Anbudspresentation

Dataskyddsombud till Svenska kyrkan

12 april 2021

XEEDA KONSULTER

Agenda

- Presentation kring bordet
- Presentation av Xeeda
- Beskrivning av vårt anbud
- Svar på utsända frågor

XEEDA KONSULTER

Presentation av Xeeda

Anna Herre

Anna kommer vara kund- och uppdragsansvarig samt hålla ihop arbetet mot Svenska kyrkan.

Anna är diplomerad dataskydds-strateg och är projektledare. Hon har som konsult arbetat med olika verksamhetsprojekt inom såväl offentlig som privat verksamhet i över 15 år.

Gabriel Axelsson

Gabriel är jurist och inriktad mot GDPR och dataskyddsfrågor. Gabriel är diplomerad dataskyddsstrateg och har flera uppdrag som dataskyddsombud samt arbetar operativt med flera av våra kunder med att höja deras mognadsnivå när det gäller GDPR bl.a. genom att informationssäkerhetsklassa system, mäta en organisations mognadsnivå.

Urban Jonsson

Urban är civilekonom och MBA med inriktning på ledning och styrning. Urban är certifierad IT-revisor (ISACA), har genomgått utbildning som informationssäkerhetsstrateg, inom GDPR och har en bakgrund av att arbeta med IT-styrning i över 30 år. Urban har arbetat med att höja mognadsnivån när det gäller dataskydd i både kommuner och privata organisationer.

Magdalena Makowski

Magdalena kommer vara leveransansvarig och arbetar som juridisk konsult och är specialiserad inom dataskyddslagstiftning och integritetsfrågor. Hon är diplomerad dataskyddsstrateg samt certifierad ”ISO/IEC 27001 Lead Implementer”. Hon har hjälpt såväl privata som offentliga aktörer att förbereda sig inför de stora förändringar som GDPR inneburit, arbetat som DSO samt stöttar upp med rådgivning kring informationssäkerhet i ett flertal kommuner

XEEDA
KONSULTER

Kort sammanfattning om Xeeda

- Konsultföretag etablerat 2004
- Oberoende företag som ägs av två partners som grundade företaget
- Ett 30-tal erfarna och resultatorienterade konsulter och underkonsulter i uppdrag
- Omsätter över 40 MSEK
- Arbetar till stor del med offentlig sektor; kommun, regioner samt myndigheter
- Flera av våra konsulter har en juridisk bakgrund
- Samtliga av våra konsulter som arbetar med informationssäkerhet har en certifiering inom området.

XEEDA KONSULTER

Vi arbetar oftast i uppdrag med en kombination av olika kompetenser och ledningsfrågor

Digitalisering

Digitaliseringen är en faktor som driver på utveckling och behovet av förändring för många organisationer.

Informationssäkerhet

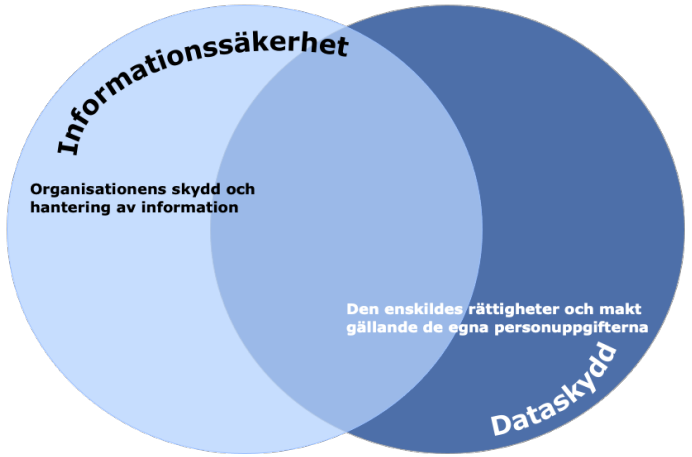
Verksamhetsutveckling

Leverantörsstyrning

Sammanfattning av Xeedas erfarenheter när det gäller informationssäkerhet och dataskyddsfrågor inom offentlig verksamhet

