Rutin

Gäller för: Västra Götalandsregionen
Innehållsansvar: Paulina Oscarsson, (pauos1), Strateg
Granskad av: Anders Andersson, (andan18), Enhetschef
Godkänd av: Mariana Vikström, (marvi36), Direktör

Giltig från: 2026-09-11
Giltig till: 2030-12-31

Personuppgifts-incidenter

Regional rutin

Ledningssystem för informationssäkerhet och dataskydd

Rubrik: Personuppgiftsincidenter - Regional rutin
Dokument-ID: RS10162-1596316381-432
Version: 1.0

VÄSTRA GÖTALANDSREGIONEN

Innehåll

Inledning

Mål: Process, organisation och resurser ska finnas för att upptäcka, utreda, dokumentera, åtgärda och rapportera personuppgiftsincidenter på ett effektivt sätt. Rutinen ska säkerställa att skyldigheter enligt artikel 33 och 34 GDPR fullgörs inom föreskrivna tidsfrister samt att samtliga incidenter dokumenteras enligt artikel 33.5 GDPR.

Enligt artikel 33 i dataskyddsförordningen är personuppgiftsansvariga skyldiga att dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Anmälan till Integritetsskyddsmyndigheten (IMY) ska ske när incidenten medför risk för registrerades fri- och rättigheter. Information till registrerade ska lämnas när incidenten sannolikt medför hög risk för registrerades fri- och rättigheter.

Regional rutin för personuppgiftsincidenter är styrande för alla förvaltningar och bolag i Västra Götalandsregionen och ingår som en del i ledningssystemet för informationssäkerhet och dataskydd (LISD). För de bolag som inte använder avvikelsehanteringssystemet MedControl PRO ska dokumentation av rapportering och hantering av personuppgiftsincidenter ske på likvärdigt sätt i annat system som bolagen finner lämpliga.

Termer och begrepp

Personuppgiftsincident

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Den kan också leda till ett obehörigt röjande av eller obehörig åtkomst till personuppgifter. Det spelar ingen roll

om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

Personuppgift

Med personuppgifter menas varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Personuppgiftsbehandling

Personuppgiftsbehandling innebär en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Personuppgiftsansvarig

I Västra Götalandsregionen är den nämnd eller bolag, som ensamt eller tillsammans med andra bestämmer ändamålen (varför) och medlen (hur) för behandlingen av personuppgifter, personuppgiftsansvarig.

Registrerad

Den identifierade eller identifierbara fysiska person vars personuppgifter behandlas.

Personuppgiftsbiträde

Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Registrerades friheter och rättigheter

Skydd för sin data och integritet, yttrandefrihet, tankefrihet, fri rörlighet, förbud mot diskriminering samt rätt till frihet, samvete och religion.

Ansvar och roller

Medarbetare

Varje medarbetare som upptäcker en personuppgiftsincident ska omgående rapportera detta i organisationens avvikelsehanteringssystem.

Dataskyddssamordnare

Dataskyddssamordnaren är ett stöd till verksamheten i dess dataskyddsarbete och verkar för en regiongemensam tillämpning av interna styrdokument och regelverk i den egna verksamheten. Varje förvaltning ska ha en utsedd dataskyddsamordnare.

Incidentsansvarig

Varje förvaltning ska utse incidentansvarig. Incidentansvarig ansvarar för samordning av utredning, riskbedömning, beslut om anmälan till IMY samt samordning av information till registrerade. Rollen kan bemannas av en grupp med kompetens inom informationssäkerhet, dataskydd och verksamhet.

Dataskyddsombud

Varje personuppgiftsansvarig ska ha ett dataskyddsombud. Dataskyddsombudet ska involveras vid bedömning av incidenter som kan medföra risk eller hög risk för registrerade samt ges möjlighet att lämna råd kring anmälan till IMY och information till registrerade.

Informationsägare

Informationsägaren ansvarar för att säkerställa implementation och efterlevnad av säkerhetsåtgärder utifrån krav på skydd för informationstillgångarna.

