Datainspektionen

Datum	Diarienr
2012-10-09	1673-2011

Folkpartiet Liberalerna
Box 2253
103 16 STOCKHOLM

Tillsyn enligt personuppgiftslagen (1998:204) – Folkpartiet Liberalernas behandling av medlemsuppgifter i ett centralt register

Datainspektionens beslut

Datainspektionen konstaterar att Folkpartiet Liberalerna inte lever upp till de krav som ställs på säkerheten vid behandling av personuppgifter i 31 § personuppgiftslagen genom följande brister:

- Det går att autentisera sig som behörig användare över öppet nät med enbart användarnamn och lösenord och få åtkomst till personuppgifter i medlemsregistret.

Datainspektionen förelägger, med stöd av 45 § första stycket personuppgiftslagen, Folkpartiet Liberalerna att:

- vidta åtgärder som innebär att åtkomst över öppet nät till personuppgifter i det centrala medlemsregistret skyddas med stark autentisering,

Datainspektionen förutsätter att Folkpartiet Liberalerna vidtar de åtgärder som planeras med anledning av pågående översyn beträffande ansvarsfördelningen för behandling av personuppgifter i det centrala medlemsregistret, bevarande av medlemsuppgifter för återvärvningsändamål, kompletteringar av information till registrerade samt komplettering och förtydligande av personuppgiftsbiträdesavtal med IT-tjänsteleverantör och underleverantör.

Datainspektionen kan komma att följa upp ärendet.

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

Bakgrund
Politiska partier har en omfattande hantering av medlemmars personuppgifter. Det förekommer också att riksdagspartierna i sina register, förutom uppom medlemmar, även behandlar uppgifter om personer som tagit kontakt för att inhämta information om partierna.

Riksdagspartierna är ideella föreningar och verksamheten är i allmänhet organiserade med en riksorganisation på nationell nivå och föreningar på regional och lokal nivå. Utöver detta finns anknutna förbund, t.ex. ungdoms- och kvinnoförbund. Riksorganisationen och föreningar på regional och lokal nivå är var för sig egna juridiska personer.

En uppgift om att någon är medlem i ett politiskt parti avslöjar politiska åsikter, vilket är känsliga personuppgifter enligt 13 § personuppgiftslagen. Det ställs särskilda krav för att behandla känsliga personuppgifter och hur uppgifterna skyddas. Enligt 17 § personuppgiftslagen får ideella organisationer med politiskt syfte inom ramen för sin verksamhet behandla känsliga personuppgifter om organisationens medlemmar och andra personer, som på grund av organisationens syfte, har regelbunden kontakt med partiet. Känsliga personuppgifter kan också behandlas med stöd av den registrerades samtycke

Under hösten 2011 inledde Datainspektionen ett projekt med syfte att granska hur samtliga riksdagspartier behandlar personuppgifter om medlemmar och andra personer som kontaktar partierna för information eller liknande och om behandlingarna uppfyller de krav som personuppgiftslagen ställer. Granskningen har även omfattat IT-säkerheten vid behandlingarna.

Redogörelse för tillsynsärendet
Som ett led i projektet har Datainspektionen den 17 januari 2012 inspekterat Folkpartiet Liberalerna riksorganisationen (fortsättningsvis Folkpartiet).

Vid inspektionen och senare skriftväxling har Folkpartiet uppgett bl.a. följande om hur partiet behandlar personuppgifter om medlemmar och andra. Vid ett möte den 16 augusti 2012 informerade Folkpartiet även om partiets planer om åtgärder med anledning av en pågående översyn av medlemsregistret.

Allmänt om partiets organisation
Partiet är organiserat i en riksorganisation, 25 länsförbund och cirka 270 kommunföreningar samt lokala avdelningar. Partiet har två kanslier; partikansliet och riksdagskansliet. Formellt är man medlem lokalt i

kommunförening och i undantagsfall kan man vara medlem direkt i ett länsförbund.

