KLASSA för IoT

NORMATIV VÄGLEDNING FÖR SYSTEMATISKT
INFORMATIONSSÄKERHETSARBETE

Sveriges
Kommuner
och Regioner

Förord

Lösningar som bygger på konceptet sakernas internet (IoT) blir allt vanligare i samhället. I den smarta staden och det smarta samhället ses IoT-system för trafikstyrning, trängselinformation och badvattentemperatur som naturliga tjänster i vardagen. I många regioner använder man också IoT-system som stöd för att leverera hälso- och sjukvård samt kollektivtrafik.

Detta innebär nya prövningar för informationssäkerhetsarbetet i organisationerna. En kraftig ökning av nya datamängder ska hanteras, ofta i kombination med information från organisationernas befintliga verksamhetssystem. Samtidigt höjs både krav och förväntningar på offentliga verksamheter att tillgängliggöra och publicera information i form av öppna och insiktsfulla data för ytterligare tjänster och innovationer. Något som aktualiserats särskilt under den pågående globala covid-19-pandemin.

I ljuset av detta har Sveriges Kommuner och Regioner i samverkan med Research Institutes of Sweden (RISE) tagit initiativ till denna vägledning *KLASSA för IoT.* Vår målsättning och den utveckling av SKR:s KLASSA-verktyg som skett parallellt, är att sänka tröskeln för att bedriva ett strukturerat informationssäkerhetsarbete.

Projektuppdraget har initierats och finansierats genom SKR:s och Trafikverkets branschprogram för stärkt samverkan kring transportplanering och samhällsutveckling i lokalt och regionalt perspektiv. Stödfinansiering har erhållits via projektet City as a Platform, ett strategiskt projekt inom ramen för det statliga innovationsprogrammet Viable Cities.

Thomas Nilsson, Certezza respektive Marika Wasserman, Governo har varit huvudförfattare. Olof Junesjö, Governo har varit projektledare och Björn Hagström, Hagström Consulting har bidragit utifrån perspektivet öppna data.
Ett stort tack riktas till medverkande kommunrepresentanter från Örebro, Stockholm, Umeå, Kalmar, Hudiksvall, Helsingborg, Linköping, Karlskrona, Västerås, Eskilstuna, Katrineholm, Malmö, Uppsala, Sundsvall, Skellefteå, Lund, Halmstad och Göteborg.

Bo Baudin, SKR, har varit initiativtagare och samordnare. Ett särskilt tack till Jeanna Thorslund, Polismyndigheten (tidigare SKR) och Claus Popp Larsen, RISE för det gemensamma förankringsarbetet.

Stockholm i november 2020

Gunilla Glasare
Avdelningschef
Avdelningen för tillväxt och samhällsbyggnad
Sveriges Kommuner och Regioner

Peter Haglund
Sektionschef

Lotta Nordström
CIO, Sektionschef
Avdelningen för ledningsstöd
Sveriges Kommuner och Regioner

Innehåll

Inledning 5
Målgrupp 5
Kort om vägledningen 5
Hur vägledningen tagits fram 6
Kort om KLASSA 6
Begrepp och termer 7
Kort om informationsklassning 9
Modell och metodik 9
Informationsägare 9
Verksamhetsperspektivet 9
Informationsklassning av IoT 11
Identifiera informationstillgångar 11
Tidpunkt för informationsklassning av IoT 11
Klassificera informationstillgångarna 12
Tillämplig lagstiftning 12
Aspekter att särskilt beakta vid klassning av IoT 14
Vägledning – specifika IoT-system 17
Smarta sensorer för trafikstyrning i stadsmiljö 17
Smart och uppkopplad gatubelysning 18
Mäta rörelsemönster i en stadsmiljö 20
Kartläggning av rörelsemönster i torgmiljö 21
Mäta badvattentemperatur 22
Central IoT-plattform 23
Vägen framåt 25
Bilaga 1. Avidentifiering 27
Sammanfattning av yttrandet 27
Risker med avidentifiering 28
Randomisering och generalisering 29
Vägen fram avseende avidentifiering 31
Bilaga 2. Kamerabevakning 32
Kamerabevakningslagen 32
EU:s dataskyddsförordning 32

Inledning

Målet är att belysa relevanta aspekter vid klassning av IoT-system och att ta fram normerande klassningar för ett antal vanliga användarfall. Detta för att göra det enklare för personer som arbetar ute i regioner och kommuner att själva ta sig an området.

För att ytterligare stödja kommuner och regioner i deras informationssäkerhetsarbete har SKR parallellt med framtagandet av denna vägledning initierat ett arbete med att ta fram en ny version av SKR:s KLASSA (KLASSA version 4). I den nya version som ser dagens ljus under våren 2021 sker en förflyttning från ett systemcentriskt fokus till ett mer informationscentriskt fokus. Ett informationscentriskt perspektiv är centralt när IoT ska informationsklassificeras.

Målgrupp

Du som läser detta material kan vara i färd med att genomföra eller planera för en informationsklassning i ett IoT-projekt. Materialet riktar sig inte enbart till de som har stor erfarenhet av denna typ av arbete utan ska också vara användbart för de som inte har arbetat så mycket med informationsklassningar tidigare.

Vår målsättning är att du med stöd av detta material ska få vägledning i de informationssäkerhetsrelaterade avvägningar som du står inför.

Vi har också exemplifierat med ett antal IoT-system som bygger på en handfull faktiska användarfall i IoT-Sverige. Notera dock att de rekommendationer som ges i detta dokument ska ses som vägledande och att du alltid måste göra dina egna avvägningar vid en informationsklassning.

Kort om vägledningen

Denna vägledning är tänkt att användas som ett stöd vid informationsklassificering av IoT-system tillsammans med övrigt stödmaterial som är framtaget av SKR. Utformningen präglas av standarderna SS-ISO/IEC 27001 och 27002 mot bakgrund av att Myndigheten för samhällsskydd och beredskap (MSB) finansierar tillgången till dessa standarder för Sveriges 290 kommuner och 21 regioner.

Under läsningen är det bra att veta att vi i huvudsak kommer att fokusera på IoT-system som informationstillgångar i enlighet med såväl standardens definition av informationstillgångar som MSB:s metodsystem[1]. Fokus ligger därmed på vilken information som behandlas i IoT-lösningen och i vilka sammanhang denna information används i olika tjänster och tillämpningar.

[1] https://www.informationssakerhet.se/

Vägledningen KLASSA för IoT är inte ett verktyg för informationsklassning utan syftar till att vägleda i informationsklassning av IoT-system oavsett om du använder dig av SKR:s eget verktyg KLASSA eller något annat motsvarande verktyg.

KLASSA för IoT kommer att kompletteras över tid i syfte att stödja SKR:s medlemmar i det systematiska informationssäkerhetsarbetet. Vissa delar kommer också att ligga till grund för ytterligare vägledningsmaterial direkt kopplat till KLASSA-verktyget.

Hur vägledningen tagits fram

För att ta fram denna vägledning har vi utgått från konkreta användarfall och sedan gjort en analys där vi lyfter fram både de aspekter som identifierats i respektive användarfall och generella aspekter som behöver beaktas vid informationsklassning av IoT-system. De kommuner som bidragit i framtagandet av materialet är bland annat Stockholms stad och Örebro kommun samt kommunerna i projektet City as a Platform (CaaP)[2].

Initialt har KLASSA för IoT huvudsakligen finansierats genom Trafikverkets och SKR:s gemensamma branschprogram för stärkt samverkan kring transportplanering och samhällsutveckling i lokalt och regionalt perspektiv via projektet Datadriven innovation för smarta samhällen samt genom det statliga innovationsprogrammet Viable Cities via det strategiska projektet City as a Platform. I arbetet framåt bidrar även det statliga innovationsprogrammet IoT Sverige samt SKR:s FoU-fond för kommunernas fastighetsfrågor.

Kort om KLASSA

För att stödja kommuner och regioner i arbetet med att klassificera informationstillgångar har SKR tillsammans med sina medlemmar tagit fram verktyget KLASSA[3]. Syftet är att klassa informationstillgångar på ett likartat sätt och att på så sätt förenkla informationsklassningen.

Vidare är syftet med KLASSA att föreslå åtgärder som organisationen kan och bör vidta för att skydda informationen, vilket också leder till att Sveriges kommuner och regioner skyddar information på ett likartat sätt.

Dessa skyddsåtgärder kan vara såväl tekniska som organisatoriska[4]. Kraven är formulerade dels som ÄR-krav vilka är riktade till den egna organisationen, dels som SKA-krav vilka är riktade till leverantörer, exempelvis i samband med upphandling och uppföljning.

---

[2] https://cityasaplatform.se/om-projektet/
[3] https://klassa-info.skl.se/
[4] Skyddsåtgärderna är formulerade med de normativa kraven i SS-ISO/IEC 27001 Bilaga A som utgångspunkt och kompletterande regulatoriska informationssäkerhetskrav från t.ex. EU:s dataskyddsförordning, lagen om informationssäkerhet för samhällsviktiga och digitala tjänster samt offentlighets- och sekretesslagen.
.