Xeeda har arbetat med ett flertal kommuner i Stockholms län med att höja deras mognadsnivån och medvetandet när det gäller informationssäkerhet och GDPR. Nedan är ett urval vad vi hjälpt kommunerna med:

- Förbereda organisationen inför och efter att GDPR infördes.
  - Sätta upp ramverk och riktlinjer för att proaktivt klara regelefterlevnad.
  - Bistått/lett det operativa dataskyddsarbetet som att granska avtal, genomföra utbildningar och stöd vid incidenthantering.
  - GAP-analyser
- Rollen som dataskyddsombud alt rådgivare
- Informationsklassning och ta fram handlingsplaner
- Informationssäkerhetspolicy och tillhörande riktlinjer
- Genomföra utbildningar för olika målgrupper
- Vägledande dokument för molntjänsthantering



XEEDA KONSULTER

Vad vi jobbar med inom informationssäkerhet

REGELEFTERLEVNAD/COMPLIANCE

- DSO
- ”Juridisk” informationssäkerhet
- Branschspecifik lagstiftning och regelverk

Tjänster

- DSO
- Informationssäkerhetspolicy
- Informationsklassning
- Roller och ansvar
- Införa ISO27001

INFORMATIONSSÄKERHET

FÖRSTÄRKNING

- Införande av ledningssystem (ISMS, ISO27001)
- Policy/instruktioner
- Organisationer med roller och ansvar
- Utbildning

