2023

KVICKGUIDE 2

Framtidens boende för äldre

Data i ett boende – Vad är data?

Data beskrivs ofta som morgondagens eller dagens ”guld” och är en central ingrediens både i vardagen och vid innovation för ett effektivt och hållbart boende. Data som samlas in i boendet används i tjänster och system både för vardag, uppföljning, utveckling och drift för att skapa förutsättningar för god livskvalitet till de boende och medarbetare.

Innehåll

Vad är data?

Data är information som representeras i en form som kan bearbetas, lagras och kommuniceras av datorsystem. Det kan vara fakta, statistik, text, bilder, ljud, videor eller andra former av information som samlas in och registreras för att användas i olika sammanhang.

Data kan vara strukturerad eller ostrukturerad. Strukturerade data är organiserad enligt en fördefinierad modell eller format, vilket underlättar analys och bearbetning. Exempel på strukturerade data inkluderar databaser med tabeller och fält. Ostrukturerade data saknar en fördefinierad struktur och kan vara svårare att bearbeta och analysera. Det kan inkludera textdokument, e-postmeddelanden, bilder, ljudinspelningar och sociala medieinlägg.

Data kan vara rå eller förädlad. Rådata är obearbetade och kan innehålla råmätningar, insamlade observationer eller okorrigerade inspelningar. Förädlade data har genomgått en bearbetnings- eller omvandlingsprocess för att rensa, filtrera, strukturera eller aggregera informationen. Förädlade data är oftast mer användbar och kan användas för analys, rapportering och beslutsfattande.

Data kan genereras från olika källor, inklusive mätningar, observationer, sensorer, formulär, transaktioner och användargenererade innehåll. Insamlade data kan lagras i databaser, filer eller andra datalagringssystem för att vara tillgängliga för senare användning och analys.

Data kan vara värdefullt för att extrahera insikter, upptäcka mönster och fatta informerade beslut. Genom att tillämpa dataanalysmetoder och tekniker kan man identifiera trender, göra prognoser och dra slutsatser från data. Data kan också användas för att utveckla modeller, algoritmer och maskininlärningssystem för att automatisera processer och fatta prediktiva beslut.

Datahantering inkluderar olika aktiviteter som insamling, lagring, bearbetning, skydd och analys av data för att säkerställa att den är korrekt, tillförlitlig, säker och användbar. Genom att hantera data på ett effektivt sätt kan organisationer dra nytta av den för att förbättra prestanda, fatta bättre beslut och driva innovation inom olika områden.

Etik och integritet vid insamlandet av data

Vid planering, införande och utveckling av digitala tjänster och Välfärdsteknik måste vi säkerställa att etiska aspekter och att den personliga integriteten beaktas i de tjänster som vi tar fram. Metoden och delaktigheten från användarna är en del som bygger förtroende för hur tjänster utvecklas. Att involvera användare och medarbetare i ett tidigt skede är ett sätt att bygga in vad som är viktigt för de boedne och medarbetarna så att deras attityder och ev rädslor och farhågor fångas. I exemplet från Haparandas arbete med det nya boendet Hemstranden arbetade projektgruppen genomgående med delaktighet av medarbetare från verksamheten och representanter från de boende genom intervjuer/samtal och workshops i hela projektprocessen.

Etik och integritet är viktigt att ta ställning till vid införande av Välfärdsteknik i vård och omsorg.

Socialstyrelsen har tagit fram utbildningar som stöd för kommuner och verksamheten för att arbeta med etik och integritetsfrågor när ny teknik ska införas, se här.

Genom alltmer tekniskt utvecklade lösningar som inkluderar AI och algoritmer behöver vi också ställa ytterligare krav på etik och integritet. Vilka krav finns vid delande av data när vi har AI och algoritmer med i driften, i verksamheten eller omsorg och vården? Just AI i vården/omsorgen diskuteras flitigt och som krav-ställare är det viktigt att ställa krav på förklarbarhet och transparens.

Sammanhanget påverkar integriteten

Individer har olika inställning till vad som upplevs privat och vi har olika behov av privatliv. Vid all datainsamling bör vi uppmärksamma att avgörande för den personliga integriteten är sammanhanget data används. Medvetenheten, anpassningsbarheten och kontrollen över vilken information om dig som är tillgänglig i vilket sammanhang påverkar den upplevda integriteten. Ett exempel är om personen i badkläder på stranden skulle bli satt på ett torg skulle det kännas obekvämt men samma klädsel känns bekvämt på stranden. Olika kontexter gör att du känner dig bekväm i en situation och inte den andra utan att du har ändrat något, i detta exempel dina kläder.

