RIKTLINJER FÖR BEHANDLING AV PERSONUPPGIFTER INOM

SKL KOMMENTUS AB OCH DESS BOLAG (KOMMENTUS)

1. BAKGRUND

Rätten till skydd av personuppgifter och den personliga integriteten tillkommer alla fysiska personer. Dessa rättigheter skyddas genom omfattande lagstiftning som innehåller regler och grundläggande principer för hur personuppgifter får behandlas under hela livscykeln från insamling till gallring. Regelverket säkerställer vissa rättigheter som varje registrerad individ kan utöva för att utöva kontroll i förhållande till behandlingen av personuppgifter. Avsikten med dessa rättigheter är att all behandling av personuppgifter ska vara transparent och förutsebar i förhållande till den registrerade.

Kommentus tar skyddet av den personliga integriteten på största allvar, både i förhållande till när Kommentus samlar in och behandlar personuppgifter för egna ändamål och när Kommentus behandlar personuppgifter för någon annans räkning i egenskap av personuppgiftsbiträde.

Dessa *Riktlinjer för behandling av personuppgifter* ("**Riktlinjerna**") beskriver vad Kommentus förväntar sig från sina anställda och andra som på olika sätt är involverade i Kommentus behandling av personuppgifter. Vidare beskriver Riktlinjerna på ett övergripande plan hur Kommentus skyddar de personuppgifter som behandlas inom ramen för Kommentus verksamhet. På motsvarande sätt beskriver dessa Riktlinjer även hur Kommentus kunder, leverantörer och samarbetspartners kan förvänta sig att Kommentus behandlar personuppgifter.

2. DEFINITIONER

"**Kommentus**"	betyder SKL Kommentus AB, org. nr. 556026-1900 inklusive dess dotterbolag AffärsConcept org. Nr. 556526-3182, SKL Kommentus Inköpscentral AB org. Nr. 556819-4798 och SKL Kommentus Media AB org. Nr. 556819-4764
"**behandling**"	betyder varje åtgärd eller serie av åtgärder som vidtas med personuppgifter såsom bl.a. insamling, inspelning, sammanställning, lagring, bearbetning eller omarbetning, mottagande, användning, röjande, överföring eller radering.
"**känsliga personuppgifter**"	betyder personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiösa eller filosofiska övertygelser, medlemskap i fackförening, genetisk data eller biometrisk data, samt uppgifter som rör hälsa, sexliv eller sexuell läggning.
"**personuppgift**"	betyder all information som är hänförlig till en identifierad eller identifierbar fysisk person.
"**personuppgiftsansvarig**"	betyder den fysiska eller juridiska person som bestämmer ändamålen och medlen för behandlingen av personuppgifter.
"**personuppgiftsbiträde**"	betyder den fysiska eller juridiska person som behandlar personuppgifter för en personuppgiftsansvarigs räkning.

"**registrerad**"	betyder en identifierbar fysisk person som kan identifieras direkt eller indirekt, särskilt genom en identifierare såsom namn, identifikationsnummer, geografisk data, elektroniska identifierare.
"**Tillämplig dataskyddslag-stiftning**"	betyder från tid till annan gällande lagstiftning, förordningar, inklusive föreskrifter som meddelats av berörda tillsynsmyndigheter, avseende skydd för fysiska personers grundläggande rättigheter och friheter och särskilt rätt till skydd av deras personuppgifter vid behandling av person-uppgifter som är tillämplig för Kommentus, inklusive lagstiftning, förordningar och föreskrifter som genomför direktiv 95/46 EG och, från och med den 25 maj 2018, Europaparlamentets och Rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

3. RIKTLINJERRIKTLINJERNAS OMFATTNING

Dessa Riktlinjer tillämpas på all behandling av personuppgifter som sker inom ramen för Kommentus verksamhet, både när Kommentus behandlar personuppgifter i egenskap av personuppgiftsansvarig och när Kommentus behandlar personuppgifter för annans räkning i egenskap av personuppgiftsbiträde. Avsikten är att all behandling av personuppgifter inom Kommentus ska ske i enlighet med dessa Riktlinjer och Tillämplig dataskyddslagstiftning.

