[Infoga logga Personuppgiftsansvarige] [Infoga logga Umeå universitet]

UTKAST 2021-12-13 – Mallförslag PUBA som behöver tecknas mellan varje enskild personuppgiftsansvarig i Ladokkonsortiet och Umeå universitet.

Personuppgiftsbiträdesavtal Ladoksystemet

Detta personuppgiftsbiträdesavtal (nedan kallat ”PUBA”) har ingåtts mellan

[Högskolans namn, org.nr, adress] (nedan kallad ”Personuppgiftsansvarige”)

och

Umeå universitet, org. nr 202100-2874, 901 87 Umeå (nedan kallad ”Personuppgiftsbiträdet”)

var för sig benämnd ”Part” och gemensamt ”Parterna”

1. Bakgrund

I 1 kap 1 § förordning (1993:1153) om redovisning av studier m.m. vid universitet och högskolor finns bestämmelser om

1. registrering av uppgifter om studier inom utbildning på grundnivå, avancerad nivå och forskarnivå vid statliga universitet och högskolor.
2. rapportering av uppgifter till Statistiska centralbyrån (SCB) om studenter för officiell statistik,
3. framställning av personalstatistik vid SCB,
4. registrering av uppgifter om studie- och yrkesmeriter vid Universitets- och högskolerådet.

Enligt förordningen ska varje högskola föra ett studieregister och där ange uppgifterna individuellt för varje student. Varje högskola äger sin egen information i studieregistret, dvs. den information som avser den egna högskolan och dokumentation av de egna studenternas studier. Varje högskola är personuppgiftsansvarig för behandling av personuppgifter i sin verksamhet, och har ett kvalitets- och registeransvar för det egna studieregistret.

Ändamålet med studieregistret är enligt förordningen att säkra att uppgifter om sökande till utbildning, genomgångna studier, betyg över utbildningar och examina bevaras. Härutöver ska uppgifterna kunna läggas till grund för uppföljning och utvärdering, för antagning av studenter, för beslut om anmälningsavgift och studieavgift, för avstängning av studieavgiftsskyldiga studenter, för administration inom respektive högskola, för ändamål som anges i 2 kap 6 och 6 a §§, för sådan officiell statistik som avses i 3 kap, samt för resurstilldelning.

Ladok är ett nationellt system för studieadministration inom högre utbildning i Sverige. Det består av ett antal delsystem och produkter som ger stöd till olika delar av den studieadministrativa processen (nedan kallat ”Ladoksystemet”). Syftet är att underlätta högskolornas dagliga arbete, lokalt och centralt, vid dokumentation och uppföljning av studieresultat samt att trygga studenternas rättssäkerhet. Ladoksystemet är realiserat som en gemensam installation. Lokala system hos respektive högskola som integreras mot Ladoksystemet har bara åtkomst till högskolans egen information.

En sammanslutning av de flesta universitet och högskolor i Sverige har i ett konsortialavtal (nedan kallat ”Konsortialavtalet”) överenskommit om samverkan i syfte att äga, finansiera och förvalta Ladoksystemet. Den fysiska infrastrukturen (nedan kallat ”Infrastrukturen”) som används för genomförandet ägs dock – på uppdrag av Ladokkonsortiet – av Personuppgiftsbiträdet som även ansvar för drift och underhåll.

Ladokkonsortiet ska genom sin verksamhet bidra till effektiva lösningar för studieadministrativt stöd för högskolorna och därigenom underlätta för parterna att både uppfylla gällande författningskrav och tillgodose egna behov. Ladokkonsortiet ska genom sin verksamhet även verka för att CSN:s behov av korrekta och fullständiga uppgifter om studerande tillgodoses.

Parterna i Ladokkonsortiet har i samband med undertecknandet av Konsortialavtalet träffat ett avtal om gemensamt personuppgiftsansvar (nedan kallat ”Avtalet om gemensamt personuppgiftsansvar”) för de behandlingar av personuppgifter som utförs i Ladoksystemet där parterna gemensamt fastställer ändamålen med och medlen för behandlingen, dvs. i de fall när högskolorna inte är självständigt personuppgiftsansvariga för behandlingen.

