Sjyst data! – Slutrapport november 2019

Vinnova Utmaningsdriven Innovation (UDI), Steg 2

Sammanfattning: Utmaningar och möjligheter

Sjyst data! är ett forsknings- och innovationsprojekt kring dataskydd och integritet. Användardata är hårdvaluta på den digitala marknaden och används i många sammanhang; allt från olika tillämpningar, appar, media, reklam och marknadsundersökningar till samhällsfunktioner som trafikövervakning, säkerhet och trygghet. Här finns stora affärsmöjligheter för företag som använder data på rätt sätt och samtidigt förbättrade tjänster och tydliga fördelar för den enskilde individen. 2016 antog EU en ny dataskyddsförordning, GDPR, som trädde i kraft i maj 2018 och ersatte dåvarande personuppgifts-lagstiftning i medlemsländerna (PUL i Sverige). Projektets hypotes har varit att användardata ska kunna utnyttjas bättre, ur flera parters perspektiv, även med ny lagstiftning på plats. En möjlighet som projektet har utrett är om det finns förutsättningar för att skapa en *integritetscertifiering* (eller liknande) för digitala tjänster. Projektet har haft som ambition att bidra till en konstruktiv affärsutveckling för avsändare av olika digitala tjänster baserade på användardata som främjar tillit utifrån juridiska, etiska och affärsmässiga krav. Förhoppningen är att även kunna bidra till att skapa ett ökat förtroende hos konsumenter gentemot avsändaren av en tjänst. De målgrupper som vi primärt riktat oss till är företag, branschorganisationer, vetenskapssamhälle och konsumenter.

Parter i projektet har varit **RISE** (projektledning), **Lunds universitet, Malmö universitet, Södertörns högskola, SEB, Kantar Sifo, IAB, Kantar Audit** (f.d. TS Mediefakta), **Urban ICT Arena, Bumbee Labs, Sandvine** och **Öresundskraft.**

Läs mer på www.sjystdata.se

Innehållsförteckning

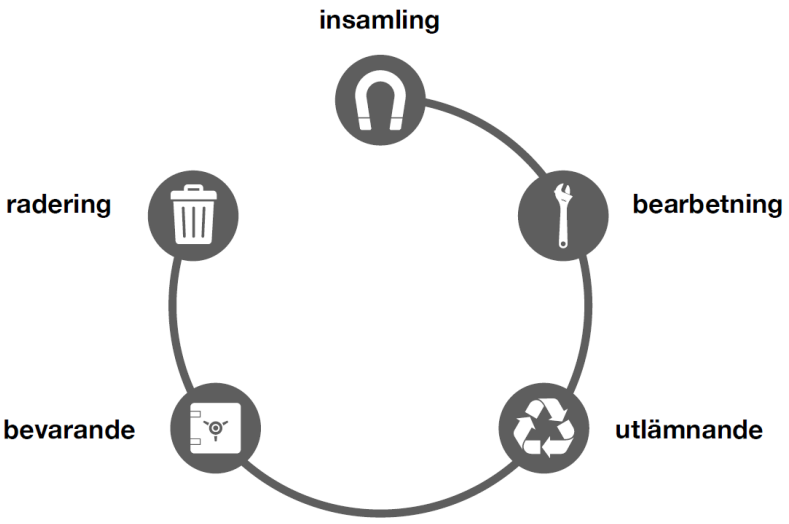
Projektets mål, genomförande och kommunikation

Ambitionen och det övergripande målet med projektet har varit att undersöka behov (användares såväl som organisationers) och identifiera mekanismer som skulle kunna underlätta ett bättre nyttjande av digitalisering och användardata samtidigt som man upprätthåller förtroendet och en god relation till kunderna (användarna). Projektet svarar direkt på EU-kommissionens identifierade utmaningar om att tillgång till, kunskap kring, samt ansvarsfull användning av persondata, är avgörande för tillväxt och europeisk konkurrenskraft. Projektet vill också bidra till att minska osäkerheten kring det juridiska läget som kommersiella aktörer känner inför nyttjandet av användardata.

Projektet har adresserat ett mycket komplext och brett område, och vi valde att dela upp det i några olika arbetspaket, med olika angreppssätt, samt ett antal piloter:

- Vägledning, riktlinjer och utvärderingsmetodik med avseende på juridiska aspekter
- Förutsättningarna för en integritetsbaserad märkning/certifiering
- Påverkan på affärsmodeller och tjänsteutveckling
- Piloter (i huvudsak olika typer av undersökningar och utvecklingsaktiviteter av ett urval av projektparter)

Samverkan mellan olika projektparter har skett såväl bilateralt som i gemensamma kvartalsvisa heldagsmöten (med samtliga projektparter), under den dryga tvååriga projekttiden, med olika teman i fokus och workshops av olika slag. För att ha ett gemensamt ramverk och språk utarbetade vi bl.a. en struktur som vi valde att kalla ”dataskyddslivscykeln”, som på ett generiskt sätt beskriver de olika situationer som är möjliga vid behandlingar av persondata. Vi använde sedan denna struktur vid ett flertal olika workshops (där samtliga projektparter deltog) som ett sätt att bryta ner olika utmaningar och frågeställningar.



Figur 1: Dataskyddslivscykeln.

Förutom de kunskaper och insikter som successivt byggts upp hos respektive projektpart under projekttiden så har vi även kommunicerat vissa delar till en extern publik. Vi har även involverat experter utifrån som deltagit i vissa av våra projektmöten för att sprida kunskap och inspirera.

De externt riktade kommunikationsaktiviteterna har understötts av en kommunikationsplan som väglett arbetet. Syftet med den externa kommunikationen har varit att löpande förmedla projektets resultat och förvärvade insikter. De främsta digitala kanalerna har varit hemsidan www.sjystdata.se, ett återkommande nyhetsbrev och i viss utsträckning respektive deltagande organisations hemsidor. Dessutom har projektet varit representerat vid olika konferenser, seminarier och bransch-dagar. I samband med publiceringen av t ex skriften *Vägledning om dataskydd: God integritet vid digital tjänste- och affärsutveckling* och några av de undersökningar som har utförts och sammanfattats i rapporter, har vi kommunicerat i olika kanaler. T ex producerade vi en kort film kring projektet och *Vägledningen* (finns här: www.youtube.com/watch?v=xeK64Tvg-Ug&t=12s).

Projektdeltagare har även deltagit i ett flertal olika externa seminarier, där vi utbytt erfarenheter och kunskap inom dataskyddsområdet. T ex deltog Ester Appelgren, forskare från Södertörns högskola i en paneldebatt på tankesmedjan *Fores*. Temat för samtalet var den kvantifierade konsumenten och debatten handlade främst om förberedelserna inför GDPR och Konsumentverkets roll i förhållande till medborgarnas medvetenhet i frågorna kring integritet i digitala sammanhang. Från projektet har också Jonas Ledendal, jurist och dataskyddsforskare från Lunds universitet, deltagit i ett flertal öppna seminarier och där spridit en del av de resultat, insikter och slutsatser som framkommit under projektets gång. Sara Leckner, medieforskare från Malmö universitet, deltog 2019 i NordMedia-konferensen redogjorde för en av undersökningarna som projektet genomfört. Projektet har också medverkat i RISE seminarier i Almedalen samt på Legal Design Geek-konferensen i London.

Dessutom har ett flertal projektdeltagare skrivit debattartiklar som publicerats i massmedia, t ex i Sydsvenskan och i Dagens Samhälle, liksom vetenskapliga artiklar och antologier (t ex SOM-institutets *Sprickor i fasaden* av Sara Leckner).

Projektet har tagit i beaktande de jämställdhetsmål som man satte upp i ansökan till Vinnova, och i stora drag har könsfördelningen i projektet varit relativt jämnt fördelad mellan kvinnor och män. Jämställdhetsaspekter har också tagits i beaktande vad gäller genomförande och analys av de olika attitydundersökningarna.

Utveckling i omvärlden

Under projektperioden, juni 2017 till november 2019, har vi kunnat bevittna stora skeenden och förändringar inom persondataområdet, såväl nationellt som internationellt. Balansgången har varit viktig men har ibland tippat över åt fel håll: värdet och nyttan för användaren av digitaliserade tjänster gentemot riskerna och hoten; innovation, intäkter och affärsnytta för företagen (avsändarna av digitala tjänster) gentemot upprätthållande av god sed och integritet.

Internetstiftelsens årliga undersökning *Svenskarna och Internet* konstaterade i oktober 2019 att svenskarnas oro för hur deras persondata på nätet hanteras (eller missbrukas) av privata företag har ökat fem år i rad, ett mönster som vi även sett i undersökningar där vi från Sjyst data!-projektet har deltagit, t ex den årliga *SOM-undersökningen* och i undersökningen *Delade Meningar*. EU:s nya dataskyddsförordning GDPR infördes i maj 2018, och fick därmed stor påverkan på såväl ekosystem, aktörer, tjänster och i slutändan även på funktioner, processer och beteenden, men även en hel del nya insikter genererades och fenomen synliggjordes inom t ex sociala medier och missbruk av persondata.

Nedan är ett axplock av de händelser eller milstolpar i omvärlden som vi noterat, diskuterat och analyserat under projektets gång, ofta i samband med att vi har haft gemensamma projektmöten eller i våra nyhetsbrev. Det har varit viktigt för projektet att följa utvecklingen i omvärlden, i och med att nya fenomen, insikter, riktlinjer och *best practices* har kommit att påverka inriktningen av de undersökningar och arbete som projektet genomfört.

