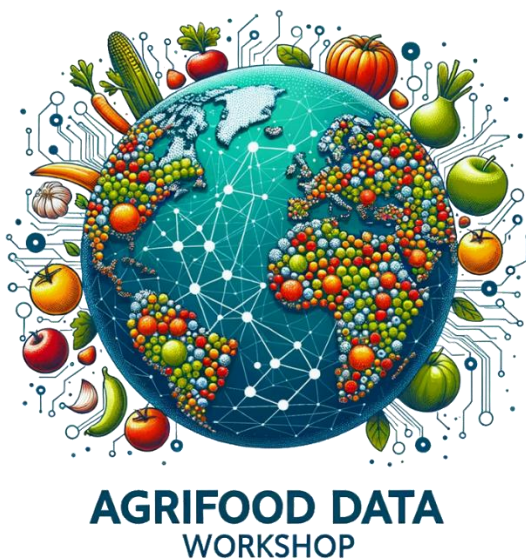




Agrifood Data Workshop – En dataverkstad för jordbruk & livsmedel

Anna Rydberg, Annika Kihlstedt, Victor Kardeby, Frida Sporre,
Kristina Andersson, Mikhail Popov, Christoffer Andresen, Leif
Carlsson

Abstract

Agrifood Data Workshop - A data workshop for agriculture and food

Agrifood Data Workshop (ADW) was a national data workshop aimed at simplifying and securing the use and sharing of data, as well as promoting innovations within the agrifood supply chain.

The workshop has provided support, tools, and methods to enhance competence and data-driven innovation among actors wishing to share data in the agrifood supply chain. The focus has been on the secure and efficient sharing of data according to the Data Governance Act, and a prototype tool for automatic data classification and publication, called “The Washing Machine,” has been demonstrated.

Key words: Data sharing, innovation, legislation, security, Data Governance Act

RISE Research Institutes of Sweden AB

RISE Rapport 2024:69

ISBN: 978-91-89971-30-1

Uppsala 2024

Innehåll

Abstract.....	1
Innehåll.....	3
Förord.....	5
Sammanfattning	6
1 Data – bränslet för den digitala ekonomin	7
1.1 Värdefulla data i areella näringar.....	8
1.2 Möjligheter med data och digital teknik i lantbruket.....	9
1.3 Hinder för användning av digitala verktyg och data i lantbruket	10
2 Data som delas	11
2.1 Öppna och licensierade data	11
2.2 Informationsklassificering	12
2.3 Standarder för datainsamling och datadelning.....	13
2.4 Spårbarhet och standarder i livsmedelskedjan	14
2.4.1 Spårbara livsmedel - ett lagkrav.....	14
2.4.2 Brist på standarder för lantbruksdata.....	16
2.5 Möjligheter och utmaningar med datadelning.....	17
2.5.1 Datadelning mellan företag.....	17
2.5.2 Delning av lantbruksdata	17
2.5.3 Delning av myndighetsdata.....	18
3 Verktyg och plattformar för datadelning.....	19
3.1 Dataområden förbinder dataplattformar.....	19
3.2 Dataplattformar i livsmedelskedjan	20
3.2.1 Lantbrukets dataplattform (Sverige).....	20
3.2.2 Exempel på andra initiativ runt datadelning	21
4 Datadrivna innovationer i livsmedelskedjan.....	23
4.1 Beslutsstödsystem med precisionsjordbruk och precisionsdjurhållning	23
4.2 Klimat- och hållbarhetsuppföljning	23
4.3 Marknadsplatser och prisjämförelser	24
4.4 Spårbarhet av produkter längs livsmedelskedjan	24
4.5 Affärs- och intäktsmodeller av datadrivna tjänster	25
4.5.1 Exempel på affärsmodeller.....	26
4.5.2 Exempel på intäktsmodeller.....	26
4.6 Hinder och möjligheter för ökad datadriven innovation	27
4.7 Utveckling av innovationer med datadelning i Sverige.....	28
5 Legala aspekter kring datadelning	31
5.1 Digitala rättigheter och principer.....	31

5.2	Dataförvaltningsförordningen	32
5.2.1	Kort om dataförvaltningsförordningen	32
5.2.2	Praktisk tillämpning av dataförvaltningsförordningen	35
5.3	Artificiell Intelligens (AI) förordningen	38
6	Informationssäkerhet	39
6.1	Säkring av lantbruksdata.....	40
6.2	Informations- och cybersäkerhet: maximera effekten	41
6.3	Tekniska säkerhetsåtgärder	42
6.3.1	Standardiserade datamodeller	42
6.3.2	Säkra och autentiserade anslutningar	43
6.3.3	Autentisering och auktorisering.....	43
6.3.4	API-säkerhet.....	43
6.3.5	Nätverkssäkerhet.....	44
6.3.6	Penetrationstestning	44
6.4	Organisatoriska lösningar	44
6.4.1	Medvetenhet och utbildning	44
6.4.2	Lösenordspolicy.....	45
6.4.3	Fler organisatoriska åtgärder	45
6.5	Rättsliga komponenter	45
6.5.1	Efterlevnad av lagar och förordningar	45
6.5.2	Begränsat ansvar genom avtal.....	46
6.5.3	Riskreducering genom försäkring	46
6.5.4	Kontinuerlig övervakning och efterlevnad	46
6.6	Slutliga rekommendationer om informationssäkerhet.....	47
6.7	Plattformer för datadelning.....	47
6.8	Automatisk maskering av data som ej ska delas	48
6.8.1	Anonymisering och Pseudonymisering.....	48
6.8.2	Utmaningar i samband med anonymisering av data	48
6.8.3	Syntetisering av Data.....	49
7	Referensarkitektur för datadelning	51
7.1	Datainsamling och analysplattformer	51
7.2	Klassificering för öppna data.....	51
8	Diskussion och slutsatser	54

Förord

Projektet *Agrifood Data Workshop – En datorverkstad för jordbruk och livsmedel*, har förmedlat stöd, verktyg och metoder till aktörer som vill dela data i livsmedelskedjan. Projektet har haft rollen av neutral sandlåda, där olika aktörer genom workshops och öppna seminarier kunnat lära sig mer om vad datadelning innebär. Ett koncept för hur data som ska delas digitalt kan maskeras har också tagits fram och demonstrerats. Projektet har fokuserat på aspekten datadelning från myndigheter, då flera myndigheter hanterar data längs livsmedelskedjan och då Dataförvaltningsförordningen började gälla under projektiden.

Rapporten är framtagen med ekonomiskt bidrag dels från Vinnova, dels från Jordbruksverket via Europeiska jordbruksfonden för landsbygdsutveckling. Projektet har pågått från november 2021 till september 2024. Projektet har letts av RISE och övriga parter i detta projekt har varit Jordbruksverket, Sensative och Hopsworks.

I en referensgrupp knuten till projektet har Viktoria Dagobert Sporrang som senare ersattes med Mats Wessman (båda från Tillväxtverket), Tove Wetterstam (MSB), Johan Wulff (Naturvårdsverket), Armina Avanes (Kodatalabbet och Växa) medverkat.

Vi vill rikta ett stort tack till alla som medverkat under projektets gång och bidragit med sin tid, kompetens och sina synpunkter. Vi vill rikta ett särskilt tack till Niklas Berg, Simon Borgmästars, Peter Bårmann, Leif Carlsson, Lina Edwardsson, Jessica Holm, Joel Håkansson, Annika Kihlstedt, Mikael Lundberg, Daniel Morgenstern, Yuju Son, Iraklis Symeonidis, samt Anders Viberg.

Ståndpunkter och slutsatser som redovisas i rapporten reflekterar författarnas. Det innebär att andra parter eller deltagare kan ha andra uppfattningar.

Om du vill veta mer om projektet eller om rapporten, ta kontakt med anna.rydberg@ri.se

Uppsala, september 2024

Författarna

Sammanfattning

Livsmedelsproduktion är en samhällskritisk bransch som genererar mycket data från en mängd olika aktörer längs värdekedjan från jord till bord. Data är en strategisk resurs för utveckling och digital innovation inom jordbruks- och livsmedelskedjan. Tillgång till högkvalitativa data är avgörande för att öka konkurrenskraften, främja hållbar tillväxt och minska resursanvändningen. Fragmenteringen i livsmedelskedjan gör dock datadelning komplicerad, vilket skapar behov av standarder och interoperabilitet för att säkerställa effektiv datadelning och integration av olika system och applikationer. Flera nationella och internationella initiativ pågår för att underlätta datadelning och lösa frågor om hur data kan delas på ett säkert och effektivt sätt.

I september 2023 trädde Dataförvaltningsförordningen i kraft, vilket ställer nya krav på myndigheter att tillgängliggöra data för maskininläsning. Att uppfylla lagen på ett säkerhetsmässigt sätt kräver nya rutiner och tillvägagångssätt hos myndigheter.

Agrifood Data Workshop (ADW) har fungerat som en nationell dataverkstad. Verkstaden har vänt sig till myndigheter som behöver stöd och verktyg för att kunna öppna upp sina data på ett säkert sätt, samt till andra dataägare som funderar på att börja dela sin data. Projektets mål har varit att förenkla och säkra användning och delning av data samt att främja innovationer inom jordbruks- och livsmedelskedjan. Detta har uppnåtts genom att sprida information om verkstadens möjligheter, locka deltagare till aktiviteter och skapa utbyten med liknande initiativ både nationellt och internationellt. En extern referensgrupp (bestående av aktörer från andra datalabb, dataplattformar och myndigheter) har bidragit med värdefulla insikter.

Dataverkstaden har förmedlat stöd, verktyg och metoder för ökad kompetens och datadriven innovation hos aktörer i livsmedelskedjan. Kartläggningar och behovsanalyser har genomförts för att identifiera juridiska och säkerhetsmässiga krav. Fokus har legat på hur myndighetsdata ska kunna delas säkert och effektivt, och en prototyp av ett verktyg för automatisk klassificering av data har utvecklats. Verktuget, kallat "Tvättmaskinen", utgår från myndighetens rutiner för säkerhetsklassificering av data och har demonstrerats som en prototyp för automatisk klassificering och publicering av data.

I april 2024 hölls en webbdemonstration av verktygsprototypen med över 70 anmälda deltagare från mer än 30 organisationer och företag, och projektets frågeställningar har rönt stort intresse hos olika myndigheter. Genom att implementera erfarenheterna från verktyget kan organisationer inte bara förbättra sin förmåga att dela data på ett säkert sätt, utan också främja innovation och effektivitet inom och bortom jordbruks- och livsmedelskedjan.

1 Data – bränslet för den digitala ekonomin

Tillgången på data ökar ständigt och data har blivit en strategisk resurs för utveckling och digital innovation. God tillgång till data utgör en allt viktigare förutsättning för ökad konkurrenskraft, hållbar tillväxt och minskad resursåtgång. Data kallas därför för bränslet i den digitala ekonomin. I oktober 2021 presenterade Regeringen en strategi¹ (uppdaterad 2022) och som syftar till att öka tillgången till data för bland annat artificiell intelligens (AI) och digital innovation i Sverige. Målet är att Sverige till år 2030 ska vara ”bäst i världen på att tillämpa digitaliseringens möjligheter” och strategin tar avstamp från EUs datastrategi² och OECDs rekommendationer³ om ökad datadelning.

EUs datastrategi antogs av kommissionen 2020 och innehåller en vision för hur EU:s inre marknad för datadelning mellan länder, branscher och företag ska växa fram. Grunden i strategin är att data används på ett sådant sätt att individens intressen sätts i centrum, i enlighet med europeiska värderingar, grundläggande rättigheter och regler. Tanken är att om allmänheten kan lita på att datadelning sker sjyst och i enlighet med gällande rätt kommer den att vilja dela med sig av data, vilket i sin tur främjar innovation. Datadrivna innovationer kommer att medföra ytterligare fördelar för allmänheten, vilket i sin tur kommer att innebära att allmänheten är villig att dela med sig av ännu mer data. På så sätt ska den inre marknaden växa fram.

Mängden data globalt förväntas öka med 530 % mellan 2018 och 2025, samtidigt som det ekonomiska värdet baserat på data förväntas uppgå till 829 miljarder Euro i de 27 EU-länderna (figur 1). Samtidigt uppskattas att 80 % av framtagna industridata aldrig används⁴.



Figur 1. I EU:s datastrategi² beräknas ökningen av den globala datavolymen öka med 530 % mellan 2018 och 2025, samtidigt som dataekonomins värde uppnår 829 miljarder Euro.

¹ Data för ett kunskapsbaserat och innovativt Sverige (regeringen.se)

² EU:s datastrategi - Europeiska kommissionen (europa.eu)

3 Enhancing Access to and Sharing of Data | OECD

⁴ [Dataakten: åtgärder för en rättvis och innovativ dataekonomi \(europa.eu\)](https://european-council.europa.eu/media/400000/attachment/data/123456789/123456789.pdf)

En värdefull datamängd utgörs av data som är förknippat med stora fördelar för samhället, miljön och ekonomin i och med att data finns tillgängliga för många och går att använda för att skapa digitala tjänster och applikationer.

Ur: Värdefulla datamängder, DIGG

1.1 Värdefulla data i areella näringar

Värdefulla datamängder⁵ omfattas av en särskild reglering i öppna data-direktivet⁶ och i öppna datalagen⁷. Värdefulla data delas upp i följande tematiska kategorier:

- Geospatiala data (kartor, bilder, fastigheter)
- Jordobservation och miljö (geologi, skyddade områden och miljöobservationer, växtlighet och arter)
- Meteorologiska data
- Statistik (befolkning, ekonomiska indikatorer)
- Företag och företagsägande
- Rörlighet (fordon, trafik, transportnätverk)

Lantmäteriet (2020)⁸ fick i uppdrag att analysera de samhällsekonomiska nyttorna av att tillgängliggöra värdefulla datamängder på kort och lång sikt. Studien identifierar 20 användningsområden inom fem sektorer, inklusive areella näringar, där mervärdet av att tillgängliggöra de föreslagna datamängderna uppskattas till 10–21 miljarder kronor.

Inom areella näringar beräknas värdet till 1100–2870 miljoner kronor årligen. Geospatiala data (exempelvis kartor, bilder och fastighetsregister) och positionering kan möjliggöra mer effektivt nyttjande av jord- och skogsbruksmark. Datamängder som fastighetsdata, geodetiska data, jordartsdata, artobservationer, rödlistade djur och växter, satellitbilder samt bild- och höjddata bedöms även kunna bidra särskilt till arbetet med FN:s miljö- och klimatmål i Agenda 2030 och de 17 hållbarhetsmålen.

Data från lantbruksbranschen betraktas, liksom data från många andra branscher, som värdefull och det pågår en kamp om kontrollen över dessa data. På EU-nivå finns intresse av att öka lantbrukares datasjälvständighet och möjligheter att tjäna pengar på sin data. Samtidigt ökar lagkraven på lantbrukare att tillhandahålla data för kontroller och statistiska beräkningar⁹.

⁵ [Värdefulla datamängder | Digg](#)

⁶ [Öppna data-direktivet - Regeringen.se](#)

⁷ [Vägledning om öppna datalagen | Digg](#)

⁸ [slutrapport---tillgangliggorande-av-sarskilt-vardefulla-datamangder.pdf \(lantmateriet.se\)](#)

⁹ European Partnership “Agriculture of Data” - Unlocking the potential of data for sustainable agriculture - Strategic Research and Innovation Agenda. Version of 18 March 2023
[e0470eed-b1a6-4040-92c7-63835d5d3b80_en \(europa.eu\)](#)

1.2 Möjligheter med data och digital teknik i lantbruket

Digitalisering av lantbruket innebär att man använder digitala teknologier i olika delar av lantbruket, som odling, förvaltning och försörjningskedjor. Målet är att modernisera och förbättra lantbruksprocesser med hjälp av data och teknik. Eftersom digitalisering täcker så många områden inom lantbruk och livsmedelssystem, har det uppstått flera relaterade begrepp som betonar olika aspekter av digital teknik och digitaliseringsprocessen. Det finns inga specifika kriterier för att avgöra vad som utgör digitala jordbruksteknologier.¹⁰

Med tillgång till lantbruksdata kan AI och maskininlärningsmetoder leda till en rad förbättringar och innovationer, såsom förbättrade fjärranalysprodukter, jordbruksmodeller, bättre hantering av leveranskedjor, smartare policyövervakning och tillämpningar i närliggande sektorer som turism, hälsa, finans och försäkring. AI spelar en avgörande roll i att analysera stora mängder data och identifiera mönster. Detta är särskilt användbart för att förutsäga skadedjur och sjukdomar, optimera skördar, förbättra beslutsfattandet och automatisera arbetet. Inom jordbrukssektorn ökar användningen av automatisering, inklusive autonoma traktorer och maskiner.

Exemplen nedan beskriver några fördelar med data och digital teknik i lantbruket¹¹:

1. **Produktionsoptimering:** Inkluderar information om var, hur och i vilken mängd mat produceras, samt användning av resurser som vatten och energi för att optimera verksamheten och ge ökad konkurrenskraft. Ett exempel är precisionsjordbruk som med hjälp av GPS-teknik, möjliggör exakt plantering och applicering av gödsel- och bekämpningsmedel, vilket minimerar resursslöseri och förbättrar skördarna.
2. **Förbättrat djurskydd:** Sensorer och datainsamlingstekniker på betesmark och i djurstallar gör det möjligt att övervaka djurhälsa i realtid, vilket kan bidra till att öka djurens välbefinnande.
3. **Förbättrade arbetsvillkor:** Med hjälp av uppkopplade sensorer och automation kan producenter övervaka och styra utrustning och maskiner i realtid, vilket minskar den fysiska arbetsbelastningen. Detta kan även hjälpa till att minska den psykiska arbetsbelastningen genom att förutsäga när tillsyn och underhåll behövs, vilket minskar driftstopp och ökar produktiviteten.
4. **Distributions- och logistikdata:** Genom att analysera data från transport- och distributionskedjan skapas insikt i hur maten transporteras, lagras och distribueras. Det kan hjälpa företag att identifiera ineffektivitet, förutsäga flaskhalsar och optimera rutter. Detta kan i sin tur hjälpa till att minska transportkostnader och koldioxidutsläpp.

