PROJEKTNR. 14401

Digitalisering av ledningsanvisning

Utredning av förutsättningar och tester

Gösta Malmqvist
Eningo AB

2025-09-29

Eningo

SBUF
Svenska Byggbranschens Utvecklingsfond

SVEVIA

Förord

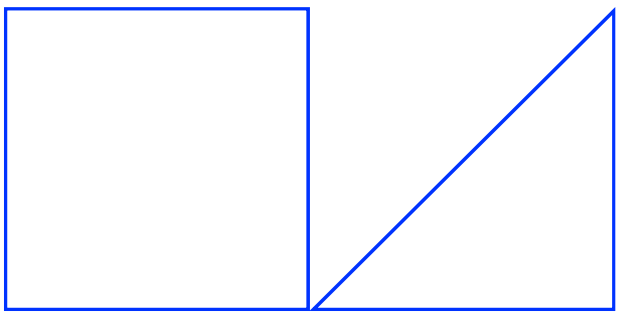
Detta projekt har genomförts som en del i ett flerårigt utvecklingsarbete med målet att digitalisera ledningsanvisning för ökad säkerhet, effektivitet och hållbarhet. Projektet har möjliggjorts genom finansiering från Svenska Byggbranschens Utvecklingsfond (SBUF) och Vinnova samt genom engagemang från samtliga projektparter. Vi vill särskilt tacka Svevia för deras centrala roll i projektet, samt Terranor för tätt samarbete och starkt engagemang. Vi riktar även ett tack till Seko för insikter kring arbetsmiljörisker vid grävskador och Skanska för värdefulla inspel och underlag för test av tredjepartsinmätning. Slutligen vill vi tacka SBUF och Vinnovaprogrammet Avancerad Digitalisering för att ha möjliggjort projektet.

Övriga deltagare är i alfabetisk ordning: BM System AB, Borås stads servicekontor, Falkenberg Energi, Kungsbacka kommun, Laholmsbuktens VA AB, Martin Grävare AB, Mölndals stad, Nordion Energi AB, Nätkraft Borås AB, RISE, Sitech Sweden AB, Statkraft Värme AB, Trimble AB, Vattenfall AB och VTI.

Referenter är i alfabetisk ordning: Bjäre Kraft, E.on, Groundhawk, Lantmäteriet, Seko Skanska samt Trafikverket.

Rapporten har författats av Gösta Malmqvist vid Eningo AB.

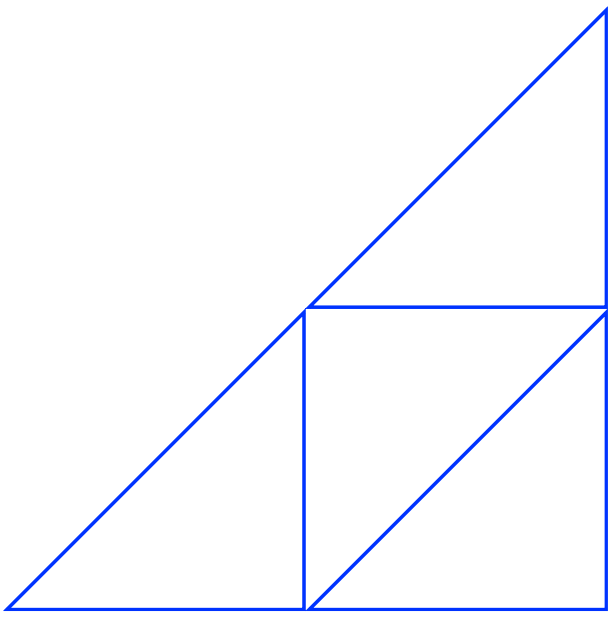
Göteborg den 29 september 2025.



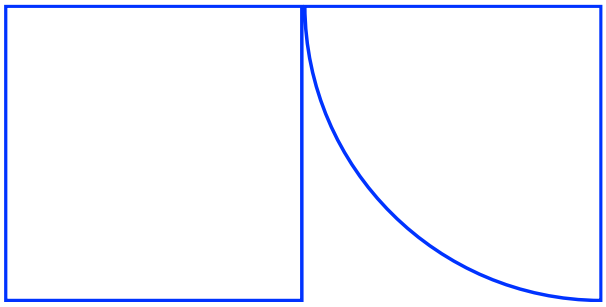
Sammanfattning

Detta projekt har syftat till att vidareutveckla ett koncept för digital ledningsanvisning som ersätter dagens manuella och fysiska utsättning. Projektet har byggt vidare på resultat från en tidigare förstudie och fokuserat på analys av förutsättningar, risker, juridik och ansvarsfördelning samt praktiska tester i fält. Resultatet är mycket positivt: digital ledningsanvisning har bekräftats vara praktiskt användbart, efterfrågat av användare och möjligt att införa utan formella hinder eller verksamhetsrisker. Ansvarsfördelning har tydliggjorts, IT-säkerhetsdesign har tagits fram, och flera lyckade fälttester har genomförts.

Projektet visar att digital ledningsanvisning både kan förbättra arbetsmiljö, minska risker och effektivisera samhällsbyggandet. Arbetet fortsätter i ett pilotprojekt med samma aktörer, vilket delfinansieras av Vinnova genom programmet Avancerad Digitalisering.



Innehåll



1. Bakgrund

Ledningsanvisning är en kritisk del av säkerhetsarbetet vid markarbeten i Sverige. Den nuvarande processen, som innebär fysisk utsättning av ledningars läge, är både tidskrävande, kostsam och sårbar. Fel eller utebliven utsättning orsakar skador på infrastruktur och medför allvarliga arbetsmiljörisker.

Projektet för digital ledningsanvisning syftar till att istället överföra ledningsdata direkt till maskinstyrningssystem och annan användarutrustning. Detta möjliggör snabb, säker och exakt information direkt i fält – vilket minskar ledtid, ökar säkerheten och eliminerar behovet av manuell utsättning i många situationer. Det aktuella projektet har byggt vidare på en avslutad förstudie och fokuserat på att utreda förutsättningarna för digital ledningsanvisning, testa konceptet praktiskt och analysera krav, ansvar och risker.

2. Syfte och mål

Syftet med detta projekt har varit att utreda praktiska, juridiska, tekniska och organisatoriska förutsättningar för digital ledningsanvisning, samt att testa konceptet i verkliga situationer. Projektet har haft som mål att ta fram en prototyp, skapa förankring kring ansvarsfördelning, identifiera och hantera risker, samt säkerställa att lösningen är förenlig med gällande lagar och IT-säkerhetskrav.

Målet har också varit att visa att lösningen är praktiskt användbar för aktörer i branschen – från entreprenörer och maskinförare till ledningsägare och systemleverantörer.

3. Genomförande

Genomförandet har delats upp i fem arbetspaket (AP1–AP5), där varje paket fokuserat på olika delar av utvecklingsarbetet. Projektet har varit testdrivet och iterativt, delvis undantaget arbetspaket 1 Förutsättningar, vilket i mindre grad byggt på resultat från tester och mer på en tidigare förstudie. Projektet har i stort följt ursprunglig plan (se Figur 1 - Projekttidplan nedan), med undantag för arbetspaket 1. Den juridiska kartläggningen som togs fram under tidigare förstudie kunde inte kompletteras som avsett då flera förslag till ny svensk lagstiftning (ex. CER och NIS2) försenats. Dessa kommer dock kunna arbetas in under efterföljande pilotprojekt. Regelbok för datadelning samt risk- och ansvarsutredning tog längre tid att förbereda och analysera än förväntat, men kunde avslutas inom reserverad reservtid.

	2024		2025	
Arbetspaket	**Q3**	**Q4**	**Q1**	**Q2**
AP1 Förutsättningar			[Reservtid]	
· Juridik	Juridiska krav exkl. kommande lagstiftning specificerade	· Krav inkl. kommande lagar specificerade · Sammanfattning för intressenter framtagen		
· Informationssäkerhet och datadelning		Regelbok för datadelning klar		
· Ansvarsfördelning och risker	Ansvarsfördelning överenskommen	Riskanalys klar		
· Hantering av varierande datakvalitet		Metod för visualisering av osäkert läge klar		
AP2 Digitala ledningsanvisningar				
· Avgränsade områden	Första fälttest genomfört	Behovsägares krav formulerade		Lyckat test parallellt med fysisk utsättning
· Vägunderhåll		Första fälttest genomfört	Behovsägares krav formulerade	
· Projektering	Behovsägares krav formulerade			
AP3 Sömlös inmätning				
· Inmätning av kontrakterad personal	Behovsägares krav formulerade	Första fälttest genomfört (gemensamt)	Inmätningsfil förmedlad mha. prototyp	
· Inmätning av tredje part		Första fälttest genomfört (gemensamt)	Behovsägares krav formulerade	Inmätningsfil förmedlad mha. prototyp
AP4 Prototyputveckling				
· Bakomliggande funktionalitet	Integration med första ledningsägare	Integration med första systemleverantör	Design för lagring och bearbetning av data klar	Data förmedlad från ledningsägare till systemlev.
· Användar-funktionalitet		Mockup av användargränssnitt klar	Första version av användargränssnitt klart	Koncept för visualisering av osäkert läge klart

Figur 1 - Projekttidplan

Projektets genomförande redovisas översiktligt nedan, med hänvisningar till bilagor med detaljerad information. Se även bifogat nyhetsbrev från 2025-05-05 för mer utförliga beskrivningar och bilder från de större aktiviteter som genomförts inom projektet fram till dess.

3.1 AP1: Förutsättningar

Inom AP1 har en fördjupad analys av intervjuer från förstudien genomförts. Identifierade risker, krav och ansvar har sammanställts och diskuterats i en halvdags fysisk workshop. Detta som en del i projektets fysiska konferens i februari 2025 i Göteborg. Därefter har två större uppföljningsmöten hållits för att stänga återstående riskpunkter. Därutöver har VTI och Eningo arbetat med framtagandet av en regelbok för rättvis och säker datadelning, vilket initierades i en gemensam fysisk workshop under nämnda projektdagar. Utkastet kommer under efterföljande pilotprojekt gå ut på remiss till

projektparterna och eventuella justeringar göras innan regelboken fastslås.

3.1.1 Leverabler från AP1

Följande leverabler har producerats inom projektet:

- Grundlig riskidentifiering där alla identifierade risker och åtgärder är accepterade av samtliga parter
- Fördelning av ansvar mellan intressentkategorier (ledningsägare, utförare, systemleverantörer och dataförmedlare)
- IT-säkerhetsdesign (endast sammanfattning bifogas)
- Utkast till regelbok för rättvis och säker datadelning mellan aktörer

3.2 AP2: Konceptdesign för digital ledningsanvisning

Arbetet har delats upp efter de tre användningsområdena: Avgränsade områden, väg-underhåll och projekteringsärende. Utvecklingen har skett iterativt baserat på resultat från förstudie och AP1 och i samverkan med prototyputveckling i AP4.

Arbetet med att förstå användar- och kundbehov har drivits genom tester på kontor och i fält samt s.k. mockups och prototyputveckling för att verifiera kravbilden i ytterligare tester. Fälttester har genomförts med hjälp av manuell dataförmedling till användarsystem med syftet att förstå hur tillgängliga ledningsdata ska presenteras för att bli värdeskapande information för utföraren, bland annat gällande hantering av osäkert läge, okänd höjd och nödvändiga metadata.

Flera lyckade fälttester har genomförts i Kungsbacka, Borås, Särö och Finspång. Dessa tester har omfattat både kombinerad fysisk och digital ledningsanvisning samt enbart digital. Särskilt viktigt var testet i Särö tillsammans med Kungsbacka kommun och Norconsult som visade att digital ledningsanvisning fungerar fullt ut i praktiken. Fälttestet utanför Finspång var kombinerad fysiskt och digital ledningsanvisning i BM Systems ledningssystem Road Service under Svevias och Bröderna Bäckströms entreprenad för trumbyten.

Två demonstrationer av digital ledningsanvisning med AR i handenhet har också genomförts. I Göteborg i november 2024 genomfördes en demonstration av AR-handenhet, totalstation och kombinerad kabelsökare och GPS-instrument för sömlös inmätning tillsammans med Vattenfall Services, Vattenfall R&D, Trimtec, Trimble och Eningo. I april 2025 i Västerås genomfördes test i Västerås tillsammans med Vattenfall Services, Vattenfall R&D, Sitech, Maicon entreprenad, RISE samt Eningo.

3.1.2 Leverabler från AP2

Följande leverabler har producerats inom projektet:

- Bevis på att digital ledningsanvisning är praktiskt användbar som ersättning för fysisk utsättning

- Verifierad användarnytta och preferens för digital anvisning
- Funktionalitet testad i både maskinstyrningssystem och vägunderhållssystem
- Fördjupad kravbild och önskemål om funktionalitet från användare i fält
- Visuellt förmedlade osäkerhetsområden har validerats som bästa metod vid relativt osäker ledningsposition

3.3 AP3: Konceptdesign för sömlös inmätning

Under konceptet sömlös inmätning ingår tre enkla och skalbara metoder för att öka inmätningsgraden för underjordiska ledningar och därmed minska antalet ledningar med osäkert läge. Under projektet har en tydlig bild tagits fram av de möjligheter och förhållanden som finns för att uppnå sömlös inmätning. Ett lyckat fälttest av tredjepartsinmätning genomfördes i Falkenberg. En prototypapp inklusive design i Figma togs fram för rapportering av felaktigt inritade ledningar och grävskador. En enkätundersökning genomfördes med 20 svar och kompletterades med en digital workshop med 15 deltagare från 10 bolag med både beställare och utförare.

Resultaten med de tre metoderna beskrivs kort nedan samt utförligt i bifogade dokument.

3.3.1 Inmätning i öppet schakt vid förläggning av nytt nät

Genom att möjliggöra snabb inmätning i små sektioner och av personal på plats kan inmätning göras i öppet schakt och inte i efterhand ovan mark, som alltför ofta sker idag. I projektet kommer vi ta fram och testa ett enkelt och sömlöst flöde från utförarens handinstrument till beställarens NIS.

3.3.2 Integrerad koordinatinmätning i samband med tonsättning under fysisk utsättning

Idag finns flera kombinationsinstrument för både kabelsökning med ton och koordinatinmätning. Dessa möjliggör samtidig utsättning och inmätning, men metoden nyttjas idag alltför sällan på grund av efterarbetet med att lägga in mätfiler och rätta dokumentationen. I projektet kommer vi ta fram och testa ett sömlöst flöde från utsättarens kombinationsinstrument till dokumentationsingenjörens NIS.

3.3.3 Nyttjande av tredjepartsinmätning vid externa schaktarbeten

Varje gång en entreprenör uppmärksammar att en ledning ligger fel i förhållande till anvisning eller karta skulle entreprenören kunna mäta in ledningen och skicka en mätfil till ledningsägaren för rättning. På så sätt skulle alla de tillfällen då fel uppmärksammas, kompetens och utrustning finns på plats och schaktet är öppet kunna tillvaratas för att höja dokumentationskvaliteten. Problemet idag är att kontaktvägar, tillit och krav på mätning samt metadata saknas, vilket hindrar en storskalig förbättring av nätdokumentation. I projektet kommer vi ta fram och testa en teknisk lösning för att enkelt skicka, granska och ta emot mätningar från tredje part.

3.3.4 Leverabler från AP 3

Följande leverabler har producerats inom projektet:

- Sammanfattning av workshop kring flödet från fält till GIS/NIS
- Enkätsammanställning av behov och utmaningar
- Informationsflödesdesign för sömlös inmätning
- Appdesign och prototyp för användarrapportering

3.4 AP4: Prototyputveckling

En teknisk prototyp togs fram för att generera filer i vektorformat från ledningsägares NIS-databaser och vidareförmedla dessa till användarsystem. Arbetet omfattade även framtagning och revision av en IT-säkerhetsdesign med stöd av informationssäkerhetsspecialister från RISE.

3.4.1 Leverabler från AP 4

Följande leverabler har producerats inom projektet:

- Prototyp för dataöverföring från NIS till maskin- och ledningssystem
- IT-säkerhetsdesign (endast sammanfattning bifogas med hänsyn till skyddsvärd information om hur informationssäkerhet upprätthålls)

3.5 AP5: Projektledning

Inom arbetspaketet har redovisning, arbetsledning, planering, intervjuer, workshops, prioritering, uppföljning och intern kommunikation genomförts. Därutöver har projektet löpande kommunicerats till branschaktörer. Två presentationer har gjorts för Energiforsk i september och december 2024 och en presentation genomfördes för Elinorr (samverkansorganisation för 18 elnätbolag) i mars 2025. Fyra artiklar har tagits fram varav tre publicerats i olika branschmedier och en planeras till RISE:s hemsida i augusti.

3.5.1 Leverabler från AP 5

Följande leverabler har producerats inom projektet:

- Tre presentationer för branschorganisationer
- Fyra artiklar i tre tidningar och en för publicering i augusti på RISE:s hemsida
    - Byggindustrin - Startup vill minska grävskador med AR-teknik och digital data
    - Entreprenad – Säkrare grävning är målet (öppen)
    - Entreprenad – Kabelkoll på sekunden (öppen)
    - Byggkoll - Utvecklar tjänst för digitala ledningsanvisningar

4. Resultat

Projektet har resulterat i flera tydliga och användbara leverabler inom alla arbetspaket. Samtliga planerade aktiviteter har genomförts och målsättningarna har uppnåtts eller överträffats. Det mest avgörande resultatet är att digital ledningsanvisning bevisats fungera praktiskt i fält och att intresset och efterfrågan från både användare och ledningsägare är mycket stort.

Nedan listas de viktigaste resultaten:

- Flera lyckade fälttester i verklig driftmiljö, inklusive ett test med endast digital ledningsanvisning
- Verifierad användarnytta för både maskinstyrningssystem och fordonsledningssystem
- Framtagna ansvarsprinciper accepterade av samtliga parter
- IT-säkerhetsdesign som bedömts som hanterbar enligt RISE:s experter
- Prototypprogramvara för överföring av ledningsdata mellan system
- Prototypapp för rapportering av grävskador och felaktigt inritade ledningar
- Dokumenterade krav och informationsflöde för sömlös inmätning

5. Slutsatser

Projektet har visat att digital ledningsanvisning är både möjlig, säker och efterfrågad. Ett antal slutsatser kan dras:

- Inga juridiska hinder har identifierats för att skriva avtal om datadelning mellan intressenter
- Inga oacceptabla risker tillkommer vid digital ledningsanvisning
- Många av dagens risker med fysisk utsättning elimineras eller minskas vid digital hantering
- Digital ledningsanvisning har bevisats fungera i praktiken
- Användarbehov och preferens för digital anvisning är starka, särskilt bland maskinförare och fältpersonal
- Ansvarsförhållanden har tydliggjorts och accepterats
- Sömlös inmätning är tekniskt möjlig och efterfrågas av både ledningsägare och entreprenörer
- För att sömlös inmätning av tredje part ska fungera för ledningsägare krävs även fotodokumentation som komplement till vektorfiler
- Visuellt förmedlade osäkerhetsområden är den bästa lösningen för att hantera ledningsdata med viss osäkerhet
- IT-säkerhet kan hanteras enligt framtagen design enligt RISE:s informationssäkerhetsspecialister

6. Tack

Projektgruppen vill rikta ett särskilt tack till Svevia som möjliggjort projektets genomförande och bidragit aktivt genom hela processen. Vi tackar även Terranor för ett mycket gott samarbete och värdefull input. Seko har bidragit med viktig information om hur arbetsmiljön påverkas och vilka risker för personskador som är förenade med grävskador på ledningar – ett område där projektets lösning kan göra stor skillnad.

Avslutningsvis vill vi tacka SBUF för det finansiella stödet och för att ni möjliggjort att detta arbete kunnat genomföras.

