Datainspektionen

Datum	Diarienr
2012-05-31	1676-2011

Socialdemokraterna
Sveavägen 68
105 60 Stockholm

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

Datainspektionens beslut

Datainspektionen konstaterar följande brister vid Socialdemokraternas behandling av personuppgifter i personregistret:

- Den information som lämnas till medlemmar och bidragsgivare om personuppgiftsbehandlingen uppfyller inte fullt ut de krav som ställs i 23-25 §§ personuppgiftslagen.
- Behandlingen av uppgifter om tidigare medlemmar för ändamålet återvärvning strider mot 13 § personuppgiftslagen när det saknas stöd enligt 15-19 §§ personuppgiftslagen för att behandla uppgifterna.
- Behandlingen av uppgifter om uteslutna strider mot 13 § personuppgiftslagen när det saknas stöd enligt 15-19 §§ personuppgiftslagen att behandla uppgifterna.
- Utlämnandet av uppgifter till A-lotterierna AB strider mot 17 § personuppgiftslagen.

Datainspektionen konstaterar att Socialdemokraterna inte lever upp till de krav som ställs på säkerheten vid behandling av personuppgifter enligt 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 personregistret.
- Det går inte, genom behandlingshistorik, att utreda vem som har haft åtkomst till personuppgifter i personregistret.

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

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

- komplettera informationen som lämnas till medlemmar och bidragsgivare om personuppgiftsbehandlingen, i enlighet med vad som framförs på s. 11-12, så att informationen uppfyller de krav som ställs i 23-25 §§ personuppgiftslagen,
- antingen upphöra med att behandla uppgifter om tidigare medlemmar för ändamålet återvärvning eller inhämta de registrerades samtycke till behandlingarna,
- antingen upphöra med att behandla uppgifter om uteslutna eller inhämta de registrerades samtycke till behandlingarna. Det gäller dock inte i den mån en behandling av uppgifterna är nödvändiga för statistikändamål eller behandlas för forskningsändamål med stöd samtycke eller 19 § första stycket personuppgiftslagen,
- antingen upphöra med att lämna ut uppgifter om medlemmar till A-lotterierna AB eller förändra rutinerna så att behandlingen har stöd av ett samtycke från medlemmen,
- vidta åtgärder som innebär att åtkomst över öppet nät till personuppgifter i personregistret skyddas med stark autentisering,
- införa sådana tekniska funktioner som även gör det möjligt att utreda vem som har haft åtkomst till vilka personuppgifter i personregistret och när.

Datainspektionen förutsätter att Socialdemokraterna ser över sin behandling av medlemsuppgifter för forsknings- och statistikändamål.

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 8 december 2011 inspekterat Socialdemokraterna.

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

Allmänt om partiets organisation
Socialdemokraternas organisation grupperas i föreningar och klubbar på lokal nivå, arbetarekommuner på kommunal nivå och 26 partidistrikt som kan sägas motsvara länsindelningar samt partistyrelsen.

En medlem i det socialdemokratiska partiet erhåller vid sitt inträde sitt partimedlemskap i en förening/klubb i den kommun där medlemmen är bosatt. De socialdemokratiska föreningarna och klubbarna är partiets grundorganisation.

Behandling av personuppgifter i medlemsregister eller liknande
Socialdemokraterna har ett centralt IT-system, i vilket uppgifter om medlemmar, supporters, bidragsgivare och prenumeranter behandlas. Det centrala IT-systemet består, i allt väsentligt, av ett personregister som kommunicerar med ett antal olika komponenter. Följande komponenter finns; Prenumeration, Medlem, Interim, Kampanj/Insamling, Reskontra.

Personuppgifter om medlemmar lagras enbart i personregistret. Där registreras uppgifter om medlemsnummer, personnummer (obligatoriskt), kontaktuppgifter, historiska adresser, svenskt medborgarskap, fackligt medlemskap (frivilligt), medlemskap i svenska kyrkan, bidrag (belopp och tidpunkt), intresseområden (förkodad), och yrke (förkodad). Det finns dessutom ett fritextfält. I personregistret görs en s.k.

familjekoppling, som innebär att om flera medlemmar ingår i samma familj kopplas familjemedlemmarnas uppgifter för att endast ett utskick ska gå till den gemensamma adressen. En utesluten medlem ”flaggas” när medlemskapet avslutas. Orsaken till uteslutningen anges enligt en i förväg bestämd kod, t.ex. ej betalt.

