SUOMEN EV.LUT. KIRKKO
EV.LUTH. KYRKAN I FINLAND
Kirkkohallitus
Kyrkostyrelsen

# Kyrkostyrelsens cirkulär nr 6/2017

27.2.2017

## FÖRBEREDELSER FÖR INFÖRANDET AV EUROPEISKA UNIONENS ALLMÄNNA DATASKYDDSFÖRORDNING

Europeiska unionens allmänna dataskyddsförordning (EU 2016/679), som reglerar behandlingen av personuppgifter, ska tillämpas från och med 25.5.2018. Förordningen ska tillämpas inom både offentliga och privata sektorn. Den ersätter personuppgiftsdirektivet från 1995 och bestämmelserna i personuppgiftslagen (523/1999) som utfärdats för det nationella verkställandet av personuppgiftsdirektivet till de delar behandlingen av personuppgifter omfattas av förordningens tillämpningsområde.

Trots att det är fråga om en förordning som tillämpas direkt på nationell nivå, ger den medlemsstaterna ett visst spelrum. Det är möjligt att inom ramarna för förordningen utfärda nationell lagstiftning som preciserar bestämmelserna i förordningen eller eventuellt också i viss mån avviker från förpliktelserna i förordningen. Justitieministeriet inrättade i februari 2016 en arbetsgrupp för att utreda behovet av nationella lagstiftningsåtgärder till följd av EU:s dataskyddsförordning. Ett möjligt förslag till en ändring av lagstiftningen om personuppgifter uppskattas bli klart under senvåren 2017.

Förordningen kommer att medföra nya administrativa uppgifter för den personuppgiftsansvarige, och det finns skäl att förbereda sig på dessa uppgifter i god tid. I detta cirkulär redogörs det för de centrala punkterna i förordningen. Hela förordningen kan läsas elektroniskt på adressen: http://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=SV

### *Dataskyddsförordningens tillämpningsområde och centrala definitioner*

Dataskyddsförordningen tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. Behandling av personuppgifter som en fysisk person utför som ett led i verksamhet av rent privat natur omfattas inte av förordningens tillämpningsområde.

Centrala definitioner:

| | |
|---|---|
| **Personuppgift** | Varje upplysning som avser en identifierad eller identifierbar fysisk person (t.ex. ett namn, ett identifikationsnummer, en lokaliseringsuppgift, online identifikatorer eller faktorer som är specifika för personens ekonomiska eller kulturella identitet). |
| **Särskilda kategorier av personuppgifter (känsliga personuppgifter)** | Uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska uppgifter, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Behandlingen av särskilda kategorier av personuppgifter regleras separat. |
| **Behandling av personuppgifter** | En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller |

| | |
|---|---|
| | ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.<br><br>Det är inte tillåtet att behandla personuppgifter om barn under 16 år utan samtycke av en förälder/vårdnadshavare. En medlemsstat får föreskriva en lägre ålder, under förutsättning att denna lägre ålder inte är under 13 år. |
| **Personuppgiftsbiträde** | En fysisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. |
| **Register** | En strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden. |
| **Personuppgiftsansvarig** | En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Om ändamålen och medlen för behandlingen bestäms av lagstiftningen kan även den personuppgiftsansvarige föreskrivas i lagstiftningen. |
| **Registrerad** | Den person vars personuppgifter behandlas. |
| **Samtycke av den registrerade** | Varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.<br><br>Om behandlingen av uppgifter grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter. |
| **Tredje part, utomstående** | En fysisk eller juridisk person, offentlig myndighet, institution eller organ som inte är den registrerade, den personuppgiftsansvarige, personuppgiftsbiträdet eller de personer som under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar är behöriga att behandla personuppgifterna. |
| **Registerbeskrivning, dataskyddsbeskrivning** | Ett dokument som varje personuppgiftsansvarig ska upprätta och hålla tillgängligt. Dokumentet ska beskriva behandlingen av personuppgifter på ett kortfattat, öppet och lättbegripligt sätt. |
| **Dataskydd och datasäkerhet** | Dataskydd innebär integritetsskydd vid behandling av personuppgifter. Datasäkerhet innebär att säkerställa uppgifternas konfidentialitet, integritet och tillgänglighet med hjälp av tekniska och organisatoriska åtgärder och förfaranden. |
| **Dataskyddsombud** | En myndighet eller ett offentligt organ, som är verksamt som personuppgiftsansvarig eller personuppgiftsbiträde, ska utse ett dataskyddsombud, vars ställning och befattningsbeskrivning bestäms av dataskyddsförordningen. Ett dataskyddsombud kan utses för flera myndigheter eller offentliga organ. |
| **Inbyggt dataskydd och dataskydd som standard** | Integrering av dataskyddsprinciperna i behandlingen av personuppgifter. Beaktande av principerna i fastställandet av behandlingsförfaranden och i samband med själva behandlingen för att säkerställa att behandlingen överensstämmer med kraven i dataskyddsförordningen. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att:<br>• i standardfallet säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas<br>• säkerställa att inga stora mängder personuppgifter samlas eller lagras samt att lagringen inte pågår längre än vad som är nödvändigt för det aktuella ändamålet |