För att användning av personuppgifter ska kännas bekvämt och tryggt för individen måste företag/verksamheten på samma sätt kunna berätta vilket sammanhang en användare befinner sig i och hur deras information kommer att användas. Sammanhanget och förväntningarna måste vara tydliga och kunna bibehållas för att etablera förtroende mellan användare och de som använder informationen i detta fall tex ett tjänsteföretag eller omsorgsverksamheten.

GDPR och Samtycke vid delande av data

Samtycke innebär att en person accepterar eller godtar ett föreslaget villkor och är en central del i GDPR. GDPR är från 2018 en EU-gemensam lag som mycket förenklat ger individen rätt att får mer kontroll över personliga uppgifter. Det innebär att individen alltid måste godkänna och ge sitt samtycke till insamling och användandet av personliga uppgifter och godkännandet ska i förväg inhämtas av den som samlar in data.

När data ska inhämtas behöver man i förväg veta vad är det vi vill göra med den. Samtycke måste inhämtas för datas tänkta användningsområde och ändras detta måste ett nytt samtycke inhämtas. Dvs vi kan bara använda data för det som det finns samtycke till.

Man får därmed inte samla in mer data än nödvändigt för ändamålet och om man inhämtat godkännande från individen och därefter vill ändra användandet av dess data måste nytt godkännande inhämtas.

Till Persondata räknas alla data som på något sätt kan hänföras till en individ inom EU. Det finns en utförlig genomgång av detta som presenteras på IMY, se här.

Samtycke och socialtjänstlagen/i vardagen

Samtyckesfrågan i ett boende är extra utmanade då en betydande andel av de boende kan ha kognitiv svikt och därmed inte alltid själv kan ta ställning och aktivt ge sitt samtycke i vardagen. Samtycke krävs vid insatsens införande men också för att bekräfta dagliga händelser/situationer. Samtycket är därför något som verksamheten hanterar dagligen i sin professionella roll för att säkerställa rätten till att leva ett skäligt liv och stöds enligt socialtjänstlagen. Vid införande och användning av Välfärdsteknik/trygghetsteknik kan samtyckesfrågan hanteras genom att värdera om värdet av att dela data är större än risk för intrång i individens integritet.

Det handlar om att göra an bedömning om det digitala stödet skapar ett värde eller om andra lösningar är lika effektivt och värdeskapande. I den sk Västeråsmodellen ges ett stöd i hur man juridiskt och praktiskt kan hantera samtyckesfrågan vid bedömningen av införandet och hanteringen av trygghetsskapande teknik som t ex trygghetskameror, se vidare här.

Val av tekniklösning styr

När det gäller Välfärdsteknik har valet av teknisk lösning av betydelse för om det aktualiserar GDPR eller inte. Vid t ex valet av tillsynsinsats kan valet mellan en sensor och en kamera ge olika behov av samtyckeskrav.

Väljer vi t ex tillsyn med hjälp av en sensor (t ex ir/värmesensor) avpersonifieras data så att informationen inte på något sätt går att hänföra till en individen. Data räknas då inte som persondata och kräver därför inte samtycke av vare sig individ eller dess anhöriga medan en insats med en traditionell bildbaserad tillsynskamera innebär insamling av persondata och behöver en dokumenterat samtycke från den boende eller i vissa fall då den boende inte själv kan fatta beslut, även dess anhöriga.

