Datainspektionen

Datum	Diarienr
2012-05-31	1674-2011

Centerpartiet
Box 2200
103 15 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) – Centerpartiets behandling av personuppgifter i ett centralt medlemsregister

Datainspektionens beslut

Datainspektionen konstaterar följande brister vid Centerpartiets behandling av personuppgifter i det centrala medlemsregistret:

- Den information som lämnas till medlemmar uppfyller inte fullt ut de krav som ställs i 23-25 §§ personuppgiftslagen.

Datainspektionen konstaterar att Centerpartiet inte lever upp till de krav som ställs på säkerheten vid behandling av personuppgifter enligt 31 § personuppgiftslagen i det centrala medlemsregistret 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 det centrala medlemsregistret.
- Det går inte att, genom behandlingshistorik, utreda vem som har haft åtkomst till vilka personuppgifter och när. Vidare går det inte, genom behandlingshistorik, att utreda vem som ändrat eller raderat personuppgifter och när förändringen inträffat.

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

- komplettera informationen som lämnas till medlemmar om personuppgiftsbehandlingen, i enlighet med vad som framförs på s. 11-12 i detta beslut, så att informationen uppfyller de krav som ställs i 23-25 §§ personuppgiftslagen.
- vidta åtgärder som innebär att åtkomst över öppet nät till personuppgifter i det centrala medlemsregistret skyddas med stark autentisering.

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

- införa och aktivera sådana tekniska funktioner som gör det möjligt att utreda vem som har haft åtkomst till vilka personuppgifter och när samt vem som ändrat eller raderat personuppgifter och när förändringen inträffat.

Mot bakgrund av vad Datainspektionen konstaterat kring Centerpartiets rutiner för gallring av uppgifter om tidigare medlemmar förutsätter myndigheten att partiet ser över gallringsrutinerna avseende det centrala medlemsregistret.

Datainspektionen förutsätter att Centerpartiet upprättar personuppgiftsbiträdesavtal enligt den presenterade projektplanen.

Datainspektionen kan komma att följa upp ärendet.

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

Riksdagspartierna är ideella föreningar och verksamheten är i allmänhet organiserad med en riksorganisation på nationell nivå och föreningar på regional och lokal nivå. Utöver detta finns det anknutna förbund, t.ex. ungdoms- och kvinnoförbund. Riksorganisation 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 är en känslig personuppgift 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 19 januari 2012 inspekterat Centerpartiet.

Vid inspektionen och senare skriftväxling med Centerpartiet har partiet uppgett bl.a. följande om partiets organisation och hur partiet behandlar personuppgifter om medlemmar och andra:

Allmänt om partiets organisation
Centerpartiets organisation är uppdelad i en riksorganisation, distrikt (motsvarande län/regioner), krets (motsvarande kommuner) och ibland underavdelningar. Varje del är en egen juridisk person, men det är inget krav att underavdelningar ska vara egna juridiska personer. I enlighet med Centerpartiets stadgar blir man i första hand medlem i kretsen, där medlemmen har rösträtt. I centerrörelsen ingår förutom Centerpartiet även Centerkvinnorna, Centerpartiets ungdomsförbund och Centerstudenter, vilka har egna stadgar. En medlem i t.ex. ungdomsförbundet blir inte automatiskt medlem i Centerpartiet.

Behandling av personuppgifter i medlemsregister eller liknande
Personuppgifter om medlemmar i Centerpartiet, Centerkvinnorna, Centerpartiets ungdomsförbund och Centerstudenter registreras i centerrörelsens medlemsregister, som togs i drift hösten 2008. All medlemsregistrering förutsätts ske i det gemensamma registret, som är ett webbaserat system och grunden för att administrativt hantera övriga system inom organisationen såsom Intranätet (Centralen), e-postsystemet samt sändlistelösningar i SMS och e-postsystem.

De uppgifter som behandlas om en medlem och som är obligatoriska är medlemsnummer, namn, information om medlemskapet och information som rör betalning av medlemsavgift. Utöver dessa kan följande uppgifter komma att behandlas; land, samhushåll, telefon, fax, e-postadress, tillfällig adress, webbadresser, kön, förtroendeuppdrag i Svenska kyrkan, födelseår/födelsedata/personnummer, tidigare medlemsnummer, hemkommun, info om medlemskap (organisatorisk hemvist), nätverk (används inte i praktiken), uppgift om tidningsprenumeration, interna och externa uppdrag, annan betalar av medlemskapet (används inte i praktiken) och gåvor (används inte i praktiken). Att uppge personnummer är frivilligt men krävs för kandidatur för Centerpartiet.

