordningen).

Dessa rättigheter har samtliga registrerade och ska säkerställas. Med tanke på den mycket korta lagringstiden av icke-anonymiserade personuppgifter kommer rätten till tillgång till personuppgifterna sällan att kunna utövas. Det kommer inte heller inträffa att felaktig registrering av personuppgifter görs då multisensorn gör en bildupptagning av vad som registreras på platsen. Denna bildupptagning kommer i personuppgiftshänseende alltid att vara korrekt utifrån det upptagningsområde som multisensorn registrerar, om inte obehörig manipulering skett. I alla avseenden kommer personuppgifterna i de flesta fall vara gallrade genom anonymisering innan dessa rättigheter kan aktualiseras.

Varje registrerad har rätt att när som helst göra invändningar mot behandlingen av personuppgifter som grundar sig på artikel 6.1. e dataskyddsförordningen, (artikel 21.1 dataskyddsförordningen). Den personuppgiftsansvarige får då inte längre behandla personuppgifterna såvida inte denne kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter.

En viktig del av intresseavvägningen i detta avseende görs redan genom tillståndsförfarandet. På grund av den korta behandlingstiden som ska gälla för behandlingen kan det också vara svårt att verifiera att en enskilds personuppgifter ens har behandlats. Icke desto mindre måste den personuppgiftsansvarige ha en organisation och förmåga att ta emot och behandla invändningar från enskilda.

2.6.2 Förhållande till personuppgiftsbiträden

Det kan förekomma att personuppgiftsansvarig har behov av att anlita personuppgiftsbiträden för att sköta installation och drift av multisensorerna. I dessa fall ska förhållandet mellan parterna regleras genom personuppgiftsbiträdesavtal i enlighet med dataskyddsförordningens regler. Eventuella personuppgiftsbiträden och underbiträden ska därtill vara skyldiga att följa de krav som ställs i den senaste versionen av denna referenskonsekvensbedömning samt de krav som ställs i de tillståndsbeslut som fattas av Integritetsskyddsmyndigheten.

2.6.3 Internationella överföringar

All personuppgiftsbehandling av multisensorerna sker i Sverige. Inga personuppgifter ska överföras till eller behandlas i något land utanför EU. Tekniska skyddsåtgärder ska implementeras så att detta inte sker.

2.6.4 Åtgärder för anonymisering

Det är av central betydelse för användning av multisensorerna att de personuppgifter som behandlas av multisensorerna omgående anonymiseras så att de uppgifter som behövs för att uppnå ändamålen kan användas utan risk för integritetsintrång för enskilda. När personuppgifterna har anonymiserats är det kvarstående uppgifterna inte längre att betrakta som personuppgifter. Av skäl 26 i dataskyddsförordningen framgår bland annat följande:

> *Principerna för dataskyddet bör […] inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar*.

Den Europeiska dataskyddsstyrelsen (tidigare Artikel 29-arbetsgruppen för skydd av personuppgifter) har publicerat ett yttrande om avidentifieringsmetoder.[10] I detta yttrande finns rekommendationer om hur dessa metoder bör hanteras.

Slutsatsen i yttrandet är att avidentifieringsmetoder kan ge integritetsgarantier och kan användas för att skapa effektiva avidentifieringsprocesser, men endast om tillämpningen av dem är utformad på lämpligt sätt. Det innebär att förutsättningarna (sammanhanget) och målet eller målen för avidentifieringsprocessen måste fastställas tydligt så att den avsedda avidentifieringen uppnås samtidigt som användbara uppgifter produceras. Vad som är den bästa möjliga lösningen måste bestämmas från fall till fall, eventuellt med hjälp av en kombination av olika metoder, samtidigt ska hänsyn tas till de praktiska rekommendationerna i yttrandet.

Ett avidentifierat dataset kan fortfarande innebära kvarstående risker för de registrerade. Avidentifiering och re-identifiering är aktiva forskningsområden och nya upptäckter offentliggörs regelbundet, men även avidentifierade uppgifter, som t.ex. statistik, kan användas för att utöka enskilda personers befintliga profiler och därigenom skapa nya problem beträffande skyddet av personuppgifter.

[10] 0829/14/EN WP216, yttrande 05/2014 om avidentifieringsmetoder, antaget den 10 april 2014.

Avidentifiering är därför inte en engångsåtgärd, och personuppgiftsansvariga ska regelbundet ompröva riskerna med behandlingen.

2.6.5 Förhandsamråd

Tillståndskravet för kamerabevakning är en precisering av kravet på konsekvensbedömning och samråd med tillsynsmyndigheten i artiklarna 35.1 och 36.1 i dataskyddsförordningen.[11]

Konsekvensbedömningar som rör kamerabevakningar som är föremål för tillstånd kan därför inte förhandssamrådas enligt dataskyddsförordningen. En ansökan om kamerabevakningstillstånd synes därför ersätta kravet på förhandssamråd. Förhandssamråd med Integritetsskyddsmyndigheten kan därför inte genomföras i dessa fall. Istället för att söka förhandssamråd för konsekvensbedömningen ska en ansökan om tillstånd lämnas in till Integritetsskyddsmyndigheten.

Denna referenskonsekvensbedömning innehåller en stor del av de uppgifter som ska finnas i en formell ansökan och är tänkt att kunna närslutas en tillståndsansökan som en enskilt personuppgiftsansvarig kommun eller kommunal nämnd gör.

[11] Prop. 2017/18:231 s. 118.

Del III

Riskanalys och riskhantering – för registrerade

3.1 Avgränsning av riskanalysen

Denna riskanalys och riskhantering är avgränsad till risker som kan uppstå för enskilda personer som registreras av en multisensor. Den tar inte sikte på de risker som kan uppstå för verksamheten eller för allmänheten i händelse av att sensorns funktionalitet eller information inte är åtkomlig, obehörigen ändras eller obehörigen görs tillgänglig. Exempel på risker som inte hanteras i denna riskanalys är till exempel om partikelhalten i luften skulle ge felaktiga data eller om styrning av trafikljus eller dirigering av vägunderhåll skulle baseras på felaktig eller korrupta uppgifter. Inte heller konsekvenser av trafikolyckor är sådant som omfattas av denna riskanalys som enbart fokuserar på risker för personer som registreras och behandlingen av dessa personuppgifter.

Vid användning av denna referenskonsekvensbedömning åligger det nyttjaren att säkerställa att de ingående värdena är relevanta för den nyttjande parten och vid behov göra nödvändiga justeringar.

3.2 Återkommande riskanalys varje år samt vid ändringar

Minst en gång per år ska det göras en översyn och bedömning av och om förändringar i omvärlden och/eller tekniska miljöer påverkar användningen av multisensorer och därmed behovet av förnyad riskanalys och riskhantering denna översyn omfattar även redan behandlade risker för att säkerställa att dessa ligger kvar på acceptabel nivå. Även vid planerade förändringar av multisensorverksamheten ska det göras en förnyad riskbedömning. Denna riskbedömning ska göra en avvägning mellan vad som kan inträffa, hur troligt det är att det inträffar och vilka konsekvenser det kan få om det inträffar.

3.3 Multisensorerna och dess förbindelser analyseras

De objekt som är föremål för analysen är generiska multisensorer med kamerafunktionalitet samt de förbindelser som dessa är kopplade till. Det beaktas att det vid drift av multisensorer för dessa ändamål finns ett behov av att använda ett stort antal multisensorer vid flera platser inom en kommun. Det rör sig således om omfattande och kontinuerlig kamerabevakning på platser där allmänheten rör sig. De komponenter som kan identifieras i detta sammanhang är

Multisensorenheten som detekterar och mäter händelser i en fysisk enhet och omsätter resultatet i digitala data.

Strömförsörjning till multisensorn och dess interna komponenter. Spänningskällan kan vara extern och kabelansluten eller utgöras av ett batteri integrerad i multisensorn.

Fysisk placering och uppsättningsanordningar samt fysiska anslutningar.

Inbäddat system för analys, fordonsidentifiering och anonymisering.

Passiv infrastruktur i form av ledningsnät, fiber, nätverkskablar eller koppar- och koaxialkablar.

Aktiv infrastruktur i form av kommunikationsnät som medger att utbyta data över datalänk.

Protokoll som definierar regler för hur kommunikation mellan multisensorn och andra delar av systemet ska överföras.

Plattform för hantering av enheter och kommunikationsnät vilket inkluderar uppdatering av mjukvara för operativsystem, fast programvara och applikationer. Det omfattar också spårning och övervakning av enheter och kommunikationsnät, insamling och lagring av loggar som i senare skede kan användas för diagnostik samt övergripande uppföljning av samtliga multisensorer i verksamheten och kommunikationsnät för att känna till aktuell status och prestanda.

Web-baserade gränssnitt för tillgång till aggregerade och anonymiserade uppgifter. Detta kan vara molnbaserat för att aggregera och processa data från spridda enheter.

Programvara för användartillämpningar, dataanalys och visualiseringar.

Säkerhetstillgångar i form av brandväggar, system för intrångsskydd och system för hantering av autentisering och rättigheter i systemet.

Information i vila, under överföring och under användning.

3.4 Hot

I arbetet med konsekvensbedömningen har ett antal hot som är av betydelse för den personuppgiftshantering som sker i multisensorverksamheten identifierats. De olika hoten kan delas in i följande kategorier:

A. Avsiktliga hot, till exempel personer eller annat som har ett syfte att orsaka någon form av skada.
B. Olyckshändelser, till exempel felaktigt handhavande
C. Hot med anledning av naturhändelser.
D. Andra omständigheter som kan inverka negativt på enskildas rättigheter och friheter.

3.5 Hothändelser

I det följande presenteras ett antal hothändelser som skulle kunna inträffa och påverka enskildas rättigheter och friheter. Listan är inte uttömmande och nya hothändelser kan komma att tillkomma i framtida versioner av denna referenskonsekvensbedömning.

A.1 Kapning av kommunikationsprotokoll, avlyssning av kommunikation – En eller flera angripare tar till exempel kontroll över kommunikationssession mellan två enheter i nätverket. Angriparen kan därigenom fånga upp information som överförs i kommunikationen. Om analys- och anonymiseringsenheten befinner sig på annat

ställe än där sensorn befinner sig skulle en sådan kapning också kunna leda till att en angripare skulle kunna ta del av och lagra den rådata som sensorn registrerar.

A.2 Tillgänglighetsattacker – En eller flera angripare får ett eller flera system att anropa en viss mottagare – exempelvis en sensor i syfte att överbelasta den eller få den att sluta fungera för en viss tid. Det kan göras genom att göra många anslutningar, överbelasta en kommunikationskanal eller upprepat repetera samma kommunikation. Detta hot inkluderar även fysiskt sabotage som skadar sensorer så att de inte längre kan generera bildströmar.

A.3 Skadlig kod – Applikationer som är utformade för att utföra oönskade och obehöriga åtgärder i ett system eller som utnyttjar svagheter för att få tillgång till systemet. Hotet kan innebära att personuppgifter inte anonymiseras som tänkt, att rådata överförs till obehöriga eller att personuppgifter obehörigen ändras.

A.4 Obehörig fysisk modifiering –Vandalisering eller sabotage av sensorn eller dess infästningsanordningar kan orsaka att sensorns upptagningsområde ändras och registrerar en annat upptagningsområde än som godkänts.

B. 1 Fel i system, konfiguration eller handhavande – Oavsiktliga fel i programvarutjänster eller applikationer eller vid konfigurering av systemen som leder till att rådata kan finnas tillgänglig för obehöriga. Handhavandefel kan leda till att anonymisering inte genomförs korrekt.

B. 2 Avbrott i nätverk – Avbrott eller fel i nätverk eller strömförsörjning kan begränsa tillgången till de personuppgifter som behandlas.

C.1 Naturhändelser – Strömavbrott, kraftig kyla eller värme, brand kraftig vind eller andra liknande naturhändelser kan orsaka bortfall i tillgängligheten samt orsaka att sensorns upptagningsområde ändras.

D1 Anonymisering inte längre funktionell – Den tekniska utvecklingen eller andra händelser gör att den data som ska anonymiseras kan kopplas till enskilda individer och därigenom inte längre kan sägas vara anonymiserad.

D.2 Omfattande lagring av anonymiserade uppgifter – När stora mängder data samlas ökar risken för att hitta och härleda uppgifter om enskilda vilket kan påverka anonymiseringen.

