Beslutad av: Eva Arrdal, direktör på Koncernkontorets stab för utförarstyrning och samordning
Beslutsdatum: 2018-05-25, rev 2018-06-01
Diarienummer: RS-2018-02985
Giltighet: från 2018-05-25

Rutin

Rapportering vid personuppgiftsincidenter

Giltighet: Förvaltningar och bolag i VGR tillämpar denna rutin

Dokumentet ersätter: Ny rutin kopplad till krav enligt Dataskyddsförordningen (GDPR)

Innehållsansvar: Enhet säkerhet och beredskap (ESB) på Koncernkontorets stab för utförarstyrning och samordning

VÄSTRA GÖTALANDSREGIONEN

Innehåll

Sammanfattning

Från den 25 maj 2018 gäller Dataskyddförordningen dvs EU-förordningen General Data Protection Regulation (GDPR) som gemensam lagstiftning för alla länder i EU.
Med GDPR följer en skyldighet att rapportera personuppgiftsincidenter där Personuppgiftsansvarig (PUA) har ett ansvar att utreda och anmäla personuppgiftsincidenter enligt särskild ordning till Datainspektionen. Den här rutinen kompletterar ordinarie avvikelsehanteringsrutin som finns inom VGR, och ger vägledning när det gäller personuppgiftsincidenter.
Rutinen ska användas av alla myndigheter och bolag inom VGR vid händelse av personuppgiftsincidenter.

1. Allmänt

GDPR innebär ett förstärkt integritetsskydd för den enskildes rätt till sina personuppgifter, och en nyhet som följer med GDPR är att det är extra viktigt för PUA att anmäla personuppgiftsincidenter skyndsamt.

2. PUA ska utse en incidentansvarig

PUA ska utse en incidentansvarig som ska säkerställa att varje personuppgiftsincident omhändertas på rätt sätt. Alla uppgifter eller misstankar om oönskade eller oplanerade händelser som rör personuppgifter ska inte anmälas till Datainspektionen.
Det är därför väsentligt att incidentansvarig gör en kortare intern undersökning för att kunna avgöra om det verkligen rör sig om en personuppgiftsincident.

3. Rapportering av personuppgiftsincidenter

Rapportering av personuppgiftsincidenter ska ske i MedControl. För de bolag som inte använder sig av MedControl ska motsvarande handläggning av personuppgiftsincidenter säkerställas i det avvikelsehanteringssystem som man använder sig av.
För användning av MedControl vid personuppgiftsincidenter så hänvisas till följande instruktion:

Lathund för handläggning av personuppgiftsincident

4. När ska de registrerade informeras?

Enligt förordningen ska de registrerade direkt och utan onödigt dröjsmål informeras om en personuppgiftsincident sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Bedömningen ska göras utifrån både allvarligheten av den potentiella eller faktiska påverkan på personer som ett resultat av en personuppgiftsincident kan ha och utifrån sannolikheten för att detta inträffar.
Information till de registrerade i anledning av en personuppgiftsincident behöver inte alltid göras. Den bedömningen får ske från fall till fall.

Följande frågeställningar är en utgångspunkt för bedömningen.

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

Om personuppgiftsincidenten är allvarlig är risken högre. Om sannolikheten för konsekvenser är stor är risken också högre.

När risken är hög måste de personer som har drabbats informeras, särskilt om det finns ett behov av att mildra en omedelbar risk för skador. En av huvudorsakerna är att du ska kunna hjälpa dem att vidta åtgärder för att skydda sig mot effekterna av en personuppgiftsincident.

På Datainspektionens hemsida, När ska vi informera de registrerade? finns exempel på olika fall av personuppgiftsincidenter. Exempelsamlingen kommer att uppdateras löpande.

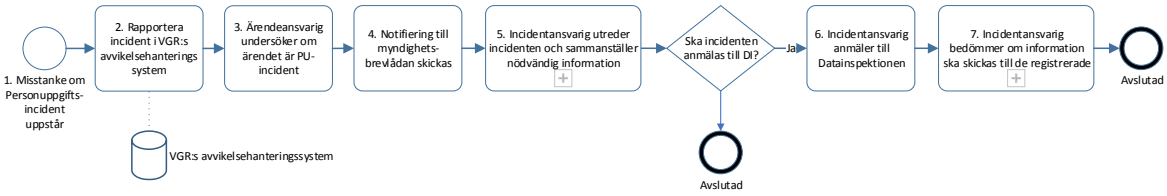
5. Anmälan till Datainspektionen

Den incidentansvarige ska skyndsamt och om så är möjligt inte senare än 72 timmar efter att ha fått vetskap om en personuppgiftsincident göra anmälan till Datainspektionen. Om anmälan inte kan göras inom denna tid ska anmälan åtföljas av en motivering till förseningen.
Om det är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter, behöver ingen anmälan göras.
Vid en anmälan så ska de blanketter som finns hos Datainspektionen användas och postas som rekommenderat brev till följande adress:

Datainspektionen
Box 8114
104 20 Stockholm

6. Process för hantering av personuppgiftsincidenter

Följande är en illustration av hanteringsordning steg för steg vid en personuppgiftsincident.



1. Misstanke om personuppgiftsincident uppstår.
2. Personuppgiftsincident rapporteras i MedControl av medarbetare som upptäckt incidenten.
3. Ärendeansvarig (dvs linjechef eller annan utsedd medarbetare) bedömer typ av händelse som kan vara:
   a) Personuppgifter som blivit förstörda.
   b) Personuppgifter som gått förlorade på annat sätt.
   c) Personuppgifter som kommit i orätta händer.
4. Notifikation går till den officiella myndighetsbrevlådan vilket innebär att:
   a) Person tar emot och skickar ärendet vidare till incidentansvarig inom respektive myndighet.
5. Incidentansvarig undersöker och utreder incidenten.
   a) Undersöker omfattning, art och konsekvenser av incidenten.
   b) Bedömer om anmälan till Datainspektionen krävs.
6. Incidentansvarig anmäler incidenten till Datainspektionen – inom 72 timmar om möjligt.
7. Eventuell rapport och information till de registrerade dvs de personer som drabbats av personuppgiftsincidenten.

7. Beredning och beslut

Rutinen har arbetats fram av arbetsgruppen för GDPR och förankrats i styrgrupp för GDPR. I utformning av rutinen har IT-specialist Ekaterina Zuckermann, VGR IT, MedControl-specialisten Goran Barasin, koncernavdelning ärendesamordning och kansli, arkivchef Charlotta Tengbert, SU, regionutvecklare Glenn Grimhage, ESB och processledare för informationssäkerhet Jan S Svensson, ESB, medverkat. Rutinen har beslutats av Eva Arrdal, direktör på Koncernkontoret, koncernstab utförarstyrning och samordning efter föredragning av Maria Fast, enhetschef för ESB.