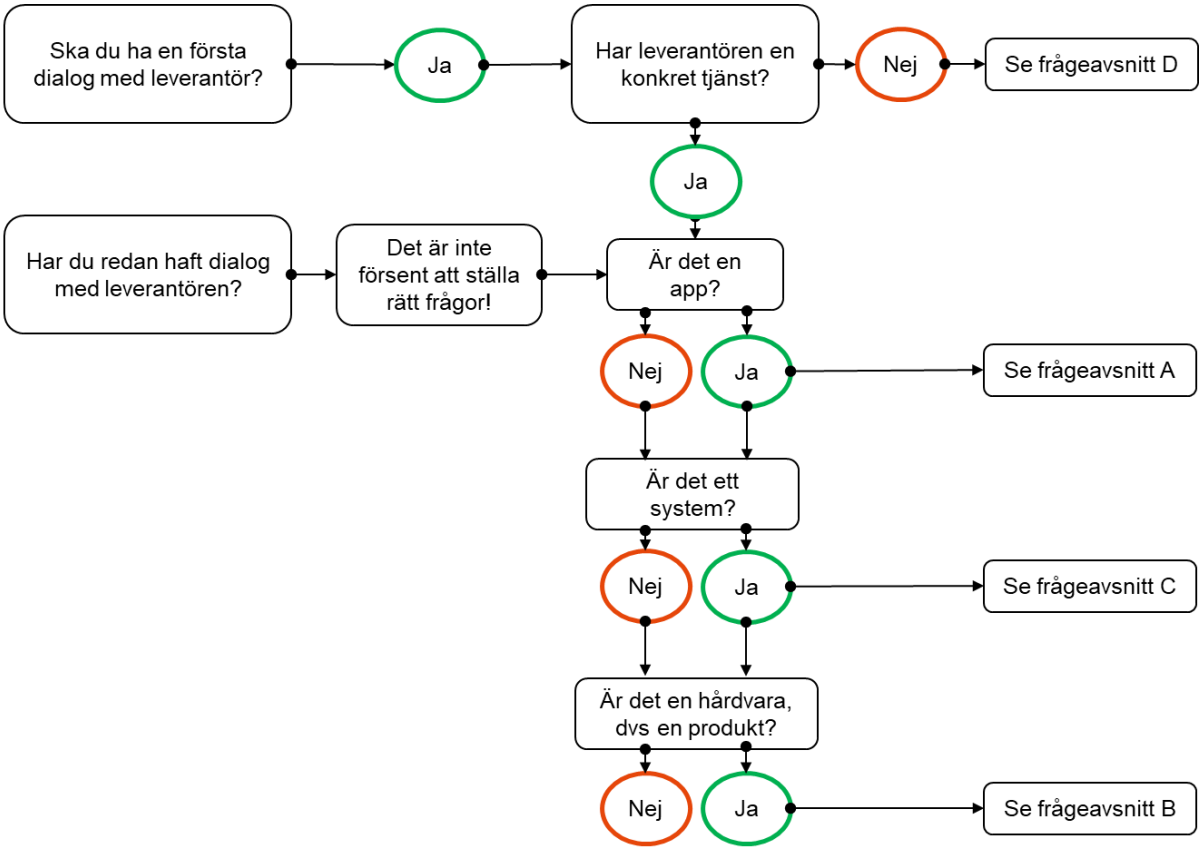
Informationssäkerhetsfrågor till första leverantörsdialogen

Ett av många sätt att underlätta verksamhetsutveckling med hjälp av hälso- och välfärdsteknik är att redan i förstudien tänka på informationssäkerhet. Det blir annars lätt extra möten, långa mejltrådar med leverantör och ökad risk för handbroms senare i processen.

Utifrån diskussioner med jurister, informationssäkerhetsamordnare, dataskyddsombud och leverantörer har jag noterat vanligt förekommande informationssäkerhetsrelaterade frågor som behöver svar innan pilot ens kommer på tapeten. Därför har jag tagit fram detta frågebatteri, som kan användas som mötesguide i första dialogen med eller skickas per mejl, till leverantörer som erbjuder digitala tjänster inom vård och omsorg. De flesta leverantörer besvarar dock minst en tredjedel av dessa under deras dragning (de börjar lära sig våra krav).