Dessa Riktlinjer syftar till att komplettera Tillämplig dataskyddslagstiftning och dess tillämpning inom ramen för Kommentus verksamhet. Behandling av personuppgifter i enlighet med dessa Riktlinjer innebär dock inte per automatik att behandlingen sker i enlighet med Tillämplig dataskyddslagstiftning.

Tillämplig dataskyddslagstiftning ska alltid gälla framför vad som föreskrivs i dessa Riktlinjer. Dessa Riktlinjer ska dock tillämpas framför Tillämplig dataskyddslagstiftning i den utsträckning dessa Riktlinjer ger registrerade ett starkare skydd för personuppgifter och den personliga integriteten.

4. GRUNDLÄGGANDE PRINCIPER FÖR BEHANDLING AV PERSONUPPGIFTER

4.1 Laglighet

Behandling av personuppgifter inom Kommentus ska alltid ske i enlighet med Tillämplig dataskyddslagstiftning.

4.2 Ändamålsbegränsning

Kommentus ska alltid uttryckligen ange de ändamål för vilka personuppgifter behandlas och endast behandla personuppgifter i enlighet med dessa dokumenterade ändamål. Personuppgifter ska inte behandlas för ändamål som är oförenliga med de ursprungliga ändamålen med behandlingen, utöver vad som är tillåtet enligt Tillämplig dataskyddslagstiftning.

4.3 Uppgiftminimering och lagringsminimering

Kommentus ska endast behandla personuppgifter som är nödvändiga för att uppfylla de ändamål för vilka personuppgifterna ursprungligen samlats in. Personuppgifter ska således endast behandlas när det är nödvändigt och får därför inte behandlas endast för att personuppgifterna kan komma att vara användbara i framtiden (*uppgiftsminimering*).

Personuppgifter ska inte heller lagras för en längre tid än vad som är nödvändigt för att uppfylla ändamålen med behandlingen eller för att efterleva rättsliga skyldigheter. Kommentus ska därför säkerställa att personuppgifter löpande gallras i enlighet med Kommentus vid var tid gällande bevarandepolicy (*lagringsminimering*).

4.4 Personuppgifter ska vara uppdaterade och korrekta

Kommentus ska vidta åtgärder för att säkerställa att de personuppgifter som behandlas är korrekta, fullständiga och uppdaterade. För det fall Kommentus behandlar inkorrekta eller ofullständiga personuppgifter ska Kommentus vidta åtgärder för att uppdatera eller rätta personuppgifterna.

4.5 Säkerhet

Kommentus säkerställer genom tekniska och organisatoriska åtgärder att personuppgifter behandlas på ett säkert sätt och Kommentus ska alltid iaktta hög sekretess vad gäller behandling av personuppgifter. Alla former av obehörig eller olaglig tillgång till system som behandlar personuppgifter ska förhindras med lämpliga säkerhetsåtgärder och en tydlig behörighetsstyrning. Inga personuppgifter får förekomma i system som inte kan garantera en lämplig säkerhet avseende behandlingen.

4.6 Transparens

All behandling av personuppgifter som utförs av Kommentus ska vara transparent i förhållande till de registrerade. Denna transparens säkerställs bland annat med klara och tydliga informationstexter till registrerade samt åtgärder för att underlätta för registrerade att utöva sina rättigheter i förhållande till behandlingen av deras personuppgifter (såsom t.ex. rätten till registerutdrag).