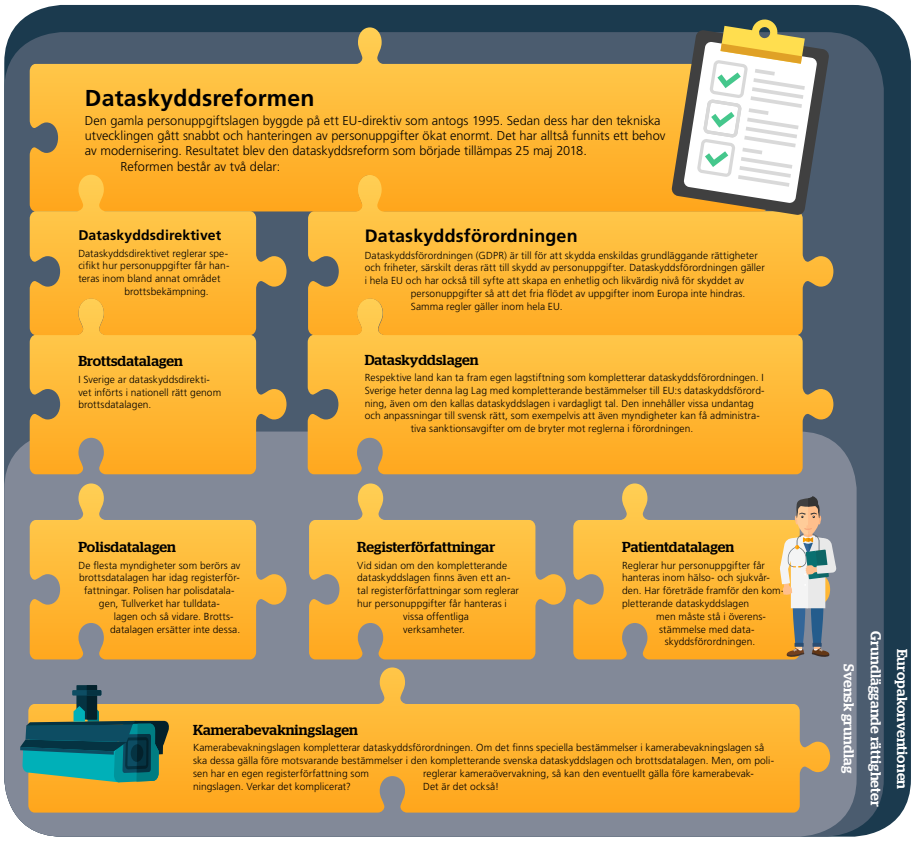
Fördjupning och checklista

Det finns en bra utbildning i GDPR hos integritetsmyndighete som ger en god översikt kring GDPR och dess olika aspekter och de har även tagit fram en checklista för inhämtande av samtycke som man kan ladda ner. Se här för mer information.

Lagar och förordningar som stöd för den personliga integriteten

När det gäller insamlande och delande av data mellan aktörer inom ett boende finns ett flertal lagar och förordningar som samspelar för att skapa ett skydd för individens personliga integritet.

Integritetsskyddsmyndigheten har visat i en överskådlig modell hur de olika lagarna och förordningarna hänger ihop. För en tydligare och läsbar bild.



Säkerhet och Klassa

Säkerhet

IT-säkerhet, eller informationsteknik-säkerhet, är en disciplin som syftar till att skydda information och data som lagras, behandlas och överförs genom datorer och IT-system från hot, risker och oönskad åtkomst. IT-säkerhet är av avgörande betydelse i dagens digitala värld, där företag, organisationer och enskilda individer är starkt beroende av IT-system och nätverk för att utföra sina uppgifter och hantera känslig information.

Här är några viktiga aspekter av IT-säkerhet:

Konfidentialitet: Det innebär att säkerställa att information endast är tillgänglig för de som har behörighet att komma åt den. Detta uppnås genom att använda kryptering och behörighetskontroller.

Integritet: IT-säkerhet syftar också till att skydda data från oavsiktliga ändringar eller obehörig manipulation. Detta görs genom att övervaka och verifiera att data förblir oförändrad.

Tillgänglighet: Det innebär att säkerställa att system och data är tillgängliga när de behövs och inte är föremål för nedstängning eller avstängning av attacker eller fel.

Autenticering och auktorisering: IT-säkerhet använder autentiserings- och auktoriseringsmekanismer för att verifiera användares identitet och bestämma vilka behörigheter de har. Detta förhindrar obehörig åtkomst.

Sårbarhetshantering: Att upptäcka och hantera sårbarheter i system och programvara är avgörande. Dessa sårbarheter kan utnyttjas av angripare om de inte åtgärdas.

Brandväggar och intrusion detection/prevention system (IDS/IPS): Dessa tekniker används för att övervaka nätverkstrafik och blockera eller varna för skadlig aktivitet.

Säkerhetspolicy och utbildning: Organisationer behöver etablera säkerhetspolicyer och utbilda sina anställda om säkerhetsbästa praxis för att minska mänskliga fel och risker.

