SÖDERTÖRNS HÖGSKOLA | STOCKHOLM
sh.se

Checklista avseende informationssäkerhet inför upphandling av system eller tjänst

1. Inledning

Södertörns högskola ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Målet med högskolans informationssäkerhetsarbete är att skydda högskolans informationstillgångar. Det är därför viktigt att analysera vilka informationssäkerhetsrisker som kan uppkomma till följd av att upphandla ett visst system eller en viss tjänst. För att kunna identifiera sådana risker vid upphandling av ett nytt system eller en ny tjänst ska systemägare eller den som avser att upphandla utgå från denna checklista.

Checklistan innehåller ett antal frågor som rör informationshantering och informationssäkerhet och som ska utredas inför upphandling. Syftet med att utreda och besvara de frågor som framgår av checklistan är att kunna ställa rätt krav på leverantören.

Vid utredning av dessa frågor kan det finnas behov av att inhämta stöd från olika kompetenser inom högskolan, såsom IT-kompetens, juridisk kompetens och arkiv- och informationsinriktad kompetens. Det är viktigt att dessa kompetenser blir involverade redan på ett tidigt stadium i processen. Detta för att undvika att högskolan upphandlar system eller tjänster som inte uppfyller kraven på informationssäkerhet eller andra rättsliga krav.

2. Frågor att utreda inför upphandling

2.1. Identifiera informationen

Innan en upphandling genomförs behöver man utreda vad för typ av information som kommer att hanteras i systemet eller tjänsten som man avser att upphandla. Det kan till exempel vara information som för närvarande ingår i ett visst system eller information som ingår i ett forskningsprojekt. Här kan man ta hjälp av högskolans informationshanteringsplan för att se vilken typ av information som förekommer inom högskolans verksamhet. Observera att det även kan vara fråga om information som inte finns med i informationshanteringsplanen.

I samband med att informationen identifieras kan det vara bra att fastställa, eller i vart fall uppskatta, mängden av information som avses att hanteras i systemet eller tjänsten som ska upphandlas.

2.2. Värdera informationen

Genom att värdera och ställa arkivkrav på system i ett initialt skede bidrar det till kostnadseffektivitet, informationssäkerhet, verksamhetsnytta och regeluppfyllnad.

Värderingen av informationen sker efter att informationen har identifierats. Ett första steg i värderingen är att bedöma om informationen utgör allmän handling eller inte. Nästa steg är att bedöma om informationen har ett bevarandevärde eller inte och hur informationen ska hanteras under hela sin livscykel.

Även om informationsvärderingen visar att systemet inte innehåller allmänna handlingar, kan det innehålla personuppgifter eller annan information som behöver hanteras ur ett GDPR- eller ett informationssäkerhets perspektiv.

Informationsvärdering görs kontinuerligt under systemets livscykel om systemet innehåller allmänna handlingar som ska bevaras och arkivkrav hanteras löpande. Alla beslut av vikt dokumenteras, exempelvis gallringsutredningar.

Frågor att utgå ifrån när värderingen genomförs:

- Kommer systemet innehålla information som ska bevaras? Har systemet i så fall en exportfunktion?
- Kommer systemet innehålla information som ska gallras? Har systemet i så fall en gallringsmodull eller ska informationen gallras när systemet avskaffas?
- Finns det en bevarandeplan för systemets livscykel gällande drift, utveckling, avveckling, gallring och arkivering?

2.3. Klassificera identifierad information

När informationen har identifierats ska informationen klassas enligt högskolans klassificeringsmodell. Klassningsresultatet kommer sedan att påverka vilka krav som ska ställas på leverantören. Om systemet eller tjänsten som är föremål för upphandling kommer att hantera information som tidigare har klassats av högskolan, kan det tidigare klassningsresultatet användas som vägledning för den aktuella informationsklassningen.

