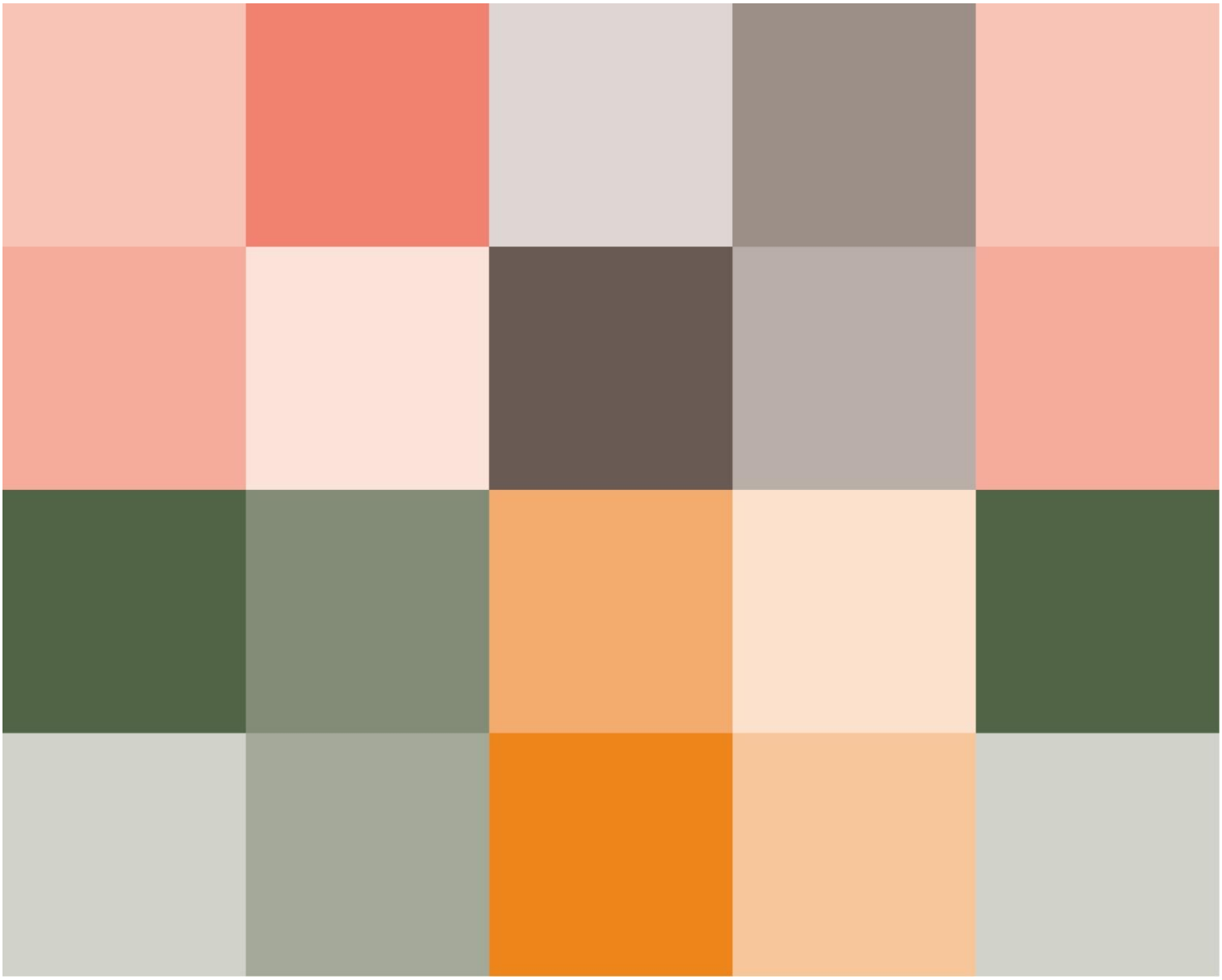


Bilaga 1

Behovsanalys & medborgarperspektiv (från uppdrag att möjliggöra lösningar för individen till kontroll och insyn av data om individen)

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Innehåll

1 Medborgarperspektiv - Attityder till delning av data i Sverige

Under 2018 aktualiserades diskussionen om hantering av användargenerad data på nätet dels på grund av att den nya dataskyddsförordningen GDPR trädde i kraft som hanterar behandling av personuppgifter och dels på grund av skandalen kring Cambridge Analytica som samlat in miljontals Facebooks-användares personliga information i syfte att påverka utgången av det amerikanska presidentvalet 2016. I centrum för diskussionen som ännu pågår är priset individen betalar, eller är redo att betala, för de digitala tjänster som olika privata aktörer erbjuder i termer av hur beteendedata samlas in, används och säljs vidare. Samma diskussion kan hållas kring vad individen är redo att betala för bättre, individualiserade offentliga tjänster i termer av vilken data dessa offentliga aktörer innehar, hur den används och i vilka syften den delas med andra offentliga (eller privata) aktörer. Frågan är om det finns skillnader i tillit till det offentligas hantering av personbundna data i jämförelse med privata aktörer och om individen är villig och kapabel till att ta ett större ansvar för regleringen av hur denna data samlas in, hanteras och delas vidare.

