Svenska kyrkan

Vägledning för inventering

För att kunna uppfylla kraven i dataskyddsförordningen är det viktigt att reda ut vilka personuppgifter som finns i IT-systemen ni använder er av och hur personuppgifterna behandlas. För att få full kännedom om alla personuppgiftsbehandlingar behövs en inventering av systemet eller systemen ni använder.

Det här dokumentet fungerar som en vägledning till inventeringen. Själva inventeringen gör ni i Exceldokumentet ”Inventeringsmall”. Området är komplext och det är därför viktigt att ni förstår hur dataskyddsförordningen fungerar innan inventeringen påbörjas. Börja därför med att läsa Informationsbladet om dataskyddsförordningen för att få en förståelse för dataskyddsförordningens allmänna regler och principer.

Besvara sedan frågorna i mallen med hjälp av inventeringsfilmen och den här vägledningen. Många av frågorna har korta beskrivningar direkt i mallen, men vi rekommenderar att ni också följer den här vägledningen.

Försök att inventera så mycket som möjligt enligt inventeringsmallen, det är bättre att försöka besvara en fråga än att inte svara alls. Kom ihåg att svaret ”vi hittar inga rutiner för gallring” också är ett svar.

Inventeringen görs inte för att ”sätta dit” någon, utan för att hitta eventuella brister som behöver åtgärdas för att Svenska kyrkan ska uppfylla kraven i dataskyddsförordningen. Inventeringsmaterialet kommer senare följas upp med rekommendationer på åtgärder att vidta för att komma tillrätta med de brister som inventeringen visat på.

Vilka ska vara med och inventera?

Vi rekommenderar att det sätts ihop en grupp på två eller fler personer som tillsammans har kunskaper om både personuppgifterna i systemet och systemets funktioner, t.ex. hur uppgifterna har hamnat i systemet, för vilka ändamål de behandlas samt hur systemet fungerar tekniskt.

Syftet med inventeringsmallen

Inventeringsmallen fungerar som ett hjälpmedel och meningen är att ni genom att svara på frågorna i mallen ska få en bättre översikt av vilka personuppgifter era system innehåller och hur de hanteras. För stift, församlingar och pastorat innebär denna inventering i första hand en kartläggning av de lokala system som förvaltas av respektive enhet. Nationell nivå använder mallen för att inventera både gemensamma system (så som Kyrksam) och system som bara finns på nationell nivå. Om ni inventerar flera system fyller ni i Excelmallen för respektive system. Om ni t.ex. inventerar 10 olika system förväntar vi oss att 10 Excel-dokument fylls i.

Svenska kyrkan

Inventeringsmaterialet innehåller också en inventeringsmall för era eventuella leverantörer (biträden/underbiträden). Vi rekommenderar att ni skickar ”leverantörsmallen” till era leverantörer och ber att de återkommer till er med sina svar. Detta för att ni ska få kunskap om hur era leverantörer behandlar personuppgifter å era vägnar. Ni kan och bör dock fylla i inventeringsmallen själva innan ni fått svar från era leverantörer. Dataskyddsprojektet kommer framöver att tillhandahålla information och rekommendationer rörande vilka krav som kan och bör ställas på leverantörer gällande deras personuppgiftshantering.

Leverantörsmallen skiljer sig från den vanliga inventeringsmallen på så vis att den t.ex. saknar frågor om ändamål med personuppgiftsbehandling. Det beror på att det inte är leverantören, utan den personuppgiftsansvarige, som bestämmer över sådana saker. Leverantören kan däremot t.ex. svara på hur de säkerställer uppgifternas säkerhet i systemet.

Inventeringsmallens disposition

Inventeringsmallen består av ett antal frågor, indelade i olika ämnesavsnitt. Längst till vänster i mallen syns ämnestiteln för varje avsnitt, t.ex. ”Personkategorier och personuppgifter” eller ”Lagring av personuppgifter”. De flesta av frågorna kompletteras med en kortare beskrivning av vad som efterfrågas eller en förklaring av centrala begrepp i frågan och eventuell hänvisning till övrigt inventeringsmaterial. Ni fyller i era svar i det vita svarsfältet (det finns inga begränsningar på hur mycket text ni kan skriva i rutan).

I kolumnen till höger om era svar hittar ni en exempelinventering av det gemensamma administrativa systemet Kyrksam. Den är till för att ge exempel på de svar som eftersöks i frågorna. Observera att exempelinventeringen **inte** är en fullständig inventering. För att åstadkomma en fullständig inventering behöver ni svara uttömmande på frågorna.

De första 13 frågorna handlar om vilka sorts personuppgifter som finns i systemet, varför de behandlas, vilken laglig grund som finns för behandlingen, hur de hämtats in och vilka de lämnas ut till.

Resterande frågor handlar om hur systemet fungerar, t.ex. hur länge personuppgifter lagras, hur behörighetsstyrningen fungerar, om det finns fritextfält, om det finns funktioner för loggning, vilka möjligheter det finns för radering och justering av uppgifter etc.

Fråga 1-13 besvaras med fördel i turordning, medan övriga frågor kan besvaras i valfri följd.

Svenska kyrkan

Vägledning till frågorna

Personkategorier och personuppgifter

Fråga 1-3 syftar till att kartlägga vilka personuppgifter som finns i systemet och varför de finns där. Definitionen av personuppgifter finns i informationsbladet.

För att underlätta kartläggningen av personuppgifter i ett IT-system är det bra att först gruppera personer som förekommer i systemet i olika ”personkategorier”. Grupperingen görs utifrån vilken egenskap personer förekommer i systemet. Till exempel:

1. Personkategori: *medlem*
   Utgörs av: personer som är medlemmar i Svenska kyrkan.
2. Personkategori: *kursdeltagare*
   Personer som anmält sig till en kurs på den kyrkliga enheten.
3. Personkategori: *affärskontakt*
   Personer som är kontaktpersoner hos företag som den kyrkliga enheten har avtalat med.

Fråga 1 – Vilka personkategorier kan ni identifiera i systemet? Lista alla personkategorier.

Identifiera och lista de personkategorier som finns i systemet utifrån beskrivningen ovan.

Fråga 2 – Varför finns personkategorierna med i systemet?

Fundera över och beskriv övergripande anledningen till att personkategorierna finns med i systemet. För vissa personkategorier kan svaret tyckas vara självklart, för andra kanske det är mindre tydligt.

Fråga 3 – Vilka typer av personuppgifter behandlar ni för varje personkategori? Beskriv uttömmande.

Utifrån de personkategorier ni identifierat ska ni utreda och beskriva vilka typer av personuppgifter som finns om varje kategori.

Till exempel:

Personkategori: medlem
Personuppgifter: *namn, personnummer, information om inträde i Svenska kyrkan, dop, konfirmation, vigsel etc.*

Svenska kyrkan

Känsliga uppgifter

Vissa personuppgifter anses extra känsliga och har därför ett starkare skydd i dataskyddsförordningen. Följande uppgifter är enligt dataskyddsförordningen känsliga:

Personuppgifter som berör medlemskap i fackförening, hälsa, etniskt ursprung, religiös eller filosofisk övertygelse, politiska åsikter, sexualliv eller sexuell läggning samt uppgifter om lagöverträdelser. Huvudregeln är att det är förbjudet att behandla känsliga uppgifter men det finns undantag från förbudet, till exempel om en person uttryckligen samtyckt till behandlingen. Uttryckligt samtycke är ett högre ställt krav än bara samtycke. Från huvudregeln i artikel 9.1 finns en rad undantag, som regleras i artikel 9.2 (som går att läsa här: https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/#9).Se avsnittet laglig grund för behandling för flera av dessa undantag, där ”laglig grund” är synonymt med ”undantag”. Om samtycke inhämtats så används grunden samtycke och personuppgiftsbehandlingen är därmed undantagen från förbudet.

Vissa av undantagen innehåller hänvisningar till nationell rätt som kan innebära att lagstiftningsåtgärder måste vidtas på varje medlemsstats nivå för att undantagen ska vara tillämpliga. Ett sådant undantag är religiösa samfunds behandling för kärnverksamheten, vilket senast i december har föreslagits gälla precis som tidigare enligt PuL.

Personnummer och samordningsnummer får enligt PuL endast behandlas om det är motiverat med hänsyn till ändamålet med behandlingen, vikten av säker identifiering eller något annat beaktansvärt skäl. Dataskyddsutredningen har föreslagit att denna bestämmelse ska gälla även för dataskyddsförordningen och bestämmelsen kommer i så fall att regleras i den svenska kompletterande lagstiftningen.

Fråga 4 – Behandlar ni känsliga uppgifter i systemet?

Se över de personuppgifter ni identifierat för varje personkategori – finns det känsliga personuppgifter? Skriv upp alla *typer* av känsliga personuppgifter ni hittat.

Fråga 5 – Om ni har svarat ja på fråga 4: vilka typer av känsliga uppgifter behandlar ni för respektive personkategori?

Efter att ha listat alla typer av känsliga personuppgifter i fråga 4, dela upp dem i grupper utifrån vilka personkategorier de är kopplade till.

Inhämtning

Det är viktigt att reda ut hur personuppgifterna har hamnat i systemet eftersom den personuppgiftsansvarige måste kunna informera den registrerade om varifrån

personuppgifterna kommer. Observera att frågorna 6 och 7 alltså inte bara syftar till känsliga personuppgifter, utan alla typer av personuppgifter. Personuppgifterna som finns i systemet kommer troligtvis från olika källor, så ni behöver utreda det här för respektive personkategori.

Fråga 6 – Har ni hämtat personuppgifterna direkt från den registrerade? Utred detta för varje personkategori.

Att hämta direkt från den registrerade kan t.ex. innebära att ni har fått uppgifterna muntligen från den registrerade och fört in uppgifterna i systemet, att den registrerade fyllt i ett formulär på er hemsida eller fyllt i uppgifter skriftligen på annat sätt. Hur uppgifterna kommit er tillhanda spelar ingen roll, utan det är faktumet att de kommit direkt från den registrerade (och inte en databas, hitta.se eller andra källor) och därefter förts in i systemet som är avgörande.

Fråga 7 – Ifall personuppgifterna inte har hämtats direkt från den registrerade, varifrån kommer de? Kommer uppgifterna från allmänt tillgängliga källor som är öppna för alla?

Med allmänt tillgängliga källor menas källor som är öppna för allmänheten. T.ex. sidor på internet som alla har tillträde till. Kyrksam är t.ex. inte en allmänt tillgänglig källa även om många inom kyrkan kan komma åt uppgifter i systemet, eftersom den inte är öppen till allmänheten. Utred och beskriv varifrån uppgifterna kommer, t.ex. vilka allmänt tillgängliga källor de kommer ifrån, eller var annars de hämtats ifrån. Utred det här för varje personkategori.

Ändamål med personuppgifter

Insamling av personuppgifter

Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Kravet på att ett ändamål ska vara berättigat innebär att det måste finnas en laglig grund för behandlingen. För att kunna bedöma om det finns en laglig grund måste ändamålet vara tydligt angivet. Ändamålet måste vara tydligt och legitimt. Det ska bestämmas och dokumenteras innan behandlingen sker och den registrerade måste sedan informeras om ändamålet.

Enligt Datainspektionen måste personuppgifter som behandlas vara relevanta i förhållande till ändamålet med behandlingen och fler uppgifter än nödvändigt, med hänsyn till ändamålen, ska inte behandlas. För att en sådan bedömning ska kunna göras krävs en viss grad av precision. Datainspektionen ansåg i ett tillsynsärende att det inte var tillåtet att samla in personuppgifter för ”framtida forskning”, eftersom ändamålet var för vagt. Deltagarna i

studien kunde inte veta vad ändamålet skulle innebära i framtiden och därmed inte förstå vad de samtyckte till.

Vidarebehandling av insamlade personuppgifter

Personuppgifter som samlats in för ett ändamål får inte vidarebehandlas på ett sätt som är oförenligt med det ursprungliga ändamålet, om inte den registrerade (1) har gett sitt samtyckte till det, (2) den nya behandlingen grundar sig på lag, exempelvis skyldighet att redovisa anställdas personuppgifter till Försäkringskassan, eller (3) den nya behandlingen är en nödvändig åtgärd i ett demokratiskt samhälle i syfte att säkerställa exempelvis den nationella säkerheten eller försvaret. Varje vidarebehandling av en personuppgift måste alltså rymmas inom ramen för det ursprungliga ändamålet som personuppgiften samlades in för, under hela tiden uppgiften finns hos Svenska kyrkan. När det inte längre finns ett ändamål med att lagra uppgiften ska den raderas (gallras) ur systemet.

För att avgöra om en vidarebehandling är förenlig med det ursprungliga ändamålet ska en sammanvägande bedömning av följande faktorer göras:

- Kopplingen mellan det gamla och det nya ändamålet
- I vilket sammanhang personuppgifterna samlades in och då särskilt förhållandet mellan Svenska kyrkan och den registrerade
- Personuppgifternas art och då särskilt ifall personuppgifterna är känsliga
- Eventuella konsekvenser för den registrerade av den fortsatta behandlingen
- Om det finns lämpliga skyddsåtgärder, exempelvis kryptering och pseudonymisering

Det finns ett undantag till denna regel. Behandlingar för vissa ändamål anses alltid vara förenliga med det ursprungliga ändamålet, nämligen:

1. Behandling för arkivändamål av allmänt intresse
2. Behandling för vetenskapliga forskningsändamål
3. Historiska forskningsändamål
4. Statistiska ändamål

Bedömningen kan vara svår att göra och det rekommenderas därför att du tar kontakt med en jurist om du är osäker på huruvida en ny behandling är förenlig med ändamålet för den ursprungliga behandlingen.

Fråga 8 – För vilket/vilka ändamål behandlas personuppgifterna för respektive personkategori?

Beskriv ändamålen med personuppgifterna ni behandlar för var och en av personkategorierna.

Fråga 9 – Finns det personuppgifter ni identifierat som möjligen onödiga eller som ni inte ser något ändamål med? Ange även eventuella personuppgifter som tidigare varit nödvändiga utifrån det ursprungliga ändamålet men som inte längre är det.

Finns det bland de personuppgifter som ni inte kan hitta något ändamål med eller som ni på annat sätt anser vara onödiga?

Laglig grund för behandling

Varje behandling av personuppgifter kräver laglig grund. En behandling är endast tillåten om något av de sex villkoren i artikel 6 i dataskyddsförordningens är uppfyllt. För varje villkor finns begränsningar och ni måste därför fundera noga innan ni avgör vad den lagliga grunden är för varje behandling. För behandling av känsliga personuppgifter är villkoren snävare och svårare att tolka. Ett av villkoren är uttryckligt samtycke, som är ett högre ställt krav än samtycke (som du kan läsa mer om nedan).

För att vissa av villkoren ska vara uppfyllda krävs att en behandling är nödvändig. Vilka typer av behandlingar som kan anses som nödvändiga är inte helt uppenbart. I vissa fall kan en behandling få utföras, även om uppgiften skulle kunna utföras utan en behandling av personuppgifter, om behandlingen i fråga skulle leda till effektivitetsvinster. EU-domstolen har tidigare ansett att ett centralt register över uppgifter som redan fanns i regionala register bidrog till att effektivisera tillämpningen av i fallet relevanta bestämmelser och att behandlingen i det centrala registret därför var nödvändig.

Det finns sex olika lagliga grunder för personuppgiftsbehandling – rättslig förpliktelse, avtal med den registrerade, skydd för grundläggande intressen, uppgift av allmänt intresse och samtycke.

Rättslig förpliktelse

Personuppgifter får behandlas om det är nödvändigt för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige, alltså en skyldighet som följer av lag. Ett exempel på det är bokföringsskyldigheten som följer av bokföringslagen.

I Dataskyddsutredningen (SOU 2017:39) har det föreslagits att begreppet ”rättslig förpliktelse” även ska innefatta förelägganden, myndighetsbeslut och domar som meddelats med stöd av gällande rätt.

I Dataskyddsutredningen föreslogs även att förpliktelser, uppgifter av allmänt intresse och myndighetsutövning som inte framgår av svensk lag eller EU-lag inte ska kunna användas som en grund för behandling av personuppgifter. Om detta blir verklighet kommer Svenska kyrkan inte att kunna stödja en behandling på en ”förpliktelse” som framgår av kyrkoordningen eller en bestämmelse från kyrkostyrelsen.

Beroende på hur lagstiftningen ser ut kan denna lagliga grund även gälla för behandling av *känsliga* personuppgifter.

Avtal med den registrerade

Det är tillåtet att behandla personuppgifter om det är nödvändigt för att fullgöra ett avtal där personen är part eller för att vidta åtgärder på begäran av personen innan ett sådant avtal ingås.

Två exempel på behandlingar som är nödvändiga i samband med avtal är behandling av personuppgifter i kund- och personaladministrativa system för fakturering och löneberäkning.

Skydd för grundläggande intressen

Det är tillåtet att behandla personuppgifter för att skydda grundläggande intressen. För att denna grund för behandling ska få användas måste det handla om ett intresse som är av avgörande betydelse för den registrerades eller någon annan persons liv. Det skulle kunna röra sig om en personuppgiftsbehandling som är nödvändig för livsavgörande vård i akuta situationer då den registrerade inte kan lämna sitt samtycke.

Denna lagliga grund gäller även för behandling av *känsliga* personuppgifter.

Uppgift av allmänt intresse

Personuppgifter får behandlas om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

För att behandlingen ska vara tillåten enligt denna grund måste den uppgift som den personuppgiftsansvariga utför:

1. Vara en del av allmänt intresse **eller** utgöra ett led i myndighetsutövning
2. Vara fastställd i enlighet med unionsrätten eller den nationella rätten
3. Vara nödvändig (proportionerlig) för ett ändamål som är nödvändigt för att utföra uppgiften

Vad som avses med allmänt intresse är inte helt uppenbart. Av dataskyddsförordningen följer att allmänintresse omfattar bland annat hälso- och sjukvårdsfrågor och socialt skydd. I datalagskommitténs betänkande nämns att uppgifter av allmänt intresse kan vara t.ex. arkivering, forskning och framtagande av statistik, etablerade idrottsorganisationers registrering av vilka personer som har vunnit svenskt mästerskap eller registrering av personer som har fått allmänt erkända utmärkelser så som Nobelpriset. Enligt Dataskyddsutredningen är det rimligt att anta att uppgifter som statliga myndigheter utför på uppdrag av riksdag eller regering är uppgifter av allmänt intresse.

Uppgifter som *enbart* framgår av kyrkoordningen kommer alltså sannolikt inte att utgöra en rättslig grund för behandling.

Det är viktigt att ha i åtanke att den registrerade kan invända mot en personuppgiftsbehandling som sker för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning kan den registrerade invända mot behandlingen. Den personuppgiftsansvariga måste då göra en bedömning om huruvida det ändå föreligger tvingande och berättigade skäl för behandling som väger tyngre än den registrerades intressen.

Denna lagliga grund gäller även för behandling av *känsliga* personuppgifter.

Intresseavvägning

Det kan vara tillåtet att behandla personuppgifter efter en intresseavvägning, om behandlingen är nödvändig för personuppgiftsansvariges eller tredje parts berättigade intressen, och de väger tyngre än personens intressen eller grundläggande rättigheter och friheter. Med tredje part menas en person som varken är personuppgiftsansvarig eller personuppgiftsbiträde.

Svenska kyrkan kan få behandla personuppgifter efter att en intresseavvägning har gjorts. Det innebär att det görs en intresseavvägning mellan vad den personuppgiftsansvariga får ut av behandlingen och risken för personens integritet. Enligt dataskyddsförordningen är direktmarknadsföring ett sådant berättigat intresse, om nyttan väger tyngre än risken. Ju känsligare (och mer omfattande) uppgifter det handlar om desto svårare blir det att hävda att intresset att behandla väger tyngre! En annan viktig sak att komma ihåg är att barns intressen

och rättigheter väger extra tungt eftersom de inte har samma möjlighet att skydda sin integritet som vuxna.

När denna grund används måste man vara beredd på att den registrerade kan invända mot en pågående behandling och den som behandlar måste då göra en ny intresseavvägning och upphöra med behandlingen om det inte finns tvingande berättigade skäl. Om den registrerade invänder mot direkt marknadsföring ska behandlingen för sådana ändamål upphöra direkt. Detta framgår av artikel 21.

Samtycke

Samtycke är en rättslig grund som ska användas i sista hand! Detta anser vi för att det är svårt att använda samtycke som laglig grund på ett korrekt sätt. Samtycke innebär att personen går med på att hans eller hennes personuppgifter behandlas för ett visst ändamål. Ett giltigt samtycke ska vara ett frivilligt, specifikt, informerat och otvetydigt medgivande från den registrerade om att den godkänner behandlingen av personuppgifterna.

Den registrerade måste alltså informeras om ändamålen för behandlingen – **innan** samtycket inhämtas genom en skriftlig, muntlig eller elektronisk förklaring. Svenska kyrkan bör alltid inhämta samtycke genom skriftlig förklaring, eftersom den personuppgiftsansvariga kan bli tvungen att i efterhand visa att den registrerade samtyckt. Begäran om samtycke måste vara lättbegriplig och det ska gå att tydligt särskilja samtycket från resten av frågorna, annars är det inte bindande. Rutor som är ikryssade på förhand, tystnad eller annan passivitet räknas inte som ett samtycke.

Samtycke bör inte användas av Svenska kyrkan som grund för att hantera anställdas personuppgifter när det finns en risk att den anställda känner sig tvingad att samtycka, eftersom samtycket då inte är frivilligt längre.

Något som är viktigt att komma ihåg är att den registrerade har rätt att när som helst återkalla sitt samtycke. Det måste vara lika lätt att återkalla som att ge samtycke. Därför bör det noga övervägas ifall samtycke är en lämplig grund att behandla personuppgifter på. Om det finns en misstanke om att den registrerade kan komma att dra tillbaka sitt samtycke och det är viktigt för verksamheten att behandlingen görs, bör en annan grund för behandling väljas om det finns en tillämplig sådan. Det anses inte lämpligt att använda en annan grund **efter** att den registrerade valt att inte samtycka eller återkallat ett tidigare samtycke.

Samtycke är däremot lämpligt att använda om man avser att samla in och behandla känsliga personuppgifter. *Uttryckligt* samtycke är ett av undantagen till huvudregeln om att det är förbjudet att behandla känsliga personuppgifter. Det kan också användas ifall man vill göra en överföring av personuppgifter till ett land utanför EU/EES.

Fråga 10 – Ange vilken laglig grund varje behandling av personuppgifter uppfyller. För vissa personkategorier kan det vara samma grund för alla behandlingar, så utgå gärna från personkategorierna.

Utgå från förklaringen av de olika grunderna ovan för att avgöra grunden för varje personuppgiftsbehandling ni identifierat. Eftersom personkategorierna ofta omfattar samma sorts personuppgifter och behandlingar kan ni med fördel göra bedömningen med utgångspunkt i kategorierna.

Fråga 11 – Finns det behandlingar som ni inte tycker passar någon av grunderna? Beskriv vilka behandlingar det gäller och vilka personkategorier de knyter an till.

Det är lika viktigt att dokumentera vilka personbehandlingar ni *inte* hittat laglig grund för. Det kan betyda att behandlingarna är otillåtna och att ni därför behöver åtgärda detta. Information och rekommendationer för sådana åtgärder ingår i de riktlinjer som dataskyddsprojektet kommer att tillhandahålla framöver.

Utlämning

Registrerade har rätt att få veta var deras personuppgifter behandlas. Därför behöver man utreda ifall personuppgifterna lämnas ut till någon annan, utanför den egna kyrkliga enheten. Ett sådant utlämnande sker exempelvis när personuppgifter lämnas ut till en annan juridisk person inom Svenska kyrkan (t.ex. från en pastoral enhet till nationell nivå eller mellan två pastorala enheter) eller om uppgifterna lämnats ut till en leverantör som behandlar de å era vägnar.

Fråga 12 – Vilka lämnar ni ut personuppgifter till, och varför? Ange även om personuppgifterna är känsliga eller inte.

Lista vilka ni lämnar ut personuppgifter till. Ni behöver inte beskriva utifrån personkategorier, men det kan vara enklast att utgå från dem.

Fråga 13 – Vilka planerar ni att lämna ut personuppgifter till, och varför?

Kommer personuppgifter att lämnas ut till andra mottagare i framtiden? Beskriv vilka det är i så fall och varför personuppgifterna lämnas ut.

Fritextfält

Fråga 14 – Finns det några fritextfält i systemet?

Ett fritextfält är ett fält där användaren av systemet kan skriva självständigt. Det skulle exempelvis kunna handla om att användaren gör noteringar om en anställds allergier eller om när ett visst avtal ska förnyas.

Det är viktigt att utreda huruvida det finns fritextfält eller ej, eftersom den som fyller i fältet kan lägga in onödiga personuppgifter på eget bevåg.

Fråga 15 – Om ni har svarat ja på fråga 14: Vad är syftet med respektive fritextfält?

Fritextfält bör undvikas om det inte finns ett verkligt behov av att använda det och därför måste det utredas om det finns ett legitimt syfte med befintliga fritextfält.

Behörighet

Dataskyddsförordningen ställer krav på att endast de som behöver åtkomst till personuppgifter ska vara behöriga att ha det. Med behörighet menas här tillgång och rätt att använda system. Tillgången kan regleras genom lösenord eller annan behörighetsstyrning, medan rätten snarare regleras genom vad som ingår i den anställdes arbetsuppgifter.

Behörighet till samma uppgifter kan vara indelas i olika nivåer där t.ex. en systemadministratör har obegränsad behörighet medan en lokal enhetsadministratör endast har behörighet att behandla uppgifter som är relevanta för dennes enhet.

Fråga 16 – Hur avgörs behörighetstilldelningen för systemet?

Förklara vilka faktorer som avgör en användares tillgång till systemet. Vissa användare kanske har tillgång till fler funktioner, exempelvis genom att de kan göra olika typer av rapporter, medan andra användare har tillgång till fler personuppgifter eftersom detta krävs för att de ska kunna utföra sina arbetsuppgifter.

Fråga 17 – Finns det idag ett behov av att styra behörigheterna ytterligare?

De personuppgifter som finns i systemet får endast behandlas av personer som måste behandla personuppgifterna i sitt dagliga arbete. En anställd ska exempelvis inte ha tillgång

till alla personuppgifter i ett system om den endast behöver veta vad telefonnumret till alla medlemmar i ett stift är. Om så är fallet bör behörigheten styras ytterligare.

Loggning

Med loggning menas en funktion för att registrera vilka aktiviteter som användare utför i ett system. Loggning avser i detta sammanhang behandling av användarnas personuppgifter kopplat till viss användning, så som en specifik persons besök av en viss webbplats.

Loggning i detta avseende är en behandling av personuppgifter som sker i det dolda, och de som loggas ska därför informeras om att loggning sker.

En annan sorts logg är för registrering av behandlingar, till exempel av att en viss personuppgift sparades av en viss person en viss dag. **Detta avsnitt avser inte sådan loggning.** En sådan logg kallas även för behandlingshistorik. De sista frågorna i inventeringsmallen handlar om sådan historik.

Fråga 18 – Används loggning för att kontrollera vilka åtgärder användare vidtar i systemet vid användning av Svenska kyrkans utrustning (dator, telefon etc.)?

Se ovan.

Fråga 19 – Om ni har svarat ja på fråga 18: Vad/vilka åtgärder är det som loggas?

Exempelvis användning av kopiator, e-post och telefon. Om e-posts innehåll eller metadata (så som avsändare, mottagare, filstorlek) loggas är detta särskilt integritetskänsligt och bör uppmärksammas.

Fråga 20 – Vad är syftet med loggningen?

Det måste finnas ett förutbestämt ändamål för loggningen, exempelvis att arbetsgivaren vill kartlägga den anställdas internetanvändning på arbetstid.

För mer information om ändamål, se fråga 8.

Fråga 21 – Hur informeras anställda om att deras IT-användning loggas?

Anställda måste vara medvetna om vilka interna regelverk som finns för loggning, hur IT-användningen kontrolleras och vad ändamålet med loggningen är. Eftersom loggningen utgör personuppgiftsbehandling (om det inte är anonyma uppgifter) har anställda rätt att veta att deras användning loggas samt vilka uppgifter som loggas.

Fråga 22 – Hur länge behöver ni logguppgifterna för respektive ändamål? Hur länge sparas de?

Personuppgifter får inte behandlas under en längre tid än vad som är nödvändigt och ska därför gallras när det inte längre finns något ändamål med behandlingen.

Fråga 23 – Är det möjligt för anställda, konsulter eller någon annan att få åtkomst till systemet via privata datorer/telefoner/annan IT-utrustning?

Arbetsgivaren är personuppgiftsansvarig och ansvarar därför för behandlingen av personuppgifter som vidtas av arbetstagaren. När den anställde använder sin privata utrustning för att arbeta i systemet kan arbetsgivarens möjligheter att kontrollera behandlingen av personuppgifter minska.

Fråga 24 – Om ni har svarat ja på fråga 23: beskriv riktlinjer som reglerar hur den anställda får använda systemet via privat utrustning.

Se ovan.

Fråga 25 – Om ni har svarat ja på fråga 23: används loggning när den anställda, konsulten eller någon annan utför i systemet via privata datorer/telefoner/annan IT-utrustning?

Se ovan.

Lagring av personuppgifter

Lagring får endast göras under en begränsad tid, så länge som lagringen är nödvändig för de ändamål för vilka personuppgifterna behandlas, enligt dataskyddsförordningens artikel 5.e.

När det inte längre finns ett behov av uppgifterna ska de raderas, eller avidentifieras så att de inte längre kan kopplas till den registrerade. Det behövs därför bestämda tidsfrister eller kriterier för uppgifternas livstid och rutiner för radering eller avidentifiering.

Det går att lagra uppgifterna 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 dataskyddsförordningen.

Det är viktigt att notera att gallring exempelvis i form av radering eller anonymisering, förutsätter ett gallringsbeslut från kyrkostyrelsen eller Riksarkivet, se informationsbladet om gallring.

Fråga 26 – Hur och var lagras de personuppgifter som ni behandlar i systemet?

Vilka lagras på server, var finns servrarna och vem hanterar dem (internt eller externt)? Vad lagras i ”molnet”?

Fråga 27 – Sker säkerhetskopiering internt?

Säkerhetskopior eller ”backup” finns till som reserv om något går fel med ”originalet”. Det kan dock vara svårare att komma åt personuppgifterna i en säkerhetskopia.

Med internt avses i våra egna system. Den säkerhetskopiering som sker *externt* kartläggs i *leverantörs*inventeringsmallen istället.

Fråga 28 – Om ni svarat ja på fråga 27: vad är det som säkerhetskopieras?

Förklaring av vad det kan vara, alltså är det hela systemet eller bara en del av det? Vissa personuppgifter men inte andra? Skriv så specifikt som möjligt (eller ”allt” om det är allt).

Fråga 29 – Om ni svarat ja på fråga 27: hur och var lagras säkerhetskopian? Hur länge lagras den?

Säkerhetskopior som sparas länge kan komma att innehålla personuppgifter som borde raderats tidigare. Automatiska metoder för gallring kan behövas.

Fråga 30 – Om ni svarat ja på fråga 27: är det tekniskt och organisatoriskt möjligt att förstöra säkerhetskopior av specifika personuppgifter i samband med att personuppgifterna gallras eller personuppgiftsbehandlingen upphör?