KLASSA har primärt varit ett verktyg för att hantera informationstillgångar i IT-system och har alltså hittills haft ett systemfokus. En förändring sker i KLASSA version 4 (KLASSAv4) som släpps under våren 2021. I denna version kommer systemfokuseringen tonas ner till förmån för ett starkare fokus på information oavsett bärare av denna. De insikter som erhållits i detta projekt har bidragit med förslag till utformningen av KLASSAv4. När KLASSAv4 släpps kommer även vägledningen KLASSA för IoT att uppdateras och inkluderas som stödmaterial i KLASSA.

Skrivningarna i den här vägledningen kan tillämpas oavsett om organisationen använder KLASSA eller något annat verktyg som stödjer det systematiska informationssäkerhetsarbetet.

Begrepp och termer

För att förenkla läsningen listar vi här den terminologi som vi utgår från. Detta är ett forskningsfält som ständigt utvecklas. Vi har huvudsakligen valt att utgå från ISO/IEC 20924 - Information technology – Internet of Things (IoT) – Vocabulary. Vi har dock översatt definitionerna till svenska.

Aktuator (actuator): IoT-enhet som ändrar en eller flera egenskaper hos en fysisk enhet på basis av en giltig datainmatning.

Aggregering (aggregation): sammanställning av information från databaser i syfte att förbereda för exempelvis databearbetning av kombinerade dataset.

Anonymisering (anonymization): Säkerställa att en specifik informationsmängd inte längre kan kopplas till en individ.

Applikation (application): mjukvara designad för att uppnå ett specifikt syfte.

Bearbetning (processing): förädling av data. Kan exempelvis utgöras av kategorisering eller automatiserad analys.

IoT: infrastruktur av sammankopplade enheter, människor, system och informationstillgångar tillsammans med tjänster som bearbetar och reagerar på information från den fysiska och virtuella världen.

IoT-enhet (device): enhet inom ett IoT-system som interagerar och kommunicerar med den fysiska världen genom avläsning (sensing) eller igångsättande (actuating).

IoT-gateway: enhet inom ett IoT-system som sammankopplar ett eller flera närliggande nätverk och de IoT-enheter som ingår i dessa nätverk med varandra och till ett eller flera accessnät.

IoT-system: system som tillhandahåller IoT-funktionalitet – kan innefatta IoT-enheter, IoT-gateways, sensorer och aktuatorer.

Sensor: IoT-enhet som mäter en eller flera egenskaper hos en eller flera fysiska enheter och genererar digitala data som kan överföras via ett nätverk.

Därutöver används terminologi för informationssäkerhet i SS-ISO/IEC 27000 och SIS-TR 50.

Kort om informationsklassning

Modell och metodik

SS-ISO/IEC 27001 och 27002 beskriver en modell och metodik för informationsklassning. Dessa standarder har legat till grund för KLASSA och MSB:s metodstöd och har också varit vägledande för utformningen. SKR har utformat modellen så att dess medlemmar kan klassa informationstillgångar på ett likartat sätt och i syfte att skapa en gemensam förståelse för krav på skydd och för tillämpningen av lämpliga skydd.

De konsekvensnivåer som används i KLASSA följer den modell[5] för klassificering av information som utarbetats av MSB och Svenska Institutet för Standarder (SIS):

- Synnerligen allvarlig skada (4)
- Allvarlig skada (3)
- Betydande skada (2)
- Måttlig skada (1)
- Försumbar skada (0)

För närmare förklaring av konsekvensnivåernas betydelse, se KLASSA:s stödmaterial[6]. Där finns också översättningar till fler modeller som beskriver konsekvensnivåer.

I denna vägledning har vi utgått från de konsekvensnivåer som finns i KLASSA.

Under avsnittet Informationsklassning av IoT-system nedan finns grundläggande vägledning kopplat till de vanligt förekommande regulatoriska kraven.

Informationsägare

En ägare ska utses för varje informationstillgång. Ägaren är bland annat ansvarig för att tillgången klassas och skyddas i relation till dess skyddsvärde, exempel på andra ansvar är åtkomststyrning. Viktigt att poängtera är att en ägare inte behöver ha formell äganderätt till informationstillgången. Om informationsägaransvaret inte har delegerats innehas det av organisationens högsta ledning.

Verksamhetsperspektivet

Ur ett verksamhetsperspektiv är syftet med informationsklassningen att värdera informationstillgångar med utgångspunkt från deras känslighet och betydelse för organisationen när det gäller konfidentialitet, riktighet och tillgänglighet.

[5] https://www.msb.se/RibData/Filer/pdf/25602.pdf
[6] https://KLASSA-info.skl.se/stodmaterial/page/vagledning

Klassningen ska göras regelbundet, minst årligen, och vid ändringar av informationstillgångens värde, känslighet och betydelse. Informationsägaren är ansvarig för att detta sker.

Ur ett användarperspektiv ska klassningen ge dem som arbetar med informationen en tydlig indikation på hur den bör hanteras och skyddas. Det behöver beaktas i behandling av informationen. Standarden ger inte någon ytterligare vägledning och här har vägledningsmaterialet till KLASSA en viktig roll att fylla. Inte minst för att modellen för informationsklassning ska tolkas på ett likartat sätt av SKR:s medlemmar och att likartade informationstillgångar klassas på ett likartat sätt och därigenom kan dra fördel av de krav på skyddsåtgärder som KLASSA föreslår. På så sätt kan man undvika situationer där man antingen klassar informationen för högt, vilket kan leda till att onödigt kostsamma säkerhetsåtgärder vidtas, eller att man klassar informationen för lågt, vilket istället kan innebära risker för verksamhetens förmåga att nå sina mål. Ett exempel på detta skulle kunna vara att informationen inte är tillgänglig i den utsträckning som behövs, genom att aspekten tillgänglighet värderats för lågt och åtgärder för hög tillgänglighet därför inte implementerats.

Informationsklassning av IoT

Identifiera informationstillgångar

SS-ISO/IEC 27001 och 27002 uttrycker tydligt att första steget är att tillgångar associerade med information ska identifieras. I komplexa scenarier är det viktigt att beskriva vilken information som identifierats för att kunna göra rätt analyser, såväl rättsligt som verksamhetsmässigt.

Vid aggregering av data och information är det viktigt att göra samlade bedömningar. Det finns inte någon algoritm för att väga samman data och information utan klassificeringen ska göras med den samlade informationsmängden i IoT-lösningen som grund. Detta arbetssätt gör också att de komponenter som är vitala för lösningen kommer att ärva den samlade bilden, exempelvis kritiska sensorers krav på riktighet. I själva lösningen kommer också informationens innehåll och därmed även skyddsvärde att förändras, exempelvis om den anonymiseras.

Se bilaga 1 för ett utförligare resonemang om avidentifieringsmetoder.

Tidpunkt för informationsklassning av IoT

Tidpunkten för informationsklassning av IoT-system är densamma som vid andra typer av tillämpningar, vilket innebär att klassning bör genomföras:

- inför en upphandling av IoT-system för att få underlag till kravställning,
- inför en produktionssättning av IoT-system för att säkerställa att nödvändiga krav är uppfyllda, och
- med regelbundenhet och då särskilt vid förändringar av IoT-system som är i drift, som en del av förvaltningsarbetet.

Klassificera informationstillgångarna

Informationsklassning inom IoT-området ska ske på motsvarande sätt som vid klassning av andra typer av informationstillgångar. Det innebär också att samma kontrollfrågor kan användas under en klassning. Exempelvis:

- Hur skyddsvärd är informationen (mätdata, statistik, mätvärden, loggar, m.m.)?
- Hur viktigt är det att informationen är korrekt och inte förvanskas avsiktligt eller oavsiktligt?
- Hur viktigt är det att informationen är tillgänglig när den behövs?

För att kunna bedöma vilka negativa effekter som skulle kunna uppstå om tillgången till informationen utsätts för ett avbrott behöver vi förstå vad den används till. Kravbilden förändras också över tid varför det för IoT-system ofta kan vara aktuellt att göra en mer frekvent klassning än för andra mer statiska tillämpningar.

Vissa IoT-lösningar kan ha höga krav på riktighet och tillgänglighet medan kravet på konfidentialitet kan vara lågt vilket medför att man kan dela informationen utan några större risker eller hinder. Ibland är det till och med önskvärt att information från det offentliga delas för att ta vara på det socioekonomiska värdet av informationen.[7] EU:s öppna datadirektiv anger också att information från den offentliga sektorn eller information som samlas in, framställs, reproduceras och sprids inom ramen för en offentlig verksamhet eller en tjänst av allmänt intresse, utgör ett betydelsefullt utgångsmaterial för produkter och tjänster med digitalt innehåll. Den kommer dessutom att bli en ännu viktigare innehållsresurs genom utvecklingen av avancerad digital teknik såsom artificiell intelligens, distribuerad databasteknik och sakernas internet.[8]

Tillämplig lagstiftning

Samtliga regler som tillämpas utifrån ett traditionellt informationsklassningsperspektiv måste beaktas i IoT-sammanhang, exempelvis:

- säkerhetsskyddslagen (2018:585),
- lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174),
- EU:s dataskyddsförordning,[9]
- lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (2018:218),

[7] Innovation genom information, SOU 2020 s. 21.
[8] Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.
[9] 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)

- kamerabevakningslag (2018:1200),
- offentlighets- och sekretesslag (2009:400), och
- upphovsrättslagen (1960:729)

Från ett IoT-perspektiv är kamerabevakningslagen (2018:1200), särskilt viktig att beakta om kameror eller multisensorer med kameraförmågor används i IoT-systemet.