4.7 Ansvarsskyldighet

När Kommentus är personuppgiftsansvarig ska Kommentus alltid kunna visa att Kommentus efterlever de grundläggande principerna för behandling av personuppgifter, att Kommentus har en laglig grund för behandlingen och att lämpliga tekniska och organisatoriska åtgärder har vidtagits för att skydda de personuppgifter som Kommentus behandlar samt att krav i Tillämplig dataskyddslagstiftning i övrigt uppfylls.

För att uppfylla kraven i Tillämplig dataskyddslagstiftning är nödvändigt att dokumentation som beskriver vilka åtgärder som vidtagits kontinuerligt uppdateras, samt att det säkerställs att Kommentus register över behandlingar av personuppgifter återspeglar de behandlingar som genomförs i praktiken.

5. LAGLIG GRUND FÖR BEHANDLING AV PERSONUPPGIFTER

När Kommentus behandlar personuppgifter i egenskap av personuppgiftsansvarig ska Kommentus alltid ange vilken laglig grund som tillämpas på behandlingen. Behandling av personuppgifter får inte ske om Kommentus inte kan stödja behandlingen på en laglig grund. Nedanstående lagliga grunder är exempel på lagliga grunder som kan tillämpas när Kommentus behandlar personuppgifter.

5.1 Samtycke

Kommentus kan behandla personuppgifter om den registrerade har samtyckt till behandlingen av personuppgifter. Behandling av personuppgifter ska dock endast ske med stöd av samtycke i den utsträckning ingen annan laglig grund är tillämplig på behandlingen, dvs. Kommentus ska endast förlita sig på samtycke i undantagsfall.

Ett samtycke är giltigt om det är otvetydigt och har lämnats frivilligt av den registrerade, mot bakgrund av klar och tydlig information som säkerställer att den registrerade har förstått samtyckets omfattning. Om samtycke lämnas för flera specifika ändamål måste den registrerade ha möjlighet att välja vilka ändamål som ska omfattas av samtycket, dvs. ett samtycke ska inhämtas till respektive behandling av personuppgifter för ett visst ändamål. Detta innebär således att ett enda samtycke inte ska omfatta flera ändamål. Vidare ska den registrerade alltid ha rätt att återkalla ett lämnat samtycke utan negativa följder, samt att det ska vara lika lätt att återkalla ett samtycke som att lämna samtycket.

Samtycke får inte användas som laglig grund för behandling av personuppgifter i förhållande till anställda eller andra registrerade om det föreligger en tydlig obalans mellan den registrerade och Kommentus, om inte Tillämplig dataskyddslagstiftning uttryckligen anger något annat.

5.2 Nödvändigt för att fullgöra eller ingå ett avtal

Kommentus kan behandla personuppgifter om det är nödvändigt för att fullgöra eller ingå ett avtal med den registrerade. Det ska tilläggas att denna lagliga grund endast är tillämplig på avtal med den registrerade och inte för att fullgöra eller genomföra avtal i allmänhet.

5.3 Nödvändigt för att efterleva en rättslig skyldighet

Kommentus kan behandla personuppgifter om behandlingen är nödvändig för att fullgöra eller efterleva en rättslig skyldighet som åligger Kommentus. En sådan rättslig skyldighet ska vara fastställd i svensk rätt eller EU-rätt för att kunna tillämpas som laglig grund för behandling av personuppgifter.

5.4 Berättigat intresse

Kommentus kan behandla personuppgifter om Kommentus har ett berättigat intresse av att behandla personuppgifterna vilket väger tyngre än den registrerades intresse av att skydda sin personliga integritet i förhållande till behandlingen. Kommentus ska alltid informera den registrerade om det berättigade intresse som Kommentus bedömer väger tyngre än den registrerades integritetsintresse. Om den registrerade motsätter sig Kommentus behandling måste Kommentus kunna påvisa ett tvingande eller övertygande berättigat intresse för att fortsatt ha rätt att behandla personuppgifterna med stöd av en intresseavvägning.