Riksorganisationen erbjuder enligt Centerpartiets stadgar central avisering för att underlätta administrationen kring avisering av medlemmar.

Den centrala aviseringen startade 2009 och allt fler föreningar inom organisationen övergår till att anlita medlemsservicefunktionen på central nivå.

Uppgifter om medlemmar i Centerpartiet, Centerkvinnorna, Centerns ungdomsförbund och Centerstudenterna registreras i medlemsregistret. Anställda och revisorer som inte är medlemmar i partiet registreras också i medlemsregistret, men i en separat grupp med noteringen ”kontakt ej medlemskap” och uppgifterna används för utskick. Intressenter registreras inte i medlemsregistret. Inte heller den som vill ha nyhetsbrev registreras där, eftersom medlemmar via intranätet kan begära att få nyhetsbrev och medlemsservice manuellt lägger då in medlemmen i en sändlista för nyhetsbrev. Därtill registreras ett fåtal personer, som inte är medlemmar, som prenumeranter av partiets tidning. Alla medlemmar får medlemstidningen hemskickad. De personer som registrerat sig för partiets nyhetsbrev men som inte är medlemmar, t.ex. journalister och politiskt intresserade, hanteras inte i medlemsregistret utan separat.

Personuppgifterna samlas in från medlemmen själv. Nya medlemmar registreras lokalt.

Uppdateringen av medlemmarnas uppgifter i medlemsregistret sker genom att medlemmarna via ”mina sidor” kan ändra uppgift om adress, telefon, e-postadress. Riksorganisationen köper även en adressändringstjänst. Uppdatering sker främst på lokal nivå, där man har personlig kännedom om sina medlemmar. Om ett brev kommer i retur kontrollerar partiet adressen via Eniro eller genom lokal kännedom. I ett pågående projekt om partiets personuppgiftsbehandling ingår att se över uppdatering av personuppgifter i registret.

Personuppgifter sparas i medlemsregistret för att administrera medlemskapet. Uppgifterna används även för att ta fram statistik, t.ex. om hur många medlemmar som partiet har, samt fakturering och bokföring. Uppgifterna används inte för återvärvning av tidigare medlemmar eller för annan marknadsföring. Vid ett utskick till medlemmar kan partiet skicka med information om en samarbetsorganisation när innehållet har koppling till partiets verksamhet.

Uppgifter om medlemmar behandlas med stöd av avtal och lämnas inte ut till tredje man.

Personuppgiftsansvar
Centerpartiets Riksorganisation ledd av partistyrelsen är personuppgiftsansvarig för de behandlingar av personuppgifter som utförs i riksorganisationens verksamhet samt ytterst ansvarig som helhet. Då varje distrikt och krets i Centerpartiet är egna juridiska personer har Centerpartiet också tolkat det som ett delat ansvar där distriktet/kretsen i sin tur är ansvariga för den behandling av personuppgifter som utförs inom ramen för lokal och regional verksamhet.

Centerpartiets stadgar styr roller och ansvarsfördelning i organisationen samt klargör vilka uppgifter som faller inom ramen för Centerpartiets verksamhet både centralt, regionalt och lokalt. Stadgarna utgör ramverket till Centerpartiets ändamål med behandling av personuppgifter. Utifrån detta är det upp till varje kretsstämma/kretsmöte, distriktsstämma/distriktsstyrelse och partistämma/partistyrelse att fatta beslut om hur organisationen ska arbeta lokalt, regionalt och nationellt. Stadgarna antas/förändras av partistämman där ombud från kretsar och distrikt har rösträtt. Alla medlemmar har närvaro-, yttrande- och förslagsrätt.

En decentraliserad syn och tradition är stark i Centerpartiet, merparten av allt arbete i organisationen sker därför lokalt och regionalt, detta gäller även behandling av personuppgifter. Merparten av all administration och kommunikation med medlemmar sker i kretsar och distrikt och utförs av ideella krafter, styrelser och anställd personal. Här anser Centerpartiet att kretsstyrelsen och distriktsstyrelsen har ett ansvar för den behandling som sker inom ramen för deras verksamhet och det är också de som fattar beslut om vem som ska ges tillgång till medlemsregistret lokalt eller regionalt.

