Gäller för: Västra Götalandsregionen
Innehållsansvar: Paulina Oscarsson, (pauos1), Regionutvecklare
Godkänd av: Johan Flarup, (johfl), Direktör
Giltig från: 2024-10-03
Giltig till: 2028-12-31

Konsekvensbedömning avseende dataskydd

Regional rutin 2024–2028

Ledningssystem för informationssäkerhet och dataskydd

Rubrik: Konsekvensbedömning avseende dataskydd - Regional rutin 2024-2028
Dokument-ID: RS10162-1596316381-259
Version: 1.0

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

Sammanfattning

Mål: Att skydda människors fri- och rättigheter och minimera riskerna vid behandling av personuppgifter.

Enligt artikel 35 i dataskyddsförordningen ska personuppgiftsansvarig före personuppgiftsbehandlingen påbörjas genomföra en konsekvensbedömning avseende dataskydd (nedan kallad konsekvensbedömning).

Syftet med en konsekvensbedömning är att

- ta reda på vilka risker som finns med att behandla personuppgifter
- ta fram rutiner och åtgärder för att bemöta dessa risker
- visa att man uppfyller dataskyddsförordningens krav.

Innan konsekvensbedömningen utförs ska en tröskelanalys avseende dataskydd göras (nedan kallad tröskelanalys). Om tröskelanalysens resultat visar på att det föreligger hög risk för de registrerades friheter och rättigheter ska en konsekvensbedömning göras.

Konsekvensbedömning ska göras

- innan en personuppgiftsbehandling påbörjas och tröskelanalysen visat att konsekvensbedömning ska göras
- om risken med en pågående personuppgiftsbehandling ändras
- för pågående personuppgiftsbehandlingar med hög risk för de registrerades friheter och rättigheter om det inte har gjorts tidigare.

Regional rutin för konsekvensbedömning avseende dataskydd är styrande för alla förvaltningar och bolag i Västra Götalandsregionen och ingår som en del i ledningssystemet för informationssäkerhet och dataskydd (LISD).

Rutinen fastställer modell för konsekvensbedömning som ska användas i Västra Götalandsregionen. Konsekvensbedömningen ska dokumenteras i regional mall och därefter hanteras enligt myndighetens informationshanteringsplan.

1. Ansvar och roller

1.1 Informationsägare

Informationsägaren ansvarar för att konsekvensbedömning genomförs om resultatet från tröskelanalysen visat att en konsekvensbedömning ska göras.

Informationsägaren ansvarar för att säkerställa implementation och efterlevnad av de krav och säkerhetsåtgärder som framkommer i konsekvensbedömningen.

Informationsägaren ska ge dataskyddsombudet möjlighet att delta på konsekvensbedömningen. Efter genomförd konsekvensbedömning ansvarar informationsägaren för att inhämta dataskyddsombudets synpunkter på genomförd konsekvensbedömning.

De interna relationerna mellan informationsägare och ägare av IS/IT-tjänst ska, när det gäller informationssäkerhet och dataskydd, utgå från informationsägarens ansvar för informationen.

1.2 Regional processägare

Vid regiongemensamma processer företräds informationsägare av regional processägare som ansvarar för att tröskelanalys avseende dataskydd genomförs för de personuppgiftsbehandlingar som utförs inom dennes process. I företrädarskapet ansvarar regional processägare för att respektive informationsägares intresse tas tillvara.

1.3 Projektägare

Informationssäkerhet och dataskydd ska vara en del av projekt. Projektägare ska inledningsvis i ett projekt säkerställa att tröskelanalys genomförts eller se till att det sker, för att kunna identifiera de säkerhetsåtgärder som personuppgiftsbehandlingen kräver. Projektägare ska i ett tidigt skede identifiera vem som är informationsägare. Då projekt avslutas och övergår i ordinarie linjeverksamhet är det informationsägare, eller regional processägare vid regiongemensam process, som övertar ansvaret för dataskyddsarbetet.

1.4 Ägare av IS/IT-tjänst

Respektive IS/IT-tjänst ska ha en ägare. Denne ansvarar för tekniska säkerhetsåtgärder i IS/IT-tjänsten, vilket innebär att införa, förvalta och följa upp utifrån den regionala processägarens alternativt informationsägarens krav på skydd för informationstillgångarna. Det är av största vikt att ägaren har god kännedom om vilken information som behandlas i IS/IT-tjänsten och hur dessa är klassade samt vilka krav som finns på hanteringen av personuppgifter som förekommer i IS/IT-tjänsten

1.5 Dataskyddssamordnare

Dataskyddssamordnaren är ett stöd till verksamheten i dess dataskyddsarbete och verkar för en regiongemensam tillämpning av styrdokument och regelverk i den egna verksamheten.

1.6 Personuppgiftsansvarig

Varje politisk nämnd eller styrelse är ansvarig för personuppgifterna som behandlas i deras verksamhet. Dataskyddsarbetet utförs i praktiken av rollerna ovan.

1.7 Dataskyddsombud

Dataskyddsombudet är en oberoende roll vars uppgift är att övervaka personuppgiftsansvarigs efterlevnad av dataskyddsförordningen. Dataskyddsombudet kan på begäran ge råd vid behandling av personuppgifter och ska alltid ges möjlighet att delta vid konsekvensbedömningen. Efter att konsekvensbedömningen genomförts ska dataskyddsombudets synpunkter inhämtas.

2. När ska en konsekvensbedömning genomföras?

En konsekvensbedömning ska genomföras när tröskelanalysen visat att det föreligger hög risk för de registrerades fri- och rättigheter. Se ”Tröskelanalys avseende dataskydd – regional rutin 2024–2028” för mer information.

3. Genomförande

I konsekvensbedömningen ingår att:

- beskriva personuppgiftsbehandlingen
- bedöma behov och proportionalitet
- identifiera åtgärder som hanterar riskerna för de registrerades rättigheter och friheter.

Vid genomförande av konsekvensbedömning ska alltid dataskyddsombudet ges möjlighet att delta.

Konsekvensbedömningen ska dokumenteras i regional mall för konsekvensbedömning avseende dataskydd.

Efter genomförd konsekvensbedömning ska dataskyddsombudets synpunkter inhämtas.

4. Samråd med tillsynsmyndighet

Om riskerna för de registrerades fri- och rättigheter förblir höga även efter genomförande av föreslagna säkerhetsåtgärder, eller på grund av brist av säkerhetsåtgärder, ska samråd med tillsynsmyndigheten Integritetskyddsmyndigheten (IMY) begäras. Det är informationsägaren som ansvarar för att ett samråd begärs.

Relaterade dokument

Termbank för informationssäkerhet - nationell terminologi för informations- och cybersäkerhetsområdet
https://termbanken.informationssakerhet.se/

Definitioner i dataskyddsförordningen
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/dataskyddsforordningen-i-fulltext/#A4

Policy - säkerhet och beredskap i Västra Götalandsregionen (dnr RS 2018-00129)

Informationssäkerhet och dataskydd - Regional riktlinje 2023–2027 (dnr RS 2023-02811)

Informationsklassning – Regional rutin 2024–2028 (Dokument-ID RS10162-1596316381-102)

Riskhantering för informationssäkerhet – Regional rutin 2024–2028 (Dokument-ID RS10162-1596316381-118)

Tröskelanalys avseende dataskydd – Regional rutin 2024–2028

Konsekvensbedömning avseende dataskydd – Regional mall

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Paulina Oscarsson, (pauos1), Regionutvecklare

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-259

Version: 1.0

Giltig från: 2024-10-03

Giltig till: 2028-12-31