Datainspektionen

Datum	Diarienr
2012-06-04	1675-2011

Kristdemokraterna
Box 2373
103 18 STOCKHOLM

Tillsyn enligt personuppgiftslagen (1998:204) - Kristdemokraternas behandling av personuppgifter i ett centralt medlemsregister

Datainspektionens beslut

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

- Den information som lämnas om behandlingen av personuppgifter till medlemmar och andra registrerade uppfyller inte fullt ut de krav som ställs i 23-25 §§ personuppgiftslagen.
- Behandlingen av uppgifter om tidigare medlemmar strider mot 13 § personuppgiftslagen när det saknas stöd i 15-19 §§ personuppgiftslagen.

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

- Det går att få åtkomst till personuppgifter i medlemsregistret över öppet nät genom att autentisera sig som behörig användare med enbart användarnamn och lösenord.
- Medlemsuppgifter skickas i en okrypterad excelfil, som en bilaga i ett e-postmeddelande, via öppet nät till ett tryckeri.
- Vid ansökan om medlemskap via webbformuläret överförs uppgifterna från sökanden okrypterat till webbservern.
- Det går inte, genom behandlingshistoriken, att utreda vem som har haft åtkomst till personuppgifter i medlemsregistret.

Datainspektionen förelägger, med stöd av 45 § första stycket personuppgiftslagen, Kristdemokraterna 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 andra registrerade om behandlingen av personuppgifter så att informationen uppfyller de krav som ställs i 23-25 §§ personuppgiftslagen (se sid. 10 Skäl för beslutet),
- antingen upphöra med att behandla uppgifter om tidigare medlemmar eller inhämta ett samtycke eller uppvisa något annat rättsligt stöd för behandlingarna,
- skydda åtkomsten till personuppgifter i det centrala medlemsregistret med stark autentisering,
- upphöra med att skicka medlemsuppgifter i en okrypterad excelfil via öppet nät till tryckeriet,
- skydda överföringen av personuppgifter via webbformuläret genom kryptering,

Datainspektionen förutsätter att Kristdemokraterna ser över sin behandling av medlemsuppgifter för statistik.

Datainspektionen förutsätter att Kristdemokraterna ser över behandlingshistoriken och inför sådana tekniska funktioner som gör det möjligt att utreda vem som har haft åtkomst till vilka personuppgifter i medlemsregistret och när.

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 genom en riksorganisation på nationell nivå och föreningar på regional och lokalnivå. Utöver detta finns 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 avslöjar politiska åsikter och 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 den. Känsliga personuppgifter kan också behandlas med 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 av personuppgifter.

Redogörelse för tillsynsärendet
Som ett led i projektet har Datainspektionen den 1 februari 2012 inspekterat Kristdemokraterna (riksorganisationen).

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

Allmänt om partiets organisation
Partiet är organiserat i en riksorganisation, distrikt på länsnivå och lokalavdelningar på kommunnivå. Enligt stadgarna är man medlem i en lokalförening.

Behandling av personuppgifter i medlemsregister eller liknande
Kristdemokraterna har ett centralt medlemsregister över samtliga medlemmar i lokalföreningarna, samt medlemmar i de associerade förbunden studentförbundet, kvinnoförbundet, ungdomsförbundet och seniorförbundet. Drift och administration av registret sker centralt. Lokalföreningarna uppmanas att använda den mjukvara som riks-organisationen erbjuder för att få åtkomst till och kunna använda det centrala medlemsregistret.

I det centrala medlemsregistret registreras även uppgifter om utställare, t.ex. vid partiets kongresser, då namn och fakturaadress registreras. Även vissa prenumeranter som inte är medlemmar och personer som uttryckligen begärt att få kontinuerlig information registreras i medlemsregistret.

För medlemmar registreras uppgifter om namn, adress, telefonnummer, personnummer, vilken lokalförening man tillhör och vilket eventuellt associerat förbund man är medlem, prenumerant av tidning, om eventuella organisatoriska och politiska uppdrag. För varje medlem

registreras ett personidnummer. Olika koder anger de olika politiska uppdrag som en medlem kan ha. I registret finns följande spärrkoder för medlemmar som inte längre är medlemmar; utträde ekonomiska skäl, ideologiska skäl och utträde övriga skäl. I 95 procent av fallen anges koden utträde övriga skäl.

Uppgifter om personnummer behövs för att undvika dubbelregistrering och för att säkert kunna identifiera att det är rätt person som registreras samt för att Ungdomsförbundet behöver uppge medlemmens personnummer när de söker bidrag.

Uppgifter om de registrerade hämtas in från de registrerade själva.

Medlemsuppgifterna används för administration av medlemskapet, hålla reda på vem som har vilket uppdrag, att informera, faktura- och statistikändamål. Uppgifterna används inte för återvärvning eller för historiska ändamål.