Behandling av personuppgifter i medlemsregister eller liknande
Folkpartiet har ett centralt medlemsregister. Där hanteras framför allt uppgifter om medlemmar men även uppgifter om intresserade, volontärer, förtroendevalda och personal. Personer som vill ingå i nätverk som Gröna Liberaler och Liberala Seniorer registreras.

Personuppgifterna samlas in från medlemmarna själva som fyller i sina uppgifter via anmälningsformulär på webben eller i en medlems-ansökan, som lämnas till lokala förbund. När personen betalt medlemsavgiften registreras uppgifterna i medlemsregistret.

För en medlem kan följande uppgifter behandlas i medlemsregistret. För- och efternamn, postadress, e-postadress, tillhörighet till lokal avdelning samt uppdrag är obligatoriska uppgifter. Uppgifter om födelseår, personnummer, kön och telefon är frivilliga uppgifter. Det finns fritextfält som används för att skriva in kommentarer. Det är möjligt att spärra uppgifter om en medlem som har en skyddad adress.

Medlemsuppgifter behandlas för att administrera medlemskap och uppdrag inom partiet samt provval. Registret används för utskick av listor, etiketter för aktiviteter och annan intern information såsom utskick av nyhetsbrev och medlemstidningen, som skickas till alla medlemmar fyra gånger om året. Därtill används uppgifterna för statistik, fakturering och bokföring. Nytt är att medlemmar och förtroendevalda som vill lämna bidrag kommer att registreras. Medlemsuppgifter behandlas med stöd av avtal med den registrerade. Folkpartiet planerar att inhämta ett samtycke från nya medlemmar för att behandla uppgifter för återvärvningsändamål om dem som inte betalt medlemsavgiften i tid. Utlämnande till tredje part kan ske medlemmar med offentliga uppdrag och medlemmar som lämnat ett samtycke till att kontaktuppgifter lämnas ut.

För andra än medlemmar registreras de uppgifter som personerna lämnar vid en anmälan, t.ex. i ett webbformulär. Obligatoriska uppgifter är namn och e-postadress. För den som prenumererar på ett nyhetsbrev registreras endast e-postadress. För t.ex. intresserade, volontärer och personer som ingår i nätverk används uppgifterna för att ge information om folkpartiet och om partiets aktiviteter. Uppgifter om intresserade,

volontärer, prenumeranter av nyhetsbrev behandlas med stöd av samtycke.

Personuppgiftsansvar
Enligt Folkpartiet är riksorganisationen personuppgiftsansvarig för behandlingen av personuppgifter i det centrala medlemsregistret. Det är riksorganisationen som bestämmer vilka uppgifter som ska registreras och hur de ska användas. Lokalföreningarna sköter medlemsvården och kan lägga till, ändra och ta bort uppgifter om en medlem.

Registret är uppbyggt med utgångspunkt från att flera länsförbund saknar anställd personal och att riksorganisationen då måste sköta all behandling av personuppgifterna för medlemmarna. Därför finns också medlemsportalen där medlemmar själva kan logga in på ”Mitt Folkparti” för att kontrollera, korrigera och begränsa kontaktuppgifter som Folkpartiet får använda. Ett nyligt beslut att centralisera medlems-avgiftshanteringen ligger i linje med strävan att hanteringen av personuppgifter i största möjliga mån ska ligga på central nivå.

Det är riksorganisationen som tillhandahåller medlemssystemet där personuppgifter behandlas. Riksorganisationen bestämmer hur personuppgifter kan behandlas, utbildar personal som ska utföra behandlingarna, utdelar behörigheter till underställd personal för att få utföra behandlingar, ger instruktioner om hur och när behandlingar ska genomföras. Gallring av uppgifterna sker via riksorganisationen. Det är också riksorganisationen som står för information till medlemmar om lokala aktiviteter då anställd personal saknas, vilket är fallet i flera länsförbund. Det är uteslutande riksorganisationen som hanterar personuppgifter om intresserade och volontärer.

Länsförbunden är, i den mån de har anställd personal, ansvariga för information till medlemmarna om lokala aktiviteter. De kan utifrån de begränsningar som medlemmarna själva gör och i den mån länsför-bunden har utbildad personal, kontakta de registrerade med utskick och e-post om lokala aktiviteter. Nya medlemmar kommer främst via anmälningsformuläret på webben, men länsförbunden kan, om de har utbildad personal, registrera nya medlemmar i medlemsregistret.