3.6 Klassificeringsmodell

För att kunna bedöma risken med ett hot görs en sammanvägning av konsekvensen av att hotet inträffar och en bedömning av sannolikheten för att hotet inträffas. För att göra detta krävs att kriterier för sannolikhet och konsekvenser definieras.

Det som anges i det följande är uppskattningar och du som använder detta underlag för din verksamhet och för en ansökan är ansvarig för att bedöma om dessa bedömningar är korrekta i förhållande till er aktuella verksamhet och göra de nödvändiga justeringar eller anpassningar som behövs för just er användning.

3.6.1 Kriterier för risknivåer

Sannolikhet

Sannolikheten är ett mått som beskriver hur ofta det bedöms att en händelse kommer att inträffa. Denna riskanalys använder skattade frekvenser i form av antalet förväntade händelser per år. I sammanhanget bör det påpekas att alla skattningar är bedömningar och att det ligger i sakens natur att resultaten aldrig kan fastställas med säkerhet när det handlar om bedömningar av framtiden.

Sannolikhet[12]	**Intervall**
Mycket hög	Händelsen inträffar mer än 10 gånger per år.
Hög	1–10 gånger per år.
Medel	0,5–1 gång per år.
Låg	0,05 – 0,5 gånger per år. (mellan en gång vart annat år till en gång per 20 år)
Mycket låg	Händelsen inträffar färre än en gång per 20 år.

Konsekvens

Konsekvensen är ett mått hur registrerades rättigheter och friheter skadas om hotet blir verklighet. Av förklarliga skäl blir beskrivningen av konskevensnivåerna nedan kortfattad och kan behöva förtydligas med exempel. Exemplen kan delas in i tre kategorier;

- materiell påverkan för enskilda.
- fysisk påverkan för enskilda, och
- psykisk påverkan för enskilda.[13]

Av betydelse för denna konsekvensbedömning är det dock framför allt psykisk påverkan för enskilda som blir relevant eftersom multisensorer inte bedöms orsaka fysisk skada för enskilda eller påverka enskildas ekonomi eller medföra annan materiell påverkan.

Konsekvenser	**Definition**	**Exempel**
Mycket stora	Registrerade kan drabbas av allvarliga eller permanenta oåterkalleliga skador som de inte kan övervinna.	- Långsiktig eller permanent psykologisk sjukdom. - Straffrättsliga påföljder. - Administrativa påföljder.

[12] Sannolikhetsskalan är utökad men bygger på metodstöd för systematiskt informationssäkerhetsarbete på informationssäkerhet.se som är en gemensam satsning av Myndigheten för samhällsskydd och beredskap. Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk, Post- och telestyrelsen, Säkerhetspolisen och Polismyndigheten.
[13] Privacy Impact Assessment (PIA) Knowledge bases, Commission Nationale Informatique & Libertés, Februari 2018.

Stora	Registrerade kan drabbas av betydande skador som de endast med stora svårigheter kan övervinna.	- Allvarlig psykisk sjukdom som t.ex. depression eller utveckling av fobi).
Medel	Registrerade kan råka ut för betydande besvär som de med kommer att kunna övervinna om än med vissa svårigheter.	- Känsla av intrång i privatlivet med oåterkallelig skada. - Känsla av brott mot grundläggande rättigheter t.ex. rätten till skydd av personuppgifter eller yttrandefrihet. - Utsatt för utpressning eller trakasserier.
Begränsade	Registrerade kan råka ut för besvär som de kan övervinna.	- Mindre psykiska besvär som t.ex. ärekränkning. - Relationsproblem med privata eller professionella bekanta, t.ex. skada för ens personliga framtoning, rykte eller anseende. - Känsla av intrång i privatlivet utan oåterkallelig skada.
Mycket begränsade	Registrerade påverkas inte eller drabbas av få besvär som de med lätthet kan övervinna.	- Rädsla för förlust av kontroll av personuppgifter. - Känsla av intrång i privatlivet utan reell eller objektiv skada.

Definitionerna av sannolikhet och konsekvens ska betraktas som ett riktmärke och kan förändras i senare revisioner av konsekvensbedömningen. Då detta är en referenskonsekvensbedömning är skattningarna generella och som användare behöver du också förhålla dig till dina egna förutsättningar och vid behov göra justeringar utifrån detta.

Geografisk omfattning

Även andra faktorer uppmärksammas i riskanalysarbetet såsom geografisk omfattning som ett hot kan aktualisera.

Geografisk omfattning	Definition
Samtliga	Samtliga sensorer som används påverkas av hotet.
Grupp	Hotet kan påverka en grupp av sensorer som används. Det kan vara samtliga sensorer på en viss utpekad plats eller samtliga sensorer på ett par geografiska platser.

Enskild	Hotet påverkar endast en sensor.

Tidsutdräkt

Ett specifikt hot eller en specifik sårbarhet har ofta en tid under vilket hotet eller sårbarheten kan vara aktuellt eller pågå. Den aspekten kan i sig innebära att allvarligheten och konsekvenserna för enskildas fri- och rättigheter påverkas. Därför uppmärksammas även dessa aspekter i riskanalysen dessa ingår inte i riskmatrisen (se kriterier för riskacceptans nedan) men beaktas ändå i den sammanvägda bedömningen. Om den geografiska omfattningen påverkar bedömningen i riskmatrisen så anges det särskilt. I MSB:s årsrapport NIS-leverantörers it-incidentrapportering framgår att rapporterade it-incidenter som medför en betydande störning i genomsnitt pågår mellan 5 och 10 timmar.[14]

Tidsutdräkt	Definition
Lång	Längre än en vecka.
Medel	Flera dagar, upp till en vecka.
Kort	Timmar eller enstaka dagar.

Skattning av säkerheten i bedömningen

För varje bedömning preciseras även en uppskattning av hur säker bedömningen är. Bedömningen görs med bästa möjliga kunskap och erfarenhet av hot, hotaktörer, sårbarheter samt tillgänglig teknik.

Osäkerhet	Definition
Hög	Stora osäkerheter kring kännedom om hot och aktörer samt teknisk kännedom gör att bedömningen är osäker.
Medel	Bedömningen omgärdas av en eller flera osäkerheter som inte kan analyseras.
Låg	Upprepade erfarenheter samt kunskap och insikter om hotet och orsaken till hotet gör att bedömningen betraktas mycket säker.

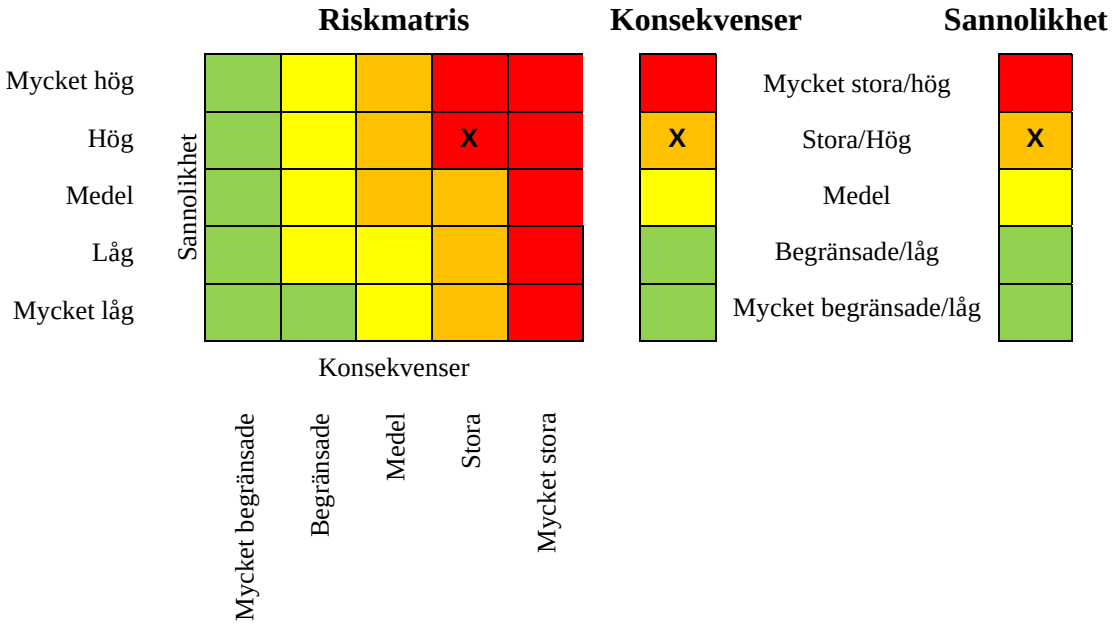
3.6.2 Kriterier för riskacceptans

När alla sannolikheter och konsekvenser bestämts sammanfattas riskerna i en riskmatris som med färger signalerar allvarlighetsgraden av ett visst hot eller viss sårbarhet i förhållande till sannolikheten att det inträffar och konsekvenser om det inträffar. Sammanvägd risk som får röd markering är kritisk att hantera så att

[14] Årsrapport NIS-leverantörers it-incidenrapportering 2020, En samlad bild över rapporterade it-incidenter i samhällsviktiga och digitala tjänster, MSB1695, februari 2021.

sannolikheten och/eller konsekvenserna minskar till en acceptabel nivå. Sammanvägd risk som får orange markering är viktig att den hanteras så att sannolikheten och/eller konsekvenserna minskar till en acceptabel nivå. Sammanvägd risk som får gul markering ska även den hanteras medan en sammanvägd riskbedömning som får grön markering bör kunna accepteras utan omedelbara åtgärder. De formulerade riskerna kan sedan omformuleras till mål som ska uppfyllas för att hantera riskerna. Dessa mål kan sedan användas som stöd i det fortsatta riskhanteringsarbetet. Det ska tilläggas att det är varje enskild användare av multisensorsystemet som har att bedöma vilken risk som kan accepteras och tillståndsmyndigheten som gör en slutlig bedömning av om ytterligare åtgärder behöver vidtas.

Riskmatrisen i denna konsekvensbedömning har en sammanvägd bedömning som är något skarpare än en del andra riskmatriser som till exempel riskmatriser för egen verksamhet. Anledningen är att denna riskanalys enbart tar sikte på konsekvenser för enskildas fri- och rättigheter och hanteringen av dessa är av mycket stor betydelse.



Figur 6 Exempel på riskmatris som visar sammanvägd riskanalys för ett specifikt hot.

3.7 Riskanalys

I detta avsnitt gås alla identifierade hot igenom och riskerna med hoten analyseras. Riskanalysen görs i enlighet med den kategorisering som gjorts av hoten samt enligt den klassificeringsmodell som presenterats i föregående avsnitt. Riskerna beskrivs sedan utifrån en riskformel enligt följande modell:

Risk för [Hot/hothändelse] mot [Tillgång] som inträffar [Frekvens] innebärande [konsekvens/kostnad].

Riskformeln används sedan för att formulera målet med vad risk- och konsekvensreducerande åtgärder ska uppnå. Målet syftar till att motverka risken och

kan därmed beskrivas i form av ett motsatsförhållande till riskformuleringen. Målformlen blir då

Målet är att uppnå ett läge där [Hot/hothändelse] förhindras/reduceras varigenom [konsekvens/kostnad] minskar eller inte uppstår.