Utöver detta behöver man även ta hänsyn till den så kallade integritetsparadoxen, det vill säga att flera uttrycker oro för integritetsintrång men fortsätter att använda tjänster på nätet utan att i någon större utsträckning skydda sig, Det finns med andra ord ett glapp mellan attityd och faktiskt beteende som bör beaktas.

2017 års SOM-undersökning[1] (SOM-institutet är en oberoende samhällsvetenskaplig forskningsorganisation vid Göteborgs universitet med fokus på samhälle, opinion och medier) visar att det är få svenskar som är positiva till att olika internetaktörer samlar in och använder deras beteendedata. 24 % av

[1] Göteborgs universitet, SOM-institutet (2019). Den nationella SOM-undersökningen 2017. Svensk nationell datatjänst. Version 1.0. https://doi.org/10.5878/n5b5-zn80

svenskarna svarade då att de helt eller delvis instämmer i att det är bra att företagen samlar in information i syfte att förbättra de tjänster de erbjuder. 59 % är negativa till detta och ungefär lika många (61 %) är negativa till att företag säljer vidare personliga data, exempelvis till annonsörer eller andra kommersiella aktörer.

Enligt Sara Leckner, docent i medieteknik och universitetslektor på Institutionen för datavetenskap och medieteknik, visar undersökningen att människor är oroade över att de inte har någon kontroll över sina data och att deras data kan komma att användas i andra sammanhang än de ursprungligen delades i, exempelvis att tredje part ska få tillgång till deras personliga information. Inställningen till insamling av personliga data kan dock skilja sig mellan olika befolkningsgrupper och förutsättningsskapande faktorer såsom ålder och utbildning.[2]

1.1 Tillit till staten och myndigheters hantering av data

Enligt OECD visar deras undersökningar att värderingar såsom integritet, rättvisa och öppenhet är starka prediktioner för nivån på allmänhetens tillit till staten och dess institutioner. Lyhördhet, handlingskraft och tillförlitlighet när det gäller att tillhandahålla offentliga tjänster och förutse nya behov är avgörande för att öka förtroendet för institutionerna.[3]

Enligt Lars Trägårdh, professor i historia och civilsamhälleskunskap vid Ersta Sköndal Bräcke högskola så kännetecknas Sverige av en relativt hög tillitsgrad i förhållande till många andra länder och tillsammans med våra nordiska grannar klassas Sverige som ett högtillitssamhälle.[4] I tillitsbarometern som högskolan publicerar så görs även kopplingar mellan tilliten som ges uttryck för mellan individer och från individer mot det lokala styret till den generella tilliten för staten som helhet. Tillit, på alla nivåer behöver underhållas och en stor del beror på beror på i vilken mån som lokala styren lever upp till sin sida av samhällskontraktet. Mer konkret att invånare upplever trygghet, säkrade rättigheter och social service och att institutioner som skolor, vårdcentraler, sjukhus, omsorgsenheter, fundamental infrastruktur, näringslivsförutsättningar

[2] Sprickor i fasaden: SOM-undersökningen 2017, Göteborg: Göteborgs universitet, 2018. S.60
[3] https://media.sitra.fi/2020/10/08100935/towards-trustworthy-health-data-ecosystems.pdf sid.18
[4] https://www.esh.se/nyhetsarkiv/2019-05-13-sa-mycket-litar-vi-pa-varandra-i-sverige.html

med mera finns på plats och fungerar bra.[5] En hög grad av tillit till staten är en förutsättning för att det även ska finna tillit till hur staten hanterar data.

Bland kritiska förtroendeskapande egenskaper är öppenhet, tillförlitlighet, medborgarregering och medborgaraffärsrelationer, kompetens, rättvisa och äkthet när det gäller sociala och kommersiella transaktioner och ledarskap.