Ladokkonsortiet har som nämnts ovan gett i uppdrag till Personuppgiftsbiträdet att äga Infrastrukturen där Ladoksystemet driftas. Ladokkonsortiet har även för konsortieparternas räkning – förutom Umeå universitet – träffat en uppdragsöverenskommelse (nedan ”Uppdragsöverenskommelsen”) med Personuppgiftsbiträdet avseende drift av Ladoksystemet. Vid utförandet av tjänsterna enligt Uppdragsöverenskommelsen kommer Personuppgiftsbiträdet att behandla personuppgifter för den Personuppgiftsansvariges räkning.

Detta PUBA kompletterar Konsortialavtalet inklusive bilagan Avtalet om gemensamt personuppgiftsansvar, och Uppdragsöverenskommelsen. Detta PUBA består av allmänna skyldigheter i huvuddokumentet och mer detaljerade bestämmelser i bilaga 1-4. I händelse av konflikt mellan bestämmelserna i detta PUBA, Konsortialavtalet eller Uppdragsöverenskommelsen ska detta PUBA - förutom när det gäller ansvarsfördelningen i enlighet med punkt 10.3 i Konsortialavtalet - ha företräde när det avser behandling av personuppgifter.

2. Syfte

Enligt artikel 28 dataskyddsförordningen (GDPR) ska all behandling av personuppgifter som utförs av ett personuppgiftsbiträde för en personuppgiftsansvarigs räkning regleras genom ett bindande avtal i vilket föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges.

Syftet med detta PUBA är att reglera Parternas rättigheter och skyldigheter som följer med uppdraget att behandla personuppgifter.

3. Definitioner

I detta PUBA används definitionerna i artikel 4 GDPR avseende bland annat följande begrepp.

Personuppgifter, behandling, pseudonymisering, personuppgiftsansvarig, personuppgiftsbiträde, personuppgiftsincident, bindande företagsbestämmelser och tillsynsmyndighet.

Ytterligare begrepp definieras enligt följande.

Gällande dataskyddslagstiftning: Europaparlamentets och Rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), och kompletterande nationell lagstiftning gällande dataskydd.

Känsliga personuppgifter: uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Registrerad: den som personuppgifterna avser.

Standardavtalsklausuler: EU-kommissionens standardavtalsklausuler för överföring till tredje land antagna den 4 juni 2021.

Underbiträde: extern leverantör anlitad av Personuppgiftsbiträdet som behandlar personuppgifter för den Personuppgiftsansvariges räkning.

Tredjeland: en stat som inte igår i Europeiska unionen eller är ansluten till Europeiska ekonomiska samarbetsområdet (EU/EES).

4. Behandling av personuppgifter

Den Personuppgiftsansvarige bestämmer ensam ändamålet med och medlen för den behandling av personuppgifter som Personuppgiftsbiträdet utför för den Personuppgiftsansvariges räkning. Huvudsyftet med behandlingen är att uppfylla kraven i förordning (1993:1153) om redovisning av studier m.m. vid universitet och högskolor. Personuppgiftsbiträdet får endast behandla personuppgifterna i enlighet med de instruktioner som framgår av detta PUBA, Konsortialavtalet och Uppdragsöverenskommelsen. Detsamma gäller för underbiträden.

Den kompletta listan av på förhand godkända underbiträden som får anlitas av Personuppgiftsbiträdet framgår av bilaga 1. Preciserade instruktioner till Personuppgiftsbiträdet avseende behandling av personuppgifter, förutsättningar för överföring av personuppgifter till tredjeland, samt säkerhet för personuppgifter framgår av bilaga 2-4.

