Kommentarer till SKL-koncernens Personuppgiftsbiträdesavtal

Innehållsförteckning

1. Bakgrund och syfte

SKL, SKL Kommentus och Inera har gemensamt tagit fram ett personuppgiftsbiträdesavtal (”PUB-avtalet”). Avtalets syfte är att säkerställa registrerades fri- och rättigheter enligt Allmänna Dataskyddsförordningen, EU 2016/679, (dataskyddsförordningen), artikel 28.3.

PUB-avtalet ska även vara ett neutralt och kvalitetssäkrat instrument som enskilda kommuner och regioner såväl som SKL, SKL Kommentus och Inera kan använda för att reglera behandlingen av personuppgifter mellan en personuppgiftsansvarig och ett personuppgiftsbiträde.

2. Om kommentaren

Denna kommentar förklarar innebörden av vissa rättigheter och skyldigheter i PUB-avtalet och i vilka situationer dessa aktualiseras. Vägledningen innehåller även exempel på ytterligare avtalsreglering som PUB-avtalet kan behöva kompletteras med när det används.

3. När behövs ett personuppgiftsbiträdesavtal?

Ett personuppgiftsbiträdesavtal behövs när ett personuppgiftsbiträde behandlar personuppgifter för en personuppgiftsansvarigs räkning. Innan personuppgiftsbiträdesavtal tecknas behöver det därför klarläggas om det förhållande som ska regleras över huvud taget innebär att någon part behandlar personuppgifter, och att det görs för den andra partens räkning.

Det är den personuppgiftsansvarige som bestämmer ändamålen med och medlen för behandlingen, och den som ger personuppgiftsbiträdet instruktioner för behandlingen. En uppdragstagare som ensam bestämmer över personuppgifternas ändamål och hantering kan i stället rättsligt sett anses ha ett eget personuppgiftsansvar, dvs. vara personuppgiftsansvarig för aktuell behandling.

Det är därför varken möjligt eller lämpligt att enbart avtala att en part ska vara personuppgiftsansvarig och en annan ska vara personuppgiftsbiträde. I stället behöver en funktionell bedömning göras av vilken roll avtalsparterna har inför varje behandling av personuppgifter.[1]

Att inte använda ett personuppgiftsbiträdesavtal när ett sådant behövs, eller att använda ett som inte uppfyller dataskyddsförordningens krav på innehåll, kan ge upphov till onödiga risker för både beställare och leverantör.

[1] Se Artikel 29-arbetsgruppens vägledning 1/2010 om personuppgiftsansvarig och personuppgiftsbiträde, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

4. Hur används PUB-avtalet?

Tanken är att SKL-koncernens avtal ska kunna användas vid alla tillfällen som det behövs ett personuppgiftsbiträdesavtal. Det huvudsakliga tillkommande arbetet med PUB-avtalet utgörs av kompletteringar av instruktionerna och listan över underbiträden (se separata mallar). Tanken är alltså att PUB-avtalet inte ska ändras. Komplettering på grund av behandlingens särskilda karaktär ska göras i instruktionerna.[2]

Av dataskyddsförordningen framgår att bl.a. föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade ska anges i det avtal som reglerar personuppgiftsbiträdets behandling (artikel 28.3).

Dessa uppgifter behöver inte nödvändigtvis anges i PUB-avtalet utan kan framgå av andra avtalsdokument, bara de är urskiljbara från andra avtalsvillkor (se t.ex. Datainspektionens beslut 2014-06-09, dnr 1822-13). Mallen för instruktioner innehåller fält för sådana uppgifter som är obligatoriska enligt dataskyddförordningen.

[2] Se ”Mall för den Personuppgiftsansvariges Instruktion för Behandling av Personuppgifter" och ”Mall för lista över underbiträden”.

5. Kommentarer till vissa punkter i PUB-avtalet

Numreringen för respektive punkt i detta avsnitt har motsvarande numrering i PUB-avtalet. Alla punkter har inte kommenterats. För det fall frågor uppstår kring någon okommenterad punkt går det bra att höra av sig till SKL, Inera eller SKL Kommentus.

1. PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

PUB-avtalet ska kompletteras med de uppgifter som framgår av fälten, t.ex. vilken roll parterna har (personuppgiftsansvarig eller personuppgiftsbiträde) samt kontaktpersoner.

2. DEFINITIONER

I PUB-avtalet används termen ”Dataskyddslagstiftning”. Av termens definition framgår att detta avser all integritets- och personuppgiftslagstiftning, samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter), som är tillämplig på den personuppgiftsbehandling som sker enligt detta PUB-avtal, inklusive nationell sådan lagstiftning och EU-lagstiftning.

Personuppgiftsbiträdet ska ge tillräckliga garantier för skyddet av den personuppgifts-ansvariges personuppgifter, i synnerhet genom ”sakkunskap” (skäl 81 i dataskyddsför-ordningen) och besitta nödvändiga kunskaper om tillämpliga författningar på data-skyddsområdet för den aktuella behandlingen av personuppgifter.

Den personuppgiftsansvarige rekommenderas dock att i mallen för instruktioner närmare ange vilka registerförfattningar som leverantören ska iaktta i syfte undvika missförstånd och underlätta biträdets allokering av resurser på tillämplig reglering.

3.2 PUB-avtalet utgör ett självständigt avtal om Behandlingen. När PUB-avtalet utgör ett av flera avtalsdokument inom ramen för ett annat avtal benämns det andra avtalet ”Huvudavtalet” i PUB-avtalet.

Av huvudavtalet bör framgå hur PUB-avtalet och andra dataskyddsrelaterade handlingar, till exempel instruktioner, förhåller sig till övriga avtalsdokument. Under en särskild rubrik (exempelvis ”Handlingarnas inbördes ordning”) slår parterna fast hur avtalsdokumenten ska förhålla sig till varandra om de skulle behöva tolkas.

> *3.3 För det fall något av det som stadgas i kap. 1, 16, 17, 18.2, 19 – 22 i PUB-avtalet regleras på annat sätt i Huvudavtalet ska Huvudavtalets reglering ha företräde.*

Denna bestämmelse öppnar för parterna att komma överens om andra villkor i angivna kapitel och punkter. Lägg märke till att parterna inte äger rätt att ändra övriga kapitel och punkter i PUB-avtalet.

4. BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION

4.1 Den Personuppgiftsansvarige utser härmed Personuppgiftsbiträdet att utföra Behandlingen för den Personuppgiftsansvariges räkning enligt vad som stadgas i detta PUB-avtal.

När personuppgifter behandlas av ett personuppgiftsbiträde ska, enligt artikel 28.3 i dataskyddsförordningen, hanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige.

Regleringen under rubrik 4 innehåller det övergripandet mandatet för personuppgifts-biträdet att för den personuppgiftsansvariges räkning behandla dennes personuppgifter och att det ska ske i enlighet med föreliggande personuppgiftsbiträdesavtal.

4.2 Den Personuppgiftsansvarige ska ge Instruktioner till Personuppgiftsbiträdet om hur det ska utföra Behandlingen.

I avtalet eller rättsakten ska föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade samt den personuppgiftsansvariges skyldigheter och rättigheter anges. Detta följer av artikel 28.3 i dataskyddsförordningen. Dessa obligatoriska uppgifter framgår inte av personupp-giftsbiträdesavtalet utan ska framgå av instruktionerna till biträdet. Angivande av dessa uppgifter kan ske i SKL-koncernens Mall för den Personuppgiftsansvariges Instruktion för Behandling av Personuppgifter eller i den personuppgiftsansvariges egna mall för instruktioner. Flera punkter i instruktionerna kan med fördel användas som underlag för Personuppgiftsansvariges registerförteckning så det är klokt att försöka använda samma typ av terminologi och formuleringar som återfinns där.