På kommunförening/lokalavdelningsnivå kan ordförande och kassör ladda ner etiketter, adress telefon listor inbetalningskort och skicka e-post inom sin kommun.

Folkpartiet planerar att tydliggöra ansvarsfördelningen hos föreningarna och håller på att upprätta dokument som ska beskriva detta.

Information till den registrerade
Folkpartiet lämnar information om personuppgiftsbehandlingen på partiets webbplats, medlemsansökan via webben och ”Mitt Folkparti”. Alla medlemmar får information om att det finns information om personuppgiftsbehandlingen på webbadressen www.folkpartiet.se/pul.

Informationen till de registrerade ska kompletteras. Det ska ske genom tillägg, exempelvis om att uppgifterna kan användas för statistikändamål, att medlemmar och förtroendevalda som vill lämna bidrag kommer att registreras och att uppgifter sparas för återvärvningsändamål.

Hur länge sparas uppgifterna?
Folkpartiet planerar att införa automatiska rutiner för gallring av samtliga personuppgifter till 2013. För medlem som begärt utträde raderas samtliga uppgifter inom tre månader. För medlem som inte betalat sin avgift har partiet nyligen beslutat att riksorganisationen ska ta över uppgiften att administrera medlemsavgifter, vilket kommer att förändra rutinen att gallra uppgifterna något. Medlemsuppgifterna kommer då att finnas kvar maximalt ett år och tre månader. Det är inte reglerat i stadgarna vilket datum en medlem ska ha betalt avgiften för innevarande år, vilket innebär att medlemmen har fram till den 31 december att betala. Folkpartiet planerar att med stöd av ett samtycke från ny medlem fortsätta lagra uppgifter om medlemmar som inte betalt medlemsavgiften i tid (ett kalenderår) under ytterligare ett år för återvärvningsändamål.

Prenumeranter av nyhetsbrev raderas när de avanmäler sig. Uppgifter om ”intressenter” sparas i 90 dagar och uppgifter om volontärer sparas högst ett år efter senaste aktivitet. Vid en kontakt finns alltid möjlighet till att avsluta sitt intresse eller volontärskap med omedelbar verkan.

IT-säkerhet
Folkpartiet anlitar en IT-tjänsteleverantör som personuppgiftsbiträde. Programvaran som levereras är anpassad till Folkpartiets krav. IT-leverantören använder i sin tur en underleverantör för leverans av driftmiljö i serverhallar, i vilka folkpartiets information hanteras helt isolerat från andra kunder i samma server-kluster. Det innebär att

Folkpartiets system nyttjar samma processorresurser som andra företag, men att ingen förutom dem av Folkpartiet autentiserade användare kan komma åt informationen i strukturerad form. Underleverantörens personal har ingen åtkomst till informationen. Det är underleverantören som sköter drift och underhåll av servrarna samt tillhandahåller det fysiska skyddet för hårdvaran. Underleverantörens serverhallar ligger i Sverige och Folkpartiets information behandlas (dvs. lagras och bearbetas) enbart där.

Partiets personuppgiftsbiträdesavtal med IT-tjänsteleverantören och med underleverantören ska kompletteras och förtydligas.

Medlemssystemet nås via ett webbgränssnitt. Inloggning kan ske antingen direkt med användarnamn och lösenord eller via Google OpenID. För inloggning via Googles OpenID krävs att användaren har registrerat ett användarnamn och lösenord hos Google OpenID. Folkpartiet har regler för sammansättning och längd av lösenord.