5.5 Behandling av känsliga personuppgifter

Känsliga personuppgifter får behandlas om den registrerade har lämnat sitt samtycke eller om behandlingen uttryckligen är tillåten enligt Tillämplig dataskyddslagstiftning. Vad gäller anställda hos Kommentus får t.ex. känsliga personuppgifter behandlas utan samtycke i den mån det är nödvändigt för att Kommentus ska kunna fullgöra sina skyldigheter inom arbetsrätten, t.ex. för att beräkna lön med hänsyn till sjukfrånvaro eller för att fullgöra rehabiliteringsåtgärder.

5.6 Personuppgifter rörande lagöverträdelser

Om inte Tillämplig dataskyddslagstiftning uttryckligen medger det ska Kommentus inte behandla personuppgifter rörande lagöverträdelser (brottsuppgifter).

6. SÄKERHET OCH INCIDENTHANTERING

6.1 Tekniska och organisatoriska åtgärder

Kommentus ska vidta tekniska och organisatoriska åtgärder för att skydda personuppgifter från olaglig eller oavsiktlig förlust eller förvanskning, samt från otillåten eller olaglig tillgång till personuppgifter. De säkerhetsåtgärder som vidtas ska vara lämpliga med hänsyn till de särskilda risker som är kopplade till en viss behandling av personuppgifter, samt den nivå av känslighet som är kopplad till personuppgifterna. Exempelvis kräver behandling av känsliga personuppgifter en högre grad av säkerhet och kontroll än behandling av personuppgifter i allmänhet.

6.2 Inbyggt dataskydd

Samtliga system som Kommentus använder för att behandla personuppgifter ska vara designade på ett sätt som möjliggör för de registrerade att utöva sina rättigheter enligt Tillämplig dataskyddslagstiftning samt för att säkerställa att personuppgifter behandlas på ett säkert och lagligt sätt. Vidare ska system som behandlar personuppgifter vara utformade för att i standardfallet efterleva de grundläggande principerna för behandling av personuppgifter. Exempelvis ska direkta identifierare (t.ex. personnummer), som inte är absolut nödvändiga för att uppnå ändamålen med behandlingen, pseudonymiseras (t.ex. genom att byta ut personnumret mot ett anställningsnummer).

6.3 Incidenthantering

För det fall en incident leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till personuppgifter som behandlas ska Kommentus så snart Kommentus fått kännedom om incidenten, utreda incidenten. Om det är sannolikt att incidenten innebär en risk för de registrerades fri- och rättigheter i förhållande till behandlingen av personuppgifter, ska Kommentus meddela tillsynsmyndigheten (Datainspektionen) senast inom 72 timmar från att incidenten upptäcktes. Om incidenten innebär en betydande risk för den personliga integriteten hos de registrerade, ska även de registrerade meddelas om incidenten.

I de fall där Kommentus behandlar personuppgifter för någon annans räkning i egenskap av personuppgiftsbiträde ska Kommentus utan dröjsmål (och senast inom den tid som i förekommande fall överenskommits med den personuppgiftsansvarige) meddela den personuppgiftsansvarige som påverkas av incidenten.

Informationssäkerhet och dataskydd är mycket viktigt för Kommentus och för det fall en incident inträffar ska Kommentus vidta åtgärder för att utreda de omständigheter som ligger bakom incidenten och även vidta åtgärder för att avhjälpa de eventuella negativa effekter som incidenten har haft, samt så långt som möjligt säkerställa att en liknande incident inte heller inträffar i framtiden.

7. DE REGISTRERADES RÄTTIGHETER

En viktig del av Kommentus arbete med att efterleva Tillämplig dataskyddslagstiftning, är att alltid iaktta de olika rättigheter som tillkommer registrerade. Kommentus ska därför vidta åtgärder för att ha möjlighet att besvara registrerades begäran avseende följande rättigheter, inbegripet både tekniska och

organisatoriska åtgärder för att säkerställa att det finns rutiner på plats för att hantera en registrerads begäran.

