Datainspektionen

Datum	Diarienr
2013-04-17	1821-2012

Ledarnas arbetslöshetskassa

Box 12110
102 23 STOCKHOLM

Tillsyn enligt personuppgiftslagen (1998:204) – Ledarnas arbetslöshetskassa

Datainspektionens beslut

Datainspektionen konstaterar att Ledarnas 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 Ledarnas arbetslöshetskassa att:

- upphöra att behandla uppgifter om medlemskap i fackförening,
- 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,
- komplettera 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.
- kryptera kommunikationen som sker med Evry via öppet nät.

Datainspektionen förutsätter att Ledarnas a-kassa

- 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,

- 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 följas upp.

Redogörelse för tillsynsärendet

Datainspektionen har den 24 januari 2013 genomfört en inspektion hos Ledarnas arbetslöshetskassa (Ledarnas a-kassa). Inspektionen har inte föranletts av något klagomål utan är ett led i Datainspektionens projekt avseende arbetslöshetskassor. Syftet med inspektionen har varit att kontrollera hur kassan behandlar personuppgifter om sina medlemmar.

Vid inspektionen och senare skriftväxling med Ledarnas a-kassa har i huvudsak följande framkommit.

Allmänt om verksamheten

Ledarnas a-kassa har cirka 82 000 medlemmar. Andelen arbetslösa medlemmar är cirka 3-4 % och andelen ersättningsberättigade medlemmar är under 2 %. Kassan har 20 anställda och har inget annat kontor än det i Stockholm. De är idag helt separerade från fackförbundet Ledarna bortsett från vissa fall av rekrytering av medlemmar.

Ledarnas a-kassa 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. Ledarnas a-kassa har tecknat nyttjanderätt till systemen från SO. Driften av Ledarnas a-kassas system sköts av företaget Evry med vilka Ledarnas a-kassa 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. Ledarnas a-kassa har möjlighet att styra utveckling av systemen genom att medverka i samarbetet inom SO.

Behandling av personuppgifter i medlemsärenden

Ansökan om medlemskap kan endast göras skriftligen och ska vara egenhändigt undertecknad. Det är inte möjligt att ansöka om medlemskap via nätet. Mellan 50 och 100 in- och utträden registreras per dag. Ledarnas a-kassa uppger att uppgifterna om medlemmarna behandlas med stöd av samtycke från de registrerade. På blanketten för medlemsansökan anges numera följande text. ”Genom underskrift godkänner du enligt personuppgiftslagen (PuL) SFS 1998:204 att information och uppgifter får lagras, sparas och bearbetas av Ledarnas arbetslöshetskassa”.

Vid ansökan ska personnummer och vissa kontaktuppgifter anges. Ledarnas a-kassa registrerar inte uppgift om fackföreningstillhörighet i Melos. Däremot framgår facktillhörighet för personer som blev medlemmar innan april 2007 då separationen mellan fackföreningen och a-kassan skedde. A-kassan kan ha behov av den uppgiften för att veta vilken fackförening de ska vända sig till för att få dokumentation om exempelvis tvistiga äldre ärenden.

Till ansökan ska den sökande bifoga ett intyg om att sökanden har en anställning som faller under Ledarnas a-kassas verksamhetsområde. Intygen skannas och läggs in i ÄGA.

I Melos finns det möjlighet att sekretessmarkera medlemsuppgifter. Detta innebär att åtkomsten till uppgifterna är begränsad till de personer som har en särskild behörighet (ca fem handläggare).

I systemet finns ett fritextfält som ledarnas a-kassa använder för noteringar. Muntliga instruktioner om vad som får antecknas har lämnats till de anställda. Det finns inga skriftliga instruktioner, men det kan framgå av vissa minnesanteckningar. Ledarnas a-kassa planerar att ta fram ett samlat dokument med skriftliga instruktioner.

Vid utträde registreras utträdesdatumet och vid uteslutning antecknas även skälen för uteslutningen. Utträdet eller en uteslutning innebär inte att uppgifterna om den tidigare medlemmen tas bort. Uppgifterna i Melos har aldrig gallrats och det finns inte heller några rutiner för gallring. Ledarnas a-kassa uppger att det kan finnas ett behov av att bevara äldre uppgifter, exempelvis om en medlem inte betalar eller vid tvistiga ärenden.

Behandling av personuppgifter i ersättningsärenden m.m.

Behandling av personuppgifter i ersättningsärenden sker i systemen ÄGA och OAS. ÄGA är ett ärendehanterings- och beslutstödssystem medan OAS är i huvudsak ett system för beräkning och hantering av ersättningsutbetalningar. Handläggare loggar in och arbetar endast i ÄGA.

