Datainspektionen

Datum	Diarienr
2012-05-31	1670-2011

Vänsterpartiet
Box 12660
112 93 Stockholm

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

Datainspektionens beslut

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

- Den information som lämnas till medlemmar om personuppgiftsbehandlingen uppfyller inte fullt ut de krav som ställs i 23-25 §§ personuppgiftslagen.
- Det saknas information och en rutin att informera prenumeranter till Vänsterpartiets tidning om hur partiet behandlar deras personuppgifter. Vänsterpartiet uppfyller därför inte de krav som ställs på information till de registrerade enligt 23-25 §§ personuppgiftslagen.
- Behandlingen av uppgifter om tidigare medlemmar för ändamålet återvärvning strider mot 13 § personuppgiftslagen när det saknas stöd enligt 15-19 §§ att behandla uppgifterna.

Datainspektionen konstaterar att Vänsterpartiet 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 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.

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

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

- komplettera informationen som lämnas till medlemmar om personuppgiftsbehandlingen, i enlighet med vad som framförs på s. 9-10, så att informationen uppfyller de krav som ställs i 23-25 §§ personuppgiftslagen,
- informera samt ta fram rutiner för att informera prenumeranter till partiets tidning på ett sådant sätt att kraven i 23-25 §§ uppfylls,
- antingen upphöra med att behandla uppgifter om tidigare medlemmar för återvärvning eller inhämta de registrerades samtycke för behandlingarna,
- vidta åtgärder som innebär att åtkomst över öppet nät till personuppgifter i det centrala medlemsregistret skyddas med stark autentisering,
- införa 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.

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. 17 § personuppgiftslagen ger ideella organisationer med politiskt syfte stöd för att 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 12 januari 2012 inspekterat Vänsterpartiet.

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

Allmänt om partiets organisation
Vänsterpartiets organisation är uppdelad i en partistyrelse, partidistrikt (24 st) samt partiföreningar (ca 300 st). Samtliga partiets medlemmar är, sedan tre år tillbaka, medlemmar i riksorganisationen. Alla medlemmar hör till en partiförening.

Det finns ett ungdomsförbund. Man blir inte automatiskt medlem i Vänsterpartiet när man går med i ungdomsförbundet.

Behandling av personuppgifter i medlemsregister eller liknande
Personuppgiftsansvar
Vänsterpartiets registrerar, sedan tre år tillbaka, medlemmar i ett centralt medlemsregister, som är en del av ett större IT-system som består av ett antal komponenter som kommunicerar med registret.

I det centrala medlemsregistret behandlas, förutom personuppgifter om medlemmar, även uppgifter om personer som anmält intresse för att få bli medlem i partiet, autogirogåvogivare samt uppgifter om prenumeranter av partiets tidning.

För medlemmar registreras uppgifter om namn, adress, medlemsnummer, telefonnummer, e-postadress, kön, ålder, personnummer, facklig tillhörighet (frivillig), arbetsplats/yrke, personkoppling i hushåll, interna och parlamentariska partiuppdrag samt betalningshistorik.

Uppgifterna om en medlem behandlas för att kunna administrera medlemskapet, fakturering, statistik och bokföring.

En person kan ansöka om medlemskap genom att fylla i en talong eller ansöka om medlemskap via partiets webbplats. Uppgifterna registreras

då i ett s.k. väntregister, där de lagras temporärt i avvaktan på att medlemskapet betalas.

Gåvogivare som inte är anmälda för autogiro, dvs. bara ger en engångsgåva, registreras inte ifall summan understiger 20 000 kr. I de fall gåvan överstiger nyssnämnda summa har Vänsterpartiet en frivillig överenskommelse med flera andra politiska partier att sådana gåvor ska offentliggöras. En person som ger en sådan gåva kommer därför att registreras för detta ändamål, men inte i ett registersystem. Uppgifter om gåvor avseende en gåvogivare, som har autogiro och som är medlem, tas bort först när personen utträtt. En person som inte är medlem och som avslutar sitt autogiro raderas i princip direkt.

Information till den registrerade
De registrerade informeras om personuppgiftsbehandlingen dels genom information på partiets webbplats dels genom information i partiets tidning.

Gallring
Uppgifterna i medlemsregistret gallras manuellt men partiet överväger att ta hjälp av en systemleverantör för att införa automatisk gallring.