Övergripande behandlingar av personuppgifter som berör organisationen som helhet sker hos Centerpartiets riksorganisation och utförs av anställd personal. Centerpartiet har också en medlemsservicefunktion dit alla medlemmar kan vända sig om de har frågor om medlemskap, betalningar m.m. Riksorganisationen ansvarar också för partiets IT-system, behörighetstilldelning, utbildning av administratörer, utbildningsinsatser och medvetenhet om hur partiet behandlar personuppgifter m.m.

Uteslutning från partiet kräver ett beslut från partistyrelsen.

Information till den registrerade
En person som vill bli medlem i Centerpartiet får information om hur personuppgifter behandlas i samband med att han eller hon fyller i en

medlemsansökan. Vidare lämnar Centerpartiet information om personuppgiftsbehandlingen avseende medlemmar i partiets medlemstidning samt på Intranätet vid användning av ”Mina sidor”.

Gallring
Centerpartiets rutiner för gallring är att under november och december varje år gå igenom medlemsregistret för att makulera obetalda medlemmar innan avisering av kommande medlemsår påbörjas.

För medlemmar som inte betalat sin medlemsavgift har Centerpartiet finns fr.o.m. 2012 möjlighet att ta bort uppgifterna snabbare än vad man kunnat göra tidigare. Det beror på att partiet ändrat i stadgarna. Ett medlemskap som inte förnyats före den 30 juni kan numera avslutas omgående. Tidigare har medlemmen haft hela det innevarande året på sig att betala medlemsavgiften.

Den som aktivt meddelar att han eller hon vill avsluta sitt medlemskap makuleras omedelbart från registret. Makulering innebär att alla uppgifter som kan knytas till en specifik person tas bort. De uppgifter som sparas är medlemsnummer, organisatorisk tillhörighet, postadress och betalningsinformation. Uppgifterna sparas för statistik och historiska ändamål.

Riksorganisationen kan inte med automatik gallra centralt i de avdelningar/kretsar som valt lokal avisering till sina medlemmar. Riksorganisationen arbetar därför aktivt med uppföljning och utbildning för att säkerställa att föreningar lokalt följer sina åtaganden.

IT-säkerhet
Det gemensamma medlemsregistret är ett webbaserat system och inloggning sker via ett webbgränssnitt. Det finns tre behörighetsnivåer till medlemsregistret; full behörighet, förslagsbehörighet och läsbehörighet.

Förslagsbehörighet innebär att ändringar i medlemsregistret måste kontrolleras och godkännas av någon med full behörighet. Full behörighet innebär möjligheter att titta, ändra och ta bort information.

Behörigheten är organisationsindelad. Varje organisation har behörighet endast till uppgifter om sina medlemmar, t.ex. inom sin krets. Det finns även centrala avdelningar i registret som bara riksorganisationen har tillgång till. Totalt har 207 användare åtkomst till medlemsregistret. Riksorganisationen har ett tiotal användare, distrikten har cirka 50 an-

vändare och lokalt 140 användare. Kvinnoförbundet, ungdomsförbundet och studenterna har tre användare med förslagsbehörighet. Partiet rekommenderar att endast ha en användare per krets eller att köpa tjänsten hos distriktet.

Vanligast är att kretsordföranden rekommenderar styrelsen, som tar beslut om att en person ska få tillgång till medlemsregistret. Ett utdrag från styrelseprotokollet för beslutet skickas till riksorganisationen, som därefter skickar en ansvarförbindelse till den blivande användaren, som denne ska fylla i och underteckna. Handlingen överlämnas till riksorganisationen via post eller fysiskt på plats.

Innan ett behörighetskonto läggs upp av Centerpartiets administrativt systemansvariga får den blivande användaren en introduktion/utbildning av medlemssystemet, som sköts av riksorganisationen. När så har skett lägger systemansvarig upp ett konto. Lösenordstilldelningen sker ofta genom personlig överlämning vid utbildningstillfället. Numera skiljs alltid användaruppgifter och lösenord åt vid tilldelning. Användaruppgifter skickas med e-post eller post och lösenordet skickas med SMS. Endast kända kontaktuppgifter i medlemsregistret används vid utskick av användarnamn och lösenord.