Säkerhetskopiering och katastrofåterställning: Att regelbundet säkerhetskopiera data och ha en plan för att återställa system i händelse av en katastrof är avgörande för att säkerställa affärscontinuitet.

Felsökning och incidenthantering: Snabb upptäckt och svar på säkerhetsincidenter är nödvändigt för att minimera skador och förhindra framtida attacker.

Uppdateringar och patchhantering: Att hålla system och programvara uppdaterade med de senaste säkerhetspatcharna är viktigt för att täppa till kända sårbarheter.

IT-säkerhet är en pågående process eftersom hotlandskapet ständigt förändras med nya teknologier och angreppsmetoder. Organisationer och individer måste vara proaktiva och anpassa sig till dessa förändringar för att säkerställa att deras information och IT-resurser förblir skyddade.

Systematiskt informationssäkerhetsarbete för att säkra grundkrav

Dataskyddsförordningens grundkrav omfattar att säkerställa informationens tillgänglighet, riktighet och konfidentialitet. Det innebär att informationssäkerhetsarbetet ska hindra att information läcker vidare, förändras/förvanskas eller förstörs men också att säkerställa att information finns tillgänglig när den behövs.

För att säkerställa dataskyddsförordningens grundkrav är det därför viktigt att arbeta strukturerat. Hos Sveriges ansvariga myndighet, Integritetsmyndigheten (Informationssäkerhet.se) finns ett metodstöd för att systematiskt arbeta med informationssäkerhetsarbete. Den är utarbetad för den som arbetar med dessa frågor i organisationen och stödjer arbetet med att uppfylla kraven i dataskyddsförordningen vilket även innefattar information om personuppgifter (och därmed även GDPR frågor).

Metodstöd i informationssäkerhet finner du här

SKRs Kompetenscenter välfärdsteknik har tagit fram en guide där aspekterna av informationssäkerhet sammanfattas avsnittsvis med grundläggande information. Länk till SKRs guider finner du här.

I kommuner och organisation är IoT naturliga tjänster i vardagen. Kraven ökar på offentliga verksamheter att tillgängliggöra information för ytterligare tjänster och innovationer vilket även ställer högre krav på informationssäkerhetsarbetet. När det gäller informationssäkerhetsarbete finns det stöd och verktyg från myndigheter till kommuner och organisationer för att arbeta vidare med informationssäkerhet.

- IMY:s (Integritetskyddsmyndigheten) beskrivning av informationssäkerhet, se här.
- MSB:s (Myndigheten för samhällsskydd och beredskap) metodstöd för systematiskt informationssäkerhetsarbete ligger på en egen portal för informationssäkerhet:
  Informationssäkerhet.se. MSB:s Metodstöd för systematiskt informationssäkerhetsarbete riktar sig till dig som arbetar med informationssäkerhet i en organisation, oavsett verksamhetsområde och storlek på organisation. Metodstödet ska kunna användas om din organisation står i startgroparna för att införa det systematiska arbetssättet men också om din organisation redan har mycket på plats.
  - Metodstödet, se här
  - Metodstöd för systematiskt informationssäkerhetsarbete, se här.
- SIS:s (Svenska Institutet för standarder) beskrivning av informationssäkerhet, se här.
- SKR:s (Sveriges Kommuner och Regioner) har både beskrivning av informationssäkerhet i generella drag samt informationssäkerhet avseende välfärdsteknik samt har tagit fram SKRs guide för tillräckligt god informationssäkerhet.
- SKR:s självskattningsverktyg. För att få en snabb överblick över vilka områden i informationssäkerhet som finns och vad som saknas, kan Kompetenscenter välfärdstekniks självskattningsverktyg användas. Se ”En guide för tillräckligt god informationssäkerhet vid ...” och SKR ” Informationssäkerhet i kommuner och regioner”

KLASSA – ett verktyg för Informationsklassning av befintliga data.

I ett säkerhetsperspektiv är informationsklassning är en metod som stöder verksamheten att välja rätt åtgärder för att skydda information. SKR erbjuder ett webbstöd för att göra klassningar består av tre delar: informationsklassning, handlingsplan och upphandlingskrav.

För att underlätta ett strukturerat informationssäkerhetsarbete har SKR tagit fram ett självskattningsverktyg som heter KLASSA vilket används för att klassa verksamhetssystem och datalagring. Klassa är skapat i samverkan med RISE för SKR:s medlemmar, kommuner och regioner.

