Förslag till nytt Personuppgiftsbiträdesavtal

I samband med att Dataskyddsförordningen träder i kraft den 25 maj 2018 så behöver personuppgiftsbiträdesavtalet mellan konsortiets parter och konsortiet uppdateras.

Ett förslag till nytt Personuppgiftsbiträdesavtal har tagits fram i samarbete med Johan Lundberg Karlsson, Universitetsjurist Luleå tekniska universitet och Magnus Hjort, Biträdande stabschef Universitet och högskolerådet.

Parter i Ladokkonsortiet bereds nu tillfälle att yttra sig över förslaget.

Om ni avstår från att lämna synpunkter önskas besked även om detta.

Remissvaren skall ha inkommit **senast 2018-04-27**, i elektronisk form under adress info@ladok.se .

Personuppgiftsbiträdesavtal

Detta personuppgiftsbiträdesavtal utgör bilaga till Konsortialavtal för Ladokkonsortiet beslutat av stämman 2017-11-23 och har träffats mellan:

Personuppgiftsansvarig: Respektive partshögskola (’Högskolan’)

Personuppgiftsbiträde: Ladokkonsortiet (’Konsortiet’)

Parterna ovan benämns härefter gemensamt som ”Parterna” och var för sig som ”Part”.

1 Definitioner

I den mån Europaparlamentets och rådets förordning (EU) 2016/679 (”Dataskyddsförordningen”) innehåller begrepp som motsvarar dem som används i avtalet ska sådana begrepp tolkas och tillämpas i enlighet med Dataskyddsförordningen.

I avtalet ska nedan angivna termer ha följande betydelse:

Avtalet

Detta personuppgiftsbiträdesavtal samt ändringar och tillägg till detta personuppgiftsbiträdesavtal som vidtagits i enlighet med bestämmelserna i detta personuppgiftsbiträdesavtal.

Behandling/Behandla

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.

Personuppgift

Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Personuppgiftsansvarig

Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Personuppgiftsbiträde

Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

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

Den som en personuppgift avser.

Tillämpliga bestämmelser

Bestämmelser och praxis hänförlig till Dataskyddsförordningen och svensk kompletteringslagstiftning till Dataskyddsförordningen.

Underbiträde

Den som behandlar personuppgifter enligt instruktioner av Konsortiet.

2 Bakgrund och syfte

2.1 Inom åtagandena som följer av Konsortialavtalet kommer Konsortiet att behandla personuppgifter samt annan information för Högskolans räkning.

2.2 I syfte att uppfylla kravet på skriftligt avtal i art. 28.3 Dataskyddsförordningen, ingår Parterna detta avtal för att reglera behandlingen av personuppgifter vid drift av den nya systemgenerationen av Ladok.

2.3 Avtalet gäller därvid all behandling som Konsortiet i egenskap av ansvarig för driften av det nya Ladoksystemet utför för Högskolans räkning.

2.4 Avtalet är uttömmande vad gäller Konsortiets behandling av Högskolans personuppgifter. Avtalet gäller så länge Konsortiet behandlar personuppgifter för Högskolans räkning.

3 Högskolans skyldigheter

3.1 Högskolan ska ansvara för att all behandling av personuppgifter sker i enlighet med avtalet och tillämpliga bestämmelser.

3.2 Högskolan ska tillhandahålla Konsortiet med den korrekta information och de personuppgifter som behövs och är ändamålsenliga för att denne ska kunna fullgöra sina skyldigheter enligt avtalet och tillämpliga bestämmelser.

4 Konsortiets ansvarsområden

4.1 Konsortiet, och dess underbiträden, ska endast behandla personuppgifter för Högskolans räkning i enlighet med Högskolans instruktioner, enligt detta avtal och tillämpliga bestämmelser. Konsortiet får inte, utan Högskolans samtycke, föreläggande från Datainspektionen eller tvingande lagstiftning

- samla in eller lämna ut personuppgifter från eller till någon tredje part om inte annat skriftligen överenskommits,
- ändra metod för behandling,
- kopiera eller återskapa personuppgifter

4.2 Konsortiet får inte överföra några personuppgifter till en stat utanför EU-området eller till en stat som inte omfattas av undantagen till förbud mot överföring till tredje land enligt tillämpliga bestämmelser. Förbudet omfattar även service, teknisk support, underhåll, utveckling och liknande tjänster av systemet.

En överföring som inte omfattas av ovanstående kräver Högskolans skriftliga samtycke och ett säkerställande av att sådan överföring sker i överensstämmelse med tillämpliga bestämmelser.

4.3 Konsortiet ska genomföra ändringar, raderingar, begränsningar och överföringar på Högskolans uttryckliga begäran, dock inte om en sådan begäran strider mot avtalet eller tillämpliga bestämmelser.

