Datainspektionen

Datum	Diarienr
2012-05-31	1672-2011

Sverigedemokraterna
Box 26
291 21 Kristianstad

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

Datainspektionens beslut

Datainspektionen konstaterar följande brister vid Sverigedemokraternas behandling av personuppgifter i 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 andra registrerade än medlemmar om hur Sverigedemokraterna behandlar deras personuppgifter. Sverigedemokraterna 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 §§ personuppgiftslagen att behandla uppgifterna.
- Behandlingen av uppgifter om uteslutna, i syfte att motverka att personer återregistreras som medlemmar, strider mot 13 § personuppgiftslagen när det saknas stöd enligt 15-19 §§ personuppgiftslagen att behandla uppgifterna.

Datainspektionen konstaterar att Sverigedemokraterna 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 till medlemsregistret via fjärråtkomst över öppet nät med enbart användarnamn och lösenord.

- Det går inte att, genom behandlingshistorik, utreda vem som har haft åtkomst till vilka personuppgifter i medlemsregistret 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, Sverigedemokraterna att:

- komplettera informationen som lämnas till medlemmar om personuppgiftsbehandlingen, i enlighet med vad som framförs på s. 10-11, så att informationen uppfyller de krav som ställs i 23-25 §§ personuppgiftslagen.
- informera samt ta fram rutiner för att informera även andra registrerade än medlemmar på ett sådant sätt att kraven i 23-25 §§ personuppgiftslagen uppfylls.
- antingen upphöra med att behandla uppgifter om tidigare medlemmar för ändamålet återvärvning eller inhämta samtycke för behandlingarna.
- antingen upphöra med att behandla uppgifter om personer som uteslutits ur partiet, i syfte att motverka att personer återregistreras som medlemmar, eller inhämta samtycke för behandlingarna.
- skydda fjärråtkomst över öppet nät till personuppgifter i medlemsregistret med stark autentisering.

Datainspektionen förutsätter att Sverigedemokraterna inför sådana tekniska funktioner som gör det möjligt att utreda vem som har haft åtkomst till vilka personuppgifter i medlemsregistret 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. 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 10 januari 2012 inspekterat Sverigedemokraterna.

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

> *Allmänt om partiets organisation*
> Sverigedemokraternas organisation är indelad i riksorganisation, distrikt (länsnivå) och lokalavdelningar (kommunalnivå) samt utland (personer som bor utomlands).
>
> Medlemmen är ansluten till riksorganisationen. Det är medlemmens folkbokföringsadress som styr var han eller hon placeras i organisationen. Därtill kan man vara medlem i ungdomsförbundet (SDU) och/eller kvinnoförbundet (SD-kvinnor), vilket inte förutsätter medlemskap i riksorganisationen.
>
> Man kan ansöka om medlemskap genom att fylla i ett formulär på riksorganisationens webbplats eller genom att betala medlemsavgiften via det inbetalningskort som riksorganisationen skickar till en intressent. Det är även möjligt att ingå ett ”ständigt medlemskap” i partiet genom att betala en klumpsumma. Medlemskapet fortsätter då att löpa så länge man inte begär utträde.

Behandling av personuppgifter i medlemsregister eller liknande
Sverigedemokraterna har ett centralt medlemsregister. Förutom partimedlemmar i Sverigedemokraterna och ungdomsförbundet omfattar medlemsregistret följande kategorier; prenumeranter, intressenter, okynnesanmälda, uteslutna medlemmar, utestängda och kandidater till val.

Med intressenter avses personer som vill ha kontinuerlig information, inte engångsutskick. Okynnesanmälda är personer som själva vänt sig till partiet och anmält att de vill bli listade som spärrade från medlemskap, t.ex. på grund av att de av någon annan blivit anmälda som medlemmar och vill förhindra att det händer igen. Med utestängda avses personer som ansökt men inte fått bli medlemmar, t.ex. för att man inte delar partiets värderingar. Det är lokalavdelningens kännedom om personen som ligger till grund för att inte godkänna en person som medlem i partiet. Med uteslutna avses medlemmar som uteslutits ur partiet, t.ex. på grund av att deras medlemskap ansetts skadligt för partiets politik. Det krävs starka skäl för uteslutning. Kandidering till val förutsätter inte partimedlemskap och uppgifter om kandidater registreras därför i denna kategori. En kommentar om utesluten eller utestängning skrivs i ett fritextfält men orsaken till uteslutning eller utestängning noteras inte.

