Instruktion för att lämna synpunkter

Eventuella synpunkter på nedanstående text lämnas genom att använda kommentarsfunktionen i Microsoft Word eller genom att ändra direkt i texten (använd funktionen ”Spåra ändringar”). Om ni anser att en text bör ändras eller tas bort ser vi gärna att ni motiverar varför. Vi ser också helst att ni lämnar förslag på hur ni anser att en alternativ text bör utformas.

Tack på förhand!

**Kommentarsfunktionen i Word:**
För att lämna en kommentar ska först den text som berörs av synpunkten markeras. Därefter väljs ”Ny kommentar” under menyn ”Granska” enligt nedanstående bild.



Synpunkten kan sedan skrivas in i kommentarrutan till höger om texten (se nedan bild).

****
**Funktionen ””Spåra ändringar” i Word**
Om ni väljer att ändra direkt i texten ser vi gärna att ni använder funktionen ”Spåra ändringar”. För att aktivera funktionen, välj ”Spårning” under menyn ”Granska” (se nedan bild) och välj sedan ”Spåra ändringar”.



I detta dokument framgår avtalsvillkor avseende informationssäkerhet och GDPR – avtalsvillkoren ska vara uppfyllda av leverantören samma dag som eventuellt ramavtal ingås

**Avtalsvillkor mellan Ramavtalsleverantören och Kammarkollegiet**

**Personal för support**

Personal som anlitas för support av journalföringssystem eller liknande (som innehåller Avropsberättigads information) ska befinna sig i ett land inom EU/EES eller i tredje land med adekvat skyddsnivå enligt beslut av Europeiska kommissionen.

**Avtalsvillkor för molntjänst**

***Autentisering***Molntjänster som används för att tillhandahålla Upphandlingsföremålet ska minst uppfölja följande.

* 1. 1. Unika personliga konton.
	2. 2. Multifaktorautentisering (MFA) för alla privilegierade användare och för alla användare som hanterar personuppgifter eller Avropsberättigads övriga information.
	3. 3. Åtkomst till system och kryptografiska nycklar ska styras med rollbaserad åtkomstkontroll (RBAC) enligt principen om minsta privilegium. Behörigheter ska minst var sjätte månad granskas och re-certifieras utifrån risk och känslighet, för att säkerställa att åtkomster förblir adekvata och proportionerliga. Utförda re-certifieringar ska loggas och arkiveras minst under den period som Ramavtalet och Kontrakt är i kraft.

***Krypterad datakommunikation***All överföring av Avropsberättigads information ska skyddas med kryptering som minst uppfyller TLS 1.2 med PFS (t.ex. ECDHE) eller motsvarande säkerhetsnivå.

Kryptering ska omfatta:

* Trafik mellan datacenter,
* Trafik mellan datacenter och Avropsberättigads nät,
* API‑anrop och batchöverföringar genom interna managementgränssnitt.

Kryptografiska nycklar som skyddar Avropsberättigads information ska lagras och hanteras i en säkerhetsmiljö som är lämpad med hänsyn till informationens känslighet och följa vedertagna branschstandarder.

***Krypterad lagringsmedia***Samtliga lagringsmedia (block, objekt, databaser, säkerhetskopior och eventuella cache/SSD) som lagrar Avropsberättigads information ska skyddas med stark kryptering. Krypteringsalgoritm och nyckellängd ska vara lämpliga utifrån informationens känslighet och följa vedertagna branschstandarder.

***Loggning***Ramavtalsleverantören ska samla, tidsstämpla (UTC via säker NTP), signera och skydda loggar mot otillbörlig ändring.

Inloggningar/autentiseringar, API-anrop, konfigurations- eller behörighetsförändringar, samt säkerhetshändelser/incidenter ska loggas. Loggarna ska lagras under den tid som är lämplig med hänsyn till risk, känslighet och vad som krävs för att uppfylla gällande rätt.

***Skydd mot skadlig kod***Molntjänster som används för att tillhandahålla Upphandlingsföremålet ska erbjuda skydd mot skadlig kod och avancerade hot genom lösningar som följer vedertagna industristandarder och bästa praxis. Skyddet ska omfatta automatiska uppdateringar, skanning av all inkommande data samt möjligheter att identifiera, isolera och hantera hot. Säkerhetsrelaterade händelser ska loggas och göras tillgängliga för vidare analys och uppföljning i Ramavtalsleverantörens loggningssystem.

***Säkerhetskopiering*** Databaser och filer som innehåller information som erhållits från Avropsberättigad ska säkerhetskopieras regelbundet och på ett sätt som säkerställer återställbarhet vid behov. Säkerhetskopior ska lagras krypterade och skyddas mot obehörig ändring under en lämplig tidsperiod. Lagringen bör ske på geografiskt separerade platser, med ett avstånd på minst tio (10) mil, för att minska riskerna vid lokal förlust eller skada.

Återställningspunkter (RPO) och återställningstider (RTO) ska fastställas baserat på behov. Detta ska återspeglas i Ramavtalsleverantörens avtal med eventuell Underleverantör som tillhandahåller tjänster för att behandla Avropsberättigads information. Nivåerna bör testas regelbundet, minst en gång i månaden, för att säkerställa att återställning kan genomföras inom fastställda tidsramar.

