Hantering av personuppgiftsincidenter Avesta kommunkoncern - Rutin

Dokumenttyp:	Rutin
Diarienummer:	KK 2021-000076 005
Sammanfattning:	Rutin för hantering av personuppgiftsincidenter
Fastställd av/datum:	t.f. kommundirektör 2021-03-19
Giltighetstid:	Tills vidare
Gäller för:	Avesta kommunkoncern
Reviderad:	
Granskad:	
Dokumentansvarig:	Kommunkansli/Kommunsekreterare
Webbansvarig:	Controller

Rutinbeskrivning för hantering av personuppgiftsincidenter

Den personuppgiftsansvarige ska ha rutiner för att dokumentera alla personuppgiftsincidenter och även en beskrivning av omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för Integritetsskyddsmyndigheten att kontrollera den personuppgiftsansvariges hantering av personuppgiftsincidenter.

Varje anställd har ansvar att hantera incidenter som upptäcks i arbetsuppgifter som den utför. Rutinbeskrivningen ska användas av alla myndigheter inom Avesta kommun och av de kommunala bolagen vid händelse av personuppgiftsincidenter.

1.Vad är en personuppgiftsincident?

En personuppgiftsincident är en händelse som rör personuppgifter. Incidenten kan till exempel handla om att personuppgifter har blivit förstörda eller ändrade, gått förlorade eller kommit i orätta händer. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. Det kan exempelvis vara fråga om uppgifter som omfattas av sekretess har lämnats ut (t.ex. via e-post) till fel person eller att personuppgifter i ett verksamhetssystem felaktigt raderats eller försvunnit på grund av ett tekniskt fel.

En vanlig typ av personuppgiftsincident är att ett brev eller ett e-postmeddelande av misstag skickas till en person som inte är behörig att ta emot uppgifterna.

Om personuppgifter skickas internt med e-post i strid med kommunala riktlinjer för IT-säkerhet har en säkerhetsincident inträffat. En sådan säkerhetsincident blir dock bara personuppgiftsincident om någon obehörig tagit emot uppgifterna i e-postmeddelandet. Finns osäkerhet kring om en händelse utgör en personuppgiftsincident, ta kontakt med dataskyddsombudet, dso@qbase.se.

Mer information om definitionen av en personuppgiftsincident finner du på Anmäl personuppgiftsincidenter - Integritetsskyddsmyndigheten (imy.se).

2.Ansvar

Samtliga förtroendevalda och medarbetare i kommunen och de kommunala bolagen har en skyldighet att agera i enlighet med denna rutinbeskrivning om det finns en misstanke om att en personuppgiftsincident har inträffat. Ansvariga chefer har en skyldighet att informera sina medarbetare om offentlighets- och sekretesslagen (2009:400), dataskyddsförordningen och annan tillämplig lagstiftning inom verksamhetsområdet. De ska vidare se till att medarbetarna känner till innehållet i denna rutinbeskrivning. Cheferna ska vidare förebygga personuppgiftsincidenter och vidta åtgärder efter inträffad incident.

Den personuppgiftsansvarige, det vill säga ansvarig nämnd eller ansvarigt bolag, har i vissa fall en skyldighet att anmäla personuppgiftsincidenten till Integritetsskyddsmyndigheten och informera den drabbade individen om händelsen.

Dataskyddsombudet har till uppdrag att bistå med enklare rådgivning vid handläggningen av en personuppgiftsincident. I de flesta fall kommer enklare rådgivning vara tillräcklig för att hantera incidenten. Efter en särskild begäran om biträde vid utredning av misstänkt personuppgiftsincident ställd till dso@qbase.se utvidgas dataskyddsombudets uppdrag till att i det enskilda fallet bistå med mer kvalificerad rådgivning, bedömningar och annat stöd för hantering av personuppgiftsincidenten.

3.Anmälan och dokumentering

Om en personuppgiftsincident har inträffat ska den i vissa fall anmälas till Integritetsskyddsmyndigheten inom 72 timmar från det att personuppgiftsincidenten upptäckts. I vissa fall ska även den person som drabbats av incidenten få information om vad som har hänt och hur skadan kan minimeras. Någon anmälan behöver inte göras om det är osannolikt att incidenten leder till några risker för enskildas fri- och rättigheter.

En personuppgiftsincident som består i att någon av misstag skickat ett internt meddelande med personuppgifter till någon inom kommunen eller ett kommunalt bolag som inte är behörig att ta

emot uppgifterna är i regel inte anmälningspliktig. Det beror på att mottagaren då oftast är ”betrodd” att inte vidta ytterligare åtgärder med uppgifterna utan snabbt skicka tillbaka dessa. Det är då osannolikt att personuppgiftsincidenten medför en risk för enskildas fri- och rättigheter. En icke anmälningspliktig personuppgiftsincident måste ändå dokumenteras.

Den som upptäcker en personuppgiftsincident ska fylla i den bifogade mallen för intern rapportering av personuppgifter. Personuppgiftshandläggaren eller den som handlägger förvaltningens/bolagets avvikelserapporteringar lägger sedan in den ifyllda mallen i det särskilda diariet för dataskyddsfrågor. Finns osäkerhet kring om en händelse utgör en personuppgiftsincident, ta kontakt med dataskyddsombudet, dso@qbase.se. Mallen för intern rapportering fylls i av den som upptäckt incidenten och lämnas sedan omgående vidare till förvaltningschef/resultatenhetschef eller VD för verksamheten. Den chef eller VD som erhållit informationen ska omgående göra en bedömning av om händelsen kan utgöra en personuppgiftsincident och om den i så fall ska anmälas till Integritetsskyddsmyndigheten. Dataskyddsombudet bör normalt kontaktas för stöd vid denna bedömning.

Om personuppgiftsincidenten är sådan att den ska anmälas till Integritetsskyddsmyndigheten fattar förvaltningschef/enhetschef eller VD för verksamheten beslut om anmälan. Verksamhetens personuppgiftshandläggare eller den som handlägger verksamhetens avvikelserapporteringar expedierar och diarieför anmälan. Om den befattningshavaren inte är i tjänst när beslutet fattas utser beslutande chef en ersättare så att anmälan kan expedieras omgående. Befattningshavaren eller ersättaren ska informera berörd chef och dataskyddsombudet när en anmälan expedierats till Integritetsskyddsmyndigheten.

Anmälan till Integritetsskyddsmyndigheten sker genom med hjälp av den blankett som Integritetsskyddsmyndigheten utarbetat och på det sätt som Integritetsskyddsmyndigheten föreskriver på sin webbplats Anmälan av personuppgiftsincident | Integritetsskyddsmyndigheten (imy.se). I förekommande fall ska även den drabbade informeras om händelsen enligt dataskyddsförordningens bestämmelser och vilka åtgärder som kan behöva vidtas. I förekommande fall ska även personuppgiftