Svenska kyrkan

Information om den nya dataskyddsförordningen

Generell information

När börjar dataskyddsförordningen gälla?

Dataskyddsförordningen gäller som svensk lag från och med den 25 maj 2018 och ersätter den nu gällande personuppgiftslagen, som bygger på dataskyddsdirektivet 95/46/EG. Förordningen kommer att kompletteras med ytterligare svensk lagstiftning på vissa områden.

Vad innebär dataskyddsförordningen för Svenska kyrkan?

Svenska kyrkan kommer att behöva förändra sin hantering av personuppgifter med anledning av att den nya förordningen träder i kraft. Kortsiktigt så innebär det att de personuppgiftsbehandlingar som görs ska inventeras, i syfte att utreda vilka specifika åtgärder som behöver vidtas. Projektgruppen på nationell nivå kommer under våren att ta fram åtgärdsrekommendationer för hur problematiska personuppgiftsbehandlingar skulle kunna korrigeras. Projektgruppen kommer utöver detta att erbjuda mallar för personuppgiftsbiträdesavtal och rekommendationer för att uppfylla informationsplikten gentemot registrerade. På längre sikt måste vissa arbetsrutiner ses över och personal kommer att behöva vidareutbildas i hur de ska handskas med personuppgifter i sitt dagliga arbete.

OBS: Detta informationsblad innehåller endast information som är relevant för inventeringen. Det finns många andra begrepp i förordningen som vi behöver känna till, men för inventeringen behöver vi ha en gemensam tolkning av just de begrepp som nämns i detta dokument. Information om dataskyddsförordningen i övrigt finns på Datainspektionens hemsida https://www.datainspektionen.se men kommer också att finnas på projektets intranät: internwww.svenskakyrkan.se/dataskydd.

Definitioner

Personuppgift

En personuppgift är varje upplysning som avser en identifierad eller identifierbar nu levande fysisk person. Det kan vara t.ex. namn, personnummer, tjänstetitel, foto, uppgift om hälsa eller uppgift om religiös eller politisk övertygelse. Så länge det går att koppla en uppgift till en viss person är det en personuppgift. Ibland är en enda upplysning tillräcklig för att identifiera personen, t.ex. ett personnummer och ibland krävs en kombination av upplysningar. Om flera olika upplysningar handlar om samma person, exempelvis för- och efternamn + yrkestitel, så utgör upplysningarna personuppgifter.

Svenska kyrkan

Personuppgiftsbehandling

Alla åtgärder som görs med personuppgifter är personuppgiftsbehandlingar. Begreppet behandling innefattar att samla in, registrera, sprida, gallra, radera, och lämna ut uppgifter. Även en passiv handling som att ”ha kvar” uppgifter i register (lagring) är en behandling av personuppgifter. Andra exempel på behandlingar är: organisering, strukturering, bearbetning, ändring, framtagning, läsning, användning, överföring, tillhandahållande, justering, sammanföring, begränsning och förstöring.

Gallring

Gallring innebär att förstöra handlingar eller uppgifter i handlingar efter fastställda regler eller vidta andra åtgärder med handlingarna som medför förlust av
– betydelsebärande data,
– möjliga sammanställningar,
– sökmöjligheter, eller
– möjligheter att bedöma handlingarnas äkthet.

Huvudregeln är att Svenska kyrkans handlingar och uppgifterna i dem ska bevaras. Detta regleras i arkivlagen (1990:782), lagen (1998:1591) om Svenska kyrkan samt kyrkoordningen.

Personuppgifter får enligt dataskyddsförordningen inte behandlas under en längre tid än vad som är nödvändigt utifrån det ändamål som uppgifterna samlades in för. Om ändamålet inte uppfylls, finns det två alternativ:

1. Personuppgifterna ska bevaras med hänsyn till arkivändamål av allmänt intresse, vetenskapliga forskningsändamål, historiska forskningsändamål eller statistiska ändamål. Se även ovan under "Ändamål med personuppgifter". Dessa undantag framgår av Dataskyddsförordningens artikel 17 punkt 3, och i artikel 89 kommenteras undantagen ytterligare. Om personuppgifterna ingår i den kategorin ska de bevaras, men tillgängligheten bör begränsas.

2. Personuppgifterna kan inte bevaras med stöd av artikel 17 punkt 3, d v s de är inte av långsiktigt intresse utöver det ursprungliga ändamålet. Men gallring av handlingar och personuppgifter är tillåten endast med stöd av generella gallringsbeslut. Riksarkivet beslutar om gallring avseende allmänna handlingar, medan kyrkostyrelsen beslutar om gallring avseende Svenska kyrkans egna handlingar. Om gallringsbeslut saknas ska man ansöka till Kyrkostyrelsen om att gallra personuppgifter.

För att genomföra gallring behövs tekniska funktioner och rutinbeskrivningar. Gallring kan vara såväl radering som anonymisering (om sätten att anonymisera är helt säkra – det ska vara omöjligt, inte bara svårt, att koppla uppgifterna till en fysisk person).

En registrerad

Begreppet ”registrerad” kommer av att lagstiftningen på området tidigare endast gällde register. I detta sammanhang är en registrerad en person vars personuppgifter förekommer i ett system.

Personuppgiftsansvarig

En personuppgiftsansvarig bestämmer varför och hur personuppgifter behandlas. Det är oftast inte en fysisk person, utan en juridisk person som till exempel en myndighet, ett företag eller som i Svenska kyrkans fall: till exempel kyrkostyrelsen på den nationella nivån, stiftsstyrelsen på stiftsnivå och kyrkorådet/församlingsrådet på lokal nivå. Det beror på vilket organ som fattar beslut om personuppgiftsbehandlingen. Vem som är personuppgiftsansvarig avgörs inte av vad som står i ett avtal utan hur det ser ut i verkligheten. Den som *faktiskt* bestämmer över personuppgiftsbehandlingens ändamål (varför) och medel (hur) är personuppgiftsansvarig för behandlingen. Personuppgiftsansvaret kan aldrig delegeras till någon annan, även om andra juridiska personer utför behandling å den personuppgiftsansvariges vägnar.

Personuppgiftsbiträde

Den som behandlar personuppgifter för den personuppgiftsansvariges räkning kallas personuppgiftsbiträde. Ett personuppgiftsbiträde kan i sin tur anlita ett eget personuppgiftsbiträde (”underbiträde”) för att utföra uppgifterna, om den personuppgiftsansvariga har godkänt det genom ett skriftligt tillstånd. Det kan vara ett generellt tillstånd eller gälla specifikt för just den underleverantören. Även biträde och underbiträde måste teckna ett avtal sinsemellan, där det framgår att underbiträdet har samma skyldighet mot den personuppgiftsansvariga som biträdet har. Oavsett hur många led av personuppgiftsbiträden som finns i en sådan kedja är det alltid den personuppgiftsansvariga som är ytterst ansvarig för att reglerna följs.

Personuppgiftsincident

I förordningen definieras begreppet "personuppgiftsincident" som en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som behandlas. Det kan också vara fråga om en incident som leder till obehörigt röjande av eller obehörig åtkomst till personuppgifterna.

Principer för personuppgiftsbehandling i GDPR

Det finns ett antal principer som alltid gäller för behandling av personuppgifter. Principerna framgår av artikel 5 i dataskyddsförordningen och den personuppgiftsansvariga måste alltid ha dessa i åtanke.

Laglighet och öppenhet

Personuppgifter ska behandlas på ett lagligt sätt och med en öppenhet för de registrerade. Kravet på laglighet innebär att all personuppgiftsbehandling måste ha stöd i dataskyddsförordningen, eftersom personuppgifter bara får behandlas om det finns en laglig grund. Mer om dessa grunder finns att läsa i inventeringsvägledningen under avsnittet ”Laglig grund för behandling”.

Öppenhetsprincipen kräver att all information och kommunikation i samband med en personuppgiftsbehandling ska finnas lättillgänglig och vara lättbegriplig för den registrerade. Framförallt är det viktigt att den registrerade vet varför och hur personuppgifterna behandlas och vem som är ansvarig för behandlingen.

Svenska kyrkan

Förordningen kommer att innebära en omfattade informationsplikt för personuppgiftsansvariga. Under våren 2018 kommer projektgruppen på nationell nivå att publicera rekommendationer och mallar för informationsgivande.

Ändamålsbegränsning

Det måste finnas ett särskilt ändamål med varför personuppgifter behandlas. Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Det innebär att det måste finnas ett tydligt syfte med varför uppgifterna samlas in och en laglig grund för behandlingen. Det går alltså inte att till exempel samla in uppgifter för ett obestämt framtida behov.

Uppgiftsminimering

Det är inte tillåtet att samla in fler personuppgifter än vad som är nödvändigt för ändamålet. En förutsättning för att kunna uppfylla kravet på uppgiftsminimering är att ett tydligt ändamål har fastställts *innan* insamlingen av personuppgifter, eftersom ändamålet utgör ramen för behandlingen.

Korrekthet

Personuppgifter som behandlas ska vara korrekta och helst uppdaterade. Felaktiga eller utdaterade uppgifter ska raderas eller rättas så snart som möjligt.

Lagringsminimering

Personuppgifter får inte sparas längre än vad som är nödvändigt utifrån ändamålet för behandlingen. När Svenska kyrkan inte längre har ett behov av uppgifterna ska de raderas eller avidentifieras så att de inte längre kan kopplas till den registrerade. Därför behövs bestämda tidsfrister eller kriterier för uppgifternas livstid och rutiner för radering eller avidentifiering.

Det går dock att lagra uppgifter en längre tid om ändamålet är arkivering för allmänt intresse, statistiska ändamål eller vetenskapliga eller historiska forskningsändamål, om det finns skyddsåtgärder för att tillgodose de registrerades rättigheter enligt förordningen.

OBS. Personuppgifter i Svenska kyrkan ska som huvudregel enligt lag bevaras. Gallringsbeslut behövs innan gallring får ske. Se informationsbladet om gallring.

Integritet och konfidentialitet

Personuppgifter ska behandlas på ett sätt som säkerställer en lämplig säkerhet för uppgifterna. Det innebär att det måste finnas en viss nivå av skydd mot att uppgifterna utsätts för till exempel otillåten eller obehörig behandling, eller att de felaktigt raderas eller skadas.

Svenska kyrkan

Dataskydd

Förutom att personuppgiftsbehandlingen i sig ska vara laglig ställer förordningen även krav på att IT-system ska ha tillräckligt hög säkerhet för personuppgifter. För att Svenska kyrkan ska uppfylla förordningens krav krävs därför att IT-systemens säkerhet ses över. Svenska kyrkan på nationell nivå kommer i och med inventeringen av de gemensamma systemen även utreda det generella behovet av säkerhetsåtgärder. I och med det kommer riktlinjer och rekommendationer att göras tillgängliga för såväl nationell nivå som för stift och församlingar.

Både den personuppgiftsansvarige och personuppgiftsbiträdet är skyldiga att vidta tekniska och organisatoriska åtgärder som är lämpliga i förhållande till risken med behandlingarna. När bedömningen av vilka åtgärder som är lämpliga görs ska hänsyn tas till den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter. Exempel på åtgärder är pseudonymisering och kryptering av personuppgifter. Det skulle också kunna handla om mer övergripande åtgärder, så som att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos systemen eller att se till så att tillgången till personuppgifterna återställs snabbt efter in incident. Det är viktigt att regelbundet testa, undersöka och utvärdera effektiviteten av de åtgärder som implementeras.

Vid bedömningen av vad som är en lämplig säkerhetsnivå är det viktigt att ta hänsyn till de risker behandlingen medför, i synnerhet risker kopplade till oavsiktlig och olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som behandlas.

Inbyggt dataskydd och dataskydd som standard (Privacy by Design och Privacy by Default)

Integritetsfrågorna i förordningen ska påverka hela systemets utformning. Den personuppgiftsansvariga måste se till att de system som används inte medför integritetsrisker och ställa tillräckliga krav på leverantörerna av systemen. Leverantören är normalt sett inte ansvarig för eventuella integritetsproblem, utan denna kravställning syftar till att den ansvariga ska se till att anlita en leverantör med tillräckligt bra integritetsskydd i förhållande till de uppgifter som behandlas. Det spelar ingen roll om det är en hårdvara, mjukvara eller tjänst som levereras (outsourcing, moln eller ”software as a service” – mjukvara som vi använder genom en molntjänst). Det är alltid den beställande personuppgiftsansvariga som ska se till att leverantören uppfyller kraven på säkerhet. Sådan säkerhet skulle kunna bestå av:

– uppgiftsminimering
– behörighetsbegränsning
– autentisering
– kryptering
– loggning (i inventeringsmallen benämns detta som behandlingshistorik)
– säkerhetskopiering

– säker utplåning
– rutiner och tydlig information om personuppgiftssäkerhet till systemets användare