

DN

Personuppgiftsbiträdesavtal Region Örebro

**Personuppgiftsbiträdesavtal mellan den personuppgiftsansvarige och
personuppgiftsbiträdet avseende Driftavtal avseende R7e-arkiv, Dnr:14dot017**

Addo Sign ID-nummer: c2ea00f2-c873-422c-bc0d-6d05f52d9357

Innehållsförteckning

1	PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER	2
2	DEFINITIONER	2
3	BAKGRUND OCH SYFTE	4
4	BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION	4
5	DEN PERSONUPPGIFTSANSVARIGES ANSVAR.....	4
6	PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN	5
7	SÄKERHETSÅTGÄRDER	5
8	SEKRETESS/TYSTNADSPLIKT	6
9	GRANSKNING, TILLSYN OCH REVISION	6
10	HANTERING AV RÄTTELSE OCH RADERING M.M.....	7
11	PERSONUPPGIFTSINCIDENTER.....	7
12	UNDERBITRÄDE.....	8
13	LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND	9
14	ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING.....	9
15	PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING	10
16	ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.	10
17	ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE	10
18	MEDDELANDE INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER	11
19	KONTAKTPERSONER.....	11
20	ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER.....	11
21	LAGVAL OCH TVISTER.....	11
22	PARTERNAS UNDERTECKNANDE AV PUB-AVTALET	11

BILAGA A: INSTRUKTION FÖR BEHANDLING AV PERSONUPPGIFTER

BILAGA B: LISTA ÖVER UNDERBITRÄDEN

PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679¹

1. PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

Personuppgiftsansvarig	Personuppgiftsbiträde
Region Halland Driftnämnden Ambulans diagnostik och hälsa Långgatan 32 302 49 Halmstad Driftnämnden Hallands sjukhus Hallands sjukhus Halmstad 301 85 Halmstad Driftnämnden Närsjukvård Träslövsvägen 68 432 37 Varberg Driftnämnden Psykiatri Träslövsvägen 432 81 Varberg	Region Örebro län Box 1613 701 16 Örebro
Organisationsnummer	Organisationsnummer
232100–0115	232100–0164
Kontaktperson för administration av detta personuppgiftsbiträdesavtal	Kontaktperson för administration av detta personuppgiftsbiträdesavtal
Namn: Dataskyddsenheten Region Halland E-post: dataskydd@regionhalland.se Tfn: 035-134800	Namn: Eva Lundberg E-post: eva.lundberg@regionorebrolan.se Tfn: 070-332 72 38
Kontaktperson för parternas samarbete om dataskydd	Kontaktpersoner för parternas samarbete om dataskydd
Namn: Dataskyddsenheten Region Halland E-post: dataskydd@regionhalland.se Tfn: 035-134800	Namn: Eva Lundberg E-post: eva.lundberg@regionorebrolan.se Tfn: 070-332 72 38

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.

Behandling

En åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättningar av Personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering,

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

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 annan lagstiftning, 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 lokaliseringssuppgift 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.

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.

3.5 I vissa situationer agerar Personuppgiftsansvarig som personuppgiftsbiträde för sina kunders räkning. Vid den behandlingen som sker förändras rollerna så att Personuppgiftsbiträdet kan komma att agera som underbiträde. Villkoren i PUB-avtalet ska inom ramen för Huvudavtalet gälla även för det fall att Personuppgiftsbiträdet agerar som underbiträde och Personuppgiftsansvarig som personuppgiftsbiträde.

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 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 Personuppgiftsbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till Personuppgifterna för sådana fysiska personer som arbetar under Personuppgiftsbitrådets 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 Personuppgiftsbitrådets 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 Personuppgiftsbiträdet 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 RÄTTELSE OCH RADERING M.M.

10.1 För det fall den Personuppgiftsansvarige begärt rättelse eller radering på grund av Personuppgiftsbitrådets 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 Personuppgiftsbiträdet 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. Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran även bistå med att utreda misstankar om eventuell obehörig Behandling och/eller åtkomst till Personuppgifterna.

11.3 Vid Personuppgiftsincident, vilken Personuppgiftsbiträdet 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 Personuppgiftsincidentens 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 förteckningen över Underbiträden, bilaga B.

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 ålägga 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 Underbitrådets Behandling gentemot den Personuppgiftsansvarige. Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarig 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 Underbitrådets kapacitet och förmåga att uppfylla sina skyldigheter enligt Dataskyddslagstiftningen. Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om

- a. Underbitrådets 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 Personuppgiftsbitrådets 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 Underbitrådets 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 godkännt 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 Personuppgiftsbitrådets anlitan 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 Personuppgiftsbitrådet 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 Personuppgiftsbitrådet erhållit genom informationsutbyte enligt PUB-avtalet.