Några av frågorna är grundläggande, medan några är tjänstespecifika. Nöj er inte med ja/nej svar utan be om detaljer. Det är inte meningen att du som projektledare, handläggare eller nyfiken medarbetare ska kunna bedöma och analysera svaren utan det får experterna ta hand om senare. Om ni dessutom väljer att gå vidare med samma leverantör, kan ni återanvända informationen till er dataskyddskonsekvensbedömning. Enkelt och effektivt!



Shadan Ghafouri, Eskilstuna kommun, 2022-06-20

Frågeavsnitt A: Applikationer

1. Vem är leverantören?
    a. Etablerad vs start-up, dotterbolag, svenskt, inom/utomeuropeiskt?
    b. Om leverantören har några underleverantörer, redogör för den/dessa.
    c. Om leverantören har några underbiträden, redogör för den/dessa.
    d. Ansvarar leverantören för teknisk support? Vart befinner sig supporten geografiskt?
2. Vad är det för tjänst? Beskriv syftet, hur det funkar och om det är en välbeprövad/ny tjänst.
3. Behandlas personuppgifter? Beskriv varför och hur.
    a. Om ja, vilken typ av kategorier personuppgifter rör det sig om?
    b. Vad för typ av inloggningsalternativ (autentisering) erbjuder leverantören?
    c. Vem har åtkomst och behörighet till personuppgifterna?
    d. Kommer personuppgifter att (behöva) krypteras?
        i. Om ja, hur och vart krypteras de?
        ii. Vem har krypteringsnyckeln?
    e. Kommer personuppgifterna att (behöva) pseudonymiseras?
        i. Om ja, hur och vem har då pseudonymiseringsnyckeln?
    f. Hur länge sparas personuppgifterna och när raderas de?
4. Hur är appen uppbyggt? (specificera)
    a. Finns det några tredjepartsfunktioner?
    b. Om ja, vem tillhandahåller dessa funktioner?
        i. Tillhandahålls tredjepartsfunktionerna av en inomeuropeisk part?
            1. Om nej, kan den ersättas med en inomeuropeisk part?
5. Loggas aktiviteter i appen?
    a. Vad loggas?
    b. Hur loggas det?
    c. Vem kan se, ändra respektive radera loggarna?
6. Förutsätter tjänsten en viss hårdvara?
7. Är appen beroende eller oberoende operativsystem?
8. Hur notifieras användare?
9. Förutsätter tjänsten en viss uppkoppling eller nätverkshastighet?
10. Fungerar appen off-line?
    a. Om ja, hur länge och vad har den för synkfunktioner?
11. Förutsätter tjänsten en viss systemintegration? Varför?
12. Har appen ett administrationssystem?
    a. Om ja, se frågeavsnitt C.
13. Förutsätter tjänsten förkunskaper hos användarna?
14. Har leverantören möjlighet att visualisera det tekniska informationsflödet med en processkarta?
15. Hur ser leverantören på möjligheten att på ett eller annat sätt integrera deras tjänst med annan leverantörs tjänst? (långsiktig planering)

Frågeavsnitt B: Hårdvara/produkt

1. Vem är leverantören?
    a. Etablerad vs start-up, dotterbolag, svenskt, inom/utomeuropeiskt?
    b. Om leverantören har några underleverantörer, redogör för den/dessa.
    c. Om leverantören har några underbiträden, redogör för den/dessa.
    d. Ansvarar leverantören för teknisk support? Vart befinner sig supporten geografiskt?
2. Vad är det för tjänst? Beskriv syftet, hur det funkar och om det är en välbeprövad/ny tjänst.
    a. Beskriv om det är en medicinteknisk produkt eller välfärdsteknik.
3. Behandlas personuppgifter? Beskriv varför och hur.
    a. Om ja, vilken typ av kategorier personuppgifter rör det sig om?
    b. Vad för typ av inloggningsalternativ (autentisering) erbjuder leverantören?
    c. Vem har åtkomst och behörighet till personuppgifterna?
    d. Kommer personuppgifter att (behöva) krypteras?
        i. Om ja, hur och vart krypteras de?
        ii. Vem har krypteringsnyckeln?
    e. Kommer personuppgifterna att (behöva) pseudonymiseras?
        i. Om ja, hur och vem har då pseudonymiseringsnyckeln?
    f. Hur länge sparas personuppgifterna och när raderas de?
4. Förutsätter tjänsten ström, batterier och/eller laddningsrutin?
5. Förutsätter tjänsten en viss uppkoppling eller nätverkshastighet?
    a. Om wifi, beskriv minimikrav för fungerande uppkoppling (glöm inte att kontakta SEF-IT för stöd i bedömning)
    b. Om mobildata, beskriv vem som tillhandahåller SIM-kort, hur mycket surfmängd som behövs och till vilken kostnad.
6. Förutsätter tjänsten en viss systemintegration? Varför?
7. Loggas aktiviteter i tjänsten?
    a. Vad loggas?
    b. Hur loggas det?
    c. Vem kan se, ändra respektive radera loggarna?
8. Förutsätter tjänsten förkunskaper hos användarna?
9. Hur ser leverantören på möjligheten att på ett eller annat sätt integrera deras tjänst med annan leverantörs tjänst? (långsiktig planering)