7. Bilagor

Följande bilagor bifogas nedan:

1. Sammanfattning av IT-säkerhetsdesign (AP4)
2. Utkast Rulebook model for a Fair Data Economy (AP1)
3. Erfarenheter från digital ledningsanvisning i Kungsbacka (AP2)
4. Sammanfattning av workshop om inmätning till GIS (AP3)
5. Nyhetsbrev #1 (AP1-5)

Följande bilagor delges vid förfrågan:

6. Fastställda risker och ansvar vid digital ledningsanvisning (AP1)
7. Research av GIS och inmätning sammanställning (AP3)
8. Sammanställning och visualiseringar av research sömlös inmätning (AP3)
9. Kod till prototypprogramvara (AP4)

Bilaga 1 IT Sammanfattning av IT-säkerhetsdesign

SBUF Summary: Strengthening Security and Compliance for Eningo's Next-Generation Utility Platform

As part of our ongoing innovation initiative supported by SBUF, we have conducted a comprehensive review and enhancement of the **Eningo platform's security and compliance strategy**. This work ensures alignment with emerging **EU cybersecurity directives (e.g., NIS2)** and international standards such as **ISO/IEC 27001**.

Key outcomes include:

- **Risk and threat modeling updates**, drawing from EU threat intelligence (ENISA) to prioritize high-impact scenarios such as supply chain compromise, data misuse, and DDoS risks.
- Drafting of a **lightweight Incident Response SOP** aligned with **NIS2 reporting timelines**, ensuring readiness ahead of the 2026 enforcement date.
- Clarification of **shared security responsibilities** between Eningo and partners, establishing a robust governance foundation for future integrations and data-sharing models.
- Inclusion of security roadmap objectives, including **TLS 1.3 migration** and **post-quantum cryptography (PQC) planning**, reflecting a future-resilient cryptographic posture.
- Review and planning for enhancements in **identity and access controls**, including MFA and session handling best practices.

This proactive effort significantly raises the platform's maturity and audit-readiness, supporting safe digitalization in the underground utility sector.

Bilaga 2 Utkast Rulebook model for a Fair Data Economy

Version 3.0

Editors: Olli Pitkänen, Marko Turpeinen & Viivi Lähteenoja, 1001 Lakes Oy

The work is funded by Sitra.

The templates in the Part 2 of the Rulebook model for data spaces enable organisations to create their own rulebooks for their data spaces and support when defining the legal relations within data spaces. the templates are provided in an editable form so that they can easily be made into an actual rulebook to be adopted by a specific data space.

Contents

Introduction to Part 2

The purpose of this rulebook model is to provide an easily accessible and usable manual on how to establish a data space and to set out general terms and conditions for data sharing agreements. This rulebook model will help organisations to form new data spaces, implement rulebooks for those data spaces, and promote fair data economy in general. With the aid of a rulebook, parties can establish a data space based on mutual trust that shares a common mission, vision, and values.

A rulebook based on this model and adapted for a real-life data space, establishes a data space governance framework, which in turn defines the data space itself. Therefore, a rulebook is the central documentation of a data space.

A rulebook also assists data providers and data users to assess any requirements imposed by applicable legislation and contracts appropriately in addition to guiding them in adopting practices that promote the use of data and management of risks. However, despite the rulebook model, it is important to note that the parties still need to ensure that all the relevant legislation, especially on the national and regional levels as well as specific legislation regulating the data in question, is considered.

The general terms of the rulebook model as well as most of the glossary, code of conduct, and checklists in contract annexes are the same for all the data spaces that use the fair data economy rulebook model. Only the specific terms are written case by case.

Therefore, it is easier and more cost-effective to create data spaces and ecosystems if the rulebooks of different data spaces have substantially similar basis. It simplifies collaboration and data sharing even between data spaces and makes it easier for an organisation to participate in several data spaces. Similar rulebooks ensure fair, sustainable, and ethical business within the

data ecosystems, which in turn enables increasing know-how, trust, and common market practises.

The following templates will enable organisations to establish rulebooks for their data spaces and have been prepared to support in defining the legal relations within their networks. During the development of these templates, it was kept in mind that data spaces will differ from one another materially in several respects and that it is not feasible to establish general templates for a rulebook that would be complete and ready to use as-is for all data spaces.

As such, the founding members must plan, design, and document each data space carefully by amending and supplementing the templates in a manner that best serves the purposes of the contractual framework they require. In this regard, the templates provided herein should constitute a baseline that serves as a generic structure for data spaces.

This Part 2 of the Rulebook is provided as an editable text document so that it can be easily modified into the actual Rulebook that can be adopted by a specific data space. Once the modifications are ready, the contracts can then be copied directly and signed by the parties involved as needed.

The templates and tools provided include:

- **Data Space Canvas** tool
- **Checklists**, including business, governance, legal, and technical
- **Rolebook** tool
- **Servicebook** tool
- the **General Terms and Conditions** (to be used as-is)
- a template for the **Constitutive Agreement**
- a template for the **Accession Agreement**
- a template for the **Governance Model**
- a template for the **Dataset Terms of Use**

We recommend that the data space's founding members work together to modify each of the templates. Various tools are provided in the templates to support the modification and adaptation work. Different roles from the different parties should be involved in the modification process from the beginning. Specifically, modifications to the Description of the Data Space, the Constitutive Agreement, the Accession Agreement, the Governance Model, and the Dataset Terms of Use, as well as getting to know the General Terms and Conditions, should always include parties' legal roles. Work on the Description of the Data Space, the Code of Conduct, and the Dataset Terms of Use will benefit from executive, business development, and technical roles' contributions in addition. It is possible and even encouraged to work on the different parts of the rulebook simultaneously, as decisions made in one context will affect possibilities in

another. We do, however, recommend beginning work with the Description of the Data Space to begin more concretely co-defining the objectives and motivations for the network.

Glossary

Sitra Rulebook v2.1 and v3.0 terminology	Notes
Data: any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording. (DA Art 2(1), DGA Art 2(1))	
Personal Data: any information relating to an identified or identifiable natural person. (GDPR Art 4(1))	
Dataset can be either a *Data set*, i.e., "a resource, comprising a collection of data published or curated by a single party and available for access or download in one or more representations", or a *Data product*, i.e., "a set of resources that complies with a data product specification and for which a data product owner has created and published a data product offering."	In the Contractual Framework of the Rulebook, "Dataset" means a collection of Data the use of which is authorised by the Data Provider via the Data Space. Datasets and their related terms and conditions are defined more in more detail in the respective Dataset Terms of Use. According to the DSSC Glossary v3.0, *Data set*: "A resource, comprising a collection of data published or curated by a single party and available for access or download in one or more representations." While, *Data product*: "A set of resources that complies with a data product specification and for which a data product owner has created and published a data product offering."
Data sharing*: Access to or processing of the same data by more than one authorised entity Data can be shared, for example, (i) by allowing access to, or the execution of operations over, the original dataset, or (ii) by giving a copy of the data to the interested entity. The way in which data is shared*	See ISO/IEC 20151.

fundamentally influences the available controls and the statements needed in the Rulebook.	
Data Space: a distributed system defined by the Rulebook and enabling secure and trustworthy data transactions between participants while supporting trust and data sovereignty. A data space is implemented by one or more infrastructures and enables one or more use cases.	In the Contractual Framework of the Rulebook, "Data Space" means the group consisting of the Parties who share Data in accordance with the Constitutive Agreement.
Rulebook: A binding set of documents that record the Data Space governance structure and thus define the Data Space.	In the DSSC Conceptual Model, a Data Space Governance Structure defines a Data Space.
Founding Member: an initial Data Space Participant that executes the Constitutive Agreement.	
Data Space Participant: a party committed to the Rulebook of a particular Data Space and having a set of rights and obligations stemming from this Rulebook.	
Data Space Governance Authority*: One or more parties that establishes, governs, manages and enforces the Rulebook of a Data Space. The Governance Model is a tool to define a contractual arrangement or a legal entity to set up the Data Space Governance Authority.*	See Governance Model
Data Provider: a Data Space Participant that, in the context of a specific data transaction, technically provides Data to the Data Users that have a right or duty to access and/or receive that Data.	In the Contractual Framework of the Rulebook, "Data Provider" means any natural person or an organisation that provides Data for the Parties to use via the Data Space.

Service Provider: a Data Space Participant that provides value adding services on top of Data or Datasets in the Data Space.	In the Contractual Framework of the Rulebook, it is defined that "Service Provider" means any of the Parties that combines, refines and processes data and provides the processed Data and/or a service, which is based on the Data, to the use of Data Users, other Service Providers or Third-Party Data Users.
Data User: a Data Space Participant to whom the right(s) to use Data are granted.	A Data User can be a 'data recipient' as defined by DA 2(14) or a 'data user' as defined by DGA 2(9). In the Contractual Framework of the Rulebook, "Data User" means any of the Parties to which Service Providers provide Data and/or services or to which the Data Provider provides Data, and which do not redistribute the Data further.
Operator: a provider of one or several technical, legal, procedural or organisational services that enable data transactions to be performed within the Data Space. These may include, for example, identity management, consent management, logging, and/or service management and may or may not fall in the scope of the data intermediation service providers defined by the DGA.	In the Contractual Framework of the Rulebook, "Operator" means any Party that provides data system or any other infrastructure services for the Data Space that are related e.g., to identity or consent management, logging or service management.
Data Rights Holder: an entity (a human being or a legal entity) that has rights and/or obligations to grant access to or share certain personal or non-personal data. The Data Rights Holder, taking into account other Data Rights Holders who have rights to the same data, may on its own behalf grant other actors' permissions to use the data. There can be any number of Data Rights Holders regarding	An actor whose permission is needed to process data, e.g. an individual data subject (GDPR), IPR rights holder (e.g. an author), a business having trade secrets, or a contracting party to have contractual rights in data.

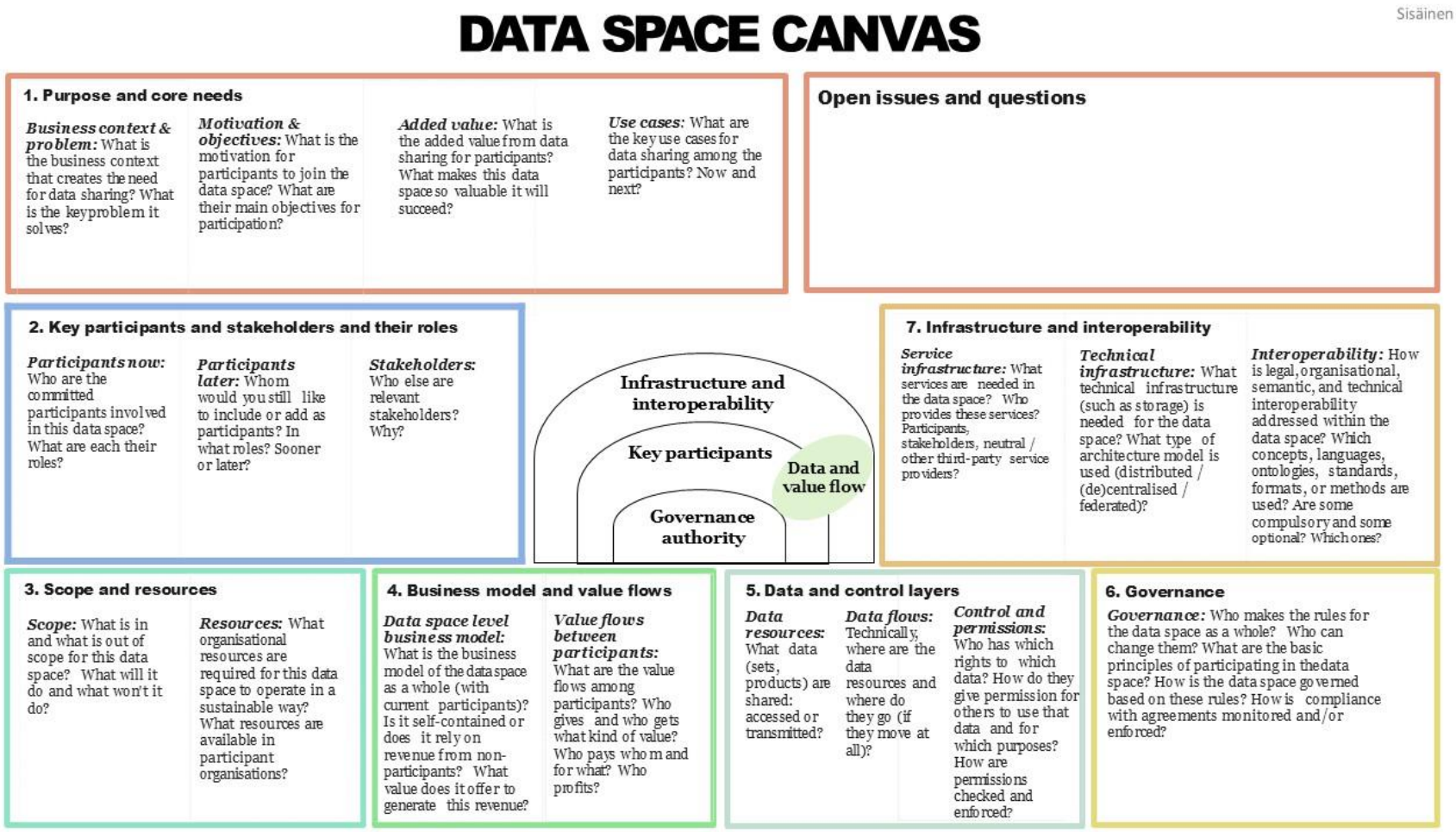
certain Data, and they may transfer such rights to others.	
Third-Party Data User: an entity (a human being or a legal entity) that is not a participant of the Data Space that the rulebook governs, but who receives or uses data technically (otherwise like a "Data User", but not a Data Space Participant).	
Permission*:* any legal right to the processing of Data (not only non-personal data as defined e.g. in the Data Governance Act). A Permission can be for example a consent, a contractual obligation, a legal obligation, a vital interest, a public interest, an exercise of official authority, a legitimate interest, or use of a connected product, if it legally authorises that specific processing of the Data.	
Permissioning: managing all kinds of legally relevant Permissions to use Data: not only active expressions of right holders' will, like consents, licenses, and agreements, but also for example direct legal rights to process Data for a specific purpose or processing data for the purposes of legitimate interests subject to certain requirements. Permissioning is a process in which all the relevant Data Space Participants and external parties, e.g. Data Rights Holders, Data Users, Third Party Data Users, Operators, and Service Providers, contribute their share.	

Data Space Canvas [TOOL]

The Data Space Canvas in the next page helps to describe the logic of the different aspects of your Data Space. Use crisp and short answers to describe the key points.

The Data Space Canvas can be completed and extended by answering the rulebook checklist questions (Business, Governance, Legal, and Technical).

Figure 1: Data Space Canvas



Checklists [TOOL]

The following thematic checklists are provided as a reference and starting point to help in the design of a data space. They serve as a complement and a deep-diving tool to the DSSC Co-Creation Method[1]. The Co-Creation Method also includes questions to consider, and it takes a sequential approach to addressing different aspects of data space development processes, whereas these checklists are arranged thematically into Business, Governance, Legal, and Technical sections. If a checklist question below is included also in a step of the Co-Creation Method, this is indicated with the notation "CCM1.2" where the first number ("1") refers to the process and the second number ("2") to the step within that process as included in v1.5 of the Co-Creation Method.

To use these checklists, provide your response for each question, also considering the contractual requirements implied. The goal is not to answer each checklist question thoroughly, but to use the questions as assistance in formulating the different aspects of the data space design. Link further materials to the topics or the chapter at the end of the section and add additional headers, if needed. Check also that the content here is in line with other parts of the rulebook, and that potential overlaps are minimised.

Business Checklist [TOOL]

The business dimension of the Data Space can be defined by answering the checklist questions in the table below. Comments provide further guidance and examples for answering these questions.

Business questions are categorised as follows:

- B1: Purpose and core needs
- B2: Business model and value flows
- B3: Data services and infrastructure

B1. Purpose and core needs

[1] https://dssc.eu/space/bv15e/766062883/Co-Creation+Method

B1.1. Key purpose and scope (CCM1.1)	Key questions: • What is the business context driving the need for data sharing? • What is the thematic scope of the data space? • What is the key problem it addresses, and what objectives does it aim to achieve? Guidance**:** • Clearly define the thematic focus of the data space (e.g., supply chain optimisation, maintenance services, or data marketplaces). • Identify the specific problem being solved and its potential impact. Examples: • Media industry: “Create a secure and reliable data space for collaboration and joint innovation. • Manufacturing: “Streamline supply chain logistics.” • Energy industry: “Provide a research platform for open innovation in renewable energy.”
Answer:	
B1.2. Motivation and objectives	Key questions: • What motivates participants to join the data space? • What are the primary goals and benefits for each participant? • How do these align with the overall objectives of the data space? Guidance: • Define key incentives for both data providers and data users. • Specify how objectives can be tracked and measured. • Identify also potential barriers to participation, such as data privacy concerns or lack of trust. Examples: • Participants gain access to aggregated analytics and insights. • Reduction of operational costs through shared data. • Fulfilment of regulatory requirements using data sharing.
Answer: 1) effektivisera I att minska grävskador, personskador och skadestånd. Snabbare hantering	

B1.3. Use cases (CCM1.1, 1.2)	Key questions: • What specific use cases should the data space support? • What problem or “job-to-be-done” justifies the need for data sharing? Guidance: • Defining how each identified use case supports and advances the broader goals, mission, scope, effects, and impacts defined for the data space. • Clearly articulate each use case with a descriptive title. • Focus on tangible, actionable applications of data. Examples: • Automotive industry: "Tracking vehicle service recalls." • Food industry: "Calculating the carbon footprint of a food product." • Media industry: “Create a federated data marketplace for 3D models used in VR production.” • Healthcare: "Optimising patient outcomes through shared diagnostic data."
Answer:	
B2. Business model and value flows	

B2.1. Business models (CCM1.1)	Key questions: • Is the data space supporting for-profit on non-profit activities? • What are the key business models applicable to the data space? • How does the data space generate and share revenue? Guidance: • Outline the benefits, value propositions, and expected outcomes that participants can derive from their involvement in each use case, providing insights into individual and collaborative business models. • Establish the business model for each participant and determine how these models contribute to collaborative value created. • *Clearly differentiate between the key business models for the participants, and the business models for data space as an enabling infrastructure.* • Define payment structures (e.g., one-time fees, subscriptions, or royalties). • Consider ethical implications of monetisation models, such as fair data valuation. Examples: • Subscription payment for real-time data streams. • Cost-sharing model for joint projects. • Revenue sharing from aggregated data analytics services.
Answer:	

B2.2. Data value (CCM1.1)	Key questions: • How is data value generated and distributed among participants? • How is the value measured, priced, and monetised? Guidance: • Explore both monetary and non-monetary valorisation mechanisms. • Define pricing models and data valuation criteria. • Consider safeguards for fair compensation, such as licensing fees or usage tracking. • Consider mechanisms for auditing data value generation and distribution. Examples: • Pricing models based on data quality or frequency of access. • Value from aggregated datasets, such as industry benchmarks. • Compensation through reciprocal data exchange ("data-for-data").
Answer:	
B2.3. Data space solution fundamentals (CCM3.1, 3.2)	Key questions: • What resources (financial, technical, and organisational) are needed to sustain the data space? • How will development and operating costs be allocated? Guidance: • Identify required resources for both development and operational phases. • Consider options like in-house development, outsourcing, or partnerships. • Include a contingency plan for funding gaps or unexpected costs. Examples: • Initial development costs shared by founding members. • Operating costs covered through subscription fees. • Technical support provided by a third-party vendor.
Answer:	

B2.4. Level of commitment (CCM1.3)	Key questions: • Are participants fully committed to the data space? • What conditions must be met before establishing long-term commitment? Guidance: • Data space must assess stakeholder business rationale for commitment and readiness for formalisation. Only if stakeholders are committed, governance framework and cooperation agreements can be created. • Define mechanisms to ensure participant engagement and trust. • Address continuity planning and strategic dependencies. • Address potential conflicts and mechanisms for conflict resolution. Examples: • Agreements to share data for a minimum period. • Penalties for early withdrawal from the data space. • Incentives for active contribution to shared goals.
Answer:	
B3. Data services and infrastructure	

B3.1. Data space services (CCM2.5, 3.3, 3.4, 4.5)	Key questions: • What ecosystem-wide data-related services are provided in the data space? • Who is responsible for these services, and how are they managed operationally? • What common rules and instructions apply to these services? Guidance: • Focus on identifying the shared responsibilities and operational aspects of services. • Clearly outline service providers, observability mechanisms, and service-level requirements. • Outline how participants will interact with these services. Examples: • Providing verifiable claims related to participants according to the agreed trust framework. • Ensuring personal data is anonymised before distribution to third parties. • Quarterly audits of data accuracy and compliance with data space standards. • Dashboards for monitoring and tracking the status of the data space.
Answer:	

B3.2. Data discovery	Key question: • How is metadata about data products discovered and shared? Guidance: • Participant can publish metadata about the available data for sharing, including their associated attributes and policies. Similarly, each participant, given the appropriate access policies, can discover such information within the data space. • Data available for sharing cannot be viewed without an applicable data sharing agreement. • Sharing can also include other data products than "raw data sets", for example results of a data analysis or AI models. Examples: • Metadata is shared in a federated catalogue to facilitate the negotiation of data sharing contracts. • Data stays at the source and only the calculation results would be shared via an API or calculated via a virtual machine loaded at the data provider.
Answer:	
B3.3. Data usage control	Key questions: • What permissions and restrictions are in place for data use? • What activities must be performed before data can be utilised? • Are there defined limitations on data access, manipulation, and distribution? • Can data be redistributed, and under what conditions? Guidance: • Specify, for example at the use case level, principles for data use, including access levels, usage duration, and sharing limitations. • Address restrictions to ensure balance between openness and control. Examples: • Data may be used for R&D purposes only, with no redistribution. • Data must be anonymised and validated before use. • On-off use license with usage reporting back to the data provider. • Further distribution allowed only with permission from the original data provider.