En behörig användare till det webbaserade systemet har ett personligt användarnamn och ett personligt lösenord. Det är tvingande att byta lösenordet var tredje månad. Det finns krav på lösenordets längd och sammansättning. Lösenordet lagras envägskrypterat. Den användare som tappar bort sitt lösenord måste begära ett nytt lösenord.

Det finns loggar i systemet, på vissa funktioner t.ex. för personrelaterade ändringar och betalningar går det att spåra vem som gjorde vad. Systemet är utformat så att man kan slå på olika inloggningsgrader och logga olika saker t.ex. larm, användarmönster på vissa funktioner samt informationsloggar. Loggarna används för att lättare kunna spåra problem/felaktigheter i systemet och sällan/aldrig för att spåra vad användare gör. Loggarna granskas inte om inget problem uppkommer, De sparas på medlemsregisterservern som en textfil. Det blir en textfil per dygn och rensning görs manuellt.

Centerpartiet har genomfört externa granskningar av informationssäkerheten och även gjort penetrationstester av systemen.

Centerpartiet har presenterat en sammanställning över samtliga personuppgiftsbiträden och meddelade att där det inte finns några personuppgiftsbiträdesavtal kommer dessa att upprättas.

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 §).

Ibland kan personuppgiftsansvaret 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 det centrala medlemsregistret får därför avgöras av de faktiska omständigheterna dvs. vem eller vilka som har bestämt över behandlingen.

Enligt Centerpartiet är riksorganisationen personuppgiftsansvarig för de behandlingar av personuppgifter som utförs i riksorganisationens verksamhet samt ytterst ansvarig för organisationen som helhet. Varje distrikt och krets har ett gemensamt ansvar med riksorganisationen för den behandling av personuppgifter som utförs inom ramen för lokal och regional verksamhet.

Datainspektionen delar Centerpartiets bedömning vad avser personuppgiftsansvaret. I sammanhanget vill dock Datainspektionen påpeka att det är viktigt att klarlägga vem som gör vad inom ramen för det gemensamma personuppgiftsansvaret och att de registrerade får korrekt information, vilket Datainspektionen återkommer till nedan.

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

Följer behandling av personuppgifter i medlemsregistret bestämmelserna i personuppgiftslagen?

Datainspektionen har inga synpunkter på hur Centerpartiet behandlar personuppgifter om medlemmar och andra i medlemsregistret utöver vad som framkommer nedan under detta samt därefter följande avsnitt.

Känsliga personuppgifter får behandlas med stöd av 15-19 §§ personuppgiftslagen. En uppgift om medlemskap i ett politiskt parti är en känslig personuppgift eftersom den avslöjar politiska åsikter. Av 17 § personuppgiftslagen framgår att en ideell organisation med politiskt syfte får, inom ramen för sin verksamhet, behandla känsliga personuppgifter om organisationens medlemmar och sådana andra personer som på grund av organisationens syfte har regelbunden kontakt med den. Om det finns ett gemensamt personuppgiftsansvar bedömer Datainspektionen att 17 § personuppgiftslagen ger såväl de lokala organisationerna som riksorganisationen en rätt att behandla uppgift om medlemskap. Det gäller trots att medlemskapet formellt är knutet till en lokalorganisation. Skälet till detta är den tydliga koppling som finns hos politiska partier mellan riksorganisationen och de lokala organisationerna vad framförallt avser verksamhetens organisation, syften och mål. Därutöver måste det även finnas stöd för behandlingen av personuppgifterna i 10 § personuppgiftslagen, vilket i detta fall är avtalet om medlemskapet under den tid detta löper.

Centerpartiet har uppgett att man har en rutin för att spara uppgifter om medlemmar som inte betalat sin medlemsavgift fram till november/december under det aktuella medlemsåret. En medlem kan dock själv begära att uppgifterna tas bort. Genom stadgeändring har man bestämt att ett medlemskap som inte förnyats senast den 30 juni det aktuella året kan avslutas.

