Svenska kyrkan

DOKUMENT			SIDA
Generella rekommendationer för åtgärder av IT-system			1(12)
UPPRÄTTAT AV	DATUM	DOKUMENTBETECKNING	VERSION
GDPR-projektet	2018-05-25	Arbetsmaterial	0.1

Åtgärdsexempel

Nedan ges ett antal exempel på olika åtgärder som den nationella nivåns projektgrupp tagit fram till ansvariga för informationssystem och IT-system som behandlar personuppgifter.

Med begreppet ”åtgärd” menas inte enbart en teknisk åtgärd, som till exempel omprogrammering av ett IT-system. Det menas även administrativa åtgärder i form av till exempel anpassning av regelverk och kontroller av korrekt hantering av personuppgifterna, samt olika former av utbildningsinsatser. En bra åtgärd kombinerar med fördel alla dessa delar.

Åtgärdsexemplen ska tolkas som just exempel på hur nationell nivå arbetar med anpassning av de gemensamma IT-systemen. Syftet med och tanken bakom de olika åtgärderna i exemplen bör kunna vara applicerbara även på lokal nivå. Den fetade texten under varje exempel lyfter fram vad åtgärden innebär generellt.

Det finns förstås fler möjliga åtgärder än de som omnämns i det här dokumentet - och vissa åtgärder är kanske inte tillämpliga i ett specifikt fall. Oavsett detta kan exemplen tjäna som inspiration till egna frågeställningar och överväganden.

Samtliga åtgärdsexempel syftar till att säkerställa en korrekt hantering personuppgifter, såväl enligt gällande lagstiftning som inomkyrkliga regelverk, till exempel dataskyddsförordningen och personuppgiftspolicy och informationssäkerhetspolicy för den nationella nivån i Svenska kyrkan.

KYRKOKANSLIET
POSTADRESS: Kyrkokansliet, 751 70 Uppsala
BESÖKSADRESS: Sysslomansgatan 4
HEMSIDA: svenskakyrkan.se

Exempel

1: Ansvar och roller

En god informationssäkerhet bygger på tydlighet. Vilka förväntningar finns, vem ansvarar för att infria detta, vem följer upp osv.

Utifrån inventeringssvaret kan det tyckas otydligt vem som är att betrakta som ägare till innehållet (informationen) respektive vem som är att betrakta som ägare till IT-systemet. Målbilden är en dokumenterad och upplevd tydlighet där informationsägaren kravställer informationssäkerhet gentemot systemägaren. Det är alltså informationsägaren, vanligtvis den som är intresserad av vad som finns i systemet, som ska uttrycka kraven.

Åtgärden innebär att tydliggöra, förankra, dokumentera och etablera detta förhållningssätt.

2: Korrekt behandling utifrån ändamål

Varje personuppgiftsbehandling ska gå att spåra till ett tydligt ändamål /syfte och vara stött på en giltig rättslig grund. Systemet behandlar personuppgifter med olika ändamål och från olika källor.

Åtgärden innebär att säkerställa dokumentation kring hur uppgifterna får användas och att säkerställa att uppgifterna inte används för annat ändamål i eller utanför systemet på kort och långt sikt.

3: Testmiljö, utvecklingsmiljö och produktionsmiljö

Nationell nivå vill och ska ha kontroll över sina personuppgiftsbehandlingar, samt bedriva ett kvalitativt

utvecklingsarbete. En del i detta är ha separata miljöer för utveckling, test och produktion. En annan del att inte använda skarp data, inklusive skarpa personuppgifter, utanför produktionsmiljön. Dels ökar det risken för incidenter, dels exponerar det personuppgifter på ett onödigt sätt, dels ökar risken att inte kunna tillgodose krav och önskemål kring radering av personuppgifter.

Åtgärden innebär att avveckla skarpa personuppgifter i testmiljön och ersätta med andra, icke-skarpa, personuppgifter, samt ta fram rutin för att undvika att det sker igen.

4: Villkor för behandling

Åtgärd: Utred och ange laglig grund för varje behandling av personuppgifter som finns i systemet.

5. Gallring eller arkivering?

Om ändamålet, för vilket personuppgifterna från början samlades in, har upphört och det inte längre finns en laglig grund för behandlingen, ska uppgifterna antingen gallras (raderas) eller arkiveras. För gallring krävs gallringsbeslut. Ändamålet måste motiveras för varje enskild personuppgift.