Vid anmälan om medlemskap via partiets webbplats lagras uppgifterna temporärt på webbservern. Innan uppgifterna registreras i medlemsregistret gör man en kontroll eftersom partiet har problem med okynnesanmälningar, dvs. att någon anmäler en annan person, t.ex. en lärare. Kontrollen går till så att Sverigedemokraterna skickar e-post till den som står som sökande, som bekräftar att han eller hon har för avsikt att bli medlem i partiet.

För medlemmar behandlas följande uppgifter i medlemsregistret; fullständigt namn, folkbokföringsadress, kontaktadress, födelsedatum, kommun, församling, introduktionsdatum, medlemskapshistorik, kön, telefonnummer, e-postadress, prenumerationsuppgifter, förtroendeuppdrag, datum för adressverifiering, tillträde till intranätet, medlemskap i SDU och SD-kvinnor samt id-nummer. Personnummer registreras om personen själv uppger det. I annat fall registreras endast födelsedatum. I registret finns det, för varje person, ett fritextfält för ytterligare kommentarer. Där fyller partiet in uppgifter som kan vara av intresse såsom yrke, bakgrund och färdigheter, t.ex. ungdomsledare, fotograf, erfarenhet av kommunalpolitik. Det finns även en kryssruta för ”fädernes

kyrka", vilket enligt partiet inte används idag. Det är en planerad framtida underkategori för kyrkopolitiskt aktiva.

Det finns en manuell rutin för att uppdatera adressuppgifter. Varje dag kontrolleras adressuppgifter för cirka 60 stycken registrerade. Kontrollen görs bland annat mot ett kreditupplysningsföretags register.

Personuppgifterna i medlemsregistret behandlas för att administrera medlemskapet, prenumerationer och för kontinuerlig information. Personuppgifterna används även för att återvärva tidigare medlemmar. Vid uteslutning av en medlem sparas personuppgifterna för att personen inte ska ansöka om nytt medlemskap. Därtill sparas personuppgifterna för statistik, fakturering och bokföringsändamål.

Personuppgifter om medlemmar behandlas för att fullgöra avtalet med medlemmen. Personuppgifter om intressenter behandlas med stöd av samtycke och uppgifter om uteslutna/utestängda behandlas med stöd av en intresseavvägning.

Personuppgiftsansvar
Det är riksorganisationen som är personuppgiftsansvarig för behandlingen av personuppgifter i medlemssystemet och webbplats. All registrering, ändring, uppdatering, gallring i medlemsregistret sker manuellt hos riksorganisationen, som även skickar ut och tar emot medlemsavgifter samt utfärdar kort för medlemskap i partiet. Distrikten har ingen direkttillgång till medlemsuppgifter utan måste gå via riksorganisationen.

Information till den registrerade
Vid anmälan om medlemskap via Sverigedemokraternas webbplats krävs att man godkänner behandlingen av personuppgifter genom att kryssa i en ruta. I samband därmed lämnas även information om personuppgiftsbehandlingen.

Vid nyregistrering och uppgiftsändring fick medlemmen tidigare en kopia via e-post med ett utdrag med vissa uppgifter från medlemsregistret. Detta har partiet upphört med. Nu skickas endast en bekräftelse på att de anmält/skickat något till Sverigedemokraterna.

Sverigedemokraterna skickar även ett årligt följebrev till sina medlemmar. Tanken är att samma information om personuppgiftsbehandlingen som ges på partiets webbplats ska lämnas i följebrevet.

Gallring
Vid inspektionen uppgav Sverigedemokraterna att personuppgifter i medlemsregistret gallras manuellt efter sju års inaktivitet samt att en person på begäran kan bli avaktiverad. I senare skriftväxling har partiet uppgett att alla personer har ett ”bäst före”-datum. Medlemsregistret gås fortlöpande igenom för att verifiera adresser, varvid personer där ”bäst före”-datumet har löpt ut raderas. I praktiken innebär det två år. Om medlemsavgiften för 2011 inte betalas skickas påminnelser ut under 2012. Vid sommaren 2013 passeras ”bäst före”-datumet om medlemmen inte betalat. Då gallras uppgiften.

IT-säkerhet
Sverigedemokraternas medlemsregister är ett internt system som partiet själva administrerar. Systemet kommunicerar inte med andra system.

Det finns två behöriga användare till medlemsystemet. En person genererar och distribuerar lösenord. De behöriga användarna har samma lösenord. Det finns regler och krav på längd på lösenord för inloggning till medlemssystemet. Det finns inga tvingande byten av lösenord.

