

till Avtal mellan
Pastoratet/församlingen
och systemleverantören
Y.

Avtal avseende behandling av personuppgifter m m (personuppgiftsbiträdesavtal)

§ 1 Bakgrund

1.1 Pastoratet/församlingen X (pastoratet) har träffat ett avtal med Systemleverantören Y (leverantören), som innebär att Y hos Trossamfundet Svenska kyrkan, för X räkning, ska hämta personuppgifter i trossamfundets datasystem. Y kommer därmed att behandla personuppgifter för vilka pastoratet är personuppgiftsansvarig enligt personuppgiftslagen (1998:204), PuL. PuL kräver att skriftligt avtal träffas mellan den som är personuppgiftsansvarig och den som är personuppgiftsbiträde (personuppgiftsbiträdesavtal). Detta avtal utgör ett sådant personuppgiftsbiträdesavtal mellan parterna.

§ 2 Behandling av personuppgifter

2.1 Leverantören får behandla personuppgifter för vilka pastoratet är personuppgiftsansvarig endast i enlighet med PuL, dess förordning och Datainspektionens föreskrifter, detta avtal samt i enlighet med pastoratets beslut.

2.2 Leverantören är skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med hänsyn till

- de tekniska möjligheter som finns,
- kostnaderna för att genomföra åtgärderna,
- de särskilda risker som finns med behandlingen av personuppgifterna
- hur känsliga de personuppgifter som behandlas är.

§ 3 Rätt till insyn

3.1 Pastoratet har en enligt PuL 31 §, 2 st, skyldighet att kontrollera att den behandling av personuppgifter som utförs av leverantören uppfyller vad som angivits i § 2 ovan.

3.2 Pastoratet har, i egenskap av personuppgiftsansvarig, rätt att vidta nödvändiga åtgärder för att förvissa sig om att leverantören kan genomföra de säkerhetsåtgärder som skall vidtas enligt § 2 ovan, samt för att förvissa sig om att leverantören verkligen vidtar dessa åtgärder. Leverantören åtar sig att se till att pastoratet får den hjälp som skäligen kan krävas för att pastoratet på enkelt sätt ska kunna förvissa sig om detta.

§. 4 Ansvar – anställda, konsulter och övriga medhjälpare

4.1 Leverantören och anställda, konsulter och övriga medhjälpare hos leverantören ska vid personuppgiftsbehandling i enlighet med detta avtal iaktta de olika regler som kan finnas för förbud att röja uppgifter (sekretess).

4.2 Leverantören ansvarar för att anställda, konsulter och övriga medhjälpare som behandlar personuppgifterna har kunskap om de säkerhetsrutiner som gäller.

4.3 Såvitt avser skyddade personuppgifter ska Skatteverkets vägledning för hantering av sekretessmarkerade personuppgifter i offentlig förvaltning följas i tillämpliga delar.

§ 5 Åtgärder vid slutförande av behandling av personuppgifter

5.1 När leverantörens behandling av personuppgifter för vilka pastoratet är personuppgiftsansvarig har slutförts ska i enlighet med avtalet mellan parterna personuppgifterna antingen återföras till pastoratet eller raderas på ett sätt så att de inte kan återskapas. Anger inte avtalet vad som skall ske med personuppgifterna ska de raderas så att de inte kan återskapas. På begäran av pastoratet ska leverantören lämna ett skriftligt besked om vilka åtgärder som vidtagits med personuppgifterna i samband med att behandlingen har slutförts.

§ 6 Ansvar - ersättning

6.1 I personuppgiftslagen stadgas att den personuppgiftsansvarige skall ersätta den registrerade för skada eller kränkning av den personliga integriteten som en behandling av personuppgifter i strid med lagen har orsakat.

6.2 Pastoratet ska äga rätt att av leverantören utfå ersättning för belopp som utbetalats som skadestånd enligt denna bestämmelse om den behandling av personuppgifter som ligger till grund för skadeståndsansättningen utförts av leverantören i strid med detta avtal och utan instruktioner av pastoratet. Ersättning kan endast utgå för skadeståndsbelopp som är slutligt fastställt av domstol eller som utbetalas efter förlikning med dem som lidit skada.

§ 7 Tillägg och ändringar

7.1 Ändringar och tillägg till detta avtal ska, för att vara giltiga, göras skriftligen och undertecknas av båda parter.

Instruktioner för behandling av personuppgifter för pastoratets räkning

Personuppgiftslagen

Leverantören ska iaktta nedanstående instruktioner vid behandling av personuppgifter. Med begreppen personuppgifter och behandling avses personuppgifter respektive behandling enligt definition i Personuppgiftslagen (1998:204) och för vilka pastoratet är personuppgiftsansvarig (Personuppgifter).

Leverantören ska iaktta Datainspektionens allmänna råd "Säkerhet för personuppgifter" (se Datainspektionens hemsida).

Säkerhetspolicy

Leverantören ska ha en uppdaterad och implementerad säkerhetspolicy som anger hur personuppgifter ska behandlas, till vem personal skall vända sig om ett intrång eller annan incident har inträffat, vilken personal som har behörighet till vilken typ av uppgifter m.m. Säkerhetspolicyen bör också behandla backup-rutiner, katastrofplaner m.m.

Personal

Anställda, konsulter och övriga medhjälpare hos leverantören ska av leverantören få information om behandling av personuppgifter.

Anställda, konsulter och övriga medhjälpare hos leverantören ska endast ha tillgång till personuppgifter som de behöver för att utföra sina arbetsuppgifter för fullgörande av ingångna avtal med pastoratet.

Behandling av personuppgifter

Leverantören ska upprätthålla en god säkerhet för personuppgifterna. Uppgifterna ska skyddas mot förstörelse genom olyckshändelse, samt mot icke begärda ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt om behandlingen innefattar överföring av uppgifterna i ett nätverk, och mot varje annat slag av otillåten behandling. Personuppgifterna får inte heller röjas till annan.

Lokaler

Lokalerna som leverantören nyttjar ska vara skyddade av adekvat larmutrustning för brand, vattenskada, intrång etc. Vidare ska det finnas rutiner samt utrustning i form av larm, spärrar, lås m.m. som reglerar tillträde till lokalerna.

Åtkomst

Leverantören ska ha ett behörighetskontrollsystem som förhindrar obehörig användning eller åtkomst av personuppgifter.

Viruskydd

Leverantören ska ha aktuella virusprogram. Uppdateringar ska installeras omgående och virusprogram ska finnas på samtliga arbetsstationer, stationära, bärbara och servrar.

Hantering av Personuppgifter

Behandlingar av personuppgifter måste kunna loggas och spåras.

Leverantören ska rätta, blockera, utplåna, ändra eller gallra personuppgifter enligt pastoratets instruktioner.

Leverantören ska inte bevara personuppgifter under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Anlitande av annat företag

Anlitar leverantören annat företag för hantering av personuppgifterna ska leverantören tillse att hantering enligt detta avtal med instruktioner iakttas även i det företaget.