Folkpartiet gör en översyn av hur och om autentisering genom tvåfaktorinloggning kan ske. Det finns tekniska möjligheter att redan nu starta tvåstegsautentisering vid inloggning i medlemssystemet. Men frågan är inte så enkel när det gäller de särskilda risker som finns med behandlingen. Krav på en alltför invecklad inloggning på lokal nivå kan enligt Folkpartiet göra att man avstår från att logga in i kontaktsystemet och i stället inrättar egna register lokalt vilket kan leda till säkerhets- och demokratiproblem. Dessutom varierar behovet av inloggning stort. Medan en person kanske loggar in en gång per år behöver andra logga in varje dag. Folkpartiet har därför ställt sig frågan om samma krav ska ställas på den som arbetar ideellt, med begränsad behörighet till systemet och inom ett begränsat geografiskt område som på de personer som har superbehörighet och åtkomst till samtliga uppgifter i systemet.

Riksorganisationen administrerar behörigheter till medlemsregistret. Det krävs ett styrelsebeslut för att riksorganisationen ska lägga upp en ny behörighet. Av dokumentet ”Policy och riktlinjer för medlems-registret inom Folkpartiet” framgår behörighetsgrad och behörighets-nivå. Dessutom är behörighetsnivåerna rollbaserade. En behörig användare med högsta behörighet på lokalföreningsnivå har t.ex. endast åtkomst till uppgifter om medlemmar tillhörande just den lokalföreningen.

Vid inloggning till medlemsregistret via webbgränssnittet är kommunikationen skyddad genom kryptering. Likaså är kommunikationen vid en anmälan om medlemskap via webbplatsen och vid inloggning till ”Mitt Folkparti” skyddade genom kryptering.

Folkpartiet har inte gjort någon övergripande penetrationstest av IT-systemen. Folkpartiet har uppgett att man under 2012/2013 ska genomföra en kartläggning av säkerhetsrisker där riksorganisationens IT-säkerhet kontrolleras och testas.

All inloggning till medlemsregistret loggas. Det inkluderar misslyckade inloggningar. När det gäller åtkomstkontroll genom behandlingshistorik går det att se vilken användare som varit inne och tittat på en medlemsprofil. Även alla ändringar i medlemsregistret loggas. Loggarna kontrolleras vid teknisk felsökning eller vid behov. Folkpartiet kan begära att systemleverantörer följer upp loggarna. Det finns planer på att införa rapporter med logguppgifter till kommunförbunden.

Informationen i medlemssystemet säkerhetskopieras dagligen.

Skäl för beslutet

Vem är personuppgiftsansvarig för behandling av personuppgifter i det centrala medlemsregistret?

Personuppgiftsansvaret definieras i personuppgiftslagen som den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter (3 §).

Personuppgiftsansvaret kan ibland framgå direkt av en bestämmelse i lag eller förordning och i andra fall kan olika avtalskonstruktioner, där personuppgiftsansvaret preciseras, beaktas vid bedömningen. I detta fall framgår personuppgiftsansvaret varken av någon författningsbestämmelse eller uttryckligen av avtal. Vem eller vilka som är personuppgiftsansvariga för behandlingen av personuppgifter i Folkpartiets medlemsregister får avgöras av de faktiska omständigheterna, dvs. vem eller vilka som har bestämt över behandlingen.

Folkpartiet anser att riksorganisationen är personuppgiftsansvarig för behandlingen av personuppgifter i det centrala medlemsregistret.

Datainspektionen ifrågasätter inte att riksorganisationen är personuppgiftsansvarig för behandlingen av personuppgifter i det centrala medlemsregistret. Frågan är dock vilken roll lokala förbund och föreningar har, dvs. om de ska

anses gemensamt personuppgiftsansvariga eller om de är personuppgiftsbiträden till riksorganisationen. Av utredningen har det bl.a. framkommit att förbunden på regional nivå är ansvariga för information till medlemmarna om lokala aktiviteter och kan kontakta de registrerade med utskick och e-post om lokala aktiviteter. Förbunden regionalt har även direktåtkomst till registret för att registrera, ändra och ta bort uppgifter i registret även om det centralt har bestämts vilka uppgifter som ska registreras. På lokal nivå har föreningarna rätt att ladda ner listor, etiketter och skicka e-post inom sitt ansvarsområde.

Folkpartiet planerar nu att tydliggöra ansvarsfördelningen. Folkpartiet håller nu på att upprätta dokument som ska beskriva detta.