För att upprätthålla förtroendet för behandlingen av personuppgifter måste individer:

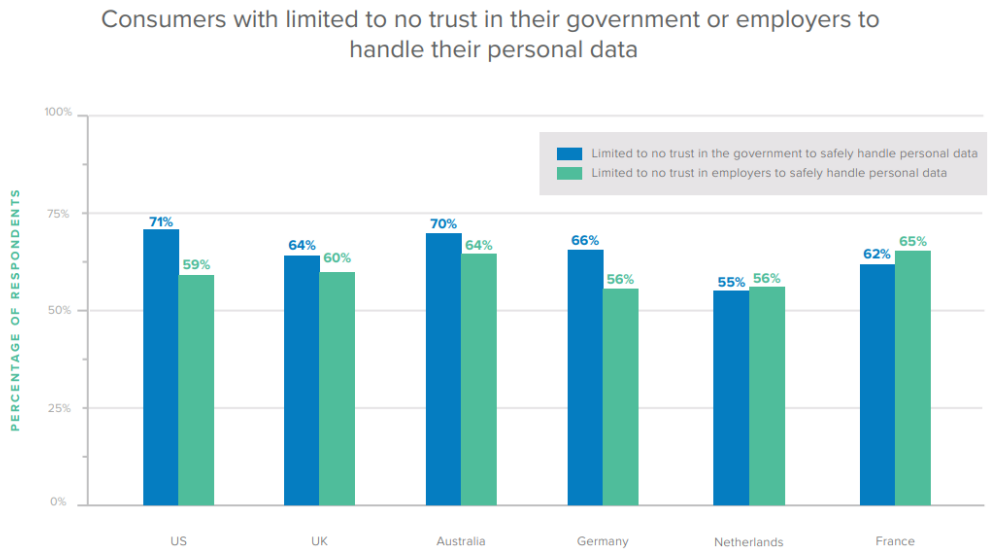
- kunna övervaka behandlingen i realtid
- hålla sig informerad om när deras uppgifter behandlas och omfattningen av behandlingen
- ges möjlighet att återkalla sitt samtycke i realtid
- ha en garanti för att deras data är skyddad som standard, vilket innebär att kontrollen över data är så enkel som möjligt
- ha befogenhet att kontrollera vem, varför och i vilket syfte deras data används.

Tillit kan alltså ses som en produkt av insyn och kontroll. Omvänt gäller att då vi har tillit, har vi inte samma behov av kontroll, men tillit förutsätter möjligheten till kontroll.

I en undersökning genomförd av företaget Okta och som jämförde attityder till datadelning mellan olika länder (USA, Storbritannien, Australien, Tyskland, Nederländerna och Frankrike) uppvisades att en betydande del av invånarna i dessa länder oroas över deras respektive regeringars förmåga att hantera data och intentioner med att samla in data. USA och Australien har enligt studien lägst förtroende för staten (71 % respektive 70 % litar inte på statens förmåga att hantera deras data på ett säkert sätt) medans endast Nederländerna och Frankrike litar mer på statens förmåga än på privata arbetsgivares förmågor på området även om det är med en marginell skillnad.[6]

[5] Tillitsbarometern, Levande Rapport version 4, 2020 sid. 7 2021.02.25 14:14
[6] https://www.okta.com/cost-of-privacy-report/2020/

Figur 1 Tillitsnivåer för hantering av personliga data



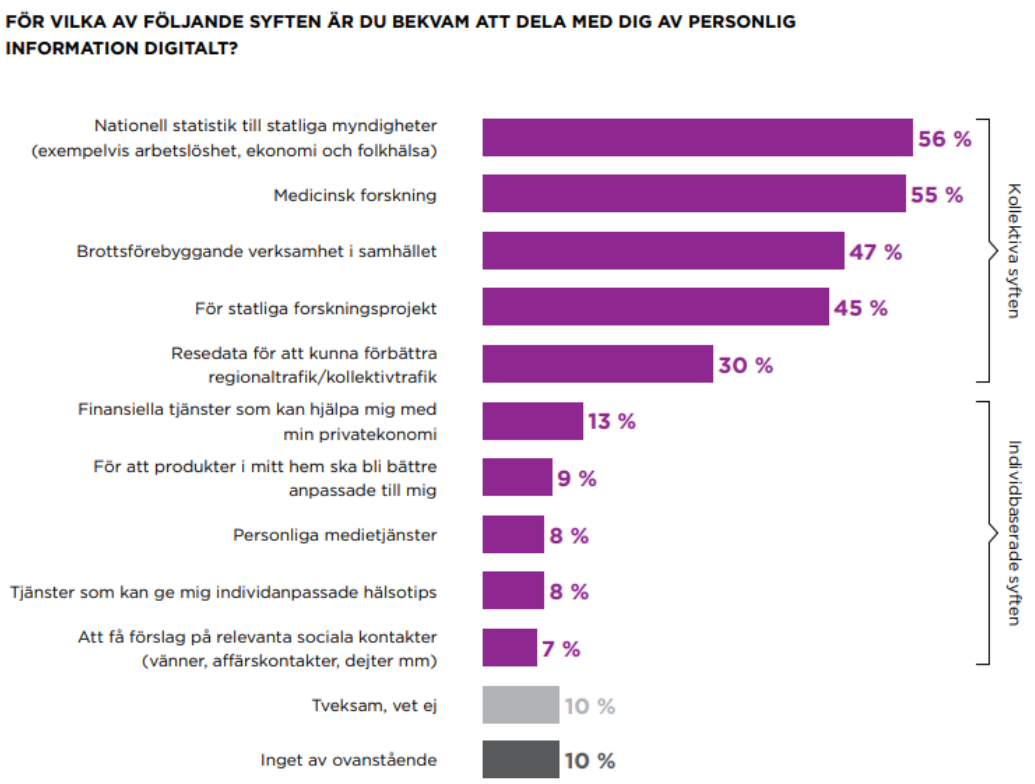
Att medborgare delar data om sig själva med en myndighet kan ge många fördelar när det gäller att skapa forskningsunderlag eller kunskap om tendenser hos större grupper. Men, delandet av data med myndigheter är förenat med en rad risker för individen som främst berör frågor om integritet och balansen i relationen mellan myndigheter och medborgare. Insyn och tillit är centrala delar för att delning av data mellan individ och myndighet ska fungera för båda parterna.