Skälet till att instruktionerna inte framgår direkt av PUB-avtalet är att avtalets standardutförande då inte skulle kunna behållas. Instruktionerna är en icke-generisk del av PUB-avtalet (eller huvudavtalet; se nästa stycke) som lämpligen kan innehålla dokumenterade omständigheter och instruktioner som är unika för den specifika behandlingen som PUB-avtalet reglerar, t.ex. föremålet för behandlingen och behandlingens varaktighet (med mera).

Det finns inga hinder mot att låta instruktionerna, liksom PUB-avtalet, ingå som bilagor till ett huvudavtal. I sådana fall ska emellertid PUB-avtalet och instruktionerna vara ”urskiljbara” från övriga villkor som gäller mellan parterna enligt huvudavtalet (se t.ex. Datainspektionens beslut 2014-06-09, dnr 1822-13).

4.3 Personuppgiftsbiträdet får endast utföra Behandlingen i enlighet med PUB-avtalet och vid var tid gällande Instruktioner.

Bestämmelsen i punkt 4.3 bygger på kravet i artikel 28.1 a att personuppgiftsbiträdet endast får behandla personuppgifter enligt dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet överföringar av personuppgifter till ett tredje land eller en internationell organisation, såvida inte behandlingen krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgiftsbiträdet omfattas av. I sådana fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt unionsrätten eller enligt en medlemsstats nationella rätt.

5. DEN PERSONUPPGIFTSANSVARIGES ANSVAR

5.1 Den Personuppgiftsansvarige ansvarar för att det vid var tid finns laglig grund för Behandlingen och för att utforma korrekta Instruktioner så att Personuppgiftsbiträdet och Underbiträdet kan fullgöra sitt eller sina uppdrag enligt detta PUB-avtal och Huvudavtal i förekommande fall.

All behandling av personuppgifter kräver en rättslig grund. Annars är det inte en tillåten behandling. De rättsliga grunderna för behandling av personuppgifter finns i artikel 6.1 i dataskyddsförordningen. Det är den personuppgiftsansvarige som ansvarar för lagenligheten i personuppgiftsbehandlingen, s.k. ansvarsskyldighet (se artikel 5.2).

Personuppgiftsbiträdet bär ett ansvar för att skydda personuppgifter enligt artikel 32 i dataskyddsförordningen. Om det ansvaret omfattar även laglighetsfrågor är oklart i nuläget. Bedömer personuppgiftsbiträdet att behandlingen saknar rättsligt stöd har denne åtminstone en skyldighet enligt personuppgiftsbiträdesavtalet att uppmärksamma den personuppgiftsansvarige på förhållandet och be om kompletterande instruktioner. Det framgår av punkten 6.5 i personuppgiftsbiträdesavtalet.

5.2 Den Personuppgiftsansvarige ska utan onödigt dröjsmål informera Personuppgiftsbiträdet om förändringar i Behandlingen vilka påverkar Personuppgiftsbiträdets skyldigheter enligt Dataskyddslagstiftningen.

Ändrade organisatoriska eller administrativa förhållanden hos personuppgiftsansvarige vilka påverkar personuppgiftsbiträdets skyldigheter ska utan onödigt dröjsmål meddelas denne. Det kan t.ex. röra sig om ändrade ansvarsförhållanden utifrån omorganisation, förändrade roller och ansvar, byte av IT-system eller ändrade arbetssätt som påverkar personuppgiftsbiträdets åtagande.

5.3 Den Personuppgiftsansvarige ansvarar för att informera Registrerade om Behandlingen och för att tillvarata Registrerades rättigheter enligt Dataskyddslagstiftningen samt vidta varje annan åtgärd som åligger den Personuppgiftsansvarige enligt Dataskyddslagstiftningen.

Enligt dataskyddsförordningen ansvarar den personuppgiftsansvarige för att informera den registrerade om behandlingen av personuppgifter eller om något undantag från informationsskyldigheten är tillämplig (se artikel 12 – 14). Den personuppgiftsansvarige ansvarar vidare för att tillvarata registrerades rättigheter. Personuppgiftsbiträdet har emellertid enligt PUB-avtalet en skyldighet att stödja den personuppgiftsansvarige i handläggningen av rättigheter, se punkten 6.4. Det följer direkt av, artikel 28.3 f i dataskyddsförordningen.

6. PERSONUPPGIFTSBITRÄDETS ANSVAR

6.1 Personuppgiftsbiträdet förbinder sig att endast utföra Behandlingen i enlighet med PUB-avtalet och Instruktioner samt att följa Dataskyddslagstiftningen. Personuppgiftsbiträdet förbinder sig även att fortlöpande hålla sig informerad om gällande rätt på området.

Bestämmelsen i punkten 6.1 erinrar personuppgiftsbiträdet om att endast utföra behandlingen av personuppgifter inom ramen för avtalets villkor samt dokumenterade instruktioner. Den tydliggör också att instruktionerna uttryckligen måste tillåta om personuppgiftsbiträdet ska ha rätt att använda uppgifterna till andra eller egna syften och ändamål.

Personuppgiftsbiträdet har vidare ett flertal skyldigheter enligt dataskyddsförordningen, bl.a. att skydda personuppgifter (artikel 32), hålla en registerförteckning (artikel 30.2), och hjälpa den personuppgiftsansvarige att fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter i enlighet med kapitel III (artikel 28.3 e). Personuppgiftsbiträdet ska också utge skadestånd till registrerade och ansvara för skada uppkommen till följd av behandlingen om denne inte har fullgjort de skyldigheter i dataskyddsförordningen som specifikt riktar sig till personuppgiftsbiträden eller agerat utanför eller i strid med den personuppgiftsansvariges lagenliga anvisningar (artikel 82.2).

6.2 Personuppgiftsbiträdet ska vidta åtgärder för att skydda Personuppgifterna mot alla slag av Behandlingar som inte är förenliga med PUB-avtalet, Instruktioner och Dataskyddslagstiftningen.

Se kommentaren under punkten 5.1.

6.3 Personuppgiftsbiträdet åtar sig säkerställa att samtliga fysiska personer som arbetar under dess ledning följer PUB-avtalet och Instruktioner samt att de fysiska personerna informeras om relevant lagstiftning.

Personuppgiftsbiträdet ansvarar enligt punkten 6.3 själv för att anställda och osjälvständiga uppdragstagare (medarbetare) är informerade om biträdets skyldigheter enligt PUB-avtalet och tillhörande instruktioner. Det är personuppgiftsbiträdet som ansvarar för eventuella fel

som dessa begår.

> *6.4 Personuppgiftsbiträdet ska på begäran från den Personuppgiftsansvarige bistå denne med att säkerställa att skyldigheterna enligt Dataskyddsförordningen, artikel 32-36, fullgörs och svara på begäran om utövande av den Registrerades rättigheter i enlighet med Dataskyddsförordningen, kap. III, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå.*

Bestämmelsen i punkten 6.4 är en direkt följd av dataskyddsförordningen, artikel 28.3 e. Huruvida personuppgiftsbiträdet ska kunna erhålla ersättning för att bistå den personuppgiftsansvarige är en fråga att överväga vid planeringen av en upphandling av en specifik tjänst alternativt uppmärksammas av leverantören vid anbudsgivningen. Dataskyddsförordningen reglerar ingen sådan rättighet för personuppgiftsbiträdet. Å andra sidan kan vissa rättigheter kräva omfattande arbete av biträdet för att tillmötesgå den registrerades rättigheter, till exempel registerutdrag.