Parterna är medvetna om att den Personuppgiftsansvarige kan behöva ändra eller utfärda ytterligare skriftliga instruktioner. Parterna ska gemensamt säkerställa att vid var tid godkända underbiträden, gällande instruktioner, förutsättningar för överföring till tredjeland, samt säkerhet för personuppgifter framgår av bilaga 1-4.

5. Personuppgiftsansvariges allmänna åtaganden

Den Personuppgiftsansvarige ansvarar för och ska säkerställa att behandlingen av personuppgifter sker i enlighet med gällande dataskyddslagstiftning, bland annat att det finns en rättslig grund för aktuella behandlingar. Vidare ska den personuppgiftsansvarige utforma skriftliga instruktioner för att Personuppgiftsbiträdet ska kunna fullgöra sitt uppdrag enligt detta PUBA, Konsortialavtalet och Uppdragsöverenskommelsen.

Den Personuppgiftsansvarige ska utan dröjsmål skriftligen informera Personuppgiftsbiträdet om förändringar i behandlingen som påverkar Personuppgiftsbiträdets skyldigheter.

Om Personuppgiftsbiträdet underrättar den Personuppgiftsansvarige om att det saknas nödvändiga instruktioner för att genomföra uppdraget eller anser att erhållna instruktioner strider mot gällande dataskyddslagstiftning bör den Personuppgiftsansvarige utan dröjsmål lämna nya instruktioner, alternativt tydliggöra eller revidera tidigare lämnade instruktioner.

6. Personuppgiftsbiträdets allmänna åtaganden

Personuppgiftsbiträdet och den eller de personer som arbetar under Personuppgiftsbiträdets ledning får bara behandla personuppgifter i enlighet med gällande dataskyddslagstiftning, detta PUBA med tillhörande skriftliga instruktioner, samt den behandling som framgår av Konsortialavtalet och Uppdragsöverenskommelsen.

Personuppgiftsbiträdet ska, i så stor utsträckning som möjligt, bistå den Personuppgiftsansvarige för att säkerställa att gällande dataskyddslagstiftning efterföljs och att den registrerades rättigheter skyddas.

Personuppgiftbiträdet ska omedelbart informera den Personuppgiftsansvarige om biträdet saknar instruktioner som bedöms nödvändiga för att genomföra uppdraget eller om Personuppgiftsbiträdet anser att en instruktion strider mot gällande dataskyddslagstiftning.

Personuppgiftsbiträdet ska föra ett register – som uppfyller kraven i artikel 30.2 GDPR – över alla kategorier av behandling som utförs för den Personuppgiftsansvariges räkning.

6.1 Kapacitet och förmåga

Personuppgiftsbiträdet garanterar att denne besitter nödvändig teknisk och organisatorisk kapacitet och förmåga, inbegripet tekniska lösningar, kompetens, ekonomiska och personella resurser, rutiner och metoder, att fullgöra sina skyldigheter enligt detta PUBA, Konsortialavtalet, Uppdragsöverenskommelsen och gällande dataskyddslagstiftning.

6.2 Övergripande säkerhetsåtgärder

Personuppgiftsbiträdet ska vidta alla lämpliga tekniska och organisatoriska säkerhetsåtgärder som krävs enligt gällande dataskyddslagstiftningen för att förhindra personuppgiftsincidenter, genom att säkerställa att behandlingen uppfyller kraven i

dataskyddsförordningen och att den registrerades rättigheter skyddas. Åtgärderna ska enligt artikel 32 GDPR inbegripa, när det är lämpligt

- pseudonymisering och kryptering av personuppgifter,
- förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
- förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
- ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Kommenterad [FR1]: Definiera.

Detaljerade instruktioner om säkerhetsåtgärder finns i bilaga 4.

6.3 Personuppgiftsincidenter
Personuppgiftsbiträdet ska underrätta den Personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident enligt artikel 33.2 GDPR. Detaljerade instruktioner om personuppgiftsincidenter finns i bilaga 4.