| | |
|---|---|
| | • säkerställa att personuppgifter i standardfallet inte görs tillgängliga för ett obegränsat antal fysiska personer<br>• garantera att de registrerades rättigheter förverkligas.<br><br>Uppfyllandet av kraven i dataskyddsförordningen ska garanteras från definitionsfasen ända till slutet av de behandlade personuppgifternas livscykel. |
| **Ansvarsskyldighet** | Ansvarsskyldigheten förpliktar en organisation att visa att följande principer för behandling av personuppgifter har följts:<br>• laglighet, korrekthet och öppenhet<br>• ändamålsbegränsning<br>• uppgiftsminimering<br>• korrekthet<br>• lagringsminimering<br>• integritet och konfidentialitet. |

***Den registrerades rättigheter***

Den personuppgiftsansvarige är skyldig att ombesörja den registrerades rättigheter. De registrerades rättigheter enligt dataskyddsförordningen motsvarar delvis rättigheterna i den nuvarande personuppgiftslagen, men förordningen ger också de registrerade nya rättigheter. Den personuppgiftsansvarige är skyldig att kontrollera den registrerades identitet, när den registrerade utövar sin rätt att få tillgång till sina uppgifter, sin rätt att korrigera eller radera uppgifter som gäller honom eller henne eller överföra sina uppgifter från ett system till ett annat. En registrerads begäran som gäller dessa rättigheter ska besvaras senast en månad efter att begäran tagits emot. Vid behov kan den personuppgiftsansvarige förlänga tiden med ytterligare två månader, om den registrerades begäran är komplicerad eller det har kommit många begäran. Uppgifterna levereras i regel i elektronisk form och kostnadsfritt.

Det ingår i ***den personuppgiftsansvariges informationsskyldighet*** att informera öppet om behandlingen av personuppgifter innan behandlingsverksamheten inleds. Dessutom ska en beskrivning av behandlingen av personuppgifter hållas offentligt tillgänglig och behovet att uppdatera beskrivningen ska kontrolleras regelbundet. Innan personuppgifter samlas in ska den personuppgiftsansvarige på ett lättbegripligt sätt informera den registrerade om följande (registerbeskrivning/dataskyddsbeskrivning):

- kontaktuppgifter för den personuppgiftsansvarige och dataskyddsombudet
- ändamålen med behandlingen av personuppgifterna och den rättsliga grunden för behandlingen
- om uppgifter utlämnas till tredje parter, mottagarna av personuppgifterna
- om personuppgifter överförs till ett tredjeland, hur dataskyddets tillräcklighet har säkerställts och var den registrerade kan få mer information om detta
- den period under vilken personuppgifterna kommer att lagras eller de kriterier som används för att fastställa denna period
- den registrerades rättigheter och hur registrerade kan utöva sina rättigheter
- den registrerades rätt att inge klagomål till en tillsynsmyndighet
- grunden för kravet på tillhandahållande av personuppgifter, huruvida den registrerade måste tillhandahålla uppgifterna och vilka konsekvenser underlåtelse att tillhandahålla uppgifter medför
- huruvida behandlingen inkluderar automatiskt beslutfattande eller profilering, och om så är fallet, den bakomliggande logiken för behandlingen samt betydelsen och följderna för den registrerade.

Om uppgifter samlas in från andra källor än den registrerade själv, ska förutom det ovan nämnda även redogöras för vilka uppgifter som samlas in, varifrån personuppgifterna kommer och huruvida uppgifterna har erhållits från allmänt tillgängliga källor.