Se bilaga 2 för ett utförligare resonemang kring kamerabevakningslagen.

I vägledningsmaterialet i KLASSA finns det några tydliga kopplingar till ovan nämnda regelverk. Lagstiftningen har också legat till grund för hur krav-katalogerna i KLASSA utformats. Exempelvis det faktum att Datainspektionen uttrycker genom tillsyn att om känsliga personuppgifter (särskilda kategorier) tillgängliggörs över öppna nät som internet och Sjunet ska åtkomst föregås av stark autentisering.

Avseende informationstillgångar som berörs av säkerhetsskyddslag (2018:585) rekommenderas konsekvensnivå **synnerligen allvarlig (4)** för samtliga säkerhetsaspekter och då är nästa steg att göra en säkerhetsskyddsanalys, förslagsvis enligt Säkerhetspolisens (SÄPO) metodik. Det ska framhållas att KLASSA idag inte har några kravkataloger som möter upp krav som följer av säkerhetsskyddslagen utan här rekommenderas Militära underrättelse- och säkerhetstjänstens (MUST) krav på säkerhetsfunktioner (KSF[10]) och den metodik som denna är förenad med. Säkerhetspolisens vägledning[11] i säkerhetsskydd med fokus på informationssäkerhet ger också rekommendationer inom området.

Avseende informationstillgångar som berörs av lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS) rekommenderas konsekvensnivå **allvarlig (3)** för samtliga säkerhetsaspekter.

Avseende informationstillgångar som berörs av EU:s dataskyddsförordning rekommenderas konsekvensnivå **betydande (2)** för samtliga säkerhetsaspekter. I sammanhang där särskilda kategorier (känsliga personuppgifter) behandlas är konsekvensnivån **allvarlig (3)** för säkerhetsaspekten konfidentialitet och i vissa fall även för riktighet.

Avseende informationstillgångar som berörs av offentlighets- och sekretesslagen (2009:400) (OSL) går det inte att göra lika självklara bedömningar av konsekvensnivån som med övriga regulatoriska krav som omnämns här. I vägledningsmaterialet för KLASSA finns en lite längre utvikning som förklarar OSL och skillnaderna mellan sekretess och klassificeringen. Vägledande är att sekretessreglerad information enligt OSL sannolikt leder till konsekvensnivån **betydande (2)** eller **allvarlig (3)** för säkerhetsaspekten konfidentialitet.

[10] http://isd.fmv.se/history/Sidor/FM-MUST-KSF.aspx

[11] https://www.sakerhetspolisen.se/download/18.f2735ce171767402ba3dc/1599633194948/Vagledning-Informationssakerhet_2020.pdf

Aspekter att särskilt beakta vid klassning av IoT

Vid informationsklassning av IoT har vi identifierat ett antal aspekter som särskilt bör beaktas vid informationsklassning. I vägledningen beskrivs ett antal av dessa aspekter tillsammans med ett resonemang kring informationsklassning i relation till dem. Värt att notera är också att IoT som område är relativt närliggande andra områden så vissa av de aspekter som belyses nedan är också aktuella inom andra mer generella områden. Vår bedömning är dock att de är särskilt aktuella inom just IoT-området.

Var informationen behandlas

Till skillnad från verksamhetssystem där all information tenderar att samlas i en databas är IoT-lösningar ofta både geografiskt och systemmässigt utspridda. IoT-lösningar innehåller ofta olika typer av sensorer som kan sättas upp såväl inomhus som i utomhusmiljöer. Viss bearbetning av informationen kan ofta ske direkt i den produkt där sensorn är installerad. Det är inte heller ovanligt att leverantören tillhandahåller någon typ av verksamhetssystem som samlar upp och behandlar data från flera sensorer. I ett tredje led kan information också lagras och bearbetas i en central IoT-plattform.

Utifrån ett informationssäkerhetsperspektiv är det relevant att beakta sitt behov av informationen. Om sensorn är en kamera blir informationen i form av rörliga bilder känslig utifrån ett sekretess- och ett personuppgiftsperspektiv. Ofta är det dock inte själva videoströmmen organisationen är intresserad av, utan snarare den anonymiserade och tolkade informationen. Det kan då vara relevant att säkerställa att den information som förs vidare till andra delar av IoT-lösningen enbart är anonymiserad data och inte exempelvis hela videoströmmen. Detta får effekten att kraven på säkerhet kan sänkas för dessa delar av lösningen och att kostnaden för lösningen därmed blir lägre.

Exempel: En kommun har en sensor som genererar en videoström ute i en gatukorsning. Men den enda data som skickas vidare till andra delar av lösningen (t.ex. en central plattform) är ”typ av trafikant, passagetidpunkt, hastighet”. Det är således enbart den anonymiserade informationen som skickas vidare, inte själva videoupptagningen (rådatan som t.ex. kan avslöja biometrisk information som skulle kunna användas för att identifiera en individ, även om det i sig inte är syftet med videoupptagningen).

Detta gör att informationstillgången som anonymiserats kan informationsklassas på ett annat sätt, eftersom åtgärden medför att graden av konfidentialitet sjunker.

Detaljnivå och aktualitet

Två andra aspekter som är särskilt relevanta att reflektera över vid klassning av informationstillgångar i IoT-lösningar är informationens detaljnivå och aktualitet, och vad detta innebär för val av skyddsnivåer.

I vissa IoT-system bearbetas och aggregeras den information som samlas in via sensorer eller genom att fånga upp mobila enheters placering och rörelser direkt vid källan. Detta skulle exempelvis kunna innebära att notera antal personer som befinner sig på en specifik plats vid en specifik tidpunkt snarare än att lagra informationen kopplat till de enskilda individerna. Då handlar det inte längre om personuppgifter och därmed sjunker skyddsvärdet ur ett konfidentialitets-perspektiv.

Även informationens aktualitet spelar in när det gäller skyddsvärdet. Exempelvis kan en historisk datapunkt ha lägre skyddsvärde än en aktuell uppgift om hur något förhåller sig precis här och nu. Ett exempel på detta är att informationen om att en ensam individ rör sig på en viss plats just i detta nu har högre skyddsvärde än historiska data om rörelsemönster.

Modularitet

I allt högre utsträckning strävar kommuner och regioner efter att bygga system som är modulära. Det innebär att man istället för att upphandla ett helhets-system som täcker alla delar av en huvudprocess, upphandlar ett antal olika moduler som kan samverka med varandra genom standardiserade gränssnitt.

Den tänkta nyttan med ett sådant tillvägagångssätt är att kommunen minskar sitt leverantörsberoende. Om en delprocess eller en del av systemet upplevs som omodern eller icke ändamålsenlig kan denna modul bytas ut utan att organisationen behöver byta ut hela lösningen. Effekten blir också att olika specialiserade produkter kan interagera med varandra på ett så sömlöst sätt som möjligt.

Detta förhållningssätt gäller särskilt utifrån ett IoT-perspektiv där olika fysiska produkter ska interagera med varandra och med centrala system. Här kan det i högsta grad vara aktuellt att byta ut, lägga till eller dra ifrån delar av den sammanhängande helheten löpande under en längre tidsperiod. Att lägga till nya punkter för att samla in data längst ut i dessa system kommer i många fall vara vanligt och då tekniken utvecklas kommer nya sensorer användas regelbundet.

Utifrån ett informationsklassningsperspektiv leder detta till att en ny informationsklassning kan behöva genomföras varje gång en förändring i systemmiljön sker. Om en applikation eller ny information tillförs kan det påverka konfidentialitet, riktighet och tillgänglighet för helheten såväl som för delar av lösningen. När nya funktioner tillförs kan det också leda till att informationen kan användas på nya sätt, vilket i sig innebär att en ny informationsklassning måste genomföras.

Informationsägarskap i IoT-lösningar

IoT-lösningar har ofta som tidigare nämnts ett antal olika beståndsdelar. Det kan vara en sensor i utomhusmiljö. Denna kan i sin tur kopplas till verksamhets-lösningar som exempelvis aggregerar och anonymiserar data. I ett tredje led finns ofta centrala IoT-plattformar där datamängder kombineras och bearbetas

vidare. I det fallet kan det vara extra intressant att resonera kring informationsägarskapet för den information som behandlas.

Här lämpar sig modellen där man tittar på ett specifikt system inte heller speciellt väl. Informationen kan också flöda över förvaltningsgränser där en specifik sensor ägs av en förvaltning, en verksamhetslösning som nyttjar informationen från sensorn ägs av en annan förvaltning och en central IoT-plattform ägs av en tredje organisatorisk enhet. Det kan också vara så att den ursprungliga informationen som samlas in av en specifik sensor förädlas och berikas med information från olika källor löpande i processen. Vem är det då som är informationsägare i de olika delarna av processen? Denna fråga har inget givet svar utan kräver en levande dialog inom organisationen. Däremot behöver ägarskapet alltid tilldelas för att skapa ett tydligt ansvarsförhållande i relation till informationen.