¹⁰ Klerkx, L., Jakku, E., & Labarthe, P. (2019). A review of social science on digital agriculture, smart farming and agriculture 4.0: New contributions and a future research agenda. *NJAS - Wageningen Journal of Life Sciences*, 90-91, Article 100315. <https://doi.org/10.1016/j.njas.2019.100315>

¹¹ [Digitaliseringen av den europeiska jordbrukssektorn | Shaping Europe's digital future](#)

5. **Miljö- och hållbarhetsdata:** Ger insikt i hur livsmedelsproduktion och -distribution påverkar miljön, vilket kan leda till förbättringar som minskar miljöpåverkan och göra det lättare för konsumenter att göra medvetna val. Genom att samla in data om resursanvändning och miljöpåverkan kan företag övervaka och förbättra sin hållbarhetsprofil.
6. **Försäljnings- och marknadsdata:** Genom att analysera försäljningssiffror, priser och trender kan företag förutse konsumenternas köpbeteende, efterfrågan och preferenser och justera sin leverans därefter. Digitaliseringen påverkar också hur lantbrukare marknadsför och säljer sina produkter, genom marknadsplatser och plattformar kan de nå en bredare kundbas och diversifiera sina intäktskällor. Detaljhandlare kan skapa skräddarsydda erbjudanden och rabatter, vilket ökar kundlojaliteten och försäljningen.
7. **Förbättrad spårbarhet** Data från hela livsmedelskedjan kan knytas samman med datadrivna lösningar, så produkter kan spåras snabbt genom hela kedjan. Det ökar transparensen och förtroendet hos konsumenterna och minskar risken för fusk med ursprung och innehåll.

Digitalisering förändrar i grunden hur mat produceras och hanteras. Genom avancerade teknologier och digitala lösningar kan lantbrukare optimera sina metoder, öka produktiviteten och främja hållbarhet. Men för att dra full nytta av digitaliseringen måste datakällor och system kunna kommunicera och dela data.

1.3 Hinder för användning av digitala verktyg och data i lantbruket

Användningen av digitala teknologier inom lantbruket har ökat både i mängd och variation. Införandet har däremot varit ojämnt fördelat, både mellan och inom länder och produktionssystem, beroende på lantbrukarnas och jordbrukssektorns egenskaper¹². Det finns flera hinder för att fullt ut implementera digital teknik i jordbrukssektorn¹³.

Det kan finnas stora **initiala kostnader och bristande kostnadseffektivitet** för att investera i, implementera och regelbundet underhålla digitala verktyg. Vissa lantbrukare saknar **tillgång till nödvändig infrastruktur** eller har **inte tillräcklig kunskap** för att effektivt använda digitala teknologier. Brist på tillförlitlig och överkomlig internetanslutning i landsbygdsområden hindrar inte bara införandet av ny teknik utan begränsar också lantbrukarnas tillgång till viktig information och resurser. Regeringen satsar nu 3,8 miljarder kronor på nya bredbandsprojekt under 2024–2027¹⁴. Målet är att alla, oavsett var i landet man bor, ska ha tillgång till snabbt och pålitligt bredband.

Det finns få bevis i lantbruket för hur digitala teknologier påverkar arbete, färdigheter, arbetskvalitet, eller lantbrukarnas arbetstillfredsställelse och välbefinnande i

¹² Campi, M., et al. (2024), "The evolving profile of new entrants in agriculture and the role of digital technologies", *OECD No. 209*, OECD Publishing, <https://doi.org/10.1787/d15ea067-en>.

¹³ [Digitaliseringen av den europeiska jordbrukssektorn | Shaping Europe's digital future](#)

¹⁴ [Ett effektivare bredbandsstöd på väg - Regeringen.se](#)

allmänhet¹⁵. Det behövs fler **relevanta exempel** på vilken nytta användningen av tekniken kan generera. Tekniken behöver även bli mer användarvänlig, robust och pålitligt, det vill säga att den klara att göra jobbet. Ekonomiska incitament som subventioner kan hjälpa till att balansera kostnaderna och fördelarna med digitalisering.

Något som blir allt viktigare vid insamling av data är att det finns en **teknisk flexibilitet**. Det innebär att system och sensorer bör vara utbytbara för att undvika inlåsnings effekter och säkerställa att man kan byta leverantörer eller teknik vid behov. **Datakvalitet** är avgörande för att effektivt hantera och analysera information inom jordbruks- och livsmedelssektorn. Höga standarder för datakvalitet säkerställer att informationen är tillförlitlig, exakt och relevant, vilket i sin tur underlättar bättre beslutsfattande och optimering av processer.

Interoperabilitet innebär att olika system och organisationer kan utbyta och använda information på ett effektivt och enhetligt sätt. Data som är relevanta för utvecklingen av databaserade lösningar inom lantbruket finns bland annat i flera offentliga och privata databaser. Bristande interoperabilitet försvårar datadelning, såväl inom offentlig förvaltning som med externa aktörer, vilket försvårar gemensam bearbetning och beräkning samt leder till ineffektivitet och sämre datakvalitet. För att förbättra interoperabiliteten behövs ett tydligt och sammanhängande regelverk som gäller för all offentlig förvaltning¹⁶.

2 Data som delas

Det finns en stor potential med att dela data, men för att aktörer ska våga dela sin data krävs att det finns förtroende för att det sker på ett korrekt sätt och att det genererar värde tillbaka till de aktörer som delar med sig av sin data. Det är också viktigt att ta ställning till om data alls ska delas eller inte, och i så fall under vilka förutsättningar den ska delas.

2.1 Öppna och licensierade data

Data kan göras mer eller mindre tillgänglig för delning. Vissa data är intern och ska endast vara tillgänglig inom organisationen. Annan data kan vara licensierad, vilket innebär att den kan göras tillgänglig för specifika parter under vissa villkor, där juridiska avtal reglerar användningen av data för motparten.

Öppna data är data som är fritt tillgänglig för alla att använda, återanvända och sprida utan begränsningar. Detta innebär att alla, inklusive privatpersoner, organisationer och företag, har rätt att använda och återanvända data för att skapa nya innovationer, analysera trender och fatta informerade beslut. Vanligtvis ska öppna data vara i maskinläsbart format enligt förbestämda standarder. Fördelarna med öppna data

¹⁵ Comi, M., F. Becot and C. Bendixsen (2023), "Automation, Climate Change, and the Future of Farm Work: Cross-Disciplinary Lessons for Studying Dynamic Changes in Agricultural Health and Safety", International Journal of Environmental Research and Public Health, Vol. 20/6, p. 4778, <https://doi.org/10.3390/ijerph20064778>.

¹⁶ [En reform för datadelning, SOU 2023:96](#)

inkluderar ökad transparens. Däremot måste vi skydda och klassificera data för att förhindra läckage av känslig information. Det är bra att vara medveten om att **även öppna data kan vara licensierad och rättighetsmärkt**.

Användningsområden för öppna data inkluderar forskning och utbildning, skapande av nya tjänster, produkter och innovationer, samt möjliggörande av ökad transparens och ansvarsskyldighet. Man kan hitta vägledning och öppna data på Sveriges Dataportal¹⁷ samt Statistikdatabasen¹⁸. Exempel på typer av öppna data är kartdata, väderdata, transportdata, ekonomiska data och statistik. Exempel på öppna data i livsmedelskedjan som finns tillgänglig är bland annat information om livsmedelsverksamheter, matsvinn, livsmedelsinköp, viss försäljning av växtskyddsmedel och mineralgödsel. På europeisk nivå finns exempelvis Europeiska Dataportalen¹⁹ som samlar öppna data från offentliga förvaltningar i hela EU. En annan plattform som gör det lättare att hitta, återanvända och dela offentlig information om hälsodata är PublicData.eu. Organisationen Open Knowledge Foundation²⁰ erbjuder verktyg och rådgivning för öppna data. Öppna data är en viktig resurs för forskning, innovation och förbättring av samhällstjänster.

2.2 Informationsklassificering

Informationsklassificering är en metod för att bestämma hur känslig information är och vilka säkerhetsåtgärder som behövs för att skydda den. Känslig information, enligt dataskyddsförordningen (GDPR), är personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv.

När det gäller säkerhetsklassning av information, finns det tre huvudsakliga klasser i Sverige:

- Säkerhetsklass 1: För information vars röjande kan orsaka *mycket allvarlig* skada för Sveriges säkerhet.
- Säkerhetsklass 2: För information vars röjande kan orsaka *allvarlig* skada för Sveriges säkerhet.
- Säkerhetsklass 3: För information vars röjande kan orsaka *skada* för Sveriges säkerhet.

Det finns olika modeller för informationsklassificering, från enkla till mycket avancerade. En effektiv informationsklassificering hjälper organisationer att förstå vilken data som kan delas och under vilka villkor.

KLASSA²¹ från SKR är ett verktyg som hjälper organisationer att systematiskt arbeta med informationssäkerhet. Även MSB har metodstöd för systematiskt

¹⁷ [Sveriges Dataportal](#)

¹⁸ [Kom igång med Statistikdatabasen \(scb.se\)](#)

¹⁹ [Den officiella portalen för europeiska data | data.europa.eu](#)

²⁰ [Open Knowledge Foundation – For a fair, sustainable and open future \(okfn.org\)](#)

²¹ [KLASSA \(skr.se\)](#)

informationssäkerhetsarbete²². Metodstödet bygger på standardserien ISO/IEC 27000 och består av fyra metodsteg:

1. **Identifiera och analysera:** Här identifieras och analyseras informationstillgångar och deras värde för organisationen.
2. **Utforma:** Detta steg inkluderar att skapa en klassningsmodell och välja säkerhetsåtgärder.
3. **Använda:** Implementering av säkerhetsåtgärder och utbildning av personal.
4. **Följa upp och förbättra:** Kontinuerlig övervakning och förbättring av informationssäkerhetsarbetet.

För att klassa information använder man en klassningsmodell som består av en klassningsmatris och stödmaterial. Värderingen av information görs utifrån vilka konsekvenser otillräckligt skydd av informationen skulle kunna få för organisationen.

För att skydda känslig information används integritetsskyddande teknologier som kryptering, anonymisering och syntetiska data, vilka beskrivs närmare i Avsnitt 6. Dessa teknologier hjälper till att ta bort eller maskera känslig information innan data delas.

2.3 Standarder för datainsamling och datadelning

För att kunna dela data effektivt är det viktigt att ha en struktur. Detta inkluderar att komma överens om standarder för hur data ska se ut och hur den ska delas. Genom att ha tydliga ramverk och standarder kan man skapa en miljö där data delas effektivt och nya tjänster kan utvecklas, vilket i sin tur kan leda till både kostnadsbesparingar och nya affärsmöjligheter.

Det är viktigt att ha standarder för att beskriva data på ett enhetligt sätt, så att olika system kan kommunicera med varandra. Ett exempel på detta är MIMS (Minimum Interoperability Mechanism), som syftar till att beskriva tjänster på ett minimalt men tillräckligt sätt.

Inom olika branscher och discipliner i Europa finns det en mängd olika standarder för datainsamling och datadelning. Dessa standarder spelar en avgörande roll i att strukturera och organisera data på ett sätt som gör det möjligt för system att effektivt interagera med varandra. Här är ett urval av de mest framträdande standarderna:

Open Data Protocol (OData): Denna standard är utformad för att publicera och konsumera datamängder över internet. Den används ofta för att få åtkomst till data från olika källor som databaser, webbtjänster och molntjänster. Ett exempel på dess användning är datamängder om miljö och klimatförändringar som publiceras av Europeiska Miljöbyrån.

²² [Metodstödet \(msb.se\)](https://www.msb.se/metodstod)

JavaScript Object Notation (JSON): JSON är en standard för att presentera data i ett strukturerat format. Den används vanligen för webbtjänster och NoSQL-databaser. Ett exempel på dess användning är databaser över kulturarv i Europa.

Extensible Markup Language (XML): XML används för strukturerad dataöverföring och lagring i relationella databaser. Ett exempel på dess användning är Europeiska Patentsökningen som publiceras av Europeiska Patentverket.

Comma Separated Values (CSV): CSV presenterar tabelldata i textformat och används ofta för kalkylprogram. Ett exempel på dess användning är statistik över europeisk handel och import/export.

Det finns även många andra standarder. Viktigt att notera är att öppna data inte alltid följer en specifik standard, vilket gör det nödvändigt att noggrant undersöka format och dokumentation när data ska läggas till i ett system. Ett initiativ till att förebygga detta problem inom Europa är att definiera *dataområden*, som är mer utförligt beskrivet i Avsnitt 3.

2.4 Spårbarhet och standarder i livsmedelskedjan

2.4.1 Spårbara livsmedel - ett lagkrav

Spårbarhet inom livsmedelssektorn är kritisk för att säkerställa livsmedelssäkerhet, hantera utbrott av livsmedelsburna sjukdomar, förbättra leveranskedjans effektivitet och tillgodose konsumenternas ökade krav på transparens i livsmedelsproduktionen. En viktig del av livsmedelslagstiftningen är lagen om spårbarhet i livsmedelskedjan som säkerställer att livsmedel kan spåras genom hela produktions-, bearbetnings- och distributionskedjan. Detta innebär att alla livsmedelsföretag, inklusive primärproducenter, tillverkare, detaljhandlare, transportörer, matmäklare och importörer, måste ha ett system för spårbarhet. De måste kunna visa varifrån de har köpt sina ingredienser eller råvaror och till vem de har levererat sina produkter, med undantag för slutkonsumenten²³.

Spårbarheten är avgörande för att:

- Spåra osäkra livsmedel eller sådana som inte uppfyller lagkraven.
- Kunna dra tillbaka livsmedel om det uppstår problem med livsmedelssäkerheten.
- Kontrollera hela livsmedelskedjan.
- Verifiera att informationen om ett livsmedel är korrekt.

Spårbarheten omfattar två typer av information: varifrån varje produkt kommer (ursprung) och vart varje produkt skickas (destination). Detta görs genom att dokumentera och lagra information om inköp, produktion och försäljning.

²³ [Spårbarhet för livsmedel \(livsmedelsverket.se\)](https://www.livsmedelsverket.se)

Det finns ingen specifik lag som beskriver hur ett spårbarhetssystem ska *utformas*, vilket ger företag friheten att anpassa systemet efter sin verksamhets omfattning och komplexitet. I praktiken innebär det att informationen inte finns samlad på ett ställe eller i samma format, utan ofta finns lokalt lagrad hos olika aktörer. Data är ofta lagrad i olika digitala format och det är fortfarande vanligt med pappersdokument.

Det finns standarder och initiativ som stöder spårbarhet inom livsmedelsindustrin. Här är några av de mest relevanta:

- **GS1 Traceability Standard²⁴:** GS1 erbjuder en omfattande ram för att spåra rörelserna av produkter genom hela leveranskedjan. Denna standard hjälper företag att uppfylla regulatoriska krav och förbättra kvalitet och effektivitet. Det inkluderar användning av GS1:s unika identifikationsnummer, streckkoder och RFID-teknik för att säkerställa att varje produkt kan spåras från produktion till slutlig konsumtion.
- **ISO 22005:** Detta är en internationell standard för spårbarhet i foder- och livsmedelskedjor. Den specificerar principer och grundläggande krav för utformning och implementering av ett spårbarhetssystem som kan tillämpas på alla stadier av produktion, bearbetning och distribution.
- **TRACE (Traceability for Sustainable Trade)²⁵:** Detta är ett initiativ utvecklat av United Nations Economic Commission for Europe (UNECE) snarare än en standard, som syftar till att använda spårbarhetstekniker för att stödja hållbara handelspraxis. Det fokuserar på att säkerställa att produkter har producerats under rättvisa och hållbara förhållanden och att produktionsdata är transparenta och tillgängliga.

Genom att följa dessa spårbarhetsstandarder och initiativ kan företag inom livsmedelsindustrin inte bara förbättra sin produktionskvalitet och effektivitet utan också bygga starkare relationer med konsumenter genom att erbjuda större transparens och ansvarighet i sina leveranskedjor.

2.4.2 Brist på standarder för lantbruksdata

För att datadelning ska vara effektivt måste det finnas standarder för hur data samlas in, lagras och delas. Detta är nödvändigt för att säkerställa interoperabilitet och skalbarhet. Utan standardisering, som säkerställer att alla system följer samma regler och dataformat, blir det svårare att jämföra och kombinera data från olika källor.

Livsmedelssektorn har problem med att olika system och aktörer inte använder samma datastandarder. Detta leder till att data inte alltid är konsekvent och att det är svårt att integrera data från olika källor. Olika organisationer använder olika format och definitioner, vilket gör det svårt att analysera och dela information effektivt.

Datadelning leder i sig inte till att nyttor realiserar. Det är först när data som delas också kan användas som nyttor kan realiserar.