6.4 Konfidentialitet och lagstadgad sekretess
Personuppgiftsbiträdet får inte utan den Personuppgiftsansvariges skriftliga medgivande lämna ut eller på annat sätt till tredje man röja information om behandlingen av personuppgifter som omfattas av detta avtal, i annat fall än när skyldighet att lämna ut personuppgifterna följer av författning eller domstolsbeslut. Om en sådan lagstadgad skyldighet föreligger ska Personuppgiftsbiträdet underrätta den Personuppgiftsansvarige om detta innan behandlingen påbörjas, under förutsättning att sådan information inte är förbjuden enligt lag.

Personuppgiftsbiträdet ska beakta att personuppgifter som behandlas för den Personuppgiftsansvariges räkning kan vara föremål för sekretess i enlighet med offentlighets- och sekretesslagen (2009:400), OSL. Personer med behörighet att behandla personuppgifter hos Personuppgiftsbiträdet ska vara införstådda med ovanstående regler om sekretess och medföljande tystnadsplikt.

Personuppgiftsbiträdet ska säkerställa att personer med behörighet att behandla personuppgifterna antingen omfattas av en lagstadgad tystnadsplikt eller har åtagit sig tystnadsplikt i ett bindande avtal.

Sekretess och tystnadsplikt enligt denna punkt ska gälla även efter det att detta PUBA upphört att gälla.

7. Granskning och revision

Personuppgiftsbiträdet ska på begäran ge den Personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som framgår av detta PUBA och gällande dataskyddslagstiftning har fullgjorts genom att hänvisa till relevant och godkänd uppförandekod eller certifiering, och/eller tillhandahålla den Personuppgiftsansvarige annan bevisning.

Den Personuppgiftsansvarige har rätt att på egen bekostnad, själv eller genom ett ombud, granska och inspektera att Personuppgiftsbiträdet följer detta PUBA. Samma rättighet ska

gälla i förhållande till underbiträden. Personuppgiftsbiträdet eller underbiträdet ska möjliggöra och bidra till sådan granskning.

Om tillsynsmyndigheten eller annan myndighet med tillsynsuppdrag inleder granskning av den Personuppgiftsansvarige ska Personuppgiftsbiträdet i skälig omfattning bistå den Personuppgiftsansvarige för att möjliggöra sådan granskning.

8. Registrerades rättigheter

Personuppgiftsbiträdet ska i skälig omfattning bistå den Personuppgiftsansvarige med att tillgodose de rättigheter som tillkommer registrerade enligt gällande dataskyddslagstiftning.

Personuppgiftsbiträdet ska utan dröjsmål vidta rättelse av felaktiga eller ofullständiga personuppgifter efter instruktion från den Personuppgiftsansvarige.

9. Konsekvensbedömning och förhandssamråd

Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska Personuppgiftsbiträdet före det att behandlingen utförs, på begäran av Personuppgiftsansvarige, bistå vid en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.

För det fall konsekvensbedömningen av den planerade behandlingen visar att behandlingen skulle leda till hög risk om den Personuppgiftsansvarige inte vidtar åtgärder för att minska risken ska Personuppgiftsbiträdet före behandlingen utförs vara den Personuppgiftsansvarige behjälplig vid samråd med tillsynsmyndigheten.

Personuppgiftsbiträdet har rätt till skälig ersättning för sådant bistånd som avses under denna punkt om inte Parterna kommer överens om annat.

10.Anlitande av underbiträde

Personuppgiftsbiträdet har rätt att anlita den eller de underbiträden som framgår av förteckningen i bilaga 1.

Personuppgiftsbiträdet ska ingå ett skriftligt avtal med sina underbiträden som ålägger underbiträdet minst samma skyldigheter i fråga om dataskydd som de som fastställts i detta PUBA. Personuppgiftsbiträdet ansvarar fullt ut gentemot den Personuppgiftsansvarige för hur underbiträdet behandlar personuppgifterna, inklusive underbiträdets säkerhetsåtgärder.

