Personuppgiftsbiträdes-avtal

Pointsharp Net iD

Classification:	Internal
Publication No.:	PSC-Lg22-11
Document version:	2.1a
Document status:	Final
Date:	23 Aug 2024

Table of Contents

Avtal enligt artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679[1].

1. Allmänna dataskyddsförordningen EU 2016/679 föreskriver att det ska finnas ett skriftligt avtal om Personuppgiftsbiträdets Behandling av Personuppgifter för Den personuppgiftsansvariges räkning.

1. PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

Personuppgiftsansvarig		**Personuppgiftsbiträde**	
Organisationsnamn		Pointsharp AB	
Momsregistreringsnummer		**Momsregistreringsnummer**	
		SE556691063301	
Postadress		**Postadress**	
		Uddvägen 7 131 54 Nacka	
Kontaktperson för administration av detta personuppgiftsbiträdesavtal		**Kontaktperson för administration av detta personuppgiftsbiträdesavtal**	
Namn:		Namn:	Niklas Brask
E-post:		E-post:	niklas.brask@pointsharp.com
Tfn:		Tfn:	+46 70 738 73 70
Kontaktperson för parternas samarbete om dataskydd		**Kontaktperson för parternas samarbete om dataskydd**	
Namn:		Namn:	Mikael Ernstson
E-post:		E-post:	mikael.ernstson@pointsharp.com
Tfn:		Tfn:	+46 70 530 99 44

2. DEFINITIONER

Utöver de begrepp som definieras i löptext, i detta personuppgiftsbiträdesavtal, ska dessa definitioner oavsett om de används i plural eller singular, i bestämd eller obestämd form, ha nedanstående innebörd när de anges med versal som begynnelsebokstav.

Term	Definition
Behandling	En åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättningar av Personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
Dataskyddslagstiftning	Avser all integritets- och personuppgiftslagstiftning, samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter), som är tillämplig på den Behandling som sker enligt detta PUB-avtal, inklusive nationell sådan lagstiftning och EU-lagstiftning.
Personuppgiftsansvarig	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamål och medlen för Behandlingen av Personuppgifter.
Instruktion	De skriftliga instruktioner som närmare anger föremål, varaktighet, art och ändamål, typ av Personuppgifter samt kategorier av Registrerade och särskilda behov som omfattas av Behandlingen.
Logg	Logg är resultatet av Loggning.
Loggning	Loggning är ett kontinuerligt insamlande av uppgifter om den Behandling av Personuppgifter som utförs enligt detta PUB-avtal och som kan knytas till en enskild fysisk person.
Personuppgiftsbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som Behandlar Personuppgifter för den Personuppgiftsansvariges räkning.
Personuppgift	Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
Personuppgiftsincident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de Personuppgifter som överförts, lagrats eller på annat sätt Behandlats.
Registrerad	Fysisk person vars Personuppgifter Behandlas.

Term	Definition
Tredje land	En stat som inte ingår i Europeiska unionen (EU) eller inte är ansluten till Europeiska ekonomiska samarbetsområdet (EES).
Underbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som i egenskap av underleverantör till Personuppgiftsbiträdet Behandlar Personuppgifter för Personuppgiftsansvariges räkning.

3. BAKGRUND OCH SYFTE

3.1 Med detta Personuppgiftsbiträdesavtal jämte Instruktioner och en eventuell förteckning över Underbiträden (nedan gemensamt "PUB-avtalet") reglerar den Personuppgiftsansvarige Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige. PUB-avtalets syfte är att säkerställa den Registrerades fri- och rättigheter vid Behandlingen, i enlighet med vad som stadgas i artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679 ("Dataskyddsförordningen").
3.2 När PUB-avtalet utgör ett av flera avtalsdokument inom ramen för ett annat avtal benämns det andra avtalet "Huvudavtalet" i PUB-avtalet.
3.3 För det fall något av det som stadgas i avsnitt 1, punkt 3.2, avsnitt 15 eller 16, punkt 17.6, avsnitt 18–20 eller 22 i PUB-avtalet regleras på annat sätt i Huvudavtalet ska Huvudavtalets reglering ha företräde.
3.4 Hänvisningar i PUB-avtalet till nationell eller unionsrättslig lagstiftning, avser vid var tid tillämpliga bestämmelser.