För att lösa dessa problem arbetar nu Standardiserings-kommittén Datadrivna jordbruks- och livsmedelssystem, som leds av Svenska institutet för standarder (SIS), med att ta fram standarder för jordbruks- och livsmedelsdata. Kommittén kommer att arbeta direkt med den internationella kommittén ISO/TC 347 "Data-driven Agrifood

²⁴ [GS1 Global Traceability Standard](#)

²⁵ [Traceability for Sustainable Trade](#)

systems" och därigenom bevaka svenska intressen och påverka internationella standarder inom området.

2.5 Möjligheter och utmaningar med datadelning

2.5.1 Datadelning mellan företag

Sitra, den finska innovationsfonden, har utforskat potentialen och fördelarna med datadelning mellan företag och organisationer²⁶. Enligt deras forskning kan datadelning leda till en rad positiva utfall, inklusive bättre produkter, tjänster och insikter. Genom att dela data kan företag öka sin innovationskapacitet, vilket i sin tur kan leda till utvecklingen av nya lösningar och tjänster. Dessutom kan tillgång till mer omfattande och varierade data förbättra kundupplevelsen. Företag kan skraddarsy sina tjänster och produkter för att bättre möta kundernas individuella behov och förväntningar, vilket kan leda till ökad kundlojalitet och affärsframgång. Datadelning kan också bidra till effektivare beslutsfattande. Med tillgång till mer och bättre data kan företag fatta mer informerade beslut, vilket kan leda till bättre affärsresultat.

Trots de många fördelarna finns det också utmaningar som måste övervinnas för att fullt ut dra nytta av datadelning. Säkerhet är en av de mest kritiska aspekterna, särskilt när det gäller delning av personlig information. Företag och organisationer måste implementera robusta säkerhetsåtgärder för att skydda data och bygga förtroende bland användare.

2.5.2 Delning av lantbruksdata

Livsmedelskedjan utgör en omfattande, delvis samhällskritisk, kedja som involverar flera aktörer, från lantbrukare och förädlare till distributörer, återförsäljare och konsumenter. Kedjan är fragmenterad och består av en mängd olika slags aktörer, små som stora, och privata som offentliga. Detta gör samordning och delningen av data komplicerad.

Globaliseringen bidrar till komplexiteten genom ökad internationell handel av livsmedel, som kräver kvalitetskontroll och överensstämmelse med internationella standarder. Dessutom är hållbarhetsfrågor, inklusive miljö- och klimatpåverkan, centrala och kräver att hela livsmedelskedjan anpassar sig för att minska klimatavtrycket.

All denna komplexitet ökar behovet av att dela data för att effektivisera livsmedelskontroller, minska fusk och synliggöra klimatpåverkan och göra det möjligt för konsumenterna att välja klimatsmarta alternativ.

²⁶<https://www.sitra.fi/en/articles/better-products-services-and-insight-data-sharing-networks-reap-rewards-of-collaboration/>

2.5.3 Delning av myndighetsdata

Det ställs höga krav på myndigheter relaterade till livsmedelsförsörjning, eftersom de har stort ansvar för att säkerställa livsmedelstillgången i landet. Myndigheters informationshantering regleras av särskilda lagkrav, samlade i offentlighets- och sekretesslagen, säkerhetsskyddslagen, dataskyddsförordningen, arkivlagen och flera andra regelverk. För att myndigheter och andra organisationer ska kunna bidra till ökad datadelning behöver deras interna IT-verksamheter parallellt gå mot en mer öppen inriktning mot datadelning.

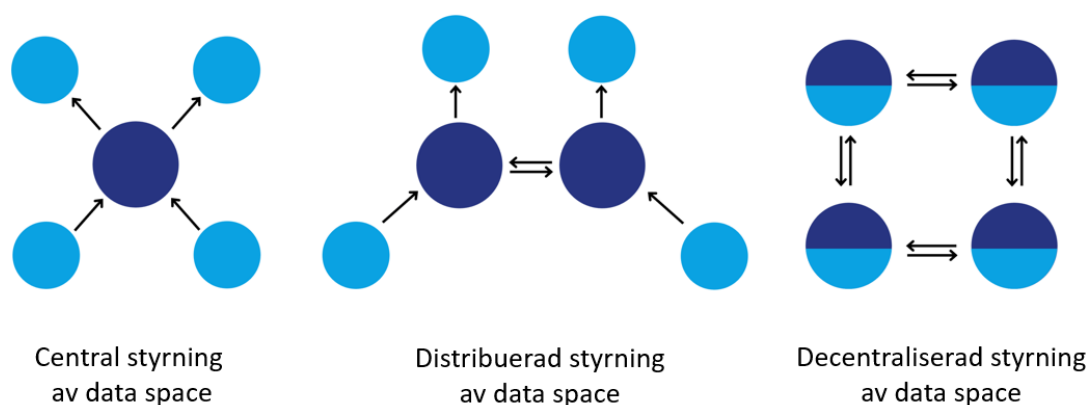
En viktig aspekt är att datadelning gör det möjligt att sammanställa information om hur livsmedelsproduktion och livsmedelsförsörjningen ser ut i landet. I det finns både en ekonomisk risk, att olika aktörer kan anpassa sina priser när de känner till utbudet, och en beredskapsrisk, att annan makt kan få för mycket information. Detta gör att tillgång till data behöver styras noga, inte bara vilken data utan också till vilka som får tillgång till olika sorters data och hur stor andel av hela datasetet som exponeras.

3 Verktyg och plattformar för datadelning

3.1 Dataområden förbinder dataplattformar

Inom EU börjar man nu se på att dela data i en kedja som föråldrat och i EUs senare regelverk för olika sektorer delas data till en central punkt – likt ett hjulnav med ekrar (figur 2). Enligt EU:s definition är “data space”, eller dataområden på svenska, en decentraliserad infrastruktur där olika aktörer kan dela och använda data på ett säkert, pålitligt och förtroendefullt sätt. Detta sker genom att följa gemensamma styrningsmekanismer samt, organisatoriska, reglerande och tekniska mekanismer²⁷. Dataområden är tänkta att förbinda data lokaliserade i olika dataplattformar. Gemensamma europeiska dataområden har som mål att göra mer data tillgänglig för åtkomst och återanvändning i en tillförlitlig och säker miljö för att gynna europeiska företag och medborgare²⁸.

Inom EU pågår ett arbete med målet att skapa en grund för en gemensam datainfrastruktur för jordbruket²⁹, Common European Agricultural Data Space (CEADS) Gemensamma Europeiska Jordbruksdataområdet. Dataområdet syftar till att stödja pålitlig datadelning inom sektorn och utvecklingen av gemensamt överenskomna affärs- och styrningsmodeller. En specifik strategi för datadelning inom sektorn håller på att utvecklas, med hänsyn till de förändrade förutsättningarna som skapas av Dataförordningen, Dataförvaltningsförordningen samt erfarenheterna från uppförandekoden för jordbruksdatadelning³⁰ genom avtalsöverenskommelser.



Figur 2 Olika modeller för styrning av data spaces (datautrymmen)³¹.

²⁷ [1.3 Definitions - JRC Data Spaces Knowledge Base - EC Public Wiki \(europa.eu\)](#)

²⁸ [Common European Data Spaces | Shaping Europe's digital future \(europa.eu\)](#)

²⁹ [AgriDataSpace](#)

³⁰ [EU Code of conduct on agricultural data sharing by contractual agreement 2020 E NGLISH.pdf](#)

³¹ [Functional Requirements | IDSA Rulebook | IDS Knowledge Base \(internationaldataspaces.org\)](#)

3.2 Dataplattformar i livsmedelskedjan

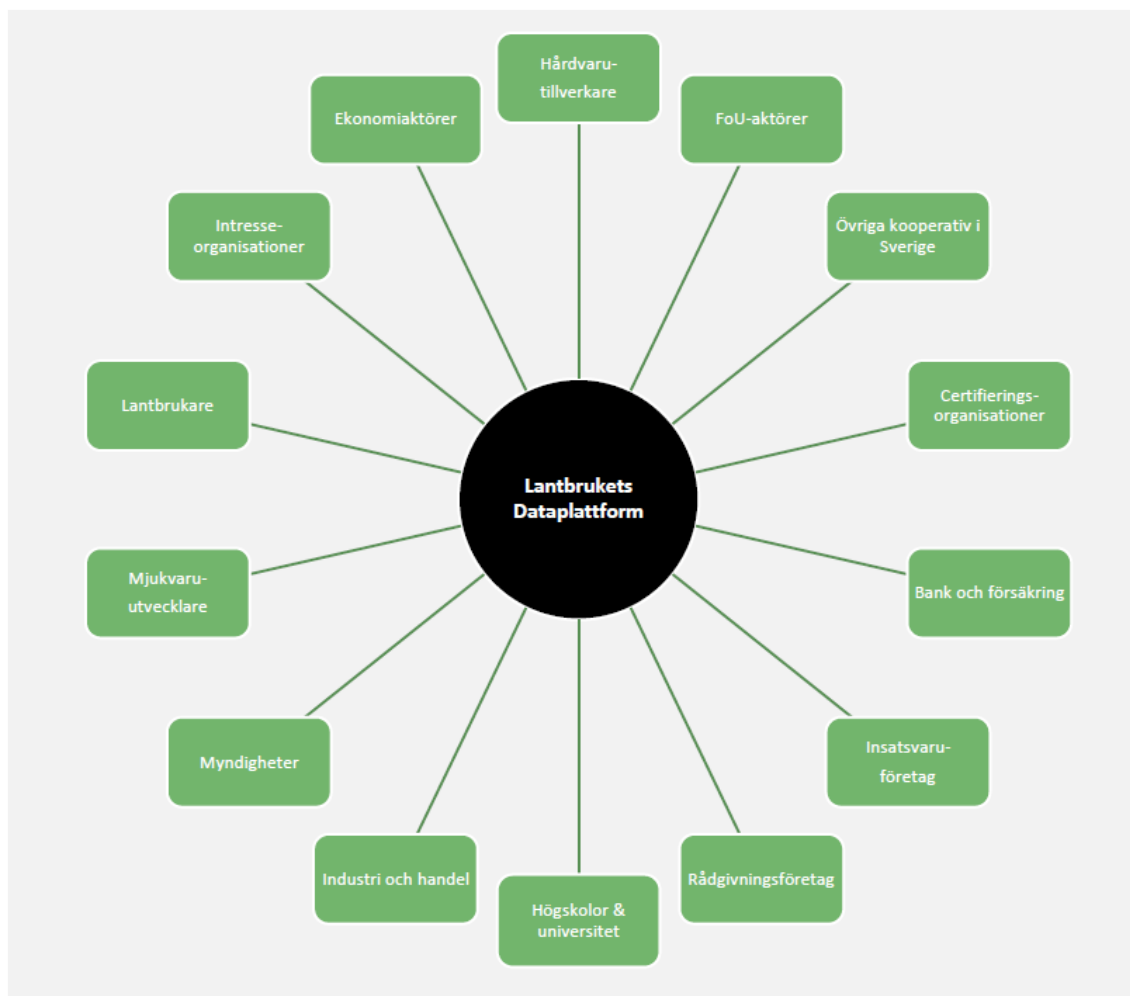
Runt om i Europa och Sverige byggs olika plattformar upp för att hantera lantbruksdata. Utöver dessa pågår också flera olika satsningar och projekt inom EU för att stödja jordbrukets datahantering som dels berör hur det datadrivna jordbruket kan understödjas regulatoriskt från EU, dels om olika projekt som utvecklar samarbeten och infrastruktur.

3.2.1 Lantbrukets dataplattform (Sverige)

I Sverige pågår en satsning på en nationell databasinfrastruktur för lantbruket (Agronod³²) som ägs av Hushållningssällskapet, Lantmännen, LRF, Växa Sverige, Arla och Scan Sverige och som delvis finansierats med offentliga medel via Jordbruksverket och EU. Tanken är att Agronod ska bli en samhällskritisk infrastruktur med stort allmänt värde som fungerar som ett nav för lantbruksdata (figur 3). Agronod-plattformen ger lantbrukare full kontroll över sin gårdsdata. Detta inkluderar möjligheten att verifiera gårdsnära mervärden med hjälp av data. Plattformen minskar behovet av manuell inmatning och administration, vilket sparar tid och resurser, och den möjliggör även för företag och organisationer att utveckla nya lösningar som stärker svenskt lantbruk och livsmedelsproduktion. Plattformen följer en rad riktlinjer, krav, principer, strategier, byggblock etc. från Sverige och från EU, för att inte skapa olika typer av inlåsningsbarrierar.

Just nu finns följande dataintegrationer till plattformen, men flerdatakällor håller på att integreras; Dataväxt (odlingsdata), Växa MinGård (mjölk- och köttproduktionsrelaterade data), Scan (slaktdata), NorFor (fodermedels näringsmässiga sammansättning), Lantmännen (produktdata) och Markkartering (markkartering och styrfiler).

³² <https://www.agronod.com/plattformen>



Figur 3 Lantbrukets dataplattform ska fungera som ett nav för jordbrukets data i Sverige³³.

3.2.2 Exempel på andra initiativ runt datadelning

DjustConnect³⁴ är en neutral plattform för datautbyte inom jordbruket som tillhandahålls av institutet ILVO i Belgien. Plattformen är utformad för att vara neutral och drivs inte av kommersiella intressen. All datadelning sker med respekt för dataägarnas rättigheter och integritet.

I Frankrike finns företaget Agdatahub³⁵ som har en plattform för att distribuera jordbruks- och livsmedelsdata som kan koppla samman olika datakällor och system för att underlätta integration och tillgång till data. Ambitionen har varit att tillsammans med offentliga och privata aktörer tillhandahålla jordbruket en gemensam, suverän, teknisk infrastruktur för delning av jordbruksdata, men företaget behöver säkra ytterligare offentlig finansiering för sin överlevnad. Agdatahub har utvecklat verktyget

³³ Jordbruksverket (2022) "Förstudie: Förslag till nationellt kunskapsnav för digitaliserat jordbruk". <https://jordbruksverket.se/download/18.dcef483186ae4990be47c4f/1678087452820/Forstudie-digitaliserat-jordbruk.pdf>

³⁴ DjustConnect

³⁵ <https://agdatahub.eu/en/>

Agriconsent³⁶, som är ett decentraliserat digitalt identitetssystem baserat på blockkedjeteknologi. System gör det möjligt för lantbrukare att säkert autentisera och kontrollera utbytet av data relaterat till jordbrukspraxis eller miljödata och tekniska data.

I Finland finns Tritom® som är en dataförmedlingstjänst som utvecklats av DataSpace Europe³⁷. Plattformen fungerar både som ett ekosystem och en integrationsplattform, där utvecklare av databaserade tjänster möter datainnehavare och där data kan utbytas enligt regler som överenskommits av ekosystemet. Användarna av tjänsten förbinder sig att följa dess regelbok, dvs gemensamma regler för ekosystemet, som följer principerna för en rättvis dataekonomi. Ingen data som förmedlas genom Tritom lagras, utan överförs endast, och överförda data krypteras och dekrypteras med hjälp av AES-standard³⁸ (Advanced Encryption Standard).

Ett sektorsspecifikt exempel på dataplattform är International Dairy Data Exchange Network³⁹ (iDDEN). iDDEN är det största internationella partnerskapet för mejeridata och representerar cirka 200 000 mejeribesättningar och 20 miljoner mjölkkor. Nätverket ägs och styrs av ett konsortium av medlemsorganisationer som kontrolleras av bönder och som tillhandahåller datatjänster för mejeriindustrin i länder som Australien, Österrike, Belgien, Kanada, Danmark, Tyskland, Island, Finland, Luxemburg, Norge, Sverige (Växa Sverige), Nederländerna och USA. Nätverket har utvecklat en standardiserad gränssnittstjänst som kallas Nordic Cattle Data Exchange⁴⁰ (NCDX), vilken löser gemensamma problem med informationsutbyte mellan gårdar, mjölkregistrering och leverantörer av mjölkrobotar och mjölkkningsutrustning.

Antalet initiativ för att dela data ökar hela tiden och allt fler företag ser nyttan med att dela data. För fler exempel på dataplattformar i jordbruket, se referens⁴¹.

³⁶ [cp_agdatahub_final_en.pdf](#)

³⁷ [Tritom - Data Intermediation Service | DataSpace Europe](#)

³⁸ [FIPS 197, Advanced Encryption Standard \(AES\) \(nist.gov\)](#)

³⁹ [iDDEN - International Dairy Data Exchange Network](#)

⁴⁰ [Comments to current proposition \(icar.org\)](#)

⁴¹ [Slutrapport förstudie databasinfrastruktur för jordbruket.pdf](#)

4 Datadrivna innovationer i livsmedelskedjan

Utvecklingen av datadrivna tjänster går just nu mycket fort, men begränsas fortfarande till viss del av tillgången på data. Ju mer data som tillgängliggörs, desto fler innovationer kommer att utvecklas. En viktig faktor för att öka tillgången på data är att visa på nyttan med att dela data.

Datadrivna tjänster utmanar och kompletterar traditionella metoder för produktion, distribution och konsumtion av mat. De bygger på insamling, analys och tillämpning av data och erbjuder innovativa lösningar för att öka effektiviteten, minska svinn och förbättra kundupplevelsen. Detta är inte bara en teknologisk utveckling, utan en fundamental förändring i hur vi närmar oss livsmedelskedjan som helhet.

I Avsnitt 4.1-4.4 listas några svenska tjänster som får exemplifiera både etablerade och nya innovationer för några av de vanligaste applikationsområdena för datadrivna tjänster i livsmedelskedjan.

4.1 Beslutsstödsystem med precisionsjordbruk och precisionsdjurhållning

Precisionsodling innebär att åtgärder som sådd, gödning och växtskyddsbekämpning i växtodlingen anpassas efter olika behov på olika platser i fältet för att få en så jämn skörd som möjligt. Det innebär också att resurserna nyttjas optimalt för att undvika onödiga läckage av kemikalier och gödningsmedel. Tekniken som används baseras på spektrala analyser från sensorer, drönare och satelliter samt exakt positionering av traktor och tröska. I Sverige erbjuder företaget *Dataväxt med flera* en rad digitala tjänster kopplade till växtodling.

Motsvarigheten inom animalieproduktion kallas för precisionsdjurhållning (PLF) där avancerade informations- och kommunikationsteknologier används för att förbättra djurvelfärd så väl som den ekonomiska och miljömässiga hållbarheten inom animalieproduktionen. Det handlar om att använda verktyg för att övervaka och styra djurproduktionen mer exakt och effektivt. Här erbjuder företag som *Agricam*, *DeLaval*, *Hencol* med flera tjänster baserade på data från animalieproduktionen.

4.2 Klimat- och hållbarhetsuppföljning

Klimatpåverkan från livsmedel beror på hur vår matproduktion och konsumtion bidrar till utsläpp av växthusgaser som koldioxid, metan och lustgas. Dessa utsläpp har en direkt påverkan på den globala uppvärmningen. En rad företag erbjuder verktyg och tjänster för att beräkna vilket klimatavtryck olika livsmedel genererar, beroende på varifrån de kommer och hur de har producerats. Klimatavtrycken är generella och inte

framtagna för specifika producenters produkter och är ett ungefärligt mått på livsmedlets klimatpåverkan.

Agronods klimatberäkningsverktyg *Agrosfär* skiljer sig från generella klimatavtrycksberäkningar genom att den möjliggör detaljerade och automatiserade klimatberäkningar baserade på riktiga data från gården. Beräkningsmodellen grundar sig på etablerade internationella standarder för klimatberäkningar, som exempelvis GHG-protokollet, men har anpassats för svenska förhållanden. Beräkningar kan göras för hela gården samt för olika produktionsgrenar som växtodling, mjölkproduktion, nötköttsproduktion och snart även för grisproduktion. Data hämtas från gårdens uppkopplade system och möjliggör detaljerad beräkning och uppföljning från år till år. Det går därför enkelt att följa den klimatiflyttning som sker baserat på de förändringar som görs på gården.

Improvin' är en plattform för hållbarhetsprestanda. Genom att samla in primärdata från bönder och använda satellitdata och algoritmer, kan Improvin' kvantifiera och verifiera utsläpp och hållbarhetsåtgärder. Bolaget jobbar idag med alla grödor som ingår i vanliga växtföljder i norra Europa.

4.3 Marknadsplatser och prisjämförelser

Det finns flera tjänster och initiativ som använder data för att förbättra transparensen och effektiviteten i livsmedelskedjan, särskilt när det gäller marknadsplatser och prisjämförelser.

Plattform Lumen från *Skira* erbjuder en oberoende marknadsplats för handel med spannmål. Lantbrukare som säljer spannmål kan jämföra priser på olika kvaliteter och tider på året både inom och utanför Sveriges gränser. Plattformen för samman säljare och köpare av spannmål där handeln sedan sker via auktion. Tjänsten ger ökad transparens genom full insyn i vad som påverkat slutpriset i form av kvalitet, läge och avstånd.

SNP Prisportal är ett nyutvecklat prisjämförelseverktyg, som hjälper nötköttsproducenter att få en bättre överblick över priset på slaktdjuren genom att publicera data på avräkningar som nötköttsproducenter skickat in till portalen anonymt. Prisportalen samlar in data om djurtyp, vikt, fett, klass och priser inklusive alla tillägg i databasen, och publicerar sedan denna data varje vecka i Skiras verktyg Lumen. Då den är slakterioberoende är det möjligt för nötköttsproducenter att jämföra sina avräkningspriser från slakterierna. Detta ger producenterna förbättrade möjligheter att förhandla fram bästa möjliga pris.

4.4 Spårbarhet av produkter längs livsmedelskedjan

På senare tid har det kommit allt fler lösningar där information om spårbarhet sparas in en blockkedja. Det kanske mest internationellt kända initiativet är IBMs privata

blockkedja *FoodTrust*⁴² som främst riktar in sig på detaljhandeln. Ett svenskt alternativ är företaget *FoodChain by Blockchain*⁴³ som är en blockkedjelösning för spårbarhet av livsmedelsprodukter, från lantbrukare till förädlare och slutligen till konsument. Blockkedjan ger möjligheter till spårbar datadelning av en produkt genom hela produktionskedjan, samtidigt som den underlättar administration och kontroll över produktionen. Färdiga lösningar finns för digital spårbarhet av drycker som öl, cider och vin och snart även för ägg. Utveckling pågår även av en tjänst att kontrollera och verifiera certifikat.

4.5 Affärs- och intäktsmodeller av datadrivna tjänster

Data som en tjänst (DaaS) inom livsmedelskedjan har potential att bli en betydande intäktskälla, särskilt i en tid då beslutsfattande i stor utsträckning är beroende av dataanalys.

En affärsmodell förklarar hur företag skapar och levererar värde. Business Model Canvas, BMC, är en verktygsmodell som skapades av Alexander Osterwalder för att underlätta skapandet av affärsmodeller. Modellen är en visuell mall som illustrerar olika delar av en affärsmodell och inkluderar nio element som representerar viktiga aspekter för ett företags överlevnad. Dessa nio element är:

1. Kundsegment
2. Värdeerbjudande
3. Distributionskanaler
4. Kundrelationer
5. Intäktsströmmar
6. Nyckelresurser
7. Nyckelaktiviteter
8. Nyckelpartners
9. Kostnadsstruktur

Denna modell används för att hjälpa företag att flytta fokus från produktcentrerat tänkande till affärsmodelltänkande. Den är användbar för både nya företag som söker rätt affärsmodell och etablerade företag som vill hantera strategier eller skapa nya tillväxtmotorer.

Lönsamheten generellt för affärsmodeller inom jordbruks- och livsmedelssektorn kan variera beroende på faktorer som geografiskt läge, marknadstillgång, teknologisk mognad och skalfördelar. Även externa faktorer som regleringar, subventioner och miljöpåverkan kan ha stor inverkan på affärsmodellens lönsamhet. Därför är det bäst att göra en noggrann analys av marknaden och de ekonomiska förutsättningarna innan man bestämmer sig för vilken affärsmodell som är mest lönsam.

⁴² [IBM Supply Chain Intelligence Suite - Food Trust](#)

⁴³ [Foodchain by blockchain - Foodchain by Blockchain](#)

4.5.1 Exempel på affärsmodeller

Genom att integrera datadrivna tjänster i livsmedelskedjan kan företag inte bara optimera sina befintliga processer utan också upptäcka nya affärsmöjligheter, skapa mervärde för sina kunder och positionera sig som ledande inom sektorn, vilket i sin tur kan leda till ytterligare affärsmöjligheter och partnerskap.

Nedan följer exempel på affärsmodeller som kan användas vid datadrivna tjänster och innovation.

Försäljning av rådata: Ett företag säljer sina råa och opolerade datamängder till andra organisationer som behöver bearbeta och analysera dem för sina specifika ändamål. Detta kan vara ett första steg, där man inledningsvis erbjuder gratis rådata för att lära känna vilket data som har ett värde.

Dataförbättring och tvättning: Förutom att erbjuda rådata kan företag också erbjuda tjänster för att förbättra, tvätta eller standardisera data för kunder som behöver mer specifik eller kvalitetskontrollerad information.

Incitament för datakvalitet från data-ägare: Ett företag belönar användare eller dataleverantörer för att bidra med högkvalitativa data genom poäng eller monetära incitament baserat på datakvalitet.

Dataaggregering och försäljning: Ett företag samlar in och bearbetar data från olika källor, aggregerar dem och säljer den aggregerade informationen till intresserade köpare.

Analys och insikter: Ett företag skapar och säljer eller ger ut detaljerade rapporter och analyser baserade på data, vilket ger insikter om prognoser, trender inom en specifik sektor, och benchmarking, exempelvis Lantmännens skördeprognoser.

Dataanalytiska tjänster: Ett företag tillhandahåller specialiserade dataanalys- och visualiseringsverktyg för att hjälpa kunder att dra insikter från de tillhandahållna datamängderna mot en avgift. Ett exempel på det är Agrosfär som beskrivits tidigare.

Anpassade rapporter: Ge användarna möjlighet att skapa skräddarsydda rapporter baserade på deras specifika behov, oavsett om det gäller att förutsäga efterfrågan, övervaka lager eller spåra produktens resa. Alternativt som analyserar specifika trender, marknadsförändringar eller konsumentbeteenden.

4.5.2 Exempel på intäktsmodeller

En vanlig intäktsmodell är att ta betalt via **direkta avgifter** från användare för tillgång till eller användning av specifika dataset. Avgiften kan vara en engångsbetalning per transaktion eller en abonnemangslösning.

Abonnemangsmodeller: En organisation kan erbjuda olika abonnemangsnivåer där användare betalar en fast avgift regelbundet (t.ex. månadsvis eller årligen) för att få tillgång till en viss mängd data eller förbättrade funktioner. En grundläggande abonnemangsnivå av datadelning kan erbjudas gratis (freemium) och sedan är det en avgift för att få tillgång till premiumfunktioner såsom uppdateringar, fördjupade insikter eller exklusiv tillgång till mer detaljerade data eller extra kapacitet. Abonnemangsmodeller används av t.ex. e-tidningar, Youtube och Spotify.

Transaktionsbaserade avgifter: En organisation tar ut avgifter varje gång en användare gör en dataförfrågan eller genomför en transaktion med hjälp av de tillhandahållna datan eller deras API. Detta kan vara baserat på antalet transaktioner eller transaktionsvärdet. Denna modell används av t.ex. Swish företagsbetalning.

EN affärsmodell kan i flera fall kombineras med **reklam och sponsringsintäkter**. Om en dataplattform blir populär och har en stor användarbas kan reklamplatser eller sponsrade innehållsmöjligheter erbjudas till företag som vill nå en specifik målgrupp.

Licensiering av data/Licensavgifter: I stället för att ge direkt tillgång kan företag licensiera sin data till andra organisationer som vill använda den i sin egen applikation, forskning eller produkt. Man tar då ut licensavgifter baserat på användningsområdet och omfattningen av användningen. Exempel på denna intäktsmodell finns hos Dataväxt (logmaster, cropMAP) och Agricam (Livsmjolk).

Partnerskap med andra företag: Flera organisationer går samman för att skapa gemensamma datatjänster eller produkter och delar intäkterna som genereras från dessa samarbeten. På så sätt kan dataanvändningen utvidgas och skapa nya intäktsmöjligheter.

Öppet API: Genom att erbjuda API-tillgång kan företag möjliggöra för tredjepartsutvecklare att bygga egna applikationer eller tjänster som drar nytta av tillgängliga data. Grundläggande öppna API:er kan exempelvis erbjudas gratis för att sedan ta betalt för premiumfunktioner eller högre användningsnivåer. Detta kallas ofta för en "freemium"-modell.

Med den insikt och expertis som kommer från att hantera och analysera data kan företag också erbjuda utbildningstjänster, seminarier eller konsultation till andra aktörer och hjälpa dem att maximera nyttan av tillgängliga datamängder.

4.6 Hinder och möjligheter för ökad datadriven innovation

Utvecklingen av datadrivna tjänster går just nu mycket fort, men begränsas fortfarande till viss del av tillgången på data. Plattformar och datadelningstjänster blir snabbt allt fler, och det blir allt enklare för aktörer som har data att dela den med andra. Ju mer data som tillgängliggörs, desto fler innovationer kommer att utvecklas. Men dessa plattformar och tjänster behöver få större spridning bland lantbrukare för att mer data ska tillgängliggöras för innovationer.

Det finns en brist på medvetenhet om möjligheterna och fördelarna med datadrivna applikationer för jordbruket. Om lantbrukare och andra aktörer inte känner till de nya möjligheterna kommer de inte att använda dem⁴⁴. Det är även viktigt att alla nya datadrivna applikationer visar en tydlig avkastning på investeringen. Den potentiella köparen av en applikation bör ha tydlig information om dess kostnader och fördelar för att kunna ta beslut om att köpa applikationen eller inte.

⁴⁴ [eip-agri seminar data revolution final report 2016 en.pdf \(europa.eu\)](#)

Lantbrukare ser ofta ett värde med att dela sin data med andra lantbrukare för att i sammanställd form kunna jämföra sin produktion med andra. Det är däremot viktigt att de har kontroll över, och förtroende för, systemet och att det inte avslöjar affärshemligheter som lantbrukarna arbetat hårt med att ta fram. Det finns också önskemål om att ta del av andra aktörers data i exempelvis värdekedjan för köttproduktion och en förståelse för att andra kan dra nytta av den data som lantbrukaren sitter på⁴⁵. Men det måste finnas en egen vinning för att lantbrukaren ska se nyttan med besväret.

Även myndigheter som enligt dataförvaltningsförordningen sedan 2023 ska underlätta storskalig delning av myndighetsdata lider av samma problem. När det är brist på resurser till verksamhetskritiska aktiviteter är det svårt att motivera varför verksamheten ska lägga tid och pengar på att dela data som inte gagnar den egna verksamheten.

4.7 Utveckling av innovationer med datadelning i Sverige

Agricultural European Innovation Partnership (EIP-AGRI) lanserades för första gången 2012 och är ett innovationsstöd inom EU:s nya gemensamma jordbrukspolitik (CAP). Syftet med stödet är att skapa fler innovativa lösningar baserade på branschens utmaningar genom bättre kopplingar mellan forskningsresultat, ny teknik och praktiskt arbete inom jordbruk, trädgård och rennärning. Det finns två typer av stöd inom EIP-AGRI; ett stöd för att bilda en innovationsgrupp och ett stöd för att genomföra ett innovationsprojekt. Innovatörer kan med full finansiering från stödet utveckla sina idéer och hitta lösningar på utmaningar.

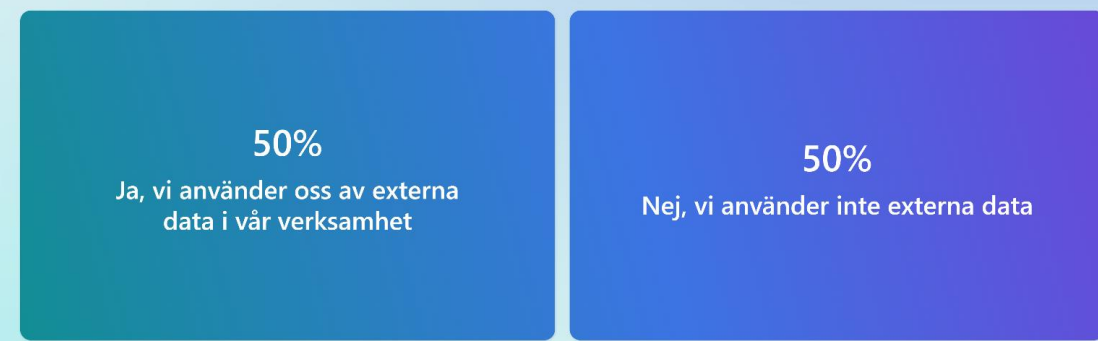
För att undersöka hur arbetet med datadrivna innovationer utvecklas inom lantbruket skickades, med hjälp av Landsbygdsnätverket, en kort webenkät ut till alla de aktörer som fått stöd från EIP-AGRI.

Enkäten handlade om *datadrivna tjänster i livsmedelskedjan* och besvarades anonymt. Som ofta är fallet vid enkätundersökningarna blev svarsfrekvensen inte särskilt hög (10 av 132 tillfrågade projekt, men där samma aktör kan ha flera projekt) och orsaken till det kan vi bara spekulera i. Det kan bero på allt ifrån brist på tid och intresse, till brist på kunskapen om vad som menas med datadrivna tjänster, eller att man inte anser sig utveckla datadrivna tjänster. Resultaten från enkäten är därmed inte vetenskapligt säkerställda, utan ska ses som en fingervisning på hur användningen av data för innovationer kan se ut i livsmedelskedjan. Vi har valt att här redovisa svaren på ett axplock av de frågor som ställdes i enkäten.

Bland de aktörer som svarade på enkäten så uppgav 5 av 10 att de konsumerar data från extern part, t.ex. myndighet eller annan organisation/företag (figur 4).

⁴⁵ A. Rydberg, C. Lindahl, L. Bark and A. Ghafoor Abbasi, 2022. Mapping information flow in the livestock supply chain for beef in Sweden. ECPLF 2022 10th European Conference on Precision Livestock Farming, p. 696-703. Vienna, Austria. 29 August - 1 September '22.

Konsumerar ni idag data från extern part, t.ex myndighet eller annan organisation/företag?