I en undersökning av svenska folkets attityder till digital integritet[7], framgår att 47 % känner sig mer bekväma om den personliga informationen sparas på statliga servrar, endast 2 % känner sig mer bekväma med att personlig information sparas på privata servrar. Undersökningen visar också att andelen svenskar som ser den ökade insamlingen och användandet av information i samhället som negativ ökar och andelen som är oroliga för att den information som de delar används i syften

[7] Delade meningar, svenska folkets attityder till digital integritet 2020 deladeMeningar2020_Web_1-9A.pdf (insightintelligence.se)

som de inte är bekväma med har mer än dubblats på fem år (22 % 2015, 49 % 2020).

Figur 2 Syften för delning av personliga data



Känslan av trygghet ökar inte heller för alla om personliga data avidentifieras. Det kan handla om att man upplever att kontrollen över data som är avidentifierad data försvinner då den kan delas utanför individens kontroll, medan företag är som använder data kopplat till individer är skyldiga att berätta hur den används. Undersökningen visar vidare att man är mer benägen att dela personlig information för kollektiva samhällsutveckling som tex medicinsk forskning och nationell statistik.

Figur 3 Upplevt tvång gällande delning av

Att statliga myndigheter delar ens personliga information mellan varandra är de flesta (58%) positiva till och det samlade förtroendet för statliga myndigheters hantering av den personlig information är relativt hög. Trots det upplever en klar majoritet att delning av data sker utifrån tvång snarare än frivillighet.

1.2 Egenmakt, ansvar och beteende

Tillgång till personliga data ökar invånarens egenmakt i relation till offentliga och privata aktörer. Detta är särskilt tydligt inom hälso- och sjukvård där insyn och kontroll över egna data ökar möjligheten till medskapande av den personliga hälso- och sjukvården.[8] Det är dock inte helt självklart att den enskilde medborgaren är villig att i alla lägen ta ett större ansvar för hur data om individen hanteras och delas.

Det visade sig att när individer fick välja mellan olika lösningar i en brittisk undersökning var alternativ som inbegrep en kollektiv ekosystemlösning där de datadrivna systemen som hanterar individens data regleras mest tilltalande för de tillfrågade. Man efterfrågade en valmöjlighet att kunna välja ett standardalternativ för delning där all datainsamling avstannar tills man har tid eller lust att välja hur och när man ska dela sina data. Individen vill utifrån denna studie även att en

[8] Sitra working paper, Sitra ISBN 978-952-347-192-4 (PDF) sid. 26

offentlig organisation ska, på uppdrag av medborgarna, sköta tillsynen så att organisationer som missköter hanteringen av personliga data tar sitt ansvar.[9]

Att lägga över ansvaret för datahanteringen på medborgarna är inte helt enkelt. I vissa fall känner individen en hopplöshet, de stora aktörerna, privata som offentliga, hanterar data som de vill i vilket fall som helst vilket leder till att individen känner ”digital uppgivenhet”. Transparens, trovärdighet och förståelse för syftet med att dela data är möjligen enklare att bygga upp från offentlig förvaltnings sida gentemot medborgaren snarare än att förse vare medborgare med den digital kompetens som krävs för att kunna fatta informerade beslut om delning och förstå ansvarsfördelningen och möjliga konsekvenser av enskilda val.

Människors inställning till att dela sina data online beror även på faktorer så som rådande normer, media rapportering kring risker med delningen, förtroende för företaget eller organisationen som tar emot data och på vilken typ av personlighet en individ har. Vilken typ av data som delas påverkar också viljan att dela och ju fler som kan se uppgifterna, desto lägre blir vilja att dela dem.