Answer: Av data bör framgå vad för typ av ledning och då ska maskin vara kunna styra hur man schaktar vid just den ledningen. I dagsläget används sunt förnuft om hur vi delar information exempelvis om vi skickar ut stora områden till frågare. Säkerhet och säkerhetsklassade anläggningar. Behov av rutin för hur mycket man kan lämna ut Av datat behöver det framgå vilken typ av ledning det är, och vilket krav kring arbetet som följer med det.	
B3.4. Consent management	Key questions: • How is personal data consent managed, monitored, and reported? • What mechanisms ensure consent aligns with usage controls? • How is interaction with consent givers facilitated? Guidance: • Provide transparency on consent-related processes to build trust with Data Space participants and individual users. • Implement consent management processes that comply with data privacy regulations (e.g., GDPR). • Define systems for capturing, updating, logging, and auditing user consents. Examples: • Consent management service for capturing, tracking, and reporting user consents. • Dynamic reporting to track consent validity and usage against policies. • Clear interfaces for individuals to revoke or update consent.
Answer: Tjänsten måste kunna behandla personuppgifter be om syfte med informationen. Om man efterfrågar säkerhetsklassad info så ska man kunna kräva att personen säkerhetsklassas. Borde inte vara personinfo i datat. Säkerhetsklassad data behöver egen hantering.	

B3.5. Data location and availability (CCM2.2)	Key questions: • Have data location and availability practices been defined? • How are data lifecycle responsibilities managed and transferred? Guidance: • Clarify under what conditions data remains available. • Define lifecycle management principles. • Define SLA commitments for data availability and reliability. Examples: • Data will be stored on EU-based servers to comply with GDPR requirements. • Real-time availability as a data stream for operational data; archival storage for historical data. • Data rights will be transferred to a specified party when the project phase ends.
Answer:	
B3.6. Data quality	Key questions: • How is data quality ensured and maintained? • What improvement actions are needed to address quality issues (e.g., missing or outdated data, or metadata)? • Who is responsible for maintaining and measuring data quality? Guidance: • Establish processes for data quality management. • Define participant roles responsible for data quality validation and improvement. • Include indicators to measure data accuracy, completeness, and timeliness. Examples: • Data products must meet predefined completeness and format requirements. • Latency of data delivery must not exceed 10 seconds. • Quarterly reviews are conducted to measure data quality using agreed quality indicators.

<table>
<tr><td colspan="2">Answer: Ledningsägare ansvarar för kvalité. Med tiden ökar kvalitén ju mer som blir inmätt.
Bra att ange kvalité på data.

Randomized task

Ledningsägare men finns ej data behövs fyskisk utsättning.</td></tr>
<tr><td>B3.7.
Operational monitoring and administration (CCM4.4)</td><td>Key questions:
How is the monitoring and reporting of system and data use achieved?
What are the traceability and logging mechanisms?
Is monitoring real-time or retrospective?
Guidance:
Define practices for tracking data access, use, and performance.
Discuss the need for monitoring all transactions, also from the viewpoint of business secrets.
Include traceability to ensure transparency and compliance with agreed-upon rules.
Examples:
Centralised logging of data transactions with timestamps and participant IDs
Dashboards displaying live metrics on data access and usage.
Logs need to be tamper-proof, provided by a trusted party, and accessible for dispute resolution or compliance checks.</td></tr>
<tr><td colspan="2">Answer: Att frågaren är på den plats som den frågar på.
Att man bara får del av informationen när man är inom grävområdet

Autonomous
Data qualilty - monitoring</td></tr>
</table>

B3.7. Data space skills and capabilities	Key questions: • What are the essential skills and capabilities needed to develop, manage, and operate the data space? • How will these skills be sourced (e.g., training, hiring, partnerships)? • What gaps currently exist in skills and capabilities, and how can they be addressed? Guidance: • Identify the core competencies needed across different areas: technical expertise, data governance, legal compliance, business development, and ecosystem management. • Ensure skills align with the needs of data operations, platform management, and ecosystem sustainability. • Identify and offer training and certification programs for participants to standardise skillsets across the data space Examples: • Data engineers for setting up data pipelines using data space connectors. • Data stewards responsible for developing and managing data quality, consistency, and interoperable metadata standards. • Ecosystem managers to develop partnerships and foster collaboration between participants. • IP specialists to manage the rights related to data products.
Answer:	

Issues and questions

[In this part, please consider open issues and questions related to the Business Checklist.]

Links to related documentation

[Add here other potential documentation related to the business design of the Data Space.]

Governance Checklist [TOOL]

The governance dimension of the data space can be defined by answering the checklist questions in the table below. Comments provide further guidance and examples for answering these questions.

Governance questions are categorised as follows:

- G.1: Key participants and stakeholders and their roles
- G.2: Governance principles and responsibilities

<table>
<tr><td colspan="2">G1.Key participants and stakeholders and their roles</td></tr>
<tr><td>G1.1.
Data space stakeholders (CCM1.1, 1.3)</td><td>Key questions:
Who are the key participants in ecosystem implementing the data space?
What additional participants or external stakeholders (e.g., regulators, industry associations) should be considered?
What are the growth ambitions for the data space?
Are there any eligibility criteria, limitations, or requirements for joining the data space?
Guidance:
Identify the categories of participants and other stakeholders.
Specify any limitations or requirements (e.g., technical readiness, trust levels, compliance) for new participants.
Ensure the ecosystem is designed for fair and trusted collaboration.
Examples:
Additional stakeholders of the data space include government agencies, and standards organisations providing oversight.
Our growth ambition is to expand membership, and to have 5 new large companies and 30 new SMEs as participants over the next 3 years.</td></tr>
<tr><td colspan="2">Answer: Dataförmedlare, ledningsägare, systemleverantörer

Myndigheter som behöver del av informationen kan vara intressenter

LÄ – till dataförmedlare till IMY, FMB – Access lend koll??</td></tr>
</table>

G1.2. Stakeholder roles (CCM1.3, 5.1)	Key questions: • Who are the founding parties, and what are their roles? • What are the defined roles of participants in the data space? • Are all critical roles fulfilled for launching and managing the data space? Guidance: • Define and differentiate roles to ensure smooth functioning of the data space. • Include both mandatory roles (e.g., data provider, governance authority) and optional ones (e.g., advisory bodies). • Establish processes for role changes or updates.. Example: • Data space governance authority ensures adherence to data space rules and policies.
Answer: Roller och Ansvar måste förtydligas, vara tydliga	
G1.3. Stakeholder rights and responsibilities (CCM3.1)	Key questions: • What are the rights of each actor in the data space? • What responsibilities are associated with each role? • How are these rights and responsibilities communicated and enforced? • Are there mechanisms to resolve disputes related to rights and responsibilities? Guidance: • Ensure there are enforcement and conflict resolution mechanisms. Examples: • Data providers are responsible for ensuring data quality and providing interoperable metadata. • Participants must adhere to data sharing agreements and usage policies.
Answer: LÄ korrekthet i data, korrekt hantering av PU Dataförmedlare – identifikation, säkerhet att info hamnar på rätt ställe, säkerhet. Användare – Använda data korrekt, gräver rätt enligt instruktion. Borde finnas någon form av avtalsförhållande mellan parterna. checklist	

G1.4. Data provision (CCM2.2)	Key questions: • What data sources are available in the data space? • Who controls access to the data? • How are data usage permissions and restrictions defined? Guidance: • Define the scope of data provision, including sources (e.g., IoT devices, enterprise systems, open data platforms). Examples: • Sensor data from smart city infrastructure (e.g., traffic lights, parking sensors). • Sales and inventory data from retail partners. • The data space includes historical data, live sensor streams, and aggregated analytics data.
Answer: En checklista hos användare av data att allt har uppfattats	

G1.5. Data space governance authority	Key questions: • Should there be a separate legal entity to govern the data space? • Is governance achievable through alternative means, such as a steering committee and contractual arrangements? • What decision-making authority and responsibilities will the data space governance authority have? • Who are the key representatives in the data space governance authority, and how are they selected? • How does the data space governance authority ensure fairness, transparency, and trust among participants? Guidance: • Clearly outline the authority and responsibilities of the data space governance authority. Include oversight, conflict resolution, and decision-making powers. • Implement mechanisms for accountability, transparency, and regular reporting to participants, such as public reporting, annual audits, and participant feedback loops. • Ensure the chosen structure aligns with applicable laws (e.g., data sharing regulations, antitrust laws). Examples: • A nonprofit consortium oversees the data space, with founding members acting as board representatives and rotating leadership every 2 years. • A steering committee with 10 elected members has authority to make decisions regarding participation rules, financial matters, and conflict resolution. • The data space operates under a steering committee but is legally represented by a registered nonprofit for managing assets, legal agreements, and compliance.
Answer:	
G2.Governance principles and responsibilities	

G2.1. Data governance (CCM2.2)	Key questions: • What are the data governance principles and responsibilities within the data space? • What are the data storage and availability principles? • What are the data lifecycle management processes (e.g., retention, archiving, and deletion)? Guidance: • Outline the rules, policies, and standards that govern data availability, quality, and usage in the data space. • Define data lifecycle management principles, such as retention periods and access revocation processes. • Implement systems for managing changes to data structures, systems, or governance rules and communicating them effectively to all participants. Examples: • General guideline is that operational data is retained for 1 year, and historical data is archived for 5 years before deletion. • All changes to commonly agreed schemas or interfaces must be approved by the data space governance authority. • Data must remain available 99.9% of the time, with daily backups performed to ensure recovery in case of failures.
Answer:	
G2.2. Risk management	Key questions: • How are risks in the data space identified, managed, and mitigated? • What processes exist for handling data-related incidents, disputes, or breaches? • What are the key risks to data integrity, security, and availability? • How are risks monitored, and how often are they reviewed? Guidance: • Define procedures to address identified risks, including mitigation strategies, escalation protocols and monitoring. • Implement a system to manage incidents such as breaches, disputes, or misuse. Examples: • In case of a data breach, participants must report the incident within 24 hours. A formal resolution process will follow, involving all affected parties. • A quarterly risk audit will assess the effectiveness of risk mitigation measures and propose updates.

Answer:

Issues and questions

[In this part, please consider open issues and questions related to the Governance Checklist.]

Links to related documentation

[Add here other potential documentation related to the governance aspects of the data space.]

Legal checklist [TOOL]

Legal questions are categorised as follows:

- L.1: Contractual premises
- L.2: Liabilities
- L.3: Content

L1. Contractual premises	
L1.1. Applicable law and dispute resolution	Key questions: • Which jurisdiction's (country's) laws are applied to the rulebook? • Have you checked what needs to be modified in the rulebook because of those national laws and have you made the respective derogations to general terms in constitutive agreement? • In which arbitration process or court shall the disputes be finally resolved? Affects: • Constitutive agreement applicable law and dispute resolution and derogations to general terms 3.3 & 4 • Dataset terms of use
Answer:	
L1.2. Permissioning (CCM2.4)	Key questions: • Has the data provider been adequately authorised to grant rights to use data on behalf of the data rights holders? • Should there be a more advanced permissioning mechanism to ensure that all the data space participants and the third-party data users will get the required permissions? Affects: • Constitutive agreement derogations to general terms 3.3 & 4 • Dataset terms of use
Answer:	
L1.3. Data sets	Key question: • Is it correct to assume that it is decided, separately for each dataset, who are granted access to the data, or should there be same rules for all the datasets, like all the data shall be available to all the data space participants?
Answer:	

L1.4. Fees	Key questions: • Is it correct to assume that unless otherwise defined in the dataset terms of use or agreed by the data space participants, the right to use the data is granted free of charge • Or should the data be subject to a charge by default?
Answer:	
L1.5. IPR	Key question: • Is it correct to assume that the provision of data within the data space does not constitute a transfer of intellectual property rights?
Answer:	
L1.6. Third-party access (CCM5.2)	Key question: • Is it correct to assume that the data can be redistributed only to the data space participants, but redistribution of the data to third party data users can be allowed in the applicable dataset terms of use?
Answer:	
L1.7. Derived materials	Key question: • Is it correct to assume that the data space participants are entitled to redistribute derived materials to third parties, subject to possible additional requirements related to intellectual property rights, and confidential information? Guidance: • It should be defined in the constitutive agreement or in the dataset terms of use what is derived material. • the dataset terms of use may specify that the derived material is shared and used e.g. Under Creative Commons CC BY license terms.
Answer:	
L1.8. Personal data	Key question: • Is it correct to assume that where the data involves personal data, by default the data recipient becomes a data controller?
Answer:	

L1.9. Indemnity	Key questions: • Is it correct to assume that the data provider indemnifies other parties against claims that its data, which is subject to any fees, infringes intellectual property rights or confidential information in the country of the data provider? • Should the data provider indemnify other parties also if the data is provided for free? Guidance: • This indemnity clause is quite broad for paid data, but does not cover free data. • The dataset terms of use template also includes the following sample provision: "the data provider shall ensure that it possess all the necessary rights and authorisations to make the data available for the use of the other parties in accordance with the applicable terms and conditions."
Answer:	
L1.10. Termination	Key questions: • Is it correct to assume that the data space participants are entitled to use the data after the termination of the constitutive agreement, in which case the constitutive agreement survives the termination, except for where the constitutive agreement is terminated as a result of data space participant's material breach? • Or should the right to use the data also terminate by default if the constitutive agreement is terminated?
Answer:	
L1.11. Audit	Key questions: • Is it correct to assume that the data provider is entitled to carry out audits related to its data? • Should some others (e.g. The data rights holders) also have auditing rights?
Answer:	

L1.12. Other contracts	Key questions: • Are there contracts outside the rulebook that need to be changed? Example: • The participants have previously entered into a cooperation agreement that contains provisions that are not compatible with the rulebook.
Answer:	
L2. Liabilities	
L2.1. *Real-world actions*	Key question: • Have the liabilities for the data-related real-world processes been defined? Affects: • Constitutive agreement • Dataset terms of use
Answer:	
L2.2. *Other contracts*	Key question: • Are there contracts outside the rulebook that need to be changed? Affects: • Other contracts • Potentially references in constitutive agreement and dataset terms of use.
Answer:	
L2.3. *3rd party participation*	Key questions: • Is the role towards 3rd parties clear? • Who is responsible for 3rd party infringements? • What commitments does the data provider give toward 3rd parties? Affects: • Constitutive agreement • Dataset terms of use
Answer:	

L2.4. *Disclaimers*	Key question: • Have the data related disclaimers been defined for data space participants? Affects: • Constitutive agreement • Dataset terms of use
Answer:	
L3. Content	
L3.1. *Applicable data types*	Key question: • Does the data contain photos, audio – or video content, computer programs, etc. that have special legal requirements? Affects: • Constitutive agreement • Data Space description • Dataset terms of use
Answer:	
L3.2. *Data base rights*	Key question: • Are database rights applicable to data (i.e., there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents)? (EU Directive on the legal protection of databases, Art. 7) Affects: • Constitutive agreement • Dataset terms of use
Answer:	

L3.3. *Common contractual aspects*	Key question: • How to define the data space's approach on common contractual aspects? Examples: • Data space participants' rights and responsibilities • Exclusivity/access • Confidentiality • Liabilities and disclaimers Affects: • Constitutive agreement • Data Space description
Answer:	
L3.4. *Data-specific aspects*	Key question: • How to define the data space's approach on data-specific aspects? Examples: • Conditions to exchange data • Clarity of usage rights • Right to assess, analyse and learn from data • Restrictions on data use within data space • IPR limitations and monitoring of IPR use management of data originating from outside current data space • Conflicts related to data utilisation Affects: • Constitutive agreement • Dataset terms of use
Answer:	

Issues and questions

In this part, please consider open issues and questions related to the Legal Checklist.

Links to related documentation

Add here other potential documentation related to the legal aspects of the Data Space.

Technical Checklist [TOOL]

Summarise and document here the key technical and security aspects and requirements. These aspects reflect common architectural requirements and design principles.

Technical questions are categorised as follows:

- T.1: Capability requirements
- T.2: System design and architecture
- T.3: Functional requirements
- T.4: Information management
- T.5: Security
- T.6: Privacy and personal data

T1. Capability requirements

T1.1. Technical solution fundamentals	Key questions: • What common technical capabilities and services will be implemented? • Who provides these key components and services, and how are they developed? • How will integration across different participants and systems be ensured? • Which functionalities of the data space can be provided by dedicated intermediary service providers? Guidance: • Ensure all key technical solutions comply with standards (e.g. Dataspace Protocol, DSP) for interoperability, governance, and trust. • The core services refer to the minimum set of services required to make the data space function and its (initial) use case(s) work. these may include federation services, participant agent services, and value creation services. • DSSC Value Creation Services building block provides an approach to manage services that extend the core functionality required by the use cases, to create additional value. These services might include data processing, integration, or user experience to maximise the value generated. • DSSC Intermediaries and Operators building block describes how intermediary services can allow participants to join a data space that do not own their own participant agent. • Adopt standard data exchange APIs, connectors, and protocols to facilitate seamless integration across participants and systems. Example: • All data endpoints and interfaces follow the data plane and control plane specifications of DSP for interoperability between systems and participants.
Answer:	

T1.2. Technical skills and capabilities	Key questions: • What technical skills and capabilities are needed to operate the data space? • How will these skills be acquired, trained, or sourced? Guidance: • Outline the technical expertise needed for data integration, data governance, and security. • Provide a strategy for upskilling participants through training or external collaborations. Example: • Data engineers for integration, data analysts for quality monitoring, and cybersecurity experts.
Answer:	
T2. System design and architecture	
T2.1. System design principles	Key questions: • What are the key principles and architectures for system design? • What existing building blocks and standards serve as a foundation? Guidance: • Define over-arching design principles like open standards, vendor independence. • Specify the functional requirements for protocols and interfaces to ensure compatibility and integration with the data models. • Ensure scalability, flexibility, and security of the architecture. • Follow the DSSC building block specifications and recommendations. Examples: • Modular architecture to enable scalability and easy integration with new tools. • The data space must specify the standards and methods for complying with regulations, identifying Trusted Service Providers (TSPs), and managing them according to Electronic Identification and Trust Services (eIDAS) regulation.

