Riskanalys och konsekvensbedömning

GDPR

Om riskanalys och konsekvensbedömning

Syftet med risk- och konsekvensbedömningen är att förebygga risker innan de uppkommer, ta fram rutiner och åtgärder för att hantera eventuella risker och kunna visa att vi följer dataskyddsförordningens krav.

Riskanalys och eventuell konsekvensbedömning dokumenteras och sparas i förbundets samarbetsrum för dataskyddsarbetet. Skicka underlaget till gdpr@seko.se.

När ska en riskanalys och konsekvensbedömning utföras?

A. innan vi påbörjar en (ny) personuppgiftsbehandling, exempelvis en ny medlemsförmån
B. om risken med en pågående behandling ändras, exempelvis byte av system eller leverantör

Initiera riskanalys och konsekvensbedömning i ett tidigt skede

Riskanalys och eventuell konsekvensbedömning bör initieras så snart som möjligt. Låt den vara en del av utvecklingsprocessen.

1. Riskanalys

Om en behandling sannolikt leder till en hög risk ska konsekvensbedömning genomföras (art. 35.1). Om en eller flera av nedanstående frågor besvarar med **JA** ska en konsekvensbedömning genomföras, se avsnitt 2.

Frågor för att bedöma risk med behandling	Ja	Nej
Omfattar behandlingen känsliga personuppgifter? *Fackliga personuppgifter är en känslig uppgift, se hela listan i art. 9.1.*		
Innebär behandlingen automatiskt beslutsfattande eller profilering? *System som fattar beslut utifrån uppgifter om individ.*		
Innebär behandlingen systematisk övervakning av allmän plats?		
Innebär behandlingen användande av ny teknik för bearbetning av personuppgifter?		

2. Konsekvensbedömning

Syftet med konsekvensbedömningen är att synliggöra eventuella risker för att möjliggöra för förbundet att vidta åtgärder innan ny behandling initieras och därmed skydda de registrerades personuppgifter i så stor utsträckning som möjligt.

Besvara nedanstående frågor innan beslut om nya behandlingar fattas.

Beskriv behandling:	Plats för beskrivning. *Exempel: Skicka medlemslista till företag X för ny medlemsförmån Y.*
Syfte med behandling:	Plats för beskrivning. *Se Dataskyddspolicy där ändamål för förbundets behandlingar finns listade, vid nytt ändamål måste även Dataskyddspolicy justeras.*
Laglig grund eller berättigat intresse	Plats för beskrivning.
Proportionalitetsbedömning	Plats för bedömning gällande om behandlingen står i proportion till syftet med behandlingen.
Bedömning av risker för de registrerades rättigheter	Plats för bedömning. *Se Dataskyddspolicy.*
Åtgärder för att hantera risker	Plats för beskrivning. *Exempel: Autentisering, kryptering, rutiner och tydlig information till systemets användare, logg över arbete i system, stöd för säkerhetskopiering, pseudonymisering av personuppgifter, öppen redovisning av personuppgifternas syfte och behandling, möjlighet för den registrerade att övervaka uppgiftsbehandlingen, minska antalet personer som har tillgång till uppgifterna, begränsa sökbegreppen så att det inte går att söka på känsliga personuppgifter, införa automatisk borttagning av personuppgifter som inte längre ska behandlas, utforma it-system så att inte fler personuppgifter än nödvändigt behandlas*
Synpunkter från dataskyddsombud	Plats för beskrivning. *Involvera alltid förbundets dataskyddsombud vid svåra bedömningar.*
Synpunkter från de registrerade	Plats för beskrivning. *Om och när det är lämpligt.*

Om möjligt och lämpligt kan konsekvensbedömningen publiceras för berörda för ökad transparens.

3. Förhandssamråd

Om konsekvensbedömningen visar att den planerade behandlingen medför höga risker som inte kan minskas genom interna åtgärder, är vi skyldiga att samråda med Datainspektionen innan vi går vidare.

Datainspektionen har att återkoppla inom åtta veckor och lämnar då eventuella råd eller förbjuder oss att gå vidare med den planerade behandlingen.

Kontakta vårt dataskyddsombud och delge vår konsekvensbedömning för att gå vidare med detta.

4. Dokumentation av bedömningar

Alla riskanalyser och konsekvensbedömningar skickas till sakkunnig som säkerställer att vi samlar all dokumentation av dessa bedömningar.

Kontakt: gdpr@seko.se