Personuppgiftsbiträdet äger rätt att anlita nya underbiträden eller ersätta befintliga underbiträden för att utföra hela eller delar av behandlingen.

Tillkommer underbiträde, eller vid byte av underbiträde, ska Personuppgiftsbiträdet skriftligen meddela den Personuppgiftsansvarige om detta utan oskäligt dröjsmål och senast fyrtiofem (45) kalenderdagar före förändringen. Meddelandet ska innehålla den information om underbiträdet som krävs enligt bilaga 1.

Kommenterad [FR2]: Hur sker detta?

Den Personuppgiftsansvarige har rätt att senast inom trettio (30) kalenderdagar från mottagande av meddelandet skriftligen invända mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde. Invändningen måste innehålla en specifik anledning till varför

underbiträdet inte får anlitas. Den Personuppgiftsansvarige har inte rätt att utan sakliga skäl vägra att godkänna underbiträdet.

11. Platsen för behandling av personuppgifter och överföring till tredjeland

Personuppgifterna får endast behandlas inom EU/EES. Personuppgiftsbiträdet får inte utan den Personuppgiftsansvariges skriftliga medgivande överföra personuppgifter till tredjeland, dvs. utanför EU/EES. För överföring av personuppgifter till tredjeland, se instruktioner i bilaga 3.

Vad som anges ovan gäller oavsett om överföringen sker inom Personuppgiftsbiträdets egen organisation eller till ett underbiträde, och gäller även åtkomst till personuppgifterna för exempelvis service, support, underhåll, utveckling, drift eller liknande hantering.

12. Ansvar för skada och sanktionsavgifter

Parternas ansvar för skada och ersättningsskyldighet regleras av artikel 82 GDPR. Vardera Part svarar enskilt för sådana sanktionsavgifter som påförs Parten enligt artikel 83 GDPR.

Om endera Part får kännedom om omständighet som kan leda till skada för den andra Parten ska Parten skyndsamt informera den andra parten om förhållandet. Parterna ska aktivt arbeta tillsammans för att förhindra och minimera sådan skada.

13. Ändringar och tillägg

Ändringar och tillägg till detta avtal ska vara skriftliga och undertecknade av Parterna för att vara giltiga. Den Personuppgiftsansvarige äger dock rätt att efter samråd med Personuppgiftsbiträdet göra nödvändiga ändringar i den vid var tid gällande instruktion som framgår av bilaga 2.

14. Avtalstid och upphörande

Detta PUBA träder i kraft när det har undertecknats av Parterna och är giltigt till dess att Personuppgiftsbiträdets behandling av personuppgifterna och Uppdragsöverenskommelsen upphört.

Instruktioner för Personuppgiftsbiträdets återlämnande av personuppgifter och radering av kopior återfinns i bilaga 2.

15. Tolkning och tillämpning

Tvister om tolkning och tillämpning av detta PUBA och därmed sammanhängande rättsförhållanden ska avgöras enligt svensk lag och enligt Konsortialavtalets tvistebestämmelser.

Detta avtal har upprättats i två (2) likalydande exemplar varav parterna tagit var sitt.

[Infoga ort och datum]	[Infoga ort och datum]
……	……..
[Infoga namn och befattning]	[Infoga namn och befattning]

[Infoga Personuppgiftsansvarige]

[Infoga Personuppgiftsbiträdet]

Personuppgiftsbiträdesavtal – Bilaga 1 (Underbiträden)

Personuppgiftsbiträdet avser att anlita följande underbiträden för behandling av personuppgifter i samband med tillhandahållande av tjänsten enligt Konsortialavtalet och Uppdragsöverenskommelsen, vilket Personuppgiftsansvarige genom att underteckna detta PUBA givit sitt samtycke till.