- Det började med en ökande mediabevakning under våren 2018 som lyfte fram en del händelser där persondata från sociala medier utnyttjats i syften som de flesta användare inte var medvetna om. Den s k Cambridge Analytica-skandalen avslöjade spridningen av miljontals Facebook-användares personliga information för politiska syften, utan användarnas vetskap, vilket bl a väckte frågor om nätjättarnas ansvar. Många användare/konsumenter fick då upp ögonen för denna typ av missbruk och även andra ”trollfenomen”. Digitaliseringen och sociala medier har också synliggjort vissa fenomen, t ex inom opinonspåverkan, på ett mer påtagligt och vardagsnära sätt än vad tidigare har varit möjligt. Men frågan kvarstår om skandalen kom att förändra någonting i grunden? Politiker, företag och användare har inte till fullo insett att de måste hjälpas åt i arbetet med att utveckla verkligt *hållbara* digitala tjänster. Dataskyddsförordningen GDPR väckte både förhoppningar och farhågor – läs t ex ett inlägg om detta från projektdeltagaren Sara Leckners debattartikel i *Dagens Samhälle* (www.dagenssamhalle.se/debatt/vi-bar-alla-ansvar-cambridge-analytica-skandalen-21641).

  I samband med dessa nyheter genomförde projektet en enkätundersökning med hjälp av projektpart Kantar Sifo (läs hela rapporten *Svenskarnas attityder till integritet och politisk opinionsbildning på nätet och i sociala medier* på www.sjystdata.se) i samband med det svenska riksdagsvalet i september 2018, och även andra organisationer undersökte dessa frågeställningar, t ex rapporten från Internetstiftelsen, *Svenskarna och internet: Valspecial 2018* (läs mer på: val2018.svenskarnaochinternet.se)

- Idag kan vi konstatera att ”trollfenomen” och subversiv påverkan via sociala medier inte har försvunnit och annonsering och marknadsföring via dessa plattformar är fortfarande omfattande. Men vi kan också se att nätjättarna har påverkats av mediebevakningen och av konsumenternas ökade medvetenhet och agerande och de har därmed ändrat en hel del i sina tjänster och infört skyddsmekanismer för att minska risken för att detta ska hända igen på ett otillbörligt sätt. T ex har Facebook och Instagram stramat åt reglerna kring politiska annonser inför kommande amerikanska valkampanjer. Man har infört en "bekräftad organisation"-märkning, via vilken politiska annonsörer måste bevisa sin legitimitet för att få annonsera på plattformarna. Alla annonsörer som vill göra reklam om politiska eller sociala frågor måste också publicera sin kontaktinformation. Man har också ökat transparensen och infört bättre möjligheter för den enskilde användaren att välja olika funktioner (i t ex appar), beroende på attityd och önskemål. Twitter och Tik Tok har nyligen (okt/nov 2019) helt stoppat politisk annonsering på sina plattformar.

- Nätjättarnas allt större och viktigare roll i vårt samhälle och det stora ansvar de bär på sina axlar har också debatterats allt livligare under de senaste åren, inte utan effekt. Ny lagstiftning såsom GDPR har också naturligtvis haft en stor inverkan på nätjättarnas agerande, inte minst inom EU. Innan GDPR infördes i maj 2018 visade t ex en studie att Facebook kartlade 73 procent av EU-användarna med intressen kopplade till känsliga personuppgifter. Det innebar att Facebook sparade uppgifter om ca 200 miljoner européer som kunde användas av tredje part för att styra t ex annonsering.

  I samband med införandet av GDPR tvingades många av dessa aktörer (och andra) att justera användarvillkor, samtycken, transparens, annonseringsmekanismer, kontroll av användardata, ansiktsigenkänning etc., något som många av oss användare inte undgick att notera. Dock upplevde många att antalet popup-rutor och samtycken ökade lavinartat efter att GDPR införts, vilket inte var syftet med detta, och dessa samtycken kvarstår än idag i en omfattning och på ett störande sätt som inte är optimalt eller ens nödvändigt i många fall.

  Projektdeltagaren Jonas Ledendal, Lunds universitet, skrev en debattartikel i Sydsvenskan den 21/5 2018 om vikten att verkligen förstå GDPR och att agera på ett konstruktivt sätt, inte bara se dataskyddsförordningen som ett hinder: ”Om GDPR får negativa konsekvenser beror det delvis på att näringslivet inte utnyttjar den inbyggda flexibilitet som finns i förordningen. Företag bör, på samma sätt som de idag arbetar med hållbarhet, strategiskt använda god integritet för att öka kundernas tillit och differentiera sina produkter. För att konkurrera med nätjättarna måste svenska företag inte bara inrikta sig på att följa GDPR utan satsa på att bli bättre på integritet.”

- Vi har det senaste året sett ett flertal av leverantörerna av digitala tjänster bättre anpassa sig till GDPR, stärka närvaron inom EU och öka satsningarna på integritetsfrämjande teknik (t ex Facebook, Google och Apple). Men samtidigt har vi också sett ett antal internationella bolag, stora som små, begränsa eller helt dra tillbaka sina tjänster från EU p g a utmaningarna och

kostnaderna förknippade med GDPR och i värsta fall risken att råka ut för vite.

- Efter GDPR:s införande så har mediegranskningen fortsatt av hur företag hanterar vår persondata, t ex granskade Dagens Nyheter (med hjälp av datasäkerhetsexperten Sam Jadali) under våren 2019 hur ett stort antal mindre företag samlar på sig användarnas positions- och surfdata (via mobilappar och plugins i webbläsarna) och säljer denna vidare till godtyckliga kunder, ofta utan användarnas vetskap (se t ex www.dn.se/din-plats-till-salu/ och www.dn.se/nyheter/sverige/svenskars-surfhistorik-avlyssnades/).

  Samtidigt samlas in och anonymiseras alltmer data via smartphones, IoT-sensorer etc. för att tillhandahålla nya verktyg att mäta och styra i ”det smarta samhället”. Många offentliga aktörer ser här möjligheterna med egna (slutna), delade och öppna data för att optimera, effektivisera och förbättra olika flöden och processer runt om i vårt samhälle. Det finns också sammanhang där lagstiftningen idag inte medger viss funktionalitet som kan vara efterfrågad av en majoritet, ett exempel är SOS Alarm som gärna skulle se en mer exakt positionering (s k AML-teknik, *Advanced Mobile Location*) av någon som ringer 112, men där LEK idag sätter stopp. Däremot är det få stater som har tagit det så långt när det gäller persondata som man har gjort i Kina med det s k ”sociala kreditsystemet” och som utnyttjas av såväl staten som kommersiella aktörer, på ett sätt som sannolikt skulle upplevas som integritetskränkande i andra stater och kulturer.

- Inom EU har nu den Europeiska dataskyddsstyrelsen (EDPB) inrättats (se https://edpb.europa.eu). EDPB är ett nytt självständigt EU-organ med helt nya befogenheter och utgörs av tillsyns-myndigheter inom hela EU. Styrelsen kan bl.a. fatta bindande beslut genom enkel majoritet i tvister om hur GDPR ska tillämpas i ett konkret tillsynsärende. EDPB ska inte förväxlas med *Europeiska datatillsynsmannen,* som är EU:s tillsynsmyndighet (motsvarar alltså Datainspektionen i Sverige). EDPB ersätter *Artikel 29-gruppen* (WP29) och ett av deras första beslut var att erkänna ett stort antal av arbetsgruppens tidigare utfärdade riktlinjer (https://edpb.europa.eu/node/89). Det innebär att vi kan räkna med fortsatt kontinuitet vad gäller tolkning och tillämpning av reglerna. De nordiska dataskyddsmyndigheterna fortsätter också sitt nära samarbete (läs mer på www.datainspektionen.se/nyheter/nordiska-dataskyddsmyndigheter-fortsatter-sitt-nara-samarbete/)

- Vad gäller tillsynen efter att GDPR införts har ett antal ärenden och granskningar påbörjats i samtliga EU-medlemsstater. Såväl privata aktörer som offentliga har granskats, inklusive fackförbund, och ett antal anmälningar av olika dignitet har inkommit till de olika tillsynsmyndigheterna, i Sveriges fall till Datainspektionen. Enligt en bedömning från EDPB så rapporterades närmare bestämt 206 326 ärenden under de nio första månaderna efter GDPR:s införande. Omkring 65 000 av de här fallen initierades av en personuppgiftsansvarig eller personuppgifts-biträde och ungefär 95 000 var klagomål. 52 procent av fallen har redan stängts och i en procent av ärendena väntar prövning i domstol. Totalt utdelades viten under denna period om ca 600 MSEK, varav det enskilt största utdelade till Google i Frankrike p g a bristande

transparens och tydlighet när det gäller att informera användarna.

I januari inledde Datainspektionen en granskning av Google efter att ha tagit emot ett klagomål från konsumentorganisationen *Sveriges Konsumenter.* Klagomålet handlade om hur Google samlar in och använder platsdata från svenska användare av Android-telefoner. En kort tid därefter meddelade Google att deras huvudsakliga verksamhetsställe för delar av deras verksamhet är Irland och att det därmed blir den irländska dataskyddsmyndigheten som bör ansvara för tillsynen, ej den svenska Datainspektionen. I Sverige utfärdade Datainspektionen i augusti 2019 det första vitet (200 kSEK) till en skola i Skellefteå som på prov har använt ansiktsigenkänning via kamera för att registrera elevers närvaro.