Medlemsuppgifter behandlas med stöd av avtal med den registrerade. Uppgifter om personer som inte är medlemmar men intresserade av information och vissa prenumeranter registreras med stöd av samtycke.

Personuppgifter i medlemsregistret lämnas inte ut för reklamändamål.

I medlemskapet ingår att alla medlemmar fyra gånger om året får tidningen Kristdemokraten. Partiet samkör då medlemsregistret och prenumerationsregistret för att göra ett urval av de medlemmar som inte är prenumeranter av tidningen. Uppgifter om namn och adress på medlemmar som inte är prenumeranter av tidningen lämnas ut i en okrypterad excelfil, som skickas som bilaga i ett e-postmeddelande till det tryckeri som trycker tidningen. Tryckeriet är ett personuppgifts-biträde till riksorganisationen. Kristdemokraterna upprättar ett skriftligt personuppgiftsbiträdesavtal med tryckeriet.

Personuppgiftsansvar
Kristdemokraterna anser att riksorganisationen är personuppgifts-ansvarig för behandlingen av personuppgifter i det centrala medlemsregistret. Riksorganisationen bestämmer över ändamålen och medlen för behandling av personuppgifter samt sköter drift och administrationen av registret centralt.

Personer som centralt anmält intresse att bli medlemmar registreras på central nivå. Om en person anmält sig lokalt registreras uppgifterna om

denne på lokal nivå. Det är endast lokalföreningarna som registrerar om en medlemsavgift är betald. Om ett medlemskap är felregistrerat kan de uppgifter som registrerats ändras lokalt men bara tas bort centralt. En medlem kan fortfarande vara medlem i något av de associerade förbunden.

Information till den registrerade
De registrerade informeras om personuppgiftsbehandlingen, dels genom de talonger som finns i partiets medlemsvärvarbroschyrer, dels genom information på webbplatsen.

Gallring av personuppgifter
En uppgift avseende en person som utträtt som medlem ur partiet och inte heller är medlem i något av de associerade förbunden gallras vid en årlig körning. Uppgifterna kan således komma att bevaras i upp till ett år. Detta gäller även personer som uteslutits eller inte har betalt medlemsavgiften. När partiet får information om att en person avlidit tas uppgifterna bort omgående.

Personer som inte längre vill ha kontinuerlig information tas helt bort från registret. Vid en kongress sparas uppgifter om utställare till dess att kongressen är över.

IT-säkerhet
Ett IT-system har utvecklats specifikt för Kristdemokraterna, som även har driftansvaret. Servern där medlemsregistret lagras är placerad i ett låst utrymme i partiets lokaler, som är försedd med larm. Ett extern företag har åtkomst till servern för underhåll av systemet.

Det finns inte någon övergripande IT-säkerhetspolicy. Internutbildning hålls för personalen varje vecka då frågor om IT-säkerhet kan tas upp. Nyanställda får en utbildning om IT.

Kristdemokraterna har inte genomfört någon extern granskning av informationssäkerheten eller några penetrationstester. Hot- och riskanalyser genomförs alltid vid införande av ett nytt IT-system.

Tre personer har åtkomst till och kan ändra och registrera uppgifter i hela medlemsregistret. Alla användare kan söka fram namnuppgift om en person i registret för att undvika dubbelregistrering vid registrering av ny medlem. Dessa har dock inte åtkomst till medlemsuppgifter om någon annan medlem än medlemmar i den förening de har behörighet till.

Tre personer på riksnivå kan dela ut behörigheter och lägga upp nya användarkonton. Ordföranden och kassören på lokalförenings- och distriktsnivå kan få behörighet att få tillgång till och registrera eller ändra uppgifter i medlemsregistret efter att föreningen eller distriktet anmält vilka dessa är till riksorganisationen. Dessa får skriva under en försäkran om att man är införstådd med vad som får registreras i registret och att man tagit del av kort sammanfattning av vad personuppgiftslagen innebär för ett föreningsregister. De får också en manual om hur man registrerar personuppgifter. Därefter ges personen behörighet att få åtkomst till registret. För att få åtkomst måste man vara ansluten till intranätet där man laddar ner en mjukvara genom vilken man autentiserar sig med användarnamn och lösenord. Användarnamn och lösenord får personen skickat till sig per post. Det finns regler för sammansättning av lösenord.

Varje natt sker ett uttag till en separat databas av uppgifter om personer som i medlemsregistret har registrerats med koder för vissa politiska uppdrag. Uppgifterna görs därefter tillgängliga på Kristdemokraternas webbplats. Uppgifter om personer med politiska uppdrag som inte vill ha sina uppgifter publicerade på webbplatsen tas bort.

En medlemsansökan kan lämnas via partiets webbplats. Överföringen av uppgifterna från den sökandes dator till partiets webbserver sker okrypterat.