Personuppgiftsbiträdet ska alltid lämna följande information om sina underbiträden i förteckningen nedan eller med en länk till hemsida:

- underbiträdets namn, organisationsnummer och säte (adress och land)
- vilka kategorier av personuppgifter som behandlas
- ändamålet med underbiträdets behandling
- platsen för underbiträdets behandling av personuppgifter

Vad gäller plats för underbiträdets behandling av personuppgifter ska detta anges som EU/EES om behandlingen sker inom EU/EES. Sker behandlingen i tredjeland, dvs. utanför EU/EES ska landet för behandlingen anges.

Vid behandling av personuppgifter i tredjeland ska även anges vilken grund enligt bilaga 3 som åberopas för överföringen av personuppgifterna till tredjeland, samt hur Europeiska dataskyddsstyrelsens (EDPB) rekommendationer 01/2020 uppfylls när dessa är tillämpbara.

1. [Infoga underbiträdets namn, underbiträdets organisationsnummer och säte, kategorier av personuppgifter, underbiträdets ändamål med behandlingen och platsen för underbiträdets behandling.]
2.

Kommenterad [FR3]: OBS.

Kommenterad [FB4R3]: Biträdet bör snarare ge information om underbiträdet.

Kommenterad [FR5]: Vilka är dessa? Finns det information om det någon annanstans?

Personuppgiftsbiträdesavtal – Bilaga 2 (Instruktioner för behandling av personuppgifter)

För behandlingen av personuppgifter ska Personuppgiftsbiträdet utöver vad som följer av Konsortialavtalet, Uppdragsöverenskommelsen och detta PUBA följa nedan angivna instruktioner.

1. Ändamål och varaktighet

Behandling av personuppgifter enligt detta PUBA får endast ske i syfte att:
Utföra förvaltnings-, support, drift- och utvecklingstjänster.

Behandlingen är begränsad till att:
Lagra och bearbeta de personuppgifter som Personuppgiftsansvarige har i Ladoksystemet, och svara på förfrågningar från och tillhandahålla support till den Personuppgiftsansvarige. Huvudsyftet med behandlingen är att uppfylla kraven i förordning (1993:1153) om redovisning av studier m.m. vid universitet och högskolor.

Personuppgifter i Ladoksystemet får inte lämnas ut till någon annan än den Personuppgiftsansvarige på medium för automatiserad behandling förutom i de fall som framgår av 2 kap. 6 § förordningen (1993:1153) om redovisning av studier m.m. vid universitet och högskolor.

Personuppgifterna ska förvaras i:
Ladoksystemet så länge som syftet för behandlingen av personuppgifterna kvarstår i enlighet med Konsortialavtalet, Uppdragsöverenskommelsen och detta PUBA.

2. Kategorier av Registrerade

Behandlingen inkluderar personuppgifter om:

- studenter
- deltagare i uppdragsutbildningar

3. Kategorier av Personuppgifter

Behandlingen inkluderar dessa kategorier av personuppgifter:
Namn, personnummer, postadress, telefonnummer, e-postadress, behörighet, urvalsgrund, skyldighet att betala anmälningsavgift och studieavgift, antagning, deltagande i utbildning och prov, studieresultat, betyg, tillgodoräknande av utbildning eller annan tillgodoräknad verksamhet, examen, samt avstängning och avskiljande från utbildning.

Behandlingen kan i vissa fall inkludera känsliga personuppgifter enligt artikel 9 GDPR eller uppgifter om lagöverträdelser enligt artikel 10 GDPR. Även uppgifter om en enskilds identitet, adress eller liknande uppgifter om en enskilds personliga förhållanden som omfattas av sekretess enligt 23 kap. 5 § OSL behandlas i systemet.

4. Upphörande av behandling av personuppgifter

Personuppgiftsbiträdet ska vid avslutad behandling återlämna personuppgifterna i ett allmänt och läsbart elektroniskt standardiserat format till den Personuppgiftsansvarige eller till den som den Personuppgiftsansvarige anvisar. När den Personuppgiftsansvarige har bekräftat läsbarheten av de överlämnade personuppgifterna ska Personuppgiftsbiträdet radera personuppgifterna så snart det är tekniskt möjligt, dock senast inom 90 dagar, från sådana

system som använts vid behandlingen på ett sådant sätt att personuppgifterna inte kan återskapas, såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt.