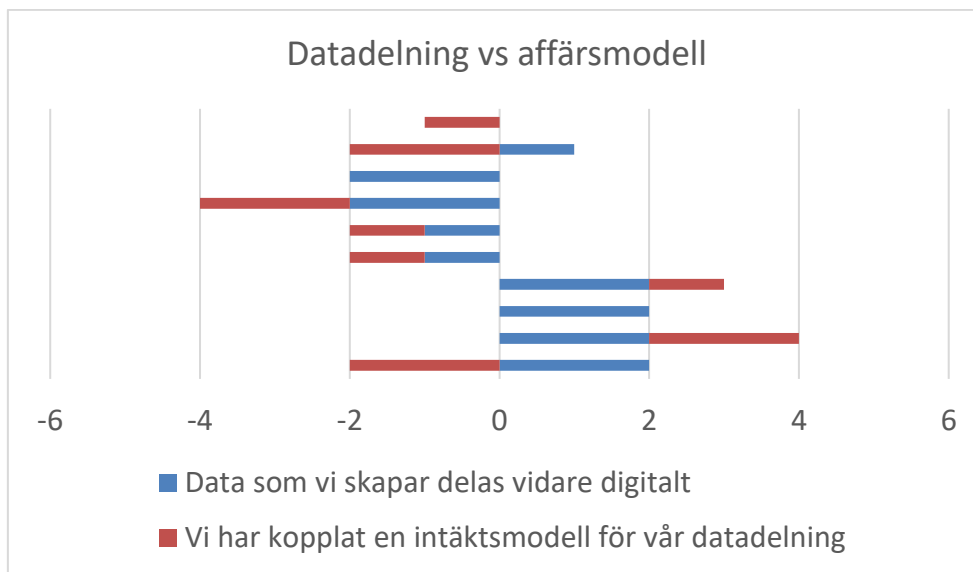
Figur 4. Hälften av de responderande innovatörerna med bidrag från EIP-AGRI säger sig dela data externt och hälften säger sig använda sig av data från extern part.

Av de som både sa sig konsumera externa data och samtidigt använda sig av externa data i sina produkter och tjänster är det knappt 2 av 5 som nyttjar data som betald tjänst. Övriga använder sig av olika former av gratistjänster. De kostnadsmodeller som angavs för data kopplad till en kostnad var att betala per transaktion eller att betala någon form av månads- eller årsavgift.

Enkäten gav inte svar på i vilken utsträckning kostnadsfria data ingår i produkter och tjänster, eller om det bara är frågan om en försumbar del. Det är även oklart om några av de som svarat på enkäten som använder gratistjänster svarat utifrån aspekten datadrivna tjänster eller enbart utifrån sin dagliga verksamhet i företaget/organisationen.

På frågan om de delar sin data externt svarade lika stor andel att de gör det. På frågan *De data/information ni delar, är det kostnadsfritt eller betald tjänst?* angav bara 2 av 5 företag som delar sin data att de tar betalt i någon form (figur 5). Det innebär eventuellt att 3 av 5 svar antingen inte utgår från datadrivna affärsmodeller utan tar avstamp i företagets egen verksamhet, eller att de inte hunnit skapa någon affärsmodell för deras innovation. Men eftersom stödet ställer krav på marknads- och affärsplaner, är det inte särskilt troligt att det är det som är orsaken. De intäktsmodeller som uppgavs här var betalar månad, årsavgift, medlemskap samt kostnad per transaktion.

Den typ av data som företagen delar idag är antingen sensor- eller produktions- och försöksdata från fält, växthus eller inomhusproduktion. Eller också är det mer marknadsorienterad data om sortiment och priser. En aktör agerar som datamäklare inom olika domäner. Det är fler som anser sig skapa data av externt värde än som faktiskt delar med sig av sin data externt. Bara två av 10 höll sig antingen neutrala eller ansåg att den data de skapade saknade externt värde. På frågan *Vilka data skulle ni vilja dela som ni inte gör idag?* angavs produktions- och försöksdata som exempel. På frågan *Vilka data skulle ni önska er som ni inte har idag?* angavs XML-filer från SAM på fält och mer data från fältförsök och inventeringar än de som samlas in och delas idag.



Figur 5. Två av tio responderande innovatörer med bidrag från EIP-AGRI säger sig både dela data externt och också ha en affärsmodell kopplat till det i någon form. Varje rad innebär en svarande innovatör. Negativa tal innebär mer eller mindre nekande svar, noll innebär varken eller och positivt svar innebär jakande svar.

Det ska det än en gång påminnas om att studien var mycket begränsad och att frågorna behöver undersökas djupare innan några statistiskt säkerställda slutsatser kan dras. Några tendenser vi trots detta tror oss se är att antalet datadrivna innovationer fortfarande är lågt i förhållande till potentialen och att det kommer finnas stor potential framöver för betydligt fler innovationer när mängden tillgängliga data ökar ytterligare och får större spridning. En reservation är att kunskapen om datasäkerhet behöver bli större allt eftersom hotbilden ökar genom ökad användning av Deep AI. Säkerhet måste därför ingå som en mycket viktig del i alla datadrivna innovationer.

5 Legala aspekter kring datadelning

Det finns många lagar och förordningar som på ett eller annat sätt påverkar hur vi delar data. De flesta har sitt ursprung från EU. Det pågår diskussioner i Sverige och EU hur offentlig sektor ska förhålla sig till lagring, hantering och åtkomst till data, med olika uppfattningar inom juridiken och inga tydliga riktlinjer.

Det pågår aktiviteter i EU med syftet att samarbeta kring gemensamma tekniska och rättsliga regler för molntjänster, samman-koppling av nationella molntjänster och molntjänstinfrastruktur samt skapandet av gemensam teknik (FIWARE, Gaia-X, SAREF m.m.) och marknadsplatser för molntjänster. Framöver kommer det alltså att finnas juridiska och tekniska riktlinjer från EU, men mycket av detta kommer inte att vara på plats innan en dataplattform driftsätts. Vi har i projektet valt att fokusera på två nya regelverk som rör data nämligen dataförvaltningsförordningen och AI förordningen då de har tillkommit under projektiden.

5.1 Digitala rättigheter och principer

EU-kommissionen ser en digital framtid som skiljer sig från utvecklingen i Kina och USA. Kommissionen vill säkerställa att människor får möjlighet att fullt ut utnyttja de möjligheter som digitalisering innebär. EU ska därför hitta sin egen väg som styrs av europeiska digitala rättigheter och principer⁴⁶ som återspeglar EU:s värden och främjar en hållbar, människocentrerad vision för den digitala omställningen. De digitala rättigheterna och principen är inte en lagstiftning utan en deklaration. Syftet med deklarationen är att påverka allt arbete under det digitala decenniet till att vägledas utifrån dessa etiska principer. De digitala rättigheterna och principerna följer här:

1. Människor i centrum för den digitala omställningen. Tekniken ska gagna och tjäna människor med full trygghet utifrån grundläggande värderingar.
2. Solidaritet och inkludering. Tekniken ska inte användas för splittring av samhället.
3. Valfrihet. Människor ska t.ex. ha rätt att valfritt välja vilka digitala tjänster de vill använda.
4. Deltagande i det digitala offentliga rummet. Människor ska ha tillgång till tillförlitlig miljö som präglas av mångfald.
5. Säkerhet, trygghet och egenmakt. Den digitala miljön ska vara skyddad, säker och trygg där alla har rätt till integritet.
6. Hållbarhet. Digitala tjänster och produkter ska utformas så att de minskar den negativa miljöpåverkan.

⁴⁶ The European Declaration on Digital Rights and Principle for the Digital Decade.

5.2 Dataförvaltningsförordningen

Dataförvaltningsförordningen⁴⁷ började tillämpas den 24 september 2023, men den beslutades om redan i maj 2022. Vi har i projektet i mellantiden arbetat med att utforska hur dataförvaltningsförordningen kommer att påverka en myndighet såsom Jordbruksverket. Dataförvaltningsförordningen fokuserar bl.a. på *hur* en myndighet delar data med externa mottagare och är en del i EU:s arbete med att skapa en inre marknad för data.

När det gäller datadelning har Sverige och EU olika bevekelsegrunder. En tidig form av datadelning är den svenska offentlighetsprincipen från 1766. Offentlighetsprincipen syftar till att allmänheten har rätt till insyn och tillgång till information om staten och kommuners verksamhet för att kunna utöva medborgerlig kontroll och för att kunna utkräva ansvar av de folkvalda i en demokrati. Redan från början var utgångspunkten att informationen var offentlig, men kunde sekretessbeläggas om det behövdes. Idag regleras detta i offentlighets- och sekretesslagen (OSL).

Andra länder ute i Europa har en annan uppfattning. Utgångspunkten är i stället att allt är hemligt, men en del kan bli offentligt. Över tid medförde det att tillgången till myndighetsinformation generellt var låg på den inre marknaden. EU insåg att detta var ett problem och skapade Digital Decade, vilket är ett program som kopplar samman EU:s mål för fortsatt digitalisering och innovation fram till 2030. Digital Decade består förenklat av tre delar. En del handlar om tekniken som behövs för att nå ökad datadelning, en annan del handlar om nya regler och den tredje delen handlar om grundläggande värderingar. Först ut i den delen som handlar om regelverk var den så kallade öppna datadirektivet från 2010, vilket möjliggjorde för myndigheter att dela öppna data med utomstående för att främja användningen av öppna data och stimulera innovation inom produkter och tjänster genom vidareutnyttjande av information.

OSL är i mycket en lagstiftning som bygger på den teknik som var tillgänglig på 1700-talet dvs. papper och penna. Exempelvis maskning (stryka över sekretessbelagd text i ett dokument med en svart penna) är fortfarande en vanlig metod när en myndighet lämnar ut en handling (dvs hur dela data). Digitalisering öppnar upp för helt andra möjligheter att dela data, vilket är nödvändigt om t.ex. en myndighet ska dela stora mängder data (big data). Öppna datadirektivet var redan från start anpassad för den senaste digitala tekniken för datadelning.

5.2.1 Kort om dataförvaltningsförordningen

Dataförvaltningsförordningen bygger vidare på öppna data regelverket och är en komplettering till detta. Förordningen handlar bl.a. om hur en myndighet kan dela data digitalt för vidareutnyttjande med utomstående avseende vissa kategorier av skyddade data genom att skapa en harmoniserad ram. Hur detta ska gå till anges i kapitel 2 i förordningen. Med skyddade data avses i detta sammanhang data som är skyddad på grund av insynsskydd för kommersiella uppgifter, statistiska uppgifter, immateriella

⁴⁷ Europaparlamentet och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten)

rättigheter eller personuppgifter. Dessa kategorier ingår inte i regelverket för öppna data.

Förordningen definierar inte vad som avses med kommersiella uppgifter. Men i begreppet brukar läggas ord som företagshemligheter, yrkeshemligheter och affärshemligheter. Kommersiella uppgifter får inte röjas till följd av vidareutnyttjande (art 5.8). Samtidigt ska en myndighet, vid begäran om utlämnande för vidareutnyttjande hjälpa till med att inhämta samtycke från den som besitter kommersiella uppgifter.

Förordningen definierar inte vad som menas med insynsskydd för statistiska uppgifter. Dataskyddsförordningen (GDPR) har en del att säga om personuppgifter som behandlas för statistiska ändamål. Det är t.ex. tillåtet att behandla känsliga personuppgifter för statistiska ändamål om lämpliga skyddsåtgärder vidtas (art 9.2.j och 89). Även OSL har regler för sekretess och statistikverksamhet (10 kap. 14 § och 24 kap. 8 §). Det är t.ex. tillåtet att lämna ut uppgifter om enskilda för statistikändamål om det står klart att den enskilde inte lider någon skada eller men av utlämnandet.

Inte heller definierar förordningen vad som avses med 3:e parts immateriella rättigheter. Enligt upphovsrätten handlar det t.ex. om data som ingår i verk eller alster såsom en bok, kod i ett datorprogram eller kartor. Innan ett utlämnande för vidareutnyttjande av data behöver myndigheten utreda de immateriella anspråk som kan finnas där.

Till den sista kategorin hör personuppgifter utanför GDPR:s tillämpningsområde. Det kan t.ex. handla om avlidna personers personuppgifter.

Varken dataförvaltningsförordningen eller öppna data regelverket tillåter delning av data som faller under allmän och nationell säkerhet samt försvaret.

Innan ett utlämnande kan ske enligt dataförvaltningsförordningen ska det alltid göras en sekretessprövning enligt OSL. Dataförvaltningsförordningen kan inte upphäva sekretess.

Det finns skillnader mellan regelverket för öppna data och dataförvaltningsförordningen. Öppna data kan delas fritt och då även vidareutnyttjas fritt för valfritt ändamål. Det finns inte heller några tekniska, ekonomiska eller juridiska begränsningar avseende öppna data. Detta gäller inte för data som delas enligt dataförvaltningsakten. Här kan en myndighet i stället ställa krav för datadelning utifrån tekniska, juridiska och ekonomiska aspekter.

Dataförvaltningsförordningen, i sig, ger heller inte någon rätt till tillgång till data utan handlar om *hur* information kan och ska tillhandahållas när data väl görs tillgänglig. Ett utlämnande kan ske om det är lämpligt. I hur:et ligger att dataförvaltningsförordningen syftar till att skapa rättvis konkurrens, likabehandling, transparens och icke-diskriminering mellan mottagare av data. En myndighet får ställa villkor för vidareutnyttjande (art 5). Villkoren ska dock vara offentliga, proportionerliga och objektivt motiverade med hänsyn till kategorierna av data, vidareutnyttjandets syfte och typerna av data för vilka vidareutnyttjande tillåts. Det går också att ha olika villkor för olika kategorier av mottagare t.ex. kommersiella/icke-kommersiella. Det är också tillåtet att vidareutnyttja data för annat ändamål än det ursprungliga syftet (både kommersiellt och icke-kommersiellt).

Dataförvaltningsförordningen ger inte rätt till fritt vidareutnyttjande. En myndighet kan ta betalt för exempelvis:

- reproduktion, tillhandahållande och spridning av data,
- klarering av upphovsrätt,
- anonymisering eller andra former av framställning av personuppgifter och affärshemligheter,
- underhåll av den säkra behandlingsmiljön,
- förvärvande av rätten att tillåta vidareutnyttjande, och
- bistånd till vidareutnyttjare som begär de registrerades samtycke och tillstånd från datainnehavare vars rättigheter och intressen kan påverkas av vidareutnyttjandet.⁴⁸

Dataförvaltningsförordningen bygger på två sorters utlämnande av data. I det första fallet säger mottagaren att jag inte behöver personuppgifter, kommersiella uppgifter etc. Då ankommer det på myndigheten att "tvätta bort" alla personuppgifter (anonymisera) och tar bort/ändra data om affärshemligheter så att konfidentiell information inte lämnas ut t.ex. genom generalisering, randomisering eller undertryckande av data. I det andra fallet säger mottagaren att jag behöver tillgång till den riktiga data eftersom det krävs för att tillgodose mitt behov. I vissa fall är det möjligt att tillåta vidareutnyttjande av riktiga data, antingen på plats hos myndigheten eller på distans. Förutsättningarna för detta är att behandlingen sker i en säker behandlingsmiljö.

Dataförvaltningsförordningen definierar en säker behandlingsmiljö enligt följande: Det är en fysisk eller virtuell miljö med organisatoriska metoder för att säkerställa överensstämmelse med unionsrätten, såsom GDPR, särskilt vad gäller de registrerades rättigheter, immateriella rättigheter samt insynsskydd, integritet och tillgänglighet för kommersiella och statistiska uppgifter, samt med tillämplig nationell rätt, och göra det möjligt för den enhet som tillhandahåller den säkra behandlingsmiljön att *fastställa och övervaka alla databehandlingsåtgärder, inbegripet förevisandet, lagringen, nedladdningen och exporten av data och beräkningen av härledda data med hjälp av dataalgoritmer*.

Om vidareutnyttjande tillåts genom en säker behandlingsmiljö, på distans eller i fysiska lokaler, ska myndigheten införa villkor som bevarar integriteten för de tekniska systemens funktionssätt i den säkra behandlingsmiljön. Myndigheten ska också förbehålla sig rätten att verifiera processen, metoderna och alla resultat från den behandling av data som görs av vidareutnyttjaren för att bevara integriteten i dataskyddet och förbehålla sig rätten att förbjuda användning av resultat som innehåller information som hotar tredje parter rättigheter och intressen (art 5.4). Det ska vara förbjudet för vidareutnyttjaren att återidentifiera de registrerade, och vidareutnyttjaren ska vidta åtgärder för att förhindra att det sker. Denna ska också informera den utlämnande myndigheten om alla uppgiftsincidenter som sker.

⁴⁸ Genomförande av EU:s dataförvaltningsförordning (Ds 2023:24) dnr Fi2023/02158

5.2.2 Praktisk tillämpning av dataförvaltningsförordningen

Dataförvaltningsförordningen ställer krav på att en myndighet ska kunna svara på en begäran om vidareutnyttjande av data från någon utomstående inom 2 månader (art 8.1). Det innebär att en myndighet behöver förbereda sig i god tid för att kunna hantera en sådan begäran dvs vara proaktiv i stället för reaktiv. Här följer projektets råd till en myndighet som vill arbeta praktiskt med dataförvaltningsförordningen:

1. **Förstå förordningen:** Innan du börjar, är det viktigt att förstå vilken typ av data som omfattas av dataförvaltningsförordningen. Detta kan kräva samråd med en juridisk rådgivare eller dataexpert.
2. **Genomför en datainventering:** Identifiera alla typer av data som din organisation samlar in, lagrar och behandlar. Detta bör inkludera allt från personuppgifter till anonymiserade data, meta-data och mer.
3. **Kategorisera data:** Kategorisera data baserat på typ och innehåll. Detta kan innefatta att dela upp data i kategorier som personuppgifter, företagsdata, tekniska data, m.m.
4. **Bedöm rättslig status:** För varje datatyp, bedöm om det är täckt av dataförvaltningsförordningen. Detta kan innefatta att titta på saker som var data kommer ifrån, hur den används, och om den delas med andra parter.
5. **Dokumentera processen:** Skapa en detaljerad rapport av din datainventering och bedömning, inklusive vilken data som omfattas av förordningen och varför. Detta dokument kan sedan användas som en referens för framtida dataskyddsinsatser och revisionskontroller.
6. **Upprätta kontinuerlig övervakning:** Lagar och förordningar förändras ständigt, och det är viktigt att organisationen har en process på plats för att regelbundet granska och uppdatera din datainventering och rättsliga bedömning.
7. **Utbilda medarbetare:** Se till att alla inom organisationen som hanterar data är medvetna om dataförvaltningsförordningen och förstår vilka skyldigheter de har under förordningen.