Informationsklassning i PoC:ar och piloter

I och med att det är vanligt att IoT-lösningar provas i mindre skala innan de rullas ut på bred front i en organisation i så kallade proof of concepts (PoC) och pilotprojekt, påverkas också informationsklassningsarbetet. Ett vägval kan vara om organisationen ska ta hänsyn till en fullt uppskalad implementation direkt vid informationsklassningen, eller om den ska börja med exempelvis ett resonemang om att en pilot i liten skala inte innebär så stora risker, och därmed sätta en lägre nivå på de olika säkerhetsperspektiven.

Framförallt gäller detta perspektiv tillgänglighet och i viss mån även kraven på riktighet, i och med att påverkan i en pilot i liten skala inte blir så märkbar på verksamheten. Skyddsvärdet avseende konfidentialitet bör dock inte påverkas av implementationens omfattning.

Om man väljer en lägre säkerhetsnivå för ett eller flera av perspektiven utifrån att det ”bara” rör sig om en pilot, finns det risk för att man inte utforskar alla utmaningar som behöver hanteras för att piloten ska kunna skalas upp. Detta kan i sin tur leda till att en bredare implementering inte blir av, i och med att viktiga knäckfrågor inte adresserats.

Om man å andra sidan tar höjd för ett fullskaligt införande kan lösningen bli onödigt kostsam i ett för tidigt skede. En rekommendation är här att ta höjd för att bygga ut både funktioner och säkerhetsåtgärder successivt samt att påverkan från regulatoriska krav alltid måste beaktas oavsett vägen framåt.

Vägledning – specifika IoT-system

För att underlätta informationsklassning i IoT-projekt har projektet KLASSA för IoT studerat ett antal projekt och tagit fram vägledningar som grund för resonemang för organisationer i motsvarande situation. Varje fall inleds med en kort beskrivning av området varpå de tre perspektiven; konfidentialitet, riktighet och tillgänglighet beskrivs i tur och ordning. Värt att poängtera är dock att IoT-system kan skilja sig åt och att en informationsklassning alltid behöver ske. Vi har också beskrivit appliceringen av en IoT-plattform. Detta fall har en annorlunda karaktär då plattformen i sig inte har en skyddsnivå utan den är i sin tur beroende av vilka informationsmängder man nyttjar plattformen till.

Smarta sensorer för trafikstyrning i stadsmiljö

Det är inte ovanligt att IoT används för styrning av trafik i en mängd olika typer av tillämpningar, allt från enklare lösningar för att t.ex. identifiera trasig utrustning till avancerade lösningar med artificiell intelligens som baserat på olika förutsättningar fattar automatiska beslut för att genomströmningen av bilar på en specifik gata ska fungera på bästa möjliga sätt.

Det IoT-system som beskrivs här används för att styra trafiken i en trafikkorsning, och omfattar ett antal så kallade multisensorer. Detta innebär att sensorer med kamerafunktion används för att samla rörliga bilder som analyseras för att bedöma trafikintensitet och trafikslag som bilar, bussar, cyklar och gångtrafikanter. Den information som samlas in och bearbetas omfattar därmed delvis personuppgifter, i och med att individer kan identifieras. Kriterierna för särskilda (så kallade känsliga) personuppgifter uppfylls dessutom, eftersom biometrisk information om individer registreras, även om detta i sig inte är syftet med att använda kameran/multisensorn.

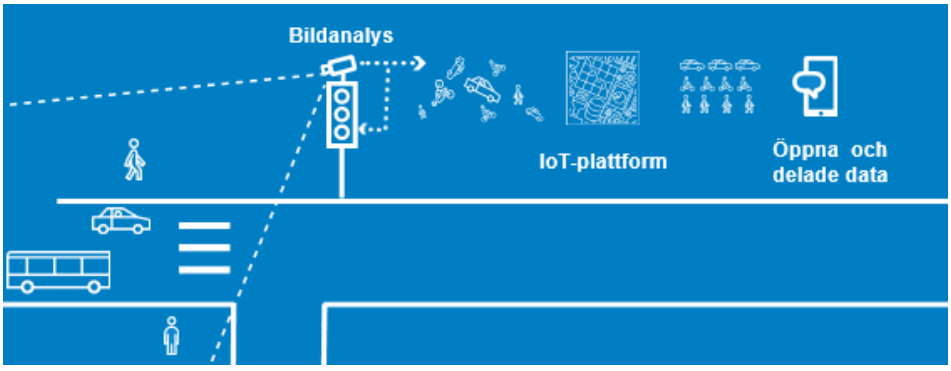

Bild 1. Visualisering av smart trafikstyrning. Källa: Smart stad-programmet i Stockholms stad

Vägledning avseende klassningsnivå – konfidentialitet

I den del av IoT-lösningen där bildbehandlingen sker, alltså i multisensorn, är konsekvensnivån för konfidentialitet **allvarlig (3)** i och med att känsliga personuppgifter behandlas mot bakgrund av insamlingens omfattning. Därefter sker en anonymisering av rådata till den bearbetade form som används i själva tillämpningen. Den bearbetade informationen beskriver enbart antal bilar, cyklister etc. vid en viss tidpunkt eller tidsintervall. Det innebär att konsekvensnivån för konfidentialitet för lösningens övriga informationstillgångar bedöms vara **måttlig (1)** för aktuella uppgifter och **försumbar (0)** för historiska uppgifter.

Det betyder också att denna bearbetade information kan delas, såväl inom organisationen som samlar in den som med externa parter i form av öppna data för att exempelvis användas i andra tillämpningar som kan vara till nytta för till exempel medborgare och besökare.

Vägledning avseende klassningsnivå – riktighet

När det gäller aspekten riktighet är det av högsta vikt att informationen som trafikgenomströmningen på en viss gata ska baseras på är riktig, dvs. inte förvanskad, eftersom felaktig information skulle kunna bidra till trafikproblem och i värsta fall även till trafikolyckor. Konsekvensnivån för riktighet ska i sådant fall bedömas som minst **betydande (2)**.

Vägledning avseende klassningsnivå – tillgänglighet

Även vad gäller tillgänglighet bedöms konsekvensnivån som **betydande (2)**, eftersom tillgången till aktuell information är avgörande för att styrningen av trafiksignalerna ska kunna utföras på ett sätt som gör att trafiken flödar utan onödiga avbrott. Den information som hanteras i systemet kan även komma att publiceras för att användas av externa aktörer, vilket också medför en risk att bristande tillgänglighet kan leda till betydande skada avseende verksamhet, ekonomi eller enskilda personer, vilket stärker valet av nivån.

Smart och uppkopplad gatubelysning

Ett annat vanligt IoT-system är smart och uppkopplad gatubelysning. En sådan belysningsanläggning kan styras på ett intelligent och resurseffektivt sätt för att ge en mer behovsanpassad belysning med rätt ljusnivå vid rätt tillfälle. I områden med färre passager kan nattsänkning och närvarostyrning sänka energiförbrukningen ytterligare utan att påverka den upplevda tryggheten negativt, och även bidra positivt till minskad ljusförorening.

Anläggningens utrustning kan också själv upptäcka och rapportera in fel för effektiv felavhjälpning, istället för att den aktör som ansvarar för driften behöver förlita sig på att allmänheten ska rapportera in upptäckta fel. Genom att anläggningen också kan rapportera in driftsinformation som ljuskällors brinntider, armaturers energiförbrukning etc. finns underlag tillgängligt för att kunna optimera drift- och förvaltningsåtgärder.

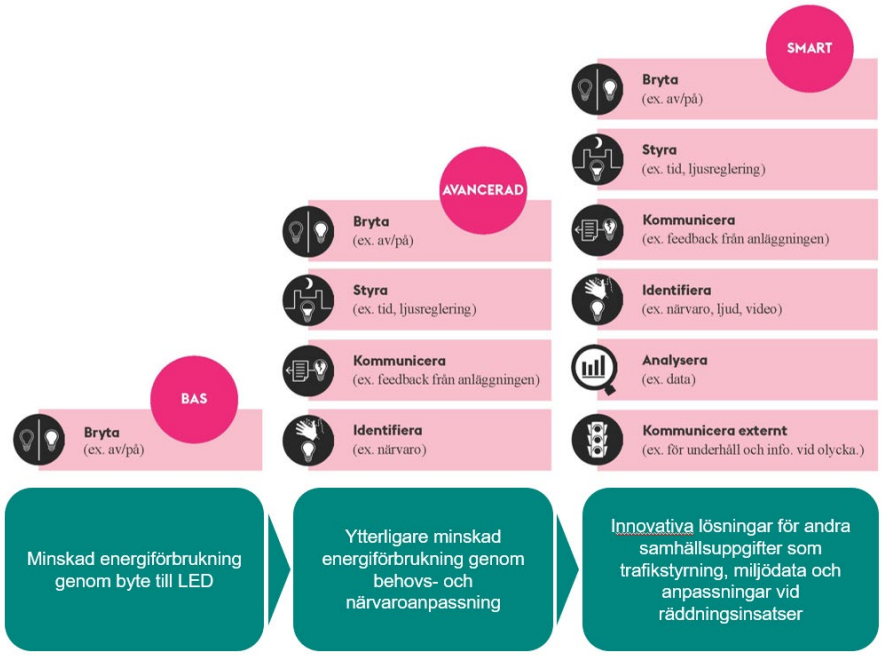

Bild 2. Visualisering av smart belysning. Källa: Smart stad-programmet i Stockholms stad

Vägledning avseende klassningsnivå – konfidentialitet

Merparten av den information som behandlas i denna typ av anläggning kan med fördel delas med andra än de som ansvarar för drift och underhåll, både inom organisationen och med externa parter, vilket gör att den ur ett konfidentialitetsperspektiv klassas på nivå **måttlig (1)** för aktuella uppgifter och **försumbar (0)** för historiska uppgifter. Detta gäller information som handlar om själva enheterna, armaturer och sensorer, driftsinformation etc. Genom att sätta konfidentialitetsnivån separat för olika delar av informationen kan man både säkerställa en korrekt hantering, organisatoriskt och tekniskt, för den del som behöver en högre nivå av skydd ur ett konfidentialitetsperspektiv och tillgängliggöra andra delar av informationen för en vidare krets utanför den egna organisationen. Detta i form av öppna data för att nyttiggöra den i fler sammanhang, som till exempel information om ljuskällor och energiförbrukning.