4.4 Konsortiet ska föra en skriftlig förteckning, inbegripet i elektronisk form, över alla kategorier av behandling som utförs för Högskolans räkning, som omfattar följande:

- Namn och kontaktuppgifter för Konsortiet och Högskolan för vars räkning Konsortiet agerar, och, i tillämpliga fall, för Högskolans eller Konsortiets företrädare samt dataskyddsombudet.
- De kategorier av behandling som har utförts för Högskolans räkning.
- I tillämpliga fall, överföringar av personuppgifter till ett tredje land eller en internationell organisation, inbegripet identifiering av tredje landet eller den internationella organisationen och dokumentationen av lämpliga skyddsåtgärder.

- Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna.

4.5 Konsortiet ska utan onödigt dröjsmål underrätta Högskolan i händelse av att behandlingen strider mot avtalet, Dataskyddsförordningen eller annan lagstiftning. Konsortiet ska därefter invänta instruktioner från Högskolan.

4.6 Konsortiet får inte lämna ut personuppgifter eller information om behandlingen av Personuppgifter utan medgivande i förväg från Högskolan utom för det fall föreläggande finns därom från Datainspektionen eller om Konsortiet är skyldig att göra det enligt tillämpliga bestämmelser.

4.7 Konsortiet ska utan onödigt dröjsmål meddela Högskolan om Konsortiet kontaktas av Datainspektionen, registrerad eller tredje part i syfte att få tillgång till personuppgifter som Konsortiet behandlar.

4.8 Högskolan äger rätt att, själv eller genom tredje man, genomföra revision gentemot Konsortiet eller på annat sätt kontrollera att Konsortiets behandling av personuppgifter följer avtalet och tillämpliga bestämmelser. Vid sådan revision eller kontroll ska Konsortiet ge Högskolan den assistans som behövs för genomförande av revision.

4.9 Konsortiet ska bereda Högskolan tillgång till lokaler och utrustning för inspektion i syfte att säkerställa att Konsortiet uppfyller sina skyldigheter enligt avtalet och tillämpliga bestämmelser. Högskolan har dock inte sådan rätt när tillgången och/eller inspektionen kan medföra säkerhets- eller integritetsrisker för de registrerade.

4.10 Konsortiet ska på begäran och utan onödigt dröjsmål visa att förpliktelserna enligt avtalet och tillämpliga bestämmelser efterlevs. Detta innefattar bland annat, men inte uteslutande, en skyldighet att tillhandahålla dokumentation, visa att godkända uppförandekoder eller certifieringar är uppfyllda samt möjliggöra och bidra till att Högskolan kan utföra nödvändiga granskningar och inspektioner.

4.11 Konsortiet ska ge Högskolan tillgång till alla de personuppgifter som Konsortiet behandlar för Högskolans räkning. Detta innefattar även tillgång till upplysningar och handlingar som Högskolan behöver för att utöva kontroll över Konsortiets efterlevnad av avtalet och tillämpliga bestämmelser. En sådan tillgång ska ges utan oskäligt dröjsmål.

4.12 Konsortiet ska vid behov och på begäran bistå Högskolan med fullgörande av de skyldigheter som denne har och som härrör från bestämmelserna i

Dataskyddsförordningen angående utförandet av konsekvensbedömningar avseende dataskydd och förhandssamråd med Datainspektionen.

4.13 Konsortiet ska vid behov och på begäran bistå Högskolan med fullgörande av de skyldigheter som denne har och som härrör från bestämmelserna i Dataskyddsförordningen angående de registrerades rättigheter.

5 Säkerhet

5.1 Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska Konsortiet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt

- pseudonymisering och kryptering av personuppgifter
- förmågan att fortlöpande säkerställa konfidentialitet, integritet och tillgänglighet,
- 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.

5.2 Konsortiet ska utvärdera riskerna med behandlingen och vidta åtgärder, såsom kryptering, för att minska dem.

5.3 Konsortiet ska vidta åtgärder för att säkerställa att varje fysisk person och juridisk person som utför arbete under Konsortiets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktioner från Högskolan.

5.4 Konsortiet ansvarar för att varje fysisk person som har tillgång till personuppgifterna som behandlas enligt avtalet har tillräckliga kunskaper och utbildning för att på ett säkert och ändamålsenligt sätt behandla Personuppgifterna.

5.5 Om Konsortiet avser att genomföra förändringar av hur personuppgifter behandlas eller i övrigt genomföra förändringar som kan påverka säkerheten för de registrerade, de registrerades rättigheter eller efterlevnaden av avtalet eller tillämpliga bestämmelser ska

Konsortiet informera Högskolan i förväg. Högskolan ska ge sitt samtycke till sådana förändringar.