17.2 I samband med återlämning ska Personuppgiftsbitrådet 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 Personuppgiftsbitrådet 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 Personuppgiftsbitrådet 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.

22.2 Om PUB-avtalet undertecknas elektroniskt lämnas signatursidan utan avseende.

Personuppgiftsansvarig Region Halland	
Ort och datum	
Underskrift	
Måns Arnrup IT-direktör	

Personuppgiftsbiträde Region Örebro	
Ort och datum	
Underskrift	
Mehmed Hasanbegovic	Befattning Förvaltningschef

BILAGA A: INSTRUKTION FÖR BEHANDLING AV PERSONUPPGIFTER

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

1. Ändamål, föremålet och arten

Behandlingens föremål är Personuppgifter som Personuppgiftsbiträdet behandlar för den Personuppgiftsansvariges räkning i samband med fullgörandet av Huvudavtalet.

Behandlingen av Personuppgifter sker i syfte att:

- Tillhandahålla och leverera tjänsten till den Personuppgiftsansvarige och fullgöra åtaganden enligt Huvudavtalet
- Ge support till användare, superanvändare och administratörer
- Genomföra tekniskt underhåll och säkerhetskopiering
- Statistik avseende felutfall samt åtgärdsstatistik

Behandlingen av Personuppgifter sker i samband med att Personuppgiftsbiträdet driftar, lagrar och genomför tekniskt bearbetning av en mjukvara för mellan- och slutarkivering på den Personuppgiftsansvariges uppdrag. Behandlingen av Personuppgifter sker även i samband med att Personuppgiftsbiträdet ger support avseende tjänsten till den Personuppgiftsansvariges medarbetare. Behandlingen av Personuppgifter sker delvis automatiserat och helt automatiserat.

2. Behandlingen omfattar följande typer av Personuppgifter

Behandlingen omfattar kontaktuppgifter, personnummer eller motsvarande, nätidentifikare, användar-id, e-postadress och kön. Behandlingen omfattar även uppgifter om hälsa, sexuell läggning och sexualliv, religiös eller filosofisk övertygelse, genetiska uppgifter, biometriska uppgifter, etniskt ursprung. Uppgifter som den Personuppgiftsansvarige laddar upp i tjänsten samt andra typer av Personuppgifter som framgår av Huvudavtalet.

3. Behandlingen omfattar vissa kategorier av Registrerade

Behandlingen omfattar den Personuppgiftsansvariges medarbetare, uppdragstagare, patienter, närstående och kontaktpersoner samt de kategorier som i övrigt följer av Huvudavtalet.

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

Behandlingen omfattar behandlingsstegen nedan samt vad som i övrigt framgår av Huvudavtalet.

Åtkomst

Personuppgiftsbiträdet kommer åt Personuppgifter i samband med tekniskt underhåll och supportärenden relaterade till mjukvaran.

Insamling

Personuppgiftsbiträdet samlar in Personuppgifter (t.ex. genom att samla in loggar) i den utsträckning det är nödvändigt i samband med tekniskt underhåll och supportärenden relaterade till mjukvaran.

Överföring och lagring

Insamlade Personuppgifter överförs till och lagras i Personuppgiftsbitrådets it-system.

Radering

Insamlade Personuppgifter och analysresultat (om de innehåller Personuppgifter) raderas efter att supportärendet är avslutat eller när de inte längre behövs för att genomföra tekniskt underhåll. PUB får dock spara de Personuppgifter som är nödvändiga för att dokumentera att supportärendet har genomförts (t.ex. kontaktuppgifter till den Personuppgiftsansvariges kontaktperson eller kommunikation via e-post) tills Huvudavtalet upphör. Sparade Personuppgifter får inte omfatta känsliga Personuppgifter eller patientuppgifter. Om det råder osäkerhet om vilka Personuppgifter som ska sparas ska Personuppgiftsbitrådet begära ytterligare skriftliga Instruktioner från den Personuppgiftsansvarige. I övrigt raderas Personuppgifter enligt den Personuppgiftsansvariges skriftliga Instruktioner.