I likhet med den rätt till insyn som föreskrivs i personuppgiftslagen ska den registrerade enligt förordningen ha ***rätt att få tillgång till sina egna personuppgifter***. Den personuppgiftsansvarige ska på begäran av den registrerade bekräfta huruvida personuppgifter som rör den registrerade håller på att behandlas och tillhandahålla en kopia av de personuppgifter som behandlas. Samtidigt ska den registrerade underrättas om de kategorier av personuppgifter som behandlingen gäller samt få en beskrivning av behandlingen av personuppgifter som innehåller de ovan nämnda punkterna (registerbeskrivning/dataskyddsbeskrivning).

I likhet med den nuvarande regleringen har den registrerade ***rätt att korrigera uppgifterna***. Den registrerade har rätt att kräva att den personuppgiftsansvarige rättar felaktiga personuppgifter som gäller den registrerade eller kompletterar bristfälliga personuppgifter.

***Rätten att bli bortglömd*** som föreskrivs i förordningen innebär att den registrerade har rätt att begära att den personuppgiftsansvarige raderar föråldrade personuppgifter som gäller den registrerade. Den registrerade har också rätt att återkalla det samtycke på vilket behandlingen grundar sig. Det ska vara lika lätt att återkalla sitt samtycke som att ge sitt samtycke. I samband med återkallandet kan den registrerade begära att uppgifter som gäller honom eller henne raderas ur systemen. Den personuppgiftsansvarige ska då radera uppgifterna om det inte finns någon annan laglig grund för behandlingen av uppgifterna. Raderingen av uppgifterna kan genomföras tekniskt till exempel så att uppgifterna i fråga inte längre uppdateras och åtkomsten till uppgifterna begränsas genom att de krypteras eller överskrivs. Rätten att bli bortglömd tillämpas inte på lagstadgade register såsom kyrkans gemensamma medlemsdatasystem.

En ny rätt är den registrerades ***rätt till dataportabilitet***. Utövandet av denna rätt förutsätter att behandlingen av personuppgifterna grundar sig på samtycke eller avtal samt att behandlingen är automatiserad. Vid en offentlig myndighet tillämpas rätten till dataportabilitet på de register som har lagrats för att sköta myndighetens frivilliga, icke-lagstadgade uppgifter. Rätten till dataportabilitet tillämpas inte på behandling som är nödvändig för att utföra en uppgift med anknytning till allmänt intresse eller vid utövande av offentlig makt.

Den registrerade har ***rätt att göra invändningar mot behandling av personuppgifter, automatiskt beslutsfattande och profilering***. Den registrerade ska, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på artikel 6.1 e eller f, inbegripet profilering som grundar sig på dessa bestämmelser. Den personuppgiftsansvarige får då inte längre behandla personuppgifterna såvida denne inte kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk. Om den registrerade invänder mot behandling för direkt marknadsföring ska personuppgifterna inte längre behandlas för sådana ändamål. Denna rätt gäller dock inte personregister som upprätthålls av en offentlig myndighet med stöd av lagen.

Dessutom har den registrerade rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, t.ex. profilering, och medför rättsverkan för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne. Denna rätt tillämpas inte om det med stöd av förordningen finns en motiverad orsak till beslutet.

En ny rätt som föreskrivs i förordningen är den registrerades ***rätt att få en anmälan om personuppgiftsincidenter***. Den personuppgiftsansvarige är skyldig att anmäla personuppgiftsincidenter personligen till de registrerade vars uppgifter berörs av incidenten. En anmälan ska göras om incidenten sannolikt medför en stor risk för individens rättigheter och friheter, till exempel i form av identitetsstölder, betalningsbedrägerier eller annan kriminell verksamhet. Anmälan som ges den registrerade ska åtminstone innehålla en tydlig och enkel beskrivning av händelsen, kontaktuppgifter till dataskyddsombudet och information om möjligheten att få mer information, en redogörelse för vilka konsekvenser personuppgiftsincidenten kan ha för den registrerade samt en beskrivning av de åtgärder den personuppgiftsansvarige kommer att vidta eller redan har vidtagit för att lindra de negativa konsekvenserna och lösa situationen.

***Den personuppgiftsansvariges skyldigheter***

Utöver verkställandet av de registrerades rättigheter innehåller dataskyddsförordningen också bestämmelser om den personuppgiftsansvariges skyldigheter. Efter att dataskyddsförordningen har trätt i kraft är det inte längre tillräckligt att uppfylla de krav som fastställs i förordningen, utan den personuppgiftsansvarige ska kunna visa hur de tekniska, administrativa och organisatoriska åtgärder som behövs för att uppfylla dataskyddsskyldigheterna säkerställs i verksamheten (***ansvarsskyldighet***).

