Rapport april 2019

GDPR och Smarta Byggnader

EN UNDERSÖKNING AV TEKNIK, INDIVID OCH SAMHÄLLE I FRAMTIDENS SMARTA BYGGNADER

SMART BUILT ENVIRONMENT

GDPR och Smarta Byggnader

En undersökning av teknik, individ och samhälle i framtidens smarta byggnader

Skriven av Cyril Holm, Jonas Anund Vogel, Marco Molinari
Tillsammans med Barbro Fröding, Katarina Bäcklund, Elin Persson och Robin Roy

Förord

Smart Built Environment är ett strategiskt innovationsprogram för hur samhälls-byggnadssektorn kan bidra till Sveriges resa mot att bli ett globalt föregångsland som realiserar de nya möjligheter som digitaliseringen för med sig. Smart Built Environment är ett av 17 strategiska innovationsprogram som har fått stöd inom ramen för Strategiska innovationsområden, en gemensam satsning mellan Vinnova, Energimyndigheten och Formas. Syftet med satsningen är att skapa förutsättningar för Sveriges internationella konkurrenskraft och bidra till hållbara lösningar på globala samhällsutmaningar.

Samhällsbyggnadssektorn är Sveriges enskilt största sektor som påverkar hela vår be-byggda miljö, men den är fragmenterad med många aktörer och processer. Att förändra samhällsbyggandet med digitaliseringen som drivkraft kräver därför samverkan mellan många olika aktörer. Smart Built Environment tar ett samlat grepp över de möjligheter som digitaliseringen innebär och blir en katalysator för spridningen av nya möjligheter och affärsmodeller.

Programmets mål är att till 2030 uppnå:

Med stöd från
VINNOVA Sveriges innovationsmyndighet
Energimyndigheten
FORMAS
Strategiska innovations-program

- 40 % minskad miljöpåverkan i ett livscykelperspektiv för nybyggnad och renovering
- 33 % minskning av total tid från planering till färdigställande för nybyggnad och renovering
- 33 % minskning av de totala byggkostnaderna
- flera nya värdekedjor och affärsmodeller baserade på livscykelperspektiv, plattformar samt nya konstellationer av aktörer

I programmet samverkar programparter från näringsliv, kommuner, myndigheter, bransch- och intresseorganisationer, institut och akademi. Tillsammans nyttiggör vi den kunskap som tas fram i programmet.

Digitaliseringen av samhällsbyggnadssektorn är ett av projekten som har genomförts i programmet. Det har letts av Cyril Holm, Juridiska institutionen, Stockholms universitet och har genomförts i samverkan med KTH Live-In Lab, Filosofiska institutionen KTH, Akademiska hus, och HSB.

Projektet söker ge vägledning för kommersiella fastighetsaktörer att hantera datahanteringsfrågor i GDPR som uppkommer vid insamlande av data som grund för miljöoptimeringar av smarta hus.

Stockholm, 20 april 2019

Sammanfattning

Denna rapports huvudfokus är att undersöka balansen, beskriven ovan, utifrån det rättsliga ramverk som GDPR utgör, samt att ge vägledning för hur kommersiella fastighetsägare rent praktiskt kan arbeta med smarta byggnader. Den pågående trenden att genom sensorer och hantering av data påverka byggnaders resursanvändning och möjligheten till ökad tjänsteleverans kommer med all sannolikhet att fortsätta och öka. Digitaliseringen av samhällsbyggnadssektorn är enbart i sin linda och vinsterna på individ, företags och samhällsnivå, dels ekonomiskt och miljömässigt, bedöms som mycket stora. För att möjliggöra potentialen av digitaliseringen, en minimering av klimatpåverkan kopplat till drift av byggnader, och samtidigt värna om individens integritet måste framtida byggnaders system för insamling och hantering av data designas varsamt.

För att möjliggöra optimering av en byggnads tekniska system, samt en minimering av klimatpåverkan kopplat till drift av byggnaden, kan en fastighetsägare behöva samla in och lagra information som faller inom ramen för GDPR. För att säkerställa att fastighetsägaren följer GDPR beskrivet ovan bör följande rutiner och åtgärder genomföras.

- Rättslig strategi
- Minimera uppgifter som går att koppla till fysisk person
- Hur kan man optimera med aggregerade uppgifter som inte kopplas till person
- Problematisera samtycken, resultatet av det är en rättslig osäker het som leder till att använda anonyma data. Det är inte kopplingen till person som är intressant, utan optimeringen.
- Problematisera anonymisering, hur gör man rent tekniskt eller sam man utgå ifrån att det är en praktisk variant av anonymisering som gäller eftersom GDPR förslår det?

I den här rapporten vill vi visa hur man kan göra det enkelt att följa GDPR, och enkelt att bygga kommersiella smarta hus i relation till GDPR. Vårt förslag innehåller följande punkter som vi sedan utvecklar nedan.

<u>Data</u>

- Minimera lagring av data och maximera momentant utnyttjande av sensordata
- Höj och förfina optimeringsgraden
  Minimera uppgifter som går att koppla till fysisk person
  Pseudonymisera data som måste lagras

<u>Organisation</u>

- Ha tydlig organisation och ansvarsfördelning runt hanteringen av data och personuppgifter i relation till GDPR.
- Alltid ha en aktuell lista på sensorer
- Använd opt-out

- Utarbeta genomarbetade skriftliga samtycken.

DEN GRUNDLÄGGANDE OBLIGATIONSRÄTTSLIGA RELATIONEN

GDPR vill som sagt skydda individer mot att personlig data används på ett sätt som kränker fysiska personers rättigheter och personliga integritet. De traditionella relationerna mellan byggare och köpare, mellan köpare och säljare, eller mellan hyresfastighetsägare och hyrestagare har som utgångspunkt att det finns en etablerad rättslig relation mellan partnerna. Den här relationen bygger på frivillighet i motsats till många fall av konsumentrelationer där data samlas in utan att konsumenten vet om det. I den här rapporten tar vi avstamp i den här fördelen och försöker presentera ett enkelt sätt att organisera verksamheten gällande personuppgifter för att inte bryta med GDPR, trots att vissa delar av GDPR är direkt krångliga.

ORGANISATION OCH TEKNIK SOM OLIKA LÖSNINGAR PÅ GDPRS KRAV

En grundhållning bakom det förslag till en relativt enkel riskminimering i relation till GDPR som vi lägger fram är att den utmaning som ”hantering” av ”personuppgifter” utgör, i huvudsak är organisatorisk och inte teknisk. Det vill säga, det som är svårt och utmanande med GDPR är att man för att minimera risken att bryta mot GDPR så måste man ha organisatorisk kontroll över anvarsfördelning och kontroll över vilka data man samlar in. Vi för fram några enkla regler för hur man kan organisera arbetet med att hantera personuppgifter enligt GDPR.

FUNKTIONSOMRÅDEN SOM ETT SÄTT ATT ORGANISERA PERSONUPPGIFTER

Sensorer och system i byggnader kan generera data som möjliggör en mängd funktioner och tjänster, t.ex. energioptimering, säkerhet och hälsa. Dessa områden kallar vi för ”funktionsområden”. Vi tror att funktionsområden är ett bra sätt att organisera datamängder eftersom ett funktionsområde ofta hanteras av en avgränsad aktör (intern eller extern) och att det på det sättet utgör en väl definierad datamängd. Framtida tjänster kopplat till byggnader och användande av byggnader kan då också förpackas som funktionsområde och ansvarig person kan utses.

Tanken här är att en smart byggnad i praktiken blir ett komplext system som ”producerar” en stor mängd data, som ofta ligger utanför GDPR men ibland kan anses vara personuppgifter. Enligt GDPR ska man både tekniskt och organisatoriskt hantera personuppgifter på ett sådant sätt att man minskar risken för att man bryter mot GDPR. Vår tanke är här alltså att en smart byggnads funktioner är ett intuitivt sätt att organisera arbetet med persondata.

Givetvis kan en organisation som styrs av funktionsområden också vara ett redskap för att klargöra hur olika tekniker används för att förebygga att man bryter mot GDPR.

TYDLIGGÖR ANSVARIG PERSON

En kanske trivial men viktig punkt; se till att det finns ett dataskyddsombud och att denne har ansvariga personer för respektive funktionsområde som ansvarar för insamlad data. Personerna bör även ha befogenhet som följer ansvaret.

UPPRÄTTA INGÅENDE SAMTYCKEN OCH MÖJLIGGÖR "OPT-OUT"

Enligt GDPR måste man ha minst en laglig grund för behandling av personuppgifter. Samtycke är den lagliga grund enligt artikel 6 GDPR som troligen bör användas i smarta byggnader. Samtycket ska dokumenteras och är ett bra tillfälle att vara transparent i förhållande till köpare/användare/hyresgäst. Här finns alltså chansen att lista all data och alla personuppgifter som (önskas) samlas in. Det är naturligtvis också användbart för att "tvinga" sig själv att ha en lista på de data man samlar in, vad man ska använda datan till, hur länge man sparar den etc. Självklart kan listan användas för att kommunicera ansvar.

En viktig fråga här är om ojämlikheten mellan två parter är så stor att samtycken enligt GDPR inte kan användas. Det är inte svårt att tänka sig en situation där en hyresvärd har en så stor "makt" över hyresgästen att. För att undvika den situation som GDPR vill adressera med sitt samtyckesförbud vid ojämlika avtalasituationer, är att arbeta med "opt-outs". Givet att den här idén måste närmare prövas rättsligt, så är den bärande tanken att den "påtryckningssituation" som kan uppstå vid samtycket undviks om det är så att den samtyckande kan "opt-out" ur samtycket och informationshanteringen. Det ska framhållas att man behöver undersöka den här idén vidare rättsligt, samt även undersöka hur stor del av en datamängd som behövs för att man ska kunna uppnå de optimeringar som är önskvärda.

Använd opt-out, dvs. ge fysiska personer tillfälle av välja att data om dem inte samlas in utan att det resulterar i negativa konsekvenser.

UPPRÄTTA EN DATAHANTERINGSPLAN

Organiseras data på ett ställe, GDPR handlar lika mycket om hur man organiserar sig för att inte bryta mot GDPR som tekniska lösningar för att undvika det.