- Datainspektionen har också löpande tagit fram olika riktlinjer, utbildande information, mallar och verktyg för att underlätta dataskyddsarbetet för organisationer, t ex vad gäller *konsekvensbedömningar*, kopplingen mellan *olika lagrum* (t ex mellan GDPR och ePrivacy), riktlinjer för *kamerabevakning*, definitioner och förtydliganden av rollerna *personuppgiftsansvarig* och *personuppgiftsbiträde* m. m. Läs mer på www.datainspektionen.se

Reflektioner, slutsatser och rekommendationer

GDPR – hinder eller möjlighet i den datadrivna ekonomin?

Den datadrivna ekonomin är en hörnsten i EU:s strategi för en digital inre marknad. För att 28 nationella marknader ska bli en enda krävs nya regelverk som undanröjer hinder för den fria rörligheten. Vid sidan av de fyra klassiska friheterna talas det numera även om en femte frihet, den *fria rörligheten för data*. Stora datamängder av hög kvalitet är avgörande för landvinningar inom områden som *big data analytics* och artificiell intelligens (AI). För att förverkliga den fulla potentialen i dataekonomin har EU de senaste åren föreslagit eller redan antagit flera nya lagar om tillgång till data och det fria flödet av data i unionen. Exempelvis ett nytt direktiv om öppna data från offentlig förvaltning (PSI-direktivet) och en ny förordning om det fria flödet av andra data än personuppgifter.

För att den digitala inre marknaden ska fungera behövs emellertid också tillit till att företag och myndigheter hanterar personliga data på ett ansvarsfullt sätt. För att personuppgifter ska kunna flöda fritt krävs en hög nivå av enhetlig skydd i alla medlemsstater. Det är därför EU antog den allmänna dataskyddsförordning (GDPR), som blev tillämplig den 25 maj 2018 och har ersatt de gemensamma dataskyddsregler som gällt sedan 1995. Projektet *Sjyst data!* handlar om hur potentialen i den datadrivna ekonomin ska kunna förverkligas på ett sätt som uppfyller dessa nya krav och skapar tillit hos kunder och andra användare så att dessa kan känna sig trygga med att dela med sig av sin data.

I projektet har vi kunnat studera genomförandet av dessa nya bestämmelser, både förberedelserna fram till den 25 maj och den fortsatta utvecklingen. Dessa erfarenheter har vi sammanställt i den *vägledning* som publiceras som ett separat dokument, ny uppdaterad version i november 2019 (du hittar den på www.sjystdata.se). Nedan följer några nyckelslutsatser från denna:

- Det finns många missuppfattningar om vad GDPR egentligen kräver, bl.a. att det numera skulle vara helt förbjudet att behandla personuppgifter. Om organisationer saknar tillräcklig kompetens om dataskydd finns det en risk att skyddet blir bristfälligt, men det finns också en inte alltid uppmärksammad risk för att företag och myndigheter avstår från att utveckla nya och förbättra digitala tjänster trots att det inte varit lagstiftarens syfte.
- En annan vanlig missuppfattning är att det alltid krävs samtycke för behandling av personuppgifter. Det saknas kunskap om att samtycke endast är en av flera rättsliga grunder för behandling. Samtycke är heller inte alltid en lämplig grund. Det är också lätt att underskatta vad som faktiskt krävs för ett juridiskt giltigt samtycke.
- Transparens är viktigt för att bygga tillit, men även här kan genomförandet av GDPR förbättras. Företag och andra organisationer har lagt ner förhållandevis stora resurser på att ta fram en ny mer heltäckande integritetspolicy och att skicka ut e-post till sina kunder och användare, men det kan ifrågasättas om detta har fått den effekt som lagstiftaren hade tänkt sig. Det finns också ett stort utrymme att använda *legal design*-metodik för att förbättra genomförandet (se avsnittet nedan i detta kapitel om *legal design*).

- Kunskapen och medvetenheten om de nya dataskyddsreglerna har blivit bättre, men behöver fortfarande höjas i de flesta organisationer. Kunskap om dataskydd finns inte sällan hos en liten grupp av specialister, ibland nästan uteslutande hos organisationens dataskyddsombud (DPO).

Effekter och påverkan på affärsmodeller och tjänsteutveckling

Digitala tjänster använder vi dagligen i en mängd olika sammanhang, och vi har som individer och användare vant oss vid hur sofistikerade och ”smarta” dessa tjänster har blivit med åren. Vi får en stor mängd funktioner, nyttor och andra värden till oss via de digitala kanalerna, ofta utan att vi behöver betala alltför höga avgifter (om ens några), t ex prenumeration av olika tjänster med tillhörande appar. Innovationen inom affärsmodelleringen för att åstadkomma dessa (ofta marknadsföringsbaserade) modeller har varit febril och när kritik har uppstått har många aktörer varit snabbfotade att anpassa funktionalitet eller affärsmodell, om så krävts. Men ny lagstiftning har också satt käppar i hjulet för vissa aktörer och deras befintliga affärsmodeller, och i vissa fall kan detta ha tvingat ut dem eller deras tjänster ur marknaden eller försvagat deras tidigare position. Ibland kan detta ha varit befogat, ur ett konsumentperspektiv, men i vissa fall har lagstiftningen givit effekter som inte varit avsiktliga (t ex att ett antal skolor har lagt ner den sedvanliga skolfotograferingen p g a rädsla att bryta mot GDPR).

Projektets resultat från olika typer av attitydundersökningar visar att majoriteten av svenskarna tänker på att de delar med sig av sin användardata (persondata) med olika internetaktörer (lämnar digitala spår etc.). Majoriteten anser sig dock inte ha något val, vilket kan vara en anledning till att de flesta ställer sig negativa till att dela användardata när de tillfrågas, i synnerhet från kommersiella aktörer. Antalet negativa har också ökat under senare år, snarare än minskat. Detta är naturligtvis problematiskt, då det finns enorm potential för affärsmodeller och förbättrade (eller helt nya) tillämpningar baserade på användargenererade data. Samtidigt visar resultaten att villigheten att dela data beror till viss del på vad man delar. Ju mindre ”personliga” data är, desto mindre negativ är man, samtidigt som det är just de kommersiella företagen som svenskarna är mest negativa att dela med sig till. Men resultaten visar också att ökad kunskap om datadelning ökar villigheten att dela vissa data. Det är alltså av stor vikt att öka kunskapen hos användarna, genom ökad, men lättillgänglig, information och öka transparensen kring hur delning och användning av data faktiskt sker, liksom syftet med delningen.

Uppenbart är att många företag har blivit försiktigare i sin kommersiella verksamhet och vad gäller utformningen av tjänster, tack vare GDPR och en ökad medvetenhet och skepsis bland användarna.

Kunskap, information och transparens

Ambitionen i projektet har varit att bidra till att kunskapsnivån höjs inom ett antal områden såsom juridik, affärsmodeller, tjänsteutveckling, märkning, certifiering, uppförandekoder och slutanvändarkunskap. Vi har kommit en bit på vägen i denna komplexa och mångfasetterade värld, men vill fortsätta att verka för att ytterligare steg tas och verktyg och stöd tas fram, något som vi hoppas kunna göra i ett nästa steg.

Det finns dock målgrupper som redan har mer kunskap än andra, och som vi observerat (i våra undersökningar) därmed är villigare att dela data redan idag, exempelvis unga, högutbildade, och frekventa internetanvändare. Dessa grupper är också de som i större utsträckning anser sig utsatts för

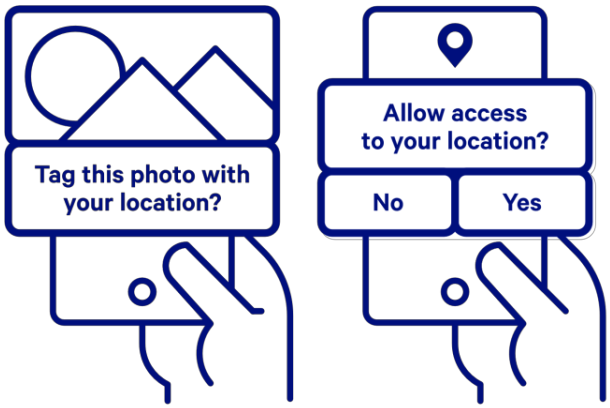
integritetsintrång i större omfattning, sannolikt på grund av kombinationen av ett mer frekvent användande och en högre medvetenhet.

Resultatet från projektet har också visat att den information som finns idag (från avsändarna av en tjänst) är bristfällig och svårtillgänglig, samt att utformning av t ex samtycken och användarvillkor långt ifrån är optimal och användarvänlig. Det är idag färre än hälften av svenskarna som läser användarvillkor, en *sänkning* sedan GDPR infördes. Kunskapsnivån om vad datadelning innebär *i praktiken* ligger också på i stort sett samma nivå som innan GDPR infördes, liksom kunskapen om hur (och om) man skyddar sina data eller inte. Däremot visar projektet att det finns en indikation på att svenskar har blivit *mer medvetna* och anser sig kunna detektera desinformation på nätet i högre utsträckning än tidigare.

Legal design

Tidigt under diskussionerna kring en potentiell certifiering (eller märkning) lyftes frågan hur man på bästa sätt kan stödja företag och organisationer att nå upp till kraven som en certifiering ställer, och då på en väldigt konkret och nära nivå som går att implementera direkt in i verksamheten eller den specifika tjänst som erbjuds.

En möjlig lösning för detta skulle vara att använda sig av s k *designmönster*, vilket är ett strukturerat sätt att beskriva "best practices", förklara god design och fånga upp erfarenheter på ett återanvändbart sätt. Strukturen innehåller en beskrivning av problemet, den föreslagna lösningen och exempel på en konkret implementation. Det finns redan idag en del exempel på designmönster för hantering och insamling av data, till exempel *Data Permissions Catalogue* (https://catalogue.projectsbyif.com), och ytterligare en samling med goda exempel hittar man här: http://ui-patterns.com/patterns.