- Klassa
- Metodstöd – Klassa för IoT

En informationsklassning görs utifrån
3 olika perspektiv:

- Konfidentialitet – att informationen kan åtkomst begränsas.
- Riktighet – information ska vara tillförlitlig, korrekt och fullständig.
- Tillgänglighet – att informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet.

Varje perspektiv graderas från nivå 0 till 4, där nivå 0 står för ”ingen eller försumbar skada” och nivå 4 står för ”synnerligen allvarlig skada”. Den 4:e nivån är så allvarligt att hanteringen av den inte stöds i Klassa utan det krävs en specialinsats för att hantera den. Tänk rikets säkerhet och väldigt hemlig information.

Case – Klassning av verksamhetsdata i ett boende

Vi har sammanställt ett case för att visa på processen och få med några tips. Caset är från ett klassificeringsarbete som genomfördes med deltagare från både verksamhet, förvaltning och styrning från två kommuner Haparanda och Hudiksvall.

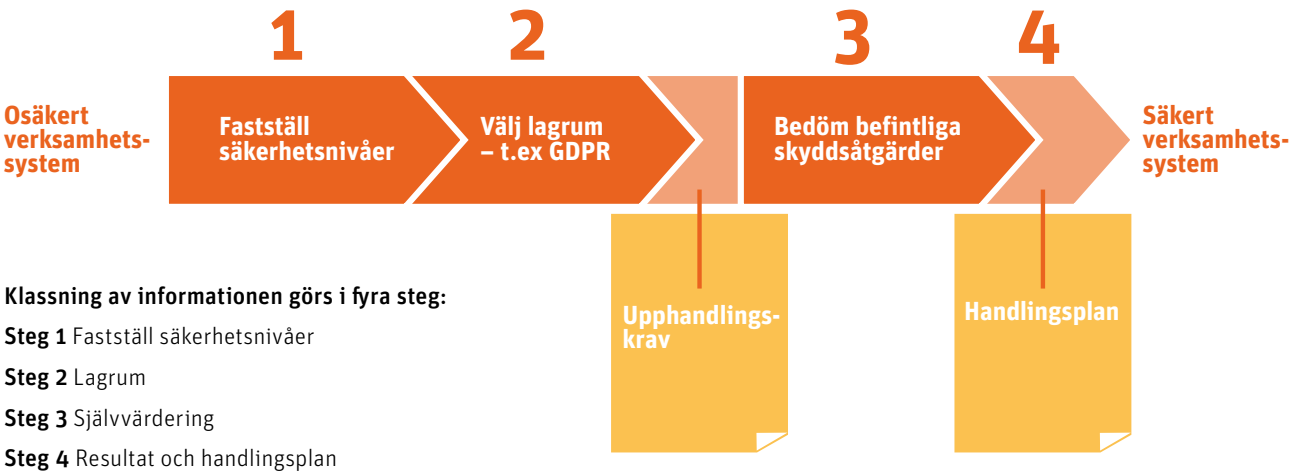
En viktig del vid klassningsarbetet är att fånga deltagare från olika områden och nivåer. Ett måste är att få med medarbetare som arbetar med systemen. Dom bidrar med verklighetsförståelse, dvs hur fungerar det egentligen vilket är en avgörande framgångsfaktor. Även systemförvaltaren har en viktig roll.

Vad är det vi klassar? Vilken information hanteras?

- Vi klassar inte system utan data/ informationsmängder.
- Data i verksamheten – Omfattningen och fokus på denna klassning är den data som verksamheten hanterar för att driva sin dagliga verksamhet.
- Det finns olika system i de två kommunerna och man har valt att fördela data på olika sätt. Data är fördelat på fler olika system i Haparanda jämfört med Hudiksvall. I Hudiksvall har man samlat mer i Treserva. I Haparanda ligger det mesta som vi klassar i verksamhetssystem.

Arbetsprocessen Informationsklassning i KLASSA

För att genomlysa arbetet med informationsklassning användes SKR:s demoversion av KLASSA. Viktigt att ta med sig är att arbetet med klassningen inte är en engångsgrej som checkas av utan ett ständigt pågående arbete. Man bör årligen följa upp arbetet med klassningen och oftast kommer nya infallsvinklar som man inte tidigare tänkt på vilket leder till ett förbättrat arbete. Nedanstående bild visar arbetsgången. Bilden är dock något missvisande då den borde vara cyklisk på grund av att det är ett ständigt pågående arbete utan avslut.