Data från sensorer och produkter/system kan variera över tid beroende på vilka funktioner som önskas. Av vikt är att upprätta en lista på sensorer och system som genererar data i byggnaden. Dels för att möjliggöra en rättssäker hantering av data, dels riskminimering och dels för att identifiera och möjliggöra framtida tjänster kopplat till data. Här kommer en lista på sensorer tagen från KTH Live-In Lab som visar vilka mätdata man kan samla in från lägenheterna i Testbed KTH. Även frekvensen på loggarna bör specificeras.

MINIMERA SPARAD DATA

Identifiera först om data behöver sparas. Om det räcker att enbart optimera byggnaderna utan att lagra data så bör det utföras. Skall däremot tjänster genereras så föreslår vi att man i samtycket för tjänsten också anger hur länge man sparar olika mätpunkter.

GDPR har en ganska krävande men också övergripande och därmed tydlig reglering som kräver att man minimerar uppgiftslagring. Vi tolkar det som att det finns ett utrymme för att spara data för optimering under en kortare tid, särskilt om den tiden specificeras till tidsutdräkt och ändamål (För forskning ser reglerna lite annorlunda ut men det rör inte den här rapporten.)

Den data som samlas in måste lagras på ett säkert sätt. Datan får lagras över lämplig period, och det som påverkar längden är komplexiteten på den tjänst som det gäller.

PSEUDONYMISERA DATA

Som vi såg i avsnitt 3.2.2. så är pseudonymiserade personuppgifter sådana data som behöver kompletteras för att direkt anknyta till en viss person. Sådan ”bakvägsidentifikation” gör att pseudonymiserade personuppgifter faller under GDPRs tillämningsområde. Exempel som lyftes fram vara:

- personliga månadskort för kommunaltrafik
- kontokortsnummer som bara anges delvis
- elektroniska nycklar
- krypterade uppgifter (t.e.x uppgifter som ”scramblats” för att sedan kunna låsas upp med en krypteringsnyckel)

Som framhållits är det viktigt att lägga märke till att det i GDPR inte krävs att den som har en pseudonymiserad personuppgift kan identifiera en person med hjälp av kompletterande uppgifter, utan endast att det är möjligt för någon att identifiera en person utifrån den pseudonymiserade personuppgiften.

GDPR uppmuntrar försiktigt till användning av pseudonymiserade personuppgifter. Med tiden kommer det att utkristallisera sig i vilken utsträckning som det kommer att vara tillåtet att använda sådana personuppgiter. I dagsläget är det vår uppfattning att man ska använda denna möjlighet så långt det är möjligt för att visa att man har för avsikt att leva upp till de krav som GDPR ställer.

Datan lagras i två separata system, där personuppgifter hålls isär från uppgifter kopplat till användandet av byggnader.

AVIDENTIFIERAD DATA

Att en personuppgift är *anomymiserad* innebär att det inte går att göra en ”baklängesidentifiering”. Det är dock tveksamt om anonymisering i en teoretisk

mening är möjlig.[1] Vi bortser från det här och accepterar att anonymisering är möjlig i en praktisk mening som anges i GDPR. Personuppgifter som är anonyma faller inte under GDPRs tillämpningsområde.

Vår uppfattning är att man i största möjliga mån bör anonymisera personuppgifter, och på grundval av aggregerad data om byggnader optimera dess system och funktionalitet. Tekniken för att avanonymisera måsta närmare studeras. Kan det göras på teknisk väg eller måste det ske genom handpåläggning.

UNDVIKA ATT HANTERA KÄNSLIGA PERSONUPPGIFTER

En allmän betraktelse är att det i stort sett är omöjligt att specificera vilken data man får samla in. All data kan teoretiskt sett härledas till känsliga personuppgifter. Exempelvis kan insamling och lagring av inomhustemperatur innebära information om inomhusnärvaro beroende på hur den bakomliggande algoritmen för byggnadsautomation är designad.

Genom sensorer och lagring av data kan man sällan nå de känsliga personuppgifterna specificerade i GDPR. Undantagen är dock religiös övertygelse och människans kropp. Religiös övertygelse skulle kunna detekteras genom att identifiera beteende som följer rytmer kopplade till religösa riter så som fasteperioder, högtider etc. Som diskuterat i Kapitel 2 är det teoretisk möjligt att identifiera enskilda elektriska apparater genom en högupplöst elsignatur vilket skulle kunna ge information kring användandet av t.ex. spis eller TV, och på så vis leda till information kring religiös övertygelse. Information kring människans kropp kan inhämtas via vissa typer av säkerhetssystem där t.ex. fingeravtryck används för öppning av dörrar. Även system för identifiering av gaser så som VOC-sensorer eller sensorer kopplade till urin/avföring faller troligen inom ramen för sensorer som kräver mer än informerat samtycke. Det finns även en kommande hälsotrend med t.ex. klockor, armband och ringar som mäter puls, temperatur, aktivitet etc. Information från dessa enheter anses med stor sannolikhet som känslig.

Om det föreligger affärsmässiga intressen att samla in och hantera känslig persondata, t.ex. genom att erbjuda tjänster till användare av byggnader, så är det rimligt att vidare undersöka data, insamling och GDPR. Som fastighetsägare är det dock av vikt att göra en risk-vinst bedömning då arbetet är både komplext och känsligt.

[1] Dorothy E. Denning och Peter J. Denning, ”The Tracker: A Threat to Statistical Database Security”, *ACM Transactions on Database Systems*, vol. 4, no. 1 (1979), pp. 76-96; och J. F. Traub, Y Yemini ach H. Wozniakowski, “The Statistical Security of a Statistical Database”, *ACM Transactions on Database Systems*, vol. 9, no. 4 (1984), pp. 672-9.

Summery

Innehållsförteckning

1 Bakgrund

Smarta byggnader är ett stort och växande fält. Egentligen är det inte fråga om ett fundamentalt nytt eller annorlunda fält; precis som inom andra fält är det fråga om att digitaliseringen ökar möjligheterna att samla in data för att sedan optimera olika funktioner och leverera tjänster baserat på dessa data.

Det som gör byggnader extra intressanta dock, är dels att människor vistas i dem under stor del av dygnet, dels att den verksamhet som bedrivs i byggnader ger upphov till mycket data. De data kan, i och med att byggnader och hem ofta kan likställas, vara av känslig karaktär och kan genom insamling och analys avslöja vilka vi är.

Det finns ett antagande om ett skyddat privatliv i ett hem som utmanas av den teknik som möjliggör optimeringar över en hel mängd områden som t.ex. energianvändning, hälsa, säkerhet och underhållning. Utifrån denna förutsättning uppstår den grundproblematik som gäller forskning om teknikutveckling och tjänsteproduktion i allmänhet; nämligen hur ska man balansera det goda som tekniken möjliggör – som till exempel bättre hälsa, mindre energianvändning, ökad säkerhet – mot det intrång i individers privata sfär som dessa optimeringar kräver.

Denna rapports huvudfokus är att undersöka balansen, beskriven ovan, utifrån det rättsliga ramverk som GDPR utgör, samt att ge vägledning för hur kommersiella fastighetsägare rent praktiskt kan arbeta med smarta byggnader.

De kommersiella aktörer som uppför byggnader kommer under de närmaste åren att vilja utnyttja de fördelar som ny teknik och digitalisering möjliggör, dels av rent ekonomiska skäl och dels eftersom användare av byggnader kommer börja kravställa nya tjänster kopplade till byggnader. Samtidigt kommer de att vara bundna av det regelverk som EU lagstiftningen GDPR utgör. Detsamma gäller forskning om smart byggnader, och därmed även den verksamhet som bedrivs inom KTH Live-In Lab. Forskning kring de effekter (t.ex. storskaliga resursoptimeringar, förbättrad inomhusmiljö, ökad hälsa och livskvalitet) som digitaliseringen möjliggör innebär att data måste samlas in. Trots det goda syftet måste även forskning följa de regler som ges i GDPR. Både i kommersiella verksamheter och i forskningen kommer frågan om lagring och bearbetning av data i databaser att vara ett aktuellt problem. Frågor som vilken typ av data får man lagra, hur länge, vilka har tillgång och hur ofta måste man gallra i data måste besvaras innan smarta byggnader på allvar kan realisera sin fulla potential. Även frågor kring vad man kan/får samla in och vill/bör samla in kommer diskuteras i rapporten.

Syftet är att undersöka och möjliggöra balans mellan teknik, individ och samhälle med tanken att teknik skall stödja de som äger, förvaltar och använder byggnader**. Målet** är att upprätta underlag/information till beställare (fastighetsägare) kring hur GDPR och andra regler påverkar uppförandet av nya smarta byggnader.

1.1 Rapportens inriktning

Smarta byggnader, liksom all datainsamling ger upphov till frågor. Det här illustreras bäst med ett exempel. En ung kvinna inhandlade kakaosmör, en stor väska, vitamintillskott och en ljusblå matta hos Target, en butikskedja i USA. Targets

automatiserade profileringsprogram identifierade den unga kvinnan som med hög sannolikhet gravid, varpå ett automatiserat gratulationsutskick gjordes till den unga kvinnan. Tonårsflickan var mycket riktigt gravid och hennes föräldrar överaskades av både hennes sexliv, liksom hennes graviditet.[2]

Det här exemplet visar hur till synes ointressant och orelaterade datapunkter snabbt kan säga mycket om fysiska personer. GDPR vill skydda individer mot att personlig data används på ett sätt som kränker fysiska personers rättigheter och personliga integritet. En stor skillnad med smarta byggnader jämfört med exemplet, är att det oftast finns ett obligationsrättsligt förhållande i grunden, alltså en rättslig relation mellan två parter, t.ex. en hyresrättsrelation, eller en relation mellan säljare och köpare av en bostadsrätt. Sådana relationer bygger på att man till vissa delar redan delar information och på något sätt är bekanta. Det är en stor fördel i relation till de krav som GDPR ställer, jämfört med en kommersiell aktör som samlar personlig data om ovetande kunder och sedan profilerar och riktar kommersiella erbjudanden till kunderna baserade på person data.

I den här rapporten tar vi avstamp i den här fördelen och presenterar ett enkelt sätt att organisera verksamheten gällande personuppgifter för att inte bryta med GDPR. En grundhållning bakom det förslag till en relativt enkel riskminimering i relation till GDPR som vi lägger fram är att den utmaning som ”hantering” av ”personuppgifter” utgör, i huvudsak är en organisatorisk och inte teknisk. Samtidigt som det här är huvudinriktningen i rapporten, kommer vi att se att den ger upphov till frågor om man kan säga att parterna i kommersiella relationer i byggindustrin är tillräckligt jämnbördiga för att samtycke enligt GDPR ska kunna användas som en laglig grund för behandling av personuppgifter. Vi återkommer till den här frågan i rapporten.