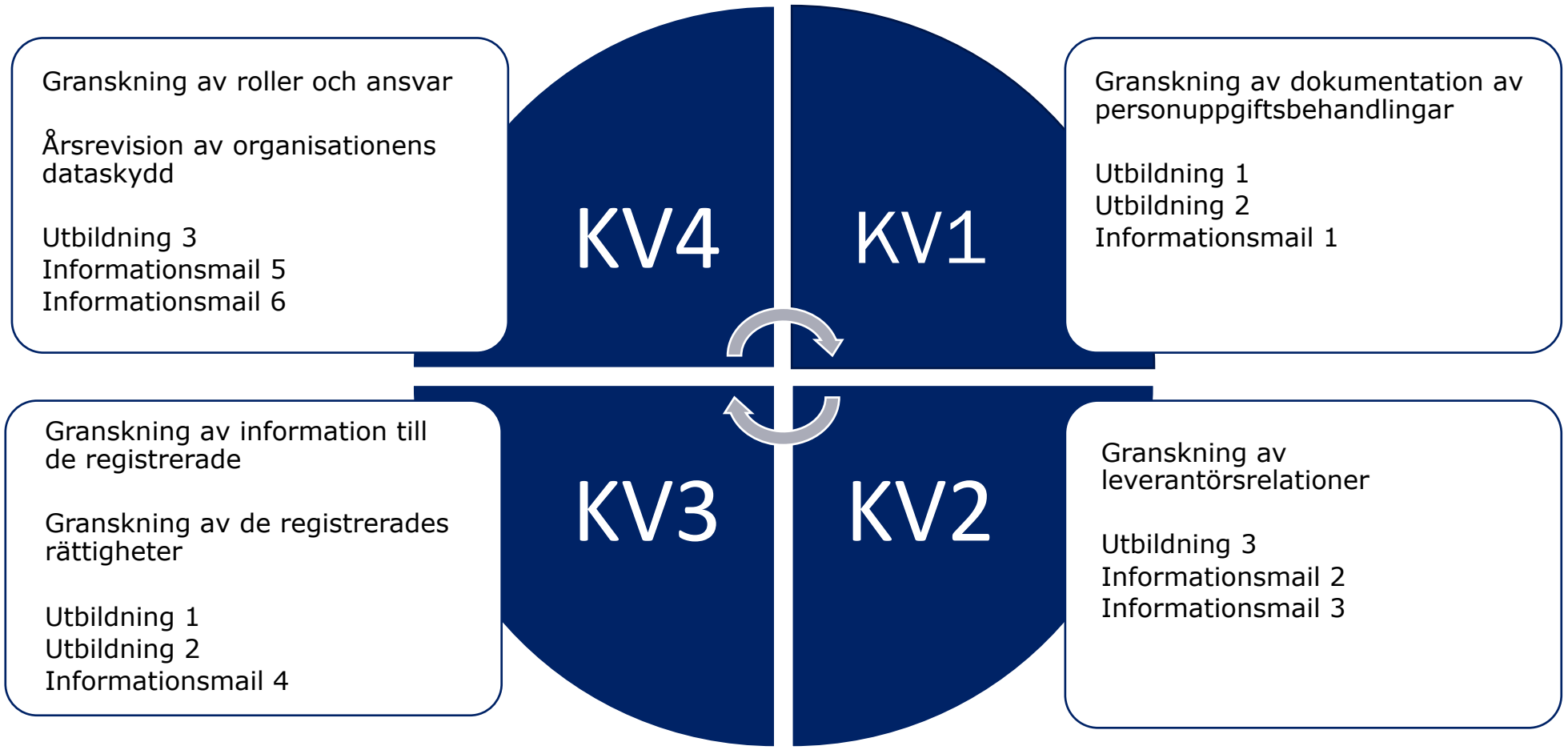
OPERATIVT ARBETE

- GAP-analyser
- Informationsklassning
- Förändringsledning och arbetssätt
- Riskarbete
- Operativt dataskyddsarbete

XEEDA KONSULTER

Presentation av vårt anbud

Vårt årshjul gör det möjligt att arbeta strukturerat och systematiskt med dataskyddsfrågor



XEEDA KONSULTER

Vad som ingår i prenumerationstjänsten

- Löpande rådgivning och rekommendationer hur verksamheten ska optimera sitt dataskyddsarbete. Det finns ingen fråga som är för liten eller för stor, utan vem som helst inom verksamheten kan alltid vända sig till dataskyddsombudet med frågor kopplade till dataskyddsförordningen eller annan dataskyddslagstiftning.
- Granskning och kontroll av vilka personuppgiftsbehandlingar som behöver justeras för att vara mer i linje med dataskyddsförordningens regler.
- Säkerställa att konsekvensbedömningen utförs korrekt och att de relevanta riskerna beaktas.
- Att vara kontaktperson för både de registrerade och Integritetsskyddsmyndigheten.
- Årlig revision (se separat bild)
- Nyhetsbrev/informationsmail
- Sammanställning av vanligt förekommande frågor som finns tillgängligt för alla
- Utbildningar (se separat bild)

XEEDA KONSULTER

Årlig revision

- Dataskyddsombudet ska övervaka efterlevnaden av dataskyddsförordningen vilket bl.a. kan göras genom att utföra granskning. Det framgår inte av dataskyddsförordningen exakt vad granskningen ska innehålla, eller när den ska utföras.
- Vår rekommendation är att en revision av en församlings eller pastorats dataskyddsarbete genomförs årligen och innehåller granskning av:
  - dokumentation av personuppgiftsbehandlingar
  - organisation och ansvar
  - information till de registrerade
  - leverantörsrelationer
  - registrerades rättigheter
- Granskningen kan sammanställas på olika sätt, exempelvis som en årsrapport.

XEEDA KONSULTER

Utbildning

Under första åren kommer vi genomföra tre olika digitala utbildningar som hålls vid två olika tillfällen vardera. Utbildningarna tar ca en timma och kommer behandla de delar av dataskyddsförordningen berörda medarbetare inom församlingarna och pastoraten bör ha en grundläggande kunskap om.

Den första utbildningen är en allmän dataskyddsutbildning där vi går igenom vad dataskyddsförordningen innebär.

- Vad är en personuppgift?
- Vad är dataskyddsförordningens syfte?
- Vad är en personuppgiftsbehandling?
- När behandlas personuppgifter i församlingarna?
- Vilka olika roller och ansvar finns?
- Vad ska jag som medarbetare tänka på?
- Vilka rättigheter har enskilda individer?

XEEDA KONSULTER

Utbildning, forts

Den andra utbildningen redogör för det praktiska arbetet med dataskyddsförordningen. Under utbildningstillfället kommer vi visa hur medarbetare ska dokumentera arbetet med dataskyddsförordningen genom användningen av Xeedas mallar.