Klassning av informationen görs i fyra steg:

Steg 1 Fastställ säkerhetsnivåer

Steg 2 Lagrum

Steg 3 Självvärdering

Steg 4 Resultat och handlingsplan

Säkerhetsnivåer

Klassning nivå 3 Läkemedel och känsliga personuppgifter.

Exempel - medicinlistor:

- ”Sköterskorna litar inte på info som ligger i verksamhetssystem utan utgår från det som ligger i system för medicinlistor när det gäller medicinlistor, vilket är där det är uppdaterat och korrekt. Men, medicinsignering ligger i kommunens system så medicinlistor finns där också. Än så länge finns inte digital medicinsk signering i alla boende (Haparanda)”

Tillgänglighet

Klassning nivå 3

Exempel datakrasch:

- ”Ju mer digitala vi blir desto mer sårbara blir vi”. Kalix datakrasch ett exempel på hur sårbart det är. – Haparanda

Exempel: SITS kortsystem – vi kommer inte in i systemet – ger ”allvarlig skada”

- Tänk på att Tidsaspekten en del av bedömningen: Allvarlig skada innehåller även en tidsaspekt. En timmes avbrott ger nivå 0 men om det är lång tid, vad händer då? Bra att tänka på vid upphandling att tidsaspekten även definieras då det är skillnad på 1 tim/månad eller 1 dygns avbrott i sträck. Rekommendation att styra detta i SLA- Service level agreement. T ex hur länge får ett avbrott pågå? Olika känslighet beroende på tjänst/data. Jmf t ex känslighet i data för trygghetslarm.

Exempel system för trygghetslarm – Hur hanterar vi störningar och hur känsliga är vi?

- Båda kommunerna hade problem med sina system för trygghetslarm ifjol. Personliga besök i stället för larm, extrainkallad personal, extra insatser fick sättas in då man inte kunde lita på larmen/data från system för trygghetslarmen. Arbetet blev påverkat men man kunde hantera detta med manuell tillsyn.

Exempel – riskbedömning förändrad omvärld – Aktuellt just nu i kommunerna:

- Hur fungerar vi i ett icke digitalt samhälle/situation? Har vi rutiner för analogt arbete? Haparanda har tex framtagna rutiner för driftsstopp i IT-stödet för samverkan vid utskrivning från sluten hälso- och sjukvård. Finns rutiner på plats för avbrott påverkar det bedömningen av klassificeringsnivå då manuella rutiner ersätter.

Självvärderingsfasen

Självvärderingen är en stor del av klassaverktyget och innehåller 132 frågor. Men vi gjorde endast en delmängd av dessa som exempel och diskussionsunderlag. Nuläget fångar vi i självvärderingen, utkomsten blir en handlingsplan och insikt i vad vi behöver utveckla.

Exempel som speglar en återkommande uppföljningsproblematik:

- Driftsleverantörer av systemet har krav på sig att dom ska genomföra utbildningar. Men, vi efterfrågar inte uppföljning av dessa från leverantören så vi vet eg inte om utbildning har genomförts.

Exempel: ”Ganska ofta skiljer sig verkligheten och styrningen åt”

- Enhetschefen ger och avslutar behörighet i systemet till medarbetare. ”det ligger kvar folk i systemet som har slutat” Ofta ligger personers behörighet kvar när dom byter för att arbeta i ett annat boende eller annan roll i kommunen. Slutar man sin anställning försvinner rättigheterna automatiskt att komma in i systemet men behörigheten ligger kvar.

Exempel – krav följs inte upp

- En hel del av säkerhetsfrågorna regleras i kraven mot leverantörer av olika tjänster som kommunen har inhandlat. T ex säkerhetskopiering. En återkommande utmaning är hur dessa krav efterlevs och att denna osäkerhet påverkar bedömningen av informationsklassningen och informations/datasäkerheten.
- Ett annat exempel är att det finns i avtal t ex att åberopa 3:de part för en utvärdering av olovlig åtkomst. Dessa åberopas inte, dvs återigen man följer inte upp fullt ut.

Handlingsplanen

Efter genomgång av steg 1–3 skapas en handlingsplan i systemet. Handlingsplanen går att ta ut i Excel där man sedan kan arbeta vidare med underlaget.