GDPR är en ”krånglig” lagstiftning, precis som många andra EU-regleringar, men som framgått fokuserar vi i den här rapporten på hur man gör det enkelt att bygga kommersiella smarta hus. Det finns en rad ganska komplicerade regler om: vad som händer vid en personuppgiftsincident (dvs. när det händer något med en personuppgift som strider mot GDPR) de sanktioner som GDPR stipulerar vid brott mot GDPR, certifiering, tillsynsmyndighet, och lika typer av samråd, rättigheter för

[2] Adam Henschke, *Ethics in the Age of Surveillance: Personal Information and Virtual Identities* (Cambridge: Cambridge University Press, 2009), p. 3. För mer om övervakning, personlig data, se t.ex. Stanley Greenstein, *Our Humanity Exposed: Predictive modelling in a Legal Context* (Stockholm: Stockholm University, 2017); Liane Colonna, *Legal Implications of Data Mining: Assessing the European Union's Data Protection Regulation Principles in Light if The United States Government's National Intelligence Data Mining Practices* (Tallinn: Ragulka, 2016); and Elisabet Fura and Mark Klamberg, “The Chilling Effect if Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA,” in *Freedom of Expression: Essays in Honour of Nicolas Bratza* (Oisterwijk: Wolf Legal Publishers, 2012), p. 463.

dem vars personuppgifter är registrerade. Vi kommer inte att säga så mycket om de många reglerna eller om övriga regler i GDPR av mer administrativ karaktär. Vad vi ska göra är visa hur man gör arbeten med behandling av personuppgifter enligt GDPR så enkelt som möjligt, så att man i så stor utsträckning som möjligt undviker svårigheterna med GDPR. Anledningen till den här ansatsen är att vi tycker att GDPRs skydd för individen är något bra, men att det också finns en risk att GDPRs ”krånglighet” leder till att byggs färre smarta byggnader. Med tanke på framförallt miljön, så tycker vi att det är viktigt att det byggs många smarta byggnader.

1.2 Rapportens innehåll

Rapporten är uppdelad i fyra delar: I Kapitel 2 av rapporten kommer vi först beskriva en smart byggnad (Testbädd KTH i KTH Live-In Lab) och de system för automation, kommunikation och datahantering byggnaden har. Vi beskriver även några exempel på vad data kan användas till. Fokus ligger på att beskriva tekniker/system som kan resultera i dels optimering av t.ex. resursanvändning och förbättrad tjänstegenerering, men vilka även kan leda till risker kring personlig integritet. I Kapitel 3 kommer vi att göra en genomgång av de mest relevanta delarna av lagstiftningen GDPR. Det är som sagt en lång och delvis komplicerad lagstiftning och här lyfter vi ur de mest centrala delarna. I Kapitel 4 lägger vi fram ett förslag på hur man arbetar med smarta byggnader och GDPR på ett sätt som är relativt enkelt. I Kapitel 5 diskuterar vi kring vägen framåt och möjliga framtida utvecklingsområden.

2 SMARTA BYGGNADER OCH DERAS SYSTEM – TESTBED KTH

2.1 BAKGRUND SMARTA BYGGNADER

Byggnader i den industrialiserade världen beräknas stå för 30-40% av den totala energianvändningen och 40% av koldioxidutsläppen (Berardi 2013). Informations- och kommunikationsteknik (IKT) har visat sig möjliggöra ökad energieffektivitet i den bebyggda miljön, t.ex. genom avancerade kontrollsystem, energiövervakning, feldetektering och främjande av mer hållbart beteende hos fastighetsägare och brukare (Faruqui, Sergici and Sharif 2010; Hargreaves, Nye and Burgess 2010, 2013). Som en konsekvens har smarta hem en hög prioritet i EU: s strategiska energiteknikhandlingsplan (Wilson, Hargreaves and Hauxwell-Baldwin 2017).

Smarta hem definieras som hemliknande miljöer med någon form av intelligens och automatik, vilket gör det möjligt för byggnadssystemen att agera beroende på brukarbeteende och leverera olika typer av anpassade tjänster

(De Silva, Morikawa and Petra 2012). Smarta hem erbjuder funktioner som går utöver kapaciteten i vanliga byggnader, till exempel förbättrad säkerhet, hemassistans och e-hälsa, ökad underhållning, kommunikation och visualisering (t.ex. genom feedback om resursanvändning), förbättrad komfort och inomhusluftkvalitet och mer effektiv energianvändning (Balta-Ozkan et al. 2013).

Smarta byggnader förväntas spela en viktig roll som enheter i smarta hållbara städer och har varit föremål för stor uppmärksamhet i litteraturen de senaste åren, se t.ex. Solaimani, Keijzer-Broers and Bouwman (2015). Smarta byggnader ses som fronten gällande teknikimplementering i byggsektorn, och den utökade användningen av sensorer förväntas öka förståelsen kring byggprocessen till att låsa upp

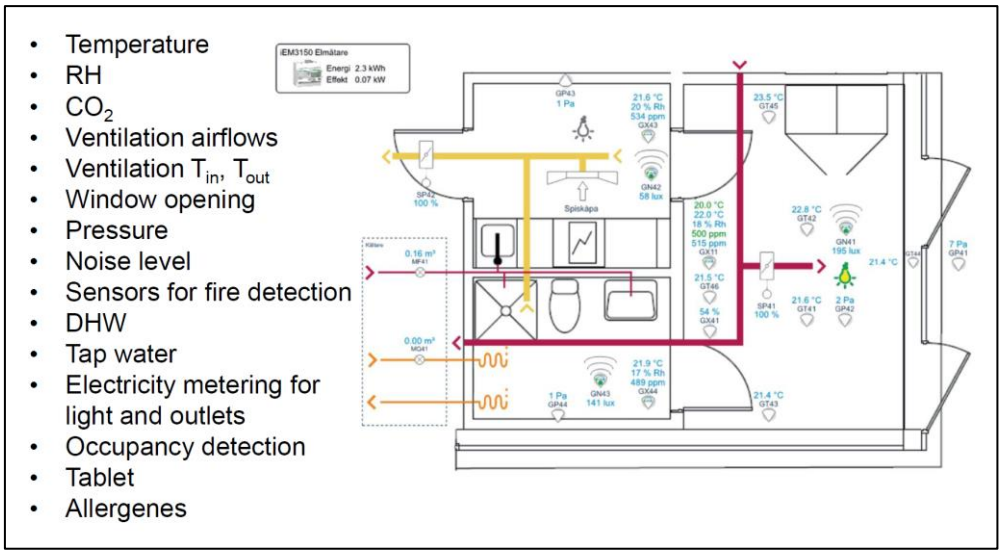
Figur 1 – Testbed KTH i genomskärning

energieffektivitetspotentialen (Prívara et al. 2011; Široký et al. 2011). Testbed KTH i KTH Live-In Lab uppvisar alla symptom kopplat till olika definitioner av smarta byggnader; Testbed KTH är en smart byggnad som använder den tekniska potentialen med ny teknik för att främja innovation inom samhällsbyggnadssektorn. KTH Live-In Lab är en plattform för forskning, test och verifiering samt utbildning och består av både virtuella och fysiska testmiljöer (Liveinlab 2018).

2.2 UPPBYGGNAD TESTBED KTH

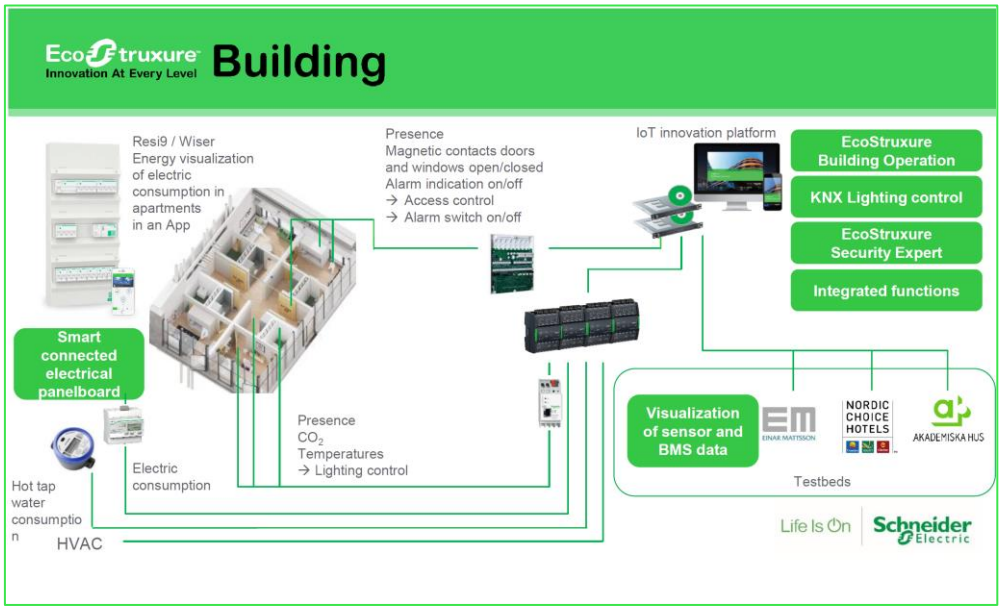
Testbed KTH är fysiskt placerat i ett av Einar Mattssons tre plusenergihus på KTH Campus Valhallavägen. Testbäddens bygglovsbefriade innovationsmiljö består av totalt 300 kvm lokalyta där olika konstellationer av lägenheter byggs upp på årlig basis. Testbädden värms upp via ett bergvärmesystem och värmen distribueras genom förvärmd tilluft. Testbädden är totalt flexibel gällande allt från planlösning och interiör till styr- och kontrollsystem. Testbädden har installationsgolv och två meter installationsutrymme ovan lägenheterna vilket möjliggör ombyggnad och nyinstallation utan påverkan på boende och utan större ombyggnadsåtgärder eller resursåtgång. Testbed KTH har egna system för uppvärmning och ventilation och även ett eget borrhål, värmepump, värmelager, solceller och databas. Testbädden har ett avancerat byggnadsautomationssystem som kan hantera alla i dagsläget använda protokoll så som modbus, m-bus, bacnet, LonWorks, KNX, Dali etc. Systemet skall även kunna hantera trådlösa/mobila protokoll så som Narrowband IoT (5G). I dagsläget

finns sensorer för temperatur, CO2, tryck, närvaro, luftfuktighet, ljusstyrka, VOC, el, dörr- och fönsteröppning, varm- och kallvattenanvändning (se Kap 4.2.6 för full lista). Samtliga enheter så som armaturer, spjäll, system (ventilation, värme mm) kan styras via inbyggda egna system eller från ett överordnat styrsystem, i dagsläget ett system från Schneider Electric.



