Datainspektionen

Datum	Diarienr
2013-04-17	1823-2012

AEA
Box 3536
103 69 STOCKHOLM

Tillsyn enligt PuL (1998:204) – Akademikernas arbetslöshetskassa

Datainspektionens beslut

Datainspektionen konstaterar att Akademikernas arbetslöshetskassa är personuppgiftsansvarig för den behandling av medlemmarnas personuppgifter som sker för kassans räkning i systemen Melos, ÄGA och OAS.

Datainspektionen förelägger med stöd av 45 § personuppgiftslagen Akademikernas arbetslöshetskassa att:

- vidta åtgärder för att begränsa åtkomsten till känsliga personuppgifter i inskannade läkarintyg så att de inte blir tillgängliga för handläggare som inte har behov av uppgifterna i intygen,
- kompletterar informationen som lämnas till medlemmarna och blivande medlemmar så att den uppfyller kraven enligt 23-25 § personuppgiftslagen, (se s. 9),
- vidta åtgärder för att avskilja personuppgifter som inte behöver användas i den dagliga verksamheten,
- införa loggning i systemen Melos och ÄGA/OAS av åtkomst till uppgifter även när uppgifterna inte ändras eller tas bort, att ta fram rutiner för att loggarna följs upp och att se till att användarna får information om förekomsten av loggningen.

Datainspektionen förutsätter att Akademikernas arbetslöshetskassa:

- tar fram skriftliga instruktioner för vad som får antecknas i fritextfält och rutiner för att upptäcka och ta bort uppgifter som av integritetsskäl inte ska finnas i dessa fält,

Postadress: Box 8114, 104 20 Stockholm
Besöksadress: Drottninggatan 29, plan 5
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00
Telefax: 08-652 86 52

- upphör med behandlingen av personuppgifter som inte måste bevaras enligt arkivlagstiftningen och som inte heller är nödvändiga att behandla (inkl. bevara) med hänsyn till ändamålet med behandlingen,
- genomför det planerade arbetet med införandet av e-legitimationer för autentisering av användarna i Internetkassan eller inför likvärdig säkerhet för autentisering.

Ärendet avslutas men kan komma att följas upp.

Redogörelse för tillsynsärendet

Datainspektionen har den 22 januari 2013 genomfört en inspektion hos Akademikernas arbetslöshetskassa (AEA). Inspektionen har inte föranletts av något klagomål utan är ett led i Datainspektionens projekt avseende arbetslöshetskassor. Syftet med inspektionen är att kontrollera hur kassan behandlar personuppgifter om sina medlemmar.

Vid inspektionen och senare skriftväxling med AEA har i huvudsak följande framkommit.

Allmänt om verksamheten

AEA är den arbetslöshetskassa i Sverige som har flesta medlemmar. I dag är cirka 652 000 personer medlemmar i AEA. Andelen ersättningsberättigade arbetslösa medlemmar är cirka 1 % (om medlemmar som får aktivitetsstöd från Försäkringskassan räknas med är andelen cirka 2 %). AEA har 130 anställda och har inget annat kontor än det i Stockholm.

AEA använder sig av flera IT-system vilka delvis är integrerade med varandra. Medlemssystemet Melos, ärendehanteringssystemet ÄGA samt Internetkassan har utvecklats av Arbetslöshetskassornas samarbetsorganisation (SO) som även har utvecklingsansvaret för OAS i vilket ersättningsbetalningar hanteras. AEA köper nyttjanderätt till systemen från SO. Driften av AEA:s system sköts av företaget Softronic med vilka AEA har biträdesavtal.

Det är SO som beslutar om den tekniska strukturen i ÄGA, OAS och Internetportalen. Varje arbetslöshetskassa bestämmer själv vilken leverantör som ska sköta driften. Det finns ingen gemensam databas med uppgifter om flera kassors medlemmar. På uppdrag av arbetslöshetskassorna sköter dock SO driften av en gemensam informationsutbytesplattform. AEA har möjlighet att styra utveckling av systemen genom att medverka i samarbetet inom SO.

Behandling av personuppgifter i medlemsärenden

Ansökan om medlemskap kan göras genom en skriftlig ansökan via post eller via AEA:s webbplats. Om den sökande använder e-legitimation för autentisering på webbplatsen behöver denne inte skicka in en undertecknad ansökan till AEA. I annat fall kan ett formulär fyllas i, skrivas ut och skickas in med post till AEA.