> *6.5 För det fall att Personuppgiftsbiträdet finner att Instruktioner är otydliga, i strid med Dataskyddslagstiftningen eller saknas och Personuppgiftsbiträdet bedömer att nya eller kompletterande Instruktioner är nödvändiga för att genomföra sina åtaganden ska Personuppgiftsbiträdet utan dröjsmål informera den Personuppgiftsansvarige, tillfälligt upphöra med Behandlingen och invänta nya Instruktioner.*

Situationen kan vanligtvis uppkomma vid ändrade organisatoriska eller administrativa förhållanden hos den personuppgiftsansvarige. Skulle situationen uppstå ska personuppgiftsbiträdet utan dröjsmål informera den personuppgiftsansvarige och tillfälligt upphöra med behandlingen. Skälet är att minimera eventuell skada som skulle kunna förvärras om behandlingen fortsatte efter underrättelsen. Begäran från biträdet om nya eller kompletterande instruktioner ska hanteras skyndsamt av den personuppgiftsansvarige. Instruktionerna ska meddelas skriftligen, t.ex. per e-post, och kan formaliseras i efterhand genom utfärdande av en ny instruktion eller en kompletterande bilaga till PUB-avtalet eller huvudavtalet.

> *6.6 För det fall att den Personuppgiftsansvarige förser Personuppgiftsbiträdet med nya eller ändrade Instruktioner ska Personuppgiftsbiträdet, utan onödigt dröjsmål från mottagandet, meddela den Personuppgiftsansvarige huruvida genomförandet av de nya Instruktionerna föranleder förändrade kostnader för Personuppgiftsbiträdet.*

PUB-avtalet reglerar inte kostnader för personuppgiftsbiträdets behandling av den personuppgiftsansvariges personuppgifter. Det förväntas att parterna reglerar priser och andra ersättningsanspråk i huvudavtalet. Motsvarande gäller om den personuppgiftsansvarige meddelar nya eller ändrade instruktioner som medför högre kostnader för personuppgiftsbiträdet än vad som avtalats i samband med upphandlingen av en tjänst. Personuppgiftsbiträdet ska påtala sina kostnadsanspråk snarast. Specifika tidsbegränsningar

bör anges i huvudavtalet. Tidsbegränsningar på över ett år kan inte anses vara rimliga.

Syftet är att inleda en dialog om eventuella kostnadsökningar för biträdet i samband med ändrade förutsättningar. Resulterar dialogen i att parterna inte kan komma överens har biträdet med stöd av punkten 16.1 rätt att säga upp PUB-avtalet med trettio dagars varsel.

Enligt punkten 7.3 i PUB-avtalet utgör tillkommande eller ändrade krav på skyddsåtgärder från den personuppgiftsansvarige, efter parternas tecknande av avtalet, alltid nya Instruktioner enligt avtalet.

7. SÄKERHETSÅTGÄRDER

7.1 Personuppgiftsbiträdet ska vidta alla tekniska och organisatoriska säkerhetsåtgärder som krävs för att förhindra Personuppgiftsincidenter, genom att säkerställa att Behandlingen uppfyller kraven i Dataskyddsförordningen och att den Registrerades rättigheter skyddas.

Punkten 7.1 är en erinran till personuppgiftsbiträdet om skyldigheten enligt artikel 28.3 c i dataskyddsförordningen att bistå den personuppgiftsansvarige med att se till att vidta alla åtgärder som krävs enligt artikel 32. I artikel 32 finns den övergripande skyldigheten för både personuppgiftsansvariga och personuppgiftsbiträden att skydda personuppgifter och därmed undvika personuppgiftsincidenter.

7.2 Personuppgiftsbiträdet ska fortlöpande säkerställa att den tekniska och organisatoriska säkerheten i samband med Behandlingen medför en lämplig nivå av konfidentialitet, integritet, tillgänglighet och motståndskraft.

Punkten 7.2 är en erinran till personuppgiftsbiträdet om skyldigheten enligt artikel 28.3c i dataskyddsförordningen att bistå den personuppgiftsansvarige med att se till att vidta alla åtgärder som krävs enligt artikel 32. Av artikel 32.1 framgår bland annat att personuppgiftsbiträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt […] förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft i tjänsterna som omfattas av personuppgiftsbehandlingen.

7.3 Eventuella tillkommande eller ändrade krav på skyddsåtgärder från den Personuppgiftsansvarige, efter parternas tecknande av PUB-avtalet, ska betraktas som nya Instruktioner enligt PUB-avtalet.

Se kommentaren under punkt 6.6

7.4 Personuppgiftbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till Personuppgifterna för sådana fysiska personer som arbetar under Person-

uppgiftsbiträdets ledning och som behöver åtkomsten för att kunna utföra sina arbetsuppgifter.

Personuppgiftsbiträdets personal kan i vissa situationer behöva åtkomst till den personuppgiftsansvariges personuppgifter för att till exempel utföra felsökning eller support. Rätten till sådan åtkomst ska framgå av den skriftliga instruktionen. Åtkomst som inte är uttryckligen tillåten ska betraktas som otillåten. Vem som får ha tillgång till vilken information kan till exempel framgå av registerförfattningar. Punkten avser personal som arbetar under personuppgiftsbiträdets ”direkta ansvar”. I artikel 4.10 i dataskyddsförordningen talas om personer som under den personuppgiftsansvariges respektive personuppgiftsbiträdets direkta ansvar har befogenhet att behandla personuppgifter.

7.5 Personuppgiftsbiträdet åtar sig att kontinuerligt Logga åtkomst till Personuppgifterna enligt PUB-avtalet i den utsträckning det krävs enligt Instruktionen. Loggar får gallras först fem (5) år efter Loggningstillfället om inte annat anges i Instruktionen. Loggar ska omfattas av erforderliga skyddsåtgärder, i enlighet med Dataskyddslagstiftningen.

Denna punkt i PUB-avtalet förutsätter förtydliganden i den skriftliga instruktionen. Som exempel kan instruktionen ställa krav på att personuppgiftsbiträdet ska logga hur personuppgifter hanteras, vilka uppgifter som ska loggas, när användare hos den personuppgiftsansvarige och personuppgiftsbiträdet tar del av personuppgifter, datum och klockslag för olika händelser som ska loggas med mera.

Kravet på bevarande av personuppgifter i fem år är hämtat från Socialstyrelsens föreskrifter och allmänna råd (HSFL-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården där det ställs krav på vårdgivare att bevara åtkomstloggar minst fem år. Inget hindrar dock att den personuppgiftsansvarige i samråd med personuppgiftsbiträdet ändrar bevarandetiden i den skriftliga instruktionen och markerar att den tiden gäller i stället för bevarandetiden i punkt 7.5.

7.6 Personuppgiftsbiträdet ska systematiskt testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa Behandlingens säkerhet .