Figur 2 - Sensorer och schematisk bild av en lägenhet i Testbed KTH

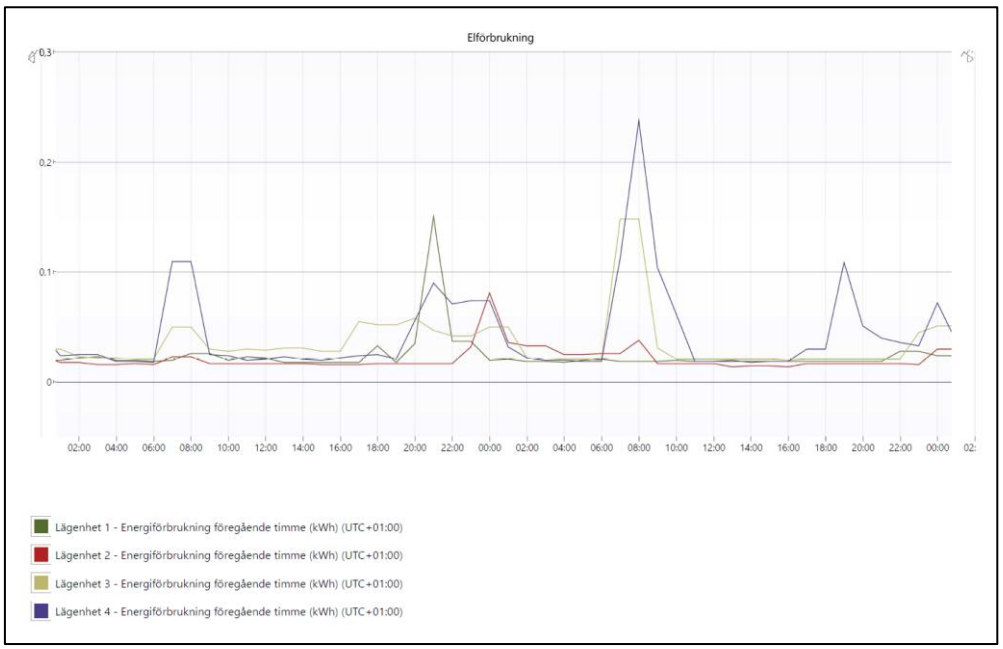
Data samlas in dels på en lokal ”Automation Server” och dels en på en överordnad virtuell ”Enterprise Server” (Microsoft SQL-server).



Figur 3 - Konceptuell skiss automationssystem och datalagring i Testbed KTH

2.2.1 Exempel data och känsliga personuppgifter

Smarta elmätare behövs i det moderna elnätet av många anledningar. De skapar tvåvägskommunikation mellan användare och nätägare och underlättar smarta tjänster, finansiell planering för användaren, distribuerad förnybar energi, nätstatistik etc. Men i huvudsak innehåller informationen om energianvändarprofilen också användarens sekretesskänsliga uppgifter. I synnerhet visar profildata användningsbeteendet kopplat till apparater som möjliggör uttömmande slutsatser om privatlivet. Till exempel om energianvändningen är olika på morgon och eftermiddag under lov kontra vanliga veckor tyder datan på att det är en familj med barn i skolåldern. Den informationen kan användas för riktade reklam- och annonsinsatser. Om energianvändningen inte ändras vid lunchtid kan det tyda på att personerna i hushållet är på ett dagligt arbete. Om någon använder apparater för matlagning under Ramadan så kan man dra slutsatsen att personerna inte är muslimer. Eftersom detta är relaterat till religiös information så kan den anses som känsliga personuppgifter och skulle därmed hamna i en kategori personuppgifter som i utgångsläget inte får behandlas enligt GDPR. Energiprofiler med högre upplösning kan även identifiera specifika apparater. Detta skulle möjliggöra att söka data för specifika apparater som till exempel är relaterade till specifika hälsoproblem och skulle återigen kunna göra att känsliga personuppgifter kommer fram ur till synes ”oskyldiga” datapunkter.



Figur 4 - Exempel elanvändning fyra lgh Testbed KTH, dock så pass låg upplösning att detektering av enskilda enheter är nästintill utesluten.

Ett annat exempel är mätning av CO2 inomhus. Förhöjda CO2-värden tyder på att det är någon eller några i byggnaden vilket i ett smart system skulle kunna trigga ökade ventilationsflöden. Frånvaro av förhöjda CO2-värden skulle samtidigt kunna indikera avsaknad av aktivitet i byggnaden och trigga en sänkning av ventilationsflöden. Med

samma system skulle även antal personer kunna avgöras vilket kan leda till att fastighetsägare får vetskap om hur många som stadigvarande vistas i respektive lägenhet/bostad. Man kan även tänka att information om tillfälliga besök under stunder av dygnet kan identifieras, vilket kan leda till allvarliga konsekvenser.

Figur 5 - CO2-signatur i tre rum i samma lägenhet, Testbed KTH

2.3 Varför sensorer och datalagring?

Den minskade kostnaden för IT-hårdvara har gjort det möjligt att installera ett växande antal sensorer i byggnader. En väl genomtänkt byggövervakningsplattform kan ge en helt ny nivå av förståelse för hur byggnader fungerar. Det gör att man exempelvis kan styra parametrar i inomhusmiljön (t.ex. temperatur, luftfuktighet och koldioxidnivå) och identifiera fel i systemen. Installation av sensorer som samlar data för optimering innebär ofta att data lagras - vilket i sin tur kan strida mot GDPR. Det ska dock framhållas att sensorer och datalagring inte nödvändigtvis är kopplade till varandra. I de följande styckena ger vi några relevanta exempel på sensordata och datalagringsapplikationer.

2.3.1 Exempel 1: Förbättrad kontroll

Sensorer kan installeras för att ge bättre lokalt inomhusklimat. Det här sättet att kontrollera inomhusklimat är vanligt i nyare kontorsbyggnader, och blir allt vanligare även i bostadshus. Av kostnadsskäl har man i bostadshus ofta använt så kallad ”open loop control”. I äldre bostadshus används ofta värmekurvan, eller skillnaden mellan vattentemperaturen hos inkommande vatten och utomhustemperatur. Eftersom förhållandena för varje termisk zon i en byggnad i princip är olika (beroende på strålning, beläggning, vind etc.) kommer en ”open loop control” att leda till suboptimerad kontroll av inomhusklimatet i en byggnads olika termiska zoner, samt till aggregerade energiförluster. Installation av sensorer samt lokal styrning av inomhusklimatet baserad på sensordata leder till ökad optimering och bättre kontroll i äldre byggnader, utan att det finns något direkt behov av att lagra data.

2.3.2 Exempel 2: Feldetektering

Installationen av sensorer ger ökad möjlighet att få en förståelse för byggnadens funktion och att identifiera fel. Grovt talat kan man säga att fel brukar uppstå antingen i (i) hårdvara (t.ex. en kretsventil som fastnat i ett läge, nedsmutsning i en värmeväxlare, eller fel på en fläkt) eller i (ii) logiken som styr kontrollen av byggandens system (t.ex. icke-optimala tröskelvärden eller kontrollregler). Manuell identifiering av fel i en byggnad är ofta tidskrävande och dyrt. Dessutom kan fel förbli oupptäckta under lång tid vilket leder till suboptimering under den tiden. Ett väl utformat byggautomatons- och styrsystem kan i stor utsträckning använda data insamlat av sensorer för att identifiera sådana fel. Även om sparade data inte är nödvändiga för att identifiera fel, så kan sparade data vara en hjälp när man jämför ett byggandssystems funktionssätt över tid.

2.3.3 Exempel 3: Information till användare om energianvändning

En annan framväxande tillämpning av sensordata i byggnader är att tillhandahålla återkoppling till användare angående deras energianvändning. Även om de här tillämpningarna är i sin linda, tycks pilotprojekt ändå visa att återkoppling av mönster för energianvändning är ett effektivt sätt att främja energieffektivt beteende. Den här återkopplingen bygger på att det finns data lagrat som kan visa energianvändning historiskt samt jämföra ”energibeteende” över tid. Typiska mätdata för inomhusmiljö är inomhustemperatur, koldioxidnivåer, och luftfuktighet; för energiflöden används data om luftflöden och temperaturer på luftflöden, och för närvaro i hemmet används typiskt rörelsesensorer.