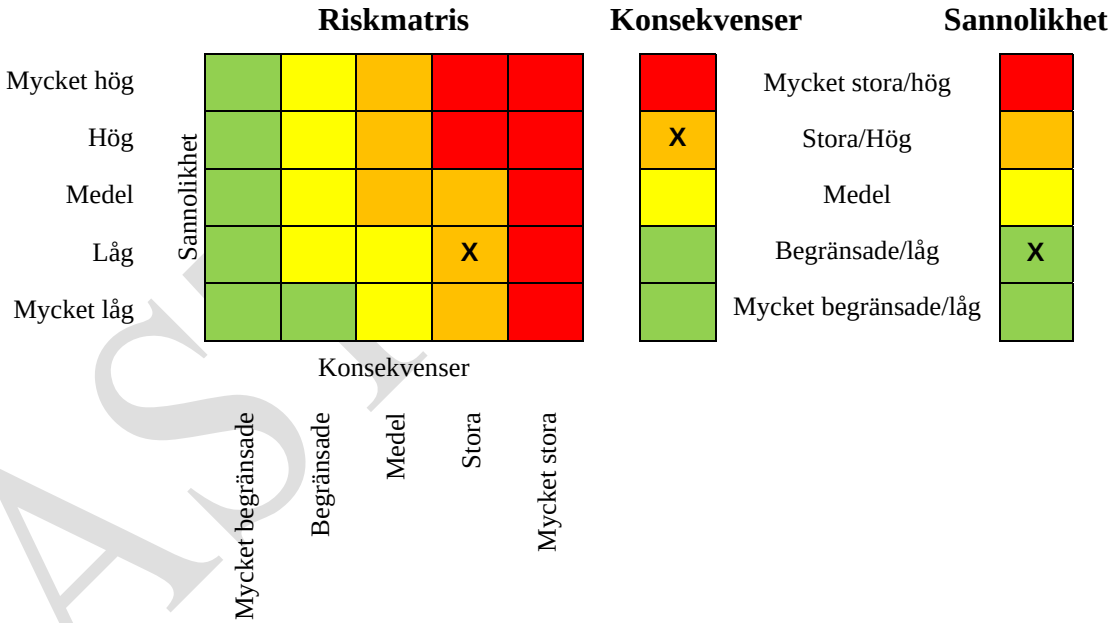
3.7.1 A.1 Kapning av kommunikationsprotokoll, avlyssning

Benämning	**A.1 Kapning av kommunikationsprotokoll, avlyssning av kommunikation**
Risk-formulering	Risk för att angripare tar kontroll över eller avlyssnar kommunikationssession mellan två enheter i sensorsystemet. Om analys- och anonymiseringsenheten befinner sig på annat ställe än där sensorn befinner sig skulle en sådan kapning också kunna leda till att en angripare skulle kunna ta del av och lagra den rådata som sensorn registrerar.

Risk					
Sannolikhet	Mycket låg	Låg	Medel	Hög	Mycket hög
Konsekvenser	Mycket begränsade	Begränsade	Medel	Stora	Mycket stora
Andra omständigheter					
Geografisk omfattning		Enskild	Grupp	Samtliga	
Hotets tidsutdräkt		Kort	Medel	Lång	
Osäkerhet		Låg	Medel	Hög	

Konsekvenser av det inträffade Konsekvenser för enskildas fri- och rättigheter
Det kan leda till allvarliga psykiska sjukdomar hos registrerade som till exempel depression eller utveckling av fobier när det blir känt att obehöriga kunnat ta del av, spåra eller lagra uppgifter om enskilda.

Målformulering
Multisensorsystemet har implementerat säkerhetsåtgärder för att snabbt upptäcka och skydda mot dataläckor och avläsning eller avläsningsförsök.



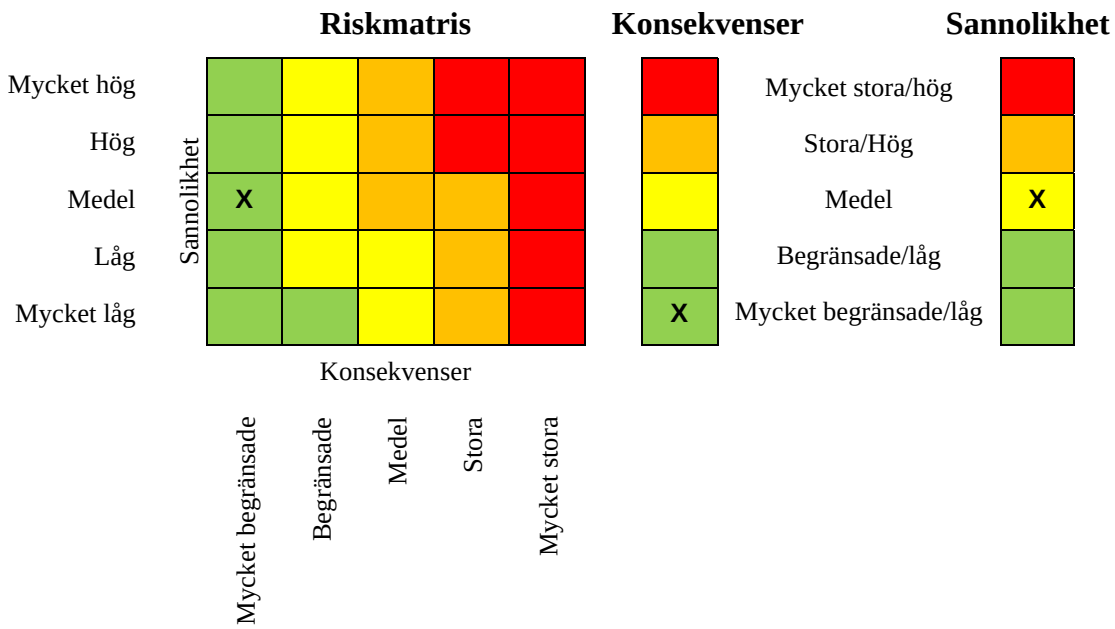
3.7.2 A.2 Tillgänglighetsattacker

Benämning	**A.2 Tillgänglighetsattacker**
Risk-formulering	Risk för att utomstående aktör orsakar att sensorer eller sensorsystemet slutar att fungera. Till exempel genom att upprätta en mängd anslutningar, överbelasta en kommunikationskanal eller upprepat repetera samma kommunikation eller fysiskt förstöra utrustning.

Risk					
Sannolikhet	Mycket låg	Låg	Medel	Hög	Mycket hög
Konsekvenser	Mycket begränsade	Begränsade	Medel	Stora	Mycket stora
Andra omständigheter					
Geografisk omfattning			Enskild	Grupp	Samtliga
Hotets tidsutdräkt			Kort	Medel	Lång
Osäkerhet			Låg	Medel	Hög

Konsekvenser av det inträffade Konsekvenser för enskildas fri- och rättigheter
Brist på tillgång gör att enskild omedelbart inte kan ta vara på sin rätt. Det kan innebära en rädsla av förlust av kontroll över sina personuppgifter och en känsla av intrång i privatlivet utan reell eller objektiv skada

Målformulering
Multisensorsystemet ska vara robust mot tillgänglighetsattacker och personuppgiftsansvarig har rutiner för att snabbt återställa funktionalitet för driften av sensorsystemet.



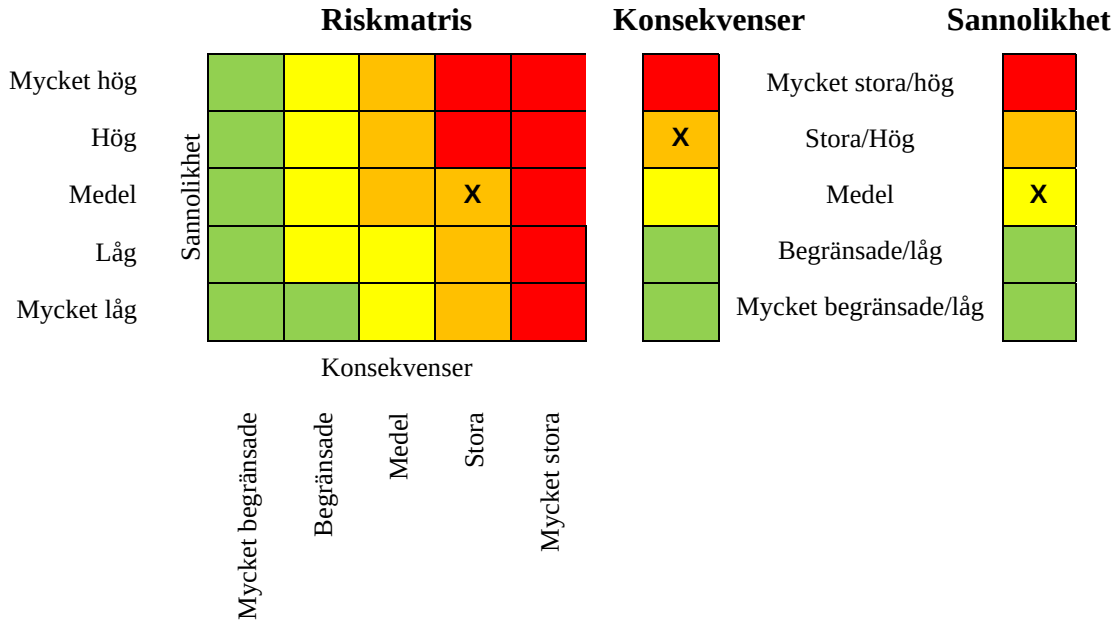
3.7.3 A.3 Skadlig kod

Benämning	**A.3 Skadlig kod**
Risk-formulering	Risk för att obehöriga applikationer utför oönskade och obehöriga åtgärder i multisensorsystemet eller som utnyttjar svagheter för att få tillgång till systemet kan leda till att personuppgifter inte anonymiseras som tänkt, att rådata överförs till obehöriga eller att personuppgifter obehörigen ändras.

Risk					
Sannolikhet	Mycket låg	Låg	Medel	Hög	Mycket hög
Konsekvenser	Mycket begränsade	Begränsade	Medel	Stora	Mycket stora
Andra omständigheter					
Geografisk omfattning			Enskild	Grupp	Samtliga
Hotets tidsutdräkt			Kort	Medel	Lång
Osäkerhet			Låg	Medel	Hög

Konsekvenser av det inträffade Konsekvenser för enskildas fri- och rättigheter
Det kan leda till allvarliga psykiska sjukdomar hos registrerade som till exempel depression eller utveckling av fobier när det blir känt att obehöriga kunnat ta del av, spåra eller lagra uppgifter om enskilda eller att uppgifterna faktiskt inte anonymiseras.

Målformulering
Multisensorsystemet har kontinuerligt uppdaterat skydd mot skadlig kod samt kan upptäcka och spåra obehörig tillgång till och ändring av uppgifter. Informationsägaren uppdaterar omgående multisensorsystemet när säkerhetsuppdateringar ges ut. Krav ställs på att leverantören vid behov uppdaterar multisensorsystemet under hela dess förväntade livslängd.



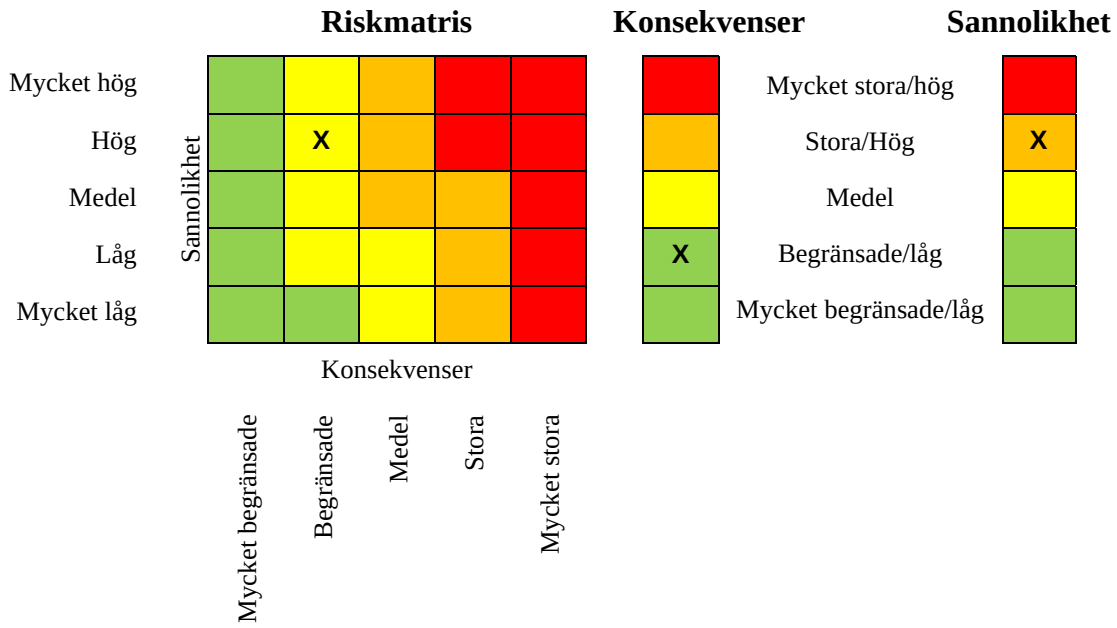
3.7.4 A.4 Obehörig fysisk modifiering

Benämning	**A.4 Obehörig fysisk modifiering**
Risk-formulering	Risk för vandalisering eller sabotage orsakar att sensorns upptagningsområde ändras och registrerar en annat upptagningsområde än som godkänts.