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

Uppgifter från andra myndigheter hämtas vid all ärendehantering som sker i ÄGA/OAS. Viss information kommer automatiskt via batchfiler, t.ex. en lista från Arbetsförmedlingen med personer som inte längre är arbetssökande. Information från exempelvis Försäkringskassan inhämtas på begäran med en särskild funktion i systemet i ett enskilt ärende. Informationsutbytet med myndigheter sker endast enligt de uppgiftsskyldigheter som stadgas i författningar. Informationsutbytet är dessutom tekniskt styrt, dvs. handläggaren kan endast fråga efter de uppgifter som är definierade i systemet. Informationsinhämtning förutsätter också att det finns ett ärende i ÄGA.

I ÄGA finns det möjlighet att göra tjänsteanteckningar samt ärendeanteckningar. Ärendeanteckningarna är tillfälliga anteckningar och kan raderas. Skriftliga instruktioner för vad en handläggare får och inte får skriva finns inte men har kommunicerats muntligen.

En ny informationsutbytesplattform som hanteras av SO började användas för ett år sedan. Syftet med den nya plattformen var att öka säkerheten vid informationsutbytet.

Gallring av medlemsuppgifter i ärendehanteringssystemet har gjorts i samband med att ÄGA togs i bruk för några år sedan. Ledarnas a-kassa har själva inga rutiner för gallring och hänvisar till SO.

Känsliga personuppgifter förekommer i ÄGA/OAS, exempelvis när en medlem skickar in ett läkarintyg. Intygen skannas in och finns tillgängliga för alla ersättningshandläggare. Innehållet i inskannade dokument är inte sökbart och det går inte att få fram dokumenten utan att ange en medlems personnummer.

Internetkassan

Medlemmarna i Ledarnas a-kassa kan kommunicera med kassan via Internetkassan som är en tjänst som tillhandahålls via internet. Autentisering av användarna av Internetkassan sker idag med användarnamn och lösenord. Arbete pågår dock inom SO med att införa autentisering av användarna i Internetkassan med hjälp av e-legitimation.

På det användaravtal som upprättas mellan kassan och användaren av Internetkassan anges följande text: ”Genom underskrift godkänner du enligt per-

sonuppgiftslagen (PuL) SFS 1998:204 att information och uppgifter får lagras, sparas och bearbetas av Ledarnas arbetslöshetskassa."

Säkerhetspolicy

Ledarnas a-kassa har en framtagen IT-säkerhetspolicy som kommuniceras till nyanställda tillsammans med muntliga instruktioner. Hur handläggarna ska arbeta i systemen diskuteras även löpande vid regelbundna möten. Hot- och riskanalys genomförs varje år och är en del i verksamhetsplanen.

Autentisering

Inloggningsförfaranden för systemen är oberoende av varandra. För att kunna logga in på systemen Melos, ÄGA och Internetkassan måste en användare först logga in på Ledarnas a-kassas 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 och OAS loggas alla ändringar och borttagningar av uppgifter. Att en handläggare bara tittar i ett ärende loggas däremot inte. Loggarna gallras inte. Ledarnas a-kassa har uppgett att loggarna kan ha betydelse för ärendehandläggningen och även mycket gamla uppgifter i loggarna kan ha betydelse för beslut i ersättningsfrågor.

Behörighetsstyrning

Chefen för Ledarnas a-kassa beslutar om behörigheter i systemen.

Det finns två grupper av handläggare, medlemshandläggare och ersättningshandläggare. Medlemshandläggare har full behörighet i Melos. I ÄGA har medlemshandläggare läsbehörighet och kan ändra medlemsuppgifter. Ersättningshandläggare har full behörighet i ÄGA men endast läsbehörighet i Melos. Därutöver finns en särskild behörighet för handläggare som hanterar medlemmar med skyddade personuppgifter (5 st). Det finns rutiner för hantering av behörigheter vid handläggares föräldraledighet e.d. samt då handläggare slutar. Kontroll av behörigheterna sker två gånger per år med hjälp av Evry.

Kommunikationssäkerhet

Kommunikationen med driftleverantören Evry och därmed kassan åtkomst till systemen sker via egen okrypterad lina. ÄGA är en webbapplikation och kommunikationen sker med http. Det går bara att komma åt ÄGA när handläggaren loggat in på nätverket. Det finns även en VPN-lösning som endast

kassaföreståndaren har åtkomst till. På grund av dålig uppkoppling används inte denna. Kontorsnätverket skyddas med brandvägg mot extern åtkomst.