På begäran ska Personuppgiftsbiträdet lämna ett skriftligt besked om vilka åtgärder som vidtagits med personuppgifterna i samband med att behandlingen slutförts. Personuppgiftsbiträdet ska säkerställa att underbiträden vidtar samma åtgärder.

5. Tillåten behandling

Personuppgiftsbiträdet får endast behandla personuppgifterna för att fullgöra det uppdrag som framgår av Konsortialavtalet, Uppdragsöverenskommelsen, detta PUBA och i enlighet med de instruktioner som lämnats av den Personuppgiftsansvarige.

Personuppgifterna får behandlas endast för ovanstående ändamål för den Personuppgiftsansvariges räkning. Personuppgiftsbiträdet får inte behandla personuppgifterna för några andra ändamål.

Personuppgiftsbiträdet ska behandla personuppgifterna i enlighet med vid var tid gällande dataskyddslagstiftning.

Vid osäkerhet om behandling, rutiner eller instruktioner ska den Personuppgiftsansvarige tillfrågas.

Personuppgiftsbiträdesavtal – Bilaga 3 (Överföring av personuppgifter till tredjeland)

Personuppgiftsbiträdet äger inte rätt att överföra personuppgifter till tredjeland eller en internationell organisation utan att den Personuppgiftsansvarige först har lämnat sitt skriftliga samtycke till en sådan överföring.

En överföring till tredjeland förutsätter under alla förhållanden (det vill säga, även för de fall där den Personuppgiftsansvarige har lämnat sitt skriftliga samtycke) att någon av följande förutsättningar är uppfyllda:

- mottagarlandet säkerställer en adekvat skyddsnivå för personuppgifter enligt artikel 45 GDPR,
- lämpliga skyddsåtgärder har vidtagits för överföringen enligt artikel 46 GDPR – till exempel genom användande av EU-kommissionens standardavtalsklausuler eller att mottagaren har fått sina bindande företagsbestämmelser godkända av behörig tillsynsmyndighet i enlighet med artikel 47 – med ytterligare skyddsåtgärder för att upprätthålla en i allt väsentligt samma nivå av skydd för grundläggande fri- och rättigheter som råder inom EU och som uppfyller Europeiska dataskyddsstyrelsens (EDPB) rekommendationer 01/2020.

Kommenterad [FR6]: Hur bestäms detta i praktiken? Det kan ju, trots rekommendationer, vara en tolkningsfråga. Ex. Vad är tillräcklig kryptering vid en överföring?

Personuppgiftsbiträdesavtal – Bilaga 4 (Säkerhet för personuppgifter)

Personuppgiftsansvarige har vid informationsklassning bedömt att uppgifterna i Ladoksystemet har behov av utökat skydd i enlighet med MSB:s föreskrifter MSBFS 2020:7 och MSBFS 2020:8 vad gäller konfidentialitet, riktighet och spårbarhet.

Vid bedömning av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandlingen medför, i synnerhet för 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.

1. Grundläggande säkerhetskrav

Personuppgiftsbiträdet ska säkerställa en säkerhetsnivå som är lämplig i förhållandet till riskerna med behandlingen. För att åstadkomma lämplig säkerhetsnivå ska Personuppgiftsbiträdet utöver kraven i detta PUBA punkt 6.2 se till att minst följande säkerhetskrav är uppfyllda:

- ett systematiskt och riskbaserat informationssäkerhetsarbete bedrivs med stöd av standarderna SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002,
- vilken eller vilka befattningar som ansvarar för att införa, förvalta, följa upp och utvärdera säkerhetsåtgärder i Ladoksystemet dokumenteras,
- förmåga säkerställs att hantera incidenter och avvikelser för att:
  1. skyndsamt upptäcka och bedöma incidenter och avvikelser, och
  2. återställa manipulerad eller förlorad information.
- endast behöriga personer hos Personuppgiftsbiträdet har tillgång till personuppgifterna,
- där det behövs och det är möjligt ska behöriga personers ansvar och ansvarsområden som står i konflikt med varandra vara separerade (separation of duties),
- de ansvarsområden som inte kan vara separerade och orsaken till detta dokumenteras,
- arbetsrutiner och arbetsuppgifter är utformade på ett sådant sätt att det blir möjligt för behöriga personer att arbeta och tänka säkerhetsmedvetet,
- behöriga personer som har tillgång till Personuppgiftsansvariges information ska ha en adekvat utbildning, erfarenhet och kompetens för sina arbetsuppgifter, och
- behöriga personer informeras om vikten av att följa gällande säkerhetsrutiner.

2. Förvaltning, drift och utveckling

Personuppgiftsbiträdet ska beakta relevanta bestämmelser och allmänna råd i MSB:s föreskrifter MSBFS 2020:7[1,2] och MSBFS 2020:8[3] för att åstadkomma lämplig säkerhetsnivå avseende:

- dokumentation av IT-miljön,
- utveckling-, test-, och utbildningsmiljöer,
- uppdelning i nätverkssegment,
- filtrering av nätverkstrafik,
- behörigheter, digitala identiteter och autentisering,

[1] https://www.msb.se/sv/regler/gallande-regler/krisberedskap-och-informationssakerhet/msbfs-20207/
[2] https://www.informationssakerhet.se/vagledning-till-msbfs-20207/
[3] https://www.msb.se/sv/regler/gallande-regler/krisberedskap-och-informationssakerhet/foreskrifter-om-rapportering-av-it-incidenter-for-statliga-myndigheter-msbfs-20208/

- kryptering,
- säkerhetskonfigurering,
- säkerhetstester och granskningar,
- ändringshantering, uppgradering och uppdatering,
- robust och korrekt tid,
- säkerhetskopiering,
- säkerhetsloggning och övervakning,
- skydd mot skadlig kod,
- skydd av utrustning,
- redundans och återställning, och
- hantering av IT-incidenter.

3. Personuppgiftsincidenter

Personuppgiftsbiträdet ska skyndsamt, dock senast inom 24 timmar, efter upptäckt av en personuppgiftsincident informera den Personuppgiftsansvarige via e-postadress [e-postadress lämpligen till den Personuppgiftsansvariges incidentorganisation] om att en personuppgiftsincident har inträffat.

Kommenterad [FR7]: Även information om misstänkta personuppgiftsincidenter och den bedömning som gjorts av att det inte är en personuppgiftsincident bör kommuniceras med den personuppgiftsansvariga.

Personuppgiftsbiträdet ska göra de rimliga efterforskningar som krävs för att kunna identifiera orsaken/orsakerna till personuppgiftsincidenten och vidta de åtgärder som är nödvändiga och rimliga inom sin kontroll för att återställa säkerheten.

Personuppgiftsbiträdet ska dokumentera alla incidenter enligt ovan, inklusive dess effekter och vidtagna åtgärder och göra dessa tillgängliga för den Personuppgiftsansvarige.

Dokumentationen gällande personuppgiftsincidenten ska i första hand skickas via e-post till e-postadressen [e-postadress lämpligen till den Personuppgiftsansvariges incidentorganisation] (om det är lämpligt med beaktande av informationens känslighet) och innehålla all nödvändig och tillgänglig information som den Personuppgiftsansvarige behöver för att kunna vidta lämpliga förebyggande åtgärder och motåtgärder samt uppfylla sina skyldigheter avseende anmälan av personuppgiftsincidenter till behörig tillsynsmyndighet samt upprätta en lokal förteckning över incidenter. Om Personuppgiftsbiträdet inte kan lämna all nödvändig dokumentation vid den initiala rapporteringen, ska Personuppgiftsbiträdet skyndsamt komplettera med nödvändig dokumentation till den Personuppgiftsansvarige.