Datum
2022-08-25

Version 01

Informationssäkerhetsgruppen

Informationssäkerhet och dataskydd - regiongemensamma inköp/anskaffning

1 Innehåll

2 Checklista för inköp/anskaffning

Beskriver vilka aktiviteter ska genomföras innan inköp/anskaffning.

Fråga	**Ja**
Har informationen kartlagts och analyserats?	☐
Har en informationsklassning genomförts?	☐
Har informationssäkerhetskrav tagits fram enligt informationsklassning?	☐
Har det tagits ställning till om ett personuppgiftsbiträdesavtal krävs?	☐
Har en riskanalys genomförts? *En riskanalys är inte alltid relevant att genomföra innan inköp men senast vid implementation av avtal.*	☐

3 Förslag på hantering vid gemensamma inköp/anskaffningar – minimum nivå

Om er organisation redan har ett arbetssätt för analys, informationsklassning samt kravställan avseende informationssäkerhet **bör ni använda det tillvägagångssättet.**

Nedan följer minimum nivå för de aktiviteter som måste genomföras.

3.1 Kartläggning och analys av information

Fråga	Ja	Nej	Kommentar
Ska leverantören hantera organisationens information?	☐	☐	Om ja: genomför informationsklassning
Ska leverantören behandla personuppgifter?	☐	☐	Om ja: Personuppgiftsbiträdesavtal måste tecknas
Ska leverantören eller tjänsten hantera information som omfattas av sekretess?	☐	☐	Om ja: tillse att krav från Offentlighets- och sekretesslagen tillgodoses samt tillse att sekretessförbindelse tecknas
Ska leverantören eller tjänsten hantera patientdata?	☐	☐	Om ja: tillse att krav från Patientdatalagen tillgodoses.
Berör det samhällsviktiga tjänster?	☐	☐	Om ja: tillse att krav från lagen om informationssäkerhet i samhällsviktiga och digitala tjänster tillgodoses.

3.2 Informationsklassning

Klassning avser	
Syfte med inköp/anskaffning:	*Exempel: ett system för att hantera incheckning till vårdbesök*
Information:	*Exempel:. ritningar, systemdokumentation ..*
Personuppgifter:	*Exempel: för- och efternamn, personnummer, bilder, uppgifter om hälsa*
Informationsklassning	
Konfidentialitet	
Motivering	
Riktighet	
Motivering	
Tillgänglighet	
Motivering	

Konsekvens	**Beskrivning**
Synnerligen allvarlig 4	Information som omfattas av säkerhetsskydd
Allvarlig 3	Mycket långa och/eller allvarliga avbrott eller störningar som leder till en avgörande inverkan på regionens förmåga att lösa uppdraget Kraftig påverkan på regionens ekonomi (> 5 % av verksamhetsbudget) Risk för liv och hälsa Allvarlig negativ effekt på enskilda individers rättigheter Förödande inverkan för externa intressenter Vite, avsked eller fängelse efter brott mot lagar, förordning eller avtal Mycket allvarlig förtroendeskada för regionens p.g.a. synnerligen omfattande negativ publicitet och negativ allmän opinion

Betydande 2	Långa och/eller allvarliga avbrott eller störningar som leder till betydande inverkan på regionens förmåga att lösa uppdraget Påtaglig ekonomisk påverkan på en eller flera verksamheter inom regionen (>1% av verksamhetsbudget) Risk för begränsade negativa effekter på hälsa Betydande negativ effekt på enskilda individers rättigheter Betydande negativ effekt för externa intressenter Vite eller varning efter brott mot lagar, förordning eller avtal Påtaglig förtroendeskada för regionen p.g.a. betydande negativ publicitet och negativ allmän opinion
Måttlig 1	Mindre avbrott och störningar i verksamheten som leder till vissa svårigheter att lösa uppdraget Viss ekonomisk påverkan på en eller flera enheter (< 1 % av verksamhetsbudget) Måttlig påverkan på liv, hälsa, rättigheter. Begränsad negativ effekt för externa intressenter Måttlig negativ effekt på enskilda individers rättigheter Varning eller erinran för försumlighet i förhållande till lagar, förordning eller avtal Mindre förtroendeskada för regionen p.g.a. negativ publicitet
Ingen eller försumbar 0	Inga eller försumbara svårigheter för verksamheten att nå målen. Ingen eller försumbar påverkan på liv, hälsa, rättigheter. Ingen märkbar skadekostnad för verksamheten/organisationen Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation. Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas inte eller i försumbar omfattning av otillgänglighet till systemet.

3.3 Definitioner

Information – är data som presenteras i ett sammanhang. Data är en representation av fakta, begrepp eller instruktioner i en form lämpad för överföring, tolkning eller bearbetning av människor eller maskiner. Information å andra sidan innebär själva innebörden av datan, vilket förutsätter att det finns en mottagare som kan tolka datan.

Patientdata - personuppgifter och journalhandlingar som finns inom Hälso- och sjukvården.

Personuppgift - Personuppgifter är all slags information som kan knytas till en fysiskt levande person. som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,

Behandling av personuppgifter - en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring,

spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Sekretess – beteckning på information som inte ska lämnas ut och därför inte blir en **offentlig** allmän handling. Sekretess innebär ett förbud mot att röja en uppgift vare sig det sker muntligen, genom utlämnande av allmän handling eller på annat sätt.

Samhällsviktig verksamhet - avses verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet. Se mer Vad är samhällsviktig verksamhet? (msb.se)

4 Kravkatalog

Se bilaga för informationssäkerhetskrav.
Kravkatalogen ska endast nyttjas om upphandlade regionen inte redan har en egen kravkatalog implementerad.

5 Information till respektive region

Innan avtalstecknande ska följande information lämnas till respektive regions dataskyddsombud:

- Kartläggning över vilken information leverantörer kommer att hantera, inklusive personuppgifter
- Resultat av informationsklassning
- Vilka informationssäkerhetskrav och dataskyddskrav som finns med i avtalet.
- Personuppgiftsbiträdesavtal inklusive instruktioner och förteckning över underbiträden.