Åtgärd: Ansök om gallringsbeslut, d v s bevarande- och gallringsutredning för personuppgifterna. Ett gallringsbeslut tar fram gallringsregler och/eller ställningstaganden om vad som ska arkiveras. Skriv in gallrings- och bevarandereglerna i dokumenthanteringsplan och ny bevarandestrategi (se SvKB 2017:1, 4 kap, §§ 17-23).

6: Stöd för gallring (radering)

Om personuppgifter ska gallras enligt beslut ska detta genomföras så fort som möjligt. Enligt SvKB 2017:2 (för lokal och regional nivå) ska detta

ske ”under kontrollerade former” och det ska vara möjligt att kontrollera och följa upp utförd gallring.

Åtgärd: Bygg in tekniskt systemstöd, d v s funktioner för automatiserad gallring som följer gallringsbeslut. Om det inte är möjligt, utforma rutiner för manuell gallring. Dokumentera gallringen genom kravspecifikation för systemet och arkivredovisningen. Rådgör med den nationella nivåns arkivarier.

7. Stöd för arkivering

Om personuppgifterna ska bevaras (kan framgå av dokumenthanteringsplan eller bevarande- och gallringsutredning) men inte kan behandlas på samma sätt som hittills i det systemet där de samlades in, måste särskilda arkiveringsåtgärder sättas in.

Vidare behandling för arkivändamål kräver att olika åtgärder vidtas för att skydda uppgifterna. Några av grundkraven är att de är avskilda från aktiva uppgifter, åtkomliga för ett minimalt antal personer samt skyddade från redigering och radering.

Principen om uppgiftsminimering kan innebära att vissa fält gallras samtidigt som andra fält arkiveras.

Åtgärd: Bygg in tekniskt systemstöd för att, som en tillfällig lösning, arkivera personuppgifterna i samma system. Undersök samtidigt möjligheterna att lägga in systemet i anslutningsplanen för Svenska kyrkans e-arkiv. Alternativt, anslut systemet direkt till e-arkivet och leverera informationen dit. Rådgör med den nationella nivåns arkivarier kring lämplig lösning.

8. Gallring av ostrukturerade personuppgifter

Personuppgifter är svårare att följa upp och håll koll på när de är ostrukturerade (information i löptext, fritextfält, bilder, filmer). När de bara ska behandlas under en viss tid måste det finnas effektiva strukturer

för att se till att de inte behandlas längre än den angivna tiden.

Åtgärd: Ta fram rutiner för att radera, anonymisera eller arkivera ostrukturerade personuppgifter när de inte längre är nödvändiga för ändamålet. Se till att det finns stöd i gallringsbeslut.

9. Fritextfält

Personuppgifter är svårare att upptäcka och hålla koll på när de finns i fritextfält. När det är nödvändigt att använda fritextfält bör innehållet kontrolleras genom att det finns tydliga rutiner för hur fritextfälten får användas.

Åtgärd: **Ta fram rutiner för hur fritextfält får användas.**

10. Information till annan part (utlämning)

Nationell nivå vill arbeta aktivt tillsammans med sina leverantörer för uppnå god säkerhet. En del i detta är tillit till leverantörens förmåga i frågor som rör säkerhet, men lika viktigt är uppföljning av det som leverantören åtagit sig att leverera.

Det handlar om att följa upp kravställningen, så väl den ursprungliga som den som växt fram med tiden, och verifiera att den fortfarande är gällande, känd och tillämpas.

Om leverantören genomgått någon form av extern granskning, till exempel SOC* eller certifiering, är även det intressant att dokumentera och regelbundet följa upp. Jämför med processen för den ursprungliga upphandlingen och då systemet valdes.

Detta är en särskilt viktig åtgärd om leverantören av systemet också har tillgång till informationen i systemet, i synnerhet personuppgifterna.

Större leverantörer kan tänkas hantera personuppgifterna på flera ställen i världen och därmed tvingas följa där gällande lagstiftning. Denna skulle i sin tur kunna krocka med hur ni vill att information och personuppgifter ska behandlas.

Leverantören kan också tänkas använda innehållet i sina system för olika former av rapporter eller som underlag för till exempel reklam eller säljstöd, vilket i sin tur skulle kunna innebära att information och personuppgifter sprids.

Åtgärden innebär att gå igenom och dokumentera ställda krav kring leveransen av systemet tillsammans med leverantören. Detta för att verifiera att kraven och säkerheten kring systemet fortfarande är giltiga, förstådda och tillämpas i leveransen av systemet - samt hur en sådan uppföljning kan göras kontinuerligt, eventuellt med fokus på olika delområden.