***Behandlingen av personuppgifter är laglig*** endast under de förutsättningar som fastställs i förordningen. Den personuppgiftsansvarige ansvarar för att personuppgifter inte behandlas utan vederbörlig rättslig grund. Enligt förordningen är förutsättningarna för laglig behandling bland annat:

- ett frivilligt, specifikt, informerat och entydigt samtycke av den registrerade, som den personuppgiftsansvarige kan visa
- genomförande av ett avtal där den registrerade är en av parterna
- den personuppgiftsansvariges lagstadgade skyldighet – förordningen tillåter nationellt spelrum
- skydd av den registrerades och en annan fysisk persons vitala intressen
- myndighetsutövning som utförs av den personuppgiftsansvarige – förordningen tillåter nationellt spelrum.

I likhet med den nuvarande personuppgiftslagen ger även förordningen vissa personuppgifter en särställning som i huvudsak förbjuder behandling, om det inte finns en i förordningen angiven grund. Till dessa hör bland annat uppgifter om en persons religiösa övertygelse. Behandling är emellertid möjlig om den registrerade uttryckligen har lämnat sitt samtycke till det. Behandling är tillåten även om den sker inom ramen för ett icke vinstdrivande organs lagliga verksamhet och med iakttagande av lämpliga skyddsåtgärder. Vidare förutsätts att behandlingen enbart rör organets medlemmar eller tidigare medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och personuppgifterna inte lämnas ut utanför organet utan den registrerades samtycke.

Behandlingen av personuppgifter under sakliga förutsättningar ska även beaktas i planeringen av nya behandlingssätt eller personregister. Behandlingen av personuppgifter ska också vara ändamålsbegränsad, dvs. den personuppgiftsansvarige ska i förväg definiera de ändamål för vilka personuppgifterna ska behandlas och säkerställa att personuppgifterna inte behandlas för andra ändamål.

De ***skyldigheter avseende dataskydd*** som fastställs i förordningen gäller alla personuppgifter som behandlas av en församling, en kyrklig samfällighet, ett stift eller en annan kyrklig myndighet, oavsett om det gäller uppgifter om församlingens medlemmar, klienter (t.ex. diakoniarbetet), samarbetspartner eller personal eller förtroendevalda inom den egna organisationen.

När uppgifter behandlas av en myndighet eller ett annat offentligt organ, ska organet enligt förordningen utse ett ***dataskyddsombud***. Samma dataskyddsombud kan utses till gemensamt dataskyddsombud för flera församlingar eller kyrkliga samfälligheter eller andra kyrkliga myndigheter. Dataskyddsombudet ska ha en oberoende ställning i organisationen och är skyldig att rapportera till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta ledning. Dataskyddsombudet ska på vederbörligt sätt och i tillräckligt god tid göras delaktig i alla frågor som gäller dataskydd. Dataskyddsombudet ska besitta tillräcklig kunskap om dataskyddslagstiftningen, tillämpningen av kraven i lagen samt praxis inom branschen. Den personuppgiftsansvarige eller personuppgiftsbiträdet kan vara dataskyddsombudets arbetsgivare, men verksamheten kan också utlokaliseras till en tjänsteleverantör. Dataskyddsombudet ska garanteras de resurser som är nödvändiga för att sköta uppgifterna samt vederbörlig åtkomst till personuppgifter och funktioner för behandling av personuppgifter. Dataskyddsombudet är en offentlig kontaktperson för både tillsynsmyndigheten och de registrerade. Dataskyddsombudet är skyldigt att följa sekretessbestämmelserna i sin uppgift och kan inte avskedas eller bestraffas på grund av uppgifter som har skötts på ett tillbörligt sätt i egenskap av dataskyddsombud. Dataskyddsombudet kan också ges andra uppgifter i organisationen, men de får inte stå i konflikt med dataskyddsombudets uppgifter eller oberoende ställning.