- Hur använder vi oss av registerförteckningsmallen och vad ska den innehålla?
- Hur använder vi oss av avtalsmallen och hur upprättar vi avtal med våra leverantörer?
- Hur använder vi oss av konsekvensbedömningsmallen och hur genomför vi en konsekvensbedömning?

Den tredje utbildningen kommer baseras på och ta upp vanliga frågor vi har fått under det första året. Detta för att ge alla ett tillfälle att höra oss resonera kring hur församlingarna och pastoraten kan arbeta med frågorna och våra rekommendationer för hur särskilda situationer kan hanteras.

XEEDA KONSULTER

Samordning mellan församlingar och pastorat

För att samordna och minska kostnaderna för församlingar och pastorat men också för att åstadkomma ett mer strukturerat och kvalitetssäkrat arbetssätt föreslår Xeeda att hantering och aktiviteter hålls samman på ett enhetligt sätt:

- Gemensamma mallar för t.ex. personuppgiftsbiträdesavtal (PuB-avtal), registerförteckning samt konsekvensbedömning.
- Enhetlig hantering av frågor som uppstår med leverantörer.
- Nyhetsbrev/informationsmail
- Utbildningar
- Erfarenhetsåterkoppling

En fråga vi gärna diskuterar vidare är hur vi även kan delge information, samt ha en dialog med de församlingar och pastorat som väljer att ha interna dataskyddsombud

XEEDA KONSULTER

Xeedas prismodell för prenumeration

Kategori	Benämning	Antal årsarbetare	Abonnemang kostnad per år inkl. moms
XS	Mycket liten ekonomisk enhet	1-10	2000 kr/år inkl moms
S	Liten ekonomisk enhet	11-25	3200 kr/år inkl moms
M	Medelstor ekonomisk enhet	26-50	4800 kr/år inkl moms
L	Större ekonomisk enhet	51-100	6400 kr/år inkl moms
XL	Extra stor ekonomisk enhet	>101	6400 kr/år inkl moms

- Abonnemangskostnaden bygger på dels den ekonomiska enhetens storlek, dels antalet timmar församlingar och pastorat köpt tjänster för historiskt.
- Vi har i vår föreslagna abonnemangskostnad lagt oss på en sådan nivå så att det ska vara gynnsamt och intressant för församlingar och pastorat att ansluta sig.
- De tjänster som vi erbjuder som tillägg är sådana tjänster som kan bli aktuella när något utöver det vanliga dataskyddsarbetet inträffar.

XEEDA KONSULTER

Vid uppstart

- Våra offererade konsulter har dokumenterad sakkunskap om dataskyddsombudets roll och uppgifter utifrån GDPR och har både genom tidigare uppdrag samt utbildningar djupgående kunskap om både dataskyddsförordningen samt dataskyddslagstiftning och hur den tillämpas nationellt och i EU
- Inför ett nytt uppdrag kommer vi att sätta oss in i hur
  - personuppgifter behandlas i Svenska kyrkan och främja för en god dataskyddskultur inom uppdragsgivarens organisation
  - kyrkoordningen och gällande lagstiftning
  - Svenska kyrkans organisation, IT-system och personuppgiftsbehandlingar
- Vi kommer skapa en funktionsbrevlåda som Xeedas konsultteam bevakar som grupp. Om en frågan inte ingår i prenumerationstjänsten kommer vi meddela detta för att församlingen/pastoratet ska kunna välja om de vill att vi ändå utreder detta.

Inför uppstart kommer vi tillsammans med uppdragsgivaren sätta upp rutiner och rapporteringsvägar för samverkan kring arbetet med dataskyddsfrågor. Vi ser gärna ett nära samarbete i syfte att höja mognadsnivån för samtliga enheter inom de tre stiften.

XEEDA KONSULTER

Svar på utsända frågor

Det första scenariot

En liten landsbygdsförsamling med mindre än 10 årsarbetare vänder sig till oss med två ärenden.

1. En medlem som valt att gå ur Svenska kyrkan vill att alla personuppgifter som finns lagrade om hen i församlingen ska tas bort.
   - Ingår i prenumerationen.
2. En nyckel till församlingshemmet där församlingsexpeditionen ligger är borttappad. Nyckeln har varit borta en dag och tillhör en vaktmästare. Nyckeln går till alla utrymmen i byggnaden.
   - Ingår inte i prenumerationen. Uppskattad tid ca 2 timmar.