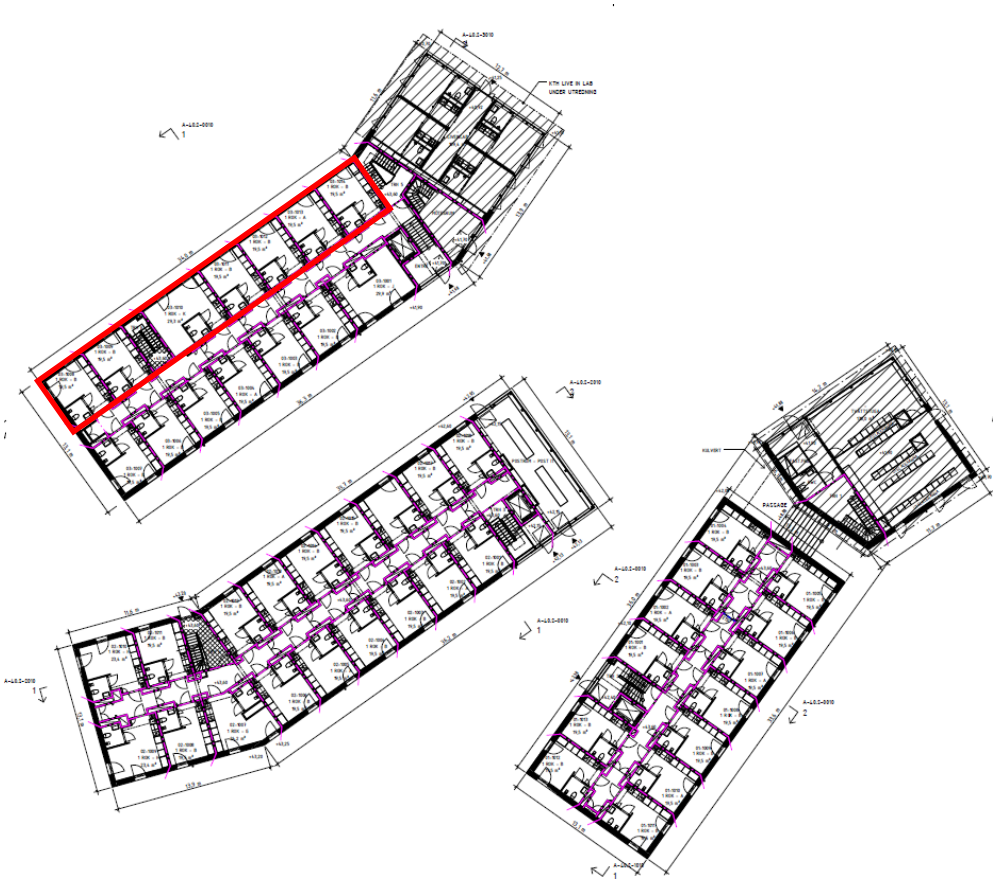
2.3.4 Exempel 4: Maskininlärning

Byggnadsenergiprestanda kan också i stor utsträckning gynnas av maskininlärning. Idag är maskininlärning vanligast i forskningsprojekt och på aggregerad nivå, t.ex. energianvändningsanalys av byggnader. Maskininlärning är tänkt att vara till nytta för både kontroll- och feldetektering och kommer sannolikt att användas för att hitta korrelationer mellan data av olika slag. Det är uppenbart att behovet av att lagra data i det här sammanhanget verkar oundvikligt. Data från olika källor, t.ex. från energistyrningsplattformen och från boendes mobiltelefoner, kan komma att behövas och lagras.

Möjligheten att deducera information och förbättra det totala systemets effektivitet genom maskininlärning kan illustreras med följande exempel. En grupp lägenheter kan väljas för att förbättra kontrollresultatet för en större uppsättning lägenheter (se Figur 6). Flera lägenheter med liknande egenskaper behövs för effektiviseringen, dessa lägenheter är markerade i rött. Det är uppenbart att ett större antal lägenheter sannolikt kommer att ge en mer robust data som underlag för effektivisering genom att sortera ur osäkerheter grundat på beteende, modellering och upplösning av data.

Det lägsta möjliga antalet lägenheter beror på komplexiteten i den större gruppen lägenheter och är svår att definiera a priori. Det är dock viktigt att framhålla att en

mindre grupp lägenheter som underlag för mätdata genom opt-out från samtycke till personuppgiftsanvändning, kan ändå vara tillräckligt underlag för optimering. Avvägningen mellan mängden data som ligger till grund för optimering, och graden av optimering som är möjlig med de data man samlar in, är en viktig skärningspunkt för den som är ansvarig för byggnadens system (jämför avsnitt om samtycken och opt-out i relation mellan avvägningar av graden av optimering)



Figur 6 – Exempel av användande av maskininlärning i KTH Live-In Lab

3 GDPR – General Data Protection Regulation - Dataskyddsförordningen

3.1 Introduktion

Dataskyddsförordningen eller General Data Protection Regulation (GDPR) är en manifestation av en europeisk tradition att tydliggöra individens suveränitet.[3]

GDPR är en lagstiftning som syftar till att avskärma information om individer genom att ge den enskilda personen en förfoganderätt till sådan information,[4] och genom att ställa strikta krav på den lagliga "behandlingen" av "personuppgifter" av andra än dem som informationen handlar om. Frågan om vem som äger personuppgifter enligt GDPR är vanligt förekommande, och även om vi sällan tänker på något som har stor ekonomisk betydelse som något som samtidigt saknar ägare, så får man nog grovt talat säga att det tycks vara GDPRs syn på saken; varken den person en personuppgift gäller, eller den som behandlar en personuppgift, äger personuppgiften. Däremot står det en kommersiell aktör fritt att behandla en personuppgift om man följer GDPRs principer för sådan behandling (artikel 5), samt har minst en laglig grund för sådan behandling (artikel 6). Samtidigt har den varom personuppgifter handlar, rättigheter som inte uppgår till en äganderätt men som ger fysiska personer rätt att bl.a. få ut all information om sig själv, att få all information om sig raderad, att när som helst ta tillbaka ett samtycke som ligger till grund för behandlingen. [Vi återkommer till den problematiken runt äganderätt till personuppgifter i en artikel i projektet.]

3.2 GDPRs tillämpningsområde

GDPRs tillämpningsområde är ”hantering” av ”personuppgifter”. Nedan ska vi först gå igenom vad personuppgift är för något i GDPRs mening och sedan göra samma sak med ”hantering” för att få en klar uppfattning om hur GDPR ska användas.

3.2.1 Vad är en ”personuppgift”

“Personuppgifter" i GDPR är uppfattad som all information som ensam, eller i kombination med annan information, kan identifiera en person.[5] Redan från denna definition förstår vi att denna lagstiftning har en mycket bred syn på dess tillämpningsområde. Tydliga exempel på "personuppgifter" inkluderar:

- personnummer,

[3] Se t.ex., Franz Wieacker, *A History of Private Law in Europe*, övers. Tony Weir, med förord av Reinhard Zimmermann (Oxford: Clarendon Press, 1995), Kapitel 2, speciellt kapitel 2; J.M Kelly, A Short History of Legal Theory (Oxford: Clarendon Press, 1992); och Randall Lesaffer, *European Legal History: A Cultural and Political Perspective* (Cambridge: Cambridge University Press, 2009).

[4] Kapitel 3; och inledningen artikel 7.

[5] artikel 4.1

- namn,
- adress,
- telefonnummer.

Exempel där information identifierar ett objekt i första hand, men därigenom också identifierar en person är:

- fastighetsinformation
- Bilregistreringsnummer,
- IP-nummer,
- GPS-position,

3.2.2 Anonymiserade och pseudonymiserade personuppgifter

Pseudonymiserade personuppgifter, dvs. data som behöver kompletteras för att direkt anknyta till en viss person, faller under GDPR så länge ”bakvägsidentifikation” är möjlig. Med bakvägsidentifikation menas att man med hjälp av information som tagits bort kan identifiera en person. Exempel på sådana uppgifter kan vara:

- personliga månadskort för kommunaltrafik
- kontokortsnummer som bara anges delvis
- elektroniska nycklar
- krypterade uppgifter (t.e.x uppgifter som ”scramblats” för att sedan kunna låsas upp med en krypteringsnyckel)

Det är viktigt att lägga märke till att det i GDPR inte krävs att den som har en pseudonymiserad personuppgift kan identifiera en person med hjälp av kompletterande uppgifter, utan endast att det är möjligt för någon att identifiera en person utifrån den pseudonymiserade personuppgiften.

Att en personuppgift är *anomymiserad* innebär att det inte går att göra en ”baklängesidentifiering”. Det är dock tveksamt om anonymisering i en teoretisk mening är möjlig.[6] Vi bortser från det här och accepterar att anonymisering är möjlig i en praktisk mening som anges i GDPR. Vi återkommer längre ner till möjligheter det här öppnar för optimering av byggnader utifrån aggregerade och anonymiserade personuppgifter.

3.2.3 Vad är ”hantering” av en personuppgift

"Hantering" av personuppgifter i GDPR betyder: "en åtgärd eller kombination av åtgärder beträffande personuppgifter […], oberoende av om de utförs automatiserat eller ej ."[7] En relativt uttömmande lista på vad som avses med ”hantering” lämnas i GDPR för att ge en uppfattning om ambitionen om denna lagstiftning och dess vida tillämpningsområde:

- insamling,

[6] Dorothy E. Denning och Peter J. Denning, ”The Tracker: A Threat to Statistical Database Security”, *ACM Transactions on Database Systems*, vol. 4, no. 1 (1979), pp. 76-96; och J. F. Traub, Y. Yemini och H. Wozniakowski, “The Statistical Security of a Statistical Database”, *ACM Transactions on Database Systems*, vol. 9, no. 4 (1984), pp. 672-9.

[7] Artikel 4.2

- inspelning,
- organisation,
- strukturering,
- lagring,
- anpassning,
- ändring,
- hämtning,
- samråd,
- använda sig av,
- upplysningar genom överföring,
- begagnade,
- avslöjas,
- sprids,
- kombinerades,
- begränsas,
- gjord tillgänglig,
- raderas,
- förstöras.

3.3 Hur hanterar man personuppgifter på ett lagligt sätt enligt DGPR?

I föregående avsnitt tittade vi närmare på GDPRs tillämpningsområde utifrån begreppen personuppgift och hantera. Om man faller inom GDPRs tillämpningsområde, då ska hanteringen av personuppgifter ske enligt de regler som uppställs i GDPR.

Den övergripande formuleringen av detta är att behandling av personuppgift endast får ske enligt samtliga GDPRs allmänna principer för behandling av personuppgift, och på minste en av de lagliga grunder för behandling av personuppgift som anges i GDPR.

3.3.1 GDPRs principer för hantering av personuppgifter

Om någon annan än ägaren av en uppsättning "personuppgifter" - det vill säga någon annan än den person som informationen handlar om - vill "hantera" dessa "personuppgifter", säger GDPR att du kan göra detta i enlighet med lagen om du följer alla allmänna principer för sådan behandling av personuppgifter som anges i GDPRs artikel 5. Dessa allmänna principer är:

- Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (laglighet, korrekthet och öppenhet).
- De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (ändamålsbegränsning).
- De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering).

- De ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (korrekthet).
- De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (lagringsminimering).
- De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).

Den personuppgiftsansvarige vid en organisation ansvarar för och ska kunna visa att de här principerna efterlevs (ansvarsskyldighet).

3.3.2 Lagliga grunder i GDPR för hantering av personuppgifter

Om "personuppgifter" behandlas enligt alla ovanstående allmänna principer måste laglig behandling också omfattas av minst en av de rättsliga grunderna för sådan behandling som anges i paragraf 6 i GDPR. Dessa rättsliga grunder är:

- Samtycke från den till vilken personuppgifterna hör (den registrerade). I de fall då ojämlikheten mellan parterna är oproportionerlig, såsom samtycke mellan myndigheter eller stora företag, kan den rättsliga grunden för samtycke för behandling av personuppgifter inte användas,
- När utförandet av ett avtal - som ägaren till personuppgifterna är part i - kräver att behandlingen av personuppgifterna behandlas,
- När någon annan än ägaren till "personuppgifter" måste behandla "personuppgifter" för att kunna uppfylla en rättslig skyldighet, såsom kraven i gällande lagstiftning,
- Behandling är nödvändig för att skydda de vitala intressena hos ägaren av personuppgifterna,
- Behandling är nödvändig för att utföra de offentliga myndigheternas uppgifter eller i allmänhetens intresse
- när de legitima intressena hos någon annan än ägaren av personuppgifterna kräver behandling av nämnda uppgifter, Dessa legitima intressen överväger dock inte de grundläggande rättigheterna och friheterna för datainnehavaren, det gäller inte heller situationer där ägaren till personuppgifterna är ett barn.