7.1 Rätt till information

Kommentus ska vidta lämpliga åtgärder för att tillhandahålla de registrerade information avseende behandlingen av de registrerades personuppgifter. Informationen ska alltid vara klar och koncis och den ska lämnas på ett klart och tydligt språk.

Kommentus strävar mot att alltid vara transparent i förhållande till de registrerade vad avser behandlingen av de registrerades personuppgifter. Ett viktigt led i detta arbete är att de registrerade erhåller korrekt och tydlig information, så att de registrerade förstår på vilket sätt deras personuppgifter behandlas av Kommentus, samt vilka rättigheter de har i förhållande till behandlingen.

7.2 Rätt till registerutdrag

Utöver rätten till information enligt punkten 7.1 ovan har registrerade rätt att på begäran få del av ytterligare information avseende behandlingen av personuppgifter om den registrerade samt i vissa fall få ett elektroniskt registerutdrag avseende de personuppgifter som Kommentus behandlar. En sådan elektronisk kopia ska tillhandahållas i ett vanligt förekommande format.

Om en registrerads begäran om tillgång är orimlig eller uppenbart ogrundad har Kommentus rätt att, i den utsträckning Tillämplig dataskyddslagstiftning tillåter, ta ut en avgift för att täcka de administrationskostnader som kan vara kopplade till tillhandahållandet av registerutdrag eller vägra att tillmötesgå begäran.

7.3 Rätt till rättelse

De registrerade ska alltid ha rätt att begära rättelse för det fall deras personuppgifter är felaktiga eller ofullständiga och Kommentus ska ha rutiner på plats som möjliggör en sådan rättelse.

7.4 Rätt till radering

Under vissa omständigheter har de registrerade rätt att begära radering av sina personuppgifter. Kommentus ska vid en sådan begäran säkerställa att personuppgifterna blir oåterkalleligt raderade från Kommentus system. Rätt till radering föreligger i följande fall:

(i) personuppgifterna är inte längre nödvändiga för att uppfylla det ändamål för vilket personuppgifterna ursprungligen samlats in;

(ii) den registrerade har återkallat sitt samtycke och Kommentus saknar annan laglig grund för att fortsatt behandla personuppgifterna;

(iii) den registrerade motsätter sig behandling som grundas på en intresseavvägning och Kommentus kan inte uppvisa ett tvingande berättigat intresse som väger tyngre än den registrerades integritetsintresse;

(iv) personuppgifterna har behandlats olagligt;

(v) Kommentus har en rättslig skyldighet att radera personuppgifterna; eller

(vi) personuppgifterna har samlats in från barn inom ramen för ett tillhandahållande av informationssamhällets tjänster.

Rätt till radering ska inte föreligga om Tillämplig dataskyddslagstiftning tillåter att Kommentus inte raderar uppgifterna, t.ex. för att Kommentus ska kunna fastställa, göra gällande eller försvara rättsliga anspråk.

7.5 Rätt till behandlingsbegränsning

Registrerade har under vissa omständigheter rätt att begära begränsning av behandlingen av deras personuppgifter. Detta innebär att Kommentus ska ha tekniska möjligheter att markera eller flagga personuppgifter som begränsade i syfte att säkerställa att personuppgifterna inte är föremål för vidare behandling (annat än att endast lagras i Kommentus system), om inte den registrerade samtycker till vidare behandling.

7.6 Rätt till dataportabilitet

För det fall den registrerade själv har tillhandahållit personuppgifterna till Kommentus och behandlingen grundas på (i) den registrerades samtycke, eller (ii) att behandlingen är nödvändig för att fullgöra eller ingå ett avtal med den registrerade, ska den registrerade ha rätt att erhålla sådana personuppgifter i ett vanligt förekommande, strukturerat och maskinläsbart format, samt ha rätt att överföra sådana personuppgifter till en annan personuppgiftsansvarig.