Åtgärden innebär även att säkerställa att det finns och tillämpas regelverk för vad en leverantör tillåts och inte tillåts göra för att bland annat förhindra vidarebehandling på eget bevåg.

11. Personuppgiftsbiträdesavtal

Åtgärd: **Personuppgiftsbiträdesavtal ska ingås med leverantören om denne är personuppgiftsbiträde. Situationerna internt i kyrkan kan vara mycket komplicerade, och i vissa fall utreds frågan därför av nationell nivå. Ta del av guiden på internwww.svenskakyrkan.se/dataskydd och rådgör med ditt stifts kontaktperson.**

12. Personuppgiftsbiträdets roll vid radering, rättelse, registerutdrag och dataportabilitet

Identifiera och dokumentera vilka beroenden ni har av leverantören: kan ni radera, rätta och exportera personuppgifter utan att blanda in

leverantören? Finns det stöd i personuppgiftsbiträdesavtalet för att kräva att de hjälper till? Vilka kontaktvägar finns med leverantören för det syftet?

Åtgärd: Utred frågan, dokumentera resultatet och anpassa eventuellt era rutiner.

13. Behörighet

Nationell nivå vill tillämpa tankesätten rätt information till rätt person vid rätt tillfälle samt principen om minsta möjliga rättigheter. En viktig del i detta är tilldelning av behörighet till och i system och tjänster, men även att behörighet avvecklas på ett kontrollerat sätt.

Från GDPR-håll vill vi lyfta frågan om avveckling av behörigheter. Risken med en behörighet som ligger kvar för länge skulle kunna bedömas som värre än om en legitim användare blir av med sin behörighet och tvingas begära återaktivering.

Åtgärden innebär att undersöka och i slutänden implementera automatiserad inaktivering av behörigheter, till exempel genom tidsbegränsning. Arbetet kan med fördel påbörjas uppifrån i behörighetshierarkin, det vill säga först för personer/konton på högsta behörighet.

14. Loggar

Nationell nivå strävar efter spårbarhet i sin informationshantering. Syftet är att bland annat att kunna följa upp att information hanteras korrekt, men också att kunna analysera eventuella incidenter: ”var gick det fel, när gick det fel, varför gick det fel och vad kan vi göra för att det inte ska kunna hända igen”. Utöver det finns behovet av att vid regelverksbrott kunna följa ett spår bakåt.

Loggarna för ett system är utifrån detta en viktig informationstillgång som ska skyddas därefter. Det är informationsägaren som ska kravställa gentemot systemägaren att tillräcklig spårbarhet uppnås, till exempel genom loggning i ett system.

Systemägaren eller en extern leverantör kan komma med förslag, men det är viktigt att informationsägaren åtminstone förstått och accepterat dessa. Annars finns risken för glapp mellan outtalad förväntan och faktiskt leverans.

I inventeringssvaret på nationell nivå beskrivs att användare inte informeras om att loggning sker. Även om det informeras övergripande kring IT-landskapet och att det där förekommer loggning, är det önskvärt att det även informeras systemvis.

Åtgärden innebär att dokumentera informationsägarens krav kring spårbarhet. Det innebär även att kontrollera - och vid behov genomföra - nödvändiga förändringar för att uppnå tillräcklig spårbarhet.

Detta inkluderar bland annat frågeställningar kring hur länge, i vilken omfattning och vilken typ av skydd loggarna i sig behöver. Gallring av loggar får inte ske utan gallringsbeslut.

Åtgärden innebär även att tydliggöra att loggning förekommer. Det ligger i vårt intresse att se till att användaren förstått att denne loggas, inte enbart i användarens intresse.

15. Privat utrustning och utlandet

Nationell nivå vill minska risker som rör informationssäkerhet. En del i detta är att minska möjliga attackytor som kan användas för att komma åt känslig information.

Å ena sidan: information får inte göras tillgänglig eller avslöjas på ett sådant sätt att den personliga integriteten eller sekretessen hotas.

Å andra sidan: information ska kunna användas i förväntad utsträckning, inom önskad tid och på rätt plats. Informationsägarens klassning av information måste ligga till grund för hur man ser på detta.

Det är relevant att ställa sig frågan om det på något sätt går och är önskvärt att begränsa åtkomsten från utlandet till systemet. Detta gäller i synnerhet om åtkomst sker över okrypterade anslutningar och privat utrustning/icke managerad utrustning. Man bör åtminstone regel- och utbildningsmässigt beskriva vad kring detta som är tillåtet, men gärna följa upp det med någon sorts teknisk begränsning.