3.4 Känsliga personuppgifter

Allt ovanstående gäller laglig behandling av personuppgifter. Det finns dock ytterligare uppgifter om individer i GDPR - "känsliga personuppgifter". Förutom att känsliga

personuppgifter identifierar en fysisk person (som ”vanliga” personuppgifter) så är gäller den information som anses vara extra skyddsvärd. Behandling av "känsliga personuppgifter" är förbjuden enligt artikel 9.1. Känsliga personuppgifter är:

- ras
- etniskt ursprung
- kön
- politiska åsikter
- religiös övertygelse
- filosofisk övertygelse
- Människans kropp
- Hälsa
- Biometrisk information
- Genetisk information

Det finns ett antal betydande undantag från förbudet mot behandling av känsliga personuppgifter,[8] till exempel när ägaren av känsliga personuppgifter samtycker till behandling eller i situationer där sysselsättning eller social trygghet föreligger. Som vi kommer att se är undantaget för att behandla känsliga personuppgifter på grundval av samtycke särskilt viktigt när det gäller smarta byggnader och sådan funktionalitet som biometriska nycklar och hälsooptimeringar baserade på data om genetik och allmän hälsa.

Här följer en uppräkning av dessa undantag från förbudet att hantera känsliga personuppgifter:

- Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen av dessa personuppgifter för ett eller flera specifika ändamål, utom då unionsrätten eller medlemsstaternas nationella rätt föreskriver att förbudet i punkt 1 inte kan upphävas av den registrerade.
- Behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt eller ett kollektivavtal som antagits med stöd av medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.
- Behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.
- Behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen enbart rör sådana organs medlemmar eller tidigare medlemmar

[8] Artikel 9.2.

eller personer som på grund av organets ändamål har regelbunden kontakt med detta och personuppgifterna inte lämnas ut utanför det organet utan den registrerades samtycke.

- Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.
- Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet.
- Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.
- Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda.
- Behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet, såsom behovet av att säkerställa ett skydd mot allvarliga gränsöverskridande hot mot hälsan eller säkerställa höga kvalitets- och säkerhetsnormer för vård och läkemedel eller medicintekniska produkter, på grundval av unionsrätten eller medlemsstaternas nationella rätt, där lämpliga och specifika åtgärder för att skydda den registrerades rättigheter och friheter fastställs, särskilt tystnadsplikt. 4.5.2016 L 119/38 Europeiska unionens officiella tidning SV
- Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

4 REKOMMENDATIONER FÖR ENKEL HANTERING AV PERSONUPPGIFTER

4.1 Introduktion

I detta kapitel för vi samman Kapitel 2 och Kapitel 3 och går igenom hur GDPR påverkar möjligheten för en kommersiell fastighetsägare att uppföra smarta byggnader. Den pågående trenden att genom sensorer och hantering av data påverka byggnaders resursanvändning och möjligheten till ökad tjänsteleverans kommer med all sannolikhet att fortsätta och öka. Digitaliseringen av samhällsbyggnadssektorn är enbart i sin linda och vinsterna på individ, företags och samhällsnivå, dels ekonomiskt och miljömässigt, bedöms som mycket stora. För att möjliggöra potentialen av digitaliseringen och samtidigt värna om individens integritet måste framtida byggnaders system för insamling och hantering av data designas varsamt.

För att möjliggöra optimering av en byggnads tekniska system, samt en minimering av klimatpåverkan kopplat till drift av byggnaden, kan en fastighetsägare behöva samla in och lagra information som faller inom ramen för GDPR. För att säkerställa att fastighetsägaren följer GDPR beskrivet ovan bör följande rutiner och åtgärder genomföras.

- Rättslig strategi
- Minimera uppgifter som går att koppla till fysisk person
- Hur kan man optimera med aggregerade uppgifter som inte kopplas till person
- Problematisera samtycken, resultatet av det är en rättslig osäker het som leder till att använda anonyma data. Det är inte kopplingen till person som är intressant, utan optimeringen.
- Problematisera anonymisering, hur gör man rent tekniskt eller sam man utgå ifrån att det är en praktisk variant av anonymisering som gäller eftersom GDPR förslår det?

I det här kapitlet vill vi – som vi sa i rapportens inledning – visa hur man kan göra det enkelt att följa GDPR, och enkelt att bygga kommersiella smarta hus i relation till GDPR. Vårt förslag innehåller följande punkter som vi utvecklar nedan.

Data

- Minimera lagring av data och maximera momentant utnyttjande av sensordata
- Höj och förfina optimeringsgraden
  Minimera uppgifter som går att koppla till fysisk person
  Pseudonymisera data som måste lagras

Organisation

- Ha tydlig organisation och ansvarsfördelning runt hanteringen av data och personuppgifter i relation till GDPR.

- Alltid ha en aktuell lista på sensorer
- Använd opt-out
- Utarbeta genomarbetade skriftliga samtycken.

4.2 Utgångspunkter

I det här avsnittet tar vi upp några utgångspunkter för hur vi ser att arbetet med GDPR kan göras enkelt, innan vi går in på de konkreta punkterna för hantering av personuppgifter.

4.2.1 Den grundläggande obligationsrättsliga relationen

Exemplet i början av rapporten med den unga kvinnan som identifierades som gravid genom några inköp visar hur stor träffsäkerhet datainsamling kan ha i förutsägelser om individer. GDPR vill som sagt skydda individer mot att personlig data används på ett sätt som kränker fysiska personers rättigheter och personligaintegritet. Men en viktig poäng med det exemplet var att de traditionella relationerna mellan byggare och köpare, mellan köpare och säljare, eller mellan hyresfastighetsägare och hyrestagare har som utgångspunkt att det finns en etablerad rättslig relation mellan partnerna. Den här relationen bygger på frivillighet i motsats till exemplet där den som det samlas data om är ovetande. Som framhållits tar vi i den här rapporten avstamp i den här fördelen och försöker presentera ett enkelt sätt att organisera verksamheten gällande personuppgifter för att inte bryta med GDPR, trots att vissa delar av GDPR är direkt krångliga.

4.2.2 Organisation och teknik som olika lösningar på GDPRs krav

En grundhållning bakom det förslag till en relativt enkel riskminimering i relation till GDPR som vi lägger fram är att den utmaning som ”hantering” av ”personuppgifter” utgör, i huvudsak är organisatorisk och inte teknisk. Det vill säga, det som är svårt och utmanande med GDPR är att man för att minimera risken att bryta mot GDPR så måste man ha organisatorisk kontroll över anvarsfördelning och kontroll över vilka data man samlar in. Vi för fram några enkla regler för hur man kan organisera arbetet med att hantera personuppgifter enligt GDPR.

4.2.3 Funktionsområden som ett sätt att organisera personuppgifter

Sensorer och system i byggnader kan generera data som möjliggör en mängd funktioner och tjänster, t.ex. energioptimering, säkerhet och hälsa. Dessa områden kallar vi för ”funktionsområden”. Vi tror att funktionsområden är ett bra sätt att organisera datamängder eftersom ett funktionsområde ofta hanteras av en avgränsad aktör (intern eller extern) och att det på det sättet utgör en väl definierad datamängd. Framtida tjänster kopplat till byggnader och användande av byggnader kan då också förpackas som funktionsområde och ansvarig person kan utses.

Tanken här är att en smart byggnad i praktiken blir ett komplext system som ”producerar” en stor mängd data, som ofta ligger utanför GDPR men ibland kan anses vara personuppgifter. Enligt GDPR ska man både tekniskt och organisatoriskt hantera

personuppgifter på ett sådant sätt att man minskar risken för att man bryter mot GDPR. Vår tanke är här alltså att en smart byggnads funktioner är ett intuitivt sätt att organisera arbetet med persondata.

Givetvis kan en organisation som styrs av funktionsområden också vara ett redskap för att klargöra hur olika tekniker används för att förebygga att man bryter mot GDPR.

4.2.4 Tydliggör ansvarig person

En kanske trivial men viktig punkt; se till att det finns ett dataskyddsombud och att denne har ansvariga personer för respektive funktionsområde som ansvarar för insamlad data. Personerna bör även ha befogenhet som följer ansvaret.

4.2.5 Upprätta ingående samtycken

Enligt GDPR måste man ha minst en laglig grund för behandling av personuppgifter. Samtycke är den lagliga grund enligt artikel 6 GDPR som troligen bör användas i smarta byggnader. Samtycket ska dokumenteras och är ett bra tillfälle att vara transparent i förhållande till köpare/användare/hyresgäst. Här finns alltså chansen att lista all data och alla personuppgifter som (önskas) samlas in. Det är naturligtvis också användbart för att ”tvinga” sig själv att ha en lista på de data man samlar in, vad man ska använda datan till, hur länge man sparar den etc. Självklart kan listan användas för att kommunicera ansvar.

En viktig fråga här är om ojämlikheten mellan två parter är så stor att samtycken enligt GDPR inte kan användas. Det är inte svårt att tänka sig en situation där en hyresvärd har en så stor ”makt” över hyresgästen att. För att undvika den situation som GDPR vill adressera med sitt samtyckesförbud vid ojämlika avtalasituationer, är att arbeta med ”opt-outs”. Givet att den här idén måste närmare prövas rättsligt, så är den bärande tanken att den ”påtryckningssituation” som kan uppstå vid samtycket undviks om det är så att den samtyckande kan ”opt-out” ur samtycket och informationshanteringen. Det ska framhållas att man behöver undersöka den här idén vidare rättsligt, samt även undersöka hur stor del av en datamängd som behövs för att man ska kunna uppnå de optimeringar som är önskvärda.

4.2.6 Upprätta en datahanteringsplan

Organiseras data på ett ställe, GDPR handlar lika mycket om hur man organiserar sig för att inte bryta mot GDPR som tekniska lösningar för att undvika det.