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.
4.2 Den Personuppgiftsansvarige ska ge skriftliga Instruktioner till Personuppgiftsbiträdet om hur det ska utföra Behandlingen.
4.3. Personuppgiftsbiträdet får endast utföra Behandlingen i enlighet med PUB-avtalet och vid var tid gällande Instruktioner.

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 med hänsyn till Behandlingens art så att Personuppgiftsbiträdet och eventuellt Underbiträde kan fullgöra sitt eller sina uppdrag enligt detta PUB-avtal och Huvudavtal i förekommande fall.
5.2 Den Personuppgiftsansvarige ska utan onödigt dröjsmål informera Personuppgiftsbiträdet om förändringar i Behandlingen vilka påverkar Personuppgiftsbiträdets skyldigheter enligt Dataskyddslagstiftningen.
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.

6. PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN

6.1 Personuppgiftsbiträdet förbinder sig att endast utföra Behandlingen i enlighet med PUB-avtalet och och för de specifika ändamål som anges i Instruktioner samt att följa Dataskyddslagstiftningen. Personuppgiftsbiträdet förbinder sig även att fortlöpande hålla sig informerad om gällande rätt på området.
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.
6.3 Personuppgiftsbiträdet åtar sig att säkerställa att samtliga fysiska personer som arbetar under dess ledning följer PUB-avtalet och Instruktioner samt att de fysiska personerna informeras om relevant lagstiftning.
6.4 Personuppgiftsbiträdet ska på begäran från den Personuppgiftsansvarige bistå denne med att säkerställa att skyldigheterna enligt artikel 32–36 i Dataskyddsförordningen 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.
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, om inte parterna kommer överens om annat.
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.

7. SÄKERHETSÅTGÄRDER

7.1 Personuppgiftsbiträdet ska vidta alla lämpliga tekniska och organisatoriska säkerhetsåtgärder som krävs enligt Dataskyddslagstiftningen för att förhindra Personuppgiftsincidenter, genom att säkerställa att Behandlingen uppfyller kraven i Dataskyddsförordningen och att den Registrerades rättigheter skyddas.
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.
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.
7.4 Personuppgiftbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till Personuppgifterna för sådana fysiska personer som arbetar under Personuppgiftsbiträdets ledning och som behöver åtkomsten för att kunna utföra sina arbetsuppgifter.
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.

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

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, varken direkt eller indirekt, såvida inte annat avtalats.
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.
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.
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.

9. GRANSKNING, TILLSYN OCH REVISION

9.1 Personuppgiftsbiträdet ska utan onödigt dröjsmål som en del av sina garantier, enligt artikel 28.1 i Dataskyddsförordningen, på den Personuppgiftsansvariges begäran kunna redovisa vilka tekniska och organisatoriska säkerhetsåtgärder som används för att Behandlingen ska uppfylla kraven enligt PUB-avtalet och artikel 28.3.h i Dataskyddsförordningen.
9.2 Personuppgiftsbiträdet ska 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.
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.

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

10. HANTERING AV RÄTTELSER 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 rättelse eller radering.
10.2 Om tekniska och organisatoriska åtgärder (t.ex. uppgraderingar eller felsökningar) vidtas av Personuppgiftsbiträdet i Behandlingen, vilka kan påverka Behandlingen, ska Personuppgiftsbiträdet skriftligt informera den Personuppgiftsansvarige om detta i enlighet med vad som stadgas om meddelanden i avsnitt 18 i PUB-avtalet. Informationen ska lämnas i god tid innan åtgärderna vidtas.

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 artikel 32.1.c i Dataskyddsförordningen.
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.
11.3 Vid Personuppgiftsincident, vilken 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.
11.4 Beskrivningen ska redogöra för:

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

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

12. UNDERBITRÄDE

12.1 Personuppgiftsbiträdet äger rätt att anlita den eller de Underbiträden som framgår av bilagd förteckning över Underbiträden.
12.2 Personuppgiftsbiträdet åtar sig att teckna ett skriftligt avtal med Underbiträdet som reglerar den Behandling som Underbiträdet utför å den Personuppgiftsansvariges vägnar samt att endast anlita Underbiträden som ger tillräckliga garantier. Underbiträdet ska genomföra lämpliga tekniska och organisatoriska åtgärder så att Behandlingen uppfyller kraven i Dataskyddslagstiftningen. I fråga om dataskydd ska avtalet åläggа Underbiträdet samma skyldigheter som åläggs Personuppgiftsbiträdet i detta PUB-avtal.
12.3 Personuppgiftsbiträdet ska i avtalet med Underbiträdet säkerställa att den Personuppgiftsansvarige har rätt att säga upp Underbiträdet och instruera Underbiträdet att exempelvis radera eller återlämna Personuppgifterna om Personuppgiftsbiträdet har upphört att existera i faktisk eller rättslig mening eller hamnat på obestånd.
12.4 Personuppgiftsbiträdet ansvarar fullt ut för Underbiträdets Behandling gentemot den Personuppgiftsansvarige. Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarige om Underbiträdet underlåter att uppfylla sina skyldigheter i PUB- avtalet.
12.5 Personuppgiftsbiträdet äger rätt att anlita nya underbiträden och ersätta befintliga underbiträden om inte annat anges i Instruktionen.
12.6 När Personuppgiftsbiträdet avser att anlita ett nytt eller ersätta ett befintligt Underbiträde ska Personuppgiftsbiträdet säkerställa Underbiträdets kapacitet och förmåga att uppfylla sina skyldigheter enligt Dataskyddslagstiftningen. Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om

a. Underbiträdets namn, organisationsnummer och säte (adress och land),
b. vilken typ av uppgifter och kategorier av Registrerade som behandlas, och
c. var Personuppgifterna ska behandlas.

12.7 Den Personuppgiftsansvarige äger rätt att inom trettio (30) dagar från dag för meddelande enligt punkten 12.6 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, punkten 16.4.
12.8 Personuppgiftsbiträdet ska vid var tid föra en korrekt och uppdaterad förteckning över de Underbiträden som anlitas för Behandling av Personuppgifter för den Personuppgiftsansvariges räkning samt göra denna förteckning tillgänglig för den Personuppgiftsansvarige. Av förteckningen ska särskilt framgå i vilket land Underbiträdet behandlar Personuppgifterna och vilka typer av Behandlingar som

Underbiträdet utför.
12.9 När Personuppgiftsbiträdet slutar använda ett Underbiträde ska Personuppgiftsbiträdet skriftligen meddela den Personuppgiftsansvarige om detta. Personuppgiftsbiträdet ska när ett avtal upphör säkerställa att Underbiträdet raderar eller återlämnar Personuppgifterna.
12.10 Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran översända en kopia av det avtal som reglerar Underbiträdets Behandling av Personuppgifter och förteckningen över Underbiträden enligt punkten 12.1.

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.
13.2 Personuppgiftsbiträdet äger endast rätt att överföra Personuppgifter till Tredje land för Behandling (t.ex. service, support, underhåll, utveckling, drift eller liknande hantering) om den Personuppgiftsansvarige på förhand skriftligen godkänt sådan överföring och utfärdat Instruktioner för detta ändamål.
13.3 Överföring till Tredje land för Behandling enligt PUB-avtalet, punkten 13.2, får endast ske om den är förenlig med Dataskyddslagstiftningen och uppfyller de krav på Behandlingen vilka ställs i PUB-avtalet och Instruktioner.

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 Dataskyddslagstiftningen ska artikel i 82 i Dataskyddsförordningen tillämpas.
14.2 Sanktionsavgifter enligt artikel 83 i Dataskyddsförordningen, eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den av PUB-avtalets parter som påförts en sådan avgift.
14.3 Om endera part får kännedom om omständighet som kan leda till skada för motparten ska parten utan onödigt dröjsmål informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.
14.4 Oaktat vad som sägs i Huvudavtalet gäller detta PUB-avtal, punkterna 14.1 och 14.2, före andra regler om fördelning mellan Parterna av krav sinsemellan såvitt avser Behandlingen.

15. PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING

15.1 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.

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

16.1 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.
16.2 Tillägg till, och ändringar i, PUB-avtalet ska vara skriftliga och undertecknade av

båda parter.
16.3 När någon av parterna får kännedom om att motparten agerar i strid med PUB-avtalet och/eller Instruktioner 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.
16.4 Om den Personuppgiftsansvarige invänder mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde, enligt detta PUB-avtal, punkten 12.7, har den Personuppgiftsansvarige rätt att säga upp PUB-avtalet att upphöra med omedelbar verkan.

17. ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE

17.1 Efter uppsägning av PUB-avtalet ska Personuppgiftsbiträdet utan onödigt dröjsmål, beroende på vad den Personuppgiftsansvarige väljer, antingen radera och intyga för den Personuppgiftsansvarige att det är utfört, eller återlämna

a. alla Personuppgifter som Behandlats för den Personuppgiftsansvariges räkning och
b. all tillhörande information såsom Loggar, Instruktioner, systemlösningar, beskrivningar och andra handlingar som Personuppgiftsbiträdet erhållit genom informationsutbyte enligt PUB-avtalet.

17.2 I samband med återlämning ska Personuppgiftsbiträdet även radera befintliga kopior av Personuppgifter och tillhörande information.
17.3 Skyldigheten att radera eller återlämna Personuppgifter eller tillhörande information gäller inte om lagring av Personuppgifterna eller informationen krävs enligt unionsrätten eller relevant nationell rätt där Behandling får utföras enligt PUB-avtalet.
17.4 Om Personuppgifter eller tillhörande information återlämnas ska det ske i ett allmänt använt och standardiserat format, om parterna inte har kommit överens om något annat format.
17.5 Till dess att uppgifterna raderas eller återlämnas ska Personuppgiftsbiträdet säkerställa efterlevnaden av PUB-avtalet.
17.6 Återlämning eller radering enligt PUB-avtalet ska vara utförd senast trettio (30) kalenderdagar räknat från tidpunkten för uppsägningen av PUB-avtalet, om inte annat anges i Instruktionen. Behandling av Personuppgifter som Personuppgiftsbiträdet utför därefter är att betrakta som otillåten Behandling.
17.7 Bestämmelser om sekretess/tystnadsplikt i avsnitt 8 ska fortsätta gälla även om PUB-avtalet i övrigt upphör att gälla.

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

18.1 Meddelanden om PUB-avtalet och dess administration inklusive uppsägning ska skickas via e-post eller på något annat av parterna överenskommet sätt till respektive parts kontaktperson för PUB-avtalet.
18.2 Meddelanden om parternas samarbete om dataskydd gällande Behandlingen ska skickas via e-post eller på något annat av parterna överenskommet sätt till respektive parts kontaktperson för parternas samarbete om dataskydd.
18.3 Ett meddelande ska anses ha kommit fram till mottagaren senast en (1) arbetsdag efter att meddelandet har skickats.

19. KONTAKTPERSONER

19.1 Parterna ska utse var sin kontaktperson för PUB-avtalet.
19.2 Parterna ska utse var sin kontaktperson för parternas samarbete om dataskydd.

20. ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER

20.1 Varje part ansvarar för att de uppgifter som anges i avsnitt 1 i PUB-avtalet alltid är aktuella och korrekta.
20.2 Ändring av uppgifter i avsnitt 1 ska meddelas motparten enligt punkt 18.1 i PUB-avtalet.

21. LAGVAL OCH TVISTER

21.1 Vid tolkning och tillämpning av PUB-avtalet gäller svensk rätt med undantag för lagvals-reglerna. Tvister med anledning av PUB-avtalet ska avgöras av behörig svensk domstol.

22. PARTERNAS UNDERTECKNANDEN AV PUB-AVTALET

22.1 Detta PUB-avtal tillhandahålls antingen i digitalt format för elektroniskt undertecknande eller i pappersformat för egenhändigt undertecknande. I sistnämnda fall upprättas avtalet i två likalydande exemplar, varav parterna erhåller varsitt.

Personuppgiftsansvarig	
Organisationsnamn	
Ort	
Datum	
Namnförtydligande	
Signatur	

Personuppgiftsbiträde	
Pointsharp AB	
Ort	
Datum	
Namnförtydligande	
Signatur	

Versionshantering

Detta dokument är baserat på Personuppgiftsbiträdesavtalet framtaget och underhållet av Sveriges Kommuner och Landsting (SKR). För mer information och originaldokument, se https://skr.se/skr/ekonomijuridik/juridik/dataskyddsforordningengdpr/personuppgiftsbitradesavtalpubavtal/vagledandekommentarerpubavtalsdokument.68501.html.