Ärende 1: Rätten att få sina personuppgifter raderade

Xeedas rekommenderade aktiviteter och som ingår i prenumerationstjänsten

1. Genom registerförteckningen vet församlingen vilka personuppgifter som behandlas och var dessa personuppgifter finns.
2. När vi vet i vilka IT-system, dokument och listor det finns personuppgifter behöver församlingen systematiskt söka efter den registrerades personuppgifter och ta bort dem. Vi rekommenderar att detta dokumenteras för att säkerställa att församlingen kan visa på regelefterlevnad.
3. Församlingen sammanställer vilka personuppgifter som har raderats och överlämnar sammanställningen till den registrerade.
4. Om den registrerades personuppgifter även behandlas av andra delar av Svenska kyrkans organisation bör församlingen uppmärksamma den registrerade om detta och meddela vem denne ska kontakta för att begära om att även dessa personuppgifter ska raderas.

XEEDA KONSULTER

Ärende 2: Borttappad nyckel

Xeedas rekommenderade aktiviteter och som är tilläggstjänster

1. Församlingen bör anmäla personuppgiftsincidenten till Integritetsskyddsmyndigheten inom 72 timmar efter det att de upptäckte att nyckeln var försvunnen.

   En personuppgiftsincident ska anmälas till Integritetsskyddsmyndigheten om det kan föreligga en risk för de registrerades rättigheter, även om församlingen inte kan bekräfta om någon skada har uppstått eller inte.

2. Församlingen bör byta ut låset till församlingshemmet.
3. Församlingen bör säkerställa att personuppgifter inte skadades under den tid som nyckeln var borttappad.

Det finns möjlighet för församlingen att använda Xeedas tilläggstjänst ”Operativ stöttning i samband med personuppgiftsincidenter”. Då hjälper Xeeda till med bedömning om det inträffade ska ses som en personuppgiftsincident, och om den bör anmälas till Integritetsskyddsmyndigheten. Xeeda övervakar arbetsprocessen för att säkerställa att anmälan upprättas. Uppskattad tid: ca 2 timmar.

XEEDA KONSULTER

Sammanfattning av det första scenariot

En liten landsbygdsförsamling med mindre än 10 årsarbetare vänder sig till oss med två ärenden.

1. En medlem som valt att gå ur Svenska kyrkan vill att alla personuppgifter som finns lagrade om hen i församlingen ska tas bort.
   - Ingår i prenumerationen.
2. En nyckel till församlingshemmet där församlingsexpeditionen ligger är borttappad. Nyckeln har varit borta en dag och tillhör en vaktmästare. Nyckeln går till alla utrymmen i byggnaden.
   - Ingår inte i prenumerationen. Uppskattad tid ca 2 timmar.

<u>Sammanfattning av kostnaden för en församling av storlek XS</u>

Prenumerationskostnaden är 2000 kr/år.

Inträffar ovan händelser tillkommer en kostnad på ca 2000 kr.

Årskostnaden varierar beroende på antalet och omfattningen av ärendena.

XEEDA KONSULTER

Det andra scenariot

Ett större pastorat med över 70 årsarbetare har precis köpt in ett nytt IT-system.

1. En systemkontroll behöver utföras då de inte vet om detta efterlever lagstiftningen. IT-systemet ligger utanför Svenska kyrkans nationella system där normalt sett dessa kontrolleras.
   - Ingår inte i prenumerationen. Uppskattad tid 3-6 timmar.
2. Ett personuppgiftbiträdesavtal som behöver upprättas som del av ett nytt avtal man tecknat med leverantör.
   - Ingår i prenumerationen.
3. En fråga har inkommit från IMY till pastoratet.
   - Ingår i prenumerationen.
4. En anställd har tappat bort sin tag till jobbet.
   - Ingår inte i prenumerationen. Uppskattad tid 2 timmar.