Punkten 7.6 säkerställer att personuppgiftsbiträdet enligt artikel 28.3 c i dataskydds-förordningen är skyldig att bistå den personuppgiftsansvarige med att se till att vidta alla åtgärder som krävs enligt artikel 32. Av artikel 32.2 framgår att bl.a. att person-uppgiftsbiträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt […] ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet. Ett annat ord för detta är penetrationstester.

8. SEKRETESS/TYSTNADSPLIKT

8.1 Personuppgiftsbiträdet och samtliga fysiska personer som arbetar under dess ledning ska vid Behandlingen iaktta såväl sekretess som tystnadsplikt. Personuppgifterna får inte nyttjas eller spridas för andra ändamål, vare sig direkt eller indirekt, såvida inte annat avtalats.

Av artikel 28 3 b) i dataskyddsförordningen framgår att personer med behörighet att behandla personuppgifterna ska ha åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

Bestämmelsen ska säkerställa att personuppgiftsbiträdet och samtliga fysiska personer som arbetar under dess ledning ska iaktta såväl sekretess som tystnadsplikt vid behandlingen. Omfattas uppgifterna av offentlighets- och sekretesslagen (2009:400) (OSL) är de känsliga och omfattas av sekretess. Detta ställer särskilda krav på personuppgiftsbiträdets skydd av uppgifterna i form av kryptering, rutiner för åtkomst, kontroller vid verkställighet av beslut om utlämnande till tredje part och loggning som ska framgå av instruktionen.

PUB-avtalet i sig innefattar en tystnadsplikt, liksom krav på individuella sekretessförbindelser av det slag som framgår av punkten 8.2. Det är verktyg för att skydda sekretessbelagda uppgifter för obehörigt röjande eller otillåten behandling, givet att tystnadsplikten är förenad med kännbara skadestånd eller viten.

Tydliga instruktioner om dataskydd utgör vidare en viktig del av den personuppgifts-ansvariges skydd av och kontroll över uppgifterna, till exempel förbud för personupp-giftsbiträdets personal att genom direktåtkomst ta del av den personuppgiftsansvariges uppgifter. Brott mot sådana instruktioner kan aktualisera brotten dataintrång eller trolöshet mot huvudman för biträdets personal.

För att ytterligare skydda uppgifterna och utöva kontroll över dem kan andra åtgärder vidtas som gör det mer eller mindre omöjligt för leverantören att faktiskt ta del av dessa. En sådan åtgärd är att uppgifterna lagras krypterade eller pseudonymiserade så att personuppgiftsbiträdet inte har åtkomst till dem, förutsatt att den personuppgiftsansvarige förfogar över kryptonyckeln.

> *8.2 Personuppgiftsbiträdet ska tillse att samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen, är bundna av sekretessförbindelse avseende Behandlingen. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag. Personuppgiftsbiträdet åtar sig även att tillse att det finns sekretessavtal med Underbiträdet samt sekretessförbindelser mellan Underbiträdet och samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen.*

Enligt artikel 32.4 i dataskyddsförordningen ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den

personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger den fysiska personen att göra det.

Punkten 8.2 säkerställer kravet på sekretess/tystnadsplikt och konkretiseras genom avtal med biträdet om sekretessförbindelser.

I vissa fall omfattas personuppgiftsbiträdet av en lagstadgad tystnadsplikt. Ett exempel på sådan tystnadsplikt finns i lagen (1997:736) om färdtjänst. Enligt 15 § i denna lag får personer som är eller har varit verksamma inom enskild verksamhet som bedrivs yrkesmässigt och som omfattas av denna lag inte obehörigen röja vad de i verksamheten fått veta om någons personliga förhållanden. Tystnadsplikten kombineras med en sekretessbrytande bestämmelse så att socialtjänsten och vårdgivare kan röja uppgifter om hälsa för färdtjänstchauffören.

Även auktoriserade tolkar och översättare omfattas av en lagstadgad tystnadsplikt, se lagen (1975:689) om tystnadsplikt för vissa tolkar och översättare. Brott mot lagstadgad tystnadsplikt är straffbart och förenad med böter eller fängelse som påföljd.

> *8.3 Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarige om eventuella kontakter med tillsynsmyndighet avseende Behandlingen. Personuppgiftsbiträdet har inte rätt att företräda den Personuppgiftsansvarige eller agera för den Personuppgiftsansvariges räkning gentemot tillsynsmyndigheter i frågor avseende Behandlingen.*

Enligt artikel 29 i dataskyddsförordningen gäller att personuppgiftsbiträdet och personer som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende och som får tillgång till personuppgifter, endast får behandla dessa på instruktion från den personuppgiftsansvarige, såvida han eller hon inte är skyldig att göra det enligt unionsrätten eller medlemsstaternas nationella rätt.

Punkten 8.3 ska säkerställa att personuppgiftsbiträdet skyndsamt ska underrätta personuppgiftsansvarig om kontakter med tillsynsmyndigheten och ska invänta instruktioner samt att biträdet inte företräder den personuppgiftsansvarig mot tillsynsmyndigheten.

Personuppgiftsbiträdet ska endast bistå med informationsförmedling angående behandlingen till tillsynsmyndigheten efter instruktion eller enligt lagkrav.

> *8.4 Om den Registrerade, tillsynsmyndighet eller tredje man begär information från Personuppgiftsbiträdet vilken rör Behandlingen, ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige om saken. Information om Behandlingen får inte lämnas till den Registrerade, tillsynsmyndighet eller tredje man utan skriftligt medgivande från den Personuppgiftsansvarige, såvida det inte framgår av tvingande lag att information ska lämnas. Personuppgiftsbiträdet ska bistå med förmedling av den informationen som omfattas av ett medgivande eller lagkrav.*

Punkten 8.4 säkerställer att personuppgiftsbiträdet ska underrätta personuppgiftsansvarig om kontakter med tillsynsmyndigheten eller tredje man. Personuppgiftsbiträdet ska endast bistå med informationsförmedling angående Behandlingen till tillsynsmyndigheten efter instruktion eller enligt lagkrav.

9. GRANSKNING, TILLSYN OCH REVISION

9.1 Personuppgiftsbiträdet ska utan onödigt dröjsmål, på den Personuppgiftsansvariges begäran, tillhandahålla den information om tekniska och organisatoriska säkerhetsåtgärder som den Personuppgiftsansvarige behöver för att kunna fastställa att Personuppgiftsbiträdet uppfyller sina åtaganden enligt PUB-avtalet och Dataskyddsförordningen, artikel 28.3 h.

Punkten 9.1 säkerställer att personuppgiftsbiträdet på lämpligt sätt ska tillhandahålla information till personuppgiftsansvarig, som visar att denne lever upp till den person-uppgiftsansvariges krav på behandlingen och vidtar alla lämpliga tekniska och organisatoriska säkerhetsåtgärder som krävs enligt dataskyddsförordningen och PUB-avtalet. På så sätt behöver den personuppgiftsansvarige inte ta i anspråk den ingripande rätten till inspektioner enligt artikel 28.3 h.

Punkterna 9.1 – 9.3 utgör en eskaleringstrappa som den personuppgiftsansvarige förfogar över för att utöva kontroll över personuppgiftsbiträdets behandling. Den erbjuder också biträdet en möjlighet att förse den personuppgiftsansvarige med information som ger tillräcklig insyn i skyddet av personuppgifter så att rätten till mer ingripande åtgärder, såsom inspektion, aldrig behöver aktualiseras.

Notera att personuppgiftsbiträdet ska kunna ge ”tillräckliga garantier” för skyddet av personuppgifter enligt artikel 28.1 i dataskyddsförordningen genom lämpliga tekniska och organisatoriska åtgärder.