På AEA:s webbplats lämnas numera information om AEA:s personuppgiftsbehandling samt om rätten till registerutdrag och till rättelse.

Vid ansökan ska personnummer och vissa kontaktuppgifter anges. AEA registrerar inte uppgift om fackföreningstillhörighet om inte medlemmen anger det frivilligt. Ett villkor för medlemskap i AEA är att man är akademiker, vilket medlemmar i vissa fackföreningar anses vara enligt AEA. Den som ansöker om medlemskap kan styrka akademikerkravet genom att redovisa sina studier alternativt åberopa medlemskap i fackförening. Den som väljer att åberopa medlemskap i fackförening anger det på medlemsansökan.

En blivande medlem kan ansöka om medlemskap i AEA via sin fackförening, under förutsättning att det är en av åtta fackföreningar som AEA har samarbetsavtal med. Fackföreningen fakturerar då sina medlemmar för medlemsavgiften i både fackföreningen och AEA. I ett sådant fall registrerar AEA medlemmens fackföreningstillhörighet.

Till ansökan ska den sökande bifoga ett intyg som visar att den sökande uppfyller kraven för medlemskap. Intygen kan skickas direkt via ansökningstjänsten på webben eller med post. De intyg som kommer till AEA i pappersform skannas och läggs in i ÄGA.

I Melos finns det möjlighet att sekretessmarkera en medlems uppgifter. En sekretessmarkering innebär att åtkomsten till uppgifterna begränsas till de personer som har en särskild behörighet.

I systemet finns ett fritextsfält som AEA använder för noteringar. Det finns inga skriftliga instruktioner för vad som får antecknas i fritextfältet.

Vid utträde registreras utträdesdatumet och vid uteslutning antecknas även skälen för uteslutningen. Utträdet eller uteslutningen innebär inte att uppgiften om den tidigare medlemmen tas bort. Uppgifterna i Melos har aldrig gallrats och det finns inte heller några rutiner för gallring.

Behandling av personuppgifter i ersättningsärenden m.m.

Behandling av personuppgifter i ersättningsärenden sker i systemen ÄGA och OAS. ÄGA är ett ärendehanteringssystem medan OAS är i huvudsak ett system för beräkning och hantering av ersättningsutbetalningar.

Vid handläggning av ersättningsfrågor kan personuppgifter hämtas om medlemmar från myndigheter och från andra arbetslöshetskassor. Uppgifter om medlemmarna lämnas också till myndigheter och andra arbetslöshetskassor. Detta informationsutbyte sker med stöd av författningsreglerade uppgiftsskyldigheter.

Uppgifter från myndigheter och andra arbetslöshetskassor hämtas endast vid behov. Information från exempelvis Försäkringskassan inhämtas på begäran med en särskild funktion i systemet i ett enskilt ärende. Informationsutbytet är dessutom tekniskt styrt, dvs. handläggaren kan endast fråga efter de uppgifter som definieras i systemet. Informationsinhämtning förutsätter att det finns ett ärende i ÄGA.

I ÄGA finns det möjlighet att göra tjänsteanteckningar och ärendeanteckningar. Ärendeanteckningar är tillfälliga anteckningar som inte sparas. Skriftliga instruktioner om vad en handläggare får och inte får skriva finns inte. AEA har hänvisat till dokumentationsskyldigheten enligt Förvaltningslagen då handläggning av ärenden om arbetslöshetsersättning och medlemskap utgör myndighetsutövning. Vidare har AEA uppgett att det inte är möjligt att på förhand definiera vilka uppgifter som kan ha betydelse för den materiella bedömningen i ett enskilt ärende.

Det sker ingen gallring av medlemsuppgifter i ärendehanteringssystemet och AEA har själva inga rutiner för gallring. Enligt AEA pågår det diskussioner inom SO om att vissa uppgifter bör kunna gallras.

Känsliga personuppgifter förekommer i ÄGA/OAS, exempelvis när en medlem skickar in ett läkarintyg. Intygen skannas in och finns tillgängliga för alla handläggare. Det är inte möjligt att begränsa åtkomsten till dessa uppgifter men på begäran av medlemmen finns möjlighet för AEA att sekretessmarkera alla uppgifter om en medlem i systemen.