En behörig användare har även fjärråtkomst till medlemsregistret. För att kunna logga in på distans i medlemsregistret krävs först att datorns hårddisk, som är krypterad, låses upp. Det sker med hjälp av ett lösenord. Därefter måste användaren logga in på sin dator med ett windows-lösenord. Sedan måste användaren aktivera VPN-förbindelsen, mellan datorn och medlemssystemet, med hjälp av ett lösenord. När VPN-förbindelsen är skapad kan användaren logga in till medlemssystemet med sitt lösenord för systemet.

Eftersom det endast finns ett användarkonto med åtkomst till medlemsregistret och två behöriga användare har partiet inte ansett det nödvändigt att föra loggar eller att göra uppföljningar av loggar.

Det finns rutiner för säkerhetskopiering av medlemsregistret. Det sker genom daglig kopiering till hårddisk, som förvaras på annan ort.

Vid Datainspektionens inspektion konstaterades att IT-utrustningen för medlemsregistret stod placerad i ett kontorslandskap dit samtliga anställda på partikansliet hade åtkomst. Efter inspektionen har partiet vidtagit åtgärd genom att placera utrustningen i ett låst skåp.

Riksorganisationen kan på begäran från distrikten mejla en lista på medlemmar för utskick, t.ex. årsmöte. Listan skickas i form av en kryp-

terad textfil som bilaga till ett mejl. Lösenordet för dekryptering av textfilen meddelas via telefon till en för riksorganisationen känd person i distriktet. På distrikts- och lokalnivå finns instruktioner om att listan ska tas bort när den har använts för sitt syfte.

Vid en ansökan om medlemskap via webbformuläret lagras personuppgifter temporärt i en webbserver till dess att man blir godkänd som medlem. När en enskild fyller i webbformuläret skyddas kommunikationen genom kryptering (https). Den som ansöker får en bekräftelse per e-post. Efter godkännande av medlemsansökan registreras uppgifterna manuellt i medlemsregistret och tas bort från webbservern.

Inloggning till webbservern kräver lösenord. Det är inte tvingande att byta lösenord. Åtkomsten till webbservern, där webbformulär för ansökan om medlemskap finns lagrad, sker över en krypterad förbindelse.

Ett personuppgiftsbiträdesavtal med riksorganisationens webbhotellsleverantör tecknades den 23 januari 2012.

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.

Mot bakgrund av vad som framkommit under redogörelsen ifrågasätter inte Datainspektionen att riksorganisationen är personuppgiftsansvarig för behandlingen av personuppgifter i det centrala medlemsregistret.

Fråga uppkommer emellertid om hanteringen av medlemslistorna innebär antingen ett gemensamt personuppgiftsansvar eller om distrikten och lokalavdelningarna är personuppgiftsbiträden till riksorganisationen.

Som Datainspektionen förstår det är det distriktet eller lokalavdelningarna som på eget initiativ begär ut uppgifter från medlemsregistret. Det finns inget krav från riksorganisationen att distrikt eller lokalförening ska skicka ut information. Lokalföreningarna bestämmer således över när, var och hur information ska skickas till de lokala medlemmarna samt vilken information som ska skickas. Vilka uppgifter samt vad uppgifterna får användas till begränsas emellertid av de villkor som riksorganisationen bestämmer. Likaså har riksorganisationen ställt villkor på t.ex. gallring av medlemslistorna.

Det är Datainspektionens bedömning att såväl riksorganisationen som distrikt och lokalföreningar har ett sådant faktiskt inflytande över medlemslistorna att de ska anses som gemensamt personuppgiftsansvariga för hanteringen av personuppgifterna i dessa. Övrig hantering av personuppgifter i medlemsregistret är riksorganisationen ensamt personuppgiftsansvarig för.

Vilka regler i personuppgiftslagen gäller för behandlingen av personuppgifter i medlemsregistret?
Datainspektionen gör bedömningen att Sverigedemokraternas 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 Sverigedemokraterna behandlar personuppgifter om medlemmar och andra registrerade 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. När 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 riksorganisationen. Skälet till detta är att det finns en tydlig koppling 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 Sverigedemokraterna behandlar uppgifter om tidigare medlemmar för återvärvning och att uppgifterna tas bort när ett s.k. ”bäst-före”-datum löpt ut. I praktiken är det två år. Därtill sparar partiet uppgifter om personer som uteslutit ur partiet. Syftet är att förhindra att dessa ska kunna bli medlemmar igen. Som rättslig grund för att spara uppgifterna om tidigare medlemmar och uteslutna medlemmar har Sverigedemokraterna hänvisat till intresseavvägningen i 10 § personuppgiftslagen.