Risk					
Sannolikhet	Mycket låg	Låg	Medel	Hög	Mycket hög
Konsekvenser	Mycket begränsade	Begränsade	Medel	Stora	Mycket stora
Andra omständigheter					
Geografisk omfattning			Enskild	Grupp	Samtliga
Hotets tidsutdräkt			Kort	Medel	Lång
Osäkerhet			Låg	Medel	Hög

Konsekvenser av det inträffade Konsekvenser för enskildas fri- och rättigheter
Om annat upptagningsområde än godkänt registreras av sensorssystemet kan de leda till en känsla av intrång i privatlivet.

Målformulering
Rutiner och regelbundna kontroller finns för att kontrollera multisensorernas upptagningsområde varje vardag. Rutinerna och kontrollerna säkerställer avstängning av sensorer som har felaktigt upptagningsområde till dess sensorn korrigerats.



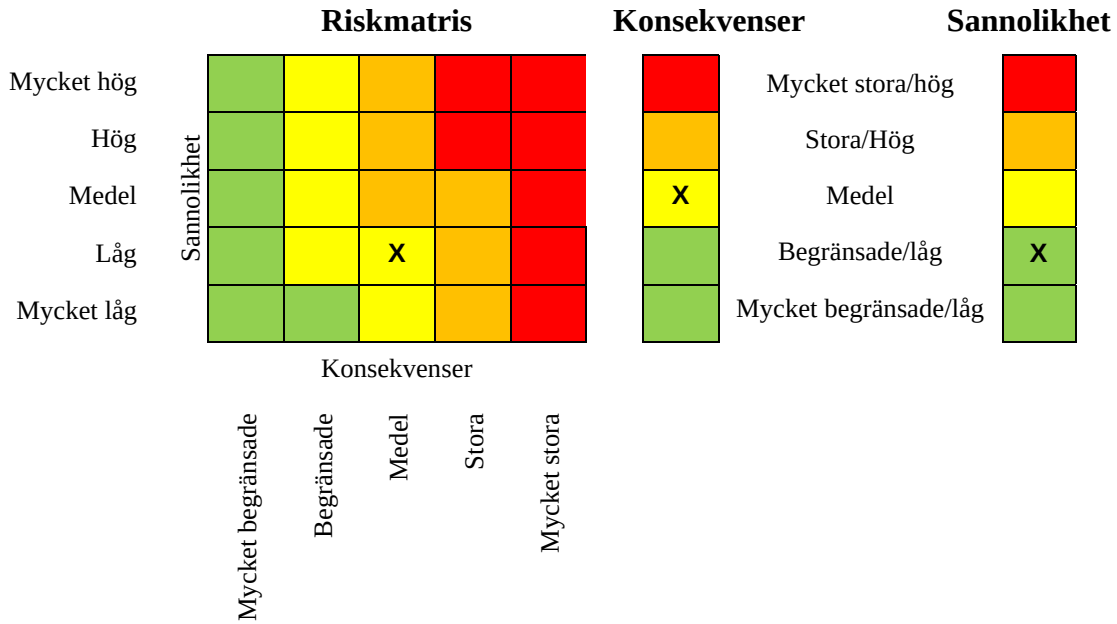
3.7.5 B.1 Fel i system, konfiguration eller handhavande

Benämning	**B.1 Fel i system, konfiguration eller handhavande**
Risk-formulering	Risk för att avsiktliga fel i programvarutjänster eller applikationer, felaktig installation eller konfigurering av multisensorsystemet leder till att rådata kan finnas tillgänglig för obehöriga eller att anonymisering inte görs korrekt.

Risk					
Sannolikhet	Mycket låg	Låg	Medel	Hög	Mycket hög
Konsekvenser	Mycket begränsade	Begränsade	Medel	Stora	Mycket stora
Andra omständigheter					
Geografisk omfattning			Enskild	Grupp	Samtliga
Hotets tidsutdräkt			Kort	Medel	Lång
Osäkerhet			Låg	Medel	Hög

Konsekvenser av det inträffade Konsekvenser för enskildas fri- och rättigheter
En enskild installatör som får tillgång till en större mängd bilder än som behövs och som inte är anonymiserade från en enskild sensor vid ett enskilt tillfälle innebär ingen eller mycket begränsad reell eller objektiv skada för intrång i privatliv. Om obehöriga får del av bilströmmars som inte anonymiserats kan det förmedla en känsla av brott mot grundläggande rättigheter.

Målformulering
Handhavandet av multisensorerna leder inte till att uppgifter hanteras eller lagras längre än vad som behövs för att lösa uppgifterna. Rutiner och regelbundna kontroller säkerställer att informationsägaren snabbt upptäcker bildströmmar som inte anonymiserats som de ska och säkerställer att de omedelbart åtgärdas.



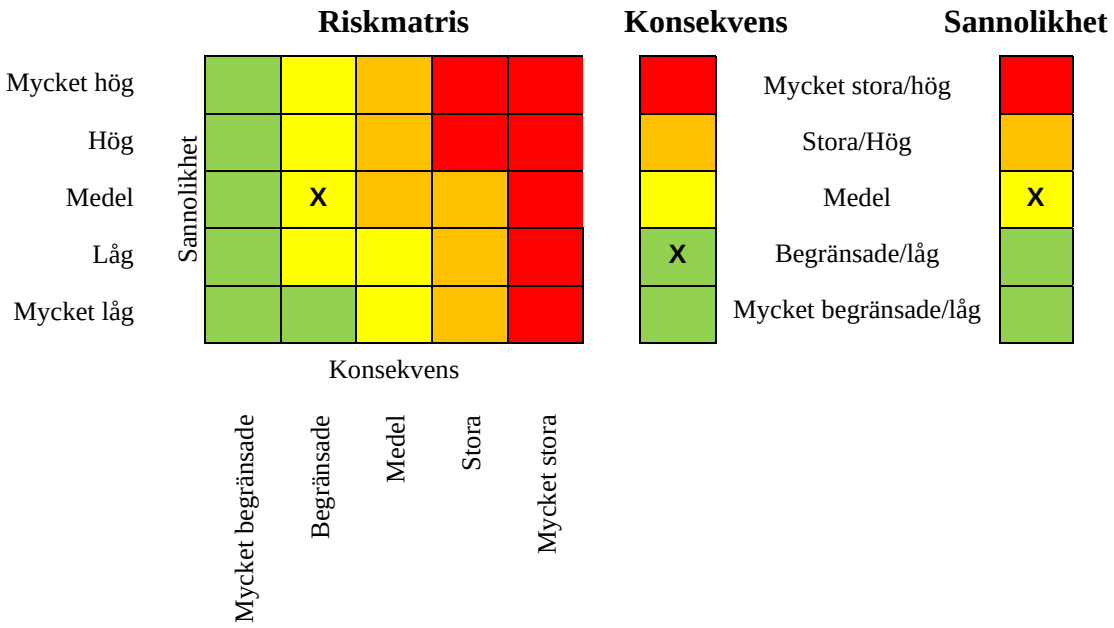
3.7.6 B.2 Avbrott i nätverk

Benämning	**B.2 Avbrott i nätverk**
Risk-formulering	Avbrott eller fel i nätverk eller strömförsörjning kan begränsa tillgången till de personuppgifter som behandlas.

Risk					
Sannolikhet	Mycket låg	Låg	Medel	Hög	Mycket hög
Konsekvens	Mycket begränsade	Begränsade	Medel	Stora	Mycket stora
Andra omständigheter					
Geografisk omfattning			Enskild	Grupp	Samtliga
Hotets tidsutdräkt			Kort	Medel	Lång
Osäkerhet			Låg	Medel	Hög

Konsekvenser av det inträffade Konsekvenser för enskildas fri- och rättigheter
Brist på tillgång gör att enskild omedelbart inte kan ta vara på sin rätt. Det kan innebära en rädsla av förlust av kontroll över sina personuppgifter och en känsla av intrång i privatlivet utan reell eller objektiv skada.

Målformulering
Multisensorsytemet har rimlig redundans i förhållande till risken för avbrott i elförsörjning eller kommunikation.



3.7.7 C.1 Naturhändelser

Benämning	**C.1 Naturhändelser**
Risk-formulering	Risk för att brand, kraftig kyla, värme eller vind eller andra liknande naturhändelser orsakar bortfall i tillgängligheten eller gör att sensorns upptagningsområde ändras.

Risk					
Sannolikhet	Mycket låg	Låg	Medel	Hög	Mycket hög
Konsekvenser	Mycket begränsade	Begränsade	Medel	Stora	Mycket stora
Andra omständigheter					
Geografisk omfattning			Enskild	Grupp	Samtliga
Hotets tidsutdräkt			Kort	Medel	Lång
Osäkerhet			Låg	Medel	Hög

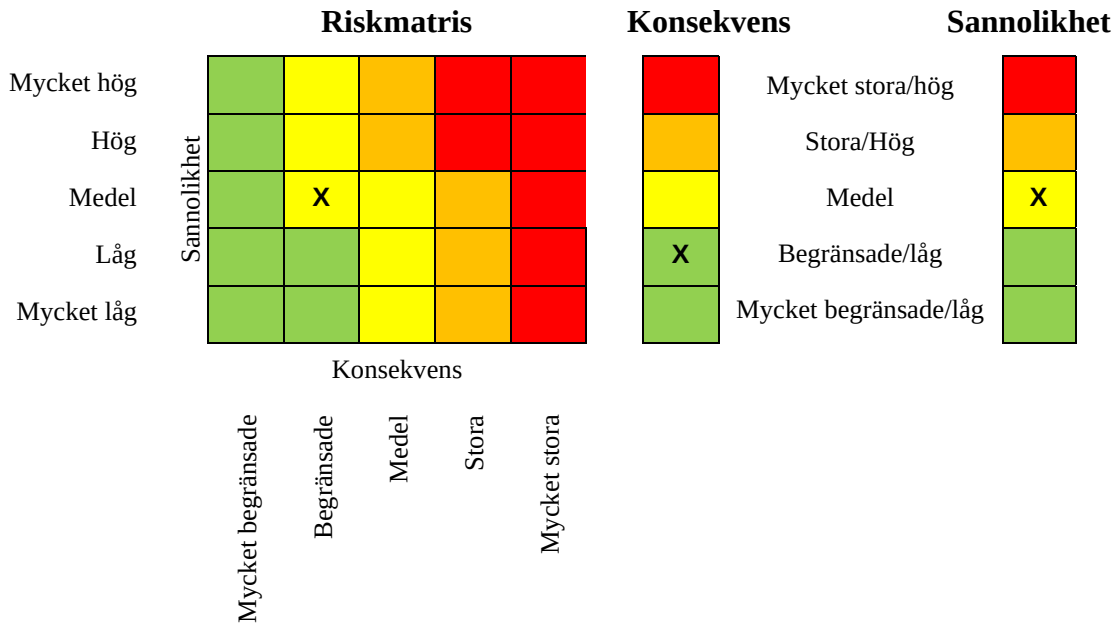
Konsekvenser av det inträffade
Konsekvenser för enskildas fri- och rättigheter

Brist på tillgång gör att enskild omedelbart inte kan ta vara på sin rätt. Det kan innebära en rädsla av förlust av kontroll över sina personuppgifter och en känsla av intrång i privatlivet utan reell eller objektiv skada.

Om annat upptagningsområde än godkänt registreras av sensorssystemet kan de leda till en känsla av intrång i privatlivet.

Målformulering

Rutiner och regelbundna kontroller finns för att kontrollera multisensorernas upptagningsområde varje vardag. Rutinen säkerställer avstängning av sensorer som har felaktigt upptagningsområde till dess sensorn korrigerats.



3.7.8 D.1 Anonymisering inte längre funktionell

Benämning	**E.1 Anonymisering inte längre funktionell**
Risk-formulering	Risk för att den tekniska utvecklingen eller andra händelser gör att den data som ska anonymiseras kan kopplas till enskilda individer och därigenom inte längre kan sägas vara anonymiserad.