I *The age of surveillance capitalism* från 2019 beskriver Socialpsykologen Shoshanna Zuboff hur teknikföretagen kommersialiserat den sista domänen som kunde kommersialiseras nämligen mänskliga erfarenheter.[10] Informationen säljs vidare och blir till inflytande över vårt beteende. Vi ombeds visa tillit till systemet där vår data byts ut mot bättre, personifierade och riktade digitala tjänster. Har man inget att dölja bör man heller inte motsätta sig denna transaktion men detta synsätt bortser ifrån dels hur mänskligt beteende och beslutsfattande fungerar (det är inte alltid rationellt) och att vi saknar insikt och kompetens för att kunna göra informerade beslut.

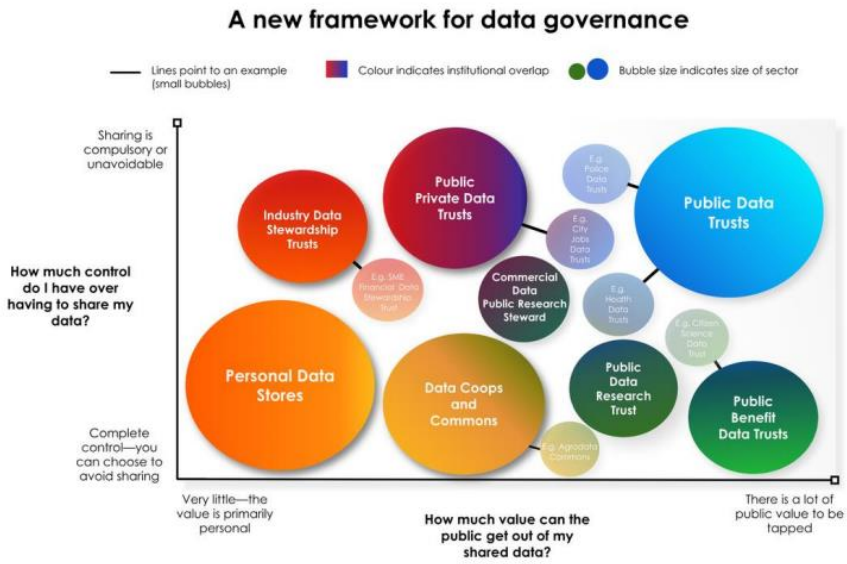
Enligt en artikel från det brittiska innovationsföretaget NESTA från 2019 kopplas tillit och förtroende ihop med datas värde. NESTA menar att felaktig användning eller överanvändning av data kan leda till misstro och misstänksamhet och i förlängningen till att data underutnyttjas. Artikeln refererar till en undersökning där majoriteten vill dela data i sammanhang där det leder till samhällsnytta, men att det råder brist på institutioner med tillräcklig tillit för att maximera sådan

[9] Public perceptions of good data management: Findings from a UK-based survey, Hartman, Kennedy, Steedman & Jones, 2020; doi:10.1177/2053951720935616

[10] Shoshana Zuboff: ‘Surveillance capitalism is an assault on human autonomy’ | Society books | The Guardian

nytta. Individer behöver känna mer tillit och ha kontroll över egna data, samtidigt som data behöver delas för att maximera nyttan. NESTA presenterar även ett ramverk för hur data skulle kunna hanteras utifrån dimensionerna individernas kontroll över datadelning respektive värdet för offentlig sektor.[11]

