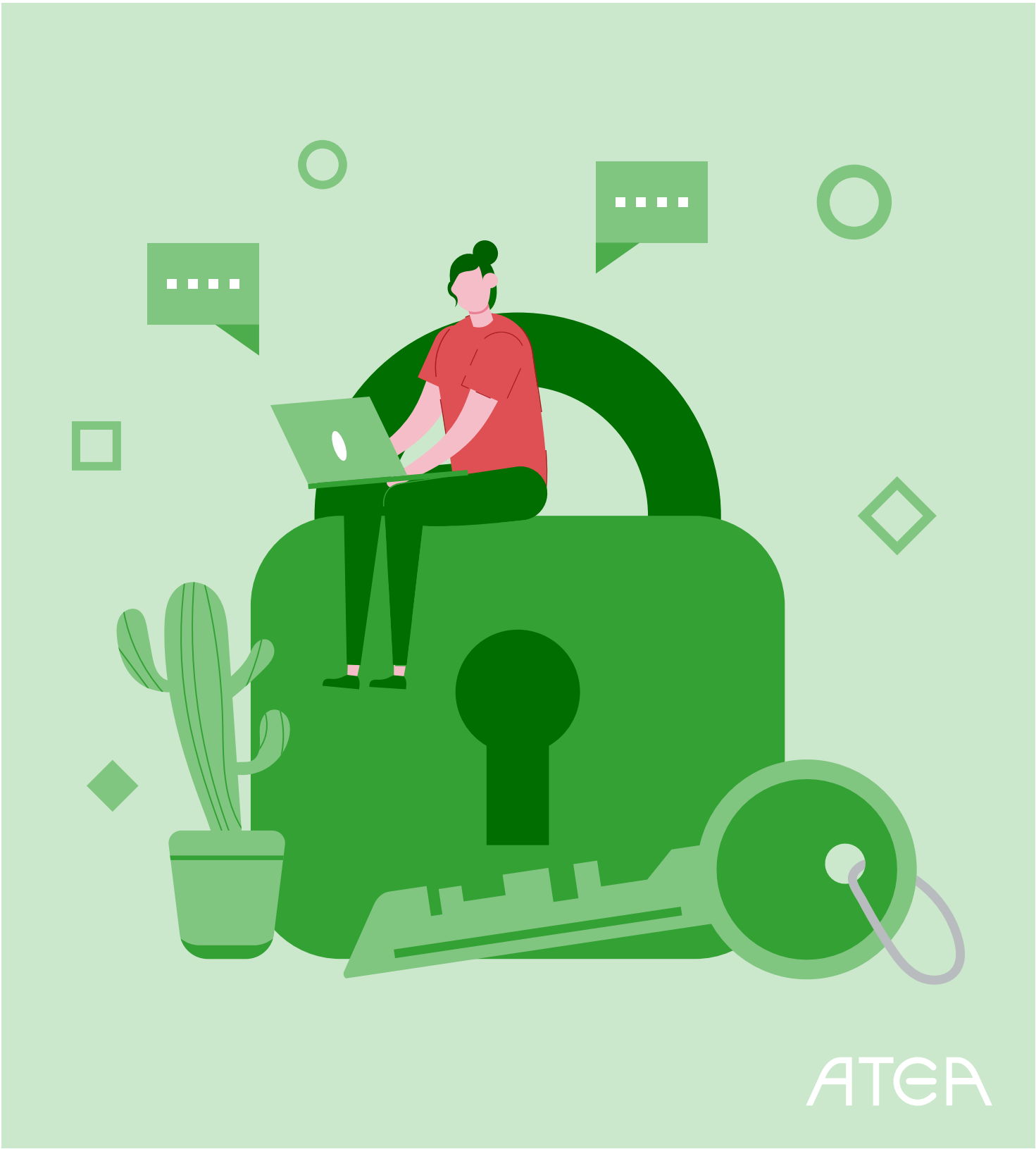
November 2023

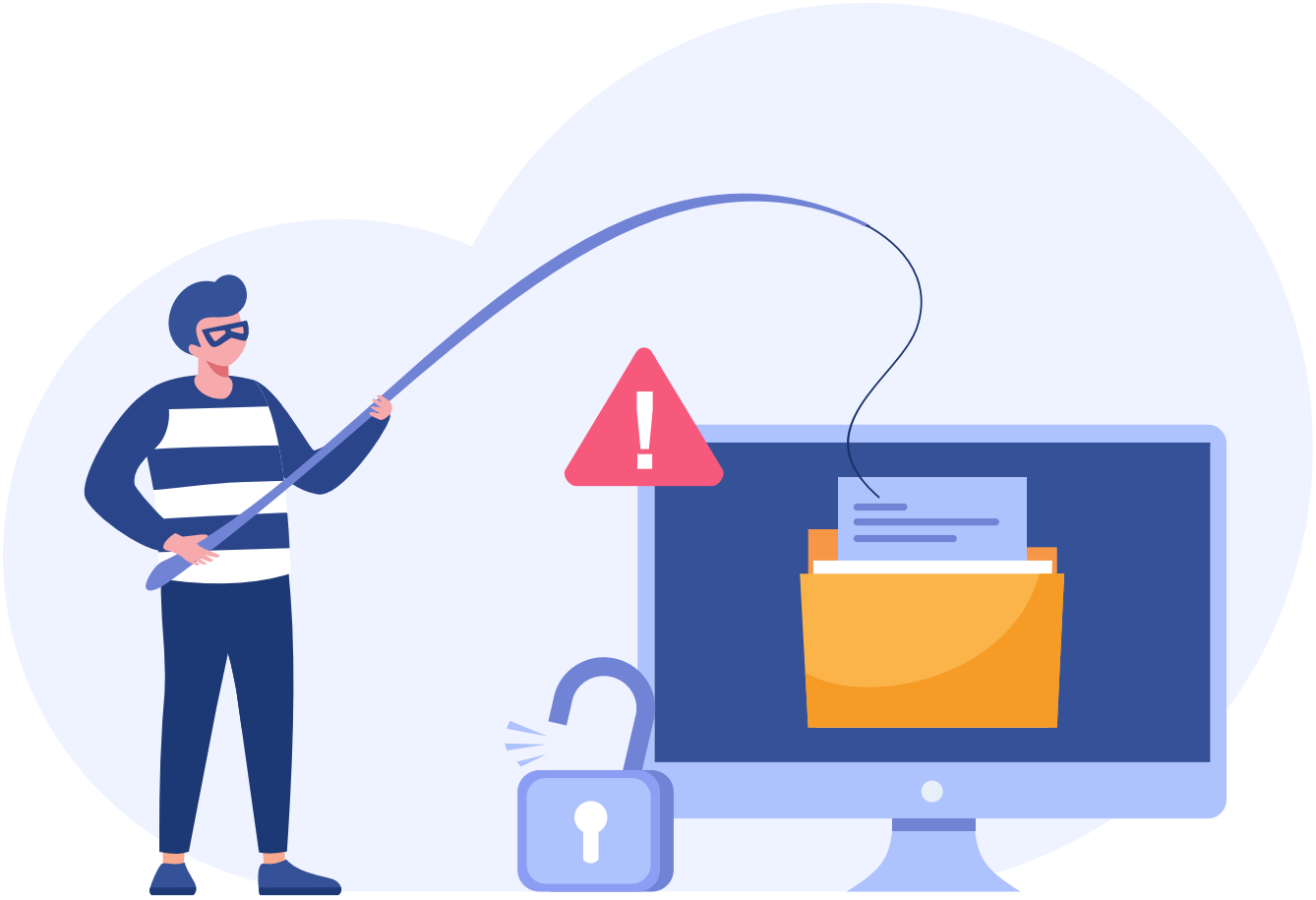
Ateas kravguide för informationssäkerhet



Detta dokument kommer att guida er genom viktiga aspekter att ta i beaktning vid utformningen av informationssäkerhetskrav i upphandlingar.