9.2 Personuppgiftsbiträdet åtar sig att minst en (1) gång om året granska säkerheten avseende Behandlingen genom en egenkontroll för att säkerställa att Behandlingen följer PUB-avtalet. Resultatet av sådan egenkontroll ska på begäran delges den Personuppgiftsansvarige.

Punkt 9.2 möjliggör för personuppgiftsbiträdet att använda egenkontroll som metod för att visa för den personuppgiftsansvarige att behandling uppfyller kraven enligt PUB-avtalet och dataskyddsförordningen, artikel 28.3 h. Egenkontroll innebär i detta fall en årlig revision av informationssäkerheten som dokumenteras. Exempel de uppföljningar av informationssäkerheten som gjorts och som är av större betydelse, de riskanalyser som har gjorts, de åtgärder som har vidtagits för förbättring av informationssäkerheten och som är av större betydelse samt den utvärdering personuppgiftsbiträdet har genomfört av skydd mot olovlig åtkomst, såväl intern som extern, till datornätverk och informationssystem.

9.3 Den Personuppgiftsansvarige äger rätt att, själv eller genom annan av denne utsedd tredje part (som inte får vara en konkurrent till Personuppgiftsbiträdet), följa upp att Personuppgiftsbiträdet uppfyller PUB-avtalets, Instruktionernas och Dataskyddslagstiftningens krav. Personuppgiftsbiträdet ska vid sådan granskning bistå den Personuppgiftsansvarige, eller den som utför granskningen i den Personuppgiftsansvariges ställe, med dokumentation, tillgång till lokaler, IT-system och andra tillgångar som behövs för att kunna granska Personuppgiftsbiträdets efterlevnad av PUB-avtalet, Instruktioner och Dataskyddslagstiftningen. Den Personuppgiftsansvarige ska säkerställa att personal som genomför granskningen är underkastade sekretess eller tystnadsplikt enligt lag eller avtal.

Punkt 9.3 säkerställer att den personuppgiftsansvarige ska ha möjlighet att följa upp att personuppgiftsbiträden lever upp till den personuppgiftsansvariges krav på personuppgiftsbehandlingen enligt artikel 28.3 c och artikel 32 i dataskyddsförordningen. Den personuppgiftsansvarige ska ges tillgång till all information som krävs för att visa att skyldigheterna enligt artikel 28.3 h har fullgjorts samt bidra till granskningar, inbegripet inspektioner. Dessa kan genomföras av den personuppgiftsansvarige själv eller av en revisor eller granskningsperson som bemyndigats av den personuppgiftsansvarige.

9.4 Personuppgiftsbiträdet äger alternativt till vad som stadgas i punkterna 9.2-9.3, rätt att erbjuda andra tillvägagångssätt för granskning av Behandlingen, exempelvis granskning genomförd av oberoende tredje part. Den Personuppgiftsansvarige ska i sådant fall äga rätt, men inte skyldighet, att tillämpa detta alternativa tillvägagångssätt för granskning. Vid sådan granskning ska Personuppgiftsbiträdet ge den Personuppgiftsansvarige eller en tredje part den assistans som behövs för utförandet av granskningen.

Punkt 9.4 möjliggör att granskningen av personuppgiftsbiträdet genomförs på ett alternativt sätt, t.ex. av en oberoende tredje part.

9.5 Personuppgiftbiträdet ska bereda tillsynsmyndighet, eller annan myndighet som har laglig rätt till det, möjlighet att göra tillsyn enligt myndighetens begäran i enlighet med vid var tid gällande lagstiftning, även om sådan tillsyn annars skulle stå i strid med bestämmelserna i PUB-avtalet

Punkt 9.5 säkerställer att personuppgiftsbiträdet även ska bereda tillsynsmyndigheten möjligheten att genomföra sådan granskning som denne har laglig rätt att utföra.

9.6 Personuppgiftsbiträdet ska tillförsäkra den Personuppgiftsansvarige rättigheter gentemot Underbiträdet vilka motsvarar den Personuppgiftsansvariges samtliga rättigheter gentemot Personuppgiftsbiträdet enligt kap. 9 i PUB-avtalet.

Punkt 9.6 säkerställer personuppgiftsbiträdets ansvar för kraven enligt artikel 28.3 för sina underbiträden. Personuppgiftsbiträdet ansvarar fullt ut för underbiträdets behandling gentemot den personuppgiftsansvarige.

10. HANTERING AV RÄTTELSE OCH RADERING M.M.

10.1 För det fall den Personuppgiftsansvarige begärt rättelse eller radering på grund av Personuppgiftsbiträdets felaktiga Behandling ska Personuppgiftsbiträdet vidta lämplig åtgärd utan onödigt dröjsmål, senast inom trettio (30) dagar, från det att Personuppgiftsbiträdet mottagit erforderlig information från den Personuppgiftsansvarige. När den Personuppgiftsansvarige begärt radering får Personuppgiftsbiträdet endast utföra Behandling av den aktuella personuppgiften som ett led i processen för radering.

Punkt 10.1 säkerställer att personuppgiftsbiträdet ska understödja den personuppgiftsansvarige med de åtgärder som behövs för att tekniskt möjliggöra att den personuppgiftsansvarige hanterar de registrerades rättigheter (som rättelse och radering av personuppgifter, m.m.), enligt artikel 28. 3 e i dataskyddsförordningen.

Personuppgiftsbiträdet kan behöva ta del av sekretessbelagda personuppgifter för att kunna verkställa raderingen. Villkoret innehåller ett medgivande (en instruktion) från den personuppgiftsansvarige till biträdet att få ta del av sådana uppgifter för att kunna utföra arbetsuppgiften. Av artikel 16 i dataskyddsförordningen följer att den registrerade har rätt att begära att felaktiga personuppgifter rättas.

Av artikel 17.3 b i dataskyddsförordningen följer dock att rätten att bli bortglömd inte gäller om behandlingen är nödvändig för att uppfylla en rättslig förpliktelse som kräver behandling enligt unionsrätten eller enligt en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av eller för att utföra en uppgift av allmänt intresse.

10.2 Om tekniska och organisatoriska åtgärder (t.ex. uppgraderingar eller felsökningar) vidtas av Personuppgiftsbiträdet i Behandlingen, vilka kan väntas påverka Behandlingen, ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige skriftligt om detta i enlighet med vad stadgas om meddelanden i 19 kap. i PUB-avtalet. Informationen ska lämnas i god tid innan åtgärderna vidtas.

Punkt 10.2 säkerställer att personuppgiftsbiträdet ska understödja den personuppgiftsansvarige med de åtgärder som behövs för att tekniskt möjliggöra att den personuppgiftsansvarige hanterar kraven enligt artikel 32.1 i dataskyddsförordningen.

11. PERSONUPPGIFTSINCIDENTER

11.1 Personuppgiftsbiträdet ska ha förmåga att återställa tillgängligheten och tillgången till Personuppgifterna i rimlig tid vid en fysisk eller teknisk incident enligt Dataskyddsförordningen, artikel 32.1 c.

Punkten 11.1 säkerställer att personuppgiftsbiträdet har förmåga att återställa tillgängligheten och tillgången till personuppgifterna i rimlig tid vid en fysisk eller teknisk incident enligt artikel 32.1 c. i dataskyddsförordningen. Det förutsätter att personuppgiftsbiträdet har en organisation och rutiner för alla slag av säkerhetsincidenthantering i sitt ledningssystem för informationssäkerhet (motsvarande).