En medlem som inte betalat årets medlemsavgift senast 31 december det år avgiften avser mister de rättigheter som följer av medlemskapet. En sådan medlem betecknas med medlemsstatus ”Passiv” i medlemsregistret och betraktas inte längre som betalande medlem. De finns kvar i registret för att möjliggöra återvärvningskampanjer, men får inte några regelbundna utskick. En medlem som aktivt begära utträde får medlemsstatus ”utträdd” i registret och uppgifterna sparas under ett år. Det för att säkerställa att medlemsansvariga i partiföreningar och ombudsmän har kännedom om att personen har utträtt och t.ex. inte av misstag återregistrerar personen som medlem. En utträdd medlem får inga medlemsutskick. En begäran om att få bli struken ur registret hörsammas alltid och uppgifterna gallras omgående.

Uppgifter i väntregistret raderas om personen själv kontaktar Vänsterpartiet eller inom ett år i de fall personen inte betalar in sin första medlemsavgift.

Uppgifter om prenumeranter av partiets tidning gallras vid uppsägningen av prenumerationen. I praktiken sker detta inom några veckor.

IT-säkerhet

Inloggning till medlemswebben, vilket ger åtkomst till personuppgifter i det centrala medlemsregistret, sker med medlemsnummer och lösenord. Webbinloggningen är skyddad med kryptering (https). Åtkomst till registret har systemadministratör, ombuden och medlemsansvariga. Även vissa medlemmar kan ha åtkomst till sina egna medlemsuppgifter. Det har varit en försöksverksamhet, som nu är under avveckling. Parallellt med inloggning via medlemswebben kan systemadministratören logga in via en PC-klient. Via PC-klienten har denne åtkomst till hela systemet. Fjärrinloggningen via PC-klienten kan i dagsläget inte ske annat än för leverantörens serviceändamål och då används en krypterad form av fjärrskrivbord som bara är möjlig från utvald IP-adress.

Inom organisationen finns ett rollbaserat behörighetskontrollsystem som styr vilken åtkomst en användare får till personuppgifterna i medlemsregistret. Det finns fyra behörighetsnivåer: superuser, ombudsmän, medlemsansvariga och vissa medlemmar. Den högsta behörigheten har superuser (2 st.), som har full behörighet och är den som registrerar nya användare i systemet. Ombudsmännen (ca 40 st.) har åtkomst till uppgifter om medlemmar som tillhör deras distrikt. Medlemsansvariga (ca 300 st) har åtkomst till uppgifter om medlemmar som hör till den egna partiföreningen. Vissa medlemmar (ca 500-600 st.) har på försök åtkomst till sina egna medlemsuppgifter.

Det är systemadministratören som delar ut behörigheter och lägger upp nya användarkonton. Detta sker efter att partiföreningarna och distrikten anmäler, via mejl, brev eller telefon, till systemadministratören att en person, medlemsansvarig eller en ombudsman, behöver få åtkomst till registret.

Inloggning till medlemsportalen, dvs. medlemsansvariga och ombudsmäns begränsade tillgänglighet till systemet, loggas. Därutöver loggas vem som gjort en förändring i medlemsregistret till viss del. Det sker ingen regelbunden loggуppföljning

Vänsterpartiet har inte gjort någon extern granskning av informationssäkerheten. Inte heller har partiet gjort några penetrationstester av IT-systemet.

Det finns rutiner för säkerhetskopiering av medlemsregistret. Varannan vecka tas en full säkerhetskopia och däremellan tas inkrementella säkerhetskopior. Säkerhetskopiorna förvaras i ett plåtskåp i ett angrän-

sande, låst, rum i partiets lokaler. Vänsterpartiet har inte prövat att återläsa information från en säkerhetskopia.

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 Vänsterpartiet är riksorganisationen personuppgiftsansvarig för behandlingen av personuppgifter i det centrala medlemsregistret.

Av utredningen i ärendet framgår att all registrering av uppgifter om medlemmar sker centralt. Viss registrering, till exempel ändring av medlemmars adresser kan göras av behörig person på partiförenings- och distriktsnivå.

Datainspektionen ifrågasätter inte att riksorganisationen är personuppgiftsansvarig för behandlingen av personuppgifter i det centrala medlemsregistret.

Frågan är dock vilken roll partiföreningar/partidistrikt har dvs. om de är personuppgiftsbiträden till riksorganisationen eller ska anses gemensamt personuppgiftsansvariga.

Som Datainspektionen förstår det använder partiföreningarna/partidistrikten uppgifter ur medlemsregistret på eget initiativ till exempel utskick av information till medlemmarna i en partiförening eller ett partidistrikt. Partiförening/partidistrikt kan dessutom genomföra vissa ändringar i medlemsregistret till exempel ändra en medlems adress.