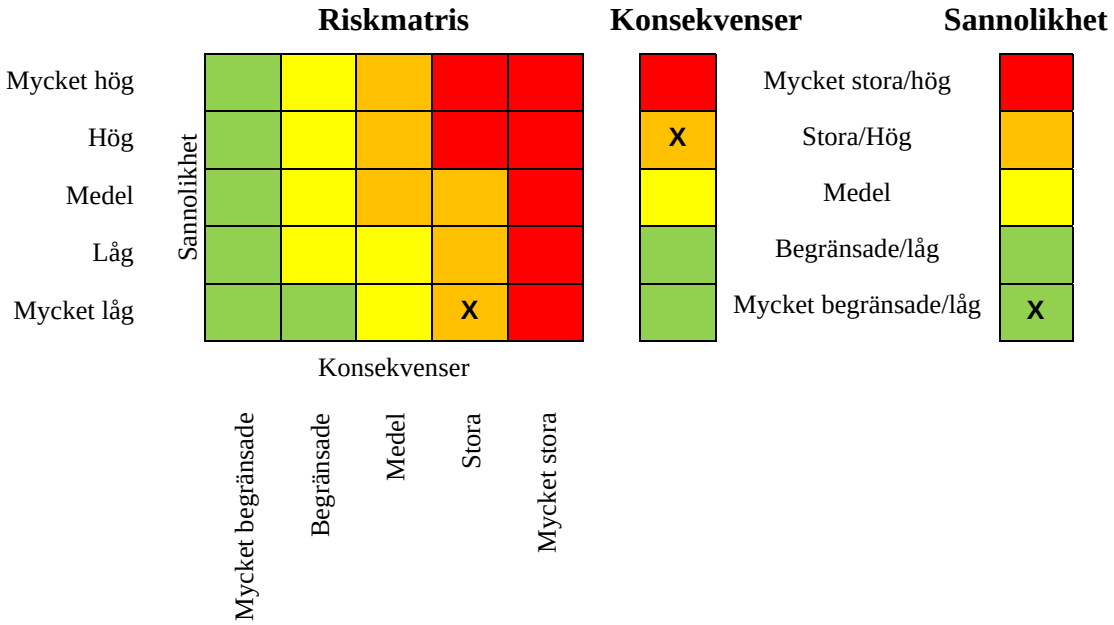
Risk					
sannolikhet	Mycket låg	Låg	Medel	Hög	Mycket hög
Konsekvenser	Mycket begränsade	Begränsade	Medel	Stora	Mycket stora
Andra omständigheter					
Geografisk omfattning			Enskild	Grupp	Samtliga
Hotets tidsutdräkt			Kort	Medel	Lång
Osäkerhet			Låg	Medel	Hög

Konsekvenser av det inträffade
Konsekvenser för enskildas fri- och rättigheter

Enskilda registrerade kan identifieras i de dataset som tidigare varit anonyma. Vilket skulle kunna innebära att enskildas rörelsemönster kan kartläggas och följas såväl historiskt som i realtid. Det kan innebära stora konsekvenser för enskilda och en känsla av långsiktig övervakning vilket skulle kunna leda till utveckling av psykiska sjukdomar såsom depression eller utveckling av fobi för allmänna platser.

Målformulering

Multisensorsystemet säkerställer anonymisering av bildströmmar och andra uppgifter som produceras av systemet under hela dess livslängd. Gallringsrutiner för anonymiserade uppgifter finns.



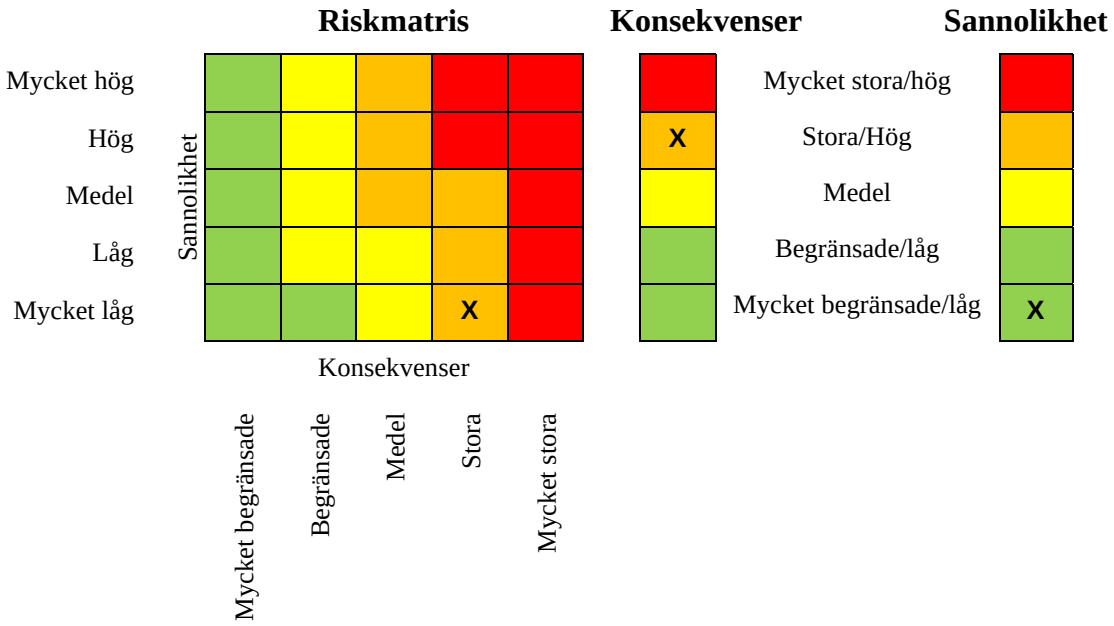
3.7.9 D.2 Omfattande lagring av anonymiserade uppgifter

Benämning	**E.2 Omfattande lagring av anonymiserade uppgifter**
Risk-formulering	Risk för att stora mängder anonymiserade uppgifter ansamlas och underlättar för framtida identifiering av enskilda.

Risk					
sannolikhet	Mycket låg	Låg	Medel	Hög	Mycket hög
Konsekvenser	Mycket begränsade	Begränsade	Medel	Stora	Mycket stora
Andra omständigheter					
Geografisk omfattning			Enskild	Grupp	Samtliga
Hotets tidsutdräkt			Kort	Medel	Lång
Osäkerhet			Låg	Medel	Hög

Konsekvenser av det inträffade Konsekvenser för enskildas fri- och rättigheter
Omfattande ansamling av anonymiserade data kan leda till att enskilda registrerade kan identifieras i de dataset som tidigare varit anonyma. Vilket skulle kunna innebära att enskildas rörelsemönster kan kartläggas och följas såväl historiskt som i realtid. Det kan innebära stora konsekvenser för enskilda och en känsla av långsiktig övervakning vilket skulle kunna leda till utveckling av psykiska sjukdomar såsom depression eller utveckling av fobi för allmänna platser.

Målformulering
Anonymiserade uppgifter lagras inte längre än vad som behövs för verksamhetens behov.



3.8 Riskhantering

Eftersom detta är en referenskonsekvensbedömning och inte en konsekvensbedömning för ett visst specifikt system från en viss specifik leverantör kan det i detta dokument inte fastställas några exakta planerade åtgärder för att hantera de risker som identifierats i denna konsekvensbedömning. Detta hanteras i detalj i samband med kravställning inför upphandling och användning av multisensorer för de ändamål som anges i detta dokument.

Riskanalysen i avsnitt 3.7 har identifierat följande nio övergripande målsättningar som ska uppnås av multisensorsystemet för att minska riskerna för enskildas fri- och rättigheter.

1. Multisensorsystemet har implementerat säkerhetsåtgärder för att snabbt upptäcka och skydda mot dataläckor och avlyssning eller avlyssningsförsök.
2. Multisensorsystemet ska vara robust mot tillgänglighetsattacker och personuppgiftsansvarig har rutiner för att snabbt återställa funktionalitet för driften av sensorsystemet.
3. Multisensorsystemet har kontinuerligt uppdaterat skydd mot skadlig kod samt kan upptäcka och spåra obehörig tillgång till och ändring av uppgifter. Informationsägaren uppdaterar omgående multisensorsystemet när säkerhetsuppdateringar ges ut. Krav ställs på att leverantören vid behov uppdaterar multisensorsystemet under hela dess förväntade livslängd.
4. Rutiner och regelbundna kontroller finns för att kontrollera multisensorernas upptagningsområde varje vardag. Rutinerna och kontrollerna säkerställer avstängning av sensorer som har felaktigt upptagningsområde till dess sensorn korrigerats.
5. Handhavandet av multisensorerna leder inte till att uppgifter hanteras eller lagras längre än vad som behövs för att lösa uppgifterna. Rutiner och regelbundna kontroller säkerställer att informationsägaren snabbt upptäcker bildströmmar som inte anonymiserats som de ska och säkerställer att de omedelbart åtgärdas.
6. Multisensorsystemet har rimlig redundans i förhållande till risken för avbrott i elförsörjning eller kommunikation.
7. Rutiner och regelbundna kontroller finns för att kontrollera multisensorernas upptagningsområde varje vardag. Rutinen säkerställer avstängning av sensorer som har felaktigt upptagningsområde till dess sensorn korrigerats.
8. Multisensorsystemet säkerställer anonymisering av bildströmmar och andra uppgifter som produceras av systemet under hela dess livslängd. Gallringsrutiner för anonymiserade uppgifter finns.
9. Anonymiserade uppgifter lagras inte längre än vad som behövs för verksamhetens behov.

Dessa målsättningar kan användas som stöd för att identifiera möjliga och riskreducerande åtgärder.

Svenska stadsnätsföreningen har tagit fram en *Vägledning för robust & säker IoT*.[15] Nedanstående grundläggande kravkatalog bygger på *Vägledning för robust & säker IoT* men har anpassats och utökats något för att passa multisensorsystem i syfte att minska riskerna för enskildas fri- och rättigheter. Denna kravkatalog uppmärksammar antal åtgärder som bedöms minska riskerna för enskildas fri- och rättigheter och bör ingå som krav vid upphandling och införande av multisensorsystem.

Exempel på åtgärder för att minska riskerna som anges i riskanalysen kan delas in i tre huvudkategorier,[16]

1. säkerhetspolicy,
2. organisation, personal och processmätvärden, samt
3. tekniska åtgärder.

3.8.1 Säkerhetspolicy

Den personuppgiftsansvariga ska ha en säkerhetspolicy eller liknande styrdokument upprättat. Säkerhetspolicyn ska inriktas på dataskydd samt informations- och it-säkerhet. Säkerhetspolicyn ska syfta till att göra arbetet mer konkret och åtgärderna mer robusta. En säkerhetspolicy ska beskriva hur den personuppgiftsansvariga ska skydda enskilda och verksamheten mot hot, inklusive dataskydds- och datasäkerhetshot och hur den personuppgiftsansvariga hanterar situationer när de inträffar. Den personuppgiftsansvariga ska även upprätta en it-säkerhetspolicy eller liknande styrdokument som identifierar regler och procedurer för alla individer som får tillgång till och använder multisensorerna. Målet för it-säkerhetspolicyn är att bevara konfidentialitet, riktighet och tillgänglighet för multisensorsystemet till skydd för enskildas fri- och rättigheter. Inom ramen för säkerhetspolicyn bör särskilt lyftas fram arbete med

1. inbyggt dataskydd,
2. inbyggd säkerhet,
3. inbyggd konfidentialitet, och
4. förvaltning av anläggningstillgångar.

3.8.1.1 Inbyggt dataskydd

Registrerade personer ska kunna utöva sina rättigheter avseende information, tillgång, och radering.

Personuppgifter ska enbart användas för de angivna ändamål för vilka de samlades in. Ytterligare behandling av personuppgifter ska vara kompatibel med angivet ändamål och de registrerade ska vara välinformerade

Behandling av personuppgifter ska minimeras. Multisensorsystemet behöver bara anonymiserad data och behöver inte obearbetade data som samlas in av

[15] Robust och säker IoT, Vägledning för Robust och Säker IoT, ver 1.0, 2020-03-01.
[16] Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, ENISA, November 2017.

multisensorerna. Multisensorsystemet ska ta bort obearbetad data så snart de har extraherat de data som krävs för aktuell databehandling.

Multisensorsystemet ska beakta och tillämpa den senaste utvecklingen rörande avidentifieringsteknik och kunna implementera denna i multisensorsystemet. Europeiska dataskyddsstyrelsens yttrande 05/2014 om avidentifieringsmetoder ska beaktas.