Figur 2: Exempel på hur ett samtycke kan utformas (från Data Permissions Catalogue)

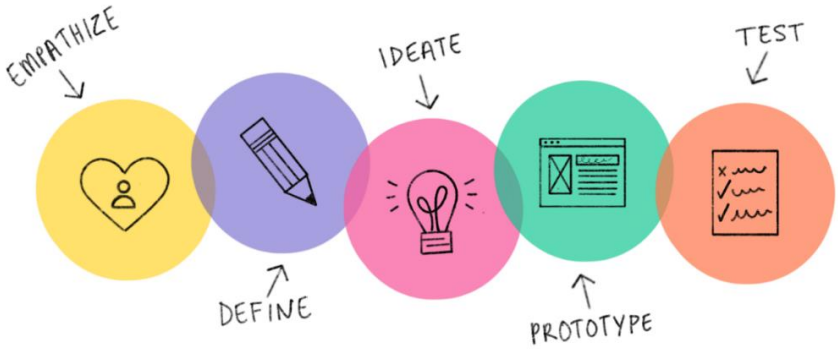
T ex kan designmönster användas i följande syften:

- Identifiera ”best practices” och vanliga sätt att lösa problem
- Samla kollektivt kunnande
- Skapa ett gemensamt språk och sätt att beskriva, undviker missförstånd
- Reducera tid och kostnad i designprocessen
- Göra att de bästa lösningarna också är de enklaste och snabbaste
- Ge konsekvent och förutsägbar design

Designmönster av denna typen är en del av ett nytt framväxande område som kallas *legal design*. Legal design är en kombination av människocentrerad design / designtänkande och juridik, med syftet att göra juridiska system och tjänster mer anpassade till människor, mer användbara, enklare, mer intuitiva, mer tillfredsställande och engagerande att använda. Utgångspunkten är de problem, utmaningar, möjligheter och begränsningar som juridiken på olika sätt skapar, i sig själv eller vid utveckling av olika sorters tjänster. Legal design riktar sig både till juridiska experter, för att kunna förändra och förbättra utformningen av det juridiska systemet, och till lekmän, för att underlätta förståelsen och användningen av samma system.

Ett exempel är GDPR:s krav att ett integritetsmeddelande (eng. privacy notice) ska vara skrivet på ett kortfattat, transparent, begripligt och lättillgängligt sätt. Hur man tar sig an detta krav och uppfyller det liknar snarast en designutmaning än en juridisk utmaning.

Detta designperspektiv testades inom projektet (bl a i workshop-format), med en metod från Legal Design Lab (http://www.legaltechdesign.com/) som tar avstamp i designtänkande (eng. design thinking), ett etablerat arbetssätt:



Figur 3: Exempel på en typisk design-process

1. Nulägesbeskrivning, utgående från vad som funkar bra och vad som funkar dåligt, både i nutid och i framtiden
2. Fokus på en individ, från det generella till det specifika. Definiera en fiktiv person (persona), vem det är som vi faktiskt pratar om
3. Omformulera utmaningen, formulera specifika problem baserat på personen
4. Brainstorm, välj ut två specifika problem och hitta lösningar som bygger på nya produkter, tjänster respektive policies
5. Prioritera idéerna från brainstorming-övningen
6. ”Prototypa”, på ett sätt som gör att idén kan testas på bästa sätt, fokus på hur idén kommuniceras på bästa sätt
7. Testa idén, för att få kritisk feedback på ett tidigt stadium

Utgångspunkten för våra workshops på området var respektive deltagares egen verksamhet, men huvudsyftet var att testa metoden och detta sätt att arbeta med projektets frågeställningar i en designworkshop-form.

Legal design, med allt som ryms inom detta vida begrepp, är en lovande väg framåt i arbetet med ett alltmer komplicerat juridiskt landskap. I fallet med dataskydd och GDPR finns det många utmaningar som olika aktörer ställs inför, och för att lösa dessa på ett sätt som inte bara uppfyller lagens krav, utan även individens behov, önskningar och krav, behövs det ett större helhetsperspektiv, och där kan designvetenskaperna bidra. Men för att kunna göra detta behövs det mer utveckling, de initiativ som finns idag (exempelvis designmönster och designmetoder) är fortfarande preliminära och ej utvecklade till sin fulla potential.

Ytterligare en intressant blogg att följa inom det framväxande området *legal design*:
http://www.openlawlab.com/

Förutsättningar för en integritetscertifiering (eller märkning)

Syfte med en märkning/certifiering

I och med stora osäkerheter och brist på kunskap hos användarna samt en bristande transparens och insyn i hur många digitala tjänster fungerar, så finns det ett tydligt behov av att vägleda konsumenterna i sina val och användande av digitala tjänster, i likhet med de konsumentvägledningar som finns för t ex livsmedel *(Krav, Svanen etc.)* och e-handel *(Trygg e-handel)*.

Figur 4: En märkning/certifiering bör adressera mer än bara de juridiska kraven för att god sed skall uppnås.

Syftet med en sådan dataskyddsrelaterad märkning/certifiering är att skapa transparens och kvalitetssäkring i form av en kvalitetsstämpel för digitala tjänster och produkter som vill visa på *god integritet.* Stämpeln ska visa på laguppfyllnad i enlighet med exempelvis GDPR, ePrivacy/LEK och andra på området relaterade uppförandekoder.

Certifieringens mål är att vara standarden på marknaden, för bolag som vill visa på att deras tjänster och produkter som hanterar personuppgifter följer ett ramverk bestående av god sed och lagar. Man vill också kunna visa på transparens då tredje part granskar rutiner för hantering av data för ett bolags produkter och tjänster. Till syvende och sist skall en märkning/certifiering bidra till att driva en sund och hållbar affärsutveckling av produkter och tjänster som gynnar såväl avsändare som mottagare.

Ett ”Sjyst data!”-sigill (eller motsvarande) kopplat till certifieringen ska kunna erbjuda flera olika sätt att visa upp att företagets produkter och tjänster erbjuder en etisk, trygg och stabil hantering av data samt att man upprätthåller en god sed och integritet mot eventuella affärspartners, men även i kommunikationen med konsumenter. En hypotes som framkommit i projektet är att ha *differentierade* sigill, exempelvis kopplade till komplexitet, omfattning och specialområden/branscher, att diskutera vidare i ett eventuellt nästa steg för själva utformningen av certifieringen.

Kort utblick

I projektet har vi hämtat inspiration från ett antal certifieringar, standards och märkningar som får anses vara etablerade på marknaden. Vi valde att titta närmare på exempelvis märkningar som *Trygg eHandel, Kravmärkt, Svanen-märkningen, Svalan* och *Bra Miljöval*, men också olika *ISO-standarder* inom ”risk management” som går att hämta inspiration från (t ex ISO 31000:2018 Risk management – Principles and guidelines: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en och ISO/IEC 29134 Privacy impact assessment – Guidelines: https://www.iso.org/obp/ui/#iso:std:62289:en)

Datatilsynet, den danska motsvarigheten till Datainspektionen har utarbetat riktlinjer för certifiering och uppförandekoder *(Vejledning om adfærdskodekser og certificeringsordninger)*: www.datatilsynet.dk/nyheder/nyhed/artikel/vejledning-om-adfaerdskodekser-og-certificeringsordninger/

För vem?

Vilka är då intressenterna? Alla företag och organisationer som jobbar med en digital affärs- och tjänsteutveckling som baseras på hantering av persondata är den *primära målgruppen* för ackreditering och märkning/certifiering. Märkningen ökar förhoppningsvis trovärdigheten för bolagets sätt att hantera persondata.

Kommunikativt riktar sig märkningen/certifieringen till allmänheten och den enskilde konsumenten och har till syfte är att vara ett viktigt verktyg i kommunikationen med konsumenten, då hanteringen av data ofta är både komplext, svårbegripligt och svårt att kommunicera tydligt kring.

Behovet och vem gynnar det?

God integritet handlar om att skapa tillit så att slutanvändare kan känna sig trygga med att dela med sig av data som är nödvändig för att utveckla eller förbättra tjänster och produkter som behövs i en digital ekonomi och ett hållbart samhälle. Det handlar också om att företag/organisationer ska ha en ”kompass” att förhålla sig till gällande hur man hanterar persondata.

Hur kan det gå till?

Bolaget i fråga väljer inför certifieringsprocessen vilka tjänster/produkter som skall certifieras. För mindre bolag kan det avse alla bolagets produkter/tjänster men för större bolag behövs sannolikt en avgränsning. Hypotesen är att själva granskningen och certifieringen görs av utvecklingsprocessen för en tjänst/produkt, eftersom digitala tjänster/produkter har en tendens att ändras och utvecklas ofta, vilket i så fall skulle kräva en ny certifiering vid varje sådant tillfälle. Certifieringsprocessen bygger på att utsedda organ kan utföra själva ackrediteringen utifrån ett uppsatt regelverk.

En certifiering kan vara såväl godkänd som icke godkänd, där det förstnämnda ställer högre krav på utformning och kräver ett ackrediterat certifieringsorgan.

Regel- & referensgrupp

Inför en fastställd kommersialisering av denna märkning/certifiering behövs en regelgrupp tillsättas som ansvarar för att ett regelverk och en process kommer på plats. Regelverket styr hur certifieringen ska se ut i detalj och vilka valideringar och kontroller som behöver genomföras.

Vid sidan av regelgruppen behövs en referensgrupp som supporterar med att säkra en utveckling av ackrediteringsreglerna och tillämpningsföreskrifter.