Case Klassa Sammanfattning och reflektion

- Centrala roller är systemägare, systemförvaltare och driftsansvariga. Men, vid övningen saknades en viss detaljkompetens från den dagliga verksamheten, dvs hur man i vardagen hanterar data/information vilket hade gett fler insikter i hur det eg. fungerar som komplement till den bild av vad hur man har tänkt att det ska fungera och de processer, ansvar och roller man har utsett idag. Detta kan vara ett bra råd till de som ska genomföra sin klassningsövning inför t ex en upphandling av ett system till ett nytt boende för att få rätt kravbild. Man behöver komma ner på golvet en nivå närmare för att se hur det eg. fungerar i en annan övning.
- Använd dataskyddsombuden. Dataskyddsombudet är en roll både för kontroll och stöd för GDPR. Rekommendation att använda denna roll som stöttande. Ha en dialog och skapa delaktighet.
- Reflektion från deltagarna var att de ser behovet och nyttan i att arbeta strukturerat med verktyget och ”att det inte var så svårt”.

Ägande av data

Ägande av data hänvisar till den juridiska och formella rätten och ansvaret för data. Det definierar vem som har kontroll över och ansvar för data och vilka rättigheter och begränsningar som gäller för dess användning, lagring, delning och hantering.

Ägandet av data kan vara individuellt eller organisatoriskt. Individuellt ägande av data innebär att en enskild person har rättigheterna och ansvaret för data som rör dem själva, till exempel personliga dokument, hälsorelaterad information eller personliga användardata. Organisatoriskt ägande av data innebär att en organisation, såsom ett företag, en myndighet eller en institution, äger och kontrollerar data som genereras eller samlas in i organisationens verksamhet.

Äganderättigheterna och ansvaret för data kan fastställas genom olika mekanismer, inklusive kontrakt, lagstiftning, användaravtal eller sekretesspolicyer. Det kan även vara beroende av specifika branschregler eller dataklassificeringsstandarder som styr vilken typ av data som kan ägas och hur den ska hanteras.

Ägande av data är en viktig aspekt inom datahantering och integritet. Det innebär att säkerställa att rättigheter och integritet för de berörda parterna respekteras och att data används på ett ansvarsfullt sätt. Det kan även innebära att fastställa behörigheter och begränsningar för åtkomst och användning av data, samt att säkerställa att data skyddas mot obehörig åtkomst, förlust eller stöld.

Det är viktigt att tydligt definiera och kommunicera ägandet av data för att undvika missförstånd och konflikter. Det kan kräva att etablera interna riktlinjer och processer för att hantera äganderätten till data och säkerställa överensstämmelse med tillämpliga regler och lagar som skyddar både individens och organisationens rättigheter och integritet i samband med datahantering.

Delning av data

Vid delning av data är det viktigt att ta hänsyn till flera aspekter för att säkerställa att delningen sker på ett ansvarsfullt och lagligt sätt.

Innan du delar data måste du överväga om det finns några sekretess- eller integritetsfrågor att ta hänsyn till. Särskilt när det gäller känsliga eller personligt identifierbara uppgifter måste du säkerställa att du har samtycke eller rättmätigt skäl att dela informationen och att den är adekvat skyddad för att undvika obehörig åtkomst eller missbruk.

Du måste vara medveten om tillämpliga lagar och regler som styr delning av data, särskilt när det gäller personuppgifter, branschspecifika regler eller immateriella rättigheter. Se till att du följer relevanta dataskyddslagar, upphovsrättslagar eller andra juridiska krav för att undvika rättsliga konsekvenser.

Innan du delar data är det viktigt att fastställa tydliga avtal och kontrakt med de mottagande parterna. Detta kan inkludera att fastställa användningsändamål, begränsningar, sekretessvillkor och eventuella överföringsavtal som säkerställer att data används enligt överenskomna villkor och inte vidarebefordras till obehöriga.

Se till att den data du delar är korrekt, tillförlitlig och av hög kvalitet. Det kan vara viktigt att dokumentera och förklara datakällor, metodik och eventuella begränsningar för att de mottagande parterna ska kunna använda och tolka informationen på rätt sätt.

Vid delning av data bör du överväga att begränsa åtkomsten till endast de nödvändiga parterna för att minimera risken för obehörig åtkomst eller dataintrång. Användning av säkerhetsåtgärder såsom kryptering, anonymisering eller pseudonymisering kan bidra till att skydda data och säkerställa att endast auktoriserade användare kan få tillgång till den.