I personregistret finns förutom uppgifter om medlemmar även uppgifter om andra, såsom supporters och prenumeranter. Med supporter avser partiet personer som på ett eller annat sätt anmält intresse för partiets politik. Med prenumeranter avses personer som prenumererar på medlemstidningen. För båda kategorier registreras kontaktuppgifter. För prenumeranter registreras dessutom betalningar samt prenumerationsuppgifter. Det finns även möjlighet att registrera personnummer och intresseområden för supportrar, men det är frivilligt. Beslut har fattats om att driften av det nuvarande supporterverktyget upphör senast vid halvårsskiftet 2012. Därefter kommer endast nyhetsbrevet finnas kvar.

Partiet har även en webbplats där en person, t.ex. kan ansöka om medlemskap. Om man använder det elektroniska formuläret för medlemsansökan på webbplatsen skickas personuppgifterna till komponenten Interim, där de lagras temporärt i avvaktan på att medlemsavgiften betalas.

Personuppgifter lagras för att administrera medlemskapet, prenumerationer och nyhetsbrev. Uppgifterna används även för att återvärva tidigare medlemmar och erbjuda medlemmarna kombilotteriet. Dessutom används uppgifterna till kampanjer för att samla in pengar till partiet. I övrigt sparas personuppgifterna för intern statistik och forskningsändamål. Uppgifterna sparas även för bokföringsändamål.

Uppgifter om medlemmar och prenumeranter behandlas för att fullgöra ett avtal med de registrerade. Uppgifter om supporters och övriga som får nyhetsbrev, behandlas med stöd av samtycke. Att erbjuda medlemmarna kombilotteriet bygger på partiets traditioner. Uppgifter om bidragsgivarna sparas enligt överenskommelse med andra partier.

Personuppgifter lämnas inte ut till tredje man. Partiet lämnar ut medlemsuppgifter till A-lotterierna AB (kombilotteriet) som till största delen ägs av partiet.

Personuppgiftsansvar
I enlighet med partiets stadgar ansvarar partiet centralt för ”utveckling av partiets gemensamma system för medlemsregister och avgiftsuppbörd. Partistyrelsen ansvarar även för ”registrering av samtliga enskilda medlemmar i partiets grundorganisationer liksom för uppbörd av medlemsavgifter. Respektive grundorganisation, arbetarekommun och partidistrikt ska ges tillgång till sin del av medlemsregistret.

Medlem i det socialdemokratiska partiet erhåller vid sitt inträde sitt partimedlemskap i grundorganisationen eller i den fria gruppen i arbetarekommunen i den primärkommun där medlemmen är bosatt.

Partistyrelsens kansli kan se, ändra och uppdatera alla medlemmars uppgifter inklusive uppgifter om givna gåvor.

Partidistrikten kan se, ändra och uppdatera sina medlemmars uppgifter, både personliga uppgifter och de uppgifter som har med medlemskapet att göra. Medlemmar bor vanligtvis inom distriktet.

Arbetarekommunerna kan se, ändra och uppdatera sina medlemmars uppgifter, både personliga uppgifter och de uppgifter som har med medlemskapet att göra. Medlemmar bor vanligtvis inom kommunen.

Den lokala organisationen, S-föreningen, kan via partiets intranät se medlemmar i den egna föreningen och vilka förtroendeuppdrag medlemmen har.

Utöver person- och medlemsuppgifter kan respektive organisationsled se och ändra uppgifter om uppdrag inom partiorganisation, landsting/region, kommun samt riksdag.

Enligt Socialdemokraterna är riksorganisationen personuppgiftsansvarig för behandling av personuppgifter i det centrala IT-systemet. I de delar som avser behandling av medlemmars personuppgifter är personuppgiftsansvaret gemensamt med respektive partidistrikt/arbetarekommun.

Information till den registrerade
På Socialdemokraternas webbplats lämnas information om hur partiets riksorganisation behandlar personuppgifter om medlemmar under rubriken ”integritetspolicy”. I samband med anmälan om medlemskap hänvisas till integritetspolicyn. Likaså informeras en gåvogivare eller en prenumerant på nyhetsbrev om integritetspolicyn i samband med att

man ger en gåva eller börjar prenumerera på partiets nyhetsbrev. Dessutom anges en länk till integritetspolicyn i varje nyhetsbrev.