Answer:	
T2.2. Metadata and data formats (CCM2.2, 4.3)	Key questions: • How will the data space manage semantics for the defined data products? • What standards are used for data and metadata formats? • What is the level of ambition for semantic interoperability, both within the data space and across data spaces? • How are metadata incompatibilities resolved? Guidance: • Plan for dynamic updates with a governance mechanism for shared semantics. Example: • The data space participants follow ISO 8000 standards to ensure metadata quality.
Answer:	
T3. Functional requirements	
T3.1. Technical interfaces (CCM4.3)	Key questions: • What technical interfaces are required, and how are they defined? • How will their evolution and backward compatibility be managed? Guidance: • Include plans for managing changes and versioning. Examples: • Certified DSP-compliant connector is a mandatory requirement for participation in the Data Space. • REST APIs are used for secure data exchange.
Answer:	

T3.2. Identity and access management (CCM1.3, 2.4, 4.1)	Key questions: • How will identities and access control be managed, i.e. IAM solutions? • How are trusted participant identities created, managed, and governed? Guidance: • Follow the DSSC building block called "Identity and Attestation Management" which explains how verified identities ensure trust and security within the data space. • Verifiable Credentials (VCs) can be used to describe digital attestations in a data space. Example: • To manage digital identities and verify their information, the data spaces will use W3C Verifiable Credentials and Decentralised Identifiers (DIDs).
Answer:	
T3.3. Data usage control solution (CCM4.2, 4.4)	Key questions: • How are permissions managed? • What standards or solutions are used? Guidance: • Consider solutions for data usage policy creation, policy libraries and user interfaces to assign the policies for data products. • The DSSC Access Control and Usage Policies Enforcement building block provides guidance on specifying role-based access controls, permission settings, and usage policies tailored to each use case to regulate data access and operations. • Open Digital Rights Language (ODRL) should be used for creating and enforcing usage policies. • Federated Services like the Policy Information Point (PIP) can support these functionalities. • Use GDPR-compliant tools and solutions for consent management. Examples: • The participants have to use ODRL to describe the data policies. • Permissions are stored securely using a blockchain-based audit trail.

Answer:	
T3.4. Transaction management (CCM4.5)	Key question: • How are data-related transactions monitored and governed? Guidance: • Consider the standardisation efforts related to trusted transactions in data spaces. Example: • Transactions are validated with digital signatures and blockchain-based confirmation.
Answer:	
T3.5. Data governance solution	Key questions: • What are the data life cycle management and data governance technical solutions? • How to manage the data over its lifecycle from creation to use to its potential deletion? • Is there a way to trace the origin and history of data within the data space? Guidance: • Utilise data governance tools for managing policies, access, and compliance. • Implement monitoring mechanisms to track data usage, changes, and lifecycle status. • DSSC Publication and Discovery building block describes that offerings can be stored and published inside a local or a centralised catalogue. • DSSC Provenance and Traceability building block provides mechanisms to track data lineage. Example: • Data is tagged with metadata that includes creation date, ownership, retention period, and expiration rules. Outdated data is archived after 1 year and securely deleted after 5 years.
Answer:	
T4. Information management	

T4.1. Change control	Key question: • What are the principles for managing changes in the data space? Example: • Git-based repositories are used to ensure controlled deployments.
Answer:	
T4.2. Data location and availability (CCM4.5)	Key question: • Where is the data located, and how is it transferred and made available? Example: • Data has a 99.9% uptime SLA, with redundancy across servers that are located in the EU.
Answer:	
T4.3. Data services (technical implementation)	Key questions: • What data services are provided in the data space? • What are the technical requirements and implementation strategies for these services? • How are these services audited in terms of quality, frequency, and compliance with standards? • Who is responsible for providing, maintaining, and monitoring these services? Guidance: • Identify services, such as federated data catalogue, identity and access management services, vocabulary service. • Specify if the services are to be implemented as centralised, federated or distributed manner. • Ensure these services are scalable, interoperable, and compliant with the data space's technical architecture. Example: • Document all federated services and provide access guidelines for participants.
Answer:	

T4.4. Data quality (technical implementation)	Key questions: • How is data quality measured, monitored, and managed within the data space? • Are there processes for addressing missing, outdated, or inaccurate data? • How is success measured in terms of data quality improvements? Guidance: • Establish clear standards for accuracy, completeness, timeliness, and consistency of data. • Implement automated tools and processes to monitor real-time and historical data quality. Example: • All incoming data undergoes automated validation checks to ensure completeness and compliance with metadata standards.
Answer:	
T5. Security	
T5.1. Security risk and threat assessment (CCM4.2)	Key question: • How are security risks identified, assessed, and mitigated? Guidance: • Data sharing is characterised by the movement of data across organisational boundaries from one physical location to another, for example via a cloud solution. • Security risk assessments need to consider not only physical security and individual organisational issues, but also the risks associated with Data Spaces and network interoperability. Example: • Annual security testing and auditing.
Answer:	

T5.2. Data and data space related threats	Key questions: • What are the key security threats to data and the operation of the data space? • What preventive measures can be implemented to address intentional and unintentional threats? Guidance: • Classify threats into categories like user-based threats (phishing, social manipulation), technical threats (data hijacking, data loss), and operational threats (insider threats, service interruptions). • Ensure that security and privacy breach notifications are specified within the contractual agreements and include penalties for non-compliance. Examples: • Role-based access control (RBAC) ensures only authorised personnel can access sensitive data. • Monitoring tools log all data access and usage to ensure compliance and detect unauthorised actions.
Answer:	
T5.3. Security objectives and regulation	Key questions: • What are the security objectives of each participant and the data space as a whole? • Are there specific regulations governing data security that must be adhered to? • How will compliance with security regulations and objectives be ensured? Guidance: • Clearly define overarching security goals, such as ensuring data confidentiality, integrity, availability, and compliance with regulatory frameworks. • Ensure that security objectives align with relevant laws, regulations, and industry standards. Examples: • Data confidentiality will be ensured through encryption, with strict access controls and monitoring mechanisms. • The Gaia-X framework provides guidelines on security through its federated trust and compliance model, which will be adopted for this data space.
Answer:	

T5.4. Risk and security management process and tools	Key questions: • What processes and tools are in place for identifying, managing, and mitigating risks and vulnerabilities? • How are exceptions, incidents, and damage control handled in the data space? • How is the probability and impact of risks evaluated? • What combination of tools and frameworks ensures transparency, security, and control? Guidance: • Once threats and vulnerabilities have been identified, the severity of the threats to the data space can be assessed, for example by determining the probability of each risk and the magnitude of the damage if the risk materialises. • This will help identify the risks that are most critical to address in the design of the data space • Define workflows for incident detection, reporting, escalation, and resolution. Examples: • Adopt a SIEM (Security Information and Event Management) system for security monitoring, threat detection, risk analysis, and reporting. • Role-based access controls and encryption address unauthorised access risks.
Answer:	
T5.5. Confidentiality of data	Key questions: • How is the confidentiality of data defined, ensured, and managed across the Data Space? • What are the processes for preventing unauthorised access or disclosure of data? Guidance: • Establish clear policies to define confidentiality levels (e.g., public, internal, confidential, highly confidential). Align these definitions with the sensitivity of the data and its impact on participants. • Implement technical measures such as encryption, access control mechanisms, and secure data transfer protocols to protect confidential data.
Answer:	
T6. Privacy and personal data	

T6.1. Inclusion of personal data (CCM2.3)	Key questions: • Does the data transmitted in the Data Space include personal data? • What are the purposes for personal data collection? Guidance: • Personal data means any information relating to an identified or identifiable individual. • Only if it can be certain that the data does not contain personal data can data protection legislation be disregarded.
Answer:	
T6.2. Personal data management solution	Key questions: • How are permissions for processing personal data technically managed, logged, monitored and reported? • Is there a needed e.g., for anonymisation? Guidance: • Anonymisation often requires a case-by-case assessment, but as a general requirement, identification must be irreversibly prevented and in such a way that the controller or other third party can no longer use the data in its possession to make the data re-identifiable. • Note also that pseudonymisation, where personal data can be traced back to a specific individual, for example by means of a code key, is still interpreted as personal data. Example: • Data is anonymised before sharing to ensure GDPR compliance.
Answer:	

T6.3. Personal data related obligations	Key questions: • What are the obligations of each party in the data space regarding personal data processing and protection? • How are data subjects' rights (e.g., access, rectification, erasure) fulfilled, and who is responsible for these obligations? Guidance: • In principle, the information obligations and right of the data subjects based on regulation apply to each party processing personal data, but a rulebook may agree on the joint handling of the information obligations for personal data. • Alternatively, they may not be agreed separately, but each party will manage its own obligations. Example: • Each participant must maintain its own GDPR compliance processes, including consent management, secure storage, and fulfilling data subjects' rights within 30 days.
Answer:	

Issues and Questions

What other issues and questions have emerged during the planning?

Links to related documentation

Add here other potential documentation related to the technology design of the data space.

References and standard

Ethical maturity model [TOOL]

The maturity model presented in next page is tool that is developed to helps organisation to evaluate its ethical maturity. However, it is developed such way that it would help the practitioners to have deeper view of situation in own organisation. Likewise, it provides conceptual and analytical tool that can be used to clarify the question “what should we do” by emphasising issues that needs not only to deal with but give deeper focus and considerations. Hence, the maturity model should not be seen as mere list of checkbox items, that is filled and forgotten. At best maturity model can serve as ground for discussion about organisational culture and values by providing different themes that help to start to critical self-investigation in personal and organisational levels.

Table 1: Ethical maturity model

	Security	Commitment to ethical practices	Transparency and communication	Sustainability	Human-centricity	Fair Networking	Purpose
Level 0	"I believe that this is very secure"	"We prefer not to commit, we are free"	"Just trust us"	"Let it burn"	"What this has to do with the people?"	"Anarchy"	"We do what we want to do"
Level 1	There are proper antivirus, firewall and other needed security tools in use, and they are properly updated.	Organisation follows regulations and the best practices of its own field.	Organisation follows the regulations and uses truthful communication.	Organisation has documented sustainability plan/program.	The individuals are recognised as stakeholder and their rights are taken account.	Organisation aligns it rules and regulations to best practices of industry	Organisation has stated reasons for data collection and usage
Level 2	There is a dedicated person to keep up with information security.	Organisation has implemented and is committed to following ethical code(s) or other codes of conduct.	Organisation supports open internal communication and responsible information sharing.	There is an evaluation model for sustainability with clear indicators.	Organisation collects information of the needs of individuals to improve people-centricity.	Organisation defines and documents practices and provides the needed information for data space participants	Organisation has transparent rules how data can be used in the future
Level 3	There are clearly documented procedures for the preparation of security threats.	There are clear well documented procedures for actions to be taken when ethical issues occur.	There is a transparent, documented plan for internal and external communication	Organisation impact on the environment is neutral or positive.	Individuals have low-level ways to communicate with the organisation and their opinions are systematically noted.	Organisation supports and encourages a fair data sharing in ecosystems.	Organisation negotiates with information sources to gain mutual understanding of fair information use
Level 4	The whole organisation has internalised the importance of security and it is constantly monitored and developed through the organisation.	Organisational policies and procedures are developed critically from ethical perspective together with all relevant stakeholders.	Organisation openly communicates its procedures and policies.	Organisation is actively advancing the sustainability of its business field.	Organisation will actively involve all relevant stakeholders in decision making.	Organisation actively seeks to ways to advance possibilities of whole ecosystems.	Organisation has clear, public, documented goals and procedure of information use

SBUF

Rolebook [TOOL]

The purpose of this tool is for a data space to define certain important roles and to record their associated rights and responsibilities.

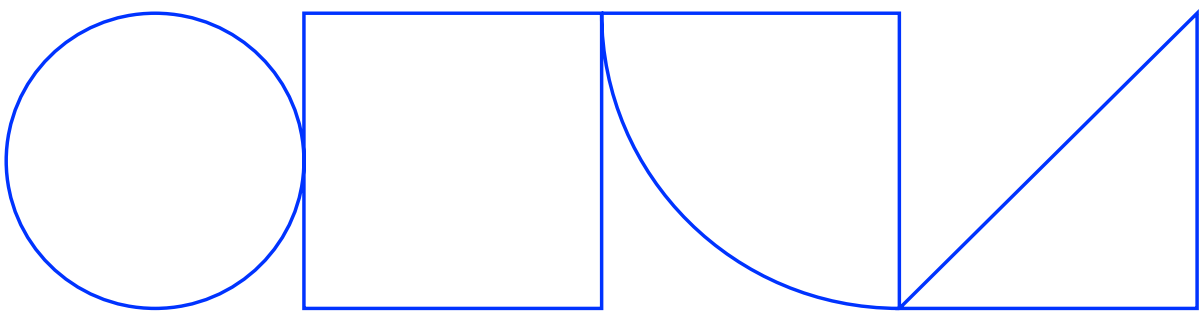
Data space roles are split into two clusters. Cluster A (Table 2) describes roles relative to the governance of an entire data space: founding members, members, and optionally additional membership categories. Note that additionally there are external stakeholders like individuals, whose personal data are processed in the dataspace and whose rights are utmost important to respect, but they are not members of the dataspace.

Founding Member is an initial data space participant that executes the Constitutive Agreement. The founding members define the original ground rules of the data space and draft the rulebook.

Additional membership categories are included for those data spaces, where there are e.g. large numbers of less-resourced participants who do not have the interest or capacity to partake in the full governance of a data space, but want to share, process, or use data in the data space, nonetheless. It is possible to define a special membership category for them to meet their need and capabilities in the data space.

Cluster B (Table 3), on the other hand, describes roles relative to a single use case within a data space: data transaction participants (data provider and data user), data rights holders, and service providers. Cluster B roles are non-exclusive. In other words, the same actor may perform multiple roles as they engage in multiple use cases in the data space, or even within a single use case.

Cluster A and Cluster B roles can be mapped against each other in a matrix that defines how the roles must, can, or cannot coincide in a specific data space (Table 4).



Cluster A roles: Data space governance perspective

Table 2: Cluster A – Roles relative to the governance of a data space

Type	Full decision-making rights	Responsibility to commit to the rulebook	Right to be represented in the governance	[Right A / Responsibility B]
Founding members	Yes, as defined in the rulebook	Define the rules, draft the contracts, sign the constitutive agreement	Yes, as defined in the rulebook	
Members	Yes, as defined in the rulebook	Yes, as founding members have defined, sign an accession agreement	Yes, as defined in the rulebook	
Additional membership categories	As defined in the rulebook	Yes, possibly more limited commitments as founding members have defined, sign a (different) accession agreement	Not necessarily, but e.g. through proxy as defined in the rulebook	

This tool is:

- **Pre-structured** with the three most common data space governance roles and the three rights and responsibilities that distinguish these roles from each other.
- **Extensible** so that data spaces can add additional and sub-types of roles and additional rights and responsibilities, such as access to or provision of core infrastructure or services, onboarding criteria, etc.
- **Partially pre-populated** leaving lot of flexibility for the founding members to adapt the model for their purposes in the rulebook.

Note that any modifications and refinements in the model should be propagated into the corresponding agreements, especially to the constitutive agreement, accession agreements (possibly different for additional membership categories) and the governance model.

Cluster B roles: Data space use case perspective

Table 3: Cluster B roles related to specific use case within a data space

Type	Sub-type	Right to provide data	Right to use data	Right to impose conditions on the use of data	[Right A / Responsibility B]
Transaction participant	**Data provider**	Yes			
	Data user		Yes		
Data rights holders	**Data rights holder**			Yes	
Service provider	**Value adding services on top of data or datasets**		Yes, for the purposes of service providing		
Operator	**Technical, legal, procedural or organisational services that enable data transactions to be performed**	Only in relation to the service, e.g. log data or authorisation data	No	Only in relation to the service, e.g. log data or authorisation data	

This tool is:

- **Pre-structured** with the most common use case roles and role types and the most relevant rights associated with a use case.
- **Extensible** so that data spaces can add sub-types of roles (e.g., specific service provider roles) and additional rights and responsibilities, such as the requirement to have a DGA DISP label to be allowed to provide certain data intermediation services in the data space.
- **Partially pre-populated** and the rest are left for the data space to define for themselves.

Cluster A and Cluster B mapping matrix

Table 4: Cluster A and Cluster B mapping matrix

		Founding member	Member	Additional membership categories
Data transaction participant	Data provider			
	Data user			
Data rights holders	Data rights holder			
Service provider				
Operator				

This tool is used for defining which Cluster A roles must always, can sometimes, or cannot ever coincide with which Cluster B roles. As an example, a data space may define core federation service providers who must always be founding members of the data space and can never be only members or in other membership categories. Or it may define that data users must always belong to a certain membership category of the data space, but data providers are not required to be so – anyone can share their data in the data space.

Servicebook [TOOL]

The purpose of this tool is to support the business design of the data space regarding services required and offered. It suggests a classification of different technical services that follows the DSSC Blueprint v1.5[2], but others may be adopted. Using this tool will help define key aspects of service governance in a data space, namely: which services are considered "core" or mandatory for the data space to function, who can provide each type of services, what additional policies apply to the provision of specific services (such as whether the costs of the service are covered by the Governance authority or by individual participants), and possibly other aspects of governing different types of services.

[2] https://dssc.eu/space/bv15e/766067344/Services+for+Implementing+Technical+Building+Blocks

Table 5. Data space service book

Type	Service	"Core" service designation	Approved provider (s)	Applicable policies	[Condition A]
Federation services	Data space registry services				
	Validation and verification services				
	Policy information point services				
	Catalogue services				
	Vocabulary services				
	Observability services				
Participant agent services	Participant agent services				
Value creation services	(Any can be defined)				

General Terms and Conditions

Applicability, Scope, and Governance

The Data Space is established by the Constitutive Agreement, which is signed by the Founding Members of the Data Space.

The provisions of these General Terms and Conditions will become applicable to and legally binding on the data sharing agreements of the Parties to the Data Space upon the execution of the Constitutive Agreement and any further Accession Agreements, as applicable.

If a discrepancy arises between any of the terms and conditions established in the Constitutive Agreement, any Accession Agreements and these General Terms and Conditions, including any of their appendices or schedules, any such discrepancy will be resolved in accordance with the following order of priority:

1. the clauses of the Constitutive Agreement

2. the clauses of any Accession Agreement(s)
3. Dataset Terms of Use and related Schedules
4. these General Terms and Conditions
5. other Appendices to the Constitutive Agreement in numerical order.

Any amendments to or derogations from these General Terms and Conditions must be agreed upon in the Constitutive Agreement in order to be valid.

Definitions

In these General Terms and Conditions, the following capitalised terms and expressions have the following meanings, and the singular (where appropriate) includes the plural and vice versa:

Accession Agreement means the agreement that governs the admission of parties to the Constitutive Agreement and the Data Space after the execution of the Constitutive Agreement.

Affiliate means any individual, company, corporation, partnership or other entity that, directly or indirectly, controls, is controlled by, or is under shared control with Party.

Appendix means any appendix to the Constitutive Agreement.

Confidential Information refers to trade secrets as defined in the EU Directive 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, point (1) of Article 2 provided it is: (a) if disclosed in writing or in other tangible form, clearly marked as confidential or proprietary by the disclosing Party at the time of disclosure, or (b) if disclosed in other than tangible form, identified as confidential at the time of disclosure and confirmed and designated in writing to the receiving Party within fourteen (14) calendar days from the disclosure as confidential information by the disclosing Party.

Constitutive Agreement means the agreement under which the Data Space is established and any of its appendices.

Data means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording, that Data Providers have distributed, transmitted, shared or otherwise made available to the Data Space based on the Constitutive Agreement and during its period of validity as further defined in the respective Dataset Terms of Use.

Data Controller has the same meaning as defined in Article 4(7) of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). It refers to anyone which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor has the same meaning as defined in Article 4(8) of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). It refers to anyone that processes personal data on behalf of the Data Controller.

Data Space means the group consisting of the Parties who share Data in accordance with the Constitutive Agreement.

Data Processing Agreement means a written contract concluded between a controller and a processor that processes Personal Data on behalf of the controller, which sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of data subjects, and the obligations and rights of the controller.

Data Provider means any natural person or an organisation that provides Data for the Parties to use via the Data Space.

Data Rights Holder means an entity (a human being or a legal entity) that alone or jointly with others has rights and/or obligations to grant access to or share certain personal or non-personal data.

Dataset means a collection of Data whose use the Data Provider authorises via the Data Space. Datasets and their related terms and conditions are defined more in more detail in the respective Dataset Terms of Use.

Dataset Terms of Use means the terms under which the Data Provider grants a right to use the Data included in the Dataset to the Service Providers and/or Data Users.

Data User means any of the Parties to which Service Providers provide Data and/or services or to which the Data Provider provides Data, and which do not redistribute the Data further.