Version	Datum	Förändringar	Ansvarig
1.1	2018-12-19	10.1, 14.1, 18.2,	PR
1.2	2019-12-17	2, 3.1, 3.3, 5.1, 6.3, 6.4, 7.1, 8.2, 9.1, 9.2, 9.6, 10.1, 10.2, 11.4, 12, 13.3, 14.2, 14.3, 17.3, 17.4, 18.2, 18.3, 18.4, 21.1, 22.1	NE
1.2.1	2020-01-02	17.4	PR
2.0	2022-12-21	1, 2, 3.1, 3.3, 5.1, 6.1, 6.5, 10.2, 12.2, 12.3, 12.4, 12.5, 12.7, 12.8, 12.9, 12.10, 14.3, 15, 16, 17, 18, 19, 20, 21, 22	HA, EW, FS
2.1	2023-04-06	Ändrat hänvisning i 16.4 till 12.7	HA, PR
2.1a	2024-02-29	Tagit bort stycke 22.2	Pointsharp

Personuppgiftsansvariges Instruktion för Behandling av Personuppgifter

Personuppgiftsansvarigs instruktion till Personuppgiftsbiträdet (Pointsharp) för behandling av personuppgifter inom tjänsten Pointsharp Net iD.

Personuppgiftsansvarig

Personuppgiftsansvarig enligt definitionen i Personuppgiftsbiträdesavtalet.

Utöver vad som redan framgår av Personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet även följa nedanstående instruktion:

1. Ändamål, föremålet och arten

1 a. Föremålet för Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige är att:

Tillhandahålla en tjänst för utfärdande och livscykelhantering av svenska e-legitimationer som ska användas av användaren för olika ändamål, exempelvis inloggning i IT-infrastruktur/webbapplikationer samt signering av elektroniska dokument.

1 b. Ändamålet med Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige är att:

Enligt avtal med den personuppgiftsansvarige tillhandahåller Pointsharp tjänsten Pointsharp Net iD svensk e-legitimation (Tjänsten). I det uppdraget agerar Pointsharp som personuppgiftsbiträde och behandlar personuppgifter för:

- Utsedd personal hos Personuppgiftsansvarig med roller i förvaltningen av RA-domänen.
- Användarna hos Personuppgiftsansvarig, det vill säga innehavarna av e-identiteterna, som hanteras i system relaterade till Tjänsten.

Ansvaret som Personuppgiftsbiträde gäller alla personuppgifter som Pointsharp kan ha tillgång till under drift, backup och andra underhållsaktiviteter, oavsett om personuppgifterna finns tillgängliga i okrypterad eller krypterad form.

Personuppgifter som rör Personuppgiftsansvarigs personal och användare ska i huvudsak lagras i krypterad form i databaser och i säkerhetskopior av dessa (i vila) samt i krypterade kanaler under transport, men kan finnas tillgängliga i okrypterad form i samband med felsökning eller annat underhåll.

1 c. Personuppgiftsbiträdets Behandling av Personuppgifter på uppdrag av den Personuppgiftsansvarige avser huvudsakligen följande behandlingsåtgärder (Behandlingens art eller natur):

- Bearbetning
- Insamling
- Lagring
- Loggning
- Läsning

- Överföring

2. Behandlingen omfattar följande typer av Personuppgifter

Behandlingen kan innehålla följande personuppgifter:

- namn,
- unik identifierare, till exempel personnummer,
- e-postadress,
- upn,
- telefonnummer,
- serienummer på nyckelbäraren,
- organisation,
- Microsoft SID (Microsoft security identifier),
- RA-roll,
- foto,
- signatur,
- elektronisk signatur,
- kontorsadress,
- titel,
- certifikat med innehåll,
- publik nyckel och
- MIFARE-nummer

3. Behandlingen omfattar vissa kategorier av Registrerade

Behandlingen av personuppgifter inkluderar följande kategorier av registrerade:

- Användare hos Personuppgiftsansvarig: anställda, konsulter eller andra personer associerade med Personuppgiftsansvarig som använder Tjänsten.
- Personal med RA-roller hos Personuppgiftsansvarig: anställda, konsulter eller annan personal som har Personuppgiftsansvarigs uppdrag att hantera sina åtaganden inom Tjänsten.

4. Ange särskilda hanteringskrav vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet

Administratörer hos Personuppgiftsbiträdet kommer att ha tillgång till att hantera personuppgifter i Tjänsten. Sådan behandling av personuppgifter ska endast utföras på begäran av en behörig representant för den personuppgiftsansvarige. Personuppgiftsansvarig ska kunna granska loggar över all utförd behandling.