Data från sensorer och produkter/system kan variera över tid beroende på vilka funktioner som önskas. Av vikt är att upprätta en lista på sensorer och system som genererar data i byggnaden. Dels för att möjliggöra en rättssäker hantering av data, dels riskminimering och dels för att identifiera och möjliggöra framtida tjänster kopplat till data. Här kommer en lista på sensorer tagen från KTH Live-In Lab som visar vilka mätdata man kan samla in från lägenheterna i Testbed KTH. Även frekvensen på loggarna bör specificeras. Den här typen av lista kan vara utgångspunkten för samtycket ovan.

- GN41 Närvarodetektor vardagsrum

- GN42 Närvarodetektor kök/hall
- GN43 Närvarodetektor badrum
- GP41 Mätgivare tryck ute
- GP42 Mätgivare tryck vardagsrum
- GP43 Mätgivare tryck kök/hall
- GP44 Mätgivare tryck badrum
- GT41 Mätgivare temperatur i tak
- GT42 Mätgivare temperatur i golv
- GT43 Mätgivare temperatur mot yttervägg
- GT44 Mätgivare temperatur mot yttervägg
- GT45 Mätgivare temperatur på innervägg
- GT46 Mätgivare temperatur på innervägg
- GX11_CO2 Reglerande koldioxidgivare vardagsrum
- GX11_RH Mätgivare luftfuktighet vardagsrum
- GX11_Temp Reglerande temperaturgivare vardagsrum
- GX41 Mätgivare VOC (Luftkvalitet)
- GX42 Mätgivare ljud vardagsrum
- GX43_CO2 Mätgivare koldioxid kök/hall
- GX43_RH Mätgivare luftfuktighet kök/hall
- GX43_Temp Mätgivare temperatur kök/hall
- GX44_CO2 Mätgivare koldioxid badrum
- GX44_RH Mätgivare luftfuktighet badrum
- GX44_Temp Mätgivare temperatur badrum
- MF41 Total varmvattenförbrukning
- MQ41 Total volymförbrukning golvvärme
- MQ41 Momentant flöde volym golvvärme
- Badrum_Närvaro_L Närvaroindikering
- Badrum_Närvaro_Lux_L Ljusstyrka
- Badrum_Uttag1_L Uttag input
- Badrum_Uttag1_S Uttag output
- Kök_Närvaro_L Närvaroindikering
- Kök_Närvaro_Lux_L Ljusstyrka
- Kök_Takbel_L Takbelysning input
- Kök_Takbel_S Takbelysning output
- Kök_Uttag1_L Uttag input
- Kök_Uttag1_S Uttag output
- Kök_Uttag2_L Uttag input
- Kök_Uttag2_S Uttag output
- Kök-Bänkbel_L Belysning input
- Kök-Bänkbel_S Belysning output
- Vardagsrum_Närvaro_L Närvaroindikering
- Vardagsrum_Närvaro_Lux_L Ljusstyrka

- Vardagsrum_Takbel_L Takbelysning input
- Vardagsrum_Takbel_S Takbelysning output
- Vardagsrum_Uttag1_L Uttag input
- Vardagsrum_Uttag1_S Uttag output
- Vardagsrum_Uttag2_L Uttag input
- Vardagsrum_Uttag2_S Uttag output
- Vardagsrum_Uttag3_L Uttag input
- Vardagsrum_Uttag3_S Uttag output

Loggar kommer logga med "Change of value"-funktion med ett delta på följande:

- Temperatur 0,2 °C
- CO2 20 ppm
- RH 2 %
- Förbrukning 0,01 m3
- Resterande 0,5

4.2.7 Minimera sparad data

Identifiera först om data behöver sparas. Om det räcker att enbart optimera byggnaderna utan att lagra data så bör det utföras. Skall däremot tjänster genereras så föreslår vi att man i samtycket för tjänsten också anger hur länge man sparar olika mätpunkter.

GDPR har en ganska krävande men också övergripande och därmed tydlig reglering som kräver att man minimerar uppgiftslagring. Vi tolkar det som att det finns ett utrymme för att spara data för optimering under en kortare tid, särskilt om den tiden specificeras till tidsutdräkt och ändamål (För forskning ser reglerna lite annorlunda ut men det rör inte den här rapporten.)

Den data som samlas in måste lagras på ett säkert sätt. Datan får lagras över lämplig period, och det som påverkar längden är komplexiteten på den tjänst som det gäller.

4.2.8 Pseudonymisera data

Som vi såg i avsnitt 3.2.2. så är pseudonymiserade personuppgifter sådana data som behöver kompletteras för att direkt anknyta till en viss person. Sådan ”bakvägsidentifikation” gör att pseudonymiserade personuppgifter faller under GDPRs tillämningsområde. Exempel som lyftes fram vara:

- personliga månadskort för kommunaltrafik
- kontokortsnummer som bara anges delvis
- elektroniska nycklar
- krypterade uppgifter (t.e.x uppgifter som ”scramblats” för att sedan kunna låsas upp med en krypteringsnyckel)

Som framhållits är det viktigt att lägga märke till att det i GDPR inte krävs att den som har en pseudonymiserad personuppgift kan identifiera en person med hjälp av kompletterande uppgifter, utan endast att det är möjligt för någon att identifiera en person utifrån den pseudonymiserade personuppgiften.

GDPR uppmuntrar försiktigt till användning av pseudonymiserade personuppgifter. Med tiden kommer det att utkristallisera sig i vilken utsträckning som det kommer att vara tillåtet att använda sådana personuppgiter. I dagsläget är det vår uppfattning att man ska använda denna möjlighet så långt det är möjligt för att visa att man har för avsikt att leva upp till de krav som GDPR ställer.

Datan lagras i två separata system, där personuppgifter hålls isär från uppgifter kopplat till användandet av byggnader.

4.2.9 Avidentifierad data

Att en personuppgift är *anomymiserad* innebär att det inte går att göra en ”baklängesidentifiering”. Det är dock tveksamt om anonymisering i en teoretisk mening är möjlig.9 Vi bortser från det här och accepterar att anonymisering är möjlig i en praktisk mening som anges i GDPR. Personuppgifter som är anonyma faller inte under GDPRs tillämpningsområde.

Vår uppfattning är att man i största möjliga mån bör anonymisera personuppgifter, och på grundval av aggregerad data om byggnader optimera dess system och funktionalitet. Tekniken för att avanonymisera måsta närmare studeras. Kan det göras på teknisk väg eller måste det ske genom handpåläggning.

4.2.10 Undvika att hantera känsliga personuppgifter

En allmän betraktelse är att det i stort sett är omöjligt att specificera vilken data man får samla in. All data kan teoretiskt sett härledas till känsliga personuppgifter. Exempelvis kan insamling och lagring av inomhustemperatur innebära information om inomhusnärvaro beroende på hur den bakomliggande algoritmen för byggnadsautomation är designad.

Genom sensorer och lagring av data kan man sällan nå de känsliga personuppgifterna specificerade i GDPR. Undantagen är dock religiös övertygelse och människans kropp. Religiös övertygelse skulle kunna detekteras genom att identifiera beteende som följer rytmer kopplade till religösa riter så som fasteperioder, högtider etc. Som diskuterat i Kapitel 2 är det teoretisk möjligt att identifiera enskilda elektriska apparater genom en högupplöst elsignatur vilket skulle kunna ge information kring användandet av t.ex. spis eller TV, och på så vis leda till information kring religiös övertygelse. Information kring människans kropp kan inhämtas via vissa typer av säkerhetssystem där t.ex. fingeravtryck används för öppning av dörrar. Även system för identifiering av gaser så som VOC-sensorer eller sensorer kopplade till urin/avföring faller troligen inom ramen för sensorer som kräver mer än informerat samtycke. Det finns även en kommande hälsotrend med t.ex. klockor, armband och ringar som mäter puls, temperatur, aktivitet etc. Information från dessa enheter anses med stor sannolikhet som känslig.

[9] Dorothy E. Denning och Peter J. Denning, ”The Tracker: A Threat to Statistical Database Security”, *ACM Transactions on Database Systems*, vol. 4, no. 1 (1979), pp. 76-96; och J. F. Traub, Y Yemini ach H. Wozniakowski, “The Statistical Security of a Statistical Database”, *ACM Transactions on Database Systems*, vol. 9, no. 4 (1984), pp. 672-9.

Om det föreligger affärsmässiga intressen att samla in och hantera känslig persondata, t.ex. genom att erbjuda tjänster till användare av byggnader, så är det rimligt att vidare undersöka data, insamling och GDPR. Som fastighetsägare är det dock av vikt att göra en risk-vinst bedömning då arbetet är både komplext och känsligt.

5 FRAMTIDA FORSKNINGSFRÅGOR OCH FÖRESLAGEN VÄG FRAMÅT

5.1 Vägen framåt

I det här avsnittet tittar vi på tre funktionsområden i smarta hus som ger upphov till personuppgifter och alltså kommer att behöva förhålla sig till DGPR. Vi ger de här funktionsområdena som exempel på kluster av information och personuppgifter som olika smart funktioner ger upphov till och som kommersiella aktörer behöver förhålla sig till. Dessa tre områden valdes utifrån den nuvarande utvecklingen inom forskning och teknik (i) energi, (ii) säkerhet och (iii) hälsa.

Men med ny ”genombrottsteknik” kommer de mest lovande funktionsområdena inom smarta byggnader att förändras. Oavsett sådana ändringar är den viktiga aspekten här dock att använda funktionalitetsområden för att illustrera hur de driver dataskapandet och hur dessa data hänför sig till GDPR. Vi vill också visa hur kombinationer av data kan tala om saker om individer som man inte har tänkt sig.

5.1.1 Energi

En vanlig applikation i en smart byggnad är att mäta koldioxidnivån i inomhusluften för att kunna bestämma när invånarna är närvarande.[10] Den kunskapen möjliggör optimeringar som att minska uppvärmning och ventilation när ingen är hemma. Om sådan "smart" funktionalitet används och om värmen som avges av boende och de apparater som de använder används som värmekällor som bidrar till att uppvärma ett bostadsutrymme, kan man till och med uppnå låga och höga inomhustemperatur. Resultatet minskar kraftigt energiförbrukningen, särskilt i kombination med solenergi och bra isolering.