Internetkassan

Medlemmarna i AEA kan kommunicera med kassan via Internetkassan som är en tjänst som tillhandahålls via internet. Autentisering av användarna sker idag med användarnamn och lösenord. Arbetet pågår dock inom SO med att

införa autentisering av användarna i Internetkassan med hjälp av e-legitimation.

Autentisering

Inloggningsförfarandet för systemen är oberoende av varandra. För att kunna logga in på systemen Melos, ÄGA och Internetkassan måste en användare först logga in på AEA:s intranät med användarnamn och lösenord.

Inloggning i Melos och ÄGA sker med användarnamn och lösenord. Det finns regler för regelbundna, tvingande byten av lösenord samt för sammansättningen och längden av lösenorden.

Loggning

I ÄGA/OAS loggas alla ändringar och borttagningar av uppgifter. Att en handläggare bara tittar i ett ärende loggas däremot inte. Loggarna gallras inte. AEA har uppgett att loggarna kan ha betydelse för ärendehandläggningen och även mycket gamla uppgifter i loggarna kan ha betydelse för beslut i ersättningsfrågor. Det sker ingen logguppföljning i syfte att kontrollera om någon använder uppgifterna för ett otillåtet ändamål.

Behörighetsstyrning

Beslut om behörighet för en anställd görs av berörd chef. Alla handläggare har åtkomst till samtliga system (med undantag för personer med sekretessmarkering).

Handläggare vid medlemsavdelningen har behörighet att ändra i medlemsregistret samt behörighet att registrera medlemsärenden i ÄGA/OAS men endast åtkomst till försäkringsärenden i ÄGA/OAS. Handläggare av ersättningsärenden har behörighet att registrera försäkringsärenden i ÄGA/OAS men endast åtkomst till medlemsregistret.

Därutöver finns särskilda behörigheter för handläggare som hanterar återkrav och för handläggare som hanterar medlemmar med skyddade personuppgifter (cirka 4 handläggare).

Det finns rutiner för hantering av behörigheter vid handläggares tjänstledighet e.d. samt då handläggare slutar. Kontroll av behörigheterna sker två gånger per år.

Kommunikationssäkerhet

Kommunikationen med Softronic sker krypterat över egen lina. ÄGA är en webbapplikation och kommunikationen sker med https. Kontorsnätverket skyddas med brandvägg mot extern åtkomst.

Övrigt

Vid tecknande av inkomstförsäkring som vissa av Saco-förbunden erbjuder sina medlemmar ger medlemmen försäkringsbolaget Saco SalusAnsvar Försäkring AB skriftlig fullmakt att ta del av medlemmens uppgifter hos AEA. Handläggare vid försäkringsbolaget har ingått förbindelse om tystnadsplikt med AEA.

Skäl för beslutet

Tillämpliga bestämmelser

AEA:s behandling av personuppgifter om medlemmar omfattas i huvudsak av personuppgiftslagen (PuL). Informationsutbyte med myndigheter och andra arbetslöshetskassor sker med stöd av uppgiftsskyldigheter enligt lag eller annan författning.

Personuppgifterna som behandlas i systemen Melos, ÄGA och OAS har strukturerats på ett sådant sätt att de s.k. hanteringsreglerna i PuL är tillämpliga (5 a § PuL).

Personuppgiftsansvar

Ansvarig för en behandling av personuppgifter (personuppgiftsansvarig) är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen (3 § PuL).

Vem som bestämmer över ändamålen avgörs genom en bedömning av de faktiska omständigheterna i det enskilda fallet. Avgörande för denna bedömning är bl.a. varför behandlingen utförs och vem som är initiativtagare till behandlingen. Att bestämma över medlen för behandlingen avser främst att bestämma över de tekniska och organisatoriska medlen för behandlingen, dvs. ”hur” behandlingen ska gå till, t.ex. vilka personuppgifter som ska behandlas, vilka tredje män som ska få tillgång till de behandlade personuppgifter och när uppgifter ska raderas.

Ändamålet med den nu aktuella behandlingen av medlemmarnas personuppgifter är att administrera medlemskap, avgifter och ersättningar enligt bestämmelser i lag och förordningar. Genom att bedriva verksamhet som arbetslöshetskassa får AEA anses ha bestämt ändamålet för behandlingen.