5.2.2.1 Myndigheten agerar på eget initiativ

Dataförvaltningsförordningen utgår ifrån att en myndighet självmant kan dela data för vidareutnyttjande utan att vänta på att någon utomstående begär ut data. Vi har i projektet tagit fram en process för hur detta kan gå till.

Steg 1: Det finns ett behov eller önskemål internt hos myndigheten att arbeta proaktivt med dataförvaltningsakten. Detta kräver en förankringsprocess inom myndigheten. Ett arbete behöver påbörjas med att identifiera och kategorisera delningsbara datamängder utifrån de fyra kategorier som nämns i dataförvaltningsförordningen.

Steg 2: En inledande juridisk analys bör genomföras. Vilka lagar och förordningar är tillämpliga?

Steg 3: Finns all kompetens som behövs inom myndigheten eller är det aktuellt att få rådgivning från en annan statlig myndighet t.ex. om vad som avses med en säker behandlingsmiljö?

Steg 4: Ta fram och förankra i högsta ledningen en policy för datadelning. Bestäm utifrån allmänna principer hur data ska delas på ett altruistiskt, affärsmässigt och lagligt sätt. Här kan FAIR-principer vara en start i arbetet. FAIR står för:

- Sökbara (findable) - informationen ska vara möjlig att söka efter och hitta
- Tillgänglig (accessible) – informationen ska vara möjlig att tillgå
- Interoperabel (interoperable) – informationen ska kunna fungera i olika system
- Återanvändningsbar (reusable) – informationen ska vara möjlig att återanvända

Steg 5: Informationsklassa informationsobjekt som avses att delas. Här föreslår vi att en myndighet arbetar med tre olika klasser. Klass 1 motsvarar tvättade data med lågt skyddsvärde (anonymiserat). Klass 2 och 3 är otvättade data med högre och högt skyddsvärde. Det kan t.ex. handla om personuppgifter.

Steg 6: Utifrån de tre olika nivåerna behöver sedan myndigheten fastställa lämpliga organisatoriska, fysiska och tekniska säkerhetsåtgärder. Det kan t.ex. handla om kryptering, begränsning av åtkomst, säkerhetskopiering och övervakning av datatrafik.

Steg 7 tvättad data (klass1): Genomför tvättning av data (se avsnitt 6.8). Besluta om vilken betrodd datadelningstjänst som ska användas för leverans t.ex. Sveriges dataportal - DIGG. Kravställ sedan betrodd datadelningstjänst.

Steg 8 otvättad data (klass 2 & 3): Implementera funktionella och säkra tekniska lösningar för lagring och delning av data utifrån säkerhetskraven från klassningen. Ordna med en säker behandlingsmiljö och se till så att det går att övervaka alla databehandlingsåtgärder.

Steg 9: Ingå avtal om datadelning.

Steg 10: Dela data i enlighet med kraven i dataförvaltningsförordningen

Steg 11: Följ upp över tid vad som händer vid datadelning och vidareutbilda personal

5.2.2.2 Myndigheten agerar på begäran om vidareutnyttjande

I exemplet ovan var det myndigheten som agerade proaktivt och funderade igenom vilken data och hur data kan delas enligt dataförvaltningsförordningen. Det andra alternativet är att en utomstående söker upp myndigheten och begär att data lämnas ut för vidareutnyttjande.

En ansökan om vidareutnyttjande bör innehålla följande information:

1. **Vem** är det som ansöker om vidareutnyttjande? Det kan t.ex. vara en erkänd forskningsenhet. I ansökan bör det också anges vilka organisatoriska enheter och personer som ska ha tillgång till data.
2. **Vilken** typ av data/uppgifter/ data sets efterfrågas?

3. Ange **ändamål** med ansökan. Vad ska data användas till och varför behövs den för vidareutnyttjande?
4. **Varför** kan ändamålet inte uppfyllas med annan data?
5. **Hur** ska personuppgifter behandlas?
6. **Vilka** analysmetoder kommer att användas?
7. **Vilken** åtkomstpunkt ska användas? Kommer data att överföras till 3:e land?
8. **Hur** kommer förväntat resultat att offentliggöras/spridas?
9. **Sekretessförsäkran** från de som tar emot data.

Steg 1: En begäran om vidareutnyttjande kommer in till myndigheten. Är ansökan komplett? Om inte kompletteringsförelägg sökande.

Steg 2: Är begärda data redan kategoriserad utifrån dataförvaltningsförordningen? Se föregående avsnitt om hur en myndighet kan arbeta proaktivt med säker behandlingsmiljö och betrodd datadelningstjänst. Om inte är det dags att gå igenom tillämpliga delar i processen som beskrevs ovan.

Steg 3: Genomför juridisk och affärsmässig analys för att säkerställa vilka lagar och förordningar som är tillämpliga för den aktuella data.

Steg 4: Undersök om samtycke för datadelning behövs. Hur kan myndigheten vara behjälplig med att inhämta samtycke? Påverkas någon som har immateriella tillgångar i begärda data? Behöver Integritetsskyddsmyndigheten tillfrågas?

Steg 5: Beslut om betrodd och juridisk åtskild dataförmedlingstjänst som ska användas i det enskilda fallet.

Steg 6: Finns det en risk för att data överförs till 3:e land utanför EU? Finns det i så fall tillräckliga skyddsåtgärder i förhållande till data? Beslut om eventuell dataöverföring till 3:e land.

Steg 7: Utred om det behövs kompletterande säkerhetsåtgärder. Identifiera och besluta om eventuella organisatoriska, fysiska eller tekniska säkerhetsåtgärder som inte redan finns implementerade inom organisationens miljö för saker datahantering.

Steg 8: Gör en kostnadsuppskattning.

Steg 9: Återkoppla till sökanden om möjliga datamängder, krav, kostnader etc. Vill sökanden fortsätta trots allt? Preliminär överenskommelse om att fortsätta. Tänk på att en myndighet har två månader (tre månader vid besvärliga fall) på sig att handlägga begäran om utlämnande av data för vidareutnyttja.

Steg 10: Teckna affärs- och sekretessavtal.

Steg 11: Implementera datadelningslösningen.

Steg 12: Följ upp över tid och utvärdera för att få kvalitetssäkrad datadelningslösning.

5.3 Artificiell Intelligens (AI) förordningen

AI förordningen, antogs av EU-parlamentet den 13 mars 2024. Det innebär att den inom ett par år kommer att införas stegvis som lagstiftning i alla länder inom EU. Syftet med förordningen är att reglera användningen av AI med fokus på hälsa, säkerhet och demokratiska rättigheter.

AI förordningen är ett så kallat horisontellt regelverk som går på tvären över många sektorer. AI förordningen är i grunden riskbaserad utifrån fyra nivåer:

- **Oacceptabel risk:** AI som räknas som oacceptabel risk är förbjuden att utveckla och använda. Förbjuden AI kan exempelvis handla om att ge medborgare poäng efter hur de sköter sig.
- **Hög risk:** Hög risk AI är tillåten om den till exempel CE-märks. Exempel inom detta område är AI som används för att sortera personer för att ge vissa en belöning, exempelvis rekrytering.
- **Transparensrisk:** Denna typ av AI är tillåten, men användare måste informeras. En användare som exempelvis pratar med en chatbot ska veta att det är en chatbot och inte en människa kommunikationen sker med.
- **Liten till minimal risk:** AI är tillåten utan restriktioner.

Det är oklart hur stor påverkan AI förordningen kommer att ha på data inom jordbruks- och livsmedelssektorn. Framför allt handlar det om hur mycket högrisk AI som kommer att användas inom jordbrukssektorn.

Inom offentlig förvaltning är det mycket viktigt att utveckla digitala verktyg som även underlättar myndigheternas interna arbetsprocesser. Maskning av data som delas digitalt är exempel på ett sådant verktyg. I en rapport⁴⁹ från 2023 fastslogs att svensk offentlig förvaltning som helhet kommer att bli kraftigt begränsade i sin möjlighet att använda AI om inte det finns en tydlig styrning och samordning för att förbereda offentlig förvaltning på den kommande förordningen.

⁴⁹ [Slutrapport: Uppdrag att främja offentlig förvaltnings förmåga att använda artificiell intelligens \(digg.se\)](https://www.digg.se/Slutrapport-Uppdrag-att-framja-offentlig-forvaltnings-formaga-att-anvanda-artificiell-intelligens)

6 Informationssäkerhet

Informationssäkerhet är en kritisk komponent inom jordbruks- och livsmedelssektorn, särskilt i en tid då digitalisering och datadelning blir alltmer centrala för verksamheten. Att skydda information från obehörig åtkomst, användning, avslöjande, störning, modifiering eller förstörelse är avgörande för att upprätthålla integriteten och tillförlitligheten i system och dataflöden.

Datadelning utgör en avgörande komponent i det moderna digitala samhället, särskilt inom jordbrukssektorn, där data från olika källor kan användas för att förbättra effektivitet och säkerhet. Delning av data inom jordbruket kan medföra betydande fördelar för många aktörer inom livsmedelssystemet, som lantbrukare, konsumenter, forskare och beslutsfattare. Alla som arbetar med att optimera jordbruksmetoder genom precisionsjordbruk, förbättra skördar och hantering av leveranskedjor, främja klimatesiliens, tillhandahålla marknadsinsikter, möjliggöra samarbete, främja innovation och forskning, stödja policyutveckling, säkerställa konsumenttransparens och underlätta riskhantering, kan dra nytta av datadelning.

Data kan hämtas från en mängd olika källor, såsom databaser och sensorer som mäter och överför information till olika dataplattformar. Dessa data samlas ofta i en central plattform för vidare bearbetning och för att säkerställa att regler följs. Efter bearbetning kan data delas via marknadsplatser där villkor för delning och användning fastställs.

För att underlätta förståelsen för läsare som kanske inte är bekanta med alla tekniska termer och koncept, ges här en kort förklaring av några centrala begrepp:

- **Informationssäkerhet:** Åtgärder och processer för att skydda information från obehörig åtkomst, användning, avslöjande, störning, modifiering eller förstörelse.
- **Cybersäkerhet:** Skydd av system, nätverk och data från digitala attacker. Cybersäkerhet är en delmängd av informationssäkerhet som fokuserar på hot i den digitala världen.
- **Security by Design:** En metod där säkerhetsåtgärder integreras i systemets design från början, snarare än att läggas till i efterhand.
- **Autentisering:** Processen att verifiera identiteten på en användare eller enhet innan åtkomst till system eller data beviljas. Exempel inkluderar användarnamn och lösenord, tvåfaktorsautentisering (2FA) och biometriska metoder.
- **Auktorisering:** Processen att ge behörighet till användare eller system att få tillgång till specifika resurser eller data. Detta sker ofta efter autentisering.
- **Kryptering:** Teknik för att skydda data genom att omvandla den till en oläslbar form som endast kan återställas med en specifik nyckel.
- **Intrångsdetekteringssystem (IDS):** System som övervakar nätverk eller system för misstänkt aktivitet och potentiella hot.
- **Honeypot:** En säkerhetsmekanism som används för att locka till sig och identifiera angripare genom att simulera sårbara system.
- **Penetrationstestning:** En metod för att utvärdera säkerheten i ett system genom att simulera attacker för att identifiera och åtgärda sårbarheter.

- Pseudonymisering: Processen att ersätta identifierbara uppgifter med pseudonymer eller koder för att skydda individers identitet.
- Syntetisering av data: Skapandet av artificiella datamängder baserade på mönster och egenskaper hos den ursprungliga datan, utan att inkludera verkliga identifierbara uppgifter.
- IoT (Internet of Things): Ett nätverk av fysiska enheter som är anslutna till internet och kan samla in och utbyta data. Exempel inkluderar sensorer, smarta apparater och andra uppkopplade enheter.
- LoRaWAN (Long Range Wide Area Network): En trådlös kommunikationsteknik som används för att ansluta IoT-enheter över långa avstånd med låg energiförbrukning.
- SSL/TLS (Secure Sockets Layer/Transport Layer Security): Kryptografiska protokoll som används för att säkra kommunikation över ett datornätverk. SSL/TLS används för att kryptera data som överförs mellan webbläsare och servrar.
- MAC-koder (Message Authentication Codes): Kryptografiska koder som används för att verifiera integriteten och äktheten av ett meddelande.
- Zero-Trust Architecture: En säkerhetsmodell där ingen enhet, användare eller systemkomponent anses vara pålitlig per automatik, även om de befinner sig inom nätverkets perimeter. All åtkomst måste verifieras och auktoriseras.
- Differential Privacy: En teknik för att anonymisera data genom att lägga till kontrollerat brus, vilket skyddar individers integritet även när data kombineras med andra datakällor.
- Deep Packet Inspection (DPI): En metod för att analysera innehållet i datapaket som överförs över ett nätverk för att identifiera och blockera skadlig trafik.
- Entropi: Ett mått på slumpmässighet eller komplexitet i ett lösenord eller en kryptografisk nyckel. Hög entropi innebär högre säkerhet.
- Kontrollkanal: En kommunikationsväg som används för att styra och övervaka nätverksresurser och dataflöden. Kontrollkanaler är kritiska för att säkerställa att data överförs säkert och effektivt.
- Ransomware-attacker: En typ av cyberattack där angripare använder skadlig programvara för att kryptera offrets data och kräver en lösensumma för att återställa åtkomsten. Ransomware-attacker kan orsaka allvarliga störningar och ekonomiska förluster för drabbade organisationer.

6.1 Säkring av lantbruksdata

Exempel på data inom livsmedelskedjan är olika geografiska data, förbrukning av insatsvaror som gödnings- och bekämpningsmedel, bränsleförbrukning, foderåtgång samt djurs läkemedelsförbrukning. Data kan ha olika informationsklasser, från öppen till extremt känslig. Dessutom används diverse olika sensorer, både trådlösa och trådbundna, och olika system för dataöverföring. Precisionsjordbruk och automatiserat jordbruk förutsätter en bred användning av uppkopplade enheter, från IoT-sensorer och styrsystem till automatiserade robotar som arbetar på marken. Att störa näringskedjan kan leda till långtgående konsekvenser och i värsta fall orsaka matbrist.

Följande kända informationssäkerhetsproblem identifierats inom lantbrukssektorn⁵⁰:

- Manipulering av data - kan förhindras med hjälp av kryptografiska signaturer.
- Angrepp på kontrollkanaler - kan riskminimeras genom inbyggd säkerhet (säkra länkar, autentisering, auktorisering, minimering av kända sidokanalattacker)
- Läckta företagshemligheter- bör skyddas genom användning av statistiska representationer och syntetiska data (bästa praxis)
- Hackade sensorer - det är osannolikt att en enda sensor kommer att bli måltavla om den inte innehåller kritisk information. I övrigt liknande åtgärd som för att förhindra angrepp på kontrollkanaler.

Dessutom har ransomware-attacker med hot om att störa verksamheten eller avslöja personlig information rapporterats inom livsmedels- och jordbruksindustrin. Troligtvis är problemen inte begränsade till de kända problemen ovan.

Internet ger oöverträffade möjligheter till uppkoppling och datautbyte, vilket kan öka inte bara obehörig åtkomst till data, utan också öppnar för fjärrstörningar av anslutna digitala system, med mål som varierar från spratt till utpressning där ransomware är ett typiskt exempel.

Det finns många punkter i kedjan där sårbarheter kan förekomma och det är viktigt att säkerställa dataintegritet och datasäkerhet genom säkra delningsplattformar och styrande ramverk när man deltar i datasamarbete inom lantbruket. Att skydda komplexa digitala system är en utmaning. Med tanke på att resurserna för skydd inte är obegränsade är det ofta omöjligt att täcka *alla* sårbara punkter på attackytan. Skyddet ökar i allmänhet med den mängd resurser som avsätts för ändamålet. Beroende på hur resurserna används finns det olika skyddsnivåer som kan uppnås för samma system. Aspekterna av informations- och cybersäkerhet omfattar inte bara tekniska, utan även organisatoriska och juridiska delar.

6.2 Informations- och cybersäkerhet: maximera effekten

För att maximera effekten av informations- och cybersäkerhetsåtgärder är det viktigt att följa bästa praxis och säkerställa att säkerhetsåtgärder är integrerade i systemets design från början (security by design). Detta inkluderar att använda starka lösenord, regelbundet uppdatera system och programvara, samt utbilda personalen i säkerhetsmedvetenhet och säkert beteende online.

Att skydda komplexa digitala system är en utmaning. Med tanke på att resurserna för skydd inte är obegränsade är det ofta omöjligt att täcka alla sårbara punkter på attackytan. Skyddet ökar i allmänhet med den mängd resurser som avsätts för ändamålet. Beroende på hur resurserna används finns det olika skyddsnivåer som kan uppnås för samma system. Aspekterna av informations- och cybersäkerhet omfattar inte bara tekniska, utan även organisatoriska och juridiska delar.

⁵⁰ RISE och Jordbruksverket, Privat samtal, maj 2023.