Andra energioptimeringar gäller varmt vatten och el.[11] Med information om konsumtionsmönstret kan man lagra förvärmt varmvatten i isolerade tankar och el i batterier, som kan användas under spikar i efterfrågan. Sådan optimering baserad på användarmönster kan finjusteras för enskilda hushåll. Prissättning kan också användas för att ytterligare fördela efterfrågan under en typisk 24-timmars konsumtionscykel

[10] Vogel, Novak och Bohn Stoltz, ”KTH Live-In Lab: Testbädd för miljöinnovationer i bostadsbyggande,” sid. 14.

[11] Ibid., Sid. 14.

eller över årstiderna; köpa under "off hours", lagra lokalt för användning vid högsta förbrukningsnivåer.

Å andra sidan är det nödvändigt att fråga vilken typ av personuppgifter dessa optimeringar kräver. Om vi börjar med att mäta koldioxidnivån i inomhusluften, bär den informationen om när någon är hemma. Med tanke på att den här personen är bosatt, är den informationen "personuppgifter" enligt GDPR, eftersom den identifierar en person. Denna information kan ses som oskyldig i sig, men tillsammans med andra uppgifter kan det avslöja aspekter av en person som den personen vill behålla privat. Information om koldioxidnivåerna ger vidare information om hur många som finns i en bostad. Detta kan vara känsligt av ett antal skäl, t.ex. gällande hyresrätten, eller av skäl som gäller religiösa uppfattningar.

Vidare kan information om användningen av el ge information om vilka typer av apparater som används och vid vilka tider. Denna information kan verka harmlös, men analyseras och kombineras med annan information. Det kan ge en bild av frågor som individer kanske vill behålla privata.

5.1.2 Säkerhet

Traditionellt har vårt hem varit en plats att söka skydd från omvärlden; en plats där vi kan uppleva komfort, förtroende och integritet, som de flesta människor är angelägna om att skydda. Lagen säkrar traditionellt hemmet som en plats av yttersta betydelse i människans liv och en plats som är så betydelsefull för att stoppa regeringen med kraft, utan otillbörlig rättslig grund.[12]

Moderna "smarta" säkerhetsanordningar, som biometriska nycklar (nycklar som fungerar på fingeravtryck eller ansiktsigenkänning), låter dig bestämma exakt vem som använde låset när som helst för att komma in i ett hus. En CCTV-kamera placerad vid en ingång till en byggnad kan du se vem som står vid dörren. Smarta larm som kan övervakas från distans, och låter dig se insidan av ett hem på din mobiltelefon, är en annan funktion som redan är populär.

Även i detta fall kan de använda personuppgifterna vara känsliga och behandlingen måste överensstämma med GDPR.[13] Information om när du går in i huset kan vara skadlig när den är kopplad till annan information. Kameror vid ingångar avslöjar mycket data om individer, liksom kameraövervakning inne i bostaden. Data kan t.ex. avslöja kön, etnicitet, religiös praxis eller olydnad och så vidare.

5.1.3 Hälsa

Hälsa är en snabbt växande sektor, inte minst när det gäller "smart" teknik som stöder ett hälsosamt liv.[14] Lägg till det en stadig tillväxt av kunskap om hur man förhindrar välfärdssjukdomar som fetma, diabetes, kranskärlssjukdomar och cancer med justeringar i hur vi lever. Genom att äta mindre och mer näringsrik, och genom att träna, kan vi väsentligt ändra sannolikheten för dessa sjukdomar. Eftersom en bostad

[12] Jämför de konstitutionella bestämmelserna som statsmakten behöver för att gå in i eller genomsöka någons hem.

[13] GDPR Artikel 9.1.

[14] Se till exempel forskningsprojektet GoodBrother; finansierat av Horizon 2020, referens: OC-2018-1-23059.

är en plats där vi avslöjar information om hur vi lever våra liv, och eftersom vi spenderar mycket tid där, kan tekniken i smarta byggnader ”knuffa”[15] oss i riktning mot större chans för fler bra år under vår levnad.

Många använder teknik i telefoner för att övervaka daglig träning, hjärtfrekvens och så vidare. Många har också verktyg för motion i sina hem utöver att träna utomhus. Det finns dock ett antal saker du kan göra i ett smart hus som är svårt att utföra utanför huset. Till exempel kan man övervaka sömnkvaliteten, eftersom dålig sömnkvalitet, speciellt snarkning kan vara en indikator på andra hälsoproblem. Vidare kan man övervaka innehållet i utandningsluft från människor och ta en läsning av innehållet. Ett slutligt exempel är att övervaka innehållet i urin och fekal materia för att leta efter indikatorer på potentiell dålig hälsa.

Det är självklart att övervakning av detta slag genererar personuppgifter, i de flesta fall känsliga personuppgifter. Många av oss skulle också ha ett stort intresse att utnyttja uppgifterna, om vi genom att basera våra matvanor och träning på dem, ökade sannolikheten för fler hälsosamma år under vår livslängd. Det är emellertid också information som de flesta av oss uppfattar som mycket privat.

5.2 Framtida forskningsfrågor

Den stora frågan för forskning i närtid gäller hur mycket data man behöver för att uppnå tillfredställande nivåer av optimering. Är det så att man inte behöver 100% av datan för detta öppnar sig möjligheter att erbjuda ”opt-outs” ur samtycken till parsonuppgiftsinsamling. Visar det sig att man kan optimera till tillfredställande nivåer på anonym data, ja då öppnar det likanden möjligheter.

[15] Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth and Happiness* (London: Penguin, 2008).

6 Referenser

Balta-Ozkan, Nazmiye, Rosemary Davidson, Martha Bicket, and Lorraine Whitmarsh. 2013. "Social Barriers to the Adoption of Smart Homes." *Energy Policy* 63 (December): 363–74. doi:10.1016/j.enpol.2013.08.043.

Berardi, Umberto. 2013. "Clarifying the New Interpretations of the Concept of Sustainable Building." *Sustainable Cities and Society* 8 (October): 72–78. doi:10.1016/j.scs.2013.01.008.

Colonna, Liane. *Legal Implications of Data Mining: Assessing the European Union's Data Protection Regulation Principles in Light if The United States Government's National Intelligence Data Mining Practices* (Tallinn: Ragulka, 2016).

Denning, Dorothy E., Peter J. Denning. "The Tracker: A Threat to Statistical Database Security", *ACM Transactions on Database Systems*, vol. 4, no. 1 (1979), pp. 76-96.

De Silva, Liyanage C., Chamin Morikawa, and Iskandar M. Petra. 2012. "State of the Art of Smart Homes." *Engineering Applications of Artificial* Intelligence 25 (7): 1313–21. doi:10.1016/j.engappai.2012.05.002.

Faruqui, Ahmad, Sanem Sergici, and Ahmed Sharif. 2010. "The Impact of Informational Feedback on Energy Consumption—A Survey of the Experimental Evidence." *Energy, Demand Response Resources: the US and International Experience Demand Response Resources: the US and International Experience*, 35 (4): 1598–1608. doi:10.1016/j.energy.2009.07.042.

Greenstein, Stanley. *Our Humanity Exposed: Predictive modelling in a Legal Context* (Stockholm: Stockholm University, 2017).

Hargreaves, Tom, Michael Nye, and Jacquelin Burgess. 2010. "Making Energy Visible: A Qualitative Field Study of How Householders Interact with Feedback from Smart Energy Monitors." *Energy Policy* 38 (10): 6111–19. doi:10.1016/j.enpol.2010.05.068.

Hargreaves, Tom, Michael Nye, and Jacquelin Burgess.. 2013. "Keeping Energy Visible? Exploring How Householders Interact with Feedback from Smart Energy Monitors in the Longer Term." *Energy Policy* 52 (January): 126–34. doi:10.1016/j.enpol.2012.03.027.

Henschke, Adam. *Ethics in the Age of Surveillance: Personal Information and Virtual Identities* (Cambridge: Cambridge University Press, 2009).

Kelly, J.M. A Short History of Legal Theory (Oxford: Clarendon Press, 1992); och Randall Lesaffer, *European Legal History: A Cultural and Political Perspective* (Cambridge: Cambridge University Press, 2009).

Klamberg, Mark, Elisabet Fura. "The Chilling Effect if Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA," in

Freedom of Expression: Essays in Honour of Nicolas Bratza (Oisterwijk: Wolf Legal Publishers, 2012).

Liveinlab 2018, https://www.liveinlab.kth.se/en/om-labbet, accessed 20181212.

Prívara, Samuel, Jan Široký, Lukáš Ferkl, and Jiří Cigler. 2011. "Model Predictive Control of a Building Heating System: The First Experience." *Energy and Buildings* 43 (2–3): 564–72. doi:10.1016/j.enbuild.2010.10.022.

Solaimani, Sam, Wally Keijzer-Broers, and Harry Bouwman. 2015. "What We Do – and Don't – Know about the Smart Home: An Analysis of the Smart Home Literature." *Indoor and Built Environment* 24 (3): 370–83. doi:10.1177/1420326X13516350.

Široký, Jan, Frauke Oldewurtel, Jiří Cigler, and Samuel Prívara. 2011. "Experimental Analysis of Model Predictive Control for an Energy Efficient Building Heating System." *Applied Energy* 88 (9): 3079–87. doi:10.1016/j.apenergy.2011.03.009.

Thaler, Richard H., Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth and Happiness* (London: Penguin, 2008).

Traub, J. F., Y. Yemini, H. Wozniakowski, "The Statistical Security of a Statistical Database", *ACM Transactions on Database Systems*, vol. 9, no. 4 (1984), pp. 672-9.

Vogel, Novak och Bohn Stoltz, *KTH Live-In Lab: Testbädd för miljöinnovationer i bostadsbyggande.*

Wieacker, Franz. *A History of Private Law in Europe*, övers. Tony Weir, med förord av Reinhard Zimmermann (Oxford: Clarendon Press, 1995).

Wilson, Charlie, Tom Hargreaves, and Richard Hauxwell-Baldwin. 2017. "Benefits and Risks of Smart Home Technologies." *Energy Policy* 103 (April): 72–83. doi:10.1016/j.enpol.2016.12.047

SMART BUILT
ENVIRONMENT

Stockholms universitet

KTH VETENSKAP OCH KONST

KTH LIVE-IN LAB

AKADEMISKA HUS

HSB LIVING LAB

Med stöd från

VINNOVA Sveriges innovationsmyndighet

Energimyndigheten

FORMAS

Strategiska innovations-program

Smart Built Environment c/o IQ Samhällsbyggnad | Drottninggatan 33 | 111 51 STOCKHOLM | info@smartbuilt.se | 070-645 16 40 | www.smartbuilt.se