När det finns en regelgrupp och ett regelverk bör ett pilotprojekt genomförs som en del i utvärderingsfasen. I denna fas behöver också beslut fattas gällande avsändare/ägare av denna tjänst.

Finansiering
För att bli certifierade behöver företaget/organisationen i fråga betala någon form av avgift. Storleken på avgiften behöver preciseras utifrån det regelverk och organisation som den tilltänkta certifieringen till slut utmynnar i. Viktigt att storleken på avgiften är rimlig, varken för hög eller för låg samt i proportion till andra liknande certifieringar. Certifieringen bör genomföras löpande, förslagsvis en gång per år för varje certifierad tjänst eller process.

Nästa steg
Certifieringsmodellen behöver finna former i form av precisering och avgränsning. Vilka områden och processer för produkter och tjänster ska kunna omfattas? Ska hela företag/organisationer kunna inkluderas? Ska certifieringen vara branschneutral eller branschspecifik?

Ett eller flera test-fall behöver sättas upp och genomföras innan kommersialisering, regelgrupp och pilotstudie sker i utvärderingsfasen.

Uppförandekoder

GDPR ger ett visst utrymme för självreglering via godkända uppförandekoder och certifiering *(se artikel 40-43 i GDPR).* Vad är då skillnaden mellan uppförandekod och certifiering/märkning? En uppförandekod utfärdas branschvis och specificerar tillämpningen av exempelvis GDPR, medan en certifiering/märkning kan användas för att visa förenlighet med GDPR i allmänhet. En uppförandekod bidrar till att t ex GDPR genomförs och efterlevs korrekt, med hänsyn till särdragen hos de olika sektorer där behandling sker, och de särskilda behoven hos mikroföretag samt små och medelstora företag. Sammanslutningar och andra organ som företräder kategorier av personuppgiftsansvariga eller personuppgiftsbiträden får utfärda uppförandekoder, ändra eller utöka sådana koder. En uppförandekod bör omfatta materiella krav för behandling av personuppgifter. När man utfärdar en (nationell) uppförandekod kring GDPR, genomförs följande steg:

1. Utkast (eller ändring) lämnas till behörig tillsynsmyndighet (Datainspektionen)
2. Myndigheten yttrar sig om utkastet eller ändringen överensstämmer med GDPR

3. Myndigheten godkänner utkastet eller ändringen om myndigheten finner att tillräckliga garantier tillhandahålls
4. Registrera och offentliggöra uppförandekoden

En uppförandekod måste också, likt en certifiering/märkning, innehålla mekanismer för övervakning av efterlevnad. Ett övervakningsorgan ska ackrediteras av behörig tillsynsmyndighet och

- visa oberoende och expertis i förhållande till kodens syfte
- visa frånvaro av intressekonflikt
- upprätta förfaranden för att utvärdera efterlevnad och mekanismer för övervakning
- upprätta mekanismer för att hantera klagomål från registrerade
- ackreditering kan återkallas av tillsynsmyndigheten

Projektet har också identifierat möjligheten med att bidra till god sed inom dataskydd via arbete med uppförandekoder, som då görs branschvis.

Attityd- och enkätundersökningar

Projektet har själv genomfört och deltagit i ett antal olika attityd-undersökningar. Syftet med dessa undersökningar har varierat, men alla med målet att öka förståelsen och insikten i hur individer ställer sig till datadelning och integritet, eller hur de ser på olika konkreta idéer och tjänstedesigner (som vi velat testa).

Här är en kort sammanfattning av de enkätundersökningar som projektet genomfört eller deltagit i:

- *SOM-undersökningen* (deltagagande i 2018 och 2019 års SOM-institutets undersökningar; genomfördes i projektet av Malmö universitet): Longitudinell, samma frågor under två år; allmänna frågor kring datadelning och integritet.

- Tre undersökningar m h a *Sifopanelen* (genomfördes av Kantar Sifo, Malmö universitet, RISE och SEB): En undersökning av allmänna attityder kring datadelning och två temabaserade fördjupande undersökningar; Inställning till integritet och desinformation i relation till svenska riksdagsvalet 2018; Inställningar till privatekonomiska frågeställningar och datadelning (2019).

- En enkätundersökning genomfördes också i stadsmiljö om attityder till personliga data med fokus på positionsdata/lokaliseringsdata registrerade genom mobilen. Enkätundersökningen genomfördes av projektparterna Bumbee Labs, Malmö universitet, Södertörn högskola, RISE och

UICTA.

- Deltagande i den årligt återkommande attitydundersökningen *Delade Meningar* (läs mer på http://www.insightintelligence.se/delade-meningar/delade-meningar-2019/).

Piloter: Utmaningar, möjligheter och nyttor

Under projekttiden har ett antal olika piloter genomförts, ibland med flera olika projektparter deltagande i samma pilot med olika bidrag och insatser. Nedan följer kortare sammanfattningar av vad dessa piloter åstadkommit och de utmaningar, svårigheter, möjligheter och nyttor som de resulterat i.

RISE – Mätningar och analyser av internettrafik

RISE har tidigare utfört mätningar av internettrafik i samarbete med ett par lokala bredbandsnät i Sverige för att bättre förstå behov och användning av olika digitala tjänster. Mätningarna, som är anonymiserade, har gjorts på hushållsnivå. RISE har vidtagit ett flertal åtgärder för att anonymisera data och säkerställa att den förvaras på ett säkert sätt. Den trafikdata som samlats in har varit behandlad så att personuppgifter ej lagrats och denna data har därmed ej omfattats av PUL. Syftet med mätningarna har varit att skapa en databas som används för forskning inom ramen för RISE verksamhet. RISE analyserar data från databasen i forskningsprojekt för att främja förståelsen för och utvecklingen av kommunikationsinfrastruktur och digitalisering. Detta kan innebära att vi studerar användar- och trafikmönster. Att ha tillgång till data från autentiska nätverk istället för att använda simulerade trafikdata ger möjligheter att bygga en mer korrekt och vetenskaplig förståelse av det digitaliserade samhället på flera olika områden, såväl tekniska aspekter som användarmönster. Detta ger i slutändan svenska aktörer (privata eller offentliga) en bättre möjlighet att utveckla sin verksamhet och sina tjänster.

Syfte och mål med piloten

Syftet var att etablera en process och teknik för att kunna återuppta dessa trafikmätningar, samt att påbörja analysarbete m a p användarmönster i jämförelse med t ex enkät- och attitydundersökningar (vad man gör vs. vad man säger att man gör).

Genomförande och resultat

För att samla in mätdata från våra samverkande stadsnät har RISE använt hårdvara och mjukvara från projektparten Sandvine (f.d. Procera). Utrustningen installeras och kontrolleras av stadsnätet i fråga i deras IT-miljö. Stadsnätet ger sedan RISE fjärråtkomst till utrustningen och därmed åtkomst till s k *obfuskerad* (anonymiserad) data. RISE har ingen direkt åtkomst till maskinerna utan är beroende av att stadsnätet ger tillgång till maskinen via deras nätverk. RISE lagrar anonymiserade data i en databas och analyserar den inom ramen för aktuella forskningsprojekt med stadsnätets godkännande.

I och med att GDPR infördes 2018 och att även hänsyn till LEK måste tas så tvingades RISE att utvärdera och fastställa ett nytt förslag på roll- och ansvarsfördelning mellan de involverade parterna (RISE, stadsnäten och leverantören av mätutrustningen). Detta är nu under framtagande, tillsammans med övriga relevanta parter inom projektet och RISE dataskyddsombud (DPO). Utmaningen som uppstod för

RISE var att vi var tvungna att göra om processen efter att GDPR trätt i kraft, och det visade sig vara mer krävande och omfattande än vi tidigare anat. Baserat på ett antal relevanta rättsfall (senaste från sommaren 2019) så har vi nu fastställt en process och en ansvars- och rollfördelning mellan de inblandade parterna (RISE, stadsnät och leverantör), för att kunna genomföra mätningar (dock har mätningar hittills endast kunnat genomföras i liten skala, i testmiljö).

SEB – Projekt RPD Hobbit

För Skandinaviska Enskilda Banken (SEB) så är de digitala tjänsterna av en alltmer större betydelse för verksamheten och relationen med kunderna. För att ytterligare stärka denna relation vill man kunna utveckla sina tjänster och erbjuda dessa på ett mer användarvänligt och personaliserat sätt, genom att t ex nyttja och analysera användardata. Hur kan SEB fortsätta att utveckla detta arbete trots att exempelvis lagstiftning på området skärps och att attityder och beteendemönster hos användarna ändras över tid?

Syfte och mål med piloten

I samband med att GDPR skulle träda i kraft i maj 2018 drev SEB ett omfattande internt GDPR-projekt. Där undersökte vi bland annat människors inställning till hur företag hanterar deras personuppgifter och personliga data. För att uppfylla förordningens krav undersökte vi både hur vi kunde göra informationen tydlig och kundvänlig samt vilka tjänster som skulle kunna vara möjliga.

Genomförande och resultat

Projektet genomförde 138 intervjuer med personer som identifierades ligga inom ramen för SEB:s kundmålgrupp. Intervjuerna genomfördes på SEB under våren 2018 och var 15-120 minuter långa. Studien leddes av personer med metodkunskap inom kvalitativ datainsamling och analys.