För en effektiv användning av skyddsbudgeten är de praktiska åtgärderna inriktade på att identifiera och ta itu med de svagaste punkterna i systemet, vars misslyckande skulle leda till större skador. De platser där systemet är sårbart kallas i vardagligt tal för *attackytan* och omfattar inte bara tekniska punkter där informationen kan nå utan även den mänskliga delen av systemet. Det uppskattas att den överväldigande majoriteten av cyberbrottsligheten begås med hjälp av social ingenjörskonst, det vill säga att människor manipuleras för att ge bort tillgång till information, och vissa uppskattningar visar att så mycket som 98 %⁵¹ av cyberattackerna involverar någon form av social ingenjörskonst.

6.3 Tekniska säkerhetsåtgärder

För att säkerställa säker och effektiv dataöverföring inom lantbrukssektorn är det viktigt att använda standardiserade datamodeller och säkra anslutningar. Standardiserade datamodeller, såsom SAREF4AGRI, AgGateway eller SIMPL, säkerställer interoperabilitet mellan olika system och möjliggör effektiv datadelning.

Krypterade anslutningar (till exempel SSL/TLS) bör användas för att skydda data under överföring. För IoT-enheter är det viktigt att använda säkerhetsprotokoll som LoRaWAN för att säkerställa att dataöverföringen är skyddad mot obehörig åtkomst. Autentisering och auktorisering är avgörande för att kontrollera åtkomst till data. Implementera stark autentisering, såsom tvåfaktorsautentisering (2FA), och använd auktoriseringstokens för att säkerställa att endast behöriga användare har tillgång till känslig information. Åtkomsträttigheter bör tilldelas baserat på principen om lägsta behörighet (least privilege) för att minimera risken för obehörig åtkomst.

För att förhindra dataförgiftning bör API-filtrerade formulär användas för att ta bort specialtecken. Nätverkstrafik bör övervakas regelbundet med hjälp av intrångsdetekteringssystem (IDS) och honeypots för att upptäcka och avskräcka angripare. Genom att genomföra regelbundna penetrationstester kan säkerhetsbrister identifieras och åtgärdas innan de utnyttjas av angripare.

6.3.1 Standardiserade datamodeller

I nuläget så finns inte någon utpekad svensk standard för datamodeller inom lantbruket. Det finns ett antal föreslagna kandidater, såsom SAREF4AGRI⁵², AgGateway⁵³, eller SIMPL. SIMPL förespråkas av EU kommissionen och support centre för a common european data space for agriculture. Standardiserade datamodeller är avgörande för att säkerställa interoperabilitet mellan olika system. Dessa tre exempelmodeller möjliggör alla en effektiv datadelning och integration, vilket är viktigt för att optimera jordbruksprocesser och förbättra beslutsfattandet. Projektet har ingen statistik över hur ofta dessa modeller används i praktiken i Sverige.

⁵¹ <https://firewalltimes.com/social-engineering-statistics/>

⁵² <https://saref.etsi.org/saref4agri/v1.1.2/>

⁵³ <https://www.aggateway.org>

6.3.2 Säkra och autentiserade anslutningar

I Sverige så är en stor del av trådburen kommunikation idag optisk. För att säkra dessa anslutningar på både nätverks- och applikationsnivåer, bör de säkerhetsåtgärder som beskrivs i referens-SJV-arkitekturen följas. Detta inkluderar användning av kryptering och autentisering för att skydda data under överföring och säkerställa att endast behöriga användare har tillgång till nätverket.

För WiFi rekommenderas att använda hårdvara med de senaste säkerhetsstandarderna, såsom WPA2 (vanligt från och med 2023) eller WPA3 om det är tillgängligt. Dessa standarder säkerställer att dataöverföringen är krypterad och skyddad mot obehörig åtkomst.

Generellt så kan man säga att klienter med tillräckligt med processorkraft, till exempel bärbara enheter och datorer, så bör anslutningarna krypteras och autentiseras med hjälp av end-to-end kryptering som till exempel SSL-TLS. För enklare IoT-enheter (resursbegränsade enheter) uppnås säker anslutning med väletablerade kommunikationsprotokoll som autentisering och dataintegritetsskydd som används i ingår i vissa kommunikationslösningar som till exempel LoRaWAN.⁵⁴

När det inte är tillgängligt bör bästa möjliga krypterings- och autentiseringsmetoder (scheman) baseras på. Autentiserade kanaler bör åtminstone skyddas med hjälp av kryptografiska primitiver som MAC-koder (Message Authentication Codes).

6.3.3 Autentisering och auktorisering

Autentisering och auktorisering är avgörande för att kontrollera åtkomst till data. Implementera stark autentisering, såsom tvåfaktorsautentisering (2FA), eller flerfaktorsautentisering med hjälp av biometriska modaliteter (till exempel fingeravtryck, ansiktsgenkänning) och smartkort. Detta gäller speciellt vid access till aggregerad och "otvättad" data.

Använd därefter auktoriseringstokens för att säkerställa att endast behöriga användare har tillgång till känslig information. Åtkomsträttigheter bör tilldelas baserat på principen om lägsta behörighet (least privilege) för att minimera risken för obehörig åtkomst.

Det bör finnas olika användarkategorier med motsvarande behörigheter. Det finns olika tekniker för åtkomstkontroll för att gruppera användare och behörigheter, till exempel rollbaserad åtkomstkontroll (RBAC). Det vill säga för de användare som får tillgång till uppgifterna via API:et eller de anställda som har tillgång till systemet.

6.3.4 API-säkerhet

För data-typer och -poster bör det finnas en filtreringsprocess som tar bort specialtecken. Det är för att undvika hot om dataförgiftning, särskilt inmatning av skript i datainnehåll. Skript kan spridas i systemet och nå systemkomponenter som kan köra och utnyttja dess programvara.

⁵⁴ https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf

6.3.5 Nätverkssäkerhet

Aggregationsnoden är ingressen för **alla aggregerade och obearbetade (otvättade) data**. Att få åtkomst via detta gränssnitt kan ge tillgång till all rådata som samlats in av systemet. Nätverkstrafik bör övervakas regelbundet med hjälp av intrångsdetekteringssystem (IDS) och möjligen honeypots för att upptäcka och avskräcka angripare. IDS kan identifiera misstänkt aktivitet och varna administratörer om potentiella hot, medan honeypots kan locka till sig och identifiera angripare genom att simulera sårbara system.

IDS kan analysera inkommande trafik efter skadliga nyttolastmönster och utgående trafik för onormalt och okontrollerat dataflöde. Detta för att undvika att en angripare har manipulerat dataklassen och kan komma åt känsligare data än vad som är tillåtet. Det kan identifieras med en IDS/IPS som övervakar trafiken och baseras till exempel på åtkomstkontrollprincipen för en viss roll eller den åtkomsttoken som en viss användare har.

6.3.5.1 Honungskrukor (honey pots)

Honungskrukor är en dyr och komplex aktivitet som höjer säkerheten i ett system. Som en extra åtgärd kan nätverkssäkerheten kompletteras med en sådan. En hone pot är en server som har klassificerad data som ser autentisk ut, och som lurar en angripare att tro att denne har fått tillgång till verkliga data. Honeypot kan anslutas till IDS som en del av systemet för att upptäcka intrång.

6.3.6 Penetrationstestning

Det bör finnas en policy för att regelbundet utvärdera systemet för potentiella cyberhot. Problemet kan vara att nya komponenter kan läggas till på grund av specifik efterfrågan, men inte utvärderas från cybersäkerhetsperspektiv. Dessutom bör det göras en bedömning av versionshanteringen av programvara där säkerhetskorrigeringar måste utföras.

6.4 Organisatoriska lösningar

För att säkerställa en hög nivå av informationssäkerhet inom jordbruks- och livsmedelssektorn är det avgörande att implementera effektiva organisatoriska lösningar. Dessa lösningar bör omfatta medvetenhet och utbildning, en stark lösenordspolicy samt ytterligare organisatoriska åtgärder.

6.4.1 Medvetenhet och utbildning

Medvetenhet och utbildning är grundläggande för att skapa en säkerhetsmedveten kultur inom organisationen. Anställda bör regelbundet utbildas i de senaste säkerhetshoten och bästa praxis för att hantera dessa. Exempel på utbildningsprogram kan inkludera:

- Workshops och seminarier: Praktiska sessioner där anställda får lära sig om aktuella säkerhetshot och hur man skyddar sig mot dem.

- E-learning moduler: Onlinekurser som anställda kan genomföra i sin egen takt, med fokus på specifika säkerhetsämnen som nätfiske och lösenordshantering.
- Simulerade attacker: Genomföra simulerade nätfiskeattacker för att testa och förbättra anställdas förmåga att identifiera och hantera sådana hot.

6.4.2 Lösenordspolicy

Det finns vanligtvis två saker att tänka på: antingen är lösenorden korta/inte tillräckligt komplexa eller *så har de aldrig ändrats från sina ursprungliga och standardinställningar*. Det innebär att systemkomponenterna kan köras med standardlösenord som är förinstallerade, till exempel i IoT-enheter. En angripare kan enkelt hämta eller gissa ett lösenord och få åtkomst till systemkomponenter, till exempel vanligtvis IoT-enheter.

Därför bör det finnas en lösenordsprincip och tillämpning för alla systementiteter (servrar, IoT-enheter). Lösenordspolicyn innehåller lösenordets acceptabla entropi, som i standardtermer definieras av längden och de tecken som ska användas.

6.4.3 Fler organisatoriska åtgärder

Utöver medvetenhet och utbildning samt en stark lösenordspolicy, bör organisationen implementera ytterligare åtgärder för att stärka informationssäkerheten:

- Incidenthanteringspolicy: Utveckla och implementera en policy för hur säkerhetsincidenter ska hanteras, inklusive rapportering, utredning och åtgärder.
- Haveriberedskap: Säkerställ att det finns regelbundna säkerhetskopieringar av data och att det finns en plan för återställning vid eventuella incidenter.
- Kontinuerlig övervakning: Implementera system för att kontinuerligt övervaka nätverk och system för potentiella säkerhetshot.
- Säkerhetsrevisioner: Genomför regelbundna säkerhetsrevisioner för att identifiera och åtgärda sårbarheter i system och processer.

Genom att implementera dessa organisatoriska lösningar kan organisationen skapa en robust säkerhetskultur och minska risken för säkerhetsincidenter.

6.5 Rättsliga komponenter

För att säkerställa att datadelning sker på ett lagligt och etiskt sätt är det viktigt att förstå och följa de rättsliga krav som gäller. Detta avsnitt beskriver de viktigaste rättsliga komponenterna som organisationer inom jordbruks- och livsmedelssektorn bör beakta.

6.5.1 Efterlevnad av lagar och förordningar

Att följa gällande lagar och förordningar är avgörande för att undvika juridiska konsekvenser och säkerställa att datadelning sker på ett ansvarsfullt sätt. Viktiga regelverk att beakta inkluderar:

- Dataskyddsförordningen (GDPR): GDPR ställer krav på hur personuppgifter ska hanteras och skyddas. Organisationer måste säkerställa att de har rättslig grund för att behandla personuppgifter och att de vidtar lämpliga säkerhetsåtgärder för att skydda dessa uppgifter.
- Offentlighets- och sekretesslagen (OSL): OSL reglerar hur offentliga myndigheter ska hantera och skydda information. Det är viktigt att förstå vilka uppgifter som omfattas av sekretess och hur dessa ska hanteras vid datadelning.
- Dataförvaltningsförordningen: Denna förordning syftar till att skapa en harmoniserad ram för datadelning inom EU. Den ställer krav på hur data ska delas och vilka säkerhetsåtgärder som måste vidtas för att skydda känslig information.

6.5.2 Begränsat ansvar genom avtal

För att minimera juridiska risker bör organisationer ingå avtal som tydligt reglerar ansvaret för datadelning. Dessa avtal bör inkludera:

- Ansvarsbegränsning: Klargör vilka parter som är ansvariga för eventuella skador som kan uppstå till följd av datadelning.
- Sekretessklausuler: Specificera hur känslig information ska skyddas och vilka åtgärder som ska vidtas för att förhindra obehörig åtkomst.
- Användningsvillkor: Definiera hur data får användas av mottagaren och vilka begränsningar som gäller för vidare delning av data.

6.5.3 Riskreducering genom försäkring

Att teckna en cyberförsäkring kan vara ett effektivt sätt att skydda organisationen mot ekonomiska förluster till följd av dataintrång eller andra säkerhetsincidenter. En cyberförsäkring kan täcka kostnader för:

- Incidenthantering: Kostnader för att hantera och återhämta sig från en säkerhetsincident, inklusive teknisk support och juridisk rådgivning.
- Skadestånd: Ersättning till tredje part för skador som uppstått till följd av ett dataintrång.
- Böter och sanktioner: Eventuella böter och sanktioner som kan åläggas organisationen till följd av brott mot dataskyddsregler.

6.5.4 Kontinuerlig övervakning och efterlevnad

För att säkerställa att organisationen kontinuerligt följer gällande lagar och förordningar bör en process för regelbunden övervakning och efterlevnad etableras. Detta kan inkludera:

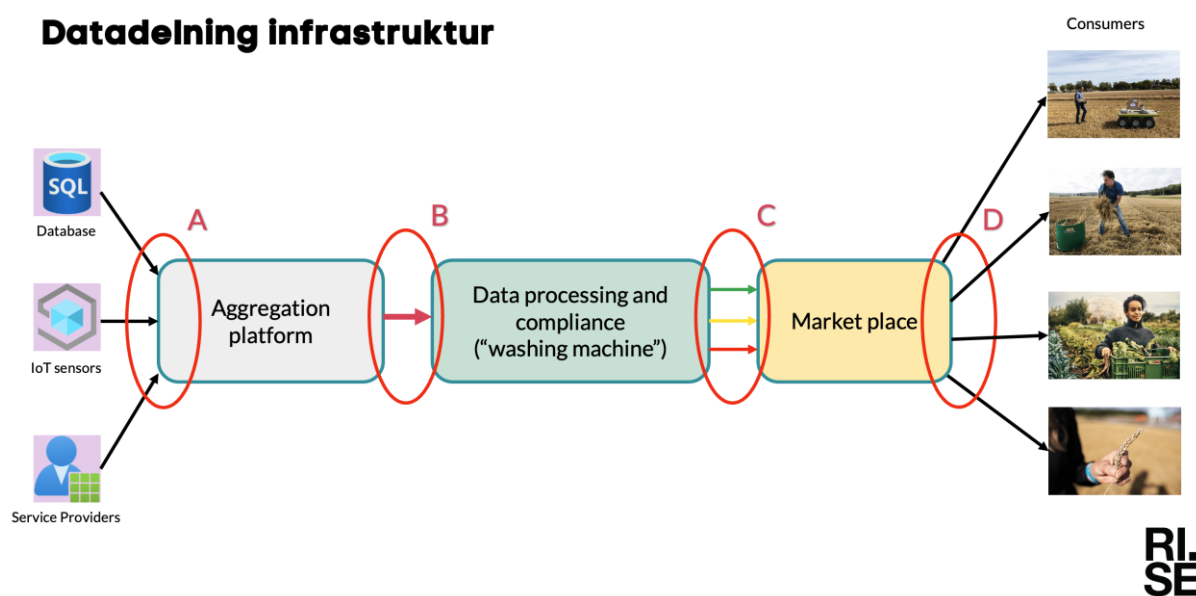
- Revisioner: Genomför regelbundna revisioner för att säkerställa att dataskyddsåtgärder är effektiva och att organisationen följer gällande regler.
- Uppdatering av policyer: Se till att interna policyer och rutiner regelbundet uppdateras för att återspegla förändringar i lagstiftningen.
- Utbildning: Fortsätt att utbilda anställda om deras ansvar och skyldigheter enligt gällande lagar och förordningar.

Genom att följa dessa rättsliga komponenter kan organisationer säkerställa att datadelning sker på ett lagligt och ansvarsfullt sätt, samtidigt som de skyddar sig mot juridiska risker.

6.6 Slutliga rekommendationer om informationssäkerhet

Information- och cybersäkerhet är som mest effektivt och har större effekt om det görs som en förebyggande åtgärd än i efterhand. Vi rekommenderar därför att man tänker igenom datadelningsmodellen och implementerar säkerhet genom design med hjälp av bästa praxis och tillgängliga verktyg. Detta kan inkludera nollförtroendearkitektur (zero-trust architecture) för bättre säkerhet och datakontroll, och reproducerbara ritningar för bättre skalbarhet av informationsarkitekturer.

6.7 Plattformer för datadelning



Figur 6. En arkitektur med hög vy för datadelning.

Plattformsbeskrivning (generisk):

I figur 6 visas en arkitektur med hög vy för datadelning. Data samlas in från ett antal källor, bland annat sensorer, databas och tjänster till vänster i bild. Uppgifterna aggregeras i aggregeringsplattformen och skickas vidare till plattformen för databehandling och regelefterlevnad ("tvättmaskin") där uppgifterna klassificeras och behandlas med hjälp av integritetsbevarande metoder för att producera ström av olika känslighet, allmänt betecknad i grönt, gult och rött, där det gröna är öppna data, det röda är känsliga data och det gula är delvis känsliga data. Uppgifterna skickas sedan till

marknadsplatsen, där de delas antingen öppet eller genom avtal som specificerar villkor inklusive användning. Datakänsligheten kan påverka hur data distribueras, men så är inte alltid fallet. Metadata i datahjälp dig att fatta delningsbeslutet. Varje uppgiftslämnare bestämmer vad som ska lämnas ut och på vilka villkor. Den övergripande plattformen katalogiserar data.