Var medveten om de etiska aspekterna av att dela data och se till att du har rättmätigt samtycke från de berörda parterna. Respektera principerna för informerat samtycke och se till att delningen av data är i linje med etiska normer och principer för att skydda människors rättigheter och intressen.

Genom att vara medveten om dessa faktorer och vidta lämpliga åtgärder kan du säkerställa att delning av data sker på ett säkert, ansvarsfullt och lagligt sätt. Det är alltid rekommenderat att rådfråga experter inom dataskydd, juridik eller relevanta områden för att följa bästa praxis och uppfylla alla nödvändiga krav.

Affärsmodeller och delning av data

Det finns ett antal faktorer att beakta vid affärsmodeller och delning av data.

Identifiera hur delning av data kan bidra till att skapa värde för din organisation. Utvärdera hur data kan användas för att förbättra produkter, tjänster, kundupplevelser eller effektivisera interna processer. Se till att delningen av data är strategiskt inriktad och stödjer dina övergripande mål och önskade effekter.

Utvärdera möjligheterna att generera intäkter genom att dela data. Det kan innebära att erbjuda data som en betald tjänst eller att ingå partnerskap eller affärsavtal där data utgör en handelsvara. Var medveten om immateriella rättigheter och licensieringsmodeller som kan användas för att skydda och kommersialisera data.

Se till att skydda känsliga affärsdata och företagshemligheter när du delar data. Implementera adekvata säkerhetsåtgärder och kontraktsvillkor för att skydda din information och minimera risken för obehörig användning eller läckage av viktig affärsinformation.

Fokusera på att ha högkvalitativ och tillförlitliga data för att stödja dina önskade effekter. Se till att data är korrekt, uppdaterad och följer branschstandarder och bästa praxis för att säkerställa att den är användbar och värdefull för din organisation.

Säkerställ att delningen av data är i linje med tillämpliga lagar och regler inom dataskydd, immateriella rättigheter och konkurrenslagstiftning. Följ etiska riktlinjer och principer för att skydda användarnas integritet och upprätthålla förtroende hos dina kunder och intressenter.

Utforska möjligheten att ingå partnerskap eller samarbeten med företag eller organisationer för att dela och utbyta data. Det kan bidra till att skapa synergier, utöka din datakapacitet och skapa nya möjligheter inom din affärsmodell.

Etablera tydliga riktlinjer, processer och avtal för hantering och delning av data. Säkerställ att datadelningsavtal tydligt definierar användningsändamål, rättigheter, ansvar och begränsningar för de inblandade parterna.

Genom att noggrant tänka på dessa faktorer kan du maximera värdet av delning av data inom din affärsmodell samtidigt som du säkerställer att lagliga, etiska och konfidentiella aspekter beaktas. Det är också viktigt att hålla sig uppdaterad om relevanta lag.

Länkar till fördjupning

- Socialstyrelsen har tagit fram utbildningar för att arbeta med etik och integritetsfrågor när ny teknik ska införas, se här.
- En genomgång av samtycke presenteras på IMY, se här.
- I Västeråsmodellen ges ett stöd i hur man juridiskt och praktiskt kan hantera samtyckesfrågan, se här.
- Utbildningar inom GDPR finns hos IMY, se här.
- En överskådlig modell hur de olika lagarna och förordningarna hänger ihop finns hos IMY. Se här.
- Metodstöd i informationssäkerhet finner du här
- SKR guide där aspekterna av informationssäkerhet sammanfattas avsnittsvis med grundläggande information, se här.
- IMY:s (Integritetskyddsmyndigheten) beskrivning av informationssäkerhet, se här.
- MSB Metodstödet, se här.
- MSB Metodstöd för systematiskt informationssäkerhetsarbete, se här.
- SIS:s (Svenska Institutet för standarder) beskrivning av informationssäkerhet, se här.
- SKR ”En guide för tillräckligt god informationssäkerhet vid ...”, se här
- SKR ” Informationssäkerhet i kommuner och regioner, se här.
- Metodstödet KLASSA (SKR), se här.
- Klassa för IoT, se här.

Kvickguide 2 är gjord i ett samarbete med Riksbyggen, RISE, Haparanda Stad och Hudiksvalls kommun.
Projektet har utförts inom Strategiska innovationsprogrammet IoT Sverige, en gemensam satsning av Vinnova, Formas och Energimyndigheten