Säkerhetskopiering

Säkerhetskopiering sker varje natt och sparas i sju generationer. Kopieringen sker i Evrys skyddade lokaler och klonas till en annan plats med samma säkerhet.

Skäl för beslutet

Tillämpliga bestämmelser

Ledarnas a-kassas behandling av personuppgifter om medlemmar omfattas av personuppgiftslagen. 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 personuppgiftslagen är tillämpliga (5 a § personuppgiftslagen).

Personuppgiftsansvar

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

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 Ledarnas a-kassa anses ha bestämt ändamålet för behandlingen.

Vad gäller medlen för behandlingen framgår det av ärendet att systemen som Ledarnas a-kassa använder har utvecklats och förvaltas av SO. Förslag till förändringar av systemen bereds av arbetsgrupper inom SO med representanter från a-kassorna. Ledarnas a-kassa har beslutat att utvecklingen och förvalt-

ningen 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. Ledarnas a-kassa får därför anses ha bestämt medlen för behandlingen.

Mot bakgrund av detta får det anses klarlagt att Ledarnas a-kassa bestämmer såväl mål som medel för behandlingen av medlemmarnas personuppgifter. Datainspektionen konstaterar därför att Ledarnas a-kassa är personuppgiftsansvariga för den behandling av medlemmarnas personuppgifter som sker för deras räkning i systemen Melos, ÄGA och OAS.

Rättslig grund för behandlingen

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

Behandling av personuppgifter som är nödvändig för den myndighetsutövning som Ledarnas a-kassa utövar har rättsligt stöd i 10 § punkten e personuppgiftslagen. 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 Ledarnas a-kassa har rättsligt stöd i 10 § punkten b personuppgiftslagen.

Övrig behandling av medlemmarnas personuppgifter som Ledarnas a-kassa utför sker, enligt Ledarnas a-kassa, 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 personuppgiftslagen är förbjuden att behandla utom i 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).

Ledarnas a-kassa har uppgett att de inte längre samlar in uppgift om medlemskap i fackförening men att sådan uppgift finns kvar för personer som blev medlemmar innan april 2007 då separationen mellan Ledarnas fackförening och a-kassan genomfördes. Enligt kassan kan de ha behov av uppgift om fackföreningstillhörighet för att veta vilken fackförening de ska vända sig till för att få dokumentation om exempelvis tvistiga äldre ersättningsärenden.

Oavsett med vilken stöd som uppgift om fackföreningsmedlemskap ursprungligen har samlats in ifrågasätter Datainspektionen om Ledarnas a-kassa har behov av uppgiften i sin verksamhet. Behovet av att behandla uppgift om medlemskap i fackförening kan inte anses nödvändig utifrån ändamålet med behandlingen, nämligen att hantera medlems- och ersättningsärenden. Antalet ärenden i vilka det finns behov av att kontrollera dokumentation från tiden innan april 2007 kan rimligen inte vara flera än att kontrollen kan skötas på annat sätt. Om uppgiften om fackföreningstillhörighet inte uppdateras kan det även ifrågasättas om uppgifterna stämmer med dagens situation. Medlemmen kan ha gå ur eller bytt fackförening sedan uppgiften registrerades. Ledarnas a-kassa har också enligt egen uppgift övervägt att ta bort uppgifter om fackföreningstillhörighet.

Mot den bakgrunden anser Datainspektionen att behandlingen av uppgift om fackföreningstillhörighet inte uppfyller de grundläggande kraven på personuppgiftsbehandling enligt 9 § personuppgiftslagen.

Datainspektionen förelägger därför Ledarnas a-kassa att upphöra att behandla uppgifter om medlemskap i fackförening.

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 Ledarnas a-kassa skannas och blir tillgängliga i ÄGA/OAS.

Läkarintyg innehåller uppgift om hälsa vilket enligt personuppgiftslagen är en känslig personuppgift som är förbjuden att behandla utom vissa i lagen särskilt angivna fall (13-19 §§). Systemen hos Ledarnas a-kassa är visserligen utformad 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 till de handläggare som den särskilda behörigheten, f.n. cirka fem handläggare).

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 det inskannade dokumentet. De inskannade läkarintygen bör därför avskiljas genom tekniska åtgärder 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 Ledarnas a-kassa att bedöma. Om det inte är möjligt att införa tekniska begränsningar så är det än viktigare att Ledarnas a-kassa på andra sätt aktivt

arbetar för att minska riskerna för otillbörlig åtkomst av personuppgifter som handläggare inte behöver för utförandet av sina arbetsuppgifter.