11.2 Personuppgiftbiträdet åtar sig att med beaktande av Behandlingens art, och den information som Personuppgiftsbiträdet har att tillgå, bistå den Personuppgiftsansvarige med att fullgöra dennes skyldigheter vid en Personuppgiftsincident beträffande Behandlingen. Personuppgiftbiträdet ska på den Personuppgiftsansvariges begäran även bistå med att utreda misstankar om eventuell obehörigs Behandling och/eller åtkomst till Personuppgifterna.

Punkten 11.2 säkerställer personuppgiftsbiträdets skyldighet enligt artikel 28.3 f. i dataskyddsförordningen; att bistå den personuppgiftsansvarige med att se till att skyldigheterna enligt artikel 32–36 fullgörs med hänsyn till typen av behandling och den information som personuppgiftsbiträdet har att tillgå.

11.3 Vid Personuppgiftsincidenter, vilka Personuppgiftbiträdet fått vetskap om, ska Personuppgiftsbiträdet utan onödigt dröjsmål skriftligen underrätta den Personuppgiftsansvarige om händelsen. Personuppgiftsbiträdet ska med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå tillhandahålla den Personuppgiftsansvarige en skriftlig beskrivning av Personuppgiftsincidenten.

Beskrivningen ska redogöra för:

1. *Personuppgiftsincidentens art och, om möjligt, de kategorier och antalet Registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,*
2. *de sannolika konsekvenserna av Personuppgiftsincidenten, och*
3. *åtgärder som har vidtagits eller föreslagits samt åtgärder för att mildra Personuppgiftincidentens potentiella negativa effekter.*

Personuppgiftsbiträdet ska enligt artikel 33.2 i dataskyddsförordningen underrätta den personuppgiftsansvarig utan onödigt dröjsmål vid händelse av personuppgiftsincident och ska i övrigt stödja den personuppgiftsansvarige med en anmälan av en personuppgiftsincident till tillsynsmyndigheten samt i förekommande fall till registrerade.

Punkten 11.3 säkerställer att det ska finnas rutiner för hantering och beskrivning samt rapportering av personuppgiftsincidenter som följer av dataskyddsförordningen.

11.4 Om det inte är möjligt för Personuppgiftsbiträdet att tillhandahålla hela beskrivningen samtidigt, enligt punkt 11.3 i PUB-avtalet, får beskrivningen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

Punkt 11.4 säkerställer att personuppgiftsbiträdet underrättar personuppgiftsansvarig om personuppgiftsincidenten även om alla uppgifter som ska ingå i beskrivningen inte finns tillgängliga initialt. Information får då lämnas i omgångar utan vidare dröjsmål.

12. UNDERBITRÄDEN

12.1 Personuppgiftsbiträdet ansvarar fullt ut för Underbiträdets Behandling gentemot den Personuppgiftsansvarige.

Punkt 12.1 säkerställer att personuppgiftbiträdet har fullt ansvar för underbiträdens behandlingar. Personuppgiftsbiträdet kan, med beaktande av samtliga punkter i PUB-avtalet, uppdra åt flera olika underbiträden att bistå i den behandling personuppgiftsbiträdet har i uppdrag att utföra. I alla fall där personuppgiftsbiträdet uppdrar åt ett eller flera underbiträden att bistå i dennes behandling, ansvar personuppgiftsbiträdet alltid fullt ut för dessas behandling mot den personuppgiftsansvarige. Den personuppgiftsansvariges instruktioner till personuppgiftsbiträdet ska givetvis inkluderas i personuppgiftsbiträdets PUB-avtal med sina underbiträden.

12.2 Personuppgiftsbiträdet äger rätt att anlita ett nytt underbiträde. När Personuppgiftsbiträdet avser att anlita ett nytt underbiträde ska Personuppgiftsbiträdet säkerställa underbiträdets kapacitet och förmåga att uppfylla sina skyldigheter enligt Dataskyddslagstiftningen. Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om

1. underbiträdets namn, organisationsnummer och säte (adress och land),

2. vilken typ av uppgifter och kategorier av Registrerade som behandlas, och

3. var Personuppgifterna ska behandlas.

Enligt artikel 28.2 i dataskyddsförordningen får personuppgiftsbiträdet inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den

personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.

En grundläggande förutsättning för att den personuppgiftsansvarige ska kunna uppfylla säkerhetskraven och kravet på kontroll av personuppgiftsbiträden är att den personuppgiftsansvarige har kännedom om vilka underbiträden som behandlar personuppgifter för dennes räkning.

Personuppgiftsbiträdet äger enligt punkten 12.2 rätt att anlita nya underbiträden och åtar sig att skriftligen meddela personuppgiftsansvarig uppgifter om dessa såsom namn, organisationsnummer, adress, kategorier av registrerade som behandlas och var uppgifterna ska behandlas. Den personuppgiftsansvarige har dock rätt att motsätta sig anlitandet av det nya underbiträdet om den personuppgiftsansvarige inte anser att underbiträdet ger tillräckliga garantier för en säker behandling (se punkten 17.4)

> *12.3 Personuppgiftsbiträdet äger rätt att upphöra med att anlita Underbiträdet. När Personuppgiftsbiträdet upphör med att anlita Underbiträdet ska Personuppgiftsbiträdet skriftligen meddela den Personuppgiftsansvarige om att det upphör med att anlita Underbiträdet.*

Den personuppgiftsansvarige behöver även veta vilka underbiträden som inte längre är aktuella för att kunna uppfylla kravet på kontroll.

> *12.4 Personuppgiftsbiträdet åtar sig att teckna ett skriftligt personuppgiftsbiträdesavtal med det nya underbiträdet och säkerställa att det nya underbiträdet åläggs samma skyldigheter som Personuppgiftsbiträdet åläggs enligt detta PUB-avtal.*

I de fall där ett personuppgiftsbiträde anlitar ett annat personuppgiftsbiträde (underbiträde) för utförande av specifik behandling på den personuppgiftsansvariges vägnar, ska enligt artikel 28.4 i dataskyddsförordningen underbiträdet, genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt, åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i avtalet eller den andra rättsakten mellan den personuppgiftsansvarige och personuppgiftsbiträdet.

> *12.5 Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran översända en kopia av det personuppgiftsbiträdesavtal som Personuppgiftsbiträdet tecknat med Underbiträdet.*

Den personuppgiftsansvarige behöver även för att kunna uppfylla kravet på kontroll veta vilka underbiträden som personuppgiftsbiträdet tecknat avtal med och att dessa uppfyller kraven i artikel 28 i dataskyddsförordningen.

> *12.6 Den Personuppgiftsansvarige äger inom 30 dagar rätt att invända mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde och att, med anledning av sådan*

invändning, säga upp detta PUB-avtal att upphöra i enlighet med vad stadgas i PUB-avtalet, punkt 17.4.

Punkt 12.6 säkerställer att den personuppgiftsansvarige har rätt att inom 30 dagar invända mot anlitandet av ett nytt underbiträde och har rätt att säga upp PUB-avtalet om denne anser att det finns en risk att det nya underbiträdet inte hanterar personuppgifterna på ett säkert sätt.

13. LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

13.1 Personuppgiftsbiträdet ska säkerställa att Personuppgifterna hanteras och lagras inom EU/EES av en fysisk eller juridisk person som är etablerad inom EU/EES, om inte PUB-avtalets parter kommer överens om något annat.