Derived Material means information derived from Data or information that is created as a result of the combination, refining and/or processing of Data with other data. In case there is a need to clarify the borderline between Data and Derived material, additional requirements for what is not considered Derived Material shall be identified in the respective Dataset Terms of Use,

Founding Members are the initial Parties that execute the Constitutive Agreement.

Governance Model means an appendix to the Constitutive Agreement that includes a network-specific description of the rules and procedures of accession (i.e., who may be admitted to the Data Space and how), applicable decision-making mechanisms, and further governance provisions regarding the administration of the Data Space.

Intellectual Property Rights means patents, trademarks, trade and business names, design rights, utility models, copyrights (including copyrights in computer software), and database rights, in each case registered or unregistered and including any similar rights to any of these rights in any jurisdiction and any pending applications or rights to apply for the registration of any of these rights.

List of Members means a list of Parties which is included as an appendix to the Constitutive Agreement, and which is updated upon the accession of new Parties and the termination of incumbent Parties.

Operator means any Party that provides data system or any other infrastructure services for the Data Space that are related e.g., to identity or consent management, logging or service management.

Operator Service Agreement means any service level agreements governing the services provided by any of the Operators to the Data Space or to its Members.

Party or **Member** means a Data Space Participant, i.e. a party to the Constitutive Agreement and/or to an Accession Agreement.

Permission means any legal right to the processing of Data.

Permissioning means managing all kinds of legally relevant Permissions to use Data.

Personal Data has the meaning set forth in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation, **GDPR**).

Schedule means any schedule to the Dataset Terms of Use.

Service Provider means any of the Parties that combines, refines and processes data and provides the processed Data and/or a service, which is based on the Data, to the use of Data Users, other Service Providers or Third-Party Data Users.

Third Party means a party other than a Party.

Third Party Data User means any Third Party that receives any Data directly or indirectly from any of the Service Providers.

Role-specific responsibilities

The potential roles defined under these General Terms and Conditions for the Parties to the Constitutive Agreement are (1) the Data Provider, (2) the Service Provider, (3)

the Data User and (4) the Operator. A Party may simultaneously occupy multiple roles. In such case, the relevant Party must comply with all applicable obligations related to each role and relevant Data. In addition, Third Party Data User is a role recognised under these General Terms and Conditions as applying to any stakeholders who are not a Party to the Constitutive Agreement but who receive Data.

A more specific determination of role-specific responsibilities may be included in the Constitutive Agreement.

Data Owner

Data Owner (Ledningsägare)

The Data Provider will be responsible for defining the Dataset Terms of Use for any Data that the Data Provider makes available within the Data Space. (ledningsägaren) This includes the right to define the purposes for which relevant Data can be processed, the right to allow the redistribution of Data to Data Users and, where applicable, to Third Party Data Users, and the right to prohibit the unauthorised use of Data and the right to cease sharing Data within the Data Space. (ledningsägare)

Data Provider (Eningo)

The Data Provider must ensure that an adequate Permissioning mechanism is in place to make sure that the Data Rights Holders (Eningo) have control over their data to the extent applicable laws require, and the Data Users are able to get the Permissions they need. (eningo) The Data Provider must notify the Parties to whom the Data Provider makes the Dataset available of any new Dataset Terms of Use, after which the Dataset Terms of Use will bind the other Parties. (eningo) Unless otherwise defined in the applicable Dataset Terms of Use, any changes introduced by the Data Provider to the applicable Dataset Terms of Use will become effective within thirty (30) days from the relevant Parties to the Data Space being sent a notification of such change. Changes to the Dataset Terms of Use must not have retroactive effect.

The Data Owner shall provide Data for the use of the Data Space in a machine-readable form and by a method as defined by the Data Provider in the applicable Dataset Terms of Use (e.g., application programming interface, downloadable package or other method).

Service Provider

The Service Provider may involve one or several Operators , and will be responsible for processing Data in accordance with the Constitutive Agreement and the applicable Dataset Terms of Use.

The Service Provider must keep records of its processing activities and deliver on request, reasonably detailed reports on usage, processing and redistribution of Data to the relevant Data Provider(s).

Data User

The Data User must use Data in accordance with the Constitutive Agreement and the applicable Dataset Terms of Use.

Operator

The Data Space may involve one Operator. The Operator(s) is responsible for providing the Data Space with services that facilitate the operations of the relevant Data Space, such as authentication, identification, and identity/consent management services or for ensuring data security or providing technical data protection solutions for the Data Space and as further defined in the applicable Operator Service Agreement.

Any Operator Service Agreement(s) concluded with the Party/Parties and the Operator(s) may be included as an Appendix to the Constitutive Agreement.

The Service Provider may involve one or several Operators , and will be responsible for processing Data in accordance with the Constitutive Agreement and the applicable Dataset Terms of Use.

The Service Provider must keep records of its processing activities and deliver on request, reasonably detailed reports on usage, processing and redistribution of Data to the relevant Data Provider(s).

Operator shall adhere to any regulatory requirements such as notifications required by applicable legislation.

Should an operator or any other participant meet the definition of a data intermediary service provider under the Data Governance Act (DGA), the requirements set out in Chapter III of the DGA apply.

Redistribution of Data

The Parties shall have the right to redistribute the Data to the other Parties, unless such redistribution has been specifically prohibited under applicable Dataset Terms of Use. Parties can redistribute Data to Third Party Data Users only if permitted under the applicable Dataset Terms of Use or applicable laws.

If the Data Provider chooses to allow redistribution of the Data to Third Party Data Users, the Data Provider shall be responsible for determining those Dataset Terms of Use which apply to the redistribution. A Service Provider must include such terms and conditions concerning Data redistribution into any agreements or terms and conditions with Third Party Data Users.

Notwithstanding the above, the Parties shall have the right to redistribute Data to their Affiliates, unless applicable Dataset Terms of use explicitly prohibit such redistribution. Each Party shall be responsible for ensure that their Affiliates comply with the Constitutive Agreement.

Derived Material and its Redistribution

Rights to Derived Material shall belong to the Party generating such Derived Material and the restrictions of use set out for the Data in the Dataset Terms of Use shall not cover Derived Material. Any restrictions for the use or redistribution of Derived Material shall be explicitly set out in the Dataset Terms of Use, if any.

The Parties are entitled to redistribute Derived Materials to the other Parties and any Third Party, unless specifically prohibited in the applicable Dataset Terms of Use.

Processing and Redistribution of Personal Data

The redistribution of any Personal Data or Derived Materials created on the basis of any Personal Data may be subject to more detailed requirements and restrictions. Each Data Controller shall on its own behalf ensure that any redistribution and other use of Derived Material shall take place in accordance with applicable data protection legislation. Additionally, any conduct between Data Controllers and Data Processors shall be subject to the applicable Data Processing Agreements. The Parties may also choose to separately agree on more detailed stipulations about the processing of Personal Data as part of the Dataset Terms of Use.

General responsibilities

Data security, protection and management

Each Party must designate a contact person for data security matters, who is responsible for the relevant Party's data systems that are connected to the Data Space and for the implementation of the Party's security policy.

Each Party to the Data Space must have, sufficient capabilities to process Data securely and in accordance with the relevant data security standards and data protection legislation. The Parties must implement and maintain suitable technical, organisational and physical measures that are in line with good market practice, by taking into account the nature of the Data processed by the Party. Each Party must have the capability to properly perform its obligations under the Constitutive Agreement and applicable Dataset Terms of Use and, where necessary, to cease processing activities without undue delay for any relevant reason.

The aforementioned capabilities include e.g. the capability to control Data and its processing by being aware of

- the origins of the Data (specifically whether the origin is the Party itself, another Party or Third Party);
- the basis for processing Data;

- the restrictions and limitations that apply to processing Data; and
- the rights and restrictions that apply to redistributing or refining Data.

Parties must also be capable of recognising Data and removing or returning it if the basis for the processing of Data expires. The obligation to remove or return Data is not applicable to Derived Materials.

Any identified data security breaches must be duly documented, rectified and reported to the affected Parties without undue delay. All involved Parties have a mutual responsibility to contribute reasonably to the investigation of any data security breaches within the Data Space.

Subcontractors

The Parties will have the right to employ subcontractors to perform their obligations under the Constitutive Agreement. Where and to the extent that the outsourced functions require it, the Parties may allow their subcontractors to access Data. The Parties will be responsible for the subcontracted performance as for their own.

Fees and costs

Data is shared within the Data Space free of charge, unless otherwise defined in the applicable Dataset Terms of Use.

Notwithstanding the above, data will always be provided free of charge if required by the Data Act or other applicable law.

Each Party will bear their own costs related to accessing the Data Space and operating as a Member of the Data Space.

Unless otherwise agreed by Parties, the joint costs incurred for the maintenance and administration of the Data Space will be allocated in equal shares between the Parties. For the avoidance of doubt, the maintenance and administration of the Data Space does not include the costs of Data where applicable and as defined in the Dataset Terms of Use in question.

Confidentiality

The Parties must use any Confidential Information they receive in connection with the operation of the Data Space and/or regarding the Data Space only for the purposes for which such Confidential Information has been provided. The Parties must not unlawfully use or disclose to Third Parties any such Confidential Information they have become aware of in the course of the operation of the Data Space.

At the expiration or termination of the Constitutive Agreement, the Parties must cease to use Confidential Information and, upon request by any Party, verifiably return or destroy any copies thereof. Notwithstanding the above, the Parties are entitled to continue to use the Data subject to clause 10.2. In addition, the Parties may retain copies of Confidential Information as required by the applicable law or competent authorities.

If a Party is, under the applicable law or an order issued by a competent authority, obliged to disclose another Party's Confidential Information to the authorities or Third Parties, the obliged Party must promptly notify the affected Party whose Confidential Information will be disclosed of such disclosure if so permitted under the applicable law or the competent authority’s order.

The confidentiality obligations established in these General Terms and Conditions will survive the termination of the Constitutive Agreement.

Intellectual property rights

The Intellectual Property Rights of the Parties must be respected and protected in connection with the operation of the Data Space.

Signing the Constitutive Agreement and sharing any Data within the Data Space does not result in the transfer of any Intellectual Property Rights. More specific provisions, if any, concerning the Intellectual Property Rights that relate to specific Datasets are included in the applicable Dataset Terms of Use. For the avoidance of doubt, any new Intellectual Property Rights created by a Party will vest in the creating Party as further defined in the applicable legislation governing Intellectual Property Rights.

Data Provider is responsible for ensuring that it has sufficient rights for the provision of Data in accordance with the Dataset Terms of Use.

The Parties are entitled to utilise software robots or other forms and applications of robotic process automation or machine learning or artificial intelligence when processing Data. In accordance with the aforementioned and the applicable Dataset Terms of Use, the

Parties have the right to learn from Data and to use any professional skills and experience acquired when processing Data.

Data protection

Any Personal Data processed within the Data Space must be processed in accordance with the applicable data protection laws and regulations.

Terms that are not defined here, have the meaning stated in the GDPR or other applicable data protection laws.

For the purposes of processing Personal Data within the Data Space, any Parties disclosing or receiving Data are, individually and separately, assumed to be controllers under the provisions of the GDPR. The said Parties are also assumed to be processing Data on their own behalf unless the Parties have concluded a written Data Processing Agreement that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of data subjects and the obligations and rights of the controller and the processer. Where any such Data Processing Agreement is applicable in general to certain Dataset(s) or services provided under the Constitutive Agreement, it must be included as an Appendix to the Constitutive Agreement.

The Parties must prevent the unauthorised and unlawful processing of Personal Data by employing appropriate technical and organisational measures. The Parties must ensure that persons allowed to process Personal Data have committed to keeping such data confidential or are bound by an appropriate statutory obligation of confidentiality.

Personal Data that is shared within the Data Space can be transferred within the European Union and the European Economic Area (EEA). This kind of Personal Data can also be transferred outside the EU and the EEA in compliance with the applicable data protection legislation and case law, unless otherwise prescribed by the applicable Dataset Terms of Use.

The Parties commit to provide reasonable assistance to the other Parties where such assistance is need in order for the other Party to comply with its obligations under the applicable data protection legislation.

Termination and validity

If the Constitutive Agreement is concluded for a fixed period, it will expire without separate notice at the end of the applicable fixed period. If the Constitutive Agreement is concluded for an indefinite period, it will expire upon termination by the Parties.

The Parties are entitled to continue to use any Data received through the Data Space prior to the termination of the Constitutive Agreement, unless otherwise determined in the applicable Dataset Terms of Use or agreed by the Parties in the Constitutive Agreement. In such case, the clauses governing use of Data in these General Terms and Conditions, Dataset Terms of Use and/or in the Constitutive Agreement, remain in force according to the Clause 17.1.

Any Party may choose to terminate the Constitutive Agreement as defined in the Constitutive Agreement. Notice of termination must be provided in writing to the the Data Provider (Eningo). In the event that there are more than two Parties to the Constitutive Agreement, the Constitutive Agreement will remain in force for the remaining Parties following the termination thereof by one Party.

Where the Parties have agreed on a process for amending the Constitutive Agreement otherwise than by the written consent of all Parties, any Party that objects to such an amendment in writing after having become aware of it will be entitled to terminate the Constitutive Agreement by notifying the other Parties thereof. The termination will become effective after the objecting Party has submitted the aforementioned notice to the other Parties, after which the amendment will enter into force unless the agreeing Parties have agreed on a later date.

In the event that there are only two Parties to the Constitutive Agreement and one Party commits a material breach of the provisions of the Constitutive Agreement, the other Party will have the unilateral right to terminate the Constitutive Agreement with immediate effect by providing the other Party with a written notice.

In the event that there are more than two Parties to the Constitutive Agreement and one Party commits a material breach of the provisions of the Constitutive Agreement, the Data Provider (eningo) will have the right to terminate the Constitutive Agreement with the breaching Party with immediate effect. Notice of any such termination must be provided in writing to all Parties.

If the breach can be rectified, the non-breaching Party/Parties may resolve to suspend the performance of their obligations under the Constitutive Agreement until the breaching Party has rectified the breach.

Where a Member’s membership in the Data Space is terminated as a consequence of the Member’s material breach of the Constitutive Agreement, the breaching Member’s right to use the Data will end at the date of the termination. The breaching Member must cease to use the Data and, upon request by any Party, verifiably return or destroy Data and any copies of Confidential Information including copies thereof. However, the breaching Member is entitled to retain the Data as required by the applicable law or competent authorities provided that the breaching Member notifies the Data Provider of such a data retention obligation by the date of termination.

Liability

The Parties will only be liable for direct damages that result from a breach of the provisions of the Constitutive Agreement as defined hereinafter and where applicable, in the Constitutive Agreement. Any other liabilities are hereby excluded, unless otherwise specifically defined in the Constitutive Agreement. Parties are not liable for loss of profits or damage that is due to a decrease or interruption in production or turnover, or other indirect or consequential damages.[2]

The Parties will not be liable for any losses, damages, costs, claims or expenses howsoever arising from a mechanical or electrical breakdown or a power failure or any other cause beyond the reasonable control of the Party; and the Parties must fully compensate any damages resulting from an intentional or grossly negligent breach of the provisions set out in the Constitutive Agreement.

Each Party, severally and not jointly, will be liable for any infringements of personal data obligations set out in the GDPR in accordance with Article 82 of the GDPR.

Force Majeure

No Party will be liable for injuries or damage that arise from events or circumstances that could not be reasonably expected beforehand and are beyond its control (*force majeure*).

A Party that is unable to perform its obligations due to an event of force majeure must inform other Parties of any such impediment without undue delay. These grounds for non-performance will expire at the moment that the force majeure event passes. This clause is subject to a long-stop date: where performance is prevented for a continuous period of one hundred and eighty (180) days or more, the Parties are entitled to terminate the Constitutive Agreement as set forth in clause 10.5 or 10.6, as applicable.

Audit

A Data Provider will be entitled to audit the Parties processing the Data made available by the Data Provider at its own expense, including also material and reasonable direct costs of the audited Party. The purpose and the scope of the audit is limited to verifying compliance with the material requirements of the Constitutive Agreement, the applicable Dataset Terms of Use, and applicable legislation.

The Parties are responsible for imposing the same auditing obligations as set out herein on their Affiliates and the Parties will act in good faith to ensure that the objectives of the Data Provider's audit rights materialise with regard to the subcontractors of a Party.

The auditing Party must notify the audited Party of the audit in writing at least thirty (30) days prior to the audit. The written notice must disclose the scope and duration of the audit and include a list of requested materials and access rights.

The audited Party is entitled to require that the audit is conducted by a mutually acceptable and/or certified independent Third Party.

The Parties are required to retain and provide to the auditing Party and/or the Third Party auditor, for the purposes of the audit, all records and documents as well as access to all necessary data systems and premises and to interview personnel that are of significant importance for the audit. Records and documents thus retained must span to the previous audit or to the accession of the audited Party to the Data Space, whichever is later.

The auditing Party and/or Third Party auditor may only request such records and documents and such access to data systems and premises and to interview personnel that are of significant importance to the audit.

All records, documents and information collected and disclosed in the course of the audit constitute Confidential Information. The auditing Party and/or Third Party auditor may not unlawfully utilise or disclose Confidential Information that it has become aware of in the course of the audit. The auditing Party represents and warrants that any Third Party auditor, where applicable, complies with the applicable confidentiality obligations. The audited Party is entitled to require that the auditing Party and/or Third Party auditor or any other persons participating in the audit sign a personal non-disclosure agreement provided that the terms and conditions of such a non-disclosure agreement are reasonable.

The results, findings and recommendations of the audit must be presented in an audit report. The audited Party is entitled to review any Third Party auditor's audit report in advance (and prior to it being provided to the relevant Data Provider(s) by the Third Party auditor). The audited Party is entitled to require the Third Party auditor to make any such changes to the audit report that are considered reasonable while taking into account the audited Party's Confidential Information and the applicable Data Provider's business interests in the Data. The audited Party must provide its response to the audit report within thirty (30) days. If no response is provided, the audited Party is considered to have accepted the contents of the report.

If the auditing Party justifiably believes the audited Party to be in material breach of the obligations imposed thereupon in the Constitutive Agreement, an additional audit may be conducted.

In the event that the audit reveals a material breach of the obligations imposed in the Constitutive Agreement or the applicable Dataset Terms of Use, the audited Party will be liable for reasonable and verifiable direct expenses incurred as a result of the audit.

Applicable laws and dispute resolution

The agreement incorporating these General Terms and Conditions is governed by and construed in accordance with the laws defined in the Constitutive Agreement.

Any dispute, controversy or claim arising out of or in relation to the agreements based on the General Terms and Conditions, or the breach, termination or validity thereof, shall be finally settled by the dispute resolution mechanism defined in the Constitutive Agreement.

Other provisions

Unless otherwise agreed by the Parties, any amendments to the Constitutive Agreement and its Appendices must be made in writing and signed by all Parties.

No Party may assign the Constitutive Agreement, either wholly or in part, without a written consent of the other Party/Parties. Notwithstanding the previous, no consent shall be required where the assignee is a company that belongs to the same group of companies as the Party pursuant to the provisions of the Swedish Accounting Act.

If any provision of the Constitutive Agreement or any applicable Dataset Terms of Use is found to be invalid by a court of law or other competent authority, the invalidity of that provision will not affect the validity of the other provisions established in the Constitutive Agreement.

Each party represents and warrants that it is validly existing and in good standing under the applicable laws of the state of its incorporation or registration. Each Party also represents and warrants that it has all required power and authority to execute, deliver, and perform its obligations under the Constitutive Agreement and, where applicable, to bind its Affiliates.

The Parties intend to create a Data Space that is subject to a single set of contractual terms, and nothing contained in the Constitutive Agreement may be construed to imply that they are partners or parties to a joint venture or the other Parties' principals, agents or employees. No Party will have any right, power, or authority, express or implied, to bind any other Party.

No delay or omission by any Party hereto to exercise any right or power hereunder will impair such right or power, nor may it be construed to be a waiver thereof. A waiver by any of

the Parties of any of the covenants to be performed by the other Parties or any breach thereof may not be construed to be a waiver of any succeeding breach thereof or of any other covenant.