Vad gäller medlen för behandlingen framgår det av ärendet att systemen som AEA använder har utvecklats och förvaltas av SO. Förslag till förändringar av systemen bereds av arbetsgrupper inom SO med representanter från a-kassorna. AEA har beslutat att utvecklingen och förvaltningen av systemen ska ske inom ramarna för det samarbete som sker i SO. Kassan har möjlighet att välja andra system än de som utvecklats av SO även om det skulle vara förenat med praktiska problem. De kan även i viss utsträckning beställa, för kassan skräddarsydda, funktioner av SO. AEA får därför anses ha bestämt medlen för behandlingen.

Mot bakgrund av detta får det anses klarlagt att AEA bestämmer såväl mål som medel för behandlingen av medlemmarnas personuppgifter. Datainspektionen konstaterar därför att AEA är personuppgiftsansvariga för behandlingen av personuppgifter avseende kassans medlemmar i systemen Melos och ÄGA/OAS.

Rättslig grund för behandlingen

För att personuppgifter ska få behandlas enligt PuL måste behandlingen vara tillåten enligt 10 §.

Behandling av personuppgifter som är nödvändig för den myndighetsutövning som AEA utövar har rättsligt stöd i 10 § punkten e PuL. Det gäller främst behandling som sker som ett led i prövningen av ärenden om arbetslöshetsersättning och av ärenden om medlemsavgift för arbetslös medlem. Den behandling av personuppgifter som är nödvändig för uppfyllelse av de författningsstadgade uppgiftsskyldigheterna som åligger AEA har rättsligt stöd i 10 § punkten b PuL.

Datainspektionen bedömer att övrig behandling av medlemmarnas personuppgifter som AEA utför kan ske med stöd av ett samtycke. Det gäller t.ex. behandling av personuppgifter om medlemmar som inte har begärt ersättning.

Behandling av uppgift om medlemskap i fackförening

Uppgift om medlemskap i fackförening är en känslig personuppgift som enligt PuL är förbjuden att behandla utom vissa i lagen särskilt angivna fall (13-19

§§). Det är bl.a. tillåtet att behandla känsliga personuppgifter med den registrerades uttryckliga samtycke (15 § PuL). Fackföreningar får även utan samtycke behandla uppgifter om sina egna medlemmar (17 § PuL).

AEA registrerar uppgift om fackföreningstillhörighet när en ansökan om medlemskap i AEA sker via en fackförening och när en blivande medlem styrker kraven för medlemskap genom att åberopa fackföreningstillhörighet. Detta sker med stöd av ett samtycke.

Datainspektionen vill med anledning av ovanstående lämna följande information. För att ett samtycke till behandling av känsliga personuppgifter ska vara giltigt krävs det att den blivande medlemmen aktivt ger uttryck för godkännande av behandlingen efter att ha fått information om hur dennes personuppgifter kommer att behandlas. Ett så kallat konkludent samtycke är i normalfallet inte godtagbart som samtycke till behandling av känsliga personuppgifter eftersom ett sådant samtycke måste vara uttryckligt.

Åtkomst till uppgifter om hälsa

En förutsättning för att en medlem ska få arbetslöshetsersättning då denne har lämnat ett arbete av hälsoskäl är att han eller hon lämnar in läkarintyg (19 c § förordningen (1997:835) om arbetslöshetsförsäkring). De läkarintyg som lämnas in till AEA skannas och blir tillgängliga i ÄGA/OAS.

Läkarintyg innehåller uppgift om hälsa vilket enligt PuL är en känslig personuppgift som är förbjuden att behandla utom vissa i lagen särskilt angivna fall (13-19 §§). Systemen hos AEA är visserligen utformade så att det inte går att söka på innehållet i de inskannade dokumenten men dokumenten är tillgängliga för alla handläggare. Endast om en medlems uppgifter har sekretessmarkerats begränsas tillgången till uppgifterna.

En grundläggande princip är att handläggare endast ska ha tillgång till uppgifter som de behöver i sitt arbete. Det kan därför ifrågasättas om andra handläggare än den som bedömer läkarintygets innehåll behöver ha tillgång till de inskannade dokumenten. De inskannade läkarintygen bör avskiljas så att de inte är direkt tillgängliga för handläggare som inte har behov av uppgifterna i intygen.