5. Ange särskilda tekniska och organisatoriska säkerhetsåtgärder vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbitrådet

Fysisk säkerhet

Lämpliga och adekvata åtgärder ska vidtas för att säkerställa den fysiska säkerheten av it-utrymmen² såsom, men inte begränsat till, skalskydd, tillträdesskydd, brandskydd, skydd mot elavbrott, stöldskydd och skydd mot skadegörelse. Vidtagna åtgärder ska säkerställa en skyddsnivå som minst motsvarar de skyddsnivåer som anges i bilaga 1 till MSB:s vägledning för fysisk informationssäkerhet i it-utrymmen.³

Inventering av datorutrustning och system

Det ska föras en förteckning över datorutrustning och system som används för Behandling av Personuppgifter. Det ska finnas dokumenterade rutiner för löpande uppdatering av denna förteckning.

Åtkomstskydd

Datorutrustning och portabla lagringsmedier som inte står under uppsikt ska låsas in för att skyddas mot obehörig användning, påverkan och stöld. I annat fall ska Personuppgifter krypteras.

Datorer och mobila enheter

Medarbetares datorer ska låsas automatiskt vid inaktivitet och kräva starkt lösenord för upplåsning. Antalet öppna kommunikationsportar i datorerna ska minimeras och brandväggar, antivirusprogram och säkerhetsuppdateringar ska installeras och uppdateras regelbundet. Hårddiskar tillhörande bärbara datorer ska alltid vara krypterade med tillräckligt stark nyckel. Lagringsminnen tillhörande mobila enheter ska krypteras med tillräckligt stark nyckel. Mobila enheter ska skyddas med ett tillräckligt starkt lösenord och raderas automatiskt om felaktigt lösenord matas in för många gånger. Det ska finnas möjlighet att radera Personuppgifter från mobila enheter via fjärråtkomst. Behandling av Personuppgifter på mobila enheter ska begränsas enligt dokumenterade rutiner. Medarbetare ska inte ha tillåtelse att behandla Personuppgifter på privata datorer eller mobila enheter.

Autentisering

Inloggning i system ska ske via personlig användaridentitet med lösenord. Lösenord ska vara tillräckligt starka och bytas regelbundet. Det ska inte vara tillåtet att överlåta eller dela inloggningsuppgifter med andra personer. Det ska föras ett register över användares inloggning i

² Med it-utrymmen avses samtliga lokaler som är avsedda för it-drift och förvarar it-utrustning.

³ MSB629, Vägledning för fysisk informationssäkerhet i it-utrymmen ISBN 978-91-7383-401-8 tillgänglig på [Vägledning för fysisk informationssäkerhet i it-utrymmen \(msb.se\)](https://www.msb.se/publikationer/2017/06/20170629-01)

system. Vid en användares upprepade felaktiga inloggningsförsök i ett system ska användarkontot avaktiveras eller spärras för en definierad tid.

Behörighetsstyrning

Medarbetares åtkomst till Personuppgifter ska styras av ett tekniskt system för behörighetskontroll. Medarbetarna ska ges minsta möjliga åtkomst vid behandling av Personuppgifter. Endast medarbetare som behöver tillgång till Personuppgifter för sitt arbete ska ges åtkomst. Det ska finnas dokumenterade rutiner för tilldelning och borttagande av behörigheter.

Åtkomstkontroll

Åtkomst till Personuppgifter ska kunna kontrolleras i efterhand genom loggar. Loggarna ska kontrolleras regelbundet i syfte att upptäcka otillåten eller obehörig tillgång till Personuppgifter.

Servrar

Åtkomst till administrativa verktyg och gränssnitt på servrar ska begränsas. Medarbetare som har administrativa rättigheter ska använda starka lösenord. Det ska inte vara tillåtet att överlåta eller dela inloggningsuppgifter med andra personer. Det ska finnas dokumenterade rutiner som säkerställer att viktiga uppdateringar för operativsystem och applikationer installeras omgående.

Nätverkssäkerhet

Nätverk ska skyddas mot externa angrepp och förlust av information. Trådlösa nätverk ska skyddas med kryptering. In- och utgående nätverkstrafik ska filtreras via exempelvis brandväggar. Mjukvara som regelbundet scannar nätverk för virus, trojaner och andra former av digitala intrång ska användas och hållas uppdaterad.

Skydd mot skadlig kod och otillförlitliga program

Endast sådana program som formellt godkänts inom verksamheten ska få finnas i systemmiljön. Det ska finnas dokumenterade rutiner för att skydda system mot virus, trojaner och andra former av digitala intrång.