Våra huvudsakliga slutsatser var att:

- I varje interaktion kan vi öka, upprätthålla eller tappa förtroende. Resultatet skiftar mellan människor, över tid och i förhållande till deras livssituationer.
- Transparens, kontroll över sina uppgifter, säkerhet och upplevd individanpassad service ökar förtroendet för avsändaren.
- För lite service eller för mycket service i förhållande till upplevt värde upplevs som ”obehagligt” och avsändaren förlorar i förtroende.
- Upprätthållande av förtroende kräver en upplevelse av värde och relevans i varje given situation.
- Vi har möjlighet att använda persondata för att kunderna ska få tjänster som ger en känsla av kontroll, som underlättar livet eller för att hantera den personliga ekonomin. Vi kan även använda persondata för relevanta erbjudanden.
- Banker anses ha det högsta förtroende att hantera personuppgifter.

Ytterligare undersökningar genomförda med hjälp av Sifo-panelen

Det har funnits indikationer på att det är svårt för deltagare i undersökningar om attityder till persondata-användning att förstå vad det egentligen innebär för dem personligen. Vi ville därför undersöka om det

var möjligt att göra kopplingen mellan persondata-användning och tjänst mer tydlig och därigenom öka validiteten. Vi ville framförallt undersöka människors attityder och förväntan på personaliserade tjänster inom ramen för bank- och finansområdet, tänkta avsändare kunde vara en bank, finansiell aktör eller ett försäkringsbolag.

Studien genomfördes i maj 2019. Det bestod av en enkät som skickades ut till Kantar Sifos Internetpanel och ca 1000 personer i åldrarna 18-79 år svarade. Enkäten bestod av 7 olika fiktiva mervärdestjänster som varje hade 3 underfrågor:

- Om man trodde att tjänsten finns eller skulle finnas inom en snar framtid
- Attityd till tjänsten utan kunskap om vilken persondata tjänsten kräver
- Attityd till tjänsten efter att man fått kunskap om vilken persondata tjänsten kräver.

Våra huvudsakliga slutsatser från denna undersökning var att människor:

- I huvudsak anser att dessa tjänster finns eller kommer finnas i snar framtid,
- rent allmänt är väldigt negativa till personaliserade mervärdestjänster inom bank & finans-området (70-90% vill inte ha dem),
- Är allra mest negativa till att använda surf- eller chat-data för att utforma personaliserade tjänster,
- Är minst negativa till mervärdestjänster som (på ytan) upplevs som *icke-kommersiella* (för banken), t.ex. vägvisning till vårdcentral baserat på korttransaktioner,
- Känner störst förtroende för en *bankaktör* att hantera personliga tjänster medan de hellre vill att andra aktörer hanterar tjänster som är mer ”opersonliga”, t.ex. vägvisning till en skoaffär,
- Blir ännu mer negativa till tjänsten när de får vetskap om vilken data som använts, detta är starkast när det gäller kvinnor och bankrelaterade tjänster,
- Allmänt är mer negativa till att använda transaktionsdata än annan data, t.ex. positionsdata.

Hantering av persondata i samband med kvalitativ research

På SEB genomför vi kontinuerligt kvalitativ research såsom intervjuer, prototyptester samt observationer. Denna research syftar till att bättre förstå våra (potentiella) kunders/användares behov så att vi tar fram tjänster som verkligen löser problem för dem. Vi behövde bättre förstå hur vi ska hantera den persondata som genereras dessa återkommande undersökningar.

Vi genomförde därmed inom projektet två stycken workshops med den avdelning som genomför studierna. Övningarna och diskussionerna leddes av forskare från Södertörns högskola och Lunds universitet (från *Sjyst data!*-projektet) och ca 25 personer deltog varje gång. Därefter tog den ansvariga avdelningen fram ett förslag på rutin som stämdes av med workshop-ledarna. De primära slutsatserna var att vi behövde införa ett strukturerat sätt att anonymisera data, lagra persondata, föra bok över vilken persondata som lagras samt kontinuerligt rensa persondata.

Bumbee Labs – Attitydundersökningar i stads- och gatumiljö

Bumbee Labs är ett litet privat företag som med hjälp av anonymiserad wifi-data från mobiler kan kartlägga flöden av rörelser i ett begränsat geografiskt område, t ex för att bättre kunna genomföra stadsplanering.

Syfte och mål med piloten

Det har varit viktigt att förstå de rädslor, frågetecken och tankar medborgarna har om sin data, i synnerhet när Bumbee Labs behandlar positionsdata (även om denna är anonymiserad) och hur människor rör sig i det offentliga rummet. Upplägget var nytt och intressant, och att få möjligheten att ställa dessa frågor till människor i en verklig kontext, dock var urvalet mycket problematiskt och antalet respondenter begränsat. Frågeställningarna har varit och är alltjämt mycket intressanta för Bumbee Labs verksamhet.

Genomförande och resultat

En enkätundersökning genomfördes kring attityder till personliga data med fokus på positionsdata/lokaliseringsdata registrerade genom mobilen. Enkätundersökningen genomfördes av projektparterna Bumbee Labs, Malmö universitet, Södertörn högskola, RISE och UICTA.

Relativt få användare ingick i studien (drygt 100 personer), och resultatet gav viss insikt kring deras attityder. Kort sagt kan man säga att ju mer respondenterna kände till om mätningarna, desto mer kritiska var de. Om en tänkt tillämpning skulle handla om samhällsnära tjänster (t ex trygghet i den offentliga miljön) så var dock responsen mer positiv. Om man vet om att mätning sker är man något mer benägen att ange att positionsdata används till samhällsplanering. Bland respondenterna med högskoleexamen finns en liten signifikant skillnad i hur mycket man bryr sig om att aktörer kan mäta mobilpositionsdata baserat på om man fick veta, respektive inte veta att mätning sker. De som fick veta bryr sig lite mer. Viktigast för att vara ok med att mätning sker är att man har förtroende för den som mäter. Mer än hälften har varit positiva till att dela med sig om man får något värde tillbaka, t ex rabatter (eller pengar), gratis tjänster, förbättrade samhällstjänster men också tydlig egennytta.

Sandvine – Affärsutveckling för kunders och egen del

Sandvine (f d Procera Networks) har i projektet haft den huvudsakliga rollen som teknikleverantör till de trafikmätningar och analyser som RISE fokuserat på i sin pilot. De har även deltagit i egenskap av expertis på området anonymisering/pseudonymisering (med s k obfuskeringsteknik), där de bidragit med kunskap, förslag och tekniska lösningar för att uppnå en hög nivå av anonymisering/pseudonymisering vid behandling av data.

Syfte och mål med piloten

Sandvine har med sin pilot utforskat de osäkerheteter som funnits kring när/hur kunddata får användas gör att operatörer avstår att använda utrustningens fulla potential med sämre kvalitet och ekonomi som resultat. Dessutom har Sandvine identifierat och analyserat de olika roller och möjligheter de själva skulle kunna ta med avseende på den nya GDPR-lagstiftningen.

Genomförande och resultat

Piloten genomfördes i huvudsak i samverkan med RISE, Lunds universitet, Malmö universitet och en stadsnätsoperatör, i form av att arbeta med olika scenarios, tekniska tester, analyser och workshops. Resultatet har tydliggjort de tekniska och legala förutsättningarna, möjligheterna och hindren, samt tydliggjort de olika möjliga roller som Sandvine kan ta. Det har också bidragit till att införa goda anonymiseringsfunktioner och neutraliseringsfunktioner utan att försvåra arbetet för operatörer. Piloten visar också på vikten av att fortsätta och ytterligare stärka Sandvines arbete med att automatisera alla beslut som berör samtliga tjänster som kräver förtroende från slutanvändare, så att manuell hantering av potentiellt känslig information kan undvikas.

Kantar Sifo – Kartläggning av allmänna och fördjupade attityder till datadelning

Kantar Sifo är ett av Sveriges största undersökningsföretag och inom ramen för projektet har Kantar Sifo genomfört ett antal undersökningar m h a den s k Sifo-panelen (se nedan).

Syfte och mål med piloten

Syftet med piloten var att bidra till förbättrade tjänster/produkter för marknadsundersökningar genom att få en bättre förståelse av konsumenters/användares attityder till datadelning, bättre insikt i de nya legala aspekterna, och att utveckla ny teknik och nya frågeställningar (t ex m h a anonymiserade reella data, genererade av användare).

Genomförande och resultat

Rent metodologiskt delade vi upp undersökningarna i två spår med följande huvudmålsättningar: 1) Att *följa förändring bland individers datadelningsvilja*, 2) Att *nå fördjupad kunskap kring skillnader i datadelningsvilja kopplat till olika fält*.

Det första spåret utgick från målsättningen att etablera en form av barometer för att kartlägga den svenska befolkningens inställning till att dela data med företag, myndigheter, andra organisation och privatpersoner. Denna datadelningsbarometer genomförde vi en utgångslägesundersökning för under 2018. I och med att det i projektets nära omgivning pågått ett antal besläktade återkommande undersökningar – *SOM-undersökningen* och *Delade Meningar* - tog vi efterhand gemensamt beslutet att istället satsa på *fördjupande* tematiserade undersökningar kring ämnesområdet.

Det andra spåret av fördjupande undersökningar genomfördes vid två olika tillfällen. I september 2018 genomförde vi i samband med riksdagsvalet en djupdykning i datadelningsvilja kopplat till politik och demokrati med en specialinriktning på uppfattningar och attityder till sociala medier och deras inverkan (i ljuset av t ex Cambridge Analytica-skandalen, samhällsdiskussionen om fake news och ryska trollfabriker). Den undersökningen genererade en publicerad rapport (*Svenskarnas attityder till integritet och politisk opinionsbildning på nätet och i sociala medier*, se bilaga 3). En andra fördjupning i attityder till datadelning gjordes tillsammans med projektparten SEB kring med ett privatekonomiskt fokus. En ny form av innovativ undersökning utformades då där ett antal fiktiva tjänster presenterades tillsammans med en beskrivning av vilken typ av dataanvändning de krävde. Respondenterna fick bedöma önskvärdheten av tjänster i takt med att de blev mer och mer datadelningskrävande och integritetsöverskridande (se sammanfattning under SEB:s pilot, tidigare i detta kapitel).