Med förstöra avses att uppgifterna inte går att återställa. Att det är organisatoriskt möjligt att förstöra inbegriper att det finns ett giltigt gallringsbeslut, se informationsbladet om gallring.

Registerutdrag och dataportabilitet

Den registrerade har rätt att på begäran få ut ett registerutdrag från den personuppgiftsansvarige. Ett registerutdrag är ett register över alla behandlingar som den personuppgiftsansvarige gör med den registrerades personuppgifter.

Den registrerade har också rätt att på begäran få ut sina uppgifter för att överföra dem till en annan personuppgiftsansvarig. Detta kallas för rätten till dataportabilitet, vilken fastställs i artikel 20 i förordningen. Den registrerade har bara denna rättighet när behandlingen grundar sig på samtycke eller avtal och behandlingen sker automatiskt.

Fråga 31 – Går det att få ut samtliga personuppgifter om en registrerad i systemet?

Se ovan.

Fråga 32 – Är det tekniskt möjligt att, i ett läsbart format, lämna ut de personuppgifter som rör en registrerad ifall den registrerade vill överföra personuppgifterna till en annan personuppgiftsansvarig?

Med läsbart format menas att uppgifterna ska tillhandahållas i ett allmänt använt och maskinläsbart format, till exempel i CSV-format. Tillhandahållandet kan ske genom att låta användaren ladda ned CSV-filen.

Fråga 33 – Är det tekniskt möjligt att överföra den registrerades personuppgifter direkt till annan personuppgiftsansvarig på den registrerades begäran?

Om det är tekniskt möjligt har den registrerade rätt att få sina uppgifterna överförda direkt från en personuppgiftsansvarig till en annan.

Svenska kyrkan

Radering och begränsning

För att hantera klagomål och begäran från registrerade behöver vi ha möjlighet att ”utan dröjsmål” vidta åtgärder med de registrerades specifika personuppgifter. Sådana åtgärder kan t.ex. vara att radera personuppgifter eller begränsa användningen av personuppgifter.

Fråga 34 – Är det tekniskt möjligt att ta bort enstaka personuppgifter ur IT-systemet och ur säkerhetskopian?

Den registrerade har rätt att få sina personuppgifter raderade bland annat om personuppgifterna inte längre är nödvändiga för de ändamål de samlats in för, eller samtycket för behandlingen har återkallats och det saknas annan rättslig grund för behandlingen (se avsnittet om laglig grund kopplat till fråga 10). Därför är det viktigt att utreda om det är möjligt att radera enstaka personuppgifter i systemet.

OBS att det finns en mängd undantag till denna regel och att en bedömning om huruvida en enstaka personuppgift ska raderas på begäran av den registrerade måste göras av en jurist och måste ha stöd av ett gallringsbeslut, se informationsbladet om gallring.

Fråga 35 – Är det tekniskt möjligt att begränsa behandlingen av den registrerades personuppgifter, så att personuppgifterna endast lagras och inte behandlas i övrigt, under tiden som den registrerade gör invändningar mot behandlingen?

När en registrerad har bett om att bli borttagen ur systemet måste en juridisk bedömning göras. Fram till att en sådan bedömning har gjorts får den registrerades personuppgifter inte fortsätta behandlas, utan bara lagras. Att radera personuppgifterna kan nämligen också vara otillåtet.

Fråga 36 – Om ni har svarat ja på fråga 35: beskriv hur behandlingen kan begränsas.

Detta kan till exempel vara att den registrerades personuppgifter fortsätter lagras men inte syns för andra än systemadministratören.

Svenska kyrkan

Överföring till land utanför EU/EES

Överföring av personuppgifter utanför EU/EES innebär en säkerhetsrisk i sig eftersom dataskyddsförordningens skydd inte gäller där. Överföring är därför som utgångspunkt förbjuden, men det finns vissa undantag. Detta följer av artiklar 44-48 i förordningen.

Huvudregeln är att personuppgifter endast får överföras till länder inom EU/EES samt de länder, områden eller organisationer som kommissionen har ansett kunna säkerställa en tillräcklig säkerhetsnivå. För övriga överföringar utanför EU/EES krävs extra skyddsåtgärder och därför bör sådana överföringar undvikas. Om en överföring till mottagare utanför EU/EES är nödvändig för verksamheten bör en jurist utreda vilken säkerhetsåtgärd som är lämplig.

Med överföring menas att personuppgifter görs tillgängliga i ett land utanför EU/EES. Detta kan t.ex. ske genom att information innehållande personuppgifter överförs via e-post, eller att ett dokument laddas upp på Dropbox (eftersom Dropbox servrar ligger i USA).

OBS. Publicering till intranätet innebär inte överföring till land utanför EU/EES **bara** för att innehållet kan ses därifrån.

Rättsläget på detta område är fortfarande oklart och det kan därför komma kompletterande inventeringsfrågor i efterhand. Om ni är osäkra på om någonting utgör en överföring eller inte kan ni ändå ta upp det i inventeringen för att kunna återkomma till det senare.

Fråga 37 – Överför ni personuppgifter till mottagare som finns i länder utanför EU/EES? På vilket sätt?

Se ovan.

Fråga 38 – Om ni har svarat ja på fråga 37: Vilka mottagare överförs uppgifterna till?

Se ovan.