Säkerhetskopior

Personuppgifter ska regelbundet (minst en gång per dag) överföras till säkerhetskopior. Säkerhetskopiorna ska förvaras avskilt och väl skyddade så att Personuppgifter kan återskapas efter en störning. Det ska finnas dokumenterade rutiner för säkerhetskopiering, återläsning av säkerhetskopior och test av återläsning av säkerhetskopior.

Datakommunikation

Anslutning för extern datakommunikation ska skyddas med sådan teknisk funktion som säkerställer att uppkopplingen är behörig. Personuppgifter som överförs via öppna nätverk (t.ex. internet) ska skyddas med kryptering.

Utplåning

Det ska finnas dokumenterade rutiner som säkerställer att Personuppgifter kan raderas när de inte längre är nödvändiga för ändamålet och att de inte är möjliga att återskapa.

Reparation och service

När reparation och service av datorutrustning utförs av annan än Personuppgiftsbiträdet eller Underbiträde, ska kontrakt som reglerar säkerhet och sekretess träffas med serviceföretaget. Vid servicebesök ska servicen ske under Personuppgiftsbitrådets eller Underbitrådets överinseende. Är detta inte möjligt ska lagringsmedier som innehåller Personuppgifter avlägsnas. Service via fjärrstyrd datakommunikation får endast ske efter säker elektronisk identifiering av den som utför servicen. Servicepersonal ska ges åtkomst i systemet endast vid servicetillfället. Finns separat kommunikationsingång för service ska den vara stängd när service inte pågår.

Rapportering av personuppgiftsincidenter

Rutin för rapportering och uppföljning av personuppgiftsincidenter och andra säkerhetsincidenter ska finnas och följas. Rutinen ska omfatta hur information ska förmedlas, till vem rapportering ska ske och hur information sammanställs. Personuppgiftsincidenten ska följas upp och de brister i organisationen som lett till att personuppgiftsincidenten inträffat ska rättas till. Rutin för att utan onödigt dröjsmål underrätta den Personuppgiftsansvarige vid misstanke om eller konstaterad personuppgiftsincident ska finnas. Personuppgiftsbiträdet ska ha förmågan att återställa tillgängligheten och åtkomsten till Personuppgifter i rimlig tid vid en inträffad personuppgiftsincident.

Rapportering av funktionsfel och brister

Det ska finnas dokumenterade rutiner för rapportering av fel, säkerhetsmässiga svagheter, brister och ändringsförslag. I rutinen ska det vara fastställt till vem och hur rapportering ska ske.

Driftdokumentation

Dokumentation som beskriver den dagliga driften av system ska vara av tillräcklig kvalitet för att garantera upprätthållandet av tillgängligheten.

Separation

Personuppgifterna ska logiskt separeras från personuppgifter som Personuppgiftsbiträdet behandlar på uppdrag av andra än den Personuppgiftsansvarige.

Pseudonymisering

Personuppgifter ska i möjligaste mån pseudonymiseras.⁴

Penetrationstester

Personuppgiftsbiträdet ska genomföra regelbundna penetrationstester (minst en gång per år).

Process för mjukvaruutveckling

Personuppgiftsbiträdet ska implementera en process för mjukvaruutveckling som följer en vedertagen metod och som innefattar ändamålsenlig manuell och automatiserad testning.

Utbildning av personal

De krav som gäller för medarbetare med tillgång till system ska vara definierade av systemägaren. Kraven ska avse såväl säkerhet som kompetens och ska vara dokumenterade och kommunicerade. Medarbetare ska regelbundet (minst en gång per år) utbildas inom dataskydd. Nyanställda medarbetare ska genomgå utbildning inom dataskydd innan de får åtkomst till Personuppgifter.

Ytterligare åtgärder

Personuppgiftsbiträdet ska vidta alla ytterligare tekniska och organisatoriska säkerhetsåtgärder som krävs enligt Tillämplig dataskyddslag eller annan författning, beslut från behörig tillsynsmyndighet, gällande administrativ praxis och rättspraxis. Sådana ytterligare åtgärder ska också vidtas om detta krävs på grund av behandlingens art, omfattning, sammanhang och ändamål samt riskerna för Registrerades fri- och rättigheter.

Dokumentation av åtgärder

Genomförandet av samtliga säkerhetsåtgärder enligt denna bilaga ska dokumenteras och tillhandahållas den Personuppgiftsansvarige på begäran.

⁴ Pseudonymisering: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

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

Inga särskilda krav utöver vad som framgår av detta PUB-avtal eller Huvudavtalet.