Vilken tillgång till personuppgifter som en enskild handläggare behöver för att kunna fullgöra sina arbetsuppgifter är naturligtvis i första hand upp till AEA att bedöma. Om det inte är möjligt att införa tekniska begränsningar så är det än viktigare att AEA på andra sätt aktivt arbetar för att minska riskerna

för åtkomst av personuppgifter som handläggarna inte behöver för sina arbetsuppgifter.

Datainspektionen förelägger AEA att vidta åtgärder för att begränsa åtkomsten till känsliga personuppgifter i inskannade läkarintyg så att de inte blir tillgängliga för handläggare som inte har behov av uppgifterna i intygen.

Fritextfält

Fritextfält ökar risken för att integritetskänsliga uppgifter som inte är relevanta för ärendehanteringen registreras. För att undvika att så sker förutsätter Datainspektionen att AEA tar fram skriftliga instruktioner för vad som får antecknas i fritextfält. De kan t.ex. innehålla uppmaning om att endast anteckna uppgifter som har betydelse för ärendet och ett antal beskrivande exempel på sådana uppgifter. Datainspektionen förutsätter även att AEA tar fram rutiner för att upptäcka och ta bort uppgifter som av integritetsskäl inte ska finnas i dessa fält.

Information till de registrerade

När AEA samlar in personuppgifter från medlemmarna eller blivande medlemmar, t.ex. vid medlemsansökan, ska kassan lämna information om behandlingen av uppgifterna (23 § PuL). Informationen som ska lämnas är bl.a. den personuppgiftsansvariges identitet, ändamålet med behandlingen och all övrig information som krävs för att den registrerade ska kunna ta till vara sina rättigheter, såsom till vem uppgifterna lämnas vidare och möjligheten att få information eller begära rättelse. Det är dock inte nödvändigt att lämna information om sådant som den registrerade redan känner till (25 § PuL).

Även när personuppgifter samlas in från någon annan än de registrerade ska information lämnas till de registrerade (24 § PuL). Denna skyldighet gäller dock inte när det gäller registrering eller utlämnande som sker med stöd av lag eller annan författning. AEA behöver därför inte informera de registrerade om det inhämtande och utlämnade av personuppgifter till myndigheter som sker med stöd av lagen (1997:238) om arbetslöshetsförsäkring (andra stycket). Lagstiftaren har dock betonat vikten av att de registrerade även i dessa fall kan få information om behandlingen. När behandlingen omfattas av en särskild lagstiftning föreskrivs därför vanligtvis en informationsskyldighet. När sådan lagstiftning saknas, såsom för arbetslöshetskassorna, ska det framgå av ändamålsbeskrivningen till vilka myndigheter och organ som personuppgifterna lämnas ut och från vilka myndigheter och organ som personuppgifter hämtas in (prop. 2007/08:160 s. 51).

AEA har således en skyldighet att informera om den personuppgiftsbehandling som inte sker med stöd av lag eller annan författning, vilket främst gäller behandlingen av personuppgifter om medlemmar som inte är arbetslösa. Informationen ska, enligt 23 § PuL, lämnas i samband med att personuppgifterna samlas in. Det kan t.ex. ske genom information på blanketten för medlemsansökan.

Datainspektionen ser positivt på att AEA, som sedan inspektionen numera på deras webbplats informerar om hur medlemmarnas personuppgifter kommer att behandlas, påbörjat ett arbete med att lämna information på samtliga blanketter som kan hämtas på deras webbplats. Datainspektionen förutsätter att arbetet fortsätter och slutförs samt att informationen som lämnas till medlemmarna och blivande medlemmar uppfyller kraven i 23-25 §§ PuL. Sådan information ska innehålla:

- uppgifter om den som är personuppgiftsansvarig, t.ex. namn, adress, telefonnummer, organisationsnummer och e-postadress,
- uppgift om ändamålen med behandlingen, det vill säga varför personuppgifterna registreras och hur de ska användas,
- övrig information som den registrerade behöver känna till, som exempelvis vilka typer av personuppgifter som ska behandlas, till vilka företag eller andra organisationer (eller typer av dessa) som uppgifterna kan komma att lämnas ut, om det är frivilligt för den registrerade att lämna uppgifter, att den registrerade har rätt att begära ett registerutdrag för att kunna kontrollera vilken information som finns registrerad om honom eller henne, att den personuppgiftsansvarige är skyldig att på begäran av den registrerade rätta uppgifter som är felaktiga, ofullständiga eller missvisande.