Datainspektionen förelägger Ledarnas a-kassa 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 Ledarnas a-kassa 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 Ledarnas a-kassa tar fram rutiner för att upptäcka och ta bort uppgifter som av integritetsskäl inte ska finnas i dessa fält.

Information till de registrerade

När Ledarnas a-kassa 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. Ledarnas a-kassa behöver därför inte informera de registrerade om det inhämtande och utlämnade av personuppgifter till myndigheter som sker med stöd av lagen (1997:238) om arbetslöshetsförsäkringen (25 § 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).

Ledarnas a-kassa har således en skyldighet att informera om sådan personuppgiftsbehandling som inte avser registrerande eller utlämnande med stöd av lag eller annan författning. Det gäller exempelvis behandling av personuppgifter om medlemmar som inte är arbetslösa. Informationen ska, när det gäller personuppgifter som samlas in från person själv, lämnas i samband med insamlingen (23 § PuL). Det kan t.ex. ske genom information på blanketten för medlemsansökan.

På Ledarnas a-kassas blankett för medlemsansökan får den sökande godkänna att ”enligt personuppgiftslagen (PuL) SFS 1998:204 att information och uppgifter får lagras, sparas och bearbetas av Ledarnas arbetslöshetskassa”. Den texten uppfyller inte de krav på information som ska lämnas enligt 25 § personuppgiftslagen.

Datainspektionen förelägger därför Ledarnas a-kassa att komplettera informationen som lämnas till medlemmarna och blivande medlemmar så att den uppfyller kraven enligt 23-25 § personuppgiftslagen. 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 Ledarnas a-kassa lämna.

Informationsutbytet med myndigheter m.fl.

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

Gallring

Ledarnas a-kassa är som personuppgiftsansvarige 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).

Ledarnas a-kassa har uppgett att uppgifter i medlemssystemet Melos aldrig har gallrats och att det inte heller finns några rutiner för gallring. Det är oklart om uppgifter i ÄGA/OAS har gallrats. Enligt kassan kan det finnas ett behov av att bevara äldre uppgifter, exempelvis om en medlem inte betalar eller vid tvistiga ärenden.

Vissa delar av den verksamhet som Ledarnas a-kassa 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 Ledarnas a-kassa som ska gallras enligt arkivlagstiftningen. I den mån uppgifterna inte måste bevaras enligt arkivlagstiftningen och uppgifterna inte heller längre behövs med anledning av ändamålet med behandlingen anser dock Datainspektionen att uppgifterna ska gallras.

Datainspektionen förutsätter därför att Ledarnas a-kassa 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.

Åtkomst till historiska uppgifter

För uppgifter i allmänna handlingar som inte gallras gäller personuppgiftslagen om handlingar 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 Ledarnas a-kassa att vidta åtgärder för att avskilja personuppgifter som inte behöver användas i den dagliga verksamheten.

Loggning

Den personuppgiftsansvarige är enligt 31 § personuppgiftslagen 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.

Ledarnas a-kassa 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 läsbehörighet i 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 när någon läser en medlems personuppgifter i systemen.

Datainspektionen förelägger därför Ledarnas a-kassa 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 § personuppgiftslagen 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 § personuppgiftslagen 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. elektroniskt kassakort. I kortet kan medlemmen ange om han eller hon har varit sjuk. Uppgift om sjukdom är sådan känslig personuppgift som avses i 13 § personuppgiftslagen. Redan av den anledningen finns det skäl att överväga en säkrare metod för autentisering än den befintliga.

Ledarnas a-kassa 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 Ledarnas a-kassa genomför det planerade arbetet med införandet av e-legitimationer för autentisering av användarna i Internetkassan eller inför likvärdig säkerhet för autentisering.

Övriga säkerhetsfrågor

Enligt Datainspektionens uppfattning ska känsliga personuppgifter som kommuniceras via öppet nät, till exempel med e-post, krypteringsskyddas på ett sådant sätt att endast den avsedda mottagaren kan ta del av innehållet.

Med hänsyn till att Ledarnas a-kassa behandlar personuppgifter om ett stort antal person och att behandlingen omfattar känsliga personuppgifter anser Datainspektionen att kommunikationen som sker via den egna linan till Evry måste krypteras.

Datainspektionen förelägger därför Ledarnas a-kassa att kryptera kommunikationen som sker med Evry via öppet nät.

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 Anna Larsson Stattin och Martin Brinnen, föredragande samt informationssäkerhetsexperten Adolf Slama.

Hans-Olof Lindblom

Martin Brinnen

Kopia:
Inspektionen för arbetslöshetsförsäkringen (IAF)