Åtgärden innebär att undersöka och utvärdera möjligheten att på olika sätt begränsa möjligheten att nå framförallt den administrativa delen av systemet (och därigenom informationen i systemet) från klienter utanför nationell nivås kontroll samt högriskmiljöer såväl inom som utanför EU.

16. Säkerhetskopiering

En god informationssäkerhet bygger på tydlighet. Vilka förväntningar finns, vem ansvarar för att infria detta, vem följer upp osv.

När det gäller säkerhetskopiering behöver informationsägaren uttrycka vilka krav som finns och systemägaren behöver hantera dessa.

Krav ska dokumenteras och regelbundet följas upp. Om man vill svara ”vi har samma backup som alla andra”, så behöver man först dokumentera vilka krav man har på säkerhetskopiering, därefter ställa dessa krav mot hur alla andra gör, och slutligen dokumentera att det matchar, alternativt att man accepterar skillnaden.

Kraven bör sedan följas upp regelbundet. Detsamma gäller förstås om säkerhetskopieringen utförs av extern part, det vill säga systemleverantören.

Åtgärden innebär att tydliggöra, förankra, dokumentera och etablera detta förhållningssätt, men även att formulera informationsägarens krav på säkerhetskopiering, kravställa och följa upp kring detta. Detta inkluderar även frågor kring hur säkerhetskopiorna skyddas, krav kring återläsningstest samt gallring. För detta ska arkivarie involveras.

17. Begränsning/förhindrande av behandling av personuppgifter vid invändning/utredning

Inventeringssvaret, 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? Svaret är ”nej”.

Åtgärden innebär att ta fram en rutin och möjligt systemstöd för att kunna hantera detta, dvs begränsa behandling av den registrerades personuppgifter under tiden som den registrerade gör invändning mot behandlingen.

18. Generellt systemstöd för automatisk utlämning av personuppgifter

Nationell nivå måste lämna ut uppgifter om vilka personuppgifter som finns kopplat till en specifik person om personen i fråga efterfrågar denna information. För att effektivisera detta utlämnande ska hanteringen i möjligaste mån automatiseras.

Åtgärden innebär att i systemet säkerställa att det finns ett API för att hämta ut personuppgifter för att automatiserat kunna lämna ut dem. Enheten för arkitektur har tagit fram en kravspecifikation som ska användas.

19. Systemdokumentation och kravställning

Nationell nivå strävar efter att uppnå kontinuitet i sin informationshantering. En viktig del i detta är dokumentation: först och främst att den finns, men även att det är uppdaterad, korrekt och begriplig för någon annan än den som skrivit den.

Åtgärden innebär att säkerställa att all tillämplig dokumentation för systemet finns tillgänglig och att underhållsansvar finns dokumenterat.

20. Incidenthantering

Nationell nivå vill med incidenthanteringen nå fram till ett proaktivt läge, där tidigare incidenter hjälper oss att identifiera och förstå hur vi kan hantera och anpassa systemet innan en ny incident inträffar. Incidenthanteringen är alltså inte bara att vara reaktiv när incidenten sker, utan också proaktiv genom att lära sig av den.

Nationell nivå kommer att formulera övergripande processer för hur personuppgiftsincidenter ska hanteras där. En del i detta blir att hantera olika typer av manuell rapportering från användare. Den andra delen handlar om att med verktyg mer eller mindre automatiserat analysera avvikelser i system, till exempel genom logganalys.

Åtgärden innebär att formulera på vilket sätt möjliga incidenter skulle kunna inträffa i systemet, till exempel överträdelse av regelverk, och komma med förslag på hur detta i första hand kan byggas bort, i andra hand automatiskt identifieras och rapporteras.

*Nationell nivå vill arbeta aktivt tillsammans med sina leverantörer för uppnå god säkerhet. En del i detta är tillit till leverantörens förmåga i frågor rörande säkerhet, men lika viktigt är uppföljning av det som leverantören åtagit sig att leverera. Det handlar om att följa upp

kravställningen, så väl den ursprungliga som den som växt fram med tiden, och verifiera att den fortfarande är gällande, känd och tillämpas. Om leverantören genomgått någon form av extern granskning, till exempel Service Organization Control (SOC) 2 med tillhörande rapport eller certifiering, är även det intressant att dokumentera och regelbundet följa upp. Jämför med processen för den ursprungliga upphandlingen och då systemet valdes.