Alla inloggningar i systemet loggas. Alla förändringar som görs i systemet loggas men i övrigt loggas inte vad som görs i systemet. Tidpunkt, datum och den MAC-adress som använts loggas. Det sker ingen logguppföljning, annat än om det uppstår frågetecken kring någon registrering.

Säkerhetskopior av medlemsregistret tas varje natt. Kristdemokraterna har kontrollerat att återläsning av kopiorna fungerar.

Skäl för beslutet

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

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

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

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

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

Frågan är om de lokala organisationerna, dvs. distrikt och lokalavdelningar har ett gemensamt personuppgiftsansvar med riksorganisationen.

I utredningen har framkommit att distrikt och lokalavdelningar kan få åtkomst till och använda det centrala medlemsregistret genom att använda den mjukvara som riksorganisationen erbjuder. Distrikt- och lokalföreningar sköter administrationen lokalt och kan registrera och ändra uppgifter om de medlemmar som tillhör respektive förenings ansvarsområde. Det är endast lokalföreningar som registrerar om en medlemsavgift är betald. Föreningarna har vid registrering av en ny medlem möjlighet att söka på samtliga medlemmars namn i registret för att undvika dubbelregistrering. I övrigt har dessa enbart tillgång till uppgifter om medlemmar i den förening man ansvarar för.

De uppgifter Datainspektionen har tagit del av talar för att de lokala organisationerna har ett sådant faktiskt inflytande över behandlingen av uppgifter avseende de medlemmar som tillhör respektive förenings ansvarsområde att personuppgiftsansvaret ska anses vara gemensamt. Det innebär att även de lokala föreningarna, dvs. distrikt och lokalavdelningar, har ett ansvar för att behandlingen av personuppgifter har stöd i personuppgiftslagen. För denna tillsyn som är riktad mot riksorganisationen 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 Kristdemokraternas 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 Kristdemokraterna behandlar personuppgifter om medlemmar och andra i det centrala medlemsregistret utöver vad som framkommer nedan under detta och 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 ideella organisationer med ett politiskt syfte inom ramen för sin verksamhet får 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. Detta gäller trots att medlemskapet formellt är knutet till en lokal förening. Skälet till detta är den tydliga koppling som finns hos politiska partier vad 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 Kristdemokraterna sparar uppgifter om personer som inte längre är medlemmar i upp till ett år. Det är fråga om medlemmar som utträtt, inte betalat medlemsavgiften i tid och som uteslutits. Kristdemokraterna har uppgett att de inte använder uppgifter om tidigare medlemmar för återvärvning eller historiska ändamål. Det är oklart för vilka ändamål partiet sparar uppgifter om tidigare medlemmar innan de avidentifieras.

Datainspektionen ifrågasätter den lagliga grunden för Kristdemokraterna att spara alla uppgifter om en tidigare medlem upp till ett år. En uppgift om att en person har varit medlem i ett politiskt parti är också en känslig personuppgift eftersom den kan anses avslöja en politisk åsikt. Om medlemskapet är avslutat kan partiet inte stödja sin behandling av uppgift om tidigare medlemskap på 17 § personuppgiftslagen. För att få spara uppgifter om tidigare medlemmar måste Kristdemokraterna finna ett stöd för behandlingen enligt 15-19 §§ personuppgiftslagen för att behandlingen ska vara tillåten. Partiet har inte visat att man inhämtat ett samtycke eller uppgett något annat stöd för att behandla uppgifter om tidigare medlemmar.

Datainspektionen konstaterar således att Kristdemokraternas behandling av uppgifter om tidigare medlemmar strider mot 13 § personuppgiftslagen.

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

Kristdemokraterna har uppgett att man använder medlemsuppgifter för statistikändamål. Datainspektionen har i detta ärende inte närmare utrett på vilket sätt som Kristdemokraterna använder personuppgifterna för ändamålet statistik. I sammanhanget vill dock Datainspektionen 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 § personuppgiftslagen och om samhällsintresset av det statistikprojekt där behandlingen inte klart väger över den risk för otillbörligt intrång i enskildas personliga integritet som behandlingen kan medföra. Bestämmelsen ger uttryck för en avvägningsnorm som innebär en helhetsbedömning av samtliga omständigheter. Statistik avseende medlemskap i politiskt parti kan enligt Datainspektionen anses ha ett sådant samhällsintresse som kan väga över intrånget i den enskildes personliga integritet. En bedömning måste göras i varje enskilt fall. Personuppgifterna för statistiska ändamål får dock inte sparas under en längre tid än vad som behövs för detta ändamål.

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

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

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

Sådan övrig information är t.ex. information om vilka kategorier av uppgifter som behandlas, kategorier av mottagare av uppgifterna, hur länge uppgifterna bevaras samt rätten att ansöka om information och få rättelse.