Det ska vara möjligt att implementera rutiner för automatisk gallring av anonymiserade uppgifter.

Förteckning över insamlade och anonymiserade uppgifter ska finnas och rutiner för gallring av anonymiserade uppgifter ska finnas.

Kontroll och verifiering av om ändamålen med behandlingen uppfylls ska genomföras regelbundet.

3.8.1.2 Inbyggd säkerhet

Arkitekturen ska kunna byggas i segment/delar som kapslar in/isolerar element i händelse av attacker.

Möjligheten att integrera olika Säkerhetspolicyer (inklusive roller och ansvar) och tekniker för en konsekvent säkerhetskontroll av olika enheter och användarnät ska kunna säkerställas.

Leverantörer ska kunna implementera testplaner för att verifiera att en produkt som installeras i ett multisensorsystem fungerar som förväntat. Testplanerna ska också omfatta felaktig beteende t. ex. handhavandefel.

Separata miljöer för utveckling, testning och produktion ska kunna användas så att operativa verksamhetsprocesser och produktionsdata inte påverkas vid fel i utvecklings- och testprocessen.

Vid utformning av lösningar för energibesparing får säkerheten inte äventyras.

Vid utformningen av säkerhetslösningar ska risken för människors säkerhet samt enskildas fri- och rättigheter vägas in.

Säkerheten för hela multisensorsystemet ska kunna hanteras genom ett konsekvent förhållningssätt under systemets hela livscykel.

3.8.1.3 Inbyggd konfidentialitet

Konfidentialitet ska vara en vägledande princip vid utformning och utveckling av multisensorsystemet och vara en integrerad del av systemet.

3.8.1.4 Förvaltning av anläggningstillgångar

Alla tillgångar som ingår i en multisensorsystemet ska kunna identifieras, verifieras och förtecknas. Detta ska hanteras i ett system för förvaltning och konfigurationskontroll.

Det ska finnas en förteckning över den hård- och mjukvarvara som är godkänd för användning i multisensorverksamheten. Förteckningen ska inkludera ägarskap för tillgångarna.

För att ha kontroll över var och hur verksamhetskritisk information hanteras ska dataflödet inom multisensorsystemet och mellan systemdelar kunna identifieras och dokumenteras.

3.8.2 Organisation, personal och processmätvärden

Den personuppgiftsansvariga ska ha organisatoriska kriterier för hantering av informationssäkerhet och dataskydd. Personalrutiner ska främja god säkerhet, säkerställa hanteringen av processer och en säker hantering av information hos den personuppgiftsansvariga. Inom ramen för organisation, personal och processmätvärden bör följande särskilt uppmärksammas

1. stöd under och efter systemets livscykel,
2. beprövade lösningar,
3. hantering av säkerhetsproblem och incidenter,
4. personalresurser, säkerhetsträning och medvetenhet, och
5. tredjepartsrelationer.

3.8.2.1 Stöd under och efter systemets livscykel

Det ska finnas en funktion för att hämta korrigeringar för kända sårbarheter i mjukvara och hårdvara fram till slutdatum för multisensorernas livscykel.

Det ska finnas en strategi för hur multisensorer och multisensorsystemet ska hanteras när produkter är uttjänta och när support inte längre ges av leverantören.

Det ska finnas en produktavvecklingsplan för att hantera uttjänta produkter och när support inte längre ges av leverantören eller när systemet av andra skäl ska avvecklas.

Tiden för hur länge uppdateringar och support löper efter produktgarantins utgång ska anges.

3.8.2.2 Beprövade lösningar

Beprövade lösningar erkända av standardiseringsorgan ska användas om möjligt, det vill säga välkända kommunikationsprotokoll och kryptografiska algoritmer.

3.8.2.3 Hantering av säkerhetsproblem och incidenter

Det ska finnas en funktion för att informera intressenter om upptäckta sårbarheter, mjukvaru- och hårdvaruuppdateringar, rättelser samt metoder för att ta itu med identifierade sårbarheter.

Det ska finnas en process för identifiering och rapportering av personuppgiftsincidenter.

Det ska finnas en process för analys och hantering av säkerhetsincidenter. För varje händelse ska det finnas ett svar på:

1. arten och omfattningen av händelsen

2. hur man ska ta kontroll över situationen
3. hur man ska kommunicera med användarna
4. hur man säkerställer en snabb och effektiv hantering av informationssäkerhetsincidenter.

Det ska finnas en offentliggjord process för sårbarhetsrapporter. Till exempel hittelön för personer som identifierar sårbarheter som den personuppgiftsansvarigas egna interna säkerhetsarbete inte upptäckt.

3.8.2.4 Personalresurser, säkerhetsträning och medvetenhet

Utbildningsaktiviteter för personalen ska dokumenteras och följas upp.

Personalrutiner ska främja dataskydd integritet och säkerhet. Personal som arbetar med multisensorsystemet ska utbildas i dataskydd och säkerhetspraxis för säker användning av systemen, och ska förstå att teknisk kompetens inte nödvändigtvis motsvarar säkerhetskompetens.

It-säkerhetsroller och ansvar för all personal ska vara infört innan drift av multisensorsystemet påbörjas.

3.8.2.5 Tredjepartsrelationer

Data som behandlas av en tredje part ska skyddas genom ett databehandlingsavtal med tredjepartsleverantören.

En tredjeparts tjänsteleverantör ska tillämpa samma policyer som den personuppgiftsansvariga, inklusive att hålla sådana uppgifter konfidentiella och med anmälningskrav vid incidenter.

Leverantören av multisensorsystemet ska ha riskhanteringspolicy eller liknande för sina leveranskedjor.

3.8.3 Tekniska åtgärder

För att minska sårbarheten i ett multisensorsystem ska säkerhetsåtgärder och god praxis implementeras och omfatta systemets tekniska element under hela dess livslängd. Tekniska mätvärden ska ge nödvändiga indata för de tekniska åtgärder som krävs för att bevara och skydda informationssäkerheten. Vid tillämpning av dessa tekniska åtgärder ska hänsyn tas till att ett multisensorsystem kan inkludera ett stort antal enheter och produkter och vissa åtgärder behöva utföras med specialiserade arkitektoniska komponenter, till exempel nätverksnoder (gateways). Tekniska åtgärder bör särskilt beakta

1. hårdvarusäkerhet,
2. förtroende och integritetshantering,
3. stark grundläggande säkerhet och konfidentialitet,
4. systemsäkerhet och tillförlitlighet,
5. säker programvara och uppdatering av fast programvara,
6. autentisering,
7. tillstånd,
8. tillgångskontroll och fysisk säkerhet,

9. kryptografi,
10. säker och betrodd kommunikation,
11. säkra gränssnitt och nätverkstjänster,
12. säker in- och utloggning,
13. loggning, samt
14. övervakning och revision.

3.8.3.1 Hårdvarusäkerhet

Det ska finnas en hårdvarubaserad, oföränderlig hårdvarukomponent som alla säkra funktioner i ett datorsystem är beroende av, som bland annat innehåller betrott exekveringsmiljö, nycklarna som används för kryptografiska funktioner och möjliggör en säker startprocess.

Hårdvara som innehåller säkerhetsfunktioner för att stärka sensorns skydd och integritet ska användas t.ex. specialiserade säkerhetschips/coprocessors [System-on-a-Chip (SoC)] som integrerar säkerhet på transistornivå, inbäddade i processorn, som understödjer:

1. Chain of trust boot-loader som autentiserar operativsystemet innan det laddas,
2. operativsystem Chain of Trust som autentiserar applikationsprogramvara innan den laddas,
3. en säker startprocess för maskinvara och låsning av kritiska delar av minnet,
4. skyddat minne (NVM / RAM / Cache) för att undvika otillåten access till enhetens data och dekompilering,
5. kryptering och anonymitet,
6. slumptalsgenerator,
7. detektering av manipulation,
8. miljöövervakning och intern kontroll,
9. en tillförlitlig exekveringsmiljö,
10. en säker kodhämtning och exekvering (integritetskontroller),
11. kod- och datasignaturer, byggda under sammanställning och lagras och verifieras under körning,
12. en pålitlig lagring av enhetsidentitet och autentiseringsmedel, inklusive skydd av nycklar i vila och vid användning,
13. skydd mot privilegierad åtkomst till säkerhetskänslig kod, samt
14. skydd mot lokala och fysiska attacker kan täckas via funktionell säkerhet.

3.8.3.2 Förtroende och integritetshantering

Kod ska vara kryptografiskt signerad för att säkerställa att den inte har manipulerats efter att ha skrivits in som säker för enheten. Endast signerad kod ska användas.

Realtidsskydd ska vara implementerat och exekverings-övervakning ska användas för att säkerställa att skadliga attacker inte skriver över kod efter att den har laddats.

Installation av programvara i system i drift ska övervakas, för att förhindra att inte autentiserad programvara och/eller filer kan installeras.

Endast behörig programvara ska tillåtas i sensorsystemet.

Startprocessen ska initiera de viktigaste hårdvarukomponenterna och starta operativsystemet. Förtroende måste etableras i startmiljön innan något förtroende för någon annan programvara eller ett exekverbart program kan hävas, så den uppstartade miljön måste verifieras och beslutas vara i ett kompromisslöst tillstånd.

Efter att ett driftavbrott har inträffat, eller om en uppgradering inte har lyckats, ska det finnas en funktion för att återställa systemet till ett tillstånd som är känt för att vara säkert.

Tillförlitliga och betrodda protokoll och mekanismer ska användas för att representera och hantera förtroende och förtroenderelationer.

Varje kommunikationskanal ska ha en tillförlitlighet som står i proportion till de säkerhetsberoende som den stöder.

3.8.3.3 Stark grundläggande säkerhet och konfidentialitet

Alla tillämpliga säkerhetsfunktioner ska vara aktiverade i grundutförande. Alla eventuella oanvända tjänster och protokoll ska vara avaktiverade som standard. En stark säkerhetskontroll måste vara något som användaren avsiktligt måste inaktivera.

Om enskilda sensorer har individuella lösenord ska det finnas funktioner och rutiner som gör det svårt att knäcka en sensors individuella lösenord.

3.8.3.4 Systemsäkerhet och tillförlitlighet

Multisensorerna ska utformas och byggas så att driftstörningar inte leder till en större störning av systemet, skada eller avbrott i säkerhetskritiska processer.

Viktiga funktioner ska fortsätta att fungera även vid avbrott i kommunikationen och kontinuerlig negativ påverkan från komprometterade enheter eller molnbaserade system. En förlust av kommunikationen får inte äventyra enhetens integritet.

Det ska finnas mekanismer för självdiagnos och självreparation för återställning efter fel, funktionsfel eller komprometterade tillstånd.

3.8.3.5 Säker programvara och uppdatering av fast programvara

Endast godkänd programvara ska få köras (Vitlistning) och eventuella makron ska vara inaktiverade.

Säkerhetsuppdateringar ska installeras så fort det går.

Automatiska uppdateringar av fast programvara ska vara aktiverade som standard.

En enhet kan erbjuda ett alternativ som inaktiverar automatiska uppdateringar av fast programvara och med krav på autentisering. Erbjuds en automatisk uppdateringsmekanism för fast programvara så ska enheterna konfigureras för att kontrollera om det finns regelbundna uppdateringar av fast programvara.

Automatiska uppdateringar av fast programvara ska inte ändra nätverksprotokollens gränssnitt på ett sätt som är oförenligt med tidigare versioner.

Uppdateringar och korrigeringsfiler ska inte ändra användarinställda inställningar, säkerhets- och/eller sekretessinställningar utan användaranmälan.

Användare ska ha möjlighet att godkänna eller avvisa uppdateringar.

Innan en uppdateringsprocess påbörjas ska följande kontrolleras:

1. att enhetens programvara / fast programvara, dess konfiguration och dess applikationer har möjlighet att uppdateras,
2. att uppdateringsservern är säker,
3. att uppdateringsfilen överförs via en säker anslutning,
4. att filen inte innehåller känsliga data (t.ex. hårdkodade uppgifter),
5. att filen är signerad av en auktoriserad tillitsenhet och krypterad med hjälp av accepterade krypteringsmetoder, samt
6. att uppdateringspaketet har sin digitala signatur, signeringscertifikat och signaturcertifikat, verifierat av enheten innan uppdateringsprocessen börjar.