Ägare IS/IT-tjänst

Ägare av IS/IT-tjänst ska delta i utredning av personuppgiftsincident genom att bidra med teknisk analys, orsaksutredning, konsekvensbedömning och vidta åtgärder som eliminerar eller minimerar risker mot skyddet för personuppgifter.

Rapportera och hantera personuppgiftsincident i avvikelsehanteringssystem

Varje medarbetare som upptäcker en personuppgiftsincident ska omgående rapportera personuppgiftsincidenten i avvikelsehanteringssystemet MedControl PRO. Stöd för rapportering finns på Insidan – System A-Ö – MedControl PRO.

Stöd för hantering av ärendet i MedControl PRO och ”steg för steg”-guide finns på Insidan – System A-Ö – MedControl PRO.

Bedömning och hantering av personuppgiftsincident

Dataskyddsombudet bör involveras så tidigt som möjligt vid bedömning och hantering av personuppgiftsincidenter för att kunna ge stöd vid bedömning och råd till hantering av personuppgiftsincident.

Typ av personuppgiftsincident

Samordningsansvarig (roll i MedControl PRO – utgörs av linjechef) bedömer om ärendet handlar om någon eller några av följande typer av personuppgiftsincident:

- konfidentialitetsincident (obehörigt röjande eller åtkomst)
- integritetsincident (obehörig ändring eller förvanskning)

- tillgänglighetsincident (förlust, förstöring eller otillgänglighet).

En incident kan omfatta flera typer samtidigt. Incidentansvarig kan justera eller komplettera kategori vid behov.

Stöd för bedömning av allvarlighetsgrad

Incidentansvarig får ärendet i MedControl PRO efter att samordningsansvarig angett typ av personuppgiftsincident och skickat ärendet vidare till orsaksutredare. Vid incidentansvarigs bedömning av allvarlighetsgrad ska följande faktorer analyseras:

- typ av incident
- uppgifternas känslighet
- mängd personuppgifter
- antal registrerade
- registrerades sårbarhet
- identifierbarhet
- möjliga konsekvenser
- sannolikhet att skada uppstår.

Vid bedömning av personuppgiftsincidenten ska IMY:s vägledning vid hantering av personuppgiftsincidenter användas. Vägledningen finns på IMY:s hemsida www.imy.se under Startsida – Verksamhet – Dataskydd – Det här gäller enligt dataskyddsförordningen – Personuppgiftsincidenter – Hantering av personuppgiftsincidenter.

Bedömningen ska dokumenteras i ärendet i MedControl PRO. Bedömning av personuppgiftsincidenten behöver göras fortlöpande om nya uppgifter tillkommer i ärendet.

Anmälan till IMY

Incidentansvarig bedömer om incidenten är ska anmälan till IMY. Anmälan ska ske skyndsamt, senast 72 timmar efter att den personuppgiftsansvarige fått kännedom om incidenten. Om tidsfristen överskrids ska orsaken dokumenteras. Anmälan kan

lämnas preliminärt och därefter kompletteras enligt artikel 33.4 GDPR.

Om personuppgiftsincidenten inte bedöms som anmälningspliktig ska skälen för detta dokumenteras i ärendet i MedControl PRO.

Bedömning av risk för registrerades fri- och rättigheter

Vid bedömning om det föreligger risk för de registrerades fri- och rättigheter ska vikt läggas på om incidenten är avsiktlig och inträffat på grund av ont uppsåt, till exempel att organisationen utsatts för ett intrång, stöld eller kopiering av hårdvara eller annan informationsbärare (dokument, fotografering av uppgifter av inneliggande patienter). Det indikerar att informationen är tänkt att användas för brottsliga handlingar. Vid ställningstagande om det föreligger en hög risk för de registrerade behöver följande frågor ställas:

- Hur allvarliga kan konsekvenserna bli?
- Hur sannolikt är det att enskilda personer drabbas?