Datainspektionen har tagit del av information som lämnas via partiets webbplats samt information som lämnats i de talonger som finns i partiets medlemsvärvarbroschyrer.

Datainspektionen konstaterar att informationen saknar uppgift om den personuppgiftsansvariges identitet, vilka personuppgifter som behandlas, hur länge uppgifterna sparas, om ändamålen, t.ex. om statistikändamål samt om rätten att ansöka om registerutdrag och rätten till rättelse.

När det är fråga om ett gemensamt personuppgiftsansvar är det också viktigt att det av informationen framgår att föreningar på regional och lokal nivå har ett gemensamt personuppgiftsansvar tillsammans med riksorganisationen vad avser behandling av medlemmars personuppgifter.

Datainspektionen konstaterar således att Kristdemokraterna inte fullt ut lever upp till de krav som ställs i 23-25 §§ personuppgiftslagen.

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

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

a. de tekniska möjligheterna som finns,
b. vad det skulle kosta att genomföra åtgärderna,
c. de särskilda risker som finns med behandlingen av personuppgifterna, och
d. hur pass känsliga de behandlade personuppgifterna är.

Fråga är om skyddet för att förhindra obehörig åtkomst till personuppgifter i det centrala medlemsregistret är tillräckligt, dvs. främst 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.

Det går att få åtkomst till personuppgifter i det centrala medlemsregistret via öppet nät genom att autentisera sig som behörig användare med enbart användarnamn och lösenord. Enligt Datainspektionen krävs stark autentisering för åtkomst till uppgifterna i det centrala medlemsregistret för att de ska anses vara tillräckligt skyddade mot obehörig åtkomst.

I bedömningen 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 att Kristdemokraterna inte lever upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att behöriga användare har åtkomst över öppet nät till personuppgifter i medlemsregistret efter autentisering med enbartlösenord och användarnamn.

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

I ärendet har framkommit att Kristdemokraterna skickar medlemsuppgifter över öppet nät via en okrypterad excelfil, som skickas som en bilaga i ett e-post-meddelande till tryckeriet. Det har även framkommit att personuppgifter som fylls i vid en medlemsansökan via webbformuläret överförs okrypterat över Internet till webbservern.

När det gäller överföring av känsliga personuppgifter via öppet nät som till exempel Internet, är det Datainspektionens uppfattning att personuppgifterna ska vara krypterade på ett sådant sätt att endast den avsedda

mottagaren kan ta del av uppgifterna. Enligt Datainspektionens uppfattning utgör behandling av personuppgifter i e-postsystem en särskild risk i sig eftersom det kan vara svårt att se till att endast behöriga får del av uppgifterna. Det gäller vid både intern och extern kommunikation.

Datainspektionen konstaterar att Kristdemokraterna inte krypterar känsliga personuppgifter via öppet nät vid överföring av medlemsuppgifter till tryckeriet och vid överföring av personuppgifter från sökande som fyllt i webbformuläret om medlemskap.

Datainspektionen förelägger, enligt 45 § första stycket personuppgiftslagen, Kristdemokraterna att upphöra med att överföra medlemsuppgifter i okrypterad excelfil via öppet nät till ett tryckeri och att kryptera överföringen av personuppgifter till webbformuläret.

Nästa fråga är om Kristdemokrater 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 person-uppgifter. 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 de 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.

Kristdemokraterna har uppgett att alla inloggningar i systemet loggas och att alla förändringar som görs i systemet loggas. I övrigt loggas inte vad som görs i systemet. Tidpunkt, datum och den dators MAC-adress som använts registreras.

Datainspektionen konstaterar att den behandlingshistorik som förs i dag inte uppfyller de krav på att partiet ska kunna utreda vem som har haft åtkomst till personuppgifter och när.

Datainspektionen förutsätter att Kristdemokrater ser över behandlings-historiken och inför sådana tekniska funktioner som gör det möjligt att utreda

vem som har haft åtkomst till vilka personuppgifter i medlemsregistret och när. Det ska också gå att utreda vem som ändrat eller raderat personuppgifter och när förändringen skett.

Det framkommit att Kristdemokraterna inte har någon informationssäkerhetspolicy eller genomfört någon övergripande extern säkerhetsgranskning eller några penetrationstester av det egenutvecklade IT- systemet.

Datainspektionen anser att en viktig del i ett strukturerat informationssäkerhetsarbete är att ha en informationssäkerhetspolicy och 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 konstaterat 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 minskning av risken för obehörig åtkomst till personuppgifterna i medlemssystemet.

Datainspektionen rekommenderar därför att Kristdemokraterna upprättar en informationssäkerhetspolicy och 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 Jonas Agnvall och Gunilla Öberg, föredragande.

Göran Gräslund

Gunilla Öberg