Informationssäkerhet är en viktig aspekt att beakta i upphandlingar för att bedöma leverantörers förmåga, skydda känslig information, minska ekonomiska och juridiska risker samt uppfylla krav och regelverk. Genom att inkludera informationssäkerhet i kravställningen kan man skapa en trygghet för alla involverade parter under hela avtalstiden.

I upphandlingar är det viktigt att göra ett gediget grundarbete för att ställa krav som är relevanta i förhållande till det som ska upphandlas. För att uppnå detta är det viktigt att ha en effektiv process redan från start där man baserat på informationsklassificeringen beskriver vilka behov av skydd informationen har och ställer tydliga krav på informationssäkerhet baserat på dessa behov.



ATEA

OBS! Den här guiden är en rekommendation som baseras på Ateas kunskap om it-branschen. Vid offentlig upphandling behöver upphandlande verksamheter själva säkerställa att de krav som ställs är förenliga med upphandlingslagstiftningen.

Varför är det viktigt att beakta informationssäkerhet i upphandlingsarbetet?

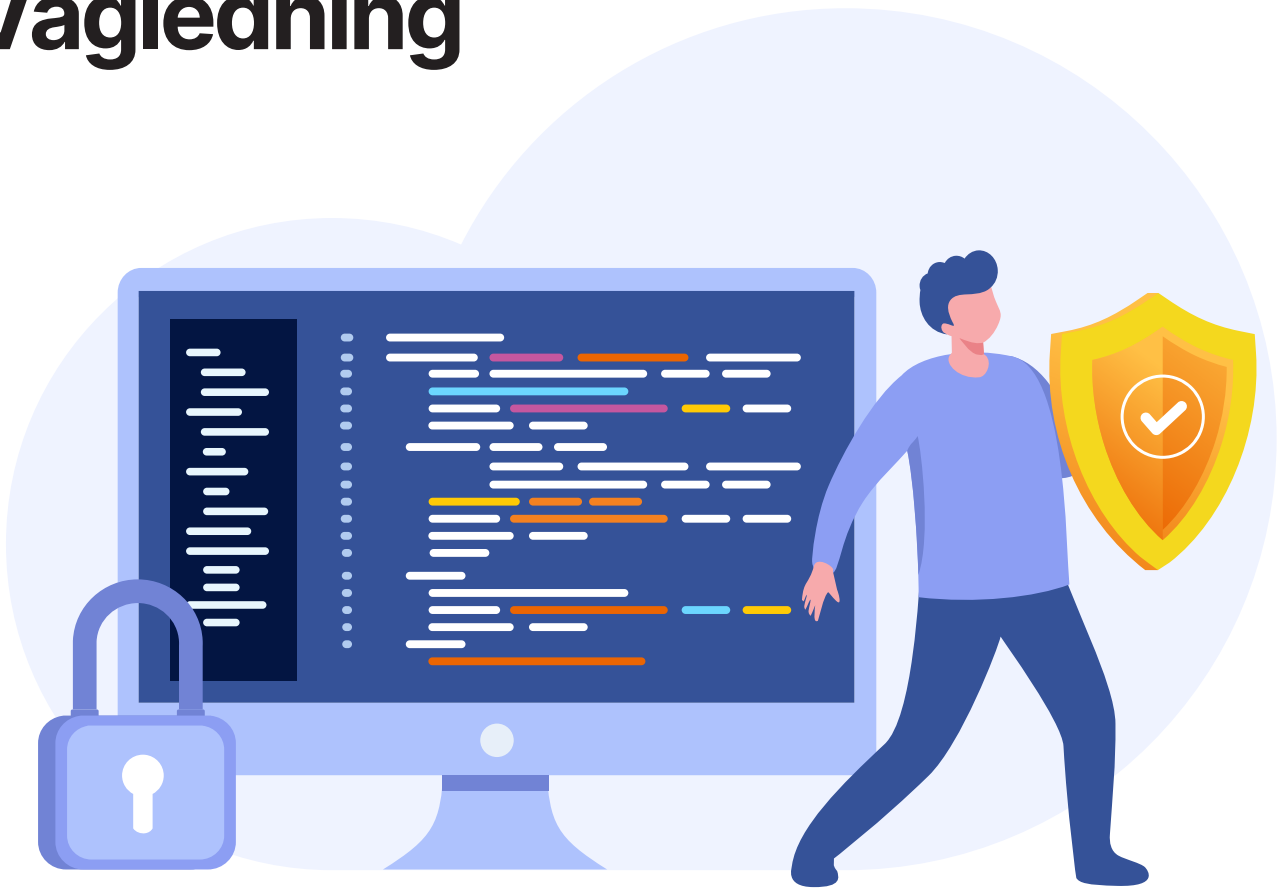
Många organisationer har interna eller externa krav på informationssäkerhet. Genom att beakta informationssäkerhet i upphandlingen kan man säkerställa att den egna organisationens krav och regelverk efterlevs i de tjänster som ska upphandlas. Det kan även bidra till att bygga förtroende hos intressenter och visa att man tar säkerheten på allvar.