Exempel på dataplattformar för delning av lantbruksdata i Sverige är Agronod⁵⁵, Skira⁵⁶ och Dataväxt⁵⁷.

6.8 Automatisk maskering av data som ej ska delas

Automatisk maskering av data är en process som används för att skydda känslig information och säkerställa att data kan delas och användas utan att kompromettera individers integritet. Detta är särskilt viktigt i sammanhang där data måste uppfylla strikta krav på konfidentialitet. Maskering av data kan uppnås genom olika tekniker, inklusive anonymisering, pseudonymisering och syntetisering av data.

6.8.1 Anonymisering och Pseudonymisering

Anonymisering är en teknik där alla identifierbara uppgifter i en datamängd tas bort eller ändras så att det inte längre är möjligt att spåra data tillbaka till en specifik individ. Detta innebär att personuppgifter som namn, personnummer och adresser ersätts med fiktiva eller generiska värden. Anonymisering är en effektiv metod för att skydda individers integritet, eftersom det eliminerar risken för att data kan återidentifieras. Anonymiserade data kan användas för analys och forskning utan att bryta mot till exempel dataskyddsförordningen (GDPR).

Pseudonymisering är en annan teknik för att skydda känslig information. Till skillnad från anonymisering, där identifierbara uppgifter helt tas bort, innebär pseudonymisering att dessa uppgifter ersätts med pseudonymer eller koder. Detta gör det svårare, men inte omöjligt, att spåra data tillbaka till en individ. Pseudonymisering används ofta när det är nödvändigt att behålla en viss nivå av identifierbarhet för att kunna koppla samman olika datamängder eller för att möjliggöra framtida återidentifiering under kontrollerade förhållanden. Pseudonymiserad data erbjuder en balans mellan dataskydd och användbarhet, vilket gör det möjligt att analysera data samtidigt som individers integritet skyddas.

6.8.2 Utmaningar i samband med anonymisering av data

En av de största utmaningarna med anonymisering av data är risken för avanonymisering när separata datamängder kombineras. Även om en enskild datamängd har anonymiserats och inte innehåller några direkt identifierbara uppgifter, kan det vara möjligt att återidentifiera individer genom att kombinera denna

⁵⁵ <https://www.agronod.com>

⁵⁶ <https://skira.com>

⁵⁷ <https://datavaxt.com/sv/>

datamängd med andra tillgängliga datakällor. Detta fenomen kallas för "avanonymisering" och uppstår när korsreferenser mellan olika datamängder avslöjar tillräckligt med information för att identifiera enskilda personer.

Till exempel kan en anonymiserad datamängd innehålla information om ålder, kön och postnummer, medan en annan datamängd kan innehålla liknande attribut tillsammans med ytterligare detaljer som yrke eller hälsotillstånd. När dessa datamängder kombineras kan de gemensamma attributen användas för att skapa en unik profil som gör det möjligt att identifiera individer, trots att varje enskild datamängd i sig är anonym.

För att minimera risken för avanonymisering är det viktigt att tillämpa robusta anonymiseringstekniker och att noggrant överväga vilka datamängder som delas och kombineras. Detta kan inkludera att använda mer avancerade anonymiseringstekniker, såsom differential privacy, som lägger till kontrollerat brus till data för att skydda individers integritet även när data kombineras. Dessutom bör organisationer ha strikta policyer och kontroller på plats för att övervaka och begränsa åtkomsten till känsliga datamängder, samt att utbilda personal om riskerna och bästa praxis för dataskydd.

6.8.3 Syntetisering av Data

Syntetisering av data är en avancerad teknik som används för att skapa nya datamängder baserade på mönster och egenskaper hos den ursprungliga datan. Syntetiska data genereras genom att använda algoritmer och maskininlärning för att modellera och reproducera de statistiska egenskaperna hos den ursprungliga datan, utan att inkludera några verkliga identifierbara uppgifter. Detta innebär att syntetiska data kan användas på samma sätt som verklig data för analys och forskning, men utan risk för att avslöja känslig information.

6.8.3.1 Fördelar med syntetiska data vid testning och utveckling

Användning av syntetiska data erbjuder flera fördelar vid testning och utveckling av tjänster som ska använda data:

- **Säkerhet:** Syntetisk data eliminerar risken för att känslig information avslöjas under testning och utveckling. Detta gör det möjligt att arbeta med realistiska datamängder utan att kompromettera integriteten hos verkliga data.
- **Tillgänglighet:** Syntetisk data kan genereras i stora mängder och anpassas efter specifika behov, vilket gör det enklare att skapa omfattande testscenarier och utföra grundliga tester.
- **Reproducerbarhet:** Eftersom syntetiska data kan genereras på ett kontrollerat sätt, är det möjligt att reproducera testscenarier exakt, vilket underlättar felsökning och förbättring av tjänster.

6.8.3.2 Fördelar med syntetiska data vid verifiering av säkerhetssystem

Syntetiska data är också mycket användbar vid verifiering av system som ska skydda känsliga data:

- Riskfri testning: Genom att använda syntetiska data kan säkerhetssystem testas och verifieras utan att riskera att verkliga känsliga data exponeras. Detta är särskilt viktigt vid penetrationstestning och andra säkerhetsrelaterade tester.
- Realistiska scenarier: Syntetisk data kan utformas för att efterlikna verkliga användningsfall och hot, vilket gör det möjligt att utföra realistiska säkerhetstester och identifiera potentiella sårbarheter.
- Kontinuerlig förbättring: Genom att regelbundet använda syntetiska data för att testa och verifiera säkerhetssystem kan organisationer kontinuerligt förbättra sina säkerhetsåtgärder och snabbt anpassa sig till nya hot.

Genom att använda syntetiska data vid både utveckling och verifiering av tjänster och säkerhetssystem kan organisationer säkerställa att deras lösningar är robusta, säkra och redo att hantera verkliga data utan att kompromettera integriteten hos känslig information.

7 Referensarkitektur för datadelning

Detta kapitel ger en översikt över den referensarkitektur som utvecklats under projektet. Det beskriver de komponenter och verktyg som används för datainsamling, aggregering och analys, med betoning på säkerhet och efterlevnad av regler och förordningar. Kapitlet beskriver exempel på olika komponenter för datainsamling och analys, följt av en beskrivning av den uppställning för klassificering och maskning för öppna data som projektet tillverkat.

7.1 Datainsamling och analysplattformar

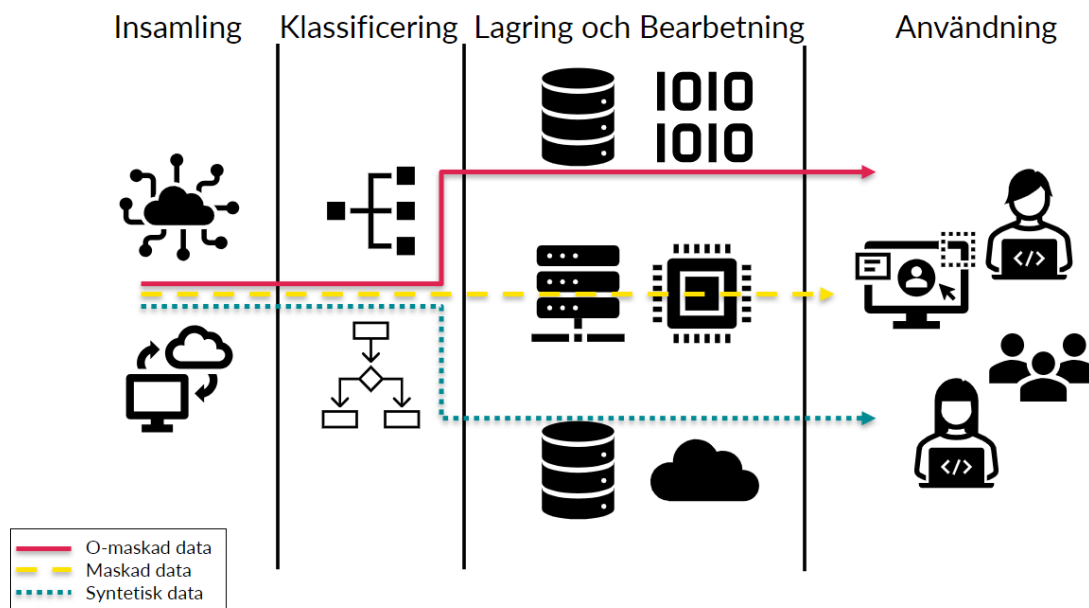
För att säkerställa en effektiv och säker datainsamling och analys inom jordbruks- och livsmedelssektorn har projektet använt två huvudsakliga komponenter: Yggio och Hopsworks. Dessa plattformar tillhandahålls av projektets samarbetspartners.

Yggio är en digital plattform för hantering av digital infrastruktur, en Digitalization Infrastructure Management System (DiMS), som erbjuder en sammanhängande driftsmiljö för all teknik och data inom en specifik domän. Plattformen används av ett brett spektrum av aktörer, inklusive städer, fastighetsbolag, energi- och vattenbolag, samt inom jordbrukssektorn. Yggio möjliggör insamling och hantering av data från olika källor, såsom sensorer och databaser, och integrerar dessa data i en central plattform. Genom att använda Yggio kan användare övervaka och optimera sina processer, vilket leder till ökad effektivitet och bättre beslutsfattande. Plattformen stödjer även säker dataöverföring och autentisering, vilket är avgörande för att skydda känslig information.

Hopsworks är en avancerad plattform för dataanalys och artificiell intelligens (AI). Den används för att experimentera med och utveckla AI-baserade tjänster inom olika domäner. Hopsworks erbjuder verktyg för att hantera stora datamängder och möjliggör komplexa analyser och maskininlärning. Plattformen stödjer hela livscykeln för datahantering, från insamling och lagring till analys och visualisering. Genom att använda Hopsworks kan forskare och utvecklare skapa innovativa lösningar som förbättrar effektiviteten och hållbarheten inom jordbruks- och livsmedelssektorn. Plattformen säkerställer också att data hanteras enligt strikta säkerhetsstandarder, vilket är avgörande för att skydda integritet och säkerhet i de data som används.

7.2 Klassificering för öppna data

En central komponent i denna plattform har internt benämnts som "Tvättmaskinen" en komponent som inte olikt sitt namn används för att bearbeta data så att den inte innehåller känsliga uppgifter genom att analysera och klassificera data, s.k. "tvätta data".



Figur 7. Översikt över dataflöde genom referensarkitekturen.

Figur 7 exemplifierar dataflödet genom plattformen. Systemet samlar in data från externa system och placerar den i en aggregeringsplattform i organisationens digitala infrastruktur. Därefter så skickas data in för klassificering i tvättmaskinen. Vidare så flyttas data till interna system, eller via särskilda utgångar till externa system baserat på vilken klass och åtgärd som tvättmaskinen utfört.

Tvättmaskinen klassificerar data genom att jämföra nya data med tidigare givna exempel på klassificerade data från organisationen. Beroende på vilket exempel som ligger "närmast" den inmatade datan så märks den upp med en rekommenderad klass inom konfidentialitet, riktighet och tillgänglighet. Beroende på tidigare vald lagringsplats och rekommenderad dataklass så hanteras data sedan vidare på olika sätt. All data skickas oförändrad till den interna plattformen. Därefter så kommer data med medium konfidentialitet maskeras genom tekniker som pseudonymisering innan den skickas vidare. Data med hög konfidentialitet skickas in i ett separat spår där nya data syntetiseras baserat på den inmatad data. Data av högsta konfidentialitet får inte förekomma i plattformen, men dess beskrivning inkluderas för att göra plattformen komplett. Data förmedlas därefter till olika digitala lagringsplatser baserat på dess erhållna konfidentialitet efter att maskering eller syntetisering är genomförd.

Tvättmaskinen är utvecklad i python och använder ett webbaserat användargränssnitt som heter streamlit som ramverk med integrering mot både dataklassificeringen och generering av syntetiska data samt håller koll på olika dataset som körs i tvättmaskinen. Ett dataset kan bestå av flera tabeller eller filer där klassificeringen sker på både individuell nivå och datasetet klassificeras som helhet. Här finns även metadata till dataset med användare, tidsstämplar men även kontrollfrågor om data som användaren svarar på om datasetet när det hanteras.

Klassificeringen använder ett bibliotek som heter dataprofiler 0.10.9 och kan känna igen känsliga data tillsammans med input från frågorna användaren svarade på i metadata.

Generering av syntetiska data använder biblioteket sdv 1.10.0 och i tvättmaskinen kan de generera både tabell-liknande data och relationsdata.

Applikationen, med bibliotek och modelldata paketeras som en Docker-image och för att kryptera kommunikationen mellan tvättmaskinen och användaren, även om den körs lokalt i organisationens infrastruktur, sker med TLS.

8 Diskussion och slutsatser

Digitaliseringen och datadrivna tjänster håller på att omforma livsmedelskedjan i grunden, från jordbruk till konsumtion. Sveriges ambition att vara i framkant av digitaliseringen fram till 2030, tillsammans med den växande betydelsen av data i beslutsfattandet, understryker potentialen i att använda data som en central resurs inom livsmedelssektorn. Med nya lagkrav och teknologiska framsteg finns det nu möjligheter att optimera produktion, distribution och konsumtion på sätt som tidigare var otänkbara.

En av de största utmaningarna med datadelning inom jordbruks- och livsmedelskedjan är att hantera stora datavolymer samtidigt som man säkerställer att känslig information skyddas. När datavolymerna stiger blir det allt svårare att manuellt klassificera och maskera data för att uppfylla säkerhets- och sekretesskrav. Här spelar projektets resultat en avgörande roll som ett verktyg för automatisk dataklassificering och maskering.

Projektet demonstrerar en lösning som möjliggör effektiv och säker datadelning genom att automatisera processen med att identifiera och klassificera data baserat på konfidentialitet, riktighet och tillgänglighet. Genom att använda avancerade algoritmer kan verktyget snabbt och noggrant bearbeta stora mängder data, vilket minskar risken för mänskliga fel och säkerställer att data hanteras enligt gällande regelverk. Detta är särskilt viktigt i en tid då datamängderna ökar exponentiellt och behovet av snabb och säker datadelning blir alltmer kritiskt.

Genom att implementera erfarenheterna från verktyget kan organisationer inte bara förbättra sin förmåga att dela data på ett säkert sätt, utan också främja innovation och effektivitet inom och bortom jordbruks- och livsmedelskedjan. Verktyget demonstrerar anonymisering, pseudonymisering och syntetisering av data, vilket gör det möjligt att skydda individers integritet samtidigt som man utnyttjar data för forskning och utveckling. Detta bidrar till att skapa en robust och hållbar datainfrastruktur som kan hantera framtidens utmaningar och möjligheter.

Data är en strategisk resurs för utveckling och digital innovation inom jordbruks- och livsmedelskedjan. Tillgång till högkvalitativa data är avgörande för att öka konkurrenskraften, främja hållbar tillväxt och minska resursanvändningen. Fragmenteringen i livsmedelskedjan gör dock datadelning komplicerad, vilket skapar behov av standarder och interoperabilitet för att säkerställa effektiv datadelning och integration av olika system och applikationer.

Hantera känslig information kräver robusta säkerhetsåtgärder. Anonymisering, pseudonymisering och syntetisering av data är viktiga tekniker för att skydda individers integritet och säkerställa att data kan delas på ett säkert sätt. Dataförvaltningsförordningen och andra relevanta lagar och förordningar ställer nya krav på myndigheter och organisationer att tillgängliggöra data för maskininläsning och säker delning. Det är viktigt att följa dessa regler för att undvika juridiska konsekvenser och säkerställa efterlevnad.

Genom att integrera datadrivna tjänster i livsmedelskedjan kan företag upptäcka nya affärsmöjligheter och skapa mervärde för sina kunder. Detta kan leda till ökad

effektivitet, minskat svinn och förbättrad kundupplevelse, samtidigt som det bidrar till att tackla globala utmaningar som hållbarhet och livsmedelssäkerhet. Det finns också ett behov av ökat samarbete mellan olika aktörer inom jordbruks- och livsmedelskedjan för att utveckla gemensamma standarder och ramverk för datadelning, vilket kan underlätta integration och användning av data över olika system och plattformar.

Framtiden för livsmedelssektorn är under stor digital transformation med teknologi och data i centrum. Genom att implementera teknologiska lösningar som demonstrerats i detta projekt och främja samarbete och standardisering kan vi skapa en hållbar och innovativ datainfrastruktur som möter framtidens utmaningar och möjligheter.

Through our international collaboration programmes with academia, industry, and the public sector, we ensure the competitiveness of the Swedish business community on an international level and contribute to a sustainable society. Our 2,800 employees support and promote all manner of innovative processes, and our roughly 100 testbeds and demonstration facilities are instrumental in developing the future-proofing of products, technologies, and services. RISE Research Institutes of Sweden is fully owned by the Swedish state.

I internationell samverkan med akademi, näringsliv och offentlig sektor bidrar vi till ett konkurrenskraftigt näringsliv och ett hållbart samhälle. RISE 2 800 medarbetare driver och stöder alla typer av innovationsprocesser. Vi erbjuder ett 100-tal test- och demonstrationsmiljöer för framtidssäkra produkter, tekniker och tjänster. RISE Research Institutes of Sweden ägs av svenska staten.



RISE Research Institutes of Sweden AB
Box 857, 501 15 BORÅS
Telefon: 010-516 50 00
E-post: info@ri.se, Internet: www.ri.se

JORDBRUK & TRÄDGÅRD II
RISE Rapport 2024:69
ISBN: 978-91-89971-30-1