Dataskyddsombudet har till uppgift att ge såväl den personuppgiftsansvarige som tjänsteinnehavare och anställda som behandlar personuppgifter information och råd om skyldigheterna enligt dataskyddsförordningen och övrig dataskyddslagstiftning. Dataskyddsombudet ska följa upp att myndigheten iakttar dataskyddsförordningen och övrig dataskyddslagstiftning samt följer förfaranden med anknytning till den personuppgiftsansvariges skydd av personuppgifter, t.ex. ansvarsfördelning, personalens utbildning och kontrollåtgärder. Dataskyddsombudet ska på begäran ge råd om konsekvensbedömningar med anknytning till dataskydd och övervaka genomförandet. Dataskyddsombudet samarbetar inte bara med tillsynsmyndigheten, utan fungerar också som stödperson för registrerade. Registrerade kan kontakta dataskyddsombudet i alla ärenden som har att göra med behandling av deras personuppgifter och utövandet av rättigheter med stöd av dataskyddsförordningen.

Utgångspunkten för dataskyddsförordningen är att identifiera och hantera risker. Den personuppgiftsansvarige och personuppgiftsbiträdet är skyldiga att bedöma riskerna i anslutning till behandlingen av personuppgifter samt välja nödvändiga hanteringsåtgärder enligt den uppskattade risknivån. I förordningen föreskrivs det att en konsekvensbedömning avseende dataskydd är en obligatorisk åtgärd i fråga om sådana åtgärder för behandling av personuppgifter där det i planeringsfasen är sannolikt att behandlingsåtgärderna medför betydande risker med tanke på individernas rättigheter och friheter. Resultaten av konsekvensbedömningen används för att definiera de hanteringsmetoder som ska tillämpas för att sänka risknivån och samtidigt säkerställa att kraven i förordningen uppfylls. Om risknivån är hög och den personuppgiftsansvarige inte förmår sänka den, ska tillsynsmyndigheten kontaktas (*förhandssamråd*). Konsekvensbedömningen omfattar ett system, ett program, en tjänst eller ett projekt som är i planeringsfasen och kommer att inkludera behandling av personuppgifter. Konsekvensbedömningen görs med stöd av de krav som fastställs i dataskyddsförordningen och övrig dataskyddslagstiftning. Alla personuppgiftsansvariga rekommenderas att göra en konsekvensbedömning.

Genom begreppen ***inbyggt dataskydd och dataskydd som standard*** förpliktar förordningen den personuppgiftsansvarige att i ett tidigt skede integrera dataskyddsprinciper och dataskyddskrav i behandlingen av personuppgifter. Uppfyllandet av kraven i dataskyddsförordningen ska garanteras i definitionsfasen och under hela livscykeln för de personuppgifter som behandlas. Med livscykel avses tidsperioden från det att personuppgifterna samlas in tills de förstörs eller raderas: 1) samtycke eller annan laglig grund, 2) insamling av uppgifter, 3) behandling, 4) möjlig överlåtelse av uppgifter, 5) arkivering och 6) förstöring eller annan radering. I praktiken innebär detta att dataskyddet integreras i såväl system- och programutvecklingen som anskaffningarna och projektadministrationen.

Enligt förordningen är den personuppgiftsansvarige alltså ***skyldig att ombesörja datasäkerheten*** under personuppgifternas hela livscykel, vilket innebär att den personuppgiftsansvarige ska vidta vederbörliga tekniska och organisatoriska åtgärder för att trygga behandlingen av personuppgifter. Personuppgifterna ska vid överföring, lagring och behandling skyddas från obehörig eller oavsiktlig förstöring, ändring, överlåtelse eller åtkomst. Genomförandet av datasäkerheten beror på organisationens storlek och övriga verksamhet och ska anpassas enligt verksamheten och de uppgifter som ska skyddas.

En ny skyldighet som ikraftträdandet av förordningen medför för den personuppgiftsansvarige är ***anmälningsskyldighet*** i fråga om personuppgiftsincidenter. Anmälningsskyldigheten omfattar både registrerade och tillsynsmyndigheten. Anmälan om en datasäkerhetsincident som gäller personuppgifter ska göras till tillsynsmyndigheten inom 72 timmar efter att incidenten har upptäckts. Anmälan ska åtminstone innehålla en beskrivning av händelsen, redogöra för de grupper av registrerade och antalet registrerade som incidenten gäller, innehålla kontaktuppgifter till dataskyddsombudet och information om möjligheten att få mer information, redogöra för vilka konsekvenser personuppgiftsincidenten kan ha för den registrerade samt beskriva de åtgärder den personuppgiftsansvarige kommer att vidta eller redan har vidtagit för att lindra de negativa konsekvenserna och lösa situationen. För att det ska vara möjligt att fullgöra anmälningsskyldigheten ska den personuppgiftsansvarige ha metoder att upptäcka avvikelser i behandlingen av personuppgifter samt möjlighet att utreda orsakerna till och följderna av en upptäckt avvikelse och avvikelsens inverkan på integritetsskyddet. Samtidigt ska det vara möjligt att förhindra att avvikelsen sprider sig och vid behov säkerställa att utomstående hjälp är tillgänglig samt analysera om det finns behov av en anmälan enligt förordningen. När situationen har korrigerats ska man identifiera nödvändiga förändringar