Fråga 39 – Om ni har svarat ja på fråga 37: I vilka länder finns mottagarna?

Se ovan.

Fråga 40 – Om ni har svarat ja på fråga 37: Vad är anledningen till att uppgifterna överförs till mottagarna?

Se ovan.

Överföring till internationell organisation

Samma regler som vid överföring till land utanför EU/EES gäller för överföring till internationella organisationer (oavsett om de ligger inom eller utanför EU/EES). Internationell organisation definieras som en organisation och dess underställda organ som lyder under folkrätten, eller ett annat organ som inrättats genom eller på grundval av en överenskommelse mellan två eller flera länder. Sådana kan vara FN, internationella Röda Korset och internationella företag.

Fråga 41 – Överför ni personuppgifter till internationella organisationer? På vilket sätt?

Se ovan.

Fråga 42 – Om ni svarat ja på fråga 41: Vilka organisationer överförs uppgifterna till?

Se ovan.

Fråga 43 – Om ni svarat ja på fråga 41: I vilka länder finns organisationerna?

Se ovan.

Fråga 44 – Om ni svarat ja på fråga 41: Vad är anledningen till att uppgifterna överförs?

Se ovan.

Gallring

Det behöver finnas tekniska funktioner och rutiner för gallring eftersom personuppgifter – som utgångspunkt – inte får behandlas under en längre tid än vad som är nödvändigt utifrån det ändamål som uppgifterna samlades in för.

Se vidare om vad som gäller särskilt för gallring i Svenska kyrkan i informationsbladet.

Gallring kan vara såväl radering som anonymisering (om sätten att anonymisera är helt säkra – det ska vara omöjligt att koppla uppgifterna till en fysisk person).

Fråga 45 – Är det möjligt att lägga in automatisk gallring av vissa uppgifter som en funktion i IT-systemet?

Se ovan.

Fråga 46 – Är det möjligt att manuellt gallra uppgifter ur IT-systemet?

Se ovan.

Fråga 47 – Finns det beslut och rutiner för gallring av uppgifter? Om ja, beskriv rutinerna och hänvisa till beslutet.

Se ovan. Med beslut avses gallringsbeslut, se informationsbladet om gallring.

Personuppgiftsincident

I dataskyddsförordningen 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 personuppgiftsincident om en säkerhetsincident leder till obehörigt röjande av eller obehörig åtkomst till de behandlade personuppgifterna.

Fråga 48 – Vilka rutiner finns för att upptäcka personuppgiftsincidenter?

Se ovan.

Fråga 49 – Vilka rutiner finns för att rapportera personuppgiftsincidenter?

Se ovan.

Personuppgiftsbiträde (leverantör)

Dataskyddsförordningen ställer krav på personuppgiftsansvarigas kontroll över deras personuppgiftsbiträden. Om ett personuppgiftsbiträde behandlar uppgifter för er räkning i strid med dataskyddsförordningen skulle ni kunna hållas ansvariga. Den personuppgiftsansvariga är skyldig att säkerställa att personuppgiftsbiträdet behandlar personuppgifterna på ett korrekt och tillräckligt säkert sätt. Förhållandet mellan den ansvarige och biträdet ska regleras i ett särskilt personuppgiftsbiträdesavtal, vilket är ett uttryckligt krav i artikel 28 punkt 3. Dataskyddsprojektet på nationell nivå kommer att leverera en mall för personuppgiftsbiträdesavtal under våren 2018.

Fråga 50 – Har ni anlitat leverantörer för att behandla personuppgifter som ni samlat in?

En sådan leverantör skulle t.ex. kunna vara en leverantör av en applikation, ett företag som sköter driften av en egenutvecklad applikation, eller ett företag som erbjuder lagring av information (som innehåller personuppgifter) så som t.ex. Google Docs eller Dropbox.

Fråga 51 – Om ni svarat ja på fråga 50: vad heter leverantörerna och vad har de för organisationsnummer?

Se ovan.

Fråga 52 – Om ni svarat ja på fråga 50: finns personuppgiftsbiträdesavtal med leverantören?

Se ovan.

Svenska kyrkan

IT-säkerhet

Generellt tänk kring IT-säkerhet är ett indirekt krav i dataskyddsförordningen. Riktlinjer så som lösenordspolicyer, automatisk låsning av datorer och riktlinjer för vad som får skrivas i e-postmeddelanden visar att vi arbetar med vår IT-säkerhet internt. Mer information om IT-säkerhet finns att läsa i avsnittet om dataskydd i informationsbladet.

Fråga 53 – Beskriv er interna IT-säkerhetspolicy och eventuell annan säkerhetspolicy.

Se ovan.

Behandlingshistorik

Fråga 54 – För ni behandlingshistorik över personuppgiftsbehandlingen?

Frågan om loggning har viss överlappning med denna fråga, men syftar till olika saker. Behandlingshistorik förs för att registrera vad som händer med personuppgifterna. Sådan historik kan innehålla uppgifter om hur, och när, en administratör har ändrat en viss personuppgift.

Fråga 55 – Hur länge sparas behandlingshistoriken?

Se ovan.

Fråga 56 – Varför sparas behandlingshistoriken?

Se ovan.

Fråga 57 – Går det att identifiera vem som har gjort vad?

Den här frågan ställs i syfte att utreda om den behandling som gjorts kan kopplas till en fysisk person, genom exempelvis IP-nummer eller namn på den som utfört behandlingen.