XEEDA KONSULTER

Ärende 1: Systemkontroll

Xeedas rekommenderade aktiviteter och som är tilläggstjänster

1. Xeeda kan hjälpa till med att göra en efterhandskontroll genom att informationssäkerhetsklassa informationen i systemet.
2. Xeeda bjuder då in några utvalda av pastoratets anställda med olika kompetenser. Tillsammans utreder vi informationens värde för pastoratet och konstaterar vilket säkerhetsbehov informationen har.
3. Informationens säkerhetsbehov är det som avgör vilka säkerhetskrav ett system måste uppfylla. Sedan jämför vi säkerhetskraven mot det inköpta systemets kapacitet.

Det finns möjlighet för pastoratet att använda Xeedas tilläggstjänst ”Inbyggt dataskydd och dataskydd som standard.” Det innebär att Xeeda bistår med t.ex. kontroll av IT-system för att säkerställa att det lever upp till dataskyddsförordningens krav.

Hur lång tid en sådan kontroll kan ta beror på en rad faktorer som t.ex. hur stort systemet är, vilka personuppgifter som ska behandlas etc. Uppskattad tid: ca 3-6 timmar.

XEEDA KONSULTER

Ärende 2: Upprätta ett personuppgiftsbiträdesavtal

Xeedas rekommenderade aktiviteter och som ingår i prenumerationen.

1. Vi rekommenderar att pastoratet använder den avtalsmall och instruktionsmall som Xeeda har tagit fram och som pastoratet har tillgång till som prenumerant.

XEEDA KONSULTER

Ärende 3: Fråga från Integritetsskyddsmyndigheten

Xeedas rekommenderade aktiviteter och som ingår i prenumerationen

1. Det är dataskyddsombudets uppgift att vara kontaktperson både för de registrerade och för Integritetsskyddsmyndigheten. Oavsett vad frågan handlar om ingår det i prenumerationen.

XEEDA KONSULTER

Ärende 4: Borttappad tag

Xeedas rekommenderade aktiviteter som är tilläggstjänster

1. Pastoratet bör anmäla personuppgiftsincidenten till Integritetsskyddsmyndigheten inom 72 timmar efter det att de upptäckte att tagen var försvunnen.

   En personuppgiftsincident ska anmälas till Integritetsskyddsmyndigheten om det kan föreligga en risk för de registrerades rättigheter, även om pastoratet inte kan bekräfta om någon skada har uppstått eller inte.

2. Pastoratet bör identifiera och avprogrammera den borttappade tagen.
3. Pastoratet bör säkerställa att personuppgifter inte skadades under den tid som nyckeln var borttappad.

Det finns möjlighet för församlingen att använda Xeedas tilläggstjänst ”Operativ stöttning i samband med personuppgiftsincidenter”. Då hjälper Xeeda till med bedömning om det inträffade ska ses som en personuppgiftsincident, och om den bör anmälas till Integritetsskyddsmyndigheten. Xeeda övervakar arbetsprocessen för att säkerställa att anmälan upprättas. Uppskattad tid: ca 2 timmar.

XEEDA KONSULTER

Det andra scenariot

Ett större pastorat med över 70 årsarbetare har precis köpt in ett nytt IT-system.

1. En systemkontroll behöver utföras då de inte vet om detta efterlever lagstiftningen. IT-systemet ligger utanför Svenska kyrkans nationella system där normalt sett dessa kontrolleras.
   - Ingår inte i prenumerationen. Uppskattad tid 3-6 timmar.
2. Ett personuppgiftbiträdesavtal som behöver upprättas som del av ett nytt avtal man tecknat med leverantör.
   - Ingår i prenumerationen.
3. En fråga har inkommit från IMY till pastoratet.
   - Ingår i prenumerationen.
4. En anställd har tappat bort sin tag till jobbet.
   - Ingår inte i prenumerationen. Uppskattad tid 2 timmar.

<u>Sammanfattning av kostnaden för en församling av storlek L</u>

Prenumerationskostnaden är 6400 kr/år.

Inträffar ovan händelser tillkommer en kostnad på ca 5000-8000 kr.

Årskostnaden varierar beroende på antalet och omfattningen av ärendena.

XEEDA KONSULTER