Gallring av personuppgifter
Det är partistyrelsen som ansvarar för och gallrar personuppgifter i det centrala IT-systemet. Av partistadgarna framgår att man är medlem i partiet i 14 månader efter den senaste påminnelsen om betalning. Uppgifter om medlemmar sparas därefter ytterligare två år för att kunna återvärva tidigare medlemmar. Därefter avpersonifieras medlemmen, vilket innebär att uppgifter om medlemmens personnummer, adress, och telefonnummer tas bort. Medlemsnumret sparas dock. Uppgifter om bidragsgivare har inte gallrats sedan IT-systemet togs i drift år 2000. Det finns ett fåtal personer som flaggats som uteslutna ur partiet och deras personuppgifter gallras inte. Uppgifter om en supporter ska tas bort direkt när en sådan person anmält att de vill bli borttagna. Likaså ska uppgifter tas bort så snart personer som har nyhetsbrev anmält att de inte längre vill ha dessa.

IT-säkerhet
Inloggning till personuppgifter i personregistret via medlemswebben sker med användarnamn och lösenord samt ett mjukt organisationscertifikat. Parallellt med inloggning via medlemswebben kan partistyrelsen logga in via en PC-klient, som är installerad i endast tio datorer. För att använda PC-klienten krävs inloggning till intranätet plus en windowsinloggning. Båda nyssnämnda inloggningar kräver användarnamn och lösenord. Via PC-klienten har användaren åtkomst till hela IT-systemet, då även personregistret. Dessutom finns det möjlighet att få åtkomst till medlemsuppgifter via medlemsportalen genom inloggning med användarnamn och lösenord.

Det finns fyra behörighetsnivåer för det centrala IT-systemet. Den högsta behörigheten har systemadministratören (en person), som är den som registrerar nya användare i behörighetskontrollsystemet. Näst högsta nivån är s.k. full behörighet (300 personer), som innebär behörighet att lägga till, ändra och läsa alla uppgifter i databasen. På behörighetsnivå 2 (50 personer) kan användaren ändra och läsa men inte lägga till uppgifter. På behörighetsnivå ett (50 personer) kan användaren endast läsa.

Behörighetstilldelningen går till så att arbetarkommunen anmäler till partidistriktets medlemsansvarig att man vill ha en användare med viss behörighet. Partidistriktet medlemsansvarig beställer, via e-post, en uppläggning av behörigheten hos administratören i partistyrelsen. Par-

tistyrelsen kontrollerar uppgifterna och lägger upp en ny behörighet. Partistyrelsen bestämmer användarnamn och lösenord, som skickas via e-post till användaren. Partistyrelsen rensar manuellt ett till användaren sänt e-postmeddelande med användarnamn och lösenord. När någon användare slutar får partistyrelse via partidistriktets medlemsansvarig ett meddelande om detta och partistyrelsen tar bort användaren från behörighetssystemet.

Kommunikationen mellan webbplats och IT-systemet (interim) är krypterad med https vid överföring av uppgifter i samband med att en person anmäler sig som medlem via webbplatsen.

Det går inte genom behandlingshistorik att avgöra i detalj vilken ändring i en person- eller medlemsuppgift som gjorts. Uppgift om vem som gjort senaste ändringen och när den gjorts sparas dock.

Skäl för beslutet

Vem är personuppgiftsansvarig för behandling av personuppgifter i personregistret?
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 Socialdemokraterna är riksorganisationen personuppgiftsansvarig för behandling av personuppgifter i personregistret. I de delar som avser behandling av medlemmars personuppgifter är personuppgiftsansvaret gemensamt med respektive partidistrikt/arbetarekommun.

Datainspektionen delar Socialdemokraternas 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 Socialdemokraternas 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 Socialdemokraterna behandlar personuppgifter om medlemmar och andra i personregistret 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 lokala föreningar/klubbar. 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.

Av vad som framkommit sparar Socialdemokraterna uppgifter om medlemmar även efter det att medlemskapet upphört. Uppgifter om en tidigare medlem kan komma att sparas upp till 14 månader efter den senaste påminnelsen och därefter ytterligare två år för ändamålet återvärvning. Därefter ”avpersonifieras” uppgifterna genom att personnummer, adress och telefonnummer tas bort.

I sammanhanget vill Datainspektionen förtydliga följande kring avpersonifiering. För att informationen ska anses avpersonifierad krävs att det inte längre går att härleda informationen till en tidigare medlem. Om det efter behandlingen fortfarande går att göra en sådan koppling måste den fortsatta behand-

lingen av informationen följa bestämmelserna i personuppgiftslagen eftersom det är fråga om en behandling av personuppgifter.