De uppgifter som Datainspektionen tagit del av talar för att partiföreningarna/partidistrikten har ett sådant faktiskt inflytande över behandlingarna av uppgifter avseende de personer som tillhör respektive förening/distrikt att

personuppgiftsansvaret ska anses vara gemensamt. Ett gemensamt personuppgiftsansvar innebär att även föreningen/distriktet har ett ansvar för att behandlingen av personuppgifter har stöd i personuppgiftslagen. För denna tillsyn, som är riktad mot riksorganisation, är det dock tillräckligt att konstatera att riksorganisationen har ett personuppgiftsansvar.

Vilka regler i personuppgiftslagen gäller för behandlingen av personuppgifter i medlemsregistret?
Datainspektionen gör bedömningen att Vänsterpartiets 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 behandlingen av personuppgifter i medlemsregistret bestämmelserna i personuppgiftslagen?
Datainspektionen har inga synpunkter på hur Vänsterpartiet 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. Datainspektionen bedömer att 17 § personuppgiftslagen ger såväl de lokala organisationerna som riksorganisationen, när det finns ett gemensamt personuppgiftsansvar, en rätt att behandla uppgift om medlemskap. Det gäller oavsett om medlemskapet formellt är knutet till riksorganisationen. 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.

I ärendet har framkommit att Vänsterpartiet behandlar uppgifter om tidigare medlemmar för återvärvning. Uppgiften om en tidigare medlem sparas i upp till ett år efter det att han/hon senast betalade sin medlemsavgift. Uppgifterna tas dock bort snarast om den registrerade begär det.

En uppgift om att en person *har varit* medlem i ett politiskt parti är även den en känslig personuppgift eftersom den kan anses avslöja en politisk åsikt. Datainspektionen har tidigare uttalat att uppgifter om tidigare medlemmar i en förening får behandlas upp till ett år för ändamålet återvärvning (se bl.a. s. 17 i Datainspektionens broschyr ”Hur länge får personuppgifter bevaras”). Grunden för detta ställningstagande är att en sådan behandling har stöd i en intresseavvägning enligt 10 § punkten f personuppgiftslagen. Intresseavvägningen kan dock inte ensamt ge stöd för att behandla känsliga personuppgifter. Det måste därför finnas ett stöd för partiets behandling enligt 15-19 §§ personuppgiftslagen för att behandlingen ska vara tillåten. Eftersom behandlingen avser en registrerad som inte längre är medlem i partiet ser Datainspektionen inte att partiet kan stödja sig på 17 § personuppgiftslagen. Inte heller ger bestämmelserna i 16 §, 18 § eller 19 § personuppgiftslagen stöd för att behandla uppgifter om en tidigare medlem för ändamålet återvärvning. Den rättsliga grund som partiet enligt Datainspektionens bedömning skulle kunna stödja sin behandling på är istället bestämmelserna i 15 § personuppgiftslagen om uttryckligt samtycke. Partiet har inte visat att man inhämtat ett sådant samtycke för behandlingen.

Datainspektionen kan således konstatera att Vänsterpartiets behandling av uppgifter om tidigare medlemmar för återvärvning strider mot 13 § personuppgiftslagen. För att partiet ska få behandla uppgifterna krävs ett samtycke från den tidigare medlemmen.

Datainspektionen förelägger därför, med stöd av 45 § första stycket personuppgiftslagen, Vänsterpartiet att antingen upphöra med att behandla uppgifter om tidigare medlemmar för ändamålet återvärvning eller inhämta de registrerades samtycke för behandlingen.

Vänsterpartiet har vidare uppgett att uppgifter i medlemsregistret sparas för statistik. Datainspektionen har i detta ärende inte närmare utrett på vilket sätt som Vänsterpartiet använder personuppgifter för statistikändamål. I sammanhanget vill dock myndigheten lämna följande vägledning. 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 i 19 § ger uttryck för en allmän avvägningsnorm där man ska göra en helhetsbedömning av samtliga omständigheter. Vid bedömningen ska beaktas bl.a. statistikprojektets vikt, hur pass kostsamt eller tidsödande det skulle vara att hämta in samtycke, i vilken utsträckning den enskilde skulle kunna skadas om man begärde samtycke och om en kontakt med den enskilde skulle kunna förrycka undersökningsresul-

tatet, hur pass svårt det är på grund av de behandlade uppgifterna att identifiera enskilda personer samt om information lämnas i någon form (prop. 1997/98:44 s. 127). Enligt Datainspektionens bedömning finns det ett klart samhällsintresse för statistik över medlemskap i ett politiskt parti. 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.