5.6 Konsortiet förbinder sig att behandla personuppgifter och annan information som uppvisar samband med avtalet i enlighet med gällande sekretesslagstiftning. Personalen som behandlar personuppgifter har ingått särskilda sekretessförbindelser samt upplysts om att tystnadsplikt föreligger enligt avtal eller gällande rätt.

5.7 Konsortiet ska tillse att samtliga anställda, konsulter och övriga som Konsortiet svarar för och som behandlar personuppgifter är bundna av ett ändamålsenligt sekretessåtagande samt att de är informerade om hur behandling av personuppgifterna får ske.

5.8 Konsortiet ansvarar för att de personer som har åtkomst till personuppgifterna är informerade om hur de får behandla personuppgifterna i enlighet med instruktionerna från Högskolan. Konsortiet ska även säkerställa att adekvat behörighetsstyrning.

5.9 Vid en misstänkt eller upptäckt Personuppgiftsincident ska Konsortiet omedelbart undersöka incidenten och vidta lämpliga åtgärder för att mildra dess potentiella negativa effekter.

5.10 Om Högskolan begär det ska en beskrivning av Personuppgiftsincidenten lämnas till Högskolan inom 48 timmar. En sådan beskrivning ska åtminstone innehålla

a) beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,

b) förmedla namnet på och kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas,

c) beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och

d) beskriva de åtgärder som Konsortiet har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

5.11 Konsortiet ska bistå Högskolan med att se till att dennes skyldigheter enligt tillämpliga bestämmelser om personuppgiftsincidenter fullgörs, med beaktande av typen av behandling och den information som Konsortiet har att tillgå. Detta gäller även om Högskolan misstänkt eller upptäckt en personuppgiftsincident.

5.12 Konsortiet ska underrätta Högskolan utan onödigt dröjsmål, dock senast inom 24 timmar, efter att ha fått vetskap om en personuppgiftsincident.

5.13 En underrättelse enligt ovan ska innehålla all den information som Högskolan behöver för att uppfylla sina skyldigheter i förhållande till Datainspektionen.

5.14 Ovanstående underrättelseskyldighet till Högskolan gäller även om Konsortiet av någon annan anledning inte kan uppfylla åtaganden enligt avtalet alternativt får kännedom om att personuppgifter har behandlats i strid med avtalet.

6 Anlitande av underbiträde

6.1 Genom detta avtal har Högskolan till Konsortiet lämnat ett allmänt skriftligt förhandstillstånd för anlitande av underbiträde. Konsortiet ska informera Högskolan om eventuella planer på att anlita nya underbiträden eller ersätta underbiträden, så att Högskolan har möjlighet att göra invändningar mot sådana förändringar. En sådan invändning utgör hinder för Konsortiet att genomföra föreslagen förändring.

6.2 Konsortiet ska vidta de åtgärder som krävs för att säkerställa att underbiträdet upprätthåller en tillräcklig skyddsnivå för de personuppgifter som behandlas samt i övrigt följer tillämpliga delar av avtalet och tillämpliga bestämmelser.

7 Ansvar för skada

7.1 Konsortiet ska hålla Högskolan skadeslös i händelse att Högskolan åsamkas skada som är hänförlig till Konsortiets eller dess underbiträdens behandling av personuppgifter i strid med avtalet eller tillämpliga bestämmelser.

8 Avtalets varaktighet samt ändringar i avtalet

8.1 Avtalet gäller från dess att det har undertecknats av Parterna och har samma avtalstid som konsortialavtalet. Avtalet upphör att gälla med omedelbar verkan om någon av Parterna säger upp det.

8.2 När Konsortiets uppdrag att behandla Högskolans personuppgifter upphör ska Konsortiet skyndsamt överlämna personuppgifterna på av Högskolan angivet medium och se till att det inte finns några uppgifter kvar i de egna systemen.

8.3 Högskolan får endast företa ändringar i avtalet i den mån det behövs för att efterleva gällande rätt.

8.4 Konsortiet äger inte rätt att påkalla ändringar i avtalet.

9 Underrättelser

9.1 Underrättelser och meddelanden enligt avtalet ska ske skriftligen. Underrättelser ska ställas till den som är Högskolans lokala objektägare. Personuppgiftsincidenter ska alltid anmälas per e-mail till den lokala objektägaren.

10 Tillämplig lag och tvister

10.1 Avtalet ska tolkas och tillämpas i enlighet med svensk rätt (utan tillämpning av dess lagvalsregler).

10.2 Tvister i anledning av detta avtals tillkomst, tillämpning eller tolkning, så och annan tvist som har sin upprinnelse i detta avtal, ska avgöras av särskild skiljeman. Sådan skiljeman utses av Sveriges universitets- och högskoleförbund. Plats för skiljeförfarande är Stockholm, Sverige.