Notices

All notices relating to these General Terms and Conditions and the Constitutive Agreement must be sent in a written or electronic form (including post or email) or delivered in person to the contact person and/or address specified by the respective Party in the Constitutive Agreement or in the applicable Accession Agreement. Each Party will be responsible for ensuring that their contact details are up-to-date. Notices will be deemed to have been received three (3) days after being sent or on proof of delivery.

Survival

Clauses 1, 2, 3, 4, 5, 8, 9, 11, 14, 16 and 17 of these General Terms and Conditions will survive the termination of the Constitutive Agreement in its entirety together with any clauses of the Constitutive Agreement that logically ought to survive the termination.

Clause 13 of these General Terms and Conditions will survive for a period of three (3) years following the termination of the Constitutive Agreement in its entirety.

Clause 7 of these General Terms and Conditions will survive for a period of five (5) years following the termination of the Constitutive Agreement in its entirety.

Constitutive Agreement [Template]

PARTIES

1. BM System AB
2. Borås kommun
3. Eningo AB
4. Falkenberg Energi Elnät AB
5. Kungsbacka kommun
6. Laholmsbuktens VA AB
7. Mölndals kommun
8. Nordion Energi AB
9. Nätkraft Borås Infra AB
10. Statkraft Värme AB
11. Svevia AB (publ)
12. Terranor AB (publ)
13. Trimble AB
14. Vattenfall AB

(Together the "**Parties**" or "**Founding Members**".)

APPENDICES

Appendix	**Description**
1	Description of the Data Space[3]
2	General Terms and Conditions

[3] Note: Please append, where appropriate, any Business or Technical documentation prepared as a result of completing the Checklist for the Rulebook as an **Appendix 1**.

3	List of Members and Contact Details[4]
4	User agreement

BACKGROUND AND PURPOSE

The Parties are contemplating the establishment of a Data Space in order to securely transfer data of utility infrastructure, primarily geospatial data of underground utility pipes and cables. The overarching purpose is to protect underground utility infrastructure from damages due to excavation, drilling and other types of ground works.

The transfer of data is two-directional, one for each of the two use cases: In the case of *digital utility location*, the utility providers send digital maps of underground infrastructure to entrepreneurs' machines and instruments so that the entrepreneurs can avoid striking any underground infrastructures. In this case, the utility providers act as Data Owners and entrepreneurs act as Data User. The data is displayed in machine control systems, maintenance management systems, building information modelling (BIM) systems, digital measurement instruments and other digital systems used by entrepreneurs. In the other case, *seamless measurements*, the entrepreneurs act as Data Owners and utility providers act as Data Users. Seamless measurements is a collective name for several fast and simple methods of mapping underground infrastructure with high precision measurements. These maps can later be used for e.g. digital utility locations. In both cases, Eningo acts as both Data Provider and Service Provider while machine control and other user system providers acts as Service Providers.

For information, the Data Space does not include or interact with the government service Ledningskollen.se. Ledningskollen is a platform for connecting entrepreneurs (questioners) planning to conduct ground works with utility owners who might have underground infrastructure in the area. Ledningskollen only provides information about the questioner and the work to be done, such as geographical area, and whether any utility owner has underground infrastructure in the area or not. Ledningskollen does not handle or provide any utility data such as maps of utilities. That information is shared between the affected parties after entrepreneur and utility owners have been connected via Ledningskollen. It is only the latter process that this Data Space is facilitating. Thus, Ledningskollen is not and cannot be an actor in this Data Space. However, Ledningskollen provides APIs so that utility mapping requests from entrepreneurs can be automatically processed by third-party solutions. This is a prerequisite to digital utility mapping, since manual request administration otherwise would be a significant threshold in the complete process. The Swedish Post and Telecom Authority

[4] Note: This Appendix should include a list of Members and necessary contact details.

who are operating Ledningskollen is positive to third-party applications and enhancements of the utility mapping service, which is why they provide these APIs.

DEFINITIONS

As used in this Agreement, including the preamble and the Appendices hereof, unless expressly otherwise stated or evident in the context, the following terms and expressions have the following meanings, the singular (where appropriate) includes the plural and vice versa, and references to Appendices and Sections mean the Appendices and Sections of this Agreement:

”Chair”	has the meaning set forth in Appendix 4.
”Qualified Majority”	has the meaning set forth in Appendix 4.
”Representatives”	has the meaning set forth in Appendix 4.
“Secretary”	has the meaning set forth in Appendix 4.
""[5]	means

Other terms and expressions have the meanings defined in **Appendix 2** (General Terms and Conditions).

THE DATA SPACE

The undersigned hereby establish a Data Space that is further described in **Appendix 1** (Description of the Data Space).

The Data Space is subject to the following provisions:[6]

[5] Note: Please list herein, where applicable, any definitions introduced in the Constitutive Agreement or its Appendices (other than General Terms and Conditions).

[6] Note: A lack of exclusivity has been adopted as the baseline, but this should not prevent the Founding Members from requiring exclusivity where it is deemed necessary. The Founding Members should carefully assess the need for exclusivity, as it may e.g. result in the need to carry out further competition law analysis.

NO EXCLUSIVITY[7]

Nothing in this Agreement prevents or restricts the Parties from participating in any other Data Spaces, platforms, ecosystems or any other cooperation or from using any services provided by Third Parties. Furthermore, sharing any of the Data within the Data Space does not prevent or restrict the respective Data Provider from sharing such Data with Third Parties at its own discretion.

GOVERNANCE OF THE DATA SPACE

The Data Space is a commercial service provided by Eningo AB, which has full ownership over it.

DEROGATIONS TO THE GENERAL TERMS AND CONDITIONS

The Parties have agreed to replace the following clauses of the General Terms and Conditions as follows:[8]

TERMINATION AND VALIDITY[9]

This Agreement is concluded and remains in force for an indefinite period and is subject to a termination period of [●] months.

NOTICES

Any notices provided under this Agreement must be submitted in writing to the Representatives listed in the Appendix 3.[10]

Any change in contact persons or relevant contact details must be disclosed immediately by the respective Party to [the secretary of the Steering Committee, as defined in Appendix 4].[11]

[7] Note: The wording of the template for the Governance Model is relatively general as the governance requirements for different types of Data Spaces may vary significantly. As a result, the Members should consider amending the Governance Model template to meet the requirements of the respective Data Space and its life cycle.

[8] Note: Please fill in the necessary details for the term and termination.

[9] Note: The Members may want to name a different contact person for formal notices and operational notices in Appendix 3.

[10] Note: Appendix 4 – Governance Model describes the duties of the secretary of the Steering Committee.

[11] Note: Please consider of liability caps should be defined separately and differently for various roles.

LIMITATION OF LIABILITY

The annual total liability of any Party[12] under this Agreement must not exceed the greater of 200 000 euro.

Notwithstanding any limitations of liability, General Data Protection Regulation (GDPR), Article 82 is applied to damages related to personal data. The above-mentioned limitation of liability does not limit the controller's right to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage in accordance with the GDPR Art. 82.

OTHER TERMS[13]

ENTRY INTO FORCE AND APPLICATION

This Agreement will enter into force when [executed (signed) by all Parties OR on _____ 20___].

APPLICABLE LAWS AND DISPUTE RESOLUTION

This Agreement is governed by and construed in accordance with the laws of _____ without regard to its principles of private international law and/or conflict of laws rules.

Any dispute, controversy or claim arising out of or in relation to the Data shared under this Agreement, or the breach, termination or validity thereof, shall be finally settled by arbitration in accordance with the Arbitration Rules of _____. The number of arbitrators shall be one, the seat of arbitration shall be _____ and the language of the arbitration shall be English.

COUNTERPARTS

This agreement has been executed in [ ] identical counterparts, one for each Party [and one for the Steering Committee].

In [city, country], on [date]

[Signatures on the next page]

[12] Note: Please consider whether it is worth setting different total liability limits for different roles.

[13] Note: Please consider any other terms that could be relevant to the Data Space, such as non-solicitation, marketing and promotional activities.

Name:	Name:
Title:	Title:
Name:	Name:
Title:	Title:

Accession Agreement [Template]

ACCEDING PARTY

[Acceding Party][14]

APPENDICES

Appendix	Description
1	Constitutive Agreement
1.1	Description of the Data Space
1.2	General Terms and Conditions
1.3	List of Members and Contact Details

[14] Note: Please insert the Acceding Party's details herein.

1.4	Code of Conduct
1.5	[Any other Appendices to the Constitutive Agreement][15]

BACKGROUND

The Acceding Party has expressed its interest to accede to the Constitutive Agreement[16] regarding [●] that was signed on [●].[17]

The Constitutive Agreement allows new [Parties][18] to accede the Data Space [provided that [●].[19]

DEFINITIONS

As used in this Agreement, including the preamble and the Appendices hereof, unless expressly otherwise stated or evident in the context, the following terms and expressions have the following meanings, the singular (where appropriate) includes the plural and vice versa, and references to Appendices and Sections mean the Appendices and Sections of this Agreement:

“Acceding Party	means the entity defined under section Acceding Party.
"Accession Agreement"	means this Agreement.
"Constitutive Agreement"	means the Constitutive Agreement regarding Data Space on [●], dated [●].

[15] Note: Please include the full list of Appendices herein.

[16] Note: If there are additional membership categories defined in the Constitutive Agreement, it should be specified here to which category the Acceding Party is joining. It may be a good idea to prepare a separate template for an Accession Agreement for each membership category to include the specific rights and duties of the members in that category.

[17] Note: Please insert a reference to the Data Space herein.

[18] Note: The Founding Members may consider it relevant to define role-specific preconditions for accession, and it may be necessary to detail herein the role(s) as which the Acceding Party joins the Data Space.

[19] Note: Please include, where applicable, a reference to the conditions for new Members of the Data Space herein.

ACCESSION TO THE CONSTITUTIVE AGREEMENT

The Acceding Party has expressed its interest in acceding to the Constitutive Agreement, and the Constitutive Agreement allows new Parties to accede to the Data Space [, subject to [●]].[20]

As the Acceding Party fulfils such requirements, the Acceding Party accedes to the Constitutive Agreement and to the Data Space under this Accession Agreement.

ENTRY INTO FORCE AND APPLICATION

This Accession Agreement will enter into force as of its execution by the Acceding Party and after it has been duly approved by the Data Space's Steering Committee.

APPLICABLE LAWS AND DISPUTE RESOLUTION

The agreement incorporating these General Terms and Conditions is governed by and construed in accordance with the laws defined in the Constitutive Agreement.

Any dispute, controversy or claim arising out of or in relation to the agreements based on the General Terms and Conditions, or the breach, termination or validity thereof, shall be finally settled by the dispute resolution mechanism defined in the Constitutive Agreement.

COUNTERPARTS

This agreement has been executed in [●][21] identical counterparts, one for [each Party/Acceding Party and one for the Steering Committee].

In _____, on _____

[Signatures on the next page]

[20] Note: Please include, where applicable and as defined in the Constitutive Agreement, the conditions for new Members of the Data Space herein.

[21] Note: Please note that this information is subject to the accession process and its governance (e.g. whether the Steering Committee has the authority to approve new Members or whether the Accession Agreement should be signed by each incumbent Member).

Name:	Name:
Title:	Title:
Name:	Name:
Title:	Title:

Dataset Terms of Use [Template]

Data Provider

_____ acts as the Data Provider.

Schedules

Schedule	Description
1	Dataset Description [no. 1][22]
2	

Background

The purpose of this Dataset Terms of Use is to define, the Data that the Data Provider makes available through the Data Space and to set out the terms and conditions for the use of such Data.

[22] Note: Where the Data Provider provides several Datasets under the Dataset Terms of Use, the Data Provider may prefer to include individual Dataset Descriptions as separate Schedules herein. It should be noted that, where the terms and conditions for different Datasets are different, the Data Provider must define separate Dataset Terms of Use for any such Datasets.

Definitions

As used in this Dataset Terms of Use, including the Schedules hereof, unless expressly otherwise stated or evident in the context, the following terms and expressions have the following meanings, the singular (where appropriate) includes the plural and vice versa, and references to Schedules and Sections mean the Schedules and Sections of this Dataset Terms of Use:

”Data Provider”	means the entity defined under section “Data Provider” above.
”User”	means any Data User, Service Provider, Operator or Third Party Data User who processes any Data that is made available by the Data Provider under these Dataset Terms of Use.
””[23]	

Other terms and expressions have the meanings defined in the General Terms and Conditions.

Applicability and Scope

These Dataset Terms of Use apply to the Dataset(s) provided by the Data Provider under the Constitutive Agreement [dated [●] [●] 202[●] / as acceded by the Data Provider under the Accession Agreement dated [●] [●] 202[●]][24] and as further defined in **Schedule 1**.

By using any such Data, the User undertakes to use the Data in compliance with these Dataset Terms of Use.

In the event that a discrepancy arises between the Constitutive Agreement or any of its appendices and these Dataset Terms of Use, these Dataset Terms of Use and its Schedules will prevail. Furthermore, in the event that a discrepancy arises between these Dataset Terms of Use and any of its Schedules, these Dataset Terms of Use will prevail.

Data

The Data as well as its location and method of distribution are defined in the Dataset Description(s) (**Schedule 1[- ●]**[25]).

[23] Note: Please list herein, where applicable, any definitions introduced in these Dataset Terms of Use.

[24] Note: Please edit based on the date on which the Data Provider has become a party to the Constitutive Agreement.

[25] Note: Where applicable, please add references to additional Schedules.

The Data Provider shall ensure that it possess all the necessary rights and authorisations to make the Data available for the use of the other Parties in accordance with the applicable terms and conditions.

Purpose(s) of use of the Data

Subject to these Data Set Terms of Use, the Data Provider hereby grants the User a non-exclusive right to use the Data for the following purposes:[26]

The User is entitled to process and redistribute the data to End Users within the data space in accordance with this Terms of Use and the Constitutive Agreement.

The End User is entitled to use the data to avoid damages on infrastructure.

The User is entitled to create and distribute new data from corrective measurements of infrastructure to the [ledningsägare].

The User is entitled to utilise software robots or other forms and applications of robotic process automation or machine learning or artificial intelligence when processing Data. In accordance with the aforementioned, the User has the right to learn from the Data and to use any professional skills and experience acquired when processing the Data.

Restrictions on the processing and Redistribution of Data

The Data may not be processed for [●].[27]

[26] Note: The following provides an example of the matters to be included in this clause with regard to the right to use the Data. The Data Provider and/or the Members of the Data Space may want to consider preparing a more specific Data Space specific template(s) for the Dataset Terms of Use to reflect the business context of the Data Space.
Please note that, in accordance with the General Terms and Conditions (clause 4), Data can be redistributed to Third Party End Users if permitted under the applicable Dataset Terms of Use. As such, please specify the redistribution right here as required. The Members or the Data Provider may also want to prepare a separate Schedule, including any terms and conditions that must be included in any redistribution agreements. Please complete the list of purposes for using the Data.

[27] Note: Please describe herein any specific restrictions that apply to the Dataset(s).

Permissioning

The Data Provider ensures that an adequate permissioning mechanism is in place to make sure that the Right Holders have control over their data to the extent applicable laws require, and the Data Users are able to get the permissions they need.[28]

Cease of provision of the Data

The Data Provider may cease the provision of the Data by notifying the other Parties of the Data Space at least [thirty (30) days] prior to the end of provision of. the concerned Data.

Derived Material

The following shall not be considered as Derived Material and the rules relating to the use of Data continue to apply in case:

[(i) the Data can be readily converted, reverted or implied from the Derived Material to recreate the Data;

(ii) the Derived Material can be used as a substitute for the Data;

individual Data Providers of the Data can be identified from the Derived Material;

the Derived Material contains any Data Provider's Confidential Information; or

(v) ...]

[For the avoidance of doubt, in case a Dataset is modified only in minor ways and used for substituting the original Dataset, it shall not be regarded as Derived Material and remains under the restrictions set out above for the Data.]

[Derived Material shall be shared and used under Creative Commons Attribution 4.0 International (https://creativecommons.org/licenses/by/4.0/) license terms.]

[Restrictions on the use and redistribution of Derived Material]

Derived Material may not be used for [●]]

[28] Note: If needed, a more extensive description of the permissioning mechanism and the distribution of respective liabilities e.g. between the Data Provider and an Operator can be included here.

Fees and payment terms

The use of Data is subject to fees and charges, as further defined in **Schedule 1**.[29]

Reporting

The use of Data is subject to the following specific reporting obligations: [●].[30]

Audit

The use of Data is subject to the following specific audit obligations: [●].[31]

Data Security

The use of Data is subject to the following specific data security obligation: [●].[32]

Confidential information

The Parties acknowledge that the Dataset, as defined in **Schedule [1]**, includes Confidential Information and that its use and processing is subject to: [●].[33]

Data protection

The Data includes personal data, and its reception and processing is subject to the following: [●].[34]

[29] Note: Where applicable, any fees or charges related to the Data should be defined and referred to herein as the default option under clause 6.1 of the General Terms and Conditions is that the Data is provided free of charge.

[30] Note: Please describe herein, where applicable, any specific reporting obligations that apply to the use of the Dataset(s).

[31] Note: Please describe herein, where applicable, any specific conditions for audits (see clause 13 of the General Terms and Conditions and the Constitutive Agreement).

[32] Note: Please describe herein, where applicable, any specific data security requirements for the Dataset(s) (see clause 5 of the General Terms and Conditions and the Constitutive Agreement).

[33] Note: Where the Dataset(s) include Confidential Information, the Data Provider should detail herein any specific requirements it deems necessary in order to make the Data available within the Data Space.

[34] Note: Clause 9 of the General Terms and Conditions defines the default terms and conditions that apply to data protection. In the event that the Data includes personal data (as data typically does, since the definition of personal data in the GDPR is very broad), the Data Provider must consider defining herein the terms and conditions for the transfer and processing of personal data in further detail. In addition, further consideration is required where the Data includes personal data (or anonymised personal data), which would be redistributed to Third Party End Users.

Intellectual Property Rights

[The Dataset is shared and shall be used in accordance with Creative Commons Attribution 4.0 International (https://creativecommons.org/licenses/by/4.0/) license terms.][35]

Disclaimer and Limitation of Liability

[**Example**: Unless otherwise expressed in these Terms, the Data Provider offers the data "as is" and "as available" with no warranty of any kind. The risk inherent in the suitability of the data for the User's purposes remains solely with the User. Notwithstanding the above, this does not limit the Data Provider's liability under clauses 3.3 and 11.3 of the General Terms and Conditions, Permissioning clause above in this Dataset Terms of Use [and clause(s) of the Constitutive Agreement]].[36]

Effects of Termination

[●][37]

Entry into force and application

This right to use the Data will enter into force when the User accesses the Data and apply until the User stops processing the Data.

Refraining from sharing Data and amendments

The Data Provider may refrain from sharing Data within the Data Space and change these terms and conditions (including but nor limited to the content or quality of the Dataset) at any time by notifying all other Members to the Data Space of such change in writing. The provision of Data will end or the modified terms will enter into force within ninety (90) days after the Data Provider has notified the other Members of the refraining of sharing or

[35] Note: Where the Data Provider considers it necessary to derogate from the default approach for Intellectual Property Rights (clause 8 of the General Terms and Conditions), Dataset specific derogations should be described herein. However, to manage the Intellectual Property Rights effectively, the Members should consider whether it would be feasible to define the default approach to Intellectual Property Rights for the Data Space by establishing a standard template for Dataset Terms of Use that apply to the specific Data Space.

[36] Note: Clause 11 of the General Terms and Conditions sets out provisions that apply to the limitation of liability. Any Dataset specific derogations regarding liability should be defined herein. Please note, where applicable, that the Members may have derogated from the liability clauses of the General Terms and Conditions, in which case such liability clauses should be referred to herein for clarity.

[37] Note: Clause 10.2 of the General Terms and Conditions stipulate that the Parties are entitled to continue to use any Data received through the Data Space prior to the termination of the Constitutive Agreement, unless otherwise determined in the applicable Dataset Terms of Use or agreed by the Parties in the Constitutive Agreement. Please add here more specific rules if needed.

amendments made to these terms and conditions, but the amendments will not apply to any Data received by the Users prior to the entry into force of the amendments.