Figur 4 Dataklassifikationer utifrån kontroll- och värdeparametrar

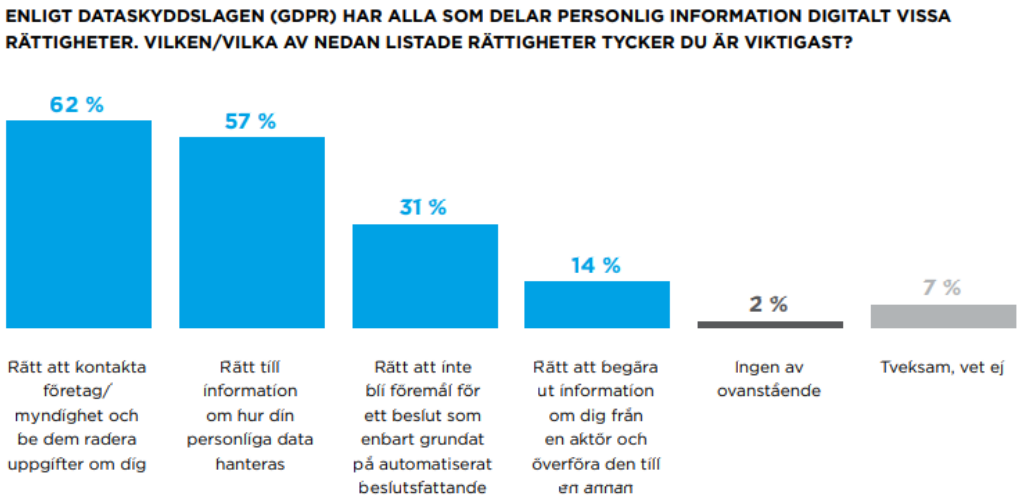


Att individen upplever en avsaknad av kontroll och val när de delar data illustreras som nämndes tidigare av att 66 procent upplever att man delar information främst för att man tvingas till det. Endast 17% uppgav att de delar information för att de vill det.[12] Olika undersökningar visar att en betydande del av tillfrågade, i Sverige och utomlands, säger sig vara oroliga för hur ens information används men det kan konstateras att de är få som utnyttjar sin rätt som konsument att begära ut information. En av tio anger i undersökningen *Delade meningar* att de bett om att få data om sig raderad och lika många har bett om att få sina uppgifter korrigerade. Endast 4% har bett om att få tillgång till sin personliga information. I undersökningar och forskning uppger individer i allmänhet att de är oroliga över

[11] The new ecosystem of trust, 2019-02-19, NESTA, Geoff Mulgan och Vincent Straub https://www.nesta.org.uk/blog/new-ecosystem-trust/

[12] Delade meningar, Svenska folkets attityder till digital integritet 2020 deladeMeningar2020_Web_1-9A.pdf (insightintelligence.se)

hur och varför deras personliga data hanteras, men det motsägs av hur de faktiskt agerar i det dagliga livet.[13]



Figur 5 Rättigheter i GDPR

1.3 Integritet och övervakning

Internetstiftelsens undersökning *svenskarna och internet 2020*, visar att närmare 1 av 5 instämmer i påståendet "Jag är oroad att myndigheter inkräktar på min personliga integritet på internet".[14] Här har pandemin och skiftet för de som kunnat fortsätta arbete från hemmet påverkat upplevelsen av att vara övervakad. Allt fler är oroade över att få sin integritet kränkt av storföretag på nätet och känslan av att vara övervakad på nätet har vuxit. under pandemin Oron för den personliga integriteten är betydligt högre bland de i privat sektor än de i offentlig sektor vilket kan säga stärka tesen att ökad insyn skapar högre tillit.

1.4 Insyn och Kontroll

I en undersökning genomförd av Kairos Future uppger 80 % av svarande att det är en rättighet att ha full insyn i alla data som finns insamlad om en.[15] När personer delar sina uppgifter med ett företag har de ofta en känsla av att de köper något till priset av sina uppgifter till exempel nyttjandet av en tjänst. Man vet även när i

[13] Data Protection Rights: What the public want and what the public want from Data Protection Authorities Prepared by the ICO for the European conference of Data Protection Authorities, Manchester - May 2015
[14] Svenskarna och internet 2020, Internetstiftelsen
[15] Fredrik Torberger, Framtidens samhällskontrakt - Minirapport 1 av 2 från studien Morgondagens Medborgare, 2019 Kairos Future

tiden man får nyttja tjänsten. Denna känsla av kontroll saknas när uppgifter delas med myndigheter och eftersom syftet inte alltid är klart det vill säga vad man får för delandet och när i tiden man kan förvänta sig något i gengäld så finns risker att myndigheter drar slutsatser om en person utifrån inkompletta uppgifter eftersom engagemanget är lägre.[16]

Den tyska konstitutionella domstolens dom om folkräkningen 1983 fastställde att om någon inte kan förutsäga med tillräcklig säkerhet vilken information om sig själv som är känd för sin sociala omgivning och hos dem med eventuell kommunikation kan göras, så hindras hen på ett avgörande sätt i sin frihet att planera eller att besluta fritt utan påverkan.[17] Kontroll kom att betyda möjligheten att utöva friheten att bestämma och man varnade redan då att modern databehandling skulle kunna komma att utgöra ett hot mot denna frihet.

Genom att utvärdera GDPR genom en beteendeobjektiv och ta hänsyn till psykologin för informationsbehandling och beslutsfattande, är det möjligt att förutsäga lagstiftningens effektivitet när det gäller att aktivt förbättra individuell kontroll.[18] Individuell kontroll definieras utifrån vilken utsträckning en individ är medveten om en situation och har den medvetna avsikten och förmågan att starta, stoppa eller upprätthålla en situation. I tabellen nedan försöker man således visa vilka verktyg GDPR nyttjar för att motverka kognitiva fallgropar som hotar individuell kontroll.