Ställningstagande och motivering ska dokumenteras i ärendet i MedControl PRO av incidentansvarig.

Information till registrerade

Om en personuppgiftsincident sannolikt leder till en hög risk för de registrerades rättigheter och friheter ska de registrerade informeras direkt och utan onödigt dröjsmål.

Incidentansvarig ansvarar för att information tas fram och lämnas till de registrerade när kriterierna enligt artikel 34 är uppfyllda. Syftet med informationen är att ge registrerade möjlighet att skydda sig från skada, exempelvis genom att byta lösenord, spärra betalmedel eller vidta andra skyddsåtgärder.

Hur informationen ska ges

Beroende på incidentens omfattning och karaktär behöver informationen ges på olika sätt. Dataskyddsombudet kan ge råd om lämplig informationsväg.

Om det är känt vilka enskilda registrerade som drabbats och det finns kontaktuppgifter som möjliggör utskick i form av sms eller e-post ska information skickas direkt till de enskilda registrerade.

Om incidenten inneburit att uppgifter som möjliggör identifiering eller lokalisering av person med skyddade personuppgifter ska personen/personerna kontaktas personligen om det är möjligt och ges information om vad som inträffat.

Innehåll information till registrerade

Vad som har hänt

Beskrivning av vad som har hänt, hur det har skett och vilken typ av säkerhetsbrist eller oönskad händelse det rör sig om.

Kontaktuppgifter

Kontaktuppgifter till incidentansvarig, dataskyddssamordnare eller dataskyddsombud som de registrerade kan vända sig till vid frågor.

Möjliga konsekvenser

Beskrivning av risker för den registrerade.

Rekommenderade skyddsåtgärder

Åtgärder den registrerade själv kan vidta.

Vidtagna åtgärder

Åtgärder som organisationen (VGR) redan genomfört eller planerar att genomföra.

Regional samordning av hantering av personuppgiftsincident

Vid incidenter som påverkar flera förvaltningar eller gemensamma system ska regional samordning ske genom koncernstab säkerhet och civil beredskap. Ansvarsfördelning, informationsutbyte, eventuell IMY-anmälan och kommunikation mellan berörda nämnder ska dokumenteras. Regional samordning omfattar även

incidenter som uppstår i VGR:s egna gemensamma system och processer, inte endast hos personuppgiftsbiträden.

När Västra Götalandsregionen är personuppgiftsbiträde

När nämnd i Västra Götalandsregionen levererar IS/IT-tjänster till personuppgiftsansvariga utanför den egna organisationen, till exempel privata vårdgivare eller kommuner, agerar den aktuella nämnden personuppgiftsbiträde. Vid inträffad säkerhetshändelse ska ägare av IS/IT-tjänst underrätta personuppgiftsansvarig utan onödigt dröjsmål. Information till personuppgiftsansvarig ska minst innehålla:

- tidpunkt för incidenten
- typ av incident
- berörda uppgifter
- preliminär konsekvensbedömning
- vidtagna eller planerade åtgärder
- kontaktperson för fortsatt hantering.

Uppföljning och lärande

Incidentsansvarig ansvarar för att personuppgiftsincidenter sammanställs och följs upp regelbundet. Uppföljningen ska omfatta statistik, trendanalyser, återkommande incidenttyper, grundorsaker och genomförda åtgärder. Resultatet ska återföras till verksamheterna inom den egna förvaltningen och integreras i det systematiska informationssäkerhetsarbetet.

Relaterade dokument

Policy för säkerhet och beredskap 2025 -2029

Informationssäkerhet och dataskydd - Regional riktlinje 2023 - 2027

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

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Paulina Oscarsson, (pauos1), Strateg

Granskad av: Anders Andersson, (andan18), Enhetschef

Godkänd av: Mariana Vikström, (marvi36), Direktör

Dokument-ID: RS10162-1596316381-432

Version: 1.0

Giltig från: 2026-09-11

Giltig till: 2030-12-31