Information som medlemmen eller den blivande medlemmen kan förväntas känna till behöver dock inte AEA lämna.

Informationsutbytet med myndigheter m.fl.

Datainspektionen har översiktligt granskat det informationsutbyte som AEA har med myndigheter och andra arbetslöshetskassor. Vad som därvid har framkommit föranleder inget påpekande från Datainspektionen.

Gallring

AEA är som personuppgiftsansvarig skyldig att se till att personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen (9 § första stycket punkten i) PuL).

AEA har uppgett att uppgifter i medlemssystemet Melos aldrig har gallrats och att det inte heller finns några rutiner för gallring. Gallring sker inte heller av medlemsuppgifter i ÄGA/OAS. AEA:s bedömning är att uppgifterna inte får gallras eftersom de kan ha betydelse för ärendehandläggningen bl.a. vid beräkning av s.k. överhoppningsbar tid och vid bedömningen av vilka som är ersättningsberättigade

Vissa delar av den verksamhet som AEA bedriver omfattas av tryckfrihetsförordningens bestämmelser om rätten att ta del av allmänna handlingar (2 kap. 4 § och bilaga till offentlighets- och sekretesslagen). Det gäller främst verksamheten som består av prövning av ärenden om arbetslöshetsersättning och av ärenden om medlemsavgift för arbetslös medlem. Uppgifter i allmänna handlingar får gallras under de förutsättningar som framgår av arkivlagen (1990:782), arkivförordningen (1991:446) och Riksarkivets föreskrifter och beslut.

Det är inte Datainspektionens uppgift att ta ställning till vilka handlingar hos AEA som ska gallras enligt arkivlagstiftningen. I den mån uppgifterna inte måste bevaras enligt arkivlagstiftning och uppgifterna inte heller längre behövs med anledning av ändamålet med behandlingen anser dock Datainspektionen att uppgifterna ska gallras.

Datainspektionen förutsätter därför att AEA upphör med behandlingen av personuppgifter som inte måste bevaras enligt arkivlagstiftning och som inte heller är nödvändiga att behandla (inkl. bevara) med hänsyn till ändamålet med behandlingen.

Åtkomst till historiska uppgifter

För uppgifter i allmänna handlingar som inte gallras gäller PuL om handlingarna bevaras i elektronisk form. För tillgången till äldre personuppgifter gäller som utgångspunkt att inte flera personuppgifter behandlas än vad som nödvändigt med hänsyn till ändamålet (9 § första stycket punkten f) PuL). Uppgifter som inte används i den dagliga verksamheten bör därför avskiljas med tekniska begränsningar så att endast personal som har behov av dessa uppgifter i sitt arbete får tillgång till dem.

Det är t.ex. inte lämpligt att det är möjligt att göra obegränsade sökningar bland äldre uppgifter om en viss medlem. Äldre uppgifter bör därför om möjligt avskiljas från ärendehanteringssystemet och läggas i ett s.k. elektroniskt arkiv. Om arkiveringsfunktionen ingår i samma system, bör systemet innehålla tekniska avgränsningar.

Datainspektionen förelägger därför AEA att vidta åtgärder för att avskilja personuppgifter som inte behöver användas i den dagliga verksamheten.

Behörighet

Dokument- och ärendehanteringssystem innehåller stora mängder personrelaterad information. En grundläggande princip är att handläggare endast bör ha elektronisk tillgång till personuppgifter som de behöver för sitt arbete. För att begränsa den elektroniska tillgången ska det finnas ett system för behörighetsstyrning. Med hjälp av detta bör åtkomstmöjligheterna tekniskt begränsas så mycket som det är faktiskt och praktiskt möjligt med hänsyn till den aktuella verksamheten och känsligheten hos personuppgifterna. Därutöver kan obehörig åtkomst begränsas genom fungerande rutiner, t.ex. arbetsrutiner, rutiner för utbildning och information till anställda samt rutiner för åtkomstkontroll.