Datainspektionen ifrågasätter den legala grunden för Centerpartiet att spara alla uppgifter om en medlem fram till november/december. En uppgift om att en person *har varit* medlem i ett politiskt parti är också en känslig personuppgift eftersom den kan anses avslöja en politisk åsikt. Om medlemskapet är avslutat kan partiet inte stödja sin behandling av uppgift om tidigare medlemskap på 17 § personuppgiftslagen. Inte heller har det framkommit att Centerpartiet i övrigt har någon grund enligt 15-19 §§ personuppgiftslagen att spara uppgifter om tidigare medlemmar efter tid då medlemskapet är avslutat. För att partiet ska få behandla uppgifterna krävs därför ett samtycke från den tidigare medlemmen. Det saknar i detta sammanhang betydelse huruvida partiet gallringsrutiner i denna del uppfyller de grundläggande kraven i 9 § personuppgiftslagen och bestämmelsen om tillåten behandling i 10 § personuppgiftslagen.

Vidare har Centerpartiet uppgett att uppgifter om tidigare medlemmar tas bort genom en ”makulering”. Med ”makulering” avser Centerpartiet att upp-

gifter om medlemmen raderas men att medlemsnummer, organisatorisk tillhörighet, postadress och betalningsinformation sparas. Uppgifterna som sparas efter en ”makulering” sparas för historiska och statistiska ändamål.

I sammanhanget vill Datainspektionen förtydliga att makuleringen måste innebära att det inte längre ska gå, direkt eller indirekt, att härleda information till en tidigare medlem för att informationen ska vara avidentifierad. Om det efter makuleringen fortfarande går att göra en sådan koppling måste den fortsatta behandlingen av informationen följa bestämmelserna i personuppgiftslagen eftersom det då är fråga om en behandling av personuppgifter.

Det bör noteras, även om Centerpartiet begränsat sig till att endast spara makulerade uppgifter om en tidigare medlem, att det finns möjligheter för ett politiskt parti att spara personuppgifter om tidigare medlemmar för statistiska ändamål. Enligt 19 § andra stycket personuppgiftslagen får känsliga personuppgifter behandlas för statistikändamål, om behandlingen är nödvändig på ett sätt som sägs i 10 § och om samhällsintresset av det statistikprojekt där behandlingen ingår klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan medföra. Bestämmelsen ger uttryck för en avvägningsnorm som innebär en helhetsbedömning av samtliga omständigheter. Statistik avseende medlemskap i politiskt parti kan enligt Datainspektionen anses ha ett sådant samhällsintresse som kan väga över intrånget i den enskildes personliga integritet. En bedömning måste göras i varje enskilt fall. Att även uppgifter om en tidigare medlem kan sparas för statistikändamål, trots att ändamålet för vilka de samlades in kan ha varit ett helt annat, framgår av 9 § tredje stycket personuppgiftslagen. Uppgifterna får dock sparas endast så länge som de behövs för detta statistikändamål. Det kan också finnas stöd i att behandla uppgift om ett tidigare medlemskap genom att uppgiften har offentliggjort i enlighet med 15 § personuppgiftslagen.

Mot bakgrund av vad Datainspektionen konstaterat kring Centerpartiets rutiner för gallring av uppgifter om tidigare medlemmar förutsätter myndigheten att partiet ser över gallringsrutinerna avseende det centrala medlemsregistret.

Lämnar Centerpartiet tillräcklig information om personuppgiftsbehandlingen?
Enligt 23-25 §§ personuppgiftslagen är den personuppgiftsansvarige skyldig att självmant lämna information till de registrerade. 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.

Datainspektionen har tagit del av information som lämnas i samband med att en medlem ansöker om medlemskap via partiets webbplats samt information som lämnats om personuppgiftsbehandlingen i ett nummer av partiets tidskrift samt på Intranätets ”Mina sidor”.

Sammantaget är den information som lämnas till medlemmar om personuppgiftsbehandlingen korrekt men det finns vissa brister.

Den lagliga grunden för Centerpartiets behandling av medlemsuppgifter för medlemsadministration är avtalet med medlemmen och behandlingen kräver därför inget samtycke. Att använda en metod där den registrerade får ”godkänna” behandlingen ger ett intryck att han eller hon kan välja om personuppgifterna får behandlas eller inte. Datainspektionen avråder därför partiet att använda en sådan metod. Om partiet däremot vill utföra en behandling som kräver ett samtycke hindrar det inte att partiet begär in ett samtycke på detta sätt vad avser just denna behandling.

Det är också viktigt att det av informationen framgår att distrikt/krets har ett gemensamt personuppgiftsansvar för behandling av personuppgifter i medlemsregistret.

Av informationen måste även framgå att uppgifter om medlemmen används för historiska och statistiska ändamål.