Informationen ska klassas i enlighet med högskolans Riktlinjer för informationssäkerhet, dnr 4347-1.1.2-2021, och Vägledning för informationsklassning.

2.4. Genomför en risk- och sårbarhetsanalys

Enligt högskolans Riktlinjer för informationssäkerhet ska en risk- och sårbarhetsanalys göras vid större planerade förändringar. En sådan analys kan även genomföras i andra sammanhang. Exempel på när en sådan analys ska genomföras är vid upphandling av ett system eller en tjänst.

Syftet med en risk- och sårbarhetsanalys är att upptäcka risker, brister och fastställa konsekvenser som kan uppkomma till följd av en oönskad händelse. I analysen ska man beskriva hotbilder, kalkylera konsekvenser och skadekostnader samt bedöma sannolikheten för att hoten kan inträffa. Analysen kan sedan resultera i åtgärder som ska genomföras omedelbart eller på längre sikt.

2.5. Ta ställning till om en konsekvensbedömning behöver göras

En konsekvensbedömning ska göras om det upphandlade systemet eller tjänsten kommer att innefatta en personuppgiftsbehandling som sannolikt leder till hög risk för enskilda personers fri- och rättigheter.

En konsekvensbedömning ska föregås av en riskbedömning. Om det i riskbedömningen bedöms att personuppgiftsbehandlingen kommer att innebära en hög risk för enskilda

personers fri- och rättigheter måste en konsekvensbedömning göras. Enligt dataskyddsförordningen ska dataskyddsombudet rådfrågas vid genomförande av en konsekvensbedömning, och det är därför viktigt att involvera högskolans dataskyddsombud. Information om hur och när en konsekvensbedömning ska göras finns på medarbetarwebben under Rättslig vägledning.

2.6. Utred vad det är för typ av system eller tjänst

När man har identifierat vilken information som ska hanteras samt genomfört informationsklassning och risk- och sårbarhetsanalys ska man utreda vad för typ av system eller tjänst som ska upphandlas. Det kommande systemet eller tjänsten ska ha en kostnadseffektiv it-drifttjänst med en väl fungerande digital förvaltning.

Ur informationssäkerhetssynpunkt är det viktigt att systemet eller tjänsten kan ha en integration mot högskolans IDP – identitetsleverantör (Active Directory AD, Azure AD, ADFS). Detta gör att inloggningar till det nya systemet eller tjänsten sker via högskolans befintliga SH-konton.

Ska systemet eller tjänsten integreras med redan befintliga system på högskolan, är det viktigt att berörda systemägare involveras tidigt i en kommande teknisk integration.

2.7. Utred rollfördelningen mellan avtalsparterna (gäller vid behandling av personuppgifter)

Om informationen innefattar personuppgifter är det viktigt att utreda rollfördelningen mellan Södertörns högskola och avtalsparten. Man behöver alltså utreda vem som har rollen som personuppgiftsansvarig och eventuellt personuppgiftsbiträde. Högskolan är ofta personuppgiftsansvarig, det vill säga den som bestämmer ändamålen för behandlingen och hur behandlingen ska ske, medan en leverantör av ett system eller en tjänst är ofta personuppgiftsbiträde. Det behöver dock inte vara så och det är därför viktigt att kartlägga förhållandet mellan parterna. Om avtalsparten är ett personuppgiftsbiträde krävs det att högskolan ingår ett personuppgiftsbiträdesavtal med leverantören. Mall för personuppgiftsbiträdesavtal finns på medarbetarwebben under Rättslig vägledning.

2.8. Nästa steg – Kravställningsprocessen

Efter att ha utrett de frågor som framgår ovan kan den som avser att upphandla gå vidare i upphandlingsprocessen med att formulera de krav som leverantören ska bemöta. Den utredning som gjorts enligt denna checklista kommer att kunna ligga till grund för kravställningen. Upphandlingsstöd kan ges av högskolans upphandlare vid kravställningsprocessen.