Om det är tekniskt möjligt ska Kommentus på den registrerades begäran föra över personuppgifterna direkt till en annan personuppgiftsansvarig.

7.7 Rätt att motsätta sig behandling

Den registrerade ska ha rätt att motsätta sig behandlingen av personuppgifter, mot bakgrund av skäl hänförliga till hans eller hennes specifika situation, om behandlingen grundas på en intresseavvägning eller om behandlingen sker för direktmarknadsföringsändamål.

För det fall en registrerad motsätter sig behandling som grundas på en intresseavvägning ska Kommentus påvisa för den registrerade att Kommentus har ett tvingande eller övertygande berättigat intresse av att behandla personuppgifterna trots att den registrerade har motsatt sig behandlingen. Om Kommentus inte kan påvisa ett sådant berättigat intresse måste behandlingen upphöra.

8. ÖVERFÖRING AV PERSONUPPGIFTER

8.1 Överföring till andra personuppgiftsansvariga

Om Kommentus för över personuppgifter till en annan personuppgiftsansvarig ska Kommentus genom avtal säkerställa att den personuppgiftsansvarige som tar emot personuppgifterna följer de tillämpliga lagar som gäller i det land där den mottagande personuppgiftsansvarige finns.

Kommentus ska även säkerställa att de registrerade får information om att deras personuppgifter kan komma att lämnas ut till andra personuppgiftsansvariga.

8.2 Överföring till personuppgiftsbiträden

Kommentus anlitar externa tjänsteleverantörer i flertalet fall som, direkt eller indirekt, kan komma att behandla personuppgifter för Kommentus räkning (personuppgiftsbiträden). Kommentus ska endast anlita personuppgiftsbiträden som kan ge tillräckliga garantier för att de efterlever de krav som ställs i Tillämplig dataskyddslagstiftning, bland annat avseende säkerhet.

För att säkerställa att anlitandet av personuppgiftsbiträden följer Tillämplig dataskyddslagstiftning ska Kommentus alltid ingå personuppgiftsbiträdesavtal med personuppgiftbiträdet, vilket ska uppfylla de krav som ställs på personuppgiftsbiträdesavtal i Tillämplig dataskyddslagstiftning. Kommentus ska, om tillämpligt, i första hand använda sin egen mall för personuppgiftsbiträdesavtal.

8.3 Överföringar utanför EU/EES

Om Kommentus för över personuppgifter till en mottagare som återfinns utanför EU/EES, ska Kommentus säkerställa att samtliga krav som ställs i Tillämplig dataskyddslagstiftning efterlevs. Detta inkluderar att säkerställa att lämpliga skyddsåtgärder finns på plats, t.ex. genom att ingå Europeiska Kommissionens standardavtalsklausuler (eller motsvarande från tid till annan gällande ramverk) med mottagande part.

9. STYRNING OCH REGELEFTERLEVNAD

Kommentus ska ha interna rutiner för att säkerställa att dessa Riktlinjer samt Tillämplig dataskyddslagstiftning efterlevs.

Kommentus ska säkerställa att samtliga medarbetare är medvetna om vikten av att skydda personuppgifter och ska därför bl.a. anordna utbildningstillfällen, t.ex. genom e-learningverktyg, där medarbetare utbildas i personuppgiftsrelaterade frågor. Utbildning av nyanställda ska vara en del av Kommentus introduktionsprogram. Alla utbildningstillfällen dokumenteras av Kommentus så att Kommentus kan följa upp vilka medarbetare som har genomgått respektive utbildning.

Kommentus anställda ska vidare hålla sig uppdaterade vad gäller alla policys och riktlinjer avseende behandling av personuppgifter som Kommentus från tid till annan fastställer.

Chefsjurist Åsa Edman är ansvarig för innehåll och förvaltning av dessa riktlinjer. Dessa riktlinjer är beslutade av SKL Kommentus ledningsgrupp den 23 maj 2018.