Kantar Sifos internetpanel

Sifopanelen är Sveriges största slumpmässigt rekryterade panel med över 100 000 panellister geografiskt fördelade över hela landet. Sifopanelen är helt och hållet Kantar Sifos egen vilket möjliggör full kontroll över panel och panellister för säkerställande av högsta möjliga kvalitet i alla undersökningar.

Sifopanelen är en av få svenska paneler som har rekryterats slumpmässigt via riksrepresentativa telefonintervjuer eller postala undersökningar, vilket är en förutsättning för att all statistisk analys. Det går alltså inte att självrekrytera sig till panelen, eftersom det skulle kunna ge skevheter i urval och resultat. Sifopanelens kvalitet, storlek och bredd säkerställer således god representativitet i de urval som ligger till grund för Sifos undersökningar, i mängder av målgrupper, intressegrupper och demografier.

Effekter och konsekvenser för projektparter

Projektet Sjyst data! har medfört olika effekter och konsekvenser för de medverkande deltagarna beroende på deras verksamheter (se bilaga 1 för enskilda projektparters respektive konsekvensanalys).

För de tre akademiska deltagarna handlar det övergripande om kompetenshöjning och samverkan, vilket har stor vikt och gör avtryck i den forskningen och utbildningen man bedriver, men också för tredje uppgiften; spridningen av forskningsresultat till samhället, vilket exempelvis skett via de rapporter, artiklar och vägledningar som projektet producerat. För de akademiska parterna har projektet bidragit till en insyn i industrins arbete kring dataskyddsfrågor och hantering av personlig integritet vid utvecklingen av kommersiella lösningar. Detta har gett insikt om vilka utmaningar som finns och som behöver lösas, exempelvis genom medvetandegörande om dataskyddsfrågor inom organisationer, ökad kompetens för hur data samlas in hos användarna, och utvecklingen av *legal design* som ett led i denna kompetensökning. Projektet har också gett en ännu större förståelse för att det vidare arbetet inom detta område kräver en tvärvetenskaplig och sektoröverskridande ansats.

För parter som bedriver forsknings- respektive kommersiell verksamhet kring internettrafikmätningar har projektet varit nödvändigt för att lösa om och hur sådana mätningar överhuvudtaget kan genomföras på laglig väg, med hänsyn tagen till såväl GDPR och LEK, liksom de senaste rönen och rättspraxis. Det har lett till utveckling av riktlinjer för hur data kring t ex deltagare, leverantörer och partners ska hanteras och vilka datahanteringsroller som man bör kunna hantera vid trafikmätningar, både vid forskning och kommersiella kundprojekt. Projektet har gjort det möjligt för att börja planera för goda anonymiseringsfunktioner och neutraliseringsfunktioner som det är möjligt utan att försvåra arbetet för dataoperatörer, och projektet har visat på vikten av att fortsätta och ytterligare stärka detta, så att manuell hantering av potentiellt känslig information kan undvikas.

För de övriga kommersiella deltagarna har Sjyst data! framför allt bidragit med två saker; dels ökad kunskap om juridiska krav och praktisk strategisk vägledning för datahantering; dels insikt och kunskap om användarnas behov och inställning till insamling av personliga data, det så kallade ”femte lagret” av digitaliseringens beståndsdelar: individen. Förändrad reglering har fått direkta ekonomiska konsekvenser för de medverkandes verksamheter. Vid sidan av strategisk vägledning, har projektet visat hur olika

verksamheter hanterat och diskuterat detta, samt gett inspiration och insikter inom nya arbetsområden där data kan komma till användning. Personaliserade tjänster kommer i ökad utsträckning vara grundläggande i all tjänsteutveckling för de medverkande parternas verksamheter. Projektet har gett ökad förståelse för komplexiteten, men också en ödmjukhet att hantera personuppgifter och att utveckla datadrivna tjänster med respekt för kundens integritet och behov. Då kraven ökar på att företag och organisationer kan garantera sjyst dataanvändning i alla steg, krävs fortsatt utveckling innan man nått dit fullt ut.

Slutord och tankar om nästa steg

Det komplexa och mångfasetterade arbetet inom de områden som projektet *Sjyst data!* har adresserat kommer fortsatt att vara viktigt för såväl individer som företag, samt vara i ständig förändring. Vi ser några naturliga idéer och fortsättningar på det arbete vi påbörjat:

- Utforma och utveckla en **första skarp version av märkning eller certifiering** inom dataskydds- och integritetsområdet. Denna ska sedan kunna skalas upp och rullas ut på bred front till företag.
- Etablera ett **”dataskyddslabb”** (alternativt utveckla ett redan etablerat labb eller testbädd), där olika företag får möjligheten att i en ”labbmiljö” testa olika case, appar, interface, funktioner etc. för att skapa bättre förståelse, insikter och designmöjligheter vid framtagande av nya koncept/tjänster. Här ska finnas en möjlighet att testa en idé eller tjänst (eller funktion) m a p exempelvis teknik, användarupplevelse, användarbehov, design, juridik, etik och ekonomi.
- Utveckla en **verktygslåda** och metodik för att applicera och införa **”legal design”-tänkande** i tjänsteutvecklingsprocesser. Ta fram ”best practices” för olika typer av kontexter och tillämpningar. Utveckla *Vägledningen* till att även inkludera dessa aspekter än mer.
- Utveckla olika typer av **undersökningsmetoder**, som ett stöd för att ytterligare och bättre kunna förstå och testa användarmönster och attityder; t ex trafikmätningar i stadsnät, mobilnät, IoT och andra typer av datakällor. Dessa mätningar och undersökningar skulle också kunna nyttjas som ett sätt att följa upp en certifierad tjänst/aktör.
- Involvera **fler kommersiella aktörer** från ett antal olika branscher (t ex detaljhandel, transport, media, fastigheter/smarta hem), för att fånga upp deras behov och idéer till en certifiering. Följa eller bidra till framtagande av uppförandekoder.

Du hittar projektets rapporter och publikationer på www.sjystdata.se

Bilagor

1. Konsekvensanalys per projektpart (sist i detta dokument)
2. Vägledning (uppdaterad, version 3; separat dokument)

Bilaga 1: Konsekvensanalys per projektpart

Lunds universitet

Lunds universitet har inte deltagit i egenskap av myndighet, utan genom mig som enskild forskare. Det är i första hand i rollen som forskare och lärare jag har haft nytta av projektet. Det har varit väldigt givande att få arbeta praktiskt med dataskyddsfrågor och att få en god insyn i hur olika organisationer arbetat med dessa frågor. Genom projektet har jag fått nya insikter om vilka utmaningar som finns och som behöver lösas, men också att dessa kräver en tvärvetenskaplig insats. Genom vår vägledning och min fortsatta forskning kommer denna kunskap att kunna spridas till det omgivande samhället. Den får också spridning genom de kurser som jag undervisar på, såsom en kurs i dataskyddsjuridik. Genom att ha deltagit i projektet kan Lunds universitet alltså förbättra den praktiska relevansen av sin forskning och utbildning.

Malmö universitet

För Malmö universitet är de direkta konsekvenserna av projektet att vi ökat vår förståelse, kunskap och insikt i alltifrån utmaningar till användarattityder. Vi har också kunnat publicera artiklar och presenterat en av projektets undersökningar på en vetenskaplig konferens på mediaområdet. Via undersökningarna har vi även skrivit ett kapitel i SOM-undersökningens publikation/bok. Indirekt är det externa forskningspengar och deltagande i samverkansprojekt med annan akademi och industri.

Södertörns högskola

För Södertörns högskola är de direkta konsekvenserna av projektet att vi ökat vår förståelse, kunskap och insikt kring de legala krav som ställs på vår verksamhet (forskning och utbildning) samt att vi fördjupat och utvecklat ny kunskap inom ett tvärvetenskapligt område som visat sig vara allt viktigare för såväl användare som avsändare av digitala tjänster, nämligen designmönster och legal design.

SEB

Allt pekar på att personaliserade tjänster är här för att stanna även om människor inte efterfrågar det så tydligt inom bank och finans idag. Vi förutspår att inom en snar framtid kommer våra kunder förutsätta att detta är grundläggande i all tjänsteutveckling.

Det vi lärt oss av studierna är att:

- gränsen mellan ”obehagligt” (dvs. för mycket service/värde och för lite service/värde) är hårfin och toleransnivån är lägre än vi trodde,
- vi behöver stötta våra kunder i den här resan genom att utmana dem, men utan att tappa i förtroende,

- rent allmänt har vi fått en ökad förståelse för komplexiteten men också en ödmjukhet att hantera personuppgifter och att utveckla datadrivna tjänster med respekt för kundens integritet och behov,
- vi måste hitta ett sätt att implementera personaliserade tjänster utan att de upplevs som integritetskränkande och utan att kunderna tappar förtroendet för oss.
  Vi borde mäta kundernas förtroende över tid. Vi genomförde en pilot för att undersöka om vi kunde prediktera kundmönster i relation till förtroende. Men vi fann inga tydliga korrelationer. Idag mäter vi kundnöjdhet men vill vidga begreppet till att även innefatta förtroende ”trust”. Just nu vet vi inte hur.
- vi har ökat kvalitén i vår persondatahantering när det gäller kvalitativ research om kunder och kunders behov.