Lämnar Vänsterpartiet 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 sparas 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 den information om personuppgiftsbehandlingen som lämnas via Vänsterpartiets webbplats.

Den lagliga grunden för Vänsterpartiets 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.

Informationen som lämnas till medlemmar saknar uppgift om vem som är personuppgiftsansvarig, vilka kategorier av personuppgifter som behandlas, hur länge uppgifterna sparas, rätten att ansöka om registerutdrag samt rätten till rättelse av felaktiga eller missvisande uppgifter. Med hänsyn till nyssnämnda brister konstaterar Datainspektionen att Vänsterpartiet inte fullt ut

lever upp till de krav på information till medlemmar som ställs i 23-25 §§ personuppgiftslagen.

Datainspektionen förelägger därför, med stöd av 45 § första stycket personuppgiftslagen, Vänsterpartiet att komplettera den skriftliga information som lämnas till medlemmar ett sådant sätt att den uppfyller de krav som ställs i 23-25 §§ personuppgiftslagen.

Prenumeranter av partiets tidning får överhuvudtaget ingen information om hur Vänsterpartiet behandlar hans/hennes personuppgifter. Mot denna bakgrund konstaterar Datainspektionen att Vänsterpartiet brister i informationen till prenumeranter och inte lever upp till de krav som ställs i 23- 25 §§ personuppgiftslagen.

Datainspektionen förelägger därför, med stöd av 45 § första stycket personuppgiftslagen, Vänsterpartiet att informera samt ta fram rutiner för att informera prenumeranter på ett sådant sätt att kraven i 23-25 §§ personuppgiftslagen uppfylls.

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.

Frågan 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 multifaktors autentisering, 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 till medlemswebben, vilket ger åtkomst till personuppgifter i det centrala medlemssystemet, sker med användarnamn och lösenord. Datainspektionen konstaterar att det sätt för autentisering som Vänsterpartiet 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 Vänsterpartiet inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att behöriga användare har åtkomst till personuppgifter i det centrala medlemsregistret efter autentisering över öppet nät med enbart lösenord och användarnamn.

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

Nästa fråga är huruvida Vänsterpartiet 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.

Det är Datainspektionens bedömning att när ett politiskt parti behandlar uppgifter om medlemmar i ett medlemsregister så 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 Vänsterpartiet registreras inloggningen till medlemsportalen samt vissa ändringar som en behörig användare utför.

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 vissa ändringar kan spåras.

Datainspektionen förelägger därför, enligt 45 § första stycket personuppgiftslagen, Vänsterpartiet 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.

En viktig del i ett strukturerat Informationssäkerhetsarbete är att vidta förebyggande åtgärder. Det finns alltid en risk att säkerhetsbrister inte uppdagas förrän någon lyckas med att utnyttja den. Det gäller i än högre grad för system som enbart används av ett fåtal organisationer. Den risken kan minskas med hjälp av en säkerhetsgranskning av IT-systemet genom en utomstående part. Penetrationstester tjänar samma syfte som säkerhetsgranskningen, nämligen att upptäcka brister för att kunna vidta åtgärder innan någon obehörig har lyckats med det. Som ovan konstaterats är uppgifter om medlemskap i ett politiskt parti känsliga personuppgifter och därför ska skyddet vara extra starkt. Kostnaderna för en extern granskning och penetrationstester kan anses vara rimliga i förhållande till minskningen av risken för obehörig åtkomst till personuppgifterna i medlemssystemet. Datainspektionen rekommenderar därför att Vänsterpartiet genomför en extern granskning av medlemsystemets IT-säkerhet samt penetrationstester i syfte att förebygga obehörigt intrång i IT-systemet.

Under inspektionen framkom att Vänsterpartiet saknar rutiner för att testa att återläsning av säkerhetskopiorna fungerar och att säkerhetskopiorna sparas inlåsta i ett plåtskåp i ett angränsande rum till server i partiets lokaler.
I Datainspektionens allmänna råd om säkerhet för personuppgifter rekommenderas att man bör ha rutiner för säkerhetskopiering för att förhindra förlust av personuppgifter. En punkt i listan över vad en personuppgiftsansvarig bör se till att göra är att regelbundet prova att det går att återskapa säkerhetskopian. En annan punkt är att man bör förvara säkerhetskopiorna skyddad

och gärna i flera exemplar på olika skyddade platser. Med detta i åtanke rekommenderar Datainspektionen Vänsterpartiet att införa rutiner för test av återläsning av säkerhetskopior samt att se över förvaringen av dessa.

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.

Göran Gräslund

Jonas Agnvall