En uppgift om att en person *har varit* medlem i ett politiskt parti är också 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 också 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 Socialdemokraternas behandling av uppgifter om tidigare medlemmar för återvärvning strider mot 13 § personuppgiftslagen. För att partiet ska få behandla uppgifterna för återvärvning behöver partiet inhämta ett samtycke från den tidigare medlemmen.

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

Socialdemokraterna har även uppgett att uppgifter i medlemsregistret sparas för statistik och forskningsändamål.

Vad först gäller behandling av känsliga personuppgifter för statistiska ändamål vill Datainspektionen påpeka följande. 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. Statistik av-

seende medlemskap i ett politiskt parti kan enligt Datainspektionen anses ha ett sådant samhällsintresse som kan väga över intrånget i den enskildes personliga integritet. En bedömning måste dock 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 endast sparas så länge som de behövs för detta statistikändamål.

Vad sedan avser användningen av känsliga personuppgifter för forskningsändamål vill Datainspektionen påpeka att en sådan forskning kräver ett samtycke från den registrerade eller, enligt 19 § första stycket personuppgiftslagen, ett godkännande enligt lagen (2003:460) om etikprövning av forskning som avser människor.

I den mån uppgifterna i personregistret, utöver statistik, används för forskning, enligt definitionen av forskning i lagen (2003:460) om etikprövning, vill Datainspektionen påpeka följande. En forskning som innefattar en behandling av känsliga personuppgifter ska etikprövas. Dessutom kräver en sådan forskning ett samtycke från den registrerade eller ett godkännande av en etikprövningsnämnd att forskningen får genomföras utan uttryckligt samtycke.

Datainspektionen förutsätter att Socialdemokraterna ser över sin behandling av medlemsuppgifter för statistik och forskningsändamål och beaktar vad som framförts ovan.

Vidare sparar Socialdemokraterna uppgifter om tidigare medlemmar som uteslutits. Även denna behandling är en behandling av känsliga personuppgifter, varför behandlingen måste ha stöd i 15-19 §§ personuppgiftslagen. Någon sådant stöd för behandlingen har Socialdemokraterna inte visat. Datainspektionen konstaterar därför att Socialdemokraternas behandling av uppgifter avseende personer som uteslutits strider mot 13 § personuppgiftslagen. Hänsyn måste dock tas till att uppgifter om uteslutna kan komma att behandlas för statistik- eller forskningsändamål.

Datainspektionen förelägger därför, med stöd av 45 § första stycket personuppgiftslagen, Socialdemokraterna att antingen upphöra med att behandla uppgifter om personer som uteslutits eller inhämta de registrerades samtycke för behandlingen. Det gäller dock inte i den mån en behandling av uppgifterna är nödvändiga för statistikändamål eller behandlas för forskningsändamål med stöd av samtycke eller 19 § första stycket personuppgiftslagen.

Utlämnande av uppgifter till A-lotteriet
Känsliga personuppgifter som behandlas av en politisk organisation får enligt 17 § personuppgiftslagen endast lämnas ut till tredje man om den registrerade uttryckligen har samtyckt till det.

Av utredningen i ärendet har framkommit att uppgifter om medlemmar lämnas ut till A-lotterierna AB (Kombilotteriet). Något rättsligt stöd för utlämnandet har Socialdemokraterna inte kunnat visa. Datainspektionen konstaterar att utlämnandet som det sker idag strider mot bestämmelsen i 17 § andra stycket personuppgiftslagen eftersom det saknas ett uttryckligt samtycke från de registrerade. För att Socialdemokraterna ska få lämna ut uppgifter till A-lotteriet krävs att medlemmen samtycker till behandlingen och att ändamålet är förenligt med de ändamål för vilka uppgifterna samlades in.

Datainspektionen förelägger därför, med stöd av 45 § första stycket personuppgiftslagen, Socialdemokraterna att antingen upphöra med att lämna ut medlemsuppgifter till A-lotterierna AB eller förändra rutinerna så att behandlingen sker med ett samtycke från medlemmarna.

Lämnar Socialdemokraterna 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 som lämnas till de registrerade på Socialdemokraternas webbplats.