UICTA

På Urban ICT Arena har Sjyst data inneburit en mängd nya insikter och har bidragit till idén om ett nytt ”lager” i det vi kallar för ”Lasagne-modellen”. Lasagne-modellen är ett sätt att beskriva digitaliseringens beståndsdelar i horisontella lager – likt lasagneplattor. Modellen används av Urban ICT Arena för illustrativa syften, som vid presentationer. Lagerna består av hårdvara, mjukvara och tjänster. Sjyst datas undersökningar om hur individerna ser på data har bidragit till en komplettering av modellen med ”det femte lagret” – individer. Det krävs individer för att samla data, och de behöver ges bättre information och eventuellt medgivande för att möjliggöra en sjystare datainsamling.

Vidare har projektet inneburit insikter för hur vår testbädd, där data samlas in av flera olika aktörer i en urban miljö, behöver jobba med frågor relaterade till GDPR och hur vi bör informera om datainsamlingen.

RISE

Forskning i GDPR-sammanhang ”…ges en vid tolkning och omfatta till exempel teknisk utveckling och demonstration, grundforskning, tillämpad forskning och privatfinansierad forskning. … Vetenskapliga forskningsändamål bör också omfatta studier som utförs av ett allmänt intresse inom folkhälsoområdet.” (skäl 159 i förordning (EU) 2016/679).

I projektet har RISE arbetat med en pilot som syftar till att bedriva forskning kring användar- och trafikmönster för internettrafik. Detta är en verksamhet som man tidigare bedrivit under ett antal år, men som i och med GDPR:s införande nu måste analyseras och behandlas i ett nytt ljus.

För vår specifika forskningsverksamhet kring internettrafikmätningar och analyser så har vi tvingats ta ett omtag, m a p såväl GDPR som LEK, och detta har tillsammans med de senaste rönen och rättspraxis har utmynnat i ett något förändrat och mer stringent förhållningssätt till den (anonymiserade/ pseudonomiserade) data som vi avser att behandla.

Vi identifierade fyra olika möjliga roller:

A. Enskilt personuppgiftsansvarig (”data controller”)

B. Gemensamt personuppgiftsansvarig

C. Personuppgiftsbiträde (hanterar personuppgifter för annans räkning) (”data processor”)

D. Ingen av ovanstående (ingendera)

Slutsatsen av den omfattande juridiska och tekniska analysen, samt tolkningarna av de senaste rättsfallen och i dialog med ansvariga, har utmynnat i att RISE måste ta rollen som gemensamt personuppgiftsansvarig tillsammans med respektive nätoperatör vars internettrafik vi avser att analysera. Detta trots att data som vi behandlar är anonymiserad/pseudonomiserad enligt de senaste tillgängliga teknikerna för detta dvs med hjälp av den s k obfuskering som leverantören av mätutrustning (Sandvine, projektpart) tillämpar. Det har att göra med att RISE påverkas indirekt av LEK och att RISE bedriver trafikmätningar i forskningsändamål och är därmed med och ”påverkar ändamål och medel” tillsammans med nätoperatören. För mer detaljer kring senaste rättspraxis, se mål i Wirtschaftsakademie Schleswig-Holstein och det s k Fashion ID-målet.

Slutsatsen har också inneburit att RISE har behövt genomföra en konsekvensbedömning enligt Datainspektionens riktlinjer tillsammans med nätoperatörerna i fråga, samt upprätta gemensamma styrdokument med dessa som beskriver vem som ansvarar för vilka delar av behandlingen av mätdata.

För RISE har insikterna och kunskapen från projektet även genererat bl a en diskussion med vår DPO, men även med en del andra projekt inom RISE som berörs av GDPR. Vi vill påpeka att många olika typer av forskningsområden och projekt både inom och utanför RISE är intresserade av att ta del av våra resultat och att det finns en stor efterfrågan av att ta del av fortsatta resultat. I sammanhanget kan också nämnas att RISE nu har tagit fram riktlinjer för hur data kring olika typer av aktörer, t ex forskningsdeltagare eller underleverantörer ska hanteras.

Kantar Sifo

Kantar Sifo har inom ramen för projektet fått en otroligt viktig interaktionsyta för sin framtida utveckling. Under en tid av stora förändringar i datalandskapet och stor osäkerhet kring effekterna och implementeringen av GDPR gav projektets partners och diskussioner juridisk och praktisk strategisk vägledning. De juridiska ramarna kring datadelning är givetvis av yttersta vikt för Kantar Sifo och förändrad reglering inom detta område får direkta ekonomiska konsekvenser såväl för oss som för de allra viktigaste av våra kunder i en bred palett av branscher. Vi har i projektet direkt bidragit med kunskaper inom undersökningsmetodik och undersökningskraft och vi har under projektet gång tillsammans med övriga partners mejslat fram en allt tydligare bild av hur datadelningsviljan ser ut och förändras hos den svenska befolkningen. Inom projektet hade vi också stora förhoppningar på en kooperativ fördjupning inom vad gränserna går mellan vad som är tekniskt möjligt och etiskt önskvärt att genomföra utifrån vad konsumenter/brukare i praktiken accepterar. Detta arbete ser vi fram emot att fördjupa i ett nästa steg där vi även bidrar i utvecklingen av den certifiering för Sjyst data! som är central för projektet och som vi driver genom projektpartnern Kantar Audit (f d TS Mediefakta), idag nära knuten till Kantar Sifo.

Den senast tre åren visar att projektet Sjyst data! har identifierat en helt central domän för vad som kommer att skilja marknadens framtida vinnare från förlorare. Alla företag, myndigheter och andra

organisationer måste givetvis i ett första steg följa lagar och regleringar, men för att lyckas krävs även att man går mycket längre i relationen till konsumenter och medborgare. Kraven ökar på att vi kan garantera sjyst dataanvändning i alla steg, och det är dit vi gemensamt strävar.

Öresundskraft

I och med att Öresundskraft endast deltog det första halvåret i projektet, sammanfattade de kort de erfarenheter och de kunskaper som de inhämtat under sitt partnerskap. Kortfattat kan man säga att påverkan på Öresundskraft handlade primärt om legala insikter och krav, samt att man tvingades börja planera och vidta vissa åtgärder, t ex tillsättandet av ett dataskyddsombud. Öresundskraft fick också genom projektet en tydligare bild vad t ex behandling av personuppgifter eller samtycke innebär och vilka krav som ställs på dessa.

Bumbee Labs

Integritetsaspekter är en mycket essentiell del av Bumbee Labs verksamhet och vi lägger mycket stort fokus och vikt på detta. Att hantera medborgarnas personuppgifter tar vi på högsta allvar. Vi försöker ligga i frontlinjen kring detta och Sjyst data har bidragit till att öka vår kunskap och få perspektiv på hur andra arbetar. Arbetet med Sjyst Data har också gett oss nya insikter och vi har hittat nya arbetsområden där vår data kan komma till användning. Det svåra med att informera medborgarna om hur deras data samlas in i olika sammanhang, är att ge rimliga och enkla förklaringar för hur data hanteras. Det finns ett stort behov av enkel och tydlig information till medborgarna och detta har projektet Sjyst Data belyst.

Sandvine (f d Procera)

Projektet har gett Sandvine en ökad förståelse av:

1. Vad en korrekt hantering av tjänsters data innebär.
2. Vilka datahanteringsroller som Sandvine behöver kunna hantera.
3. Hur Sandvine skall undvika dessa datahanteringsroller i kundprojekt.

Vi har också genom diskussioner med våra partners i projektet lärt oss mer om vad det innebär att *obfuskera* (pseudonymisera/anonymisera) data så att informationen blir “anonymiserad”: att alltid överstiga ett minsta antal IP-adresser och en minsta geografisk utbredning i varje bit information som hanteras av en mänsklig operatör.

Vi har också genom workshops med våra partners lärt oss mer om vad det innebär att obfuskera tjänster så att information “inte avslöjar etnisk tillhörighet, religion, kön, funktionsnedsättning, sexuell läggning, politisk åsikt eller ålder”: att alltid ha en sammansättning av tjänster som täcker hela detta spektrum i varje bit information som hanteras av en mänsklig operatör.

Vi kom också fram till att det är svårt att etablera absoluta gränsen för när något är tillräckligt obfuskerat. Den största svårigheten är att information blir mer känslig tillsammans med annan information, så att flera bitar information som vardera bara är något lite känslig kan bli mer känslig när dessa sammansätts.

Projektet har gjort det möjligt för oss att börja planera för så goda anonymiseringsfunktioner och neutraliseringsfunktioner som det är möjligt utan att försvåra arbetet för dataoperatörer. Projektet visar också på vikten av att fortsätta och ytterligare stärka vårt arbete med att automatisera alla beslut som berör samtliga tjänster som kräver förtroende från slutanvändare, så att manuell hantering av potentiellt känslig information kan undvikas.

IAB

Projektet har gett oss ett värdefullt nätverk och bra insikter om vad GDPR innebär och hur det påverkar oss som företag/organisation, samt våra medlemmar. Vi har i och med detta fått vägledning kring hur vi i vår egen verksamhet ska efterleva och förhålla oss till den nya lagstiftningen.

Kantar Audit (f d TS Mediefakta)

Sjyst data!-projektet har gett oss ett värdefullt nätverk och bättre kunskaper och insikter om vad GDPR innebär och hur det påverkar oss som företag/organisation. Vi har i och med detta fått vägledning kring hur vi i vår egen verksamhet ska efterleva och förhålla oss till den nya lagstiftningen.