7. Lokalisering och överföring av Personuppgifter till Tredje land

Behandlingen kommer att utföras på utrustning som befinner sig i EU/EES.

8. Behandlingens varaktighet

Personuppgiftsbiträdet Behandlar Personuppgifter under PUB-avtalets varaktighet.

9. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet

Personuppgiftsbiträdet driftar den gemensamt förvaltade applikationen R7e-arkiv som ägs av de, i Samverkan R7e-arkiv, ingående regionerna. Den centrala förvaltningens, i Samverkan R7e-arkiv, huvudsakliga inriktning är att förvalta och utveckla R7e-arkiv och de programvaror och tjänster som krävs för att importera, lagra, utsöka och lämna ut information.

Personuppgiftsbiträdet får endast Behandla Personuppgifter i den utsträckning det är nödvändigt för att utföra tekniskt underhåll och hantera supportärenden av applikationen R7e-arkiv som ägs av samverkansorganisationen.

Personuppgiftsbiträdet får inte självständigt utföra eller ansvara för gallring, radering, utlämnande, rättelse eller annan Behandling av Personuppgifter som hanteras i den gemensamt ägda applikationen R7e-arkiv. Sådan Behandling regleras och utförs enbart av den Personuppgiftsansvarige eller på uppdrag av den Personuppgiftsansvarige.

Personuppgiftsbiträdet får anlita Underbiträden för Behandling av Personuppgifter endast efter uttryckligt uppdrag från den Personuppgiftsansvarige.
I de fall Personuppgiftsbiträdet tecknar avtal med Underbiträden för hantering av applikationen, sker detta på uppdrag av och i enlighet med Instruktioner från Samverkan R7e-arkiv.

Personuppgiftsansvarig ska godkänna varje Underbiträde innan avtal ingås.
Personuppgiftsbiträdet ska säkerställa att Underbiträdet åläggs samma skyldigheter som Personuppgiftsbiträdet enligt detta avtal.
Personuppgiftsbiträdet ansvarar för att Underbiträden följer tillämpliga dataskyddsregler och de Instruktioner som ges av den Personuppgiftsansvarig.





BILAGA B: LISTA ÖVER UNDERBITRÄDEN

Nedan anges de Underbiträden som anlitats för Behandling av Personuppgifter under detta Personuppgiftsbiträdesavtal. Förteckningen ska justeras och uppdateras varje gång ett nytt Underbiträde anlitas eller Underbiträde ersätts.

Bolag/ organisation	Adress och kontaktuppgifter	Lokalisering av Personuppgifter (adress, land)	Typer av Personuppgifter som Behandlas av Underbiträdet	Ändamål med Underbitrådets Behandling	Behandlingstid	Ytterligare information om Underbitrådets Behandling av Personuppgifter
Eficode AB 556686-2032	Vasagatan 36, 111 20 Stockholm	EU	Namn, e- postadress, telefonnummer	Drift och underhåll av systemmiljöer för ärende- hantering	Under PUB avtalets varaktighet	

Signaturerna i detta dokument är juridiskt bindande. Dokumentet är signerat med Addo Sign säkra digitala signatur.
Undertecknarens identitet registreras fysiskt i det elektroniska PDF-dokumentet och visas nedan.
Alla tider anges i koordinerad universell tid (Coordinated Universal Time, UTC).

Undertecknare

  MEHMED HASANBEGOVIC a01EvNFUeOj1zojs0TwrqA 2025-11-07 13:34:59Z	  Måns Arnrup IT-direktör BiXWQbfY41Hk2Hrnqfjhzw 2025-11-07 13:49:57Z
---	--

Dokument i försändelsen

PUB - Region Örebro (R7e-arkiv).pdf SHA256: ae288a79bc3e7070c70cea637584e8fb6741f063596eeef3bf9e1361508db66

Addo Sign ID-nummer: c2ea00f2-c873-422c-bc0d-6d05f52d9357



Dokumentet signeras digitalt med den säkra signeringstjänsten Addo Sign. Signaturbeviset i dokumentet säkras och valideras med det matematiska hashvärdet för originaldokumentet.

Dokumentet är låst för ändringar och tidsstämplat med ett certifikat från en betrodd tredje part. Alla kryptografiska signeringsbevis är inbäddade i PDF-dokumentet ifall de ska användas för validering i framtiden.

Hur man verifierar dokumentets äkthet

Dokumentet är skyddat med ett Adobe CDS-certifikat. När dokumentet öppnas i Adobe Reader ser det ut att vara signerat genom Addo Sign signeringstjänst.