3.8.3.6 Autentisering

Inloggningsförsök ska skyddas mot s.k. brute force-attacker (en metod för att hitta exempelvis lösenord genom att pröva alla möjliga kombinationer) och/eller andra misstänksamma inloggningsförsök (till exempel automatiserade inloggningsrobotar etcetera) genom att låsa eller inaktivera användar- och supportkonton (er) efter ett rimligt antal ogiltiga inloggningsförsök.

Autentiseringsuppgifter, inklusive men inte begränsade till användarlösenord, ska vara innehålla slumpdata (saltade), Hashsummeberäknade och/eller krypterade.

Lösenordsåterställning eller återställningsmekanismen ska vara robust och inte ge en angripare information som avser ett giltigt konto. Detta gäller också för viktiga uppdaterings- och återhämtningsmekanismer.

Utformningen av autentiserings- och auktoriseringssystemen (unika per enhet) ska baseras på identifierade hotmodeller på systemnivå.

Multisensorerna ska innehålla mekanismer för att på ett tillförlitligt sätt kunna verifiera sina backend-tjänster och för att stödja applikationer.

Standardlösenord och standardanvändarnamn, ska ändras efter den ursprungliga installationen, svaga, inga eller tomma lösenord ska inte tillåtas.

Godkännandemekanismer ska använda starka lösenord eller personliga identifikationsnummer (PIN-koder). Tvåfaktorsautentisering rekommenderas.

3.8.3.7 Tillstånd

Det ska finnas ett dokumenterat arbetssätt med tydliga processer och rutiner för att förvalta användarkonton, roller och behörigheter. Arbetssättet ska inkludera hur ansvaret för förvaltningen ser ut.

De olika användarkategorier som finns i verksamheten ska kartläggas och definieras för att fastställa behovet av regelbunden uppföljning och kontroll av dessa.

Ansvar och ansvarsområden som står i konflikt med varandra ska skiljas så att ingen enskild person kan få tillgång till, ändra eller använda tillgångar utan tillstånd eller upptäckt.

Fast programvara för enheter ska utformas för att isolera priviligierad kod, processer och data från de delar av den fasta programvaran som inte behöver åtkomst till dem.

För att minska risken för att kompromitterad kod får tillgång till säkerhetskänslig kod och/eller data ska enhetshårdvara tillhandahålla ett isoleringskoncept.

Administratörsrättigheterna och behörigheterna för tillåtna åtgärder för ett visst system ska begränsas.

Regelverk för Åtkomstkontroll och finkorniga auktorisationsmekanismer -såsom Attributbaserad åtkomstkontroll eller Rollbaserad åtkomstkontroll - för att utföra privilegierade åtgärder, åtkomst till filer och kataloger, applikationer, etc. ska implementeras. Principen om minst behörighet bör tillämpas det vill säga applikationerna måste fungera på lägsta möjliga privilegienivå.

Använd automatiserade och centrala verktyg för att styra åtkomst och behörigheter samt till att hålla en aktuell översikt av alla de konton och dess behörigheter som de har över tid. Godkännande av behörigheter/användarrättigheter måste kunna spåras till en ansvarig person och när i tiden ändringar av rättigheten skedde.

3.8.3.8 Tillgångskontroll och fysisk säkerhet

Eftersom vissa enheter, till exempel sensorer eller nätverksnoder, kan behöva hanteras på distans snarare än att manövreras manuellt på plats ska åtgärder för att detektera och hantera manipulering vidtas.

Detektering och reaktion på manipulering av hårdvara ska inte förlita sig på nätverksanslutning.

Enheter ska endast ha de fysiska externa portar (till exempel USB) som är nödvändiga för dess funktion.

Test/debug-läge ska inte kunna användas för att komma åt och/eller skada enheterna.

Dataintegritet och konfidentialitet ska hanteras genom åtkomstkontroll. Har någon/något fått tillstånd att få tillgång till särskilda processer är det nödvändigt att tillämpa den definierade säkerhetspolicyn.

Enheter ska inte enkelt kunna demonteras och datalagringsmedium ska vara krypterade i vila och inte enkelt kunna tas bort.

3.8.3.9 Kryptografi

Kryptografiska nycklar ska hanteras säkert.

Enheter ska byggas så att de är kompatibla med lämplig kryptering och säkerhetsteknik (inklusive säker identifiering, säker konfiguration).

En korrekt och effektiv användning av kryptografi ska användas för att skydda konfidentialitet och riktighet av data och information (inklusive kontrollmeddelanden) både vid överföring och i vila. Osäkra protokoll ska vara inaktiverade. Robustheten för implementationen ska verifieras.

Det ska finnas skalbara nyckelhanteringssystem.

3.8.3.10 Säker och betrodd kommunikation

Kommunikationssäkerheten ska tillhandahållas med hjälp av moderna standardiserade säkerhetsprotokoll.

Sammankopplingar ska alltid verifieras.

Det ska finnas funktioner för att upptäcka, identifiera och verifiera/autentisera enheter som ansluts till nätverket innan förtroende upprättas.

Specifika portar och/eller nätverksanslutningar för selektiv anslutning ska vara inaktiverade.

Automatisk portscanning ska göras regelbundet mot alla servrar som bedöms vara centrala och ska jämföras mot godkänd konfiguration. Om förändringar upptäcks, och som inte är en del av verksamhetens godkända konfiguration, ska det loggas, rapporteras automatiskt och gås igenom manuellt.

De olika säkerhetsaspekterna för informationen – konfidentialitet, riktighet, tillgänglighet– ska garanteras under överföringen i nätverket och vid lagringen i applikationen eller i molnet, med hjälp av datakrypteringsmetoder för att minimera nätverkshot, såsom återspelning, avlyssning och paketanalyserarare.

För att minska risken för automatiska attacker ska det ska finnas möjlighet att kontrollera trafiken, hastighet/mängd som skickas eller tas emot av ett nätverk.

Sensorerna ska vara restriktiva istället för tillåtande vid kommunikation.

Sensorerna ska inte förlita sig enbart på nätverksbrandväggen för att begränsa kommunikationen om vissa kommunikationer mellan enheterna i sensorsystemet inte går igenom en brandvägg.

Dataintegritet ska garanteras för att möjliggöra tillförlitligt datautbyte.

Autentiseringsinformation till exempel lösenord eller certifikat ska inte exponeras vid intern eller extern nätverkstrafik.

Obehöriga anslutningar till enheten eller andra enheter som produkten är ansluten till, och på alla nivåer i protokollen, ska förhindras.

Sensorer ska meddela och/eller begära en användarbekräftelse när de initialt integreras, kopplas ihop och/ eller ansluts till andra enheter, plattformar eller tjänster.

3.8.3.11 Säkra gränssnitt och nätverkstjänster

Protokoll ska utformas för att säkerställa att om en enda enhet är komprometterad, så ska denna inte kunna påverka övriga systemenheter.

Eventuella felmeddelanden ska ge/visa endast den korta informationen användaren behöver - den får inte avslöja känslig information som kan utnyttjas av en angripare, till exempel ett fel-ID, en version av webbservern etc.

Användarsessionen i webbgränssnittet ska vara helt krypterad från enheten till backend-tjänsterna, och de ska inte vara mottagliga för skadlig kodning som till

exempel ”Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection and HTML Injection”.

Samma hemliga nyckel ska undvikas i en hel produktfamilj, eftersom tillgång till nyckeln för en enda enhet skulle räcka för att avslöja resten av produktfamiljen. Varje enhet ska ha egengenererade nycklar.

En DDoS-resistent och lastbalanserad infrastruktur ska implementeras för att skydda tjänsterna mot DDoS-attacker som kan påverka enheten själv eller andra enheter och/eller användare i det lokala nätverket eller andra nätverk.

Endast nödvändiga portar ska vara öppna och tillgängliga.

Nätverkselement ska delas upp i separata komponenter (risksegmentering) för att hjälpa till att isolera säkerhetsbrott och minimera den totala risken.

Segmentera nätverken och filtrera trafiken mellan nätverken.

3.8.3.12 Säker in- och utmatning

Validering av att data är säker för användning ska ske vid inmatning (validering) och utmatning (filtrering) av data.

3.8.3.13 Loggning

Det ska finnas en rutin för logghantering.

Det ska finnas ett loggningssystem som registrerar händelser som rör användarautentisering, hantering av konton och åtkomsträttigheter, ändringar av säkerhetsregler och systemets funktion. Loggarna måste också bevaras under angiven tid i varaktigt lagringsutrymme och kunna återvinnas via en autentiserad anslutning.

Loggar ska vara konfigurerade så att de skickas centralt och analyseras.

Alla system som loggas ska synkroniseras mot samma tidkälla och tidszon.

Det ska finnas tillräcklig behörighetsstyrning för att ta del av innehållet i loggar. Loggar ska skyddas mot obehörig förändring.

Loggningsinställningar och loggningsdata ska valideras.

Loggar ska kunna synkroniseras mot minst två referenstidskällor så att aktiviteter förses med en korrekt tidsstämpel och kan läsas av kronologiskt.

Loggarna ska arkiveras och signeras digitalt med jämna mellanrum för att bevara riktigheten i loggarna.

Loggar ska använda ett standardiserat format så att de enkelt kan läsas av tredje parts logganalysverktyg.

Behovet av loggning av metadata och/eller innehåll bör vägas mot användarens respektive verksamhetens behov av skydd för konfidentialitet och bör beskrivas.

3.8.3.14 Övervakning och revision

Regelbundna granskningar och översyner av säkerhetskontrollerna ska utföras för att säkerställa att kontrollerna är effektiva.

Penetrationstest ska utföras minst en gång per år.

Det ska genomföras en regelbunden övervakning för att verifiera en enhets beteende, upptäcka skadlig kod och upptäcka integritetsfel.

Det ska finnas ett automatiserat system för övervakning av konfiguration som verifierar alla externt testbara element och som varnar när obehöriga ändringar förekommer. Detta inkluderar funktionalitet för att övervaka ändringar i brandväggskonfiguration (t ex öppning av nya portar), nya administrativa användare och nya tjänster som körs i ett system.

Automatiska verktyg för att säkerställa att kritiska systemfiler inte har ändrats ska användas. Kontrollerna bör identifiera misstänkta systemändringar såsom ändringar av ägare och behörigheter för filer eller kataloger, användning av alternativa dataströmmar som kan användas till att dölja illasinnade aktiviteter samt införande av extra filer till mappar som är avsedda för operativsystemet. Upptäckt av sådant kan indikera på skadlig kod som angripare lämnat eller filer som är felaktigt lagda vid batch- distributionsprocesser.

3.9 Kvarstående risker och kontinuitetsplanering

De sammantagna åtgärder som nämnts ovan i form av mål och grundläggande krav på ett multisensorsystem på såväl system som användning ger ett verktyg för att minska riskerna för enskildas fri- och rättigheter till en acceptabel nivå i förhållande till de samhällsekonomiska nyttor som multisensorer kan generera.

Icke desto mindre går det inte att bortse från att användning av multisensorer kan innebära en mycket omfattande kamerabevakning av ett stort antal allmänna platser inom tätbebyggt område och på landsbygden inom en kommun. Även om multisensorsystemet fungerar precis som det är tänkt, det vill säga inom mycket kort tid anonymiserar de uppgifter som behövs för ändamålet och information om detta finns tillgänglig för alla på ett öppet, fullständigt och transparant sätt i omedelbar och medelbar anslutning till multisensorerna. Så kan det ändå inte uteslutas att enbart förekomsten av en stor mängd kameror i den offentliga miljön kan skapa en känsla hos enskilda av att vara övervakad även om det inte orsakar någon reell eller objektiv skada.

Därför är det viktigt att användning av multisensorer för dessa ändamål endast används i enlighet med tillstånd från Integritetsskyddsmyndigheten, att den personuppgiftsansvarig är transparent, kontinuerligt ser över verksamheten samt kontrollerar att den följer de tillstånd och villkor som Integritetsskyddsmyndigheten meddelar och ser till att verksamheten kan granskas och revideras utan allvarliga anmärkningar.