och utvecklingsåtgärder samt se till att händelsen dokumenteras och bevisen sparas. Vid behov ska en undersökningsbegäran om datasäkerhetsavvikelsen göras till polisen och avvikelsen ska eventuellt också anmälas till Cybersäkerhetscentret, som lyder under Kommunikationsverket.

Den personuppgiftsansvarige eller det utsedda dataskyddsombudet är ***skyldiga att samarbeta med tillsynsmyndigheten*** på tillsynsmyndighetens begäran eller i samband med förhandssamråd med tillsynsmyndigheten. En nyhet i dataskyddsförordningen är att tillsynsmyndigheten får rätt att påföra sanktionsavgifter eller administrativa påföljder för den personuppgiftsansvarige och/eller personuppgiftsbiträdet om skyldigheterna i dataskyddsförordningen försummas. Tillsynsmyndigheten har också rätt att granska den personuppgiftsansvariges genomförande av dataskyddet. Metoderna som används för den offentliga förvaltningen preciseras i takt med att lagstiftningsarbetet framskrider.

***Åtgärdsrekommendationer***

Församlingar, kyrkliga samfälligheter, domkapitel och andra kyrkliga myndigheter som fungerar som personuppgiftsansvariga bör inleda förberedelser inför ikraftträdandet av förordningen.

En av de viktigaste förstahandsåtgärderna är att få organisationens ledning att delta i och stödja dataskyddsarbetet. Både tjänstemännens och de förtroendevaldas ledning ansvarar för att reservera tillräckliga resurser för en bedömning av nuläget samt för att befullmäktiga och möjliggöra genomförandet av de utvecklingsåtgärder som har identifierats med stöd av bedömningen. Ledningens medvetenhet om tillståndet för organisationens dataskydd är även i fortsättningen en del av fullgörandet av den personuppgiftsansvariges ansvarsskyldighet. Det bör ingå i det utsedda dataskyddsombudets ansvarsområde att regelbundet rapportera exempelvis till kyrkorådet eller det gemensamma kyrkorådet eller att åtminstone sammanställa en årsrapport.

I första hand ska man också bedöma nuläget i fråga om behandlingen av personuppgifter och genomförandet av dataskyddet samt i förhållande till kraven i dataskyddsförordningen (***analys av nuläget***). Bedömningen ska i synnerhet omfatta verkställandet av de registrerades rättigheter och genomförandet av en riskfokuserad verksamhet. Med stöd av bedömningen kan man identifiera brister och utvecklingsobjekt samt planera åtgärder som bör vidtas för att utveckla nuläget.

En viktig del av analysen av nuläget är att sammanställa en helhetsbild av de personuppgifter som organisationen har samlat in och behandlat; vilka personregister organisationen har och var samt på uppdrag av vem personuppgifterna behandlas. Även datasäkerhetskraven för avtal ska utvärderas med tanke på skyddet av personuppgifter och vid behov ska avtalen kompletteras så att de överensstämmer med kraven i dataskyddsförordningen. Ett hjälpmedel i inventeringen av personuppgifter och avtal är modellering av personuppgifternas dataflöde, dvs. att beskriva de behandlade personuppgiftstyperna, personuppgifternas källor, programmen och systemen för behandling av personuppgifter, behandlarnas roller och hur personuppgifterna överförs mellan de ovan nämnda, behandlingens fysiska placering och huruvida personuppgifter överlåts eller överförs vidare till tredje parter samt hur länge personuppgifter behandlas och hur de kommer att förstöras.