Frågeavsnitt C: System

1. Vem är leverantören?
    a. Etablerad vs start-up, dotterbolag, svenskt, inom/utomeuropeiskt?
    b. Om leverantören har några underleverantörer, redogör för den/dessa.
    c. Om leverantören har några underbiträden, redogör för den/dessa.
    d. Ansvarar leverantören för teknisk support? Vart befinner sig supporten geografiskt?
2. Vad är det för tjänst? Beskriv syftet, hur det funkar och om det är en välbeprövad/ny tjänst.
3. Behandlas personuppgifter? Beskriv varför och hur.
    a. Om ja, vilken typ av kategorier personuppgifter rör det sig om?
    b. Vad för typ av inloggningsalternativ (autentisering) erbjuder leverantören?
    c. Vem har åtkomst och behörighet till personuppgifterna?
    d. Kommer personuppgifter att (behöva) krypteras?
        i. Om ja, hur och vart krypteras de?
        ii. Vem har krypteringsnyckeln?
    e. Kommer personuppgifterna att (behöva) pseudonymiseras?
        i. Om ja, hur och vem har då pseudonymiseringsnyckeln?
    f. Hur länge sparas personuppgifterna och när raderas de?
4. Hur är systemet tekniskt uppbyggt? (specificera)
5. Är det en molntjänst?
    a. Vart är molnet?
    b. Vem äger molnet?
    c. Vem har tillgång till molnet?
    d. Vad görs med personuppgifterna i/via molnet?
6. Kan tjänsten erbjudas via server?
    a. Vems server?
    b. Finns eller behövs back-up server?
    c. Vad kommer kommunen respektive leverantören att ha tillgång till?
7. Förutsätter tjänsten en viss hårdvara?
8. Förutsätter tjänsten en viss uppkoppling eller nätverkshastighet?
9. Förutsätter tjänsten en viss systemintegration? Varför?
10. Loggas aktiviteter i systemet?
    a. Vad loggas?
    b. Hur loggas det?
    c. Vem kan se, ändra respektive radera loggarna?
11. Förutsätter tjänsten förkunskaper hos användarna?
12. Har leverantören möjlighet att visualisera det tekniska informationsflödet med en processkarta?
13. Hur ser leverantören på möjligheten att på ett eller annat sätt integrera deras tjänst med annan leverantörs tjänst? (långsiktig planering)

Frågeavsnitt D: Ingen konkret tjänst – innovation

1. Vem är leverantören?
    a. Etablerad vs start-up, dotterbolag, svenskt, inom/utomeuropeiskt?
    b. Om leverantören har några underleverantörer, redogör för den/dessa.
    c. Om leverantören har några underbiträden, redogör för den/dessa.
    d. Ansvarar leverantören för teknisk support? Vart befinner sig supporten geografiskt?
2. Vad är det för verksamhetsbehov som leverantören förväntas tillgodose?
3. Vad har leverantören för förväntningar på oss?
4. Finns det befintliga lösningar på marknaden?
    a. Om ja, varför kan inte de tillgodose verksamhetsbehovet?
5. Kommer det krävas behandling av personuppgifter? Beskriv varför och vilken typ av kategorier personuppgifter det rör sig om.
6. Vem kan tänkas behöva ha åtkomst och behörighet till personuppgifterna?
7. Vad för typ av stöd erbjuder leverantören i utvecklingen av tjänsten?
8. Vem kommer äga slutprodukten?
9. Behövs en etikprövning?
10. Rör det sig om en pilot? Beskriv uppskattad tidsplan.
11. Rör det sig om en längre innovationsutveckling? Beskriv uppskattad tidsplan.
12. Säkerställ regelrätt samarbete genom att kontakta jurist och upphandlare.