Other terms

[●][38]

For the avoidance of doubt, it is acknowledged that above terms and conditions shall in no way restrict the rights of the users that are based on applicable mandatory law. In case of any discrepancy between such mandatory law and these terms and conditions, the mandatory law shall prevail.

Applicable laws and dispute resolution[39]

The agreement incorporating these General Terms and Conditions is governed by and construed in accordance with the laws defined in the Constitutive Agreement.

Any dispute, controversy or claim arising out of or in relation to the agreements based on the General Terms and Conditions, or the breach, termination or validity thereof, shall be finally settled by the dispute resolution mechanism defined in the Constitutive Agreement.

[38] Note: The Data Provider (and the Members of the Data Space) should consider, on a case-by-case basis, whether any other terms regarding the use of Data are considered necessary.

[39] Note: Please note that this clause is potentially relevant only where the Data can be redistributed to Third Party End Users as one of the conditions, which should be included in the agreement governing the redistribution of the Data to Third Party End Users. Please consider if it is enough here to refer to the Constitutive Agreement or should the applicable law and dispute resolution be defined more precisely.

Digital Ledningsanvisning

Första fälttestet i Kungsbacka

Grävmaskinisten Leo

Det första fälttestet för Digital Ledningsanvisning genomfördes i Kungsbacka, arrangerat av projektdeltagarna från **Kungsbacka kommun**, tillsammans med **E.ON** och **Eningo**. Där fick vi möjlighet att träffa Leo från anläggningsföretaget Martin Grävare, en erfaren grävmaskinist med lång bakgrund inom bygg- och anläggningsbranschen. Innan vårt besök kände han inte till vårt innovationsprojekt kring digital ledningsanvisning, utan visste bara att vi skulle observera hur maskinstyrningssystem används vid grävarbeten.

Leo använder alltid maskinstyrningsfiler när han gräver, oavsett om en fysisk utsättning har gjorts eller inte. Maskinstyrningsfilerna skickas direkt till maskinstyrningssystemet, som är kopplat till grävmaskinens unika identifieringsnummer. Detta gör att Leo snabbt kan konfigurera skopan och mäta in ledningsanvisningen genom att använda maskinstyrningssystemets inmätningsfunktion för att sätta ut koordinatpunkter. När allt är inställt och kontrollerat, är han redo att börja gräva.

Han skrattade när vi berättar att vi initialt hade tänkt föra över maskinstyrningsfilerna via ett USB-minne under första fälttestet. **”Det är en gammal metod som man slutade med för 10 år sen, men det kanske fortfarande finns några enstaka fall kvar”** säger han.

Lättanvänd teknik

När vi frågar hur lätt eller svårt det är att använda maskinstyrning och maskinstyrningsfiler, svarar Leo utan tvekan: **”Det är hur smidigt som helst. Det går**

nästan inte att göra fel.”
Han visade ledningsanvisningen på skärmen och hur han mätte in ledningarna med hjälp av styrningssystemet och skopans placering.

Fysiska markeringar vs. digitala kartor

Vi frågade Leo om han föredrar att ledningsägaren gör en fysisk utsättning, jämfört med att enbart arbeta utifrån ledningsanvisningen i maskinstyrningssystemet. **”Det spelar egentligen ingen roll”** säger han, men tillägger att han tycker det är onödigt eftersom han mäter ändå in ledningarna med maskinstyrningssystemet. **”Dessutom håller inte färgen. Vips så snöar det eller dammar så är spraymarkeringarna borta.”** berättar han.

Behovet av tydliga osäkerhetszoner

Leo ser mycket positivt på idén att kunna se osäkerhetszoner direkt i maskinstyrningssystemet. Detta är något han länge har upplevt som en brist. **”Om en ledningsägare vet att en ledning inte är inmätt på 10 år och att dess faktiska läge kan avvika med 10 meter, är det information som är viktig för oss som gräver”** säger han. Att kunna se denna typ av osäkerhet i systemet skulle enligt honom vara mycket hjälpsamt.

Han påpekar också att man idag aldrig riktigt vet hur tillförlitlig informationen är, vilket leder till att man kan bli avtrubbad i sitt arbete. **”Det går inte att vara på helspänn hela tiden”** förklarar han.

Förhöjd risk och olyckor

Leo har också uttryckt ett behov av att kunna identifiera om han gräver i områden med förhöjd risk, som närheten till högspännings- eller gasledningar, något han i dagsläget inte kan se i sitt system. Lyckligtvis har inga allvarliga olyckor inträffat hittills. **”Vid avgrävningar av spänningssatta ledningar ska strömmen automatiskt brytas, men vid de tillfällen olyckor skett har kablarna ofta legat kvar i schaktet och fräst “** berättar han.

Tidsbesparingar och akuta situationer

"Man hade kunnat spara mycket tid om man hade kunnat få filerna direkt i systemet" säger Leo och undrar varför det ska vara så svårt egentligen.
Vid akuta ärenden, som när ett vattenrör läcker, förklarar han att grävning ofta måste påbörjas omedelbart, utan att det finns tid för en ledningsanvisning. **"Idag har man inget**

annat val än att riskera att gräva av ledningar som ligger nära en akut läcka" säger han. Leo tror att det skulle göra stor skillnad om ledningsanvisningar kunde göras direkt från grävmaskinen i sådana situationer, vilket skulle öka både säkerheten och effektiviteten i arbetet.

Risker med digitalisering och ny teknik

Leo berättar att det är ovanligt att han råkar gräva av en ledning, och han tror att det beror på hans tålamod. Han understryker att hans kollegor också är skickliga och att de känner till marken och ledningarna väl. **”Man lär sig med tiden att veta när det inte kommer att stämma med kartan, vilket det ofta inte gör.”** säger han. Han påpekar att det är en svår balans mellan att arbeta metodiskt och effektivt. Leo tillägger att det aldrig känns bra att gräva av en ledning och behöva meddela det. **”Det är ingen kul känsla”** säger han.

Vi frågade Leo om han ser några risker med digital ledningsanvisning, till exempel att man stirrar sig blind på skärmen eller förlitar sig för mycket på digital information och börjar ta större risker. **”Nej det tror jag inte”** svarar han.
”Första tiden med maskinstyrningssystem stirrar man på skärmen i stället för på marken, men det går över snabbt. Det var samma sak när färddatorer i bilar kom, men sen vande sig förarna,” förklarar han.

Han är dock skeptisk till AR-teknik i maskinstyrningssystemen. **”Det finns ingen nytta med det och man ska inte krångla till det”.**

Spärra skopan

Leo tror att det kan uppstå problem om skopans automatiska spärrfunktion används för flitigt. **”Ibland går det inte att gräva för hand, till exempel om marken är för hård eller om det finns stora stenar. Då får man gräva försiktigt eller använda en jordsug.”** säger han. Han använder dock gärna spärrfunktionen vid luftledningar eftersom det är lätt att glömma bort att fokusera uppåt när man arbetar med marken. Det är något han använder sig av ibland.

Sömlös inmätning

Vi frågade hur Leo ser på att använda maskinstyrningssystemet för att mäta in ledningarnas exakta position när schaktet är öppet och skicka datan till ledningsägaren

via en feedbackloop. **”Det gör jag redan idag så det är inga konstigheter”** säger han. Leo mäter in ledningarnas placeringar både innan han börjar gräva och när han grävt sig ner till ledningarna. Den enda skillnaden är att han inte skickar informationen till ledningsägaren. Det viktiga, menar han, är att processen för att skicka informationen är smidig och enkel för att det ska fungera i praktiken. **“Blir det för krångligt gör folk det inte”.**

Kungsbacka Kommun: Sara Andersson och Sara Karlsson. E.ON: Johan Persson, Mats Kivi, Gabriella Rystrand och Alexander Lage. Eningo: Gösta Malmqvist, Eveline Nordlund och Jacqueline Wettergren.

Text och bild: Eningo
Kungsbacka 12 November 2024

Samanfattning av digital workshop med Eningo

Utförd den 16/5-25

Upplägg och deltagare

Workshoppens syfte var att **visualisera** ett flöde av olika uppgifter och moment samt fundera kring eventuella problem som kan uppstå under det flödet. På slutet fanns det även tid att idégenerera kort om eventuella lösningar på de problem eller osäkerheter som identifierats.

Genom att samarbeta i uppdelade grupper där deltagarna har olika erfarenheter kunde vi med ett bredare perspektiv skapa större förståelse för de delar vi kanske inte vanligtvis arbetar med.

Workshoppen bestod av tre stycken övningar samt en ice-breaker för deltagarna att lära känna varandra lite mer inom grupperna.

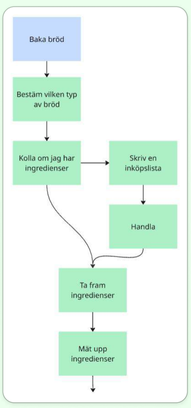
Följande företag som var med och bidrog i workshoppen:

-Mölndal energi
-Kungsbacka kommun
-ConsistIT
-Vattenfall eldistribution
-E.ON
-Fiberstaden
-Gävle energi
-Nätkraft Borås
-LBVA
-RISE

Övning 1: Flödeskarta

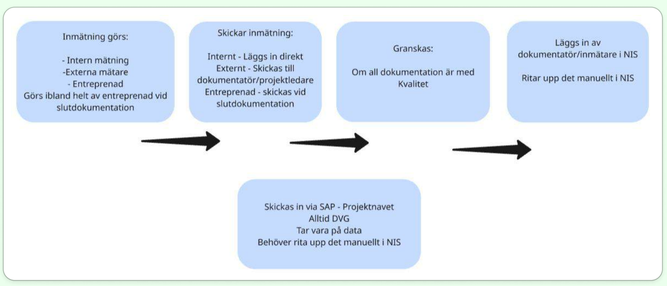
En flödeskarta (även kallad flödesschema eller på engelska flowchart) är en visuell representation av en process, ett arbetsflöde eller ett system. Den visar steg-för-steg-hur något fungerar eller utförs, med hjälp av olika symboler som kopplas ihop med pilar.

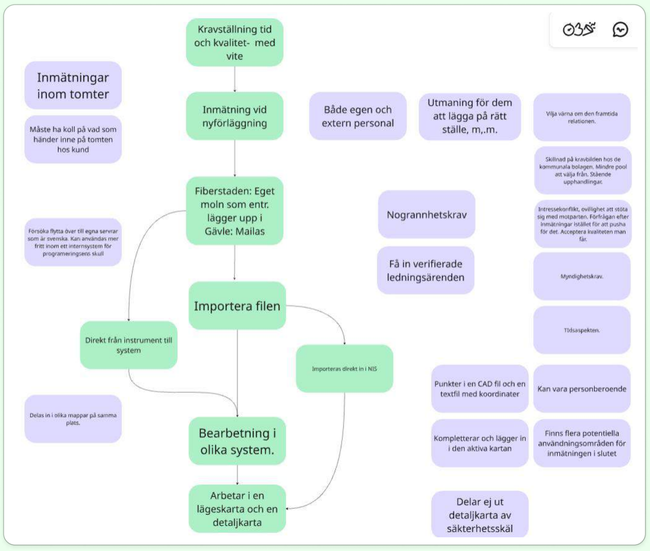
Exempel:



I övningen skulle deltagarna tillsammans skapa en flödeskarta över hela händelseförloppet från att mätteknikern mäter in till att inmätningsfilen är färdigarbetad i NIS/GIS. Deltagarna kom fram till en startpunkt att utgå ifrån och skapade en gemensam flödeskarta.

Resultat





Syftet med övningen var att skapa en grund att arbeta uifrån i nästa övning där de ska fundera på positiva och negativa aspekter med flödet.

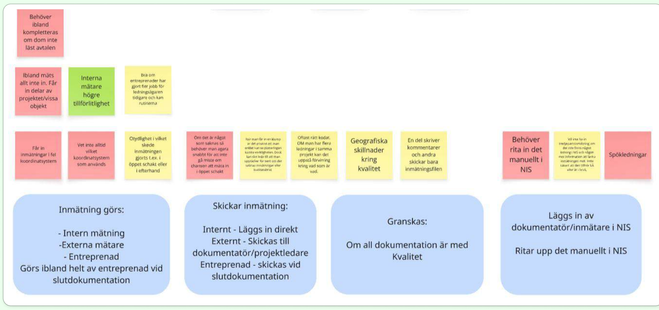
Övning 2: Samarbetsanalys

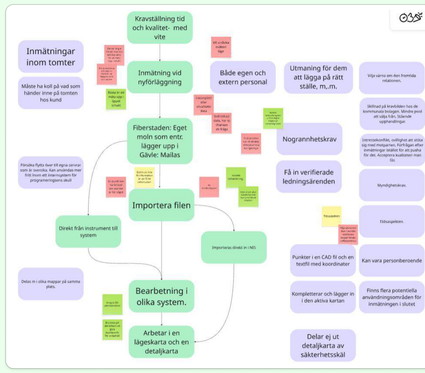
I denna samarbetsanalys skulle deltagarna titta på den flödeskarta de skapat och lyfta fram delar som är bra och identifiera delar som skulle kunna förbättras.

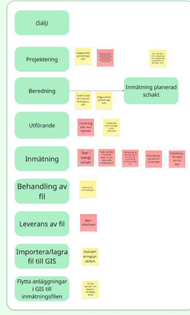
Deltagarna diskuterade och skrev på post-its som de placerade ut i flödeskartan. Smärtpunkter var röda post-its, saker som är otydliga eller osäkra var gula och fungerande delar var gröna.

Syftet med övningen var att ifrågasätta flödet. Skulle man kunna optimera det, göra det snabbare eller smidigare? Deltagarna hade olika uppfattningar om individuella delar av flödet eftersom de har olika lösningar i sina roller och på sina arbetsplatser.

Resultat







Sammanfattning av problemen kring inmätning och GIS från samarbetsanalysen

1. Bristande kravställning och uppföljning
   - Otydliga instruktioner vid upphandling och inmätning leder till felaktiga eller inkompletta leveranser.
   - Externa inmätningar följer inte alltid krav, och uppföljning saknas – varken viten eller incitament används effektivt.
   - Projektledare och GIS-ansvariga prioriterar olika saker, vilket skapar glapp i kvalitetskontrollen.

2. Försenade och felaktiga leveranser
   - Inmätning sker ofta i stängt schakt, vilket minskar datakvaliteten.
   - Leveranser av relationshandlingar kommer ofta för sent – ibland flera månader efter projektavslut.
   - Sen inmätning innebär risk att data är inaktuell (t.ex. p.g.a. snö eller återfyllt schakt).

3. Tekniska hinder och konverteringsproblem
   - Filer kommer i olika referenssystem och versioner, vilket skapar problem vid import.
   - Filer levereras som punktmoln utan linjer eller med felaktig/oklar symbolik.
   - Ineffektiva och manuella processer – mycket handpåläggning och låg grad av automatisering.

4. Kompetens- och kommunikationsluckor
   - Skillnader i teknisk kompetens skapar personberoende kvalitet – vissa vet exakt hur det ska göras, andra inte.
   - Inmätare får sällan återkoppling när något är fel – ingen lärande slinga etableras.
   - Brist på gemensamma rutiner och processer – mycket görs på olika sätt beroende på individ och organisation.

5. Oenhetlig dokumentation och kodning
   - Olika aktörer och kommuner använder egna kodsystem, vilket försvårar tolkning och integration.
   - Filnamngivning och lagring sker utan gemensamma konventioner – leder till förvirring och tappad information.
   - Kartor och dokumentation blir svårtolkade på grund av överflöd av symboler och texter utan enhetlig ritstandard.

Övning 3: Lösningsverkstad

I den sista övningen skulle deltagarna välja ut 1-2 post-its som är gula eller röda och komma fram till förbättringar som skulle kunna lösa de problem eller osäkerheter som de identifierat.

För att förstå grundorsaken som orsakat att problemet uppstått kunde de ta hjälp av metoden “fem varför”. “Fem varför” fungerar som en kontinuerlig ifrågastättninga av problemet genom att fortsätta fråga “varför” upp till fem gånger.

Genom öppen diskussion kunde deltagarna resonera kring och skriva ner lösningsförslagen.

Resultat

Sammanfattning av lösningsförslag från lösningsverkstad

1. Förbättrad inmätning och arbetsflöde
   - Mäta in i öppet schakt och löpande under arbetets gång
     – Följ ledningsförläggningen i realtid för att öka noggrannheten.
     – Undvik att vänta till efter att schaktet fyllts igen.
   - Dela upp projekt i snuttar/etapper
     – Möjliggör delinmätningar för att sprida arbetsbördan och förenkla hantering.
   - Stråkinmätning istället för enstaka punkter
     – Säkerställer logiska sammanhängande ledningar.

2. Tydligare kravställning och dokumentation
   - Skapa och följ en tydlig checklista
     – Exempel: koordinatsystem, mätmetod, filformat, struktur.
   - Gör det enklare eller mer bindande att följa krav
     – Tydliga avtal och konsekvenser vid avvikelser.
   - Tydlig överenskommelse i uppstart
     – Alla aktörer ska veta vad som gäller – från teknik till leveransformat.

3. Struktur och kvalitet i datahantering
   - Kontrollera metadata och dokumentation före import
     – Kvalitetssäkring av inmätningsfiler och korrekt attributdata.
   - Säkerställ att samma inmätning inte skickas in flera gånger
     – Undvik dubbletter och kaos i GIS-systemet.
   - Slutdokumentation ska vara klar före slutbesiktning
     – Förbättrar möjligheten att verifiera genomförandet.

4. Återkoppling och kommunikation
   - Direkt digital återkoppling från fältet
     – Möjliggör snabbare kommunikation mellan fält och GIS/systemansvariga.
   - Korrekt namngivna och kodade filer
     – Förutsättning för en smidig inläsning och förståelse av datan.
   - Återanvänd inplanerad information i nybyggen
     – Effektivisera genom att nyttja befintlig planeringsdata istället för att duplicera arbete.

Bilaga 5, Nyhetsbrev #1 (AP1-5)

Gösta Malmqvist

From: Gösta Malmqvist <gosta.malmqvist@eningo.se>
Sent: den 5 maj 2025 15:51
To: Gösta Malmqvist
Subject: Nyhetsbrev #1 Innovationsprojektet digital ledningsanvisning

Follow Up Flag: Follow up
Flag Status: Flagged

View in browser

Digital Ledningsanvisning

Vad har hänt sen sist i projektet?

Hej alla!

Här kommer en uppdatering om vad som hänt i innovationsprojekt.
Det rör på sig inom flera spår – här är det senaste!