Figur 6 Hot mot individuell kontroll i en kontext av en dataekonomi[19]

	Stage 1 information receiving stage	Stage 2 approval and primary use stage	Stage 3 secondary uses of data (reuse) stage

[16] Share and share alike? An examination of trust, anonymisation and data sharing with particular reference to an exploratory
research project investigating attitudes to sharing personal data with the public sector, Marion Oswald, DOI: 10.2966/scrip.110314.245 sid. 253

[17] Abstract of the German Federal Constitutional Court's Judgment of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES]

[18] van Ooijen, I., Vrabec, H.U. Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. J Consum Policy 42, 91–107 (2019). https://doi.org/10.1007/s10603-018-9399-7

[19] van Ooijen, I., Vrabec, H.U. Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. J Consum Policy 42, 91–107 (2019). https://doi.org/10.1007/s10603-018-9399-7

Cognitive processing and decision-making pitfalls that threaten individual control	• Information complexity and literacy • Information overload • Information asymmetry	• Context and choice architecture	Data Affordances: • Intangibility • Invisibility • Scope • Flow
Legal provisions in the GDPR addressing these threats to individual control	• Information notices • Icons	• Consent requirements • Default settigs	Data subject rights: • Right to data access and portability • Right to erasure

1.4.1 Engelsk studie på Personal Data Stores (PDS)

PDS är en individualiserad lösning på individens upplevda underskott av tillit till hur persondata hanteras. En PDS kan liknas vid att man omgärdar all sina personliga data bakom en mur som har bevakade in- och utgångar, en lösning som sägs bemyndiga individen, eftersom man får kontroll. Bemyndigandet är kopplat till att individen får bättre möjligheter att skydda sina data och sin integritet och samtidigt underlättas handel och intäktsgenerering. Individens data kan alltså sparas på en fysisk enhet som användaren själv äger eller en molnbaserad tjänst.[20] Eftersom individen med hjälp av PDS får kontroll över databehandlingen samt tillgång till hur överföringen av deras data sker, presenteras lösningen som förtroendeingivande. Exempel av den här lösningen är Solid, Databox och tjänsten DigiMe. Undersökningen på individers syn på PDS-lösningen genomfördes empiriskt med hjälp av fokusgruppintervjuer och frågeformulär.[21]

Respondenterna i fokusgruppintervjuerna håller med om att PDS kan ge mer kontroll, många delade önskan om att man själv föredrog att kontrollera vad ens privata data användes till. Speciellt när data redan insamlats så ville man vara den som dikterar vad data ska användas till. PDS-lösningen upplevdes som rättvis

[20] H. Janssen, J. Cobbe, C. Norval, J. Singh, 'Decentralised data processing: personal data stores and the GDPR', (2020) Vol. 9 International Data Privacy Law. https://doi.org/10.1093/idpl/ipaa016, pp 356 - 384

[21] Public perceptions of good data management: Findings from a UK-based survey, Hartman, Kennedy, Steedman, & Jones, 2020; Steedman et al., 2020, p. 821

eftersom man kan välja vilken data som ska delas, och det utan att det påverkar deras tillgång till en tjänst. Två problem som uppmärksammades var dock tid och säkerhet.

Att hantera sina egna data kommer att kräva mycket tid, även om själva transparensen upplevdes som attraktiv, så ansågs den aktiva rollen som man måste ta för att kontrollera och hantera data innebära en massa krångel. Eventuellt kunde man tänka sig att anförtro sina data till en tillförlitlig mellanhand, men att avgöra när man skulle göra det är beroende av hur mycket tid man skulle behöva lägga ner själv vilket är svårt att uppskatta. Att med hjälp av en PDS-lösning kunna fatta genomtänkta beslut om vad ens data får användas till tyckte de allra flesta i slutändan skulle ta för mycket tid. Det finns en oro för att överrumplas av förfrågningar om tillgång till data.

Respondenterna ställde krav på att själva hanteringsprocessen måste vara fullkomligt enkelt och synnerligen användarvänlig. Om inte, skulle en PDS-lösning antagligen inte skilja sig från hur man idag godkänner villkor på sociala media plattformar med mera utan sätta sig in i villkoren. Flera respondenter upplever en omöjlighet med att kunna överväga sina val noggrant, och individen upplever en likgiltighet eller digital uppgivenhet som även kallas digital resignation. Ett sätt att motverka resignationen kunna vara möjligheten att välja ett standardalternativ som innebär att alla förfrågningar nekas. Vid ett senare tillfälle kan individen, när man känner att man har tid, välja att säga ja till vissa fall av förfrågningar.