Med hänsyn till de brister som framkommit ovan konstaterar Datainspektionen att Centerpartiet inte fullt ut lever upp till de krav som ställs på informationen i 23-25 §§ personuppgiftslagen.

Datainspektionen förelägger därför Centerpartiet att komplettera den skriftliga informationen som lämnas till medlemmar om personuppgiftsbehandlingen så att den uppfyller de krav som ställs i 23-25 §§ personuppgiftslagen.

I sammanhanget vill Datainspektionen rekommendera Centerpartiet att komplettera information på webbplatsen med den information som lämnats i

partiets tidskrift. På flera sätt är denna information tydligare och Datainspektionen ser flera fördelar med att ha information lättillgänglig på Internet.

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, och
d. hur pass känsliga de behandlade personuppgifterna är.

Fråga är om skyddet för att förhindra obehörig åtkomst till personuppgifter i det centrala medlemsregistret är tillräckligt dvs. framförallt hur en behörig användare autentiseras.

Som tidigare konstaterats är en uppgift om medlemskap i ett politiskt parti 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 personuppgifter får lämnas ut via öppet nät, t.ex. Internet, endast till identifierade användare vars identitet är säkerställd med stark autentisering (se bl.a. dnr 116-2010). 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.

Inloggning över öppet nät till det webbaserade systemet, vilket ger åtkomst till det centrala medlemssystemet, sker med användarnamn och lösenord. Datainspektionen konstaterar att det sätt för autentisering som Centerpartiet använder inte är tillräckligt säkert eftersom det inte är fråga om en stark autentisering. Detta innebär i sin tur att personuppgifterna inte är tillräckligt skyddade.

I detta 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.

Datainspektionen konstaterar således att Centerpartiet inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att behöriga användare har åtkomst över öppet nät till personuppgifter i det centrala medlemsregistret efter autentisering med enbart lösenord och användarnamn.

Datainspektionen förelägger därför, enligt 45 § första stycket personuppgiftslagen, Centerpartiet att vidta åtgärder som innebär att åtkomst över öppet nät till personuppgifter i det centrala medlemsregistret skyddas med stark autentisering.

Nästa fråga är om Centerpartiet uppfyller de krav som kan ställas på åtkomstkontroll genom behandlingshistorik.

Enligt Datainspektionens allmänna råd för säkerhet vid behandling av personuppgifter bör en behandlingshistorik normalt vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av personuppgifter. Behandlingshistoriken bör, beroende på känsligheten hos personuppgifterna, ange till exempel läsning, ändring, utplåning eller kopiering av personuppgifter. En behandlingshistorik har också en förebyggande funktion, vilket förutsätter att användarna informeras om att det förs en behandlingshistorik och att den kontrolleras.

Datainspektionen bedömer att när ett politiskt parti behandlar uppgifter om medlemmar i ett medlemsregister måste det vara möjligt att utreda vem som haft åtkomst till vilka personuppgifter i medlemsregistret och när. Vidare ska det gå att utreda vem som ändrat eller raderat personuppgifter och när förändringen skett.

Enligt Centerpartiet finns det tekniska möjligheter att spåra ändringar i medlemsregistret. Det används dock i praktiken endast för att spåra tekniska problem och felaktigheter.

Datainspektionen konstaterar att den behandlingshistorik som förs idag inte uppfyller de krav på att partiet ska kunna utreda vem som har haft åtkomst till personuppgifter och när. Endast ändringar kan spåras och det under förutsättning att funktionen aktiverats, vilket synes vara vid undantagssituationer.

Datainspektionen förelägger därför, enligt 45 § första stycket personuppgiftslagen, Centerpartiet att införa och aktivera sådana tekniska funktioner som

gör det möjligt att utreda vem som har haft åtkomst till vilka personuppgifter i medlemsregistret och när. Vidare ska det gå att utreda vem som ändrat eller raderat personuppgifter och när förändringen skett.

Centerpartiet har presenterat en sammanställning över samtliga personuppgiftsbiträden och meddelade att där det inte finns några personuppgiftsbiträdesavtalen kommer dessa att upprättas. Datainspektionen förutsätter att Centerpartiet upprättar personuppgiftsbiträdesavtal enligt den presenterade projektplanen.

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 juristerna Gunilla Öberg och Jonas Agnvall, föredragande.

Göran Gräslund

Jonas Agnvall