Grojektdeltagare

SVEVIA · Falkenberg Energi · Nätkraft Borås · vti · Vattenfall · Kungsbacka · Servicekontoret · Borås Stad · terranor · Mölndals Stad · RI.SE · Eningo · Martin Gräfvare · Statkraft · Laholmsbuktens VA · Nordion Energi

Systemleverantörer

BM System · Trimble · SITECH

Referentgrupp

Lantmäteriet · Bjäre Kraft · Trafikverket · seko · e.on

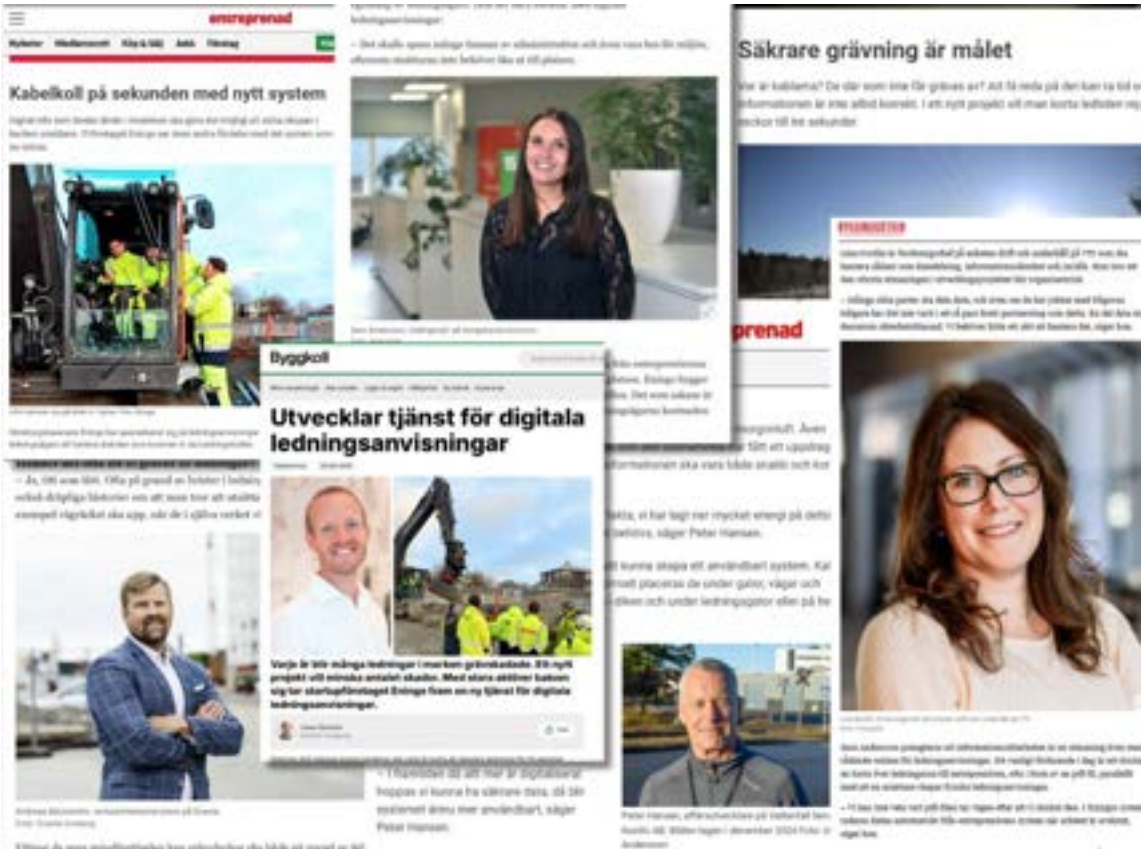
Finansiärer

SBUF Svenska Byggbranschens Utvecklingsfond · Avancerad Digitalisering · VINNOVA Sveriges innovationsmyndighet

Ett uppmärksammat projekt

Intresset för projektet har varit fantastiskt – redan fyra gånger har det uppmärksammats i tidningar, och det blir allt tydligare att behovet av en lösning är stort.

Vi är hela 24 aktörer som gått samman med en gemensam ambition: att skapa förbättringar och sätta en ny standard för hela branschen.
Det känns inspirerande att så många delar vår övertygelse: det är dags att modernisera och effektivisera den här viktiga delen av samhällsbyggandet.



Intressanta reflektioner från projektdeltagare

I artiklarna intervjuas bland annat Andreas Bäckström - verksamhetsutvecklare på Svevia, Lina Nordin, forskningschef på VTI, Peter Hansen - affärsutvecklare på Vattenfall Services och Sara Andersson - utvecklare på Kungsbacka kommun.

Tack för intressant läsning och att ni delade med er av era reflektioner!

Länkar till artiklarna

- Kabelkoll på sekunden med nytt system
- Eningo tar fram tjänst med digital ledningsanvisning
- Digitala ledningsanvisningar ska minska grävolyckor - Byggindustrin
- Säkrare grävning är målet

Vi välkomnar en ny projektpartner

Vi lärde känna Martin Grävare under vårt första fälttest i Kungsbacka, där grävmaskinisten Leo delade med sig av sina erfarenheter.

**Sedan dess har vi haft fortsatt kontakt och påbörjat ett pilottest.
De ser att Digital Ledningsanvisning kommer göra stor skillnad – och för oss har det varit ovärderligt att få arbeta nära dem.**

Martin Nielsen, VD för Martin Grävare.

Samtliga utrustade med maskinstyrning

Martin Grävare, med bas i Tvååker, har lång erfarenhet och djup insikt i branschen. Företaget grundades 2011 och har idag 26 anställda samt 20 grävmaskiner – alla utrustade med maskinstyrningssystem.

Bild från när vi besökte kontoret i Tvååker.

Test och utvärdering i en verklighetsnära miljö

Tillsammans med Martin Grävare kommer vi nu att testa Digital ledningsanvisning och sömlös inmätning – med fokus på funktionalitet och användarvänlighet.
Genom att utvärdera prototyper i en verklighetsnära miljö säkerställer vi att slutprodukten möter branschens behov och förväntningar.

Alla parter har nu signerat anslutningsavtalet, och vi inväntar Vinnovas godkännande av Martin Grävares inträde i projektet.

Vi ser verkligen fram emot att fortsätta utvecklingen tillsammans!

Ny referent

Vi har även glädjen att välkomna en ny referent in i projektet – det finska bolaget Groundhawk. De är specialiserade på smidig och användarvänlig dokumentation och inmätning i öppet schakt.
Tanken är att Groundhawk även ska testa att ta emot digitala ledningsanvisningar som ett alternativ för aktörer som saknar maskinstyrningssystem.

Förutsättningar för systemförändring
Risk- & Ansvarsutredning

Projektdagarna i Göteborg

Under två dagar samlades experter från hela ekosystemet – från ledningsägare och entreprenörer till jurister, forskare och tekniкspecialister – med ett gemensamt mål: att driva arbetet framåt mot en ny digital branschstandard.

Givande panelsamtal

Projektdagarna inleddes med ett panelsamtal där representanter från både ledningsägare och entreprenörsled delade insikter kring ansvar, utmaningar och möjliga lösningar.
Att få ta del av varandras perspektiv var mycket värdefullt och lade grunden för givande diskussioner under resten av dagarna.

Paneldeltagarna:

- Johan Sponton – Marknadsspecialist, Vattenfall Eldistribution
- Sara Andersson – Utvecklare, Kungsbacka kommun
- Charlotte Herner – Risk & Insurance Manager, Svevia
- Ann Assarsson – Agreement coordinator, E.ON
- Peter Hansen – Affärsutvecklare, Vattenfall Services

Arbetsgrupper om ansvar och risker

I arbetsgrupper diskuterade vi ansvar och risker och enades kring hanteringen av 28 av 32 identifierade risker samt fördelningen av 19 av 22 ansvarsområden. Underlaget bygger på förstudien och insikter från intervjuer och samtal med projektdeltagare. Efter projektdagarna har utredningen färdigställts.
Läs mer om det nedan.

Johan Sponton (Vattenfall Eldistribution), Kristian Sandström (Servicekontoret Borås), Sten Stenbeck (RISE), Emma Pakki (VTI) och Charlotte Herner (Svevia).

Punkter under projektdagarna

Gösta Malmqvist (Eningo) presenterade projektets framsteg och nästa steg.
VTI-teamet delade insikter om rättvis datadelning, digital mognad och ledde gruppdiskussioner.
Jacqueline Wettergren (Eningo) visade möjligheterna med sömlös och noggrann inmätning.
UX-studenterna Noah Törnell och Caroline Nordlund presenterade sin prototyp för enkel rapportering av avvikelser och grävskador.

Kvällen avslutades med en gemensam middag och möjlighet att lära känna varandra bättre.

Stort tack till alla som deltog under projektdagarna – till paneldeltagarna, samtalsmoderator Sten Stenbeck, och till VTI som såg till att vi fick nyttja deras fina lokaler.

Juridik

Lina Nordin och Emma Pakki från VTI under projektdagarna.

Regelboken för rättvis datadelning och den fördjupade juridikutredningen

Jeanette Andersson (forskande jurist), Emma Pakki (forskningsassistent) och Lina Nordin (forskningschef) på VTI har gått igenom frågorna från workshopen och sammanställt svaren som ligger till grund för regelboken för rättvis datadelning. Ett första utkast av regelboken håller på att tas fram.

Parallellt arbetar Jeanette och Emma med att färdigställa den fördjupade juridikutredningen. Arbetet utgår från ett legalt perspektiv och omfattar även relevanta delar av NIS2-direktivet.

Färdigställd utredning

Under projektdagarna arbetade vi vidare med de identifierade riskerna och ansvarsfrågorna från förstudien.
De kvarvarande punkterna har nu behandlats i en mötesserie, uppdelad i

två arbetsmöten, där vi tillsammans analyserat och utrett de sista risker och ansvarsfrågor.

Teresa Kalisky, projektledare på RISE.

Arbetsmötesserie

Mötesserien leddes av Teresa Kalisky från RISE, som med sin breda erfarenhet – bland annat som park-, gata- och VA-chef samt utredare i Vårgårda kommun – har bidragit med både struktur och fördjupning. Ett stort tack till Teresa och Sten Stenbeck (RISE) för att han introducerade oss.

Samanställning av ansvar och risker

Samtliga identifierade ansvar och risker har nu värderats och accepterats. De åtgärdsförslag som tagits fram för att eliminera eller mitigera vissa risker kommer att implementeras i lösningsdesignen. Samtliga risker kommer också att fortsätta bevakas under projektets gång, och vid behov omvärderas.

Den fastställda sammanställningen har skickats ut till alla projektdeltagare.

Avgränsade Arbetsområden
Fälttester

Sara Karlsson (Kungsbacka Kommun), Eveline Nordlund (Eningo), Sara Andersson (Kungsbacka Kommun), Mats Kivi (Kungsbacka Kommun), Alexander Lage (E.ON), Johan Persson (E.ON), Gabriela Rystrand (E.ON) och Gösta Malmqvist (Eningo)

Kungsbacka 6 december 2024

Första fälttestet

Tillsammans med Kungsbacka Kommun och E.ON besöke vi ett projekt i Kungsbacka. Under fälttestet träffade vi Leo från Martin Grävare, en erfaren grävmaskinist som delade med sig av sina insikter om maskinstyrning och tankar kring digital ledningsanvisning.

Viktig information för de som gräver

Han är positiv till initiativet och ser stor potential i att göra deras arbete säkrare och mer effektivt – särskilt vid akuta grävningar.
Han lyfter även behovet av tydlig information om osäkerhetsområden direkt i systemet.

Mats Kivi (Kungsbacka Kommun), Sara Andersson (Kungsbacka Kommun) , Gösta Malmqvist (Eningo) och Leo (Martin Grävare).

Arbete han gör ändå

Leo mäter alltid in ledningarnas placeringar i öppet schakt.
Anledningen är att han behöver det i sitt eget arbete.
Det är information som han gärna skulle skicka till ledningsägaren när han ser att det inte stämmer med ledningsanvisningen.
Det viktiga, menar han, är att processen för att skicka informationen är smidig och enkel för att det ska fungera i praktiken.

Johan Persson (E.ON), Leo (Martin Grävare) och Alexander Lage (E.ON)

Borås 17 Februari 2025

Andra fälttestet

Tillsammans med representanter från Nätkraft Borås, Terranor, Servicekontoret i Borås Stad, och VTI fick vi möjlighet att diskutera grävskador, maskinstyrning och de praktiska utmaningar som våra användare möter i vardagen.

Anders Magnusson (Terranor), Emma Pakki (VTI), Lina Nordin (VTI), Mattias Sandström (Servicekontoren Borås), Maria Zettergren (Nätkraft Borås), Gösta Malmqvist (Eningo), Kristian Sandström (Nätkraft Borås) och Eveline Nordlund (Eningo)

Borås - Ett gott exempel

Borås Nätkraft och Servicekontoret (Borås stads driftenhet) har etablerat ett välfungerande samarbete.
Vid entreprenadarbeten har de som rutin att ta tillvara på de inmätta ledningarna i öppet schakt – ett smart sätt att effektivisera arbetet och bidra till bättre dokumentation.

Gösta Malmqvist (Eningo), Mattias Sandström (Servicekontoren Borås), Eveline Nordlund (Eningo) och Lina Nordin (VTI)

Digital mognad med utrymme för förbättring

Det råder ingen tvekan om att markanläggningsbranschen besitter både hög digital mognad och djup branschkunskap. Samtidigt är behovet av standardiserade digitala processer fortsatt tydligt. Vi ser stora möjligheter att förbättra informationsflödet, minska fel och skapa smidigare arbetsflöden – och vi är taggade på att ta oss an den utmaningen tillsammans med er.

Särö 26 Mars 2025

Tredje fälttestet

Tredje fälttest genomfördes på Särö under ett av Norconsult borrarbeten tillsammans med E.ON, Terranor, Trimble och RISE och Kungsbacka Kommun.

Digitalt - Utan fysisk utsättning

Kungsbacka Kommuns ledningsanvisning skickades digitalt - utan fysisk utsättning. Norcunsult använde sedan den digitala ledningsnavisningen för att anpassa placeringen av borrprover.

Geotekniska markundersökningar

Norconsults borrningar handlar ofta om geotekniska markundersökningar, ibland över 100 meter ner, inför exempelvis nybyggnation eller nyförläggning av nät. Otroligt spännande att höra om de verkliga utmaningarna och riskerna som finns när man arbetar djupt under marken.

Inte bara grävskador

När vi pratar ledningsanvisningar handlar det ofta om grävning – men verkligheten är bredare än så.
Borrning är ett exempel där riskerna är lika stora, men där det inte finns något som motsvarar försiktig handschaktning. Borrning är exakt. Det kräver precision och att kartunderlagen är pålitliga.

Digital ledningsanvisning handlar om mer än att ersätta pinnar i marken – det handlar om att ge rätt information, vid rätt tidpunkt, oavsett metod eller projekt.

Gösta Malmqvist (Eningo), Teresa Kalisy (RISE) och Anders Magnusson (Terranor)

Sömlös inmätning
Pilottester

Tredjepartsinmätning i Falkenberg

JONAB har ett 6 månader långt projekt för VIVAB i Falkenberg där de anlitat Martin Grävare att utföra schaktarbetet.
Där kommer vi att arbeta med tredjepartsinmätning - vilket innebär att Martin Grävare kommer använda maskinstyrningssystemet för att passa på att mäta in befintliga ledningar för Falkenberg Energi.

Syftet är att få en bättre förståelse för processen, hur vi kan säkerställa att tredjepartsinmätning håller rätt kvalitet och samtidigt är så smidig att den kan bli en ny standard för branschen.

Jacqueline Wettergren (Eningo) och Anders Sjökvist (Falkenberg Energi)

Smidigare dokumentation vid nyförläggning

E.ON och Ölandskraft kommer att testa att mäta in nyförlagda ledningar på ett mer effektivt sätt i ett av deras projekt i Kalmar-regionen med Groundhawk som

är nytillkomna referenter i projektet. Syftet är att testa nya metoder som gör det smidigare för utföraren att mäta in nyförlagda ledningar innan man schaktar igen för att få en mer kvalitativ och effektiv dokumentation.

Utveckling
Prototyp & Användargränssnitt

User Experience
- Avgörande för digitalisering

För att digitalisering ska fungera i praktiken krävs användarupplevelser som är enkla, intuitiva och matchar verkliga behov. Lösningar som är smidiga och utan friktion ökar både viljan och möjligheten att använda nya digitala lösningar.

Caroline Nordlund från Yrgos UX-utbildning under ett av användartesterna.

Nyckeln till uppdaterade ledningskartor

UX-studenterna från Yrgo har fokuserat på att förstå och förbättra feedback-loopen som är ett avgörande steg för att hålla ledningskartor uppdaterade och pålitliga.
"Vi har arbetat med hela upplevelsen – från första intryck till daglig användning", säger Caroline Nordlund.

Noah Törnell & Caroline Nordlund från Yrgos UX-utbildning.

Prototypen

Genom intervjuer och användartester med grävmaskinister, arbetsledare och ledningsägare har de identifierat behov och skapat en användarvänlig prototyp.

Appen kommer göra det möjligt för arbetsledare att:

- Godkänna inmätningar från grävmaskinister
- Rapportera okända ledningar
- Anmäla skador direkt till ledningsägare

"Nu är vårt examensarbete avslutat. Stort tack till alla som bidragit – och till Eningo för förtroendet och möjligheten att göra skillnad!" Säger Noah Törnell.
Prototypen har nu överlämnats, och nästa fas tar vid för vidareutveckling.

Nästa steg
- Hur blir det sömlöst även för ledningsägarna?

Törnell fortsätter sin andra LIA-period hos oss med fokus på att den nya informationen kan tas emot och hanteras utan att skapa merarbete för ledningsägaren.

Inbjudan till digital workshop: Att utforska flödet från inmätning till GIS/NIS

Som en del i arbetet med att ta fram kravspecifikationen för sömlös inmätning bjuder vi in till en digital workshop den **15 maj.**
Noah Törnell och Eveline Nordlund håller i workshopen.

Syftet är att bättre förstå hur dokumentationsarbetet ser ut i dag – och hur det kan förenklas för att undvika flaskhalsar.

Vi ber er gärna skicka vidare inbjudan till kollegor som arbetar med inmätning, dokumentation eller GIS/NIS. Ju fler perspektiv vi får, desto bättre.
Ni är naturligtvis även själva varmt välkomna att delta!

🗓️ **När:** 15/5 kl.10.00–12.00
🌐 **Var:** Verktyg: Miro + videomöte (kräver ingen tidigare erfarenhet)
👉 **Anmälan:** https://forms.office.com/e/GQJEDHRCdj
📰 **LinkedIn-inbjudan**: https://www.linkedin.com/events/digitalworkshop-attutforskafl-d7325077533706653697/

IT-säkerhetsarbetet

Eningo tar just nu fram en grunddesign för vår säkerhetsarkitektur, som planeras vara klar i maj. När den är färdig bjuder vi in till en särskild IT-säkerhetsgrupp, där deltagare från projektet får möjlighet att granska och lämna feedback på upplägget.

Tillsammans med säkerhetsspecialister från Vattenfall, Laholmsbuktens VA och RISE

Arbetet kommer genomföras tillsammans med säkerhetsspecialister från Vattenfall, Laholmbuktens VA och RISE. Fokus ligger på att skapa en robust och flexibel lösning med tydliga roller, säker datahantering och framtidssäkrad integration.

Säkerheten byggs utifrån erkända internationella standarder som ISO 27001 och NIS2-direktivet, samt bästa praxis från OWASP. Plattformens arkitektur utformas för att skydda känslig information, säkra integrationer med externa system (som Trimble och BM System), och skapa spårbarhet i varje steg.

Bland annat omfattar säkerhetsramverket:

- Kryptering av all data i vila och under överföring
- Rollbaserad åtkomstkontroll för olika användartyper
- Isolerad infrastruktur med redundans och övervakning
- Loggning och incidenthantering enligt kommande krav i NIS2
- Stöd för federerad inloggning och begränsad tredjepartsåtkomst via säkrade API:er

Var med och bidra till säkerhetsarbetet

Vill du eller någon hos er bidra med input till vårt säkerhetsarbete? Kontakta oss gärna! Vi ser gärna en så bred uppslutning som möjligt – era perspektiv är viktiga för att vi ska kunna bygga en lösning som möter branschens faktiska behov.

Till sist: Några ord från projektledaren Gösta Malmqvist

"Jag är otroligt nöjd och stolt över det arbete som vi tillsammans åstadkommit hittills. Vi har en bra takt inom samtliga områden, har nått flera betydande milstolpar och vi följer planen som förväntat. Vi har byggt en solid grund och nu ser vi fram emot att bygga vidare och ta nästa steg i utvecklingen."

Tester med endast Digital Ledningsanvisning

"Nästa steg för oss är att växla upp IT-säkerhetsarbetet samt att ta nästa steg i testerna. Innan semestrarna har vi som målsättning att genomföra fler tester med endast digital ledningsanvisning. Vi har säkerställt att BM Systems plattform Road Service kan hantera digital ledningsanvisning och ska nu komma igång på allvar med testerna inom vägunderhåll."

Stort tack Peter

"Peter från Vattenfall Services gick i pension förra veckan, efter en karriär som verkligen gjort avtryck. Vi har haft förmånen att ha honom med i innovationsprojektet, där han spelat en nyckelroll i att driva utvecklingen framåt.
Med teknisk nyfikenhet, operativ erfarenhet och stor förståelse för både ledarskap och människor har Peter bidragit med ovärderlig kunskap. Vi är tacksamma för allt han gjort. Stort grattis till en välförtjänt pension!"

- Jag ser fram emot en intensiv senvår och är riktigt peppad på att fortsätta den här resan tillsammans med er alla. Stort tack för ert engagemang så här långt. Vi har en spännande tid framför oss!

Med vänliga hälsningar
Gösta Malmqvist