Gällande säkerhet ansåg respondenterna att PDS-lösningen inte innebar en ökad säkerhet gentemot andra lösningar och även om tanken på att kunna kontrollera sina data var tilltalande så var de flesta respondenterna skeptiska till lösningens datahantering. Om tidsåtgången för att få insyn och kontroll skapade en känsla av uppgivenhet och resignation så skapade säkerhetsfrågan en känsla av maktlöshet då individen inte upplever att man har ett juridiskt skydd.

Sammanfattningsvis kan man säga att enligt studien så ogillar individen hur dagens kommersiella organisationer kontrollerar personliga data i utbyte mot de digitala tjänster man tillhandahåller. Man föredrar en metod som ger individen kontroll över sina data men den önskade lösningen borde inkluderar en tillhörande reglerande enhet då individen vill ha stöd i själva tillsynen av datahanteringen.

2 Estimering av ekonomiskt värde av personuppgifts-mobilitet

2.1 Estimering utifrån open banking sektorn

I en rapport[22] från engelska ministeriet för digitalisering, kultur, media och sport (DCMS) undersöktes 2018 potentialen för att stimulera innovation och konkurrens genom personuppgiftsportabilitet. I rapporten estimeras att i ett läge där personliga data från offentlig sektor och från näringsliv kan flöda i ett säkert system som ger individer kontroll över sin data, skulle den ekonomiska påverkan på BNP från ökad produktivitet och konkurrensfördelar som möjliggörs uppgå till cirka 322.6 miljarder SEK (£27,8 miljarder). Detta är i ett tidigt skede innan innovation baserad på denna personuppgiftsmobilitet hunnit skapa nya

[22] DCMS_Ctrl-Shift_Data_mobility_report_full.pdf (ctrl-shift.co.uk)

användningsområden. Beloppet motsvarar en ökning av BNP i Sverige med cirka 4,27 miljarder SEK.

Beräkningarna är i stor del gjorda på marknadseffekter av *open banking* i Storbritannien. Med termen *open banking* menas att man låter en tredjepartslösning, som en applikation, lägga om processer i en bank.[23] Om en bank öppnar sina API:er för marknaden kan vem som helst utveckla tredjepartslösningar som kan stödja processer och ersätta framtidens betalningslösningar. I modellen följer kvantifieringen av den potentiella effekten av datamobilitet tre steg:

1. Uppskatta värdet av datamobilitet för en sektor och definiera detta som en andel av BNP
2. Justera denna andel, eller påverkan, eftersom inte alla sektorer kommer att påverkas lika. Antagandet är att effekterna av datamobilitet är proportionella effekten av *open banking* när det gäller dataintensiteten för en viss sektor.
3. Tillämpa den justerade påverkan på BNP

2018 fann en annan studie att *open banking* genererar £1,069 miljarder av ytterligare värde för Storbritanniens GDP. Genom att jämföra detta med storleken på den brittiska detaljbanksektorn kan ett sektorsspecifikt påverkansvärde för datamobilitet härledas. Detta värde justeras sedan för att reflektera att alla sektorer kommer påverkas i olika grad av ökad datamobilitet. Justeringen estimeras genom att identifiera ett antal dataflöden eller digitala kärnrelationer individer har med olika företag inom en sektor. Antalet relationer inom en sektor påverkar värdet den ökade dataportabiliteten anses komma att utgöra.

2.2 Estimering av värdet av personal data store (PDS) marknaden

I en tidigare undersökning från 2014 försökte man estimera det potentiella värdet på PDS-marknaden för att se om möjligheterna till att bedriva vinstförande företag som PDS-leverantör var tillräckliga för att marknaden skulle växa. Frågan var hur mycket medborgare och organisationer skulle kunna tänkas vara villiga att betala för dessa tjänster.

[23] https://www.pwc.se/sv/bank-kapital/open-banking.html

Studien fokuserade på att estimera det potentiella marknadsvärdet i Storbritannien för så kallade Personal Information Management Systems eller PIMS.[24] Enligt deras utredning så var organisationer villiga att betala mellan cirka 35 – 60 SEK per relation och för att få behörig åtkomst till individens data och tillåten kommunikation med kunder. Vidare uppskattades det att varje individ i Storbritannien upprätthåller mellan 30 och 100 relationer med banker, appar, återförsäljare, myndigheter och andra organisationer. Genom att kombinera dessa två uppskattningar med antalet vuxna och hushåll i Storbritannien estimerades värdet på PIMS-marknaden kunna uppgå till cirka 135 miljarder SEK i Storbritannien.

Beräkningsformeln är således relativt enkel:

Befolkning x antal relationer per person x monetär värdering av varje relation = potentiellt värde av marknaden.

[24] 107Ctrl-Shift, *Personal Information Management Systems: An analysis of an emerging market*, 2014.