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

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

Datainspektionen konstaterar vidare att behandlingen av uppgifter om uteslutna, i syfte att förhindra att dessa återregistreras som medlemmar, saknar stöd i 15-19 §§ personuppgiftslagen.

Datainspektionen förelägger därför, med stöd av 45 § första stycket personuppgiftslagen, Sverigedemokraterna att antingen upphöra med att behandla uppgifter om personer som uteslutits ur partiet, i syfte att förhindra att dessa återregistreras som medlemmar, eller inhämta samtycke för behandlingarna.

Sverigedemokraterna har även uppgett att man använder medlemsuppgifter för statistikändamål. Datainspektionen har i detta ärende inte närmare utrett på vilket sätt som Sverigedemokraterna 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 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 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.

Lämnar Sverigedemokraterna 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 Sverigedemokraternas webbplats.

Den lagliga grunden för Sverigedemokraternas 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. Det hindrar dock inte att ett parti, som vill använda uppgifter om medlemmar för andra ändamål än medlemsadministration begär in ett separat samtycke för denna behandling. Som framkommit tidigare kan samtycke t.ex. vara ett sätt att få behandla uppgifter om tidigare medlemmar för återvärvning.

Datainspektionen konstaterar att informationen som lämnas till blivande medlemmar saknar uppgift om vilka kategorier av personuppgifter som behandlas, hur länge uppgifterna sparas samt att uppgifterna används för fler ändamål än utskick av information.

Vidare konstateras det att det saknas information om att medlemmars kontaktuppgifter lämnas ut till distrikt och lokalavdelningar i form av listor. Det är också viktigt att det av informationen framgår att distrikt och lokalföreningar har ett gemensamt personuppgiftsansvar för behandling av personuppgifter i medlemslistorna.

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

Intressenter, okynnesanmälda, kandidater till val som inte är medlemmar, utestängda och uteslutna personer får ingen information om hur Sverigedemokraterna behandlar dessa kategoriers personuppgifter.

Datainspektionen förelägger därför, med stöd av 45 § första stycket personuppgiftslagen, Sverigedemokraterna att informera samt ta fram rutiner för att informera även andra registrerade än medlemmar 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.

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

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

Datainspektionen har flera gånger tidigare bedömt att känsliga 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.

Sverigedemokraterna har två behöriga användare till det centrala medlemsregistret. En av dessa har fjärråtkomst till medlemsregistret. För att kunna logga in på distans i medlemregistret krävs först att datorns hårddisk, som är krypterad, låses upp. Det sker med hjälp av ett lösenord. Nästa steg är att logga in på den egna datorn med ett lösenord. Därefter måste användaren aktivera en VPN-förbindelse, med hjälp av lösenord, mellan den egna datorn och den datorn på Sverigedemokraternas kansli. När VPN-förbindelsen är skapad kan användaren logga in till medlemsregistret med sitt lösenord för systemet. Detta innebär att vid inloggning via fjärråtkomst autentiseras den behörige användaren med användarnamn och lösenord. Därmed uppfylls inte kravet på stark autentisering, vilket i sin tur innebär att personuppgifterna i medlemsregistret inte är tillräckligt skyddade mot obehörig åtkomst.

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 inloggnings-

uppgifterna 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 Sverigedemokraterna inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att en behörig användare har åtkomst över öppet nätt till personuppgifter i medlemsregistret efter autentisering med enbart lösenord och användarnamn.

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

Nästa fråga är huruvida Sverigedemokraterna 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. En behandlingshistorik behövs normalt inte om endast en person använder utrustningen.

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. Det ska också finnas rutiner för en sådan uppföljning. Det behöver inte vara regelbundna kontroller utan det kan räcka att man vid en incident kan utreda vem som har haft åtkomst till eller ändrat uppgifter i medlemsregistret.

Sverigedemokraterna har uppgett att det endast finns ett användarkonto som ger åtkomst till personuppgifter i medlemsregistret och att två personer använder sig av detta konto. Partiet har av den anledningen inte ansett det nödvändigt att ha en behandlingshistorik.

Datainspektionen bedömer att Sverigedemokraterna måste ha en behandlingshistorik som gör det möjligt att utreda vem som haft åtkomst, ändrat eller raderat personuppgifter i medlemsregistret och när händelsen inträffade. Det gäller oavsett att det är ett fåtal personer som har behörig åtkomst till personuppgifter i medlemsregistret. Av det följer att varje användare ska ha ett personligt konto vid inloggning.

Datainspektionen förutsätter att Sverigedemokraterna inför 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.

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