Det finns möjlighet att inom ramen för en ideell organisation som består av fler juridiska personer att låta organisationen på riksnivå bestämma över behandlingen, t.ex. förandet av ett gemensamt medlemsregister på sådant sätt att den organisationen ensamt är personuppgiftsansvarig. De andra juridiska personerna inom organisationen är då personuppgiftsbiträden när de hanterar personuppgifter.

Datainspektionen uppfattar att Folkpartiets ansvarsfördelning kommer att innebära att organisationer på regional och lokal nivå är personuppgiftsbiträden till riksorganisationen, som är ensamt personuppgiftsansvarig för det centrala medlemsregistret.

Om det blir så upplyser Datainspektionen om att Folkpartiet i enlighet med 30 § personuppgiftslagen ska upprätta ett skriftligt avtal med organisationerna på regional och lokal nivå. I avtalet ska det särskilt föreskrivas att personuppgifterna i medlemsregistret bara får behandlas av biträdena i enlighet med instruktioner från den personuppgiftsansvarige, dvs. riksorganisationen.

Vilka regler i personuppgiftslagen gäller för behandlingen av personuppgifter i medlemsregistret?
Datainspektionen gör bedömningen att Folkpartiets behandling av personuppgifter i medlemsregistret är en automatiserad behandling enligt 5 § personuppgiftslagen. Undantaget i 5 a § personuppgiftslagen för ostrukturerad behandling är inte tillämplig, vilket medför att de s.k. hanteringsreglerna i personuppgiftslagen gäller för behandlingarna av personuppgifter i medlemsregistret.

Följer behandlingen av personuppgifter i medlemsregistret bestämmelser i personuppgiftslagen?
Datainspektionen har inga synpunkter på hur Folkpartiet behandlar personuppgifter om medlemmar och andra i det centrala medlemsregistret utöver vad som framkommer nedan under detta samt därefter följande avsnitt.

Lämnar Folkpartiet tillräcklig information om personuppgiftsbehandlingen?
Enligt 23-25 §§ personuppgiftslagen är den personuppgiftsansvarige skyldig att självmant lämna information till de registrerade, i detta fall medlem, prenumerant, intressent eller volontär. Informationen ska innehålla uppgift om:

- Den personuppgiftsansvariges identitet,
- Ändamålen med behandlingen och
- All övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter i samband med behandlingen.

Sådan övrig information är t.ex. information om vilka kategorier av uppgifter som behandlas, kategorier av mottagare av uppgifterna, hur länge uppgifterna bevaras samt rätten att gratis en gång årligen efter ansökan erhålla information och rätten att få rättelse av felaktiga eller missvisande uppgifter.

Om partiet behandlar personuppgifter med stöd av samtycke, vilket partiet uppgett, vill Datainspektionen påpeka att ett giltigt samtycke enligt personuppgiftslagen kräver att den registrerade fått tillräcklig information för att kunna avgöra om ett samtycke till behandlingen ska lämnas.

Datainspektionen har tagit del av den information om personuppgifts-behandling som lämnas via Folkpartiets webbplats. Med hänsyn till aviserade kompletteringar av informationen till registrerade exempelvis om att uppgifterna kan användas för statistikändamål, att medlemmar och förtroendevalda som vill lämna bidrag kommer att registreras, att uppgifter sparas för återvärvningsändamål, har Datainspektionen inga synpunkter på informationen.

IT-säkerhet
Den personuppgiftsansvarige ska enligt 31 § personuppgiftslagen vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

a. de tekniska möjligheterna som finns,
b. vad det skulle kosta att genomföra åtgärderna,

c. de särskilda risker som finns med behandlingen av personuppgifterna,
d. hur pass känsliga personuppgifterna som behandlas är.

Fråga är om personuppgifterna i medlemsregistret är tillräckligt skyddade mot obehörig åtkomst, dvs. hur en behörig användare autentiseras.