I händelse av att spårningsloggning är aktiverat för felsökning kan personuppgifter tillfälligt komma att finnas i loggfiler som används under felsökning. Loggfiler ska raderas omedelbart efter att felsökningen har utförts.

En bakgrundskontroll ska göras för all personal innan de tillsätts en roll som ger tillgång till personuppgifter tillhörande Personuppgiftsansvarig. Utsedd personal ska ha visat sig vara lämplig att inneha rollen och ska ha genomgått utbildning i hantering av personuppgifter i enlighet med GDPR och detta personuppgiftsbiträdesavtal.

4.1. Säkerhetskopior

Säkerhetskopior som innehåller personuppgifter ska skyddas till minst samma nivå som systemet eller applikationen där personuppgifterna normalt används eller lagras.

Kompletta säkerhetskopior av systemen ska sparas i högst två år innan de roteras på ett sådant sätt att säkerhetskopior äldre än två år förstörs.

5. Ange särskilda tekniska och organisatoriska säkerhetsåtgärder som gäller för Personuppgiftsbiträdets Behandling av Personuppgifter

5.1. Personuppgifter och känsliga uppgifter i applikationsdatabaser

Alla känsliga uppgifter i applikationsdatabaserna (inklusive personuppgifter) måste lagras krypterade. Systemadministratörer hos Personuppgiftsbiträdet och dess underleverantörer ska endast ha tillgång till personuppgifter i krypterad form.

Tillgång till hårdvara och kryptonycklar ska hanteras via en process där minst två (2) personer i förening krävs för att hantera de nycklar som används för skydd av personuppgifter och känsliga uppgifter i databaser.

5.2. Personuppgifter och känsliga uppgifter under transport

All kommunikation mellan system och applikationer ska skyddas med teknik baserad på asymmetrisk och symmetrisk kryptering. Skydd av personuppgifter under överföring bör inte bara förlita sig på TLS, utan bör använda ett extra krypteringslager.

5.3. Automatisk registrering av personuppgifter

Personuppgiftsbiträde ska genomföra en automatisk hämtning och registrering av Microsoft SID som är läsbart från AD hos den Personuppgiftsansvarige. Detta för att möjliggöra domäninloggning med e-legitimationen.

6. Ange särskilda krav på Loggning vad gäller Behandling av Personuppgifter samt vilka som ska ha tillgång till dem

Loggar ska sparas i minst tio (10) år innan de rensas (ändring från Personuppgiftsbiträdesavtal, avsnitt 7.5).

I loggar ska det framgå vilka personer som har och har haft tillgång till personuppgifter och vid ändring av personuppgifter ska det framgå vad som har ändrats.

Exempel på loggar som Personuppgiftsbiträdets personal kan komma att hantera och som innehåller personuppgifter:

- Behörigheter för åtkomst till personuppgifter och ändringar i behörigheterna.
- Logisk åtkomst till Tjänsten.
- Alla ändringar av personuppgifter i Tjänsten.
- Felsökningsloggar för applikationer.
- Händelser relaterade till utfärdande och hantering av certifikat

Endast personal hos Personuppgiftsansvarig som har utsetts till en roll som ger tillgång till personuppgifter ska ha tillgång till loggarna.

6.1. Spårningsloggning (trace logging)

I samband med felsökning kan det finnas behov av att slå på spårningsloggning för de olika serverapplikationerna för att få information som är mer detaljerad och för att underlätta felsökning. Dessa spårningsloggar innehåller personuppgifter och ska därför hanteras med största försiktighet.

Så snart spårningsloggar har analyserats ska de omgående raderas i systemen och på alla andra tillfälliga lagringsplatser eller lagringsmedia som använts för analysen.

7. Lokalisering och överföring av Personuppgifter till Tredje land

Personuppgifter får inte överföras till eller behandlas i tredje land.

8. Behandlingens varaktighet

Under Personuppgiftsbiträdetsavtalets giltighetstid.

Personuppgifter i loggar som Pointsharp måste bevara efter personuppgiftsbiträdesavtalets upphörande, på grund av spårbarhetskrav, kommer behandlas i enlighet med personuppgiftsbiträdesavtalet tills loggarna gallras bort efter 10 år.

9. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av biträdet/biträdena

9.1. Avvikelser och kompletteringar av skrivningar i Personuppgiftsbiträdesavtalets huvuddokument

- Stycke 7.5:
  Rensning av loggfiler får ske först efter tio (10) år istället för de angivna fem (5) åren.
- Stycke 16.1:
  För Personuppgiftsbiträdesavtalet gäller samma uppsägningstid som för huvudavtalet mellan parterna, se Pointsharp Net iD Svensk e-legitimation Kundavtal-Villkor avsnitt 18.1.
- Stycke 17:1:
  Loggar kommer inte att raderas i samband med avtalets upphörande, det kommer att ske efter 10 år, se avsnitt 8 i denna instruktion.

Lista över underbiträden

Bilaga 2 – Lista över godkända Underbiträden

Den Personuppgiftsansvarige godkänner att Personuppgiftsbiträdet anlitar nedanstående Underbiträden för Behandling av Personuppgifter.

Bolag/ organisation	**Adress och kontaktuppgifter**	**Lokalisering av Personuppgifter (adress, land)**	**Typer av Personuppgifter som Behandlas av Underbiträdet**	**Ändamål med Underbiträdets Behandling**	**Behandlingstid**	**Ytterligare information om Underbiträdets Behandling av Personuppgifter**
Orange Business Digital Sweden AB 556638-0639	Gårdsvägen 6, 169 70 Solna Telefon: +46 8 501 126 00	Solna och Upplands Väsby Sverige	Se Pointsharp Net iD Svensk e-legitimation Personuppgiftsansvariges Instruktion för Behandling av Personuppgifter avsnitt 2 for information om vilka personuppgifter det kan röra sig om.	Driftleverantör. Tillhandahåller serverdrift för alla de komponenter som ingår i Tjänsten och är nödvändiga för utfärdande och giltighetskontroll av Svensk e-legitimation.	Under huvudavtalets giltighet samt därefter hantering av personuppgifter som är nödvändiga för att uppfylla krav i regulatorisk dokumentation (utifrån krav från DIGG, CP/CPS och tillitsramverk)	All data är krypterad vid transport och i vila i databaser. Oranges drift av IT-tjänster är ISO/IEC 27001-certifierad och datorhallarna är PCI-DSS certifierade.

Bolag/ organisation	Adress och kontaktuppgifter	Lokalisering av Personuppgifter (adress, land)	Typer av Personuppgifter som Behandlas av Underbiträdet	Ändamål med Underbiträdets Behandling	Behandlingstid	Ytterligare information om Underbiträdets Behandling av Personuppgifter
Thales DIS Sweden AB 556343-7218	Glasfibergatan 12, 125 45 Älvsjö Telefon: +46 8 517 95700	Stockholm Sverige	Personuppgifter som framgår fysiskt på kortet, finns lagrade i kortens chip eller på annat sätt är knutna till korten. • namn, • unik identifierare, till exempel personnummer • titel, • e-postadress, • upn, • kortserienummer • organisation, • Microsoft SID (Microsoft security identifier), • foto, • certifikat med publik nyckel (innehållande ovan nämnda personuppgifter), • namnteckning, • MIFARE-nummer, • kontorsadress,	Beställning, utfärdande och leverans av ordinarie kort i de fall kunden använder smartkort personaliserade i kortfabrik.	Under huvudavtalets giltighet samt därefter hantering av personuppgifter som är nödvändiga för att uppfylla krav i regulatorisk dokumentation (utifrån krav från DIGG, CP/CPS och tillitsramverk)	Thales säkerhetsinfrastruktur är baserad på ISO/IEC 27001. Den största delen av produktionen är certifierad enligt ISO/IEC 27001, vilket omfattar den del av verksamheten där råmaterial för smartkort tillverkas, dvs där personalisering av pass och nationellt id-kort (NID) sker

Bolag/ organisation	Adress och kontaktuppgifter	Lokalisering av Personuppgifter (adress, land)	Typer av Personuppgifter som Behandlas av Underbiträdet	Ändamål med Underbiträdets Behandling	Behandlingstid	Ytterligare information om Underbiträdets Behandling av Personuppgifter
			• säkerhetskod (PUK), • privat nyckel			

POINTSHARP

Website
https://www.pointsharp.com

Disclaimer
Specifications subject to change without further notice, unless stated otherwise in agreement.

Classification: Internal
Publ. No.: PSC-Lg22-11
Document version: 2.1a
Document status: Final
OID:
Published: 23 Aug 2024