3.10 Etiska överväganden

Två rapporter som EU-kommissionen står bakom har beaktats för att förstå och belysa potentiella etiska risker. Många av principerna i dessa dokument återspeglas redan i dataskyddsförordningens regelverk samt andra lagar och regler, men det etiska

resonemanget är mer långtgående än dessa, bland annat på grund av att många etiska frågor inte är föremål för så specifik forskning eller har uppnått sådan konsensus att de kan ligga till grund för reglering.

I snabbrörliga processer som kännetecknas av stark innovation, som till exempel samhällets digitalisering, är det inte sällan så att utredningar ställer frågor för första gången. Etik är en levande fråga som behöver diskuteras och analyseras som en del av utvecklingsprocesser, och framför allt, aldrig förmodas vara ”färdigutredd” – det som inte var en uppenbar etisk problematik när man formulerade ett system kan vid närmare påseende, när systemet har använts ett tag, bli framstå som ett uppenbart problem.

Expertpanelrapporten från EU-kommissionen Ethics and data protection[17] berör etiska frågor som gäller all datainsamling och -behandling. I rapporten noteras ett antal indikatorer som kan innebära högre etisk risk, varav följande kan ses som relevanta för multisensorer.

- Känsligt data (i vilket politiska åsikter, fackligt engagemang och sexuell orientering ingår)
    - Det här är information som potentiellt kan härledas från rörelsemönster.
- Data om barn, sårbara individer och personer som inte givit samtycke.
- Databehandling i stor skala eller komplex, till exempel genom systematisk övervakning av en publikt tillgänglig plats, behandling eller analys av persondata i större skala eller flera dataset.
- Profilering av individer eller grupper.
- Automatiserat beslutstagande eller användning av artificiell intelligens för att analysera persondata.
- Databehandling i tredje land, det vill säga utanför EU och EES.

Med stöd i EU-kommissionens rekommendationer bör det göras en detaljerad etikanalys om högre etisk risk riskerar att föreligga, i vilket ingår planerad datainsamling och behandling, möjliga etiska risker och vilka praktiska steg som bör tas för att mildra riskerna.

I avsnitt 2.1 i detta dokument avhandlas ändamålet med behandlingen enligt denna referenskonsekvensbedömning och om en användare avviker från det angivna ändamålet är det viktigt att göra en förnyad avvägning av de etiska riskerna i relation till det allmänna intresset för dessa ytterligare ändamål. Som noteras i avsnitt 2.2.1 är den verksamhet som en kommunal myndighet bedriver av allmänt intresse, men ur en etisk synvinkel är det alltid önskvärt att kommunen gör en avvägning av de etiska riskerna i relation till det allmänna intresset i det enskilda fallet.

[17] Ethics and data protection, EU-Kommissionen, 2018.

Det ska noga framhållas att dataskyddsförordningen ställer krav på att personuppgifter som inhämtas och behandlas för ett särskilt angivet ändamål senare inte får användas för ändamål som är oförenligt med dessa ändamål, artikel 5 b dataskyddsförordningen.

När ett multisensorsystem används och genererar data kan det leda till att nya tidigare oförutsedda användningsområden för den anonymiserade datan upptäcks och efterfrågas. Även om ett sådant nytt användningsområde principiellt inte skulle vara oförenligt med det ursprungliga ändamålet bör ändamålen med behandlingen ändå uppdateras med den nya användningen. På detta sätt beaktas dels principen om öppenhet, dels hanteras risken för ändamålsglidning.

Ändamålsglidning kan ses som ett kontraktsbrott mot individen, särskilt som individer sällan har möjlighet att hålla sig uppdaterade om förändringar i reglerna runt deras insamlade persondata. PKU-registret blev föremål för diskussion när polisen i samband med utredningen av mordet på Anna Lindh fick tillgång till uppgifter ur registret trots att föräldrar endast lämnat medgivande på villkoret att deras barns blodprov endast ska användas till vård- och forskningssyften.[18] Utredningen Framtidens biobanker påpekade att ändamålsglidning riskerade att påverka tilliten till vård och forskning, och noterade att oklarheter i tillämpningsområdets avgränsning riskerar att inte bara försvaga rättssäkerheten och skyddet av den enskilda provgivaren, utan även att minska förtroende för lagen och för biobankerna.[19] Fortsatt tillit och tillvaratagande av individens intressen gynnas av tydliga och avgränsade ändamål som inte förändras ogenomtänkt.

Eftersom det finns uppenbara risker för enskildas fri- och rättigheter vid användning av multisensorer är det nödvändigt att tillämpa dataminimering, det vill säga att bara samla in, behandla, tillgängliggöra (internt och externt) samt lagra data i den mån detta tydligt behövs för att uppfylla ändamålet, och ta hänsyn till proportionalitetsprincipen. Att spara data, även om det är anonymiserat, innebär alltid en risk, som måste vägas mot värdet av att spara data. Anonymiserade videofilmer från kamerabevakning ska därför inte sparas längre än nödvändigt. En rutin för gallring av anonymiserat videomaterial måste därför finnas hos den personuppgiftsansvariga.

Som angetts i avsnitt 3.9 måste den personuppgiftsansvariga regelbundet omvärdera risken för avanonymisering (re-identifiering). Det finns en ständig risk för re-identifiering på grund av ny teknik, nya uppgifter eller läcka till tredje part med större möjlighet till re-identifiering.

EU-kommissionens oberoende expertgrupp på hög nivå för AI har tagit fram Etiska riktlinjer för tillförlitlig AI.[20] Riktlinjerna påpekar att tillförlitlig AI har tre

[18] Åklagarens agerande kritiserades av Justitieombudsmannen, JO 2006/07 s. 54, dnr. 5010-2003. Agerandet resulterade också i att Socialstyrelsen öppnade SOU 2018:4 s.175. ett tillsynsärende och kritiserade företrädarna för biobanken för att ha tillmötesgått åklagarens önskemål utan att begära tingsrättens prövning av frågan, se Tillhandahållande av vävnadsprover vid utredning av brott, Socialstyrelsen, dnr 51-10082/2003.
[19] SOU 2018:4 s.175.
[20] Etiska riktlinjer för tillförlitlig AI, 2019.

komponenter som ska finnas med under systemets hela livscykel. Den bör vara laglig, etisk och robust. Eftersom etiska frågor runt AI inbegriper frågor runt insamling, lagring och analys av data är dessa av relevans för referenskonsekvensbedömningen. Riktlinjerna berör framför allt de två senare punkterna; etisk och robust, samt innehåller vägledning om vilka grundläggande rättigheter som kan anses särskilt lämpliga att reflektera över etiskt.

Riktlinjerna beskriver fyra etiska principer som har sina rötter i de grundläggande rättigheterna:

i. respekt för människans autonomi,
ii. förebyggande av skada,
iii. rättvisa, och
iv. förklarbarhet.

Respekt för människans autonomi

Respekten för människors frihet och autonomi ska garanteras, och de ska ges möjligheten att fullt ut bestämma över sina egna liv och kunna delta i en demokratisk process. Expertgruppen noterar här att man måste säkerställa mänsklig tillsyn och kontroll över processerna. Inom ramen för denna konsekvensbedömning betyder det att det måste finnas mänsklig tillsyn vid automatisk anonymisering av videoströmmar, och denna tillsyn bör göras av individer som är medvetna om riskerna. Förutom den personuppgiftsansvarigas egna löpande tillsyn och kontroll, finns ett dataskyddsombud som ska övervaka efterlevnaden av dataskyddsförordningen och Integritetsskyddsmyndigheten utgör ytterligare en instans för insyn, tillstånd och tillsyn.

En annan fråga som behöver uppmärksammas är vilka som får tillgång till det slutliga datat. Kommissionens expertgrupp noterar att system bör utformas för att ”förhöja och stärka” individer. System bör inte ”oberättigat underordna, tvinga, vilseleda, manipulera, betinga eller leda människor. ”

När en personuppgiftsansvarig behandlar komplex data som till exempel video (även anonymiserad video) finns en osäkerhet om vad som kan komma att utläsas ur datat. Förutsägelseanalyser ("predictive analytics") på komplext, mänskligt genererat data för att förutspå individbeteenden, framtida händelser och samhällstrender är ett växande område som kan ha implikationer för framtida demokrati och individers möjligheter att inte bli manipulerade eller ledda.

Förebyggande av skada

System bör inte orsaka eller förvärra skada, eller på annat sätt påverka människor negativt. Systemet måste vara såväl tekniskt som analytiskt robust. Det måste gå att lita på att resultaten är tillförlitliga om de ska ligga till grund för beslut, och de som tar besluten måste förstå vilka begränsningar som finns i den genererade datamängden.

Om till exempel data samlas in i en viss stadsdel med vissa sociokulturella egenskaper, så måste detta faktum beaktas vid beslut baserade på denna data för en annan stadsdel som kan ha andra sociokulturella egenskaper.

Sårbara personer och grupper bör särskilt uppmärksammas och inkluderas i processen runt ändamål och metod. Detta hanteras bland annat genom tillståndsprocessen hos Integritetsskyddsmyndigheten, där villkor och begränsningar i tillstånd också beaktar dessa aspekter.

Det ska i sammanhanget också beaktas att den personuppgiftsansvariga kommunala nämnden har betydligt större kontroll och inflytande över uppgifterna samt mer information om behandlingen än vad enskilda registrerade medborgare. Som angetts i avsnitt 1.3 ska den anonymiserade datan göras öppet tillgänglig för vidare användning för såväl kommersiella som icke-kommersiella ändamål. Det gör att registrerade på likande villkor kan få tillgång till datan och själv skapa värde av uppgifterna.

Rättvisa

Den personuppgiftsansvariga ska vinnlägga sig om en jämlik och rättvis fördelning av både risker och fördelar, så de grupper och individer som löper störst risk också vinner på att databehandlingen görs. Den proportionalitetsbedömning som gjorts i referenskonsekvensbedömningen tar höjd för detta och bedömningen måste löpande ses över av den personuppgiftsansvariga.

Förklarbarhet

Förklarbarhet, både internt för beslutstagare och andra personer som hanterar datat i sin professionella roll inom kommunen, och externt för medborgarna, är avgörande för att behålla tillit och förtroende. I detta ingår transparens gentemot medborgarna, men också utbildningsinsatser som pedagogiska förklaringar, så att de som påverkas direkt och indirekt har möjlighet att utvärdera frågan själva och i förlängningen påverka. Detta hanteras genom de informationsinsatser som beskrivs i avsnitt 2.5.

Referenser

Förarbeten

Prop. 2017/18:105, Ny Dataskyddslag

Prop. 2017/18:231, Ny kamerabevakningslag

SOU 2018:4 Framtidens biobanker, Slutbetänkande av Utredningen om regleringen av biobanker

Myndighetsbeslut

Datainspektionens beslut den 16 januari 2019, dnr. DI-2018-13200

JO 2006/07 s. 54, dnr. 5010-2003

Socialstyrelsen, dnr 51-10082/2003, Tillhandahållande av vävnadsprover vid utredning av brott.

Övriga källor

Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, ENISA, November 2017

Ethics and data protection, EU-Kommissionen, 2018

Etiska riktlinjer för tillförlitlig AI, EU-Kommissionens expertgrupp på hög nivå för AI-frågor, 2019

FN:s utvecklingsprogram (UNDP), Globala målen http://www.globalamalen.se, hämtad 2021-03-03.

ISO 31000:2018(E) riktlinjer för riskhantering

MSB:s vägledning för risk- och sårbarhetsanalyser (MSB245 2011).

Privacy Impact Assessment (PIA) Knowledge bases, Commission Nationale Informatique & Libertés, Februari 2018.

Privacy Impact Assessment (PIA) Methodology, February 2018 edition, Commission Nationale Informatique & Libertés, Februari 2018

Robust och säker IoT, Vägledning för Robust och Säker IoT, ver 1.0, 2020-03-01.

Svensk standard, SS-ISO/IEC 29134:2020 Informationsteknik – Säkerhetstekniker – Riktlinjer för konsekvensbedömning avseende personlig integritet

WP 248 rev. 01, Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, antagna den 4 april 2017 av Arbetsgruppen för skydd av enskilda med avseende på behandling av personuppgifter (artikel 29-gruppen).

WP216, yttrande 05/2014 om avidentifieringsmetoder, antaget den 10 april 2014

En samlad bild över rapporterade it-incidenter i samhällsviktiga och digitala tjänster, årsrapport NIS-leverantörers it-incidenrapportering 2020, MSB1695, februari 2021.