AEA har uppgett att det är nödvändigt att samtliga handläggare har åtkomst till systemen då alla handläggare svarar i telefon och måste kunna komma åt uppgifter om den medlem som ringer in. Det är förvisso i första hand upp till AEA att avgöra vilken åtkomst en handläggare ska ha för att kunna fullgöra sina arbetsuppgifter men ett sådant upplägg där alla anställda kan titta på alla ärenden medför integritetsrisker. Det kan därför finnas skäl att generellt sett begränsa åtkomsten till personuppgifter. Detta är något som AEA måste överväga. Om det inte är möjligt att införa tekniska begränsningar så är det desto viktigare att AEA på andra sätt aktivt arbetar för att minska riskerna för otillbörlig åtkomst av personuppgifter som handläggare inte behöver för att kunna utföra sina arbetsuppgifter.

Loggning

Den personuppgiftsansvarige är enligt 31 § PuL skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska ställas i relation till de tekniska möjligheter som finns, kostnaderna för åtgärderna, de risker med behandlingen som finns samt de behandlade uppgifternas känslighet.

AEA har uppgett att ändringar och borttagningar av uppgifter i ÄGA/OAS loggas. Däremot loggas inte att en handläggare bara tittar i ett ärende.

Med hänsyn till att känsliga personuppgifter om bl.a. medlemmarnas hälsa och fackföreningstillhörighet behandlas i systemet och att samtliga handläggare har åtkomst till såväl Melos som ÄGA/OAS anser Datainspektionen att

det finns ett behov av att kunna kontrollera att åtkomsten till uppgifterna inte används för ett otillåtet syfte. För en sådan kontroll ska vara möjlig är det nödvändigt att även logga läsning av en medlems personuppgifter i systemen.

Datainspektionen förelägger därför AEA att införa loggning i Melos och ÄGA/OAS av åtkomst till uppgifter även när uppgifterna inte ändras eller tas bort, att ta fram rutiner för att loggarna följs upp och att se till att användarna får information om förekomsten av loggningen.

Säkerhet för Internetkassan

För vissa e-tjänster som tillhandahålls över öppna nät såsom Internet kan det finnas behov av att verifiera identiteten hos användarna (autentisering). Valet av autentiseringsmetod bör utgå från känsligheten hos de personuppgifter som behandlas, mängden uppgifter och de risker som är förknippade med behandlingen. En bedömning av lämpliga säkerhetsåtgärder enligt 31 § PuL måste göras utifrån förutsättningarna i det enskilda fallet.

E-tjänster där användarna kan ta del av känsliga personuppgifter kräver normalt mer avancerade metoder för autentisering, som exempelvis e-legitimation eller engångslösenord. Med känsliga personuppgifter avses här känsliga personuppgifter enligt 13 § PuL och andra uppgifter som annars är särskilt integritetskänsliga, t.ex. uppgifter om lagöverträdelser och uppgifter som är sekretessreglerade.

I Internetkassan kan en medlem bl.a. fylla i s.k. elektroniska kassakort. I kortet kan medlemmen ange om han eller hon har varit sjuk. Uppgift om sjukdom är en sådan känslig personuppgift som avses i 13 § PuL. Redan av den anledningen finns det skäl att överväga en säkrare metod för autentisering än den befintliga.

AEA har uppgett att de deltar i ett arbete inom SO som går ut på att införa autentisering i Internetkassan med hjälp av e-legitimation. Datainspektionen anser att en sådan åtgärd skulle ge en lämplig säkerhet för den avsedda behandlingen.

Datainspektionen förutsätter att AEA genomför det planerade arbetet med införandet av e-legitimationer för autentisering av användarna i Internetkassan eller inför likvärdig säkerhet för autentisering.

Hur man överklagar

Om ni vill överklaga beslutet skall ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Inspektionen måste ha fått ert överklagande inom tre veckor från den dag ni fick ta del av beslutet, annars kan överklagandet inte prövas. Datainspektionen sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av tf generaldirektör Hans-Olof Lindblom i närvaro av tillsynschefen Catharina Fernquist, juristerna Martin Brinnen och Anna Larsson Stattin, föredragande samt informationssäkerhetsspecialisten Adolf Slama.

Hans-Olof Lindblom Anna Larsson Stattin

Kopia:
Inspektionen för arbetslöshetsförsäkringen (IAF)