För det första kan det konstateras att de uppgifter som Folkpartiet behandlar i medlemsregistret per definition enligt 13 § personuppgiftslagen är känsliga personuppgifter eftersom en uppgift om ett medlemskap i ett politiskt parti är en känslig personuppgift. Det innebär att kravet på skydd mot obehörig åtkomst kan ställas högre än annars.

Datainspektionen har flera gånger tidigare bedömt att känsliga person-uppgifter får lämnas ut via öppet nät, t.ex. Internet, endast till identifierade användare vars identitet är säkerställd med stark autentisering (se bl.a. 116-2012). Stark autentisering, också kallat multifaktorsautentisering, kan realiseras på olika sätt. Det kan ske exempelvis med e-legitimation, men även andra tekniska funktioner för asymmetrisk kryptering samt vissa lösningar för engångslösenord och liknande kan användas. Det finns standardlösningar för stark autentisering på marknaden som kan förvärvas för en i sammanhanget låg kostnad.

Folkpartiets medlemssystem kan nås via ett webbgränssnitt. Inloggning kan ske antingen direkt med användarnamn och lösenord eller via Google OpenID. För inloggning via Googles OpenID krävs att användaren har registrerat ett användarnamn och lösenord hos Google OpenID. Därmed uppfylls inte kravet på stark autentisering, vilket i sin tur innebär att personuppgifterna i medlemsregistret inte är tillräckligt skyddade mot obehörig åtkomst.

I bedömningarna vägs in att ett lösenord är lätt att stjäla och den som har blivit bestulen på ett lösenord kommer kanske inte att upptäcka att så har skett. Stark autentisering försvårar för obehöriga att komma över de nödvändiga inloggningsuppgifterna som behövs för att kunna autentisera sig. Samtidigt underlättar det för den behörige att upptäcka förlusten av en eller flera faktorer. Det krävs att man samtidigt har tillgång till något fysiskt, t.ex. en mobiltelefon och att man har kunskap om det statiska lösenordet.

Av utredningen har kommit fram att folkpartiet har möjligheten att implementera en lösning som innebär en flerfaktorsautentisering men att man ställer sig tveksam till att införa lösningen. Detta eftersom man befarar att vissa användare kan ha svårt att ha hand om lösningen och därför försöker

att hitta ett alternativt sätt att behandla medlemsuppgifter utanför det av folkpartiet tillhandahållna medlemsregistret.

Med hänsyn till att medlemsregistret är åtkomligt via Internet bedömer Datainspektionen att på det sätt inloggningen sker idag inte är tillräcklig för att skydda känsliga personuppgifter mot obehörig åtkomst. Ett sätt för folkpartiet att minska risken för att vissa användare väljer att inte använda sig av det centrala registret kan vara att bistå användarna med utbildning och support av en vald lösning för stark autentisering. Folkpartiet har också möjlighet att vara tydlig i sina instruktioner till användarna om vad som gäller.

Datainspektionen konstaterar således att Folkpartiet inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att en behörig användare har åtkomst över Internet till personuppgifter i medlemsregistret enbart efter autentisering genom att uppge ett användarnamn och ett lösenord.

Datainspektionen förelägger, enligt 45 § första stycket personuppgiftslagen, Folkpartiet att vidta åtgärder som innebär att åtkomst över Internet till personuppgifter i medlemsregistret skyddas med stark autentisering.

I utredningen framkom att Folkpartiet inte har gjort någon övergripande penetrationstest av IT-systemen, men att man under 2012/2013 ska kartlägga säkerhetsrisker och genomföra IT-säkerhetstester. Detta ligger väl i linje med Datainspektionens rekommendationer. Datainspektionen anser att väl genomförda säkerhetstester är ett lämpligt sätt att kontrollerar att de genom en sårbarhetsanalys identifierade och implementerade säkerhetsåtgärderna verkligen fungerar som det var tänkt.

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 generaldirektören Göran Gräslund i närvaro av chefsjuristen Hans-Olof Lindblom, tillsynschefen Catharina Fernquist, IT-säkerhetsspecialisten Adolf Slama och juristen Gunilla Öberg, föredraganden.

Göran Gräslund

Gunilla Öberg