Vid anmälan om medlemskap via Socialdemokraternas webbplats krävs att man godkänner behandlingen av personuppgifter genom att kryssa i en ruta. I samband med detta lämnas den information som framkommer under redogörelsen för tillsynsärendet.

Den lagliga grunden för Socialdemokraternas 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 av 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, t.ex. ett utlämnande av medlemsuppgifter till A-lotterierna AB, hindrar det inte att partiet begär in ett samtycke på detta sätt vad avser just denna behandling.

Informationen som lämnas till blivande medlemmar saknar information om flera av de kategorier av personuppgifter som behandlas t.ex. medlemsnummer, svensk medborgarskap, facklig medborgarskap, intresseområden och yrke. Det saknas också information om att medlemsuppgifterna kan komma att användas för återvärvning, erbjudande av kombilotteriet, insamlingskampanjer, intern statistik, forskningsändamål samt bokföring. Det är också viktigt att det av informationen framgår att partidistrikt/arbetarekommuner har ett gemensamt personuppgiftsansvar tillsammans med riksorganisationen vad avser behandling av medlemmars personuppgifter.

Med hänsyn till nyssnämnda brister konstaterar Datainspektionen att Socialdemokraterna 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, Socialdemokraterna att komplettera information som lämnas till medlemmar om personuppgiftsbehandlingen på ett sådant sätt att den uppfyller de krav som ställs i 23-25 §§ personuppgiftslagen.

Vad sedan gäller information till andra kategorier av registrerade än medlemmar konstaterar Datainspektionen att det brister i informationen hur länge uppgifter sparas om gåvogivare och för vilka ändamål. Sådan väsentlig information som ska lämnas till en gåvogivare innefattar även information om att gåvornas belopp och tidpunkt registreras.

Datainspektionen förelägger därför, med stöd av 45 § första stycket personuppgiftslagen, Socialdemokraterna att komplettera information som lämnas till bidragsgivare om personuppgiftsbehandlingen på ett sådant sätt att den uppfyller de krav som ställs i 23-25 §§ personuppgiftslagen.

Det konstateras vidare att det saknas information till personer som registreras som supportrar i Socialdemokraternas personregister. Såsom Datainspektio-

nen uppfattar det håller partiet på att avveckla denna registrering, varför det saknas skäl för Datainspektionen att vidta någon åtgärd i denna del.

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 personregistret 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 personregistret, sker över öppet nät med användarnamn och lösenord samt ett mjukt organisationscertifikat. Parallellt med inloggning via medlemswebben kan partistyrelsen logga in via en PC-klient. För att använda PC-klienten krävs inloggning till intranätet plus en windowsinloggning. Båda nyssnämnda inloggningar kräver användarnamn och lösenord. Via PC-klienten har användaren åtkomst till hela IT-systemet, då även personregistret. Datainspektionen konstaterar att de sätt för autentisering som Socialdemokraterna tillämpar är inte tillräckliga eftersom inget av dem innebär en stark autentisering. Detta innebär i sin tur att personuppgifter 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 Socialdemokraterna inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att behöriga användare har åtkomst över öppet nät till personuppgifter i personregistret efter autentisering med enbart lösenord och användarnamn.

Datainspektionen förelägger, enligt 45 § första stycket personuppgiftslagen, Socialdemokraterna att vidta åtgärder som innebär att åtkomst över öppet nät till personuppgifter i personregistret skyddas med stark autentisering.

Nästa fråga är huruvida Socialdemokraterna 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.

Datainspektionens 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 Socialdemokraterna för partiet en behandlingshistorik över vem som har gjort en ändring och när. Det går dock inte att avgöra i detalj vilken ändring i en person- eller medlemsuppgift som gjorts. Det förekommer ingen regelbunden granskning av behandlingshistoriken.

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 om användaren gjort en ändring går detta att

spåra genom partiets behandlingshistorik. Någon regelbunden granskning av behandlingshistoriken krävs inte. Det är tillräckligt att genomföra granskning vid en incident. Det ska dock finnas rutiner för granskningen.

Datainspektionen förelägger, enligt 45 § första stycket personuppgiftslagen, Socialdemokraterna att införa sådana tekniska funktioner som även gör det möjligt att utreda vem som har haft åtkomst till vilka personuppgifter i medlemsregistret och när.

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 Socialdemokraterna genomför en extern granskning av medlemsystemets IT-säkerhet samt penetrationstester i syfte att förebygga obehörigt intrång i IT-systemet.

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