När datasystem och avtal granskas bör registerbeskrivningarna uppdateras så att de motsvarar innehållet i den informationsskyldighet som föreskrivs för den personuppgiftsansvarige i förordningen. Samtidigt ska man kontrollera vad som har avtalats om överlåtelse av personuppgifter i synnerhet utanför EES-området och huruvida detta har beaktats även i ett eventuellt avtal med tjänsteleverantören. Dessutom ska man se till att det finns uppdaterade och vederbörliga beskrivningar av behandlingen av personuppgifter i dataskyddsbeskrivningen och de kommunikationskanaler som används, t.ex. internetsidor. Det finns också skäl att kontrollera om eventuella personuppgiftsincidenter har beaktats i organisationens beredskaps- och kriskommunikationsplan på det sätt som förutsätts i förordningen.

När användningsändamålen för personuppgifterna, programmen och systemen för behandling av personuppgifter samt situationerna i samband med överföring av personuppgifter har klarlagts, rekommenderas en ***riskanalys***, så

att man kan identifiera och dimensionera nödvändiga hanteringsåtgärder samt vid behov skapa en riskhanteringsmodell.

Det är bra om dataskyddsombudet utses i god tid. Dataskyddsombudet ska ha tillräcklig kompetens och behörighet för att sköta sin uppgift. Vid behov ska utbildning ordnas för den person som utses. För att garantera dataskyddsombudets oberoende finns det skäl att i samband med utnämnandet noggrant överväga var personen befinner sig i organisationen. Uppgiften kan också utlokaliseras eller så kan församlingarna eller de kyrkliga samfälligheterna och domkapitlen utse ett gemensamt dataskyddsombud. Om ägandet och behandlingen av personuppgifter har splittrats mellan flera uppgiftsområden eller enheter inom en församling eller kyrklig samfällighet, är det ändamålsenligt att dessutom grunda en intern dataskyddsorganisation, till vilken representanter från uppgiftsområdena eller enheterna i fråga utses.

Den kyrkliga myndigheten ska se till att tjänsteinnehavare och anställda som hanterar personuppgifter eller deltar i processer skapade för att garantera de registrerades rättigheter är tillräckligt kunniga inom dataskydd och datasäkerhet. Man bör också i förväg fundera över de förfarandeprocesser som tillämpas för att trygga de registrerades rättigheter, till exempel den personuppgiftsansvariges informationsskyldighet, begäran om samtycke för insamling av uppgifter samt rätten att få åtkomst till sina uppgifter.

Dataskyddsförordningen ska också beaktas i pågående systemprojekt och programutvecklingar samt i nya systemprojekt från och med konkurrensutsättningen av projekten. Enligt förordningen är en organisation skyldig att ordna behandlingen av personuppgifter på ett sådant sätt att förordningen, dataskyddsprinciperna och de registrerades rättigheter beaktas effektivt i all behandling av uppgifter.

***Mer information***

Mer information om verkställandet av Europeiska Unionens allmänna dataskyddsförordning finns bland annat på dataombudsmannens webbsidor www.tietosuoja.fi/sv, samt på webbsidorna för ledningsgruppen för datasäkerheten inom statsförvaltningen (VAHTI) www.vm.fi/vahti. Detta cirkulär baserar sig delvis på VAHTI-rapporten 1/2016 om totalreformen av EU:s dataskydd, som har publicerats på VAHTI:s webbsidor.

På justitieministeriets webbsidor finns mer information om det pågående lagstiftningsprojektet http://oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/henkilotietojensuojakansallisenlainsaadannontarkistaminen_0.html.

Mer information om innehållet i detta cirkulär fås av ecklesiastikråd Pirjo Pihlaja och datasäkerhetschef Jussi Mukari fornamn.efternamn@evl.fi Kyrkostyrelsen följer verkställandet av dataskyddsförordningen samt strävar efter att informera om sådant som gäller verkställandet av förordningen och precisera anvisningarna med anknytning till förordningen under de kommande 18 månaderna.

KYRKOSTYRELSEN

Jukka Keskitalo

Pirjo Pihlaja

ISSN 1797-0334

Suomen evankelis-luterilainen kirkko
Evangelisk-lutherska kyrkan i Finland
Kirkkohallitus / Kyrkostyrelsen

Eteläranta 8 / Södra Kajen 8
PL / PB 210
00131 Helsinki / Helsingfors

vaihde / växel 09 180 21 / faksi / fax 09 180 2350
kirkkohallitus@evl.fi / kyrkostyrelsen@evl.fi
evl.fi

Y-tunnus / FO-nummer 0118950-3
IBAN: FI47 8000 1000 0676 87
BIC: DABAFIHH