**Informationssäkerhetsarbete**Ramavtalsleverantören ska bedriva ett strukturerat och dokumenterat arbete med informationssäkerhet som minst omfattar den personal som nyttjas vid tillhandahållandet av Upphandlingsföremålet.

Inom ramen för informationssäkerhetsarbetet ska Ramavtalsleverantören:

1. arbeta efter en upprättad och av ledningen beslutad informationssäkerhetspolicy
2. ha fastställda och mätbara informationssäkerhetsmål,
3. arbeta med uppföljning av fastställda informationssäkerhetsmål,
4. ha rutiner för att identifiera och hantera risker utifrån fastställda informationssäkerhetsmål,
5. ha rutiner för hantering och rapportering vid säkerhetsincidenter,
6. ha en tydlig ansvarsfördelning inom organisationen gällande informationssäkerhetsarbetet,
7. säkerställa att anställda regelbundet informeras om hur information får hanteras,
8. säkerställa att anställda har teknisk tillgång till kundens data enbart i de fall det är nödvändigt för att kunna fullgöra uppdrag.

Ramavtalsleverantören ska genomföra regelbundna revisioner av informationssäkerhetsarbetet och på begäran av Kammarkollegiet kunna visa upp relevant dokumentation som styrker efterlevnaden av ovan ställda krav.

Om Ramavtalsleverantören inte uppfyller ovanstående krav och villkor kan det resultera i vite och andra påföljder enligt avsnitt *Avtalsbrott och* påföljder.

**Säkerhetsutbildning för personal**Ramavtalsleverantören ska själv eller genom anlitad Underleverantör/franchisetagare säkerställa att alla butiksanställda regelbundet, minst en gång årligen, får utbildning gällande hantering av patientdata enligt patientdatalagen, dataskyddsförordningen och gällande lagar om cybersäkerhet.

**Avtalsvillkor mellan Avropsberättigad myndighet och Ramavtalsleverantören**

**Generella krav gällande behandling av personuppgifter**

Om Ramavtalsleverantörens tillhandahållande av Upphandlingsföremål

innefattar behandling av personuppgifter ska behandlingen följa Europaparlamentets och rådets förordning (EU) 2016/679 (dataskyddsförordningen) med tillhörande genomförandeförfattningar. Det innebär bland annat en skyldighet för Ramavtalsleverantören att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas inom ramen för Kontraktet.

Ramavtalsleverantören ska på begäran av Avropsberättigad ingå de avtal som krävs för att uppfylla dataskyddsförordningen.

Ramavtalsleverantören ska säkerställa att anlitad Underleverantör som behandlar personuppgifter ingår de avtal med Avropsberättigad som krävs enligt dataskyddsförordningen.

**Behandling av information i journalföringssystem**

 Ramavtalsleverantören ska försäkra sig om att IT-system som används för journalföring lever upp till krav enligt dataskyddsförordningen och gällande lagar om cybersäkerhet.

Ramavtalsleverantören ska på begäran av Avropsberättigad kunna visa på vilka åtgärder som Ramavtalsleverantören eller anlitad Underleverantör har vidtagit för att säkerställa att personuppgifter i IT-system som används för journalföring behandlas inom EU/EES eller inom tredje land med adekvat skyddsnivå enligt beslut av Europeiska kommissionen.

**Tillgång till information vid upphörande av molntjänst**

För det fall Upphandlingsföremålet innefattar behandling av Avropsberättigads information i en molntjänst garanterar Ramavtalsleverantören i händelse av molntjänstens upphörande, oaktat orsak därtill, att

1. under en övergångsperiod om minst sex (6) månader, eller en annan period som Avropsberättigad anger, hjälpa Avropsberättigad med överföringen av molntjänsten till en annan leverantör eller tillbaka till Avropsberättigad enligt Avropsberättigads instruktioner. Säkerhetsåtgärder ska vidtas för att säkerställa att dataintegritet och konfidentialitet upprätthålls under övergångsperioden.
2. på Avropsberättigads begäran, fortsätta att tillhandahålla molntjänsten enligt Kontraktet och avtalade priser för nyttjande av Upphandlingsföremål under den tid som överföringen pågår.
3. överlämna och/eller radera Avropsberättigads information och alla kopior från Ramavtalsleverantören och dess Underleverantörers system, utan dröjsmål, enligt Avropsberättigads instruktion. Eventuell radering ska vara förenligt med eventuella lagstadgande krav.

Om inte annat anges i Kontrakt ska Avropsberättigads information överföras i ett standardformat för strukturerad data som är läsbart och möjligt att använda i andra sammanhang. Loggfiler, revisionsdata, accessdata och liknande metadata ska tillhandahållas i ett format som säkerställer dess användbarhet för Avropsberättigad utan hinder.

Avropsberättigad ska ha rätt att kontrollverifiera att all information har överförts korrekt och att alla kopior har raderats. Eventuella kostnader förknippade med överföringsprocessen ska bäras av Ramavtalsleverantören, såvida inte annat framgår av Kontrakt.

Under övergångsperioden ska regelbunden kommunikation ske mellan parterna för att säkerställa en smidig övergång. Specifika kontaktpunkter ska utses för detta ändamål.