Punkt 13.1 säkerställer att personuppgiftsbiträdets behandling av personuppgifterna sker inom EU/EES och av en fysisk eller juridisk person som är etablerad inom EU/EES, såvida parterna inte kommit överens om någonting annat. Dataskyddsförordningen medför att alla EU/EES-länder har ett likvärdigt skydd för personuppgifter. Det innebär att personuppgifter kan överföras fritt mellan dessa länder utan några begränsningar. För länder utanför EU/EES (s.k. tredje länder) finns generellt inte en lagstiftning som ger motsvarande garantier. Av den anledningen stadgar dataskyddsförordningen att överföring endast får ske under särskilda förhållanden. Möjligheterna för tillåten överföring av personuppgifter som är under behandling eller är avsedd att behandlas i ett tredje land kan delas in i följande tre grupper:

1. EU-kommissionen har beslutat att tredje landet säkerställer en adekvat skyddsnivå,
2. den som behandlar personuppgifterna har vidtagit lämpliga skyddsåtgärder inför överföringen och det finns lagstadgade rättigheter och effektiva rättsmedel för registrerade eller
3. det föreligger ett undantag enligt artikel 49.1 första stycket i dataskyddsförordningen.

Om personuppgifter ska behandlas utanför EU/EES är det parternas skyldighet att säkerställa att något av undantagen ovan är tillämpligt. Den personuppgiftsansvarige ska också på förhand ha givit sitt skriftliga godkännande till överföringen och utfärdat instruktioner för detta ändamål.

14. ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING

14.1 Vid ersättning för skada i samband med Behandling som, genom fastställd dom eller förlikning, ska utgå till den Registrerade på grund av överträdelse av bestämmelse i PUB-avtalet, Instruktioner och/eller tillämplig bestämmelse i Data-skyddslagstiftningen ska artikel 82 i Dataskyddsförordningen tillämpas.

I punkt 14.1 regleras ansvaret mellan parterna för det fall en registrerad lider skada till följd av att en eller båda parterna har behandlat personuppgifter i strid med dataskyddsförordningen. Punkten reglerar inte ansvar för annan typ av skada och påverkar inte parternas möjlighet att införa ansvarsbegränsningar för skador som beror på att huvudavtalet inte följs avseende exempelvis leveranser eller SLA (se vidare kommentaren under punkten 14.4).

Punkten hänvisar till artikel 82 i dataskyddsförordningen och syftet är att den ska tolkas i enlighet med rättsutvecklingen inom artikelns tillämpningsområde. I artikel 82 stadgas utförligt när en personuppgiftsansvarig respektive ett personuppgiftsbiträde kan bli ansvarig för ideella och materiella skador hos den registrerade och möjligheterna till regressrätt.

Den personuppgiftsansvarige är enligt artikel 82 ansvarig för skada som orsakats av behandling som strider mot dataskyddsförordningen. Personuppgiftsbiträdets ansvar är enligt artikel 82.2 begränsat till situationer där

1. denne inte har fullgjort de skyldigheter i dataskyddsförordningen som specifikt riktar sig till personuppgiftsbiträden eller
2. agerat utanför eller i strid med den personuppgiftsansvariges lagenliga anvisningar.

Av artikel 82.4 i dataskyddsförordningen följer dock att parterna är solidariskt ansvariga gentemot den registrerade om båda medverkat vid samma behandling och enligt artikel 82.3 inte kan visa att de inte på något sätt är ansvariga för den händelse som orsakat skadan.

Regressmöjligheten i artikel 82.5 ger den part som har betalat ut full ersättning rätt att från den andra parten återkräva den del av ersättningen som motsvarar den andra par-tens del av ansvaret enligt artikel 82.2.

14.2 Sanktionsavgifter enligt Dataskyddsförordningen, artikel 83, eller Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning 6 kap. 2 § ska bäras av den av PUB-avtalets parter som påförts en sådan avgift.

Punkt 14.2 regerar att en eventuell administrativ sanktionsavgift ska bäras av den part som påförts avgiften av tillsynsmyndigheten. Av artikel 83 följer att avgiften har till syfte att i varje enskilt fall vara effektiv, proportionell och avskräckande. Vidare ska tillsynsmyndigheten bland annat vid påförandet av avgiften ta hänsyn till graden av ansvar hos den personuppgiftsansvarige eller personuppgiftsbiträdet med beaktande av de tekniska och organisatoriska åtgärder som genomförts av dem i enlighet med artikel 25 och 32.

14.3 Om endera part får kännedom om omständighet som kan leda till skada för motparten ska parten omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

Punkt 14.3 reglerar parternas informationsskyldighet gentemot varandra och grundas på allmänna skadeståndsrättsliga principer om att lämpliga åtgärder ska vidtas för att minska

uppkommen skada och följderna av en sådan.

14.4 Oaktat vad sägs i Huvudavtalet gäller detta PUB-avtal, punkter 14.1 och 14.2, före andra regler om fördelning mellan Parterna av krav sinsemellan såvitt avser Behandlingen.

Punkt 14.4 reglerar att parterna inte kan avtala om någon annan ansvarsfördelning gällande skadestånd till registrerad som uppstår i samband med personuppgiftsbehandling eller administrativ sanktionsavgift än vad som stadgas i punkterna 14.1 och 14.2. Skälet är att det följer av artikel 28.1 och skäl 81 i dataskyddsförordningen att en personuppgiftsansvarig endast får anlita personuppgiftsbiträden som kan ge ”tillräckliga garantier” om att genomföra lämpliga tekniska och organisatoriska åtgärder så att behandlingen uppfyller kraven i förordningen och säkerställer att den registrerades rättigheter skyddas. Att personuppgiftsbiträdet friskriver sig från eventuell skada, och därmed helt eller delvis övervältrar sitt ansvar för skyddet av personuppgifter på den personuppgiftsansvarige, torde inte vara förenligt med kravet på ”tillräckliga garantier ”.

Det ska framhållas att ansvar för skador på grund av exempelvis felaktiga eller försenade leveranser kan regleras i huvudavtalet utan hinder av punkten 14.4 i PUB-avtalet. Villkoret hindrar alltså inte parterna från att i huvudavtalet reglera eventuella ansvarsbegränsningar för skada som beror på att huvudavtalet inte följs.

15. LAGVAL OCH TVISTELÖSNING

För detta avtal gäller svensk rätt. Eventuell tolkning eller tvist i anledning av PUB-avtalet, som parterna inte kan lösa på egen hand, ska avgöras av svensk allmän domstol

Eventuell tolkning eller tvist i anledning av PUB-avtalet, som parterna inte kan lösa på egen hand, ska avgöras av svensk allmän domstol och enligt svensk rätt. Punkten kan inte avtalas bort eller ändras enligt punkten 3.3.

16. PUB-AVTALETS TECKNANDE; AVTALSTID OCH UPPSÄGNING

16.1 PUB-avtalet gäller från och med den tidpunkt PUB-avtalet undertecknats av båda parter och tillsvidare. Parterna äger ömsesidig rätt att säga upp PUB-avtalet att upphöra med trettio (30) dagars varsel.

Punkt 16.1 reglerar vad som gäller mellan parterna för det fall avtalstiden inte följer av huvudavtalet. Det är fullt möjligt för parterna att avtala om annan avtals- eller uppsägningstid i huvudavtalet. Huvudavtalets reglering ska i sådant fall ha företräde (jmf. punkten 3.3).

17. ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.

17.1 Endera part i PUB-avtalet äger rätt att påkalla omförhandling av PUB-avtalet om motpartens ägarförhållanden ändras väsentligt eller om tillämplig lagstiftning, eller tolkningen av den, ändras på ett för Behandlingen avgörande sätt. Påkallande av omförhandling enligt första meningen innebär inte att PUB-avtalet till någon del upphör att gälla utan endast att en omförhandling om PUB-avtalet ska påbörjas.

Punkt 17.1 föreskriver att båda parterna har rätt till omförhandling om ägarförhållandena ändras väsentligt eller om tillämplig lagstiftning eller tolkningen av lagstiftningen ändras på ett för behandlingen avgörande sätt. En ny majoritetsägare från tredje land skulle kunna vara väsentlig ändring av ägarförhållandena. Omförhandlingen ska i första hand syfta till att försöka hitta en lösning så att avtalet kan fortsätta löpa.

17.3 När någon av parterna får kännedom om att motparten agerar i strid med PUB-avtalet, Instruktioner och/eller Dataskyddslagstiftningen, ska parten utan dröjsmål meddela motparten om agerandet. Därefter äger parten rätt att med omedelbar verkan upphöra att utföra sina förpliktelser enligt PUB-avtalet till den tidpunkt motparten förklarat att agerandet upphört och förklaringen accepterats av den part som påtalat agerandet.

Punkt 17.3 ålägger båda parterna en skyldighet att utan dröjsmål meddela motparten om denne agerar i strid med PUB-avtalet. Därefter får parten rätt att omedelbart sluta utföra de uppgifter som åligger parten enligt PUB-avtalet. För det fall parten inte upphör med behandlingen finns en uppenbar risk att partens ansvar enligt dataskyddsförordningen ökar väsentligt. När motparten har rättat till de brister som parten har påtalat och den påtalande parten har accepterat förklaringen kan avtalet fortsätta löpa.

17.4 Om den Personuppgiftsansvarige invänder mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde, enligt detta PUB-avtal, punkt 12.6, har den Personuppgiftsansvarige rätt att säga upp PUB-avtalet att upphöra med omedelbar verkan. Om Personuppgiftsbiträdet Behandlar Personuppgifterna efter den tidpunkt som anges i punkt 18.2 gäller vad stadgas i punkter 18.3-18.4.

Punkt 17.4 säkerställer att artikel 28.2 jämte skäl 81 i dataskyddsförordningen infrias. I artikel 28.2 föreskrivs att ett personuppgiftsbiträde inte får anlita ett annat person-uppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträde eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar. Villkoret ger den personuppgiftsansvarige rätt att säga upp avtalet för det fall den personuppgiftsansvarige inte anser att underbiträdet har tillräcklig sakkunskap, tillförlitlighet

och resurser för att genomföra tekniska och organisatoriska åtgärder som uppfyller kraven i dataskyddsförordningen (jmf skäl 81 i dataskyddsförordningen).

18. ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE

18.1 Vid uppsägning av PUB-avtalet ska den Personuppgiftsansvarige utan onödigt dröjsmål begära att Personuppgiftsbiträdet överlämnar samtliga Personuppgifter till den Personuppgiftsansvarige eller raderar dem, enligt dennes önskemål. Om Personuppgifterna överlämnas ska det ske i ett öppet och standardiserat format. Med samtliga Personuppgifter avses alla Personuppgifter vilka har omfattats av Behandlingen samt annan tillhörande information såsom Loggar, Instruktioner, systemlösningar, beskrivningar och andra handlingar som Personuppgiftsbiträdet erhållit genom informationsutbyte enligt PUB-avtalet.

Punkt 18.1 föreskriver att den personuppgiftsansvarige så snart som möjligt ska meddela om personuppgiftsbiträdet om denne ska radera eller återlämna samtliga personuppgifter till den personuppgiftsansvarige. Personuppgiftsbiträdet ska, efter raderingen eller återlämnandet, inte ha några personuppgifter kvar. För det fall det finns lagkrav som kräver att personuppgiftsbiträdet behåller uppgifter får biträdet behålla de uppgifter som behövs för att uppfylla lagkravet (jmf. 28.3 g i dataskyddsförordningen) i ett sådant fall finns laglig rätt att behandla uppgifter enligt artikel 6.1 c. I sådant fall blir personuppgiftsbiträdet ansvarig för den behandlingen.

18.2 Överlämning och radering enligt PUB-avtalet, punkt 18.1, ska vara utförda senast trettio (30) dagar räknat från den tidpunkt uppsägning gjorts enligt detta PUB-avtal, punkt 16.1

Punkt 18.2 reglerar vad som gäller mellan parterna för det fall annan uppsägningstid inte har reglerats i huvudavtalet. Det är fullt möjligt för parterna att avtala om annan återlämning eller raderingstid i huvudavtalet. Huvudavtalets reglering ska i sådant fall ha företräde (jmf. punkten 3.3).

18.3 Behandling som utförs av Personuppgiftsbiträdet efter den tidpunkt som stadgas i punkt 18.2 är att betrakta som en otillåten Behandling.

För det fall det finns lagkrav som kräver att personuppgiftsbiträdet behåller uppgifter får biträdet behålla de uppgifter som behövs för att uppfylla lagkravet (jmf. 28.3 g i dataskyddsförordningen). I sådant fall blir personuppgiftsbiträdet ansvarig för den behandlingen.

18.4 Bestämmelser om sekretess/tystnadsplikt i 8 kap. PUB-avtalet ska fortsätta gälla även om PUB-avtalet i övrigt upphör av gälla.

Punkt 18.4 reglerar att för det fall att personuppgiftsbiträdet blivit personuppgiftsansvarig för behandlingen kvarstår sekretess/tystnadsplikten.

19. MEDDELANDEN INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER

19.1 Meddelanden om PUB-avtalet och dess administration inklusive uppsägning ska skickas till respektive parts kontaktperson för PUB-avtalet.

Meddelande om PUB-avtalets administration får endast skickas till parts kontaktperson såvida parterna inte kommit överens om något annat i huvudavtalet.

19.2 Meddelanden om parternas samarbete om dataskydd, gällande Behandlingen, ska skickas till respektive parts kontaktperson för parternas samarbete om dataskydd.

Meddelande om dataskydd vid behandlingen får endast skickas till parts kontaktperson för dataskydd. såvida parterna inte kommit överens om något annat i huvudavtalet.

19.3 Meddelanden inom ramen för PUB-avtalet och Instruktioner ska skickas skriftligt. Ett meddelande ska anses ha kommit fram till mottagaren senast en (1) arbetsdag efter att meddelandet har skickats.

Meddelandet kan skickas skriftligt vilket inte utesluter att det skickas per e-post.

21. ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER

21.1 Varje part ansvarar för att de uppgifter som anges i 1 kap. i PUB-avtalet alltid är aktuella. Ändring av uppgifter i 1 kap. ska meddelas skriftligt enligt punkt 19.1 i PUB-avtalet.

Punkt 21.1 säkerställer att det alltid finns kontaktpersoner som kan ta emot meddelanden enligt avtalet. Parterna ansvarar för att kontaktpersonernas uppgifter ständigt är aktuella.

VERSIONSHANTERING

Version	Datum	Förändringar	Ansvarig
1.1	19-08-09	PUNKT 7.6	PÅL RESARE