Säkerställa leverantörens förmåga att hantera informationssäkerhet
Genom att beakta informationssäkerhet i upphandlingen kan man bedöma leverantörens förmåga att hantera och skydda känslig information på ett säkert sätt. Detta kan inkludera att utvärdera leverantörens informationssäkerhetspolicy, rutiner för incidenthantering och personalens kompetens inom området.

Minimera risker för dataintrång och skadlig programvara
Genom att ställa krav på informationssäkerhet i en upphandling kan man minimera risken för dataintrång och skadlig programvara under avtalstiden. Detta kan inkludera krav på säkra nätverksanslutningar, uppdaterade säkerhetsprotokoll och säkerhetsåtgärder för att förhindra obehörig åtkomst.

Minska ekonomiska och juridiska risker
Om informationssäkerheten hotas finns risk för allvarliga ekonomiska och juridiska konsekvenser för både den upphandlande organisationen och leverantören. Genom att beakta informationssäkerhet kan man minska risken för ekonomiska förluster, såsom kostnader för att hantera incidenter eller förlust av affärskritisk information. Dessutom kan det hjälpa till att undvika rättsliga tvister och straffrättsliga åtgärder.

Vägledning



Informationsklassificering
Första steget är att genomföra en informationsklassificering. Det är en process som hjälper er att identifiera vilken typ av information som är mest känslig eller värdefull för att ge informationen förutsättningar att skyddas på korrekt sätt. Vad som är lämpliga säkerhetsåtgärder beror på informationstypen (t.ex. konfidentiell information, företagshemligheter eller personuppgifter). Exempel på skyddsåtgärder som informationsklassificering kan resultera i är åtkomstbegränsning av information, kryptering, säkerhetskopiering eller fysisk begränsning till information. Om en informationsklassificering inte redan är gjord är det ett bra första steg för att förstå:

- vilken information som leverantören kommer att få tillgång till under avtalstiden
- vilket värde informationen har för er organisation

Vid behov ta stöd av metodstöd från MSB[1] eller ta hjälp av er CISO (Chief Information Security Officer), informationssäkerhetssamordnare, informationssäkerhetstrateg eller motsvarande.

Frågor som bör redas ut innan upphandlingsunderlaget utformas:

- **Vilka uppgifter kommer att hanteras av leverantören under avtalstiden?**
- **Vilka skyddsvärden finns och vad ska skyddas?**
  Kommer leverantören att behandla sekretessbelagda uppgifter, känsliga personuppgifter eller uppgifter som är känsliga för organisationen?
- **Vilka interna och externa krav finns att förhålla sig till?**
  Kanske behöver ni ställa särskilda krav på leverantören om denna kommer att leverera något till den samhällsviktiga verksamheten som ni ansvarar för?
  Se mer information om detta under avsnittet ”Ytterligare vägledning”.

Roller i personuppgiftsbehandlingen
Det är inte alltid helt enkelt att reda ut de olika rollerna i en personuppgiftsbehandling. Man bör tänka igenom rollfördelningen i leveransen och klargöra om den kommer att innebära att leverantören ska utföra behandling av personuppgifter för er räkning baserat på era instruktioner (om en biträdessituation kommer att uppstå).

Enligt Dataskyddsförordningen är personuppgiftsansvarig den som bestämmer **ändamål och medel** för behandlingen av personuppgifter och är ansvarig för hur personuppgifterna behandlas genom hela livscykeln. Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning och **i enlighet med dennes instruktioner**.

[1] www.informationssakerhet.se/metodstodet/anvanda/#klassning-av-information

Om leverantören kommer att agera personuppgiftsbiträde är det viktigt att identifiera:

- Vilka typer av personuppgifter som omfattas? (Alla typer av personuppgifter har inte samma behov av skydd)
- Lämpliga tekniska och organisatoriska säkerhetsåtgärder som personuppgiftsbiträdet behöver vidta för att skydda personuppgifterna.
- Om personuppgifterna kan och får överföras till ett tredje land utan adekvat skyddsnivå. Se vägledning från EDPB[2].

Med hjälp av en rollanalys kan man identifiera respektive parts roll så att man vet om ett personuppgiftsbiträdesavtal ska finnas med i upphandlingsunderlaget eller inte. Vid behov ta hjälp av vägledning från EDPB[3] eller Danska Datatilsynet[4].

Riskanalys

Nästa steg är att göra att en riskanalys för att förstå de risker som är förknippade med att hantera informationen. Dessa parametrar är en bra början att utgå ifrån vid formulering av informationssäkerhetskrav på leverantörer. Detta säkerställer att varan/tjänsten uppfyller de krav på informationssäkerhet som ni identifierat som nödvändiga.

Samarbeta med kravställning

Baserat på informationsklassificering och riskanalyser ska lämpliga krav på säkerhetsåtgärder formuleras. För att säkerställa att kraven kan hanteras i praktiken behöver ni som upphandlande enhet involvera rätt kompetenser från er organisation vid framtagning av kravställningen för att få input från olika perspektiv så att ni kan skapa er en helhetsbild. Exempel på kompetenser som kan behöva involveras är informationssäkerhet, dataskydd, IT och juridik.

Kraven ska bidra till att uppnå er säkerhetsnivå

För att undvika missförstånd eller feltolkningar från leverantören är det viktigt att vara tydlig i kravställningen så att kraven är enkla att förstå och tolka. Tänk igenom hur kraven i upphandlingen formuleras och att det inte finns utrymme för tolkning av kraven samt om det kan finnas mer än en säkerhetsåtgärd för att uppfylla likvärdigt skydd för informationen. En alltför detaljerad kravställning kan utesluta leverantörer då de kan ha motsvarande skydd på plats men inte exakt det som efterfrågas. Man kan också överväga om kraven behöver vara uppfyllda av leverantören på anbudsdagen, först vid avtalsstart eller om det är tillräckligt att de uppfylls vid en senare tidpunkt under kontraktstiden.

Att arbeta efter erkända standarder såsom ISO/IEC 27001

Kravställningen bör inte vara för detaljerad utan i stället öppna upp för ett samarbete mellan parterna där samverkan kan ske för att över tid uppnå ändamålsenliga skyddsåtgärder anpassade till informationens värde. Detta ger leverantörer utrymme att beskriva sitt arbete vilket ger er en bättre möjlighet att utvärdera hur leverantören arbetar med informationssäkerhet och vilka möjligheter som finns gällande tekniska säkerhetsåtgärder.

Utgå ifrån erkända standarder för att identifiera möjliga informationssäkerhetskrav på varan eller tjänsten som ska upphandlas. I Sverige är det standard att utgå ifrån Ledningssystem för Informationssäkerhet ISO/IEC 27001 (LIS) eller likvärdiga erkända ramverk. Det viktigaste är inte att leverantören är certifierad utan att de har ett etablerat riskbaserat och systematiskt arbetssätt.

Uppföljning och efterlevnad

Tänk på att tydliggöra i upphandlingen hur ni kommer att följa upp och säkerställa att leverantörerna uppfyller de fastställda informationssäkerhetskraven under hela avtalstiden.

Inför avtalssignering

Innan signering bör ni kontrollera att leverantör verkligen uppfattat kravställning korrekt. En god rutin är att alltid boka möte med leverantör innan signering för att säkerställa/följa upp att leverantören har uppfattat informationssäkerhetskraven korrekt.

KOM IHÅG att dokumentera överenskommelser av informell karaktär och sådant som kommuniceras muntligt.

[2] edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
[3] edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en
[4] www.datatilsynet.dk/hvad-siger-reglerne/grundlaeggende-begreber/dataansvarlig-og-databehandler/dataansvarlig-og-databehandler

Att undvika

Undvik krav i stil med att anbudsgivaren ska garantera komplett efterlevnad då detta i realiteten är en omöjlighet. Det ni kan ställa krav på, och också följa upp, är att anbudsgivaren har ett riskbaserat och systematiskt arbete kring informationssäkerhet som innehåller en process för ständiga förbättringar.

Undvik även att ha ett standardiserat frågeformulär med krav som inte förändras beroende på vad som ska upphandlas. Alla upphandlingar och leveranser är unika och kraven behöver anpassas efter upphandlingsområdet.

KONTAKTA OSS! Vi på Atea hjälper gärna till med stöd, tips och råd.

Ytterligare vägledning

Vilka interna och externa krav finns att förhålla sig till?

Exempel på interna krav

- Policyer – avsiktsförklaringar för er organisation
- Strategier, riktlinjer eller motsvarande – mer detaljerade styrningar kring hur er organisation kan, bör eller ska agera

Exempel på externa krav

- EU-förordningar, EU direktiv och internationella konventioner
- Svenska lagar och förordningar
- Myndighetsföreskrifter

Biträdessituation – vad gäller?

Hur vet vi om det kommer uppstå en biträdessituation eller inte?

Det är inte i alla fall som ett avtal mellan två parter innebär att det finns en part som har rollen som personuppgiftsbiträde trots att personuppgiftsbehandlingar förekommer. Ibland kan båda parterna agera enskilt personuppgiftsansvariga där man delar uppgifter sinsemellan för att kunna uppfylla ett avtal.

Indikationer på att en biträdessituation uppstår:

- Om avtalet eller en del av avtalet innehåller en direkt anvisning om behandling av personuppgifter, t.ex. vid en backuptjänst när leverantören ska bearbeta, lagra, eller radera era personuppgifter.
- Om ni ensamt beslutar om
  - syften och väsentliga hjälpmedel och användning av personuppgifter (inklusive bearbetningssteg såsom insamling och radering)
  - vilka it-stöd eller metoder som ska användas
  - organisering av arbetet som påverkar behandlingen
  - tekniska och organisatoriska åtgärder kopplade till behandlingen
  - att anlita en annan organisation för att få hjälp med behandlingen
  - att personuppgifterna ska återlämnas eller raderas

Indikationer på att en biträdessituation <u>inte</u> uppstår:

- Om avtalet mellan er och leverantören i första hand avser tillhandahållande av en tjänst som inte innebär att leverantören ska behandla era personuppgifter, till exempel vid licensförsäljning.

Att teckna ett personuppgiftsbiträdesavtal med en part som inte agerar personuppgiftsbiträde är inte förenligt med dataskyddsförordningen, och innebär att man avtalar om ett ansvar som i praktiken inte är möjlig att leva upp till.

Tre goda ting

1. Välj en leverantör som arbetar utefter erkända standarder inom informationssäkerhet såsom ISO/ IEC 27001 eller likvärdigt för de väsentliga delarna i anbudsgivarens verksamhet som direkt medverkar till fullgörandet av kontraktet.

2. Involvera rätt kompetenser från er organisation vid framtagning av kravställningen, till exempel gällande informationssäkerhet, dataskydd, it och juridik beroende på vad det är för typ av upphandling.

3. Säkerställ att parterna är överens om innehållet i avtalet, dess innebörd och rollfördelning innan avtal signeras.