Vägledning avseende klassningsnivå – riktighet

Den information som används för att styra belysningen behöver vara korrekt, framförallt för att inte riskera att hela eller delar av anläggningen är släckt när den skulle ha varit tänd. Den skada som då skulle kunna uppstå kan bedömas vara på nivå **betydande (2)**.

När det gäller den information som används för att avhjälpa fel, och för att i övrigt optimera drift- och underhållsarbetet, är det huvudsakligen insatser av den typ som skulle innebära att skadeverkningen kan bedömas som något lägre

och därmed landa på nivå **måttlig (1)**. När det gäller användaruppgifter kan riskbedömningen avseende negativ påverkan vid fel medföra att nivå betydande (2) kan vara aktuell, i och med att exempelvis larm skulle kunna gå till fel mottagare och därmed riskera att inte bli åtgärdade.

Vägledning avseende klassningsnivå – tillgänglighet

För att inte riskera att ett avbrott avseende tillgänglighet till informationen i belysningsanläggningen även medför ett avbrott i funktioner, som t.ex. att ljuskällorna släcks, är lösningen utformad så att styrparametrar även lagras lokalt i enheterna. Detta innebär t.ex. att armaturernas styrenheter själva kan hålla information om det senast kända schemat. På så sätt minskar risken för att ett tillgänglighetsavbrott medför allvarliga störningar. Men i och med att den ”smarta och uppkopplade” funktionaliteten då försvinner, som exempelvis förmågan att kunna få automatiska felrapporter från anläggningen, är tillgängligheten ändå en viktig aspekt för att upprätthålla anläggningens förmåga. Detta innebär att nivå **måttlig (1)** eller möjligen även nivå **betydande (2)** kan vara aktuell.

Mäta rörelsemönster i en stadsmiljö

En allt vanligare IoT-applicering är att placera ut sensorer i stadsmiljö som fångar information från enskilda individers mobiltelefoner i syfte att bättre förstå hur människor rör sig i stadsmiljön. Konkret kan det innebära att sensorerna ”sniffar” sig till Media access control-adresser (MAC-adresser) från de enheter som har sitt WiFi aktiverat. En MAC-adress är en unik identifierare för ett nätverkskort. Dessa är normalt knutna till respektive nätverkskort och dess tillverkare. På senare tid har leverantörer dock börjat implementera dynamiska MAC-adresser utifrån integritetsskäl. Dessa är då unika identifikatorer under en begränsad tid för att sedan förändras.

Kommersiellt kan detta bland annat vara relevant för näringslivet i staden som kan se effekter av reklamkampanjer på genomströmning av människor. Men det kan också vara av intresse utifrån ett stadsplaneringsperspektiv. Med en bättre förståelse för hur människor faktiskt tar sig från punkt A till punkt B kan anpassningar ske i stadsmiljön – hinder kan elimineras och flödet förbättras.

Vägledning avseende klassningsnivå – konfidentialitet

I det här fallet specifikt, kan vi se en MAC-adress som en personuppgift. En kunnig person skulle kunna utnyttja sensorerna för att övervaka enskilda individer. I sammanhanget finns det två tillsynsärenden från Datainspektionen som bör beaktas (dnr 2729-2014[12] och 1702-2015[13]). Visserligen genomförda

[12] https://www.datainspektionen.se/globalassets/dokument/beslut/2015-06-23-vasteras.pdf
[13] https://www.datainspektionen.se/globalassets/dokument/beslut/2015-11-02-vasteras-citysamverkan.pdf

innan EU:S dataskyddsförordning trädde i kraft men som vägledningsmaterial fungerar de fortfarande.

När MAC-adressen inte är anonymiserad bör klassningen landa på minst **betydande (2)** eller till och med **allvarlig (3)** med tanke på insamlingens omfattning. Dock har många av dessa lösningar funktionalitet som anonymiserar och aggregerar data innan de förs vidare. Det medför att konsekvensnivån för konfidentialitet sänks när informationen väl har förts vidare till databasen. Syftet med informationen i dess anonyma och aggregerade version är till och med att den ska spridas. Alltså kan klassningen med fördel landa på **försumbar (0)**.

Vägledning avseende klassningsnivå – riktighet

Med tanke på att datainsamlingen från början är ungefärlig i den applicering vi analyserar nu sjunker klassningsnivån med avseende på riktighet. Det kommunen i det här fallet är ute efter är mönster och tendenser. Då är det inte nödvändigt att informationen är riktig ner på decimalnivå. Däremot är kommunen beroende av att informationen är huvudsakligen korrekt. Om beslut ska baseras på den tillgängliga informationen måste de kunna lita på den. En rimlig klassning av riktighet skulle alltså kunna vara **måttlig (1)** i det här fallet.

Vägledning avseende klassningsnivå – tillgänglighet

Den applicering vi analyserar för närvarande ska utgöra ett beslutsunderlag till de målgrupper som vill använda den. Det sker alltså ingen större verksamhetspåverkan om ett driftsavbrott skulle ske. Bedömningen är en klassning gällande tillgänglighet på nivån **måttlig (1)**.

Kartläggning av rörelsemönster i torgmiljö

I detta scenario var syftet att kartlägga ett rörelsemönster över ett större torg för att använda insamlade data för planering av trafikströmmar över torget. Samma tekniska införande kan också användas för flera olika tillämpningsområden, exempelvis kartläggning av abnorma beteendemönster såsom folksamlingar, trängsel och slagsmål.

Rådata som produceras av multisensorn kan innehålla personuppgifter. Anonymisering sker direkt i multisensorn eller i separat enhet i direkt anslutning till sensorn. Data som används i nästa led, tillämpningsdata, är anonymiserad, det vill säga att inga personer kan identifieras. En del anonymiseringsenheter gör om personer till punkter medan andra genom konturer kan avgöra om det är en vuxen, ett barn, en rullstolsburen och så vidare. Men i det överenskomna användningsområdet är det punkter som representerar personer.

Vägledning avseende klassningsnivå – konfidentialitet

Det är viktigt att analysen med avseende på konsekvensnivån konfidentialitet - baseras på två informationsmängder. Dels innan anonymiseringen, i den

ursprungliga ”råa” formen, och dels efter anonymiseringen, i den bearbetade formen som används i själva tillämpningen. Med betryggande avidentifiering uppskattas att konfidentialiteten efter anonymisering sänks ner mot **försumbar (0)**. Om den icke anonymiserade informationen skulle hamna i orätta händer skulle de ha en **allvarlig (3)** påverkan. Andra exemplifierade användningsområden har sannolikt likartad klassning.

Vägledning avseende klassningsnivå – riktighet

För att kunna fatta rätt beslut i planering av trafikströmmarna är det viktigt att informationen är korrekt. En felaktig planering kan leda till besvär eller ekonomisk skada för såväl andra organisationer som för enskilda. Klassning avseende riktighet bedöms till **betydande (2)**. Andra exemplifierade användningsområden kan ha likartad klassning, men konsekvensen behöver beaktas för att säkerställa det.

Vägledning avseende klassningsnivå – tillgänglighet

Om informationen inte finns tillgänglig har den ringa påverkan på planeringsarbetet förutsatt att det inte rör sig om lång frånvaro av tillgänglighet. Klassningen avseende tillgänglighet bedöms till **försumbar (0)**. Andra exemplifierade användningsområden har sannolikt inte likartad klassning, utan konsekvensen behöver beaktas för att säkerställa det.

Mäta badvattentemperatur

I och med att nya tekniska innovationer utvecklas kan också den kommunala servicen bli mer omfattande och ta sig nya uttryck. Ett sådant modernare uttryck är att mäta badvattentemperatur och förmedla den via kommunens kommunikationskanaler. Detta är en tjänst som är särskilt efterfrågad på sommaren. Rent tekniskt placeras sensorer som mäter temperaturen ute vid de kommunala badplatserna. Informationen förmedlas krypterat till mottagningspunkter och vidare till en nätverksserver. Sedan kan informationen publiceras såväl i kommunens kanaler som via öppna API:er.

Vägledning avseende klassningsnivå – konfidentialitet

Den information som finns i denna typ av IoT-system tenderar att ha relativt låga krav på konfidentialitet. Tanken är att den ska kunna delas öppet och att andra tjänster också ska kunna byggas med informationen som grund. Visserligen innehåller den information som förmedlas både tidsstämpel och en koordinat samt vattnets tillstånd (alltså dess temperatur) men all denna information är av okänslig karaktär om den skulle hamna på avvägar. Om vattentemperaturen till exempel mättes i sötvattentäkter skulle informationen kunna vara av känslig karaktär utifrån ett säkerhetsperspektiv. Med den aktuella appliceringen är bedömningen dock att klassningen bör vara **försumbar (0)**.

Vägledning avseende klassningsnivå – riktighet

Informationen i den beskrivna appliceringen används av kommuninvånarna för att få en bild av hur varmt det är i vattnet inför ett besök på en badplats. Det som eventuellt kan påverkas är kommunens varumärke men bedömningen är trots det att skadan vid oriktig information är **försumbar (0)**.

Vägledning avseende klassningsnivå – tillgänglighet

På motsvarande sätt som med klassningsnivån för riktighet är bedömningen att påverkan med avseende på tillgänglighet inte är speciellt stor. Om informationen inte finns tillgänglig för kommuninvånarna kan det på sin höjd skapa en besvikelse eller en olägenhet. Bedömningen är således att klassningsnivån för tillgänglighet bör vara **försumbar (0)**.

Central IoT-plattform

Förutom verksamhetsspecifika lösningar för exempelvis trafikstyrning eller belysning kan en organisation välja att hantera, lagra och bearbeta den insamlade informationen från IoT-enheter i en central IoT-plattform. Den kan även användas för att skicka ut styrsignaler till anslutna aktuatorer utifrån förutbestämda eller dynamiska scenarier. Förutbestämda betyder i det här sammanhanget att regelverket är fast medan dynamiska innebär att hänsyn tas till ett antal variabler i omgivningen. IoT-plattformen kan också användas för att administrera själva IoT-enheterna, såväl sensorer som aktuatorer.

Att organisationer väljer att upphandla centrala IoT-plattformar beror ofta på dessa plattformars förmåga att hantera den typ av informationsströmmar som genereras av IoT-lösningar. IoT-plattformar är byggda för att kunna hantera många datapunkter med en mycket liten datamängd i varje. Med hjälp av IoT-plattformar kan också information delas vidare till resten av organisationen eller till andra externa parter på ett kontrollerat sätt via API:er.

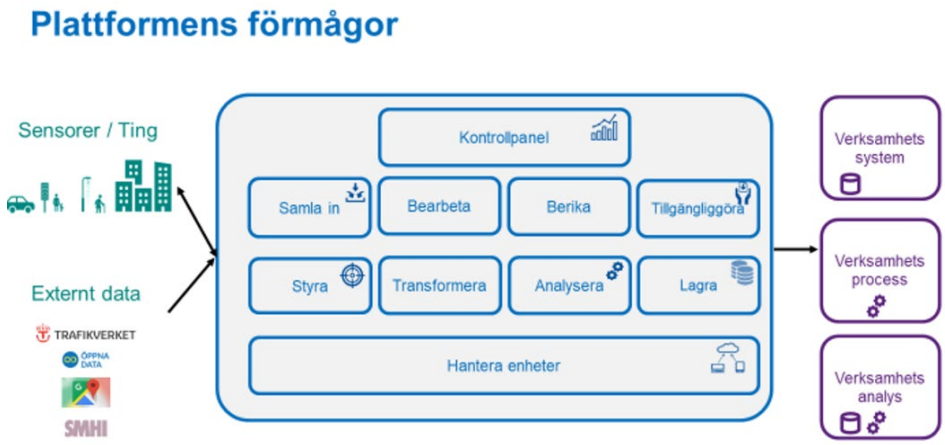

Bild 3. Visualisering av en IoT-plattform. Källa: Smart stad-programmet i Stockholms stad

Vid informationsklassning av denna typ av plattform är det än mer tydligt att fokus behöver vara på den information som behandlas. Beroende på vilken information som samlas in, lagras och bearbetas bedöms de olika perspektiven ur ett informationsklassningsperspektiv. I det här sammanhanget går det inte att ge en tydlig vägledning då en IoT-plattform enbart är en behållare för information som samlats in av andra IoT-system. Själva informationsklassningen behöver således baseras på data som finns i det aktuella systemet. Det är inte ovanligt att organisationer segmenterar informationen i sina IoT-plattformar för att kunna ha olika säkerhetsnivå på olika delar och där stor del av informationen till och med kan vara öppen.

För en organisation som står inför upphandling av en ny IoT-plattform har vi identifierat tre möjliga resonemang som kan föras inför upphandlingen som resulterar i olika tillvägagångssätt:

1. Utgå från känd information

För att komma fram till upphandlingskraven vad gäller informationssäkerhet kan man inledningsvis utgå från de kända informationsströmmarna, de som kommer att implementeras först, och informationsklassa lösningen utifrån detta. Vid varje tillkommande informationsström, informationsbearbetning eller ny tillämpning som använder informationen på ett nytt sätt, behöver informationsklassningen omvärderas för att bedöma om den nya situationen innebär att bedömningen av informationsklassningen förändrats. Detta gäller bedömningen av såväl konfidentialitet som riktighet och tillgänglighet.

2. Ta höjd för det värsta scenariot

Ett alternativt tillvägagångssätt kan vara att inför en upphandling informationsklassa utifrån den sannolikt högsta nivån som kan bli aktuell över tid, vilket skulle kunna innebära nivån synnerligen allvarlig (4) för såväl konfidentialitet som riktighet och tillgänglighet. Detta innebär dock att mer avancerade säkerhetsåtgärder behöver vidtas för att möta denna höga nivå, även om den egentligen inte är nödvändig. I och med detta blir lösningen också sannolikt mer kostsam att implementera och eventuellt även att drifta och förvalta än om en lägre nivå, och därmed lägre informationssäkerhetskrav, skulle vara applicerbar.

3. Möjliggör utveckling

Att istället säkerställa att lösningen är tillräckligt flexibel och utvecklingsbar över tid så att nödvändiga utökningar av säkerhetsåtgärder kan tillföras när nya behov uppstår, är sannolikt ett mer kostnadseffektivt tillvägagångssätt än alternativ 2 ovan.

Vägen framåt

Denna vägledning gör inte anspråk på att vara heltäckande. Vägledningen kommer att behöva utvecklas successivt för att möta ett ökat behov av handgripligt stöd till organisationer så att de kan arbeta vidare och utveckla sitt eget arbete med informationssäkerhet vid införande och förvaltning av IoT-system.

Nedan listas exempel på ett antal områden som identifierats som intressanta ur lokalt/regionalt perspektiv:

Samhällets infrastrukturtjänster – återvinning, avfallshantering, vatten- och energianvändning, utryckningsfordon och drönartjänster, positionering av arbetsfordon och redskap, läckagedetektering i ledningsnät.

Tjänster för den byggda miljön – monitorering av byggnader, infrastrukturanläggningar, parkering, park- och naturområden för optimering av underhåll, drift och skötsel, bevattningssystem, snöröjningstjänster, positioneringstjänster.

Mobilitet – kollektivtrafik, mobilitet som tjänst, cyklister, fotgängare och mikromobilitet, trafikinformation och trafikledning, uppkopplade och automatiserade fordon, godstransporter och citylogistik, parkeringstjänster.

Samhällsplanering och offentliga rummet – trygghet och säkerhet, flöden, personer i stråk, folksamlingar och trängsel, rörelsemönster, buller- och luftkvalitetsmätningar, trafikmönster, klimatanpassning, dagvattenmängder.

Trygghet och hälsa – tjänster för ökat kvarboende i egna hemmet, miljö, fall- och olycksdetektion, trygghetslarm, smarta lås och larm, aktivitetsövervakning, socialt nätverkande, bevakningskameror, utökat utbud av autentiseringsmetoder.

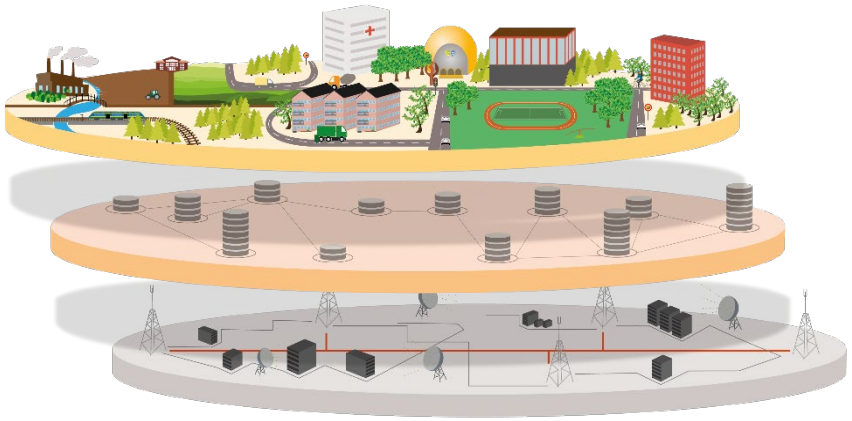

Bild 4. Successiv utveckling av KLASSA för IoT inom flera områden kommer att stärka samhällets aktörers förmåga att tillhandahålla samhällsservice och välfärdstjänster av god kvalitet i framtiden.

Arbetet med vägledningen fortsätter utifrån ambitionen att skapa en normativ grundplattform med handgripligt stödmaterial, klassningsmodeller för frekvent förekommande IoT-system och en metodik för analys av aggregerade informationsmängder.

SKR välkomnar därför alla initiativ till samverkan som kan bidra i det fortsatta arbetet med att utveckla samt successivt komplettera stödmaterial för informationsklassning av IoT. Vi ser därför fram emot att ni hör av er med förslag på tillämpningar av IoT där genomförda informationsklassningar skulle kunna ligga till grund för publicering av ett fritt tillgängligt, normativt stödmaterial.

Förslag, idéer, synpunkter och konkreta önskemål om samarbeten eller samverkan kan skickas till bo.baudin@skr.se alternativt klassa@skr.se

Vid färdigställandet av denna skrift pågår ett flertal relaterade projektinitiativ inom SKR, några av dessa är:

Datadriven innovation för smarta samhällen

Ramverk för dataplattformar, IoT och digital tvilling

Bildanalys för framtidens trafikstyrning

Beställarnätverk Vägledning Framtidens samhällen

Drönare i samhället

Digital samhällsbyggnadsprocess

Normativ vägledning för systematiskt informationssäkerhetsarbete – fastighetsperspektivet.

Bilaga 1. Avidentifiering

En utmaning med exempelvis multisensorer är att säkerställa att användningsområdet är det tänkta och att skydda fysiska personer mot otillbörligt intrång i den personliga integriteten. European Data Protection Board (EDPB), tidigare Article 29 Working Party, har under 2014 publicerat ett yttrande om avidentifieringsmetod (Yttrande 05/2014 om avidentifieringsmetoder, antaget den 10 april 2014, hädanefter förkortat till yttrandet). EDPB har därefter inte publicerat något nytt material på området. Yttrandet avsåg behandling av personuppgifter med avidentifieringsmetod under det tidigare dataskyddsdirektivet. Men då detta direktiv i huvuddrag återfinns i nu gällande dataskyddsförordning äger yttrandet fortsatt relevans för bedömningen av avidentifieringsmetod och dess förenlighet med dataskyddsförordningen.

I yttrandet används två termer:

Anonymisering - I dataskyddsförordningen, beaktandesats 26, stadgas att helt anonymiserade uppgifter, det vill säga uppgifter som är avidentifierade och därmed inte kan hänföras till en enskild fysisk person, inte omfattas av dataskyddsförordningen då dessa inte räknas som personuppgifter. Det springande kravet är därmed anonymiseringen och dess beständighet. Om uppgifterna med rimlig ansträngning kan reidentifieras är dessa inte att anse som anonymiserade, utan är istället pseudonymiserade.

Pseudonymisering - I artikel 4 dataskyddsförordningen stadgas att behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, är att behandla personuppgifter på ett pseudonymiserat sätt. Det är fortfarande personuppgifter som behandlas då de pseudonymiserade uppgifterna kan omvandlas till personuppgifter igen.

Sammanfattning av yttrandet

När en datasamling är helt avidentifierad (anonymiserad) och enskilda personer inte längre går att identifiera i samlingen, är dataskyddslagstiftningen inte tillämplig på samlingen (se beaktandesats 26 dataskyddsförordningen). Viktigt att poängtera är att dataskyddslagstiftningen gäller fram till dess att personuppgifterna är helt anonymiserade, det vill säga fram till dess att avidentifiering genomförts. Avidentifieringen i sig är en vidarebehandling efter en tidigare behandling av personuppgifter, som exempelvis kan vara ”insamling för statistikändamål”. Detta betyder att även denna vidarebehandling (avidentifieringen) kräver både att det ursprungliga ändamålet med behandlingen fortsatt följs och att det finns en laglig grund för avidentifieringen. Det går alltså inte att förändra eller utöka det syfte för vilket personuppgifterna ursprungligen samlades in (s.k. ändamålsglidning) (s.7).

Avidentifiering innebär att tillräckligt med beståndsdelar måste tas bort från samlingen för att förhindra identifiering - och detta behöver vara oåterkalleligt (s. 5-6)! För att något ska anses vara identifierbart krävs att man med olika hjälpmedel, som rimligen kan användas, åter kan få reda på uppgifter om enskilda. Sammanhanget och omständigheterna i det enskilda fallet inverkar direkt på identifierbarheten (s. 9). Rimlighetsbedömningen av vilka hjälpmedel som kan användas styrs av flera faktorer; kostnaden, det kunnande som krävs för att använda hjälpmedlet, hur sannolikt ett hjälpmedel är och hur allvarlig användningen skulle vara. Det ska även tas i beaktande att informations- och kommunikationsteknikens utveckling kan medföra att identifieringsrisken ökar med tiden (s. 9).

Det är inte bara antagonister eller dylikt som avses när det gäller identifiering med hjälpmedel enligt ovan. Även när en personuppgiftsansvarig (eller annan behörig) inte utplånar ursprungliga identifierbara uppgifter på händelsenivå, för att därefter överlämna en del av eller hela samlingen av uppgifter vidare i en pseudonymiserad form, utgör denna samling fortfarande personuppgifter (s. 9). Yttrandet lämnar här ett exempel på en sådan situation (från s. 9, längst ner):

″Om en organisation samlar in uppgifter om enskilda personers resor utgör de individuella resemönstren på händelsenivå fortfarande personuppgifter för varje part, så länge som den registeransvarige (eller någon annan part) fortfarande har tillgång till ursprungliga rådata, även om direkt identifierare har avlägsnats från det dataset som tillhandahålls till tredje parter. Men om den registeransvarige utplånar rådata och endast tillhandahåller statistik som aggregerats på hög nivå till tredje parter, såsom "på måndagar är det 160 % fler passagerare på reseträcka X än på tisdagar" kan detta räknas som anonyma uppgifter."

Det ska även nämnas att pseudonymiserade uppgifter legalt inte anses vara anonymiserade uppgifter (s. 11) och dataskyddslagstiftningen gäller därför fortfarande för pseudonymiserade uppgifter.

Risker med avidentifiering

Enligt yttrandet finns det tre återkommande risker med avidentifiering: särskiljbarhet, länkbarhet och inferens (s.12). Särskiljbarhet innebär att det finns möjlighet att identifiera information till en enskild person i informationssamlingen. Länkbarhet är risken för att information om en enskild person eller grupp kan länkas samman mellan en eller flera informationssamlingar. Inferens innebär att det är möjligt att med signifikant sannolikhet komma fram till värdet av ett attribut med hjälp av värdet från flera andra attribut.

En lösning som skyddar mot dessa tre risker ska vara motståndskraftig mot reidentifiering som utförs med de mest sannolika och rimliga verktyg som den registeransvarige och eventuell annan person kan utnyttja (s.12)

Randomisering och generalisering

Enligt yttrandet är randomisering och generalisering i stort de två samlingar av metoder som finns för avidentifiering. Syftet med randomiseringsmetoder är att genom att påverka sanningshalten i information, ta bort kopplingen mellan sagda information och den enskilda personen. Rationalen bakom metoden är att om uppgifterna är tillräckligt osäkra så ska de inte längre kunna hänföras till en viss enskild person. Syftet med generaliseringsmetoder är att generalisera, eller späda ut, enskilda uppgifter (i yttrandet kallat ”attribut”) genom att ändra den relativa storleksordningen. Detta kan ske genom att aggregera upp uppgifter på en högre mer generaliserad nivå, exempelvis genom att ange region istället för stad eller år istället för fullständigt datum. Det är självklart möjligt att kombinera randomiserings- och generaliseringsmetoder för ett starkare integritetsskydd och det kan även behövas flera olika sorters randomiserings- och generaliseringsmetoder på samma dataset för att åstadkomma en säker avidentifiering.

Randomisering

I yttrandet tas flera metoder för randomisering upp. Här tas huvuddragen i dessa upp. För mer information om dessa och en genomgång av varje metods påverkan på de tre riskerna särskiljbarhet, länkbarhet och inferens samt information om vanliga misstag vid användning av teknikerna, hänvisas vid varje metod till de sidor i yttrandet där metoden behandlas.

- **Brustillägg** (s.13) – Vid användning av randomiseringsmetoden brustillägg ändras uppgifter i ett dataset så att de blir mindre exakta samtidigt som den övergripande fördelningen bevaras. Som exempel tas upp att om en persons längd ursprungligen angavs avrundad till närmaste centimeter kan det dataset där brustillägg har använts istället innehålla en längduppgift med noggrannheten ± 10 cm.
- **Permutation** (s.14) – Vid permutation blandas värdena för uppgifter som är ordnade i en tabell på så sätt att vissa av uppgifterna artificiellt länkas till andra registrerade. Metoden uppges vara användbar när det är viktigt att bevara den exakta fördelningen av varje uppgift i ett dataset.
- **Differentiell integritet** (s.15-16) – I det fall en personuppgiftsansvarig själv vill behålla ett dataset med personuppgifter för egen räkning men vill kunna lämna ut anonymiserade uppgifter till tredje part kan randomiseringsmetoden differentiell integritet användas. Vid sökfrågor från tredje part hänförliga till datasetet kan den personuppgiftsansvarige lägga till slumpmässigt brus för att på så sätt anonymisera uppgifterna som tredje man begär innan dessa lämnas ut. Metoden differentiell integritet ger den personuppgiftsansvarige information inför varje nytt utlämnande om hur mycket brus som behöver läggas till och i vilken form detta ska göras för att en tillräcklig avidentifiering ska ske.

Generalisering

I yttrandet tas flera metoder för generalisering upp. Här tas huvuddragen i dessa upp. För mer information om dessa samt en genomgång av varje metods påverkan på de tre riskerna särskiljbarhet, länkbarhet och inferens samt information om vanliga misstag vid användning av teknikerna hänvisas vid varje metod till de sidor i yttrandet där metoden behandlas.

- **Aggregering och k-anonymitet** (s.17-18) – Aggregerings- och k-anonymitetsmetoder syftar till att förhindra att registrerade särskiljs genom att gruppera dem med minst k andra personer. För att uppnå detta generaliseras värdet på de enskilda uppgifterna (attributen) så att varje enskild person har samma värde. Genom att till exempel sänka detaljrikedomen (granulariteten) för en plats från en stad till ett land kan ett större antal registrerade inbegripas. Enskilda födelsedatum kan generaliseras till ett datumintervall eller grupperas per månad eller år.
- **L-diversitet/t-närhet** (s.18-20) – L-diversitet utvidgar k-anonymitet för att säkerställa att deterministiska inferensattacker inte längre är möjliga genom att se till att varje uppgift (attribut) i varje ekvivalensklass har minst l olika värden. Ett grundläggande mål att uppnå är att begränsa förekomsten av ekvivalensklasser med dålig attributvariabilitet, så att en angripare med bakgrundskunskap om en viss registrerad alltid lämnas med en betydande ovisshet. L-diversitet är lämpligt för att skydda uppgifter mot inferensattacker när attributvärdena är väl fördelade. T-närhet är en förfining av l-diversitet, eftersom syftet är att skapa ekvivalensklasser som liknar den ursprungliga fördelningen av attribut i tabellen. Metoden är användbar när det är viktigt att bevara uppgifterna så nära de ursprungliga som möjligt. I detta syfte används ytterligare en begränsningsregel på ekvivalensklassen, nämligen inte bara att det ska finnas minst l olika värden inom varje ekvivalensklass, utan också att varje värde representeras så många gånger som krävs för att avspegla varje attributs ursprungliga fördelning.

Vägen fram avseende avidentifiering

Avidentifiering är av yttersta vikt för den breda användningen av exempelvis multisensorer. Yttrandet redogör för olika avidentifieringsmetoder som kan användas för att se till att personuppgifter anonymiseras och därmed inte längre är att betrakta som personuppgifter. Detta leder till att dataskyddsförordningen inte längre är tillämplig.

Sannolikt är ingen av de metoder för avidentifiering som behandlas, vare sig det är randomiseringsmetoder eller generaliseringsmetoder, ensam tillräcklig för att möta de tre riskerna särskiljningsbarhet, länkbarhet och inferens som finns vid avidentifiering. En del av dessa risker kan dock mötas helt eller delvis av en viss metod. Det krävs därför en omsorgsfull utformning av tillämpningen av en viss metod på den specifika situationen och tillämpning av en kombination av metoderna som ett sätt att göra resultatet mer tillförlitligt. Det är även viktigt att ha en process för kontinuerlig översyn av anonymiseringen på plats för att kunna stävja att nya metoder för att reidentifiera uppgifterna används för att åter igen göra de anonymiserade uppgifterna till personuppgifter.

Vilka metoder som än används för att anonymisera personuppgifter gäller det att dessa tillräckligt väl minskar risken för särskiljbarhet, länkbarhet och inferens för att en anonymisering i dataskyddsförordningens mening ska kunna göras gällande. I annat fall kan personuppgifter på sin höjd anses vara pseudonymiserade.

Skillnaden mellan anonymisering och pseudonymisering är stor. Anonymisering av personuppgifter innebär att dataskyddsförordningen inte längre är tillämplig på uppgifterna, medan en pseudonymisering av personuppgifter enbart är en säkerhetsåtgärd som gör att personuppgifterna anses vara bättre skyddade vid eventuella personuppgiftsincidenter och dylikt, men fortfarande är det personuppgifter som behandlas.

Konsekvensen vid en otillräcklig anonymisering är därför att dataskyddsförordningen fortfarande gäller, då uppgifterna fortfarande betraktas som personuppgifter.

Bilaga 2. Kamerabevakning

Multisensorer är exempel på enheter som försetts med flera funktioner/sensorer, ofta med inbyggd kamera vilket gör att ett flertal lagar måste beaktas.

För att skydda fysiska personer mot otillbörligt intrång i den personliga integriteten har enheterna, eller implementeringen av dem, ofta försetts med intelligens som har förmåga att helt eller delvis anonymisera informationen. Se bilaga 1 för resonemang kring avidentifieringsmetoder. Det innebär att användaren av multisensorn inte ser de faktiska kamerabilderna utan bara får del av den anonymiserade information som multisensorn har fått till uppgift att bidra med.

Kamerabevakningslagen

Givet resonemangen kring avidentifiering och klassificering av information i olika steg återstår det faktum att en lösning med multisensor innehållande en kamera kan kräva tillstånd enligt kamerabevakningslagen (2018:1200).

3 § *Med kamerabevakning avses att en tv-kamera, ett annat optisk-elektroniskt instrument eller en därmed jämförbar utrustning, utan att manövreras på platsen, används på ett sätt som innebär varaktig eller regelbundet upprepad personbevakning*

Tillämpningar som använder multisensorer får normalt inte åtkomst till rådata utan endast anonymiserade tillämpningsdata, förutsatt att anonymisering sker enligt EDPB:s yttrande 05/2014, varför SKR:s Bildanalysprojekt undersöker om kamerabevakningstillstånd krävs för multisensorer i enlighet med resonemanget här.

EU:s dataskyddsförordning

Oaktat om användningen av multisensorer är tillståndspliktig eller ej enligt kamerabevakningslagen (2018:1200), ställs krav på att användningen av multisensorer inte strider mot EU:s dataskyddsförordning, exempelvis:

artikel 5 genom att behandla de registrerades personuppgifter på ett för den personliga integriteten mer ingripande sätt, och omfattat fler personuppgifter än vad som är nödvändigt, för det angivna ändamålet,

artikel 6 genom att behandla personuppgifter för ett intresse som inte väger tyngre än de registrerades intressen, och

artikel 13 genom att tillhandahålla bristfällig information till de registrerade.

Detta gäller i synnerhet för rådata. Det gäller inte för den avidentifierade informationen, tillämpningsdata, förutsatt att avidentifieringen innebär fullständig anonymisering. Här rekommenderas att ta fram en konsekvensbedömning och genomföra ett förhandssamråd med Datainspektionen för att

säkerställa att det givna resonemanget, dvs. att åtkomst till rådata enbart medges under kort tid och inte regelbundet samt att enbart behörig personal ges åtkomst till rådata vid kalibrering och service av utrustningen, inte är i strid med dataskyddsförordningen samt att den avidentifieringsmetod som används är ändamålsenlig.

Vidare är det självklart att åtkomst till rådata skyddas med lämpliga tekniska och organisatoriska skyddsåtgärder som följer av informationens skyddsvärde. Kontroll- och kravkatalogen i KLASSA är en grund för dessa åtgärder. Konsekvensnivån för rådata är sannolikt **allvarlig (3)** vilket betyder att merparten av alla skyddsåtgärder i kontroll- och kravkatalogen i KLASSA ska påföras.

KLASSA för IoT

Du som läser detta material kan vara i färd med att genomföra eller planera för en informationsklassning i ett IoT-projekt. Materialet riktar sig inte enbart till de som har stor erfarenhet av denna typ av arbete utan ska också vara användbart för de som inte har arbetat så mycket med informationsklassningar tidigare.

Målet är att belysa relevanta aspekter vid klassning av IoT-system och att ta fram normerande klassningar för ett antal vanliga användarfall. Detta för att göra det enklare för personer som arbetar ute i regioner och kommuner att själva ta sig an området.

Parallellt med framtagandet av denna vägledning har SKR initierat ett arbete med att ta fram en ny version av SKR:s verktyg KLASSA (KLASSA version 4). I den nya version som ser dagens ljus under våren 2021 sker en förflyttning från ett systemcentriskt fokus till ett mer informationscentriskt fokus. Ett informationscentriskt perspektiv är centralt när IoT ska informationsklassificeras.

KLASSA för IoT kommer att kompletteras över tid i syfte att stödja SKR:s medlemmar i det systematiska informationssäkerhetsarbetet. Vissa delar kommer också att ligga till grund för ytterligare vägledningsmaterial direkt kopplat till KLASSA-verktyget.

Upplysningar om innehållet
Bo, Baudin, bo.baudin@skr.se

© Sveriges Kommuner och Regioner, 2020
ISBN/Beställningsnummer: 978-91-7585-844-9
Text: Andreas Dahlqvist, Catlin Högfeldt Eberdal, Anders Henning, Thomas Nilsson, samtliga Certezza, Marika Wasserman och Olof Junesjö, Governo, Björn Hagström, Hagström Consulting, Bo Baudin, SKR
Illustrationer: Smart stad-programmet i Stockholms stad & Sanna Ranman, SKR
Produktion: SKR

ISBN: 978-91-7585-844-9
Ladda ner på webbutik.skr.se
Post: 118 82 Stockholm | **Besök:** Hornsgatan 20
Telefon: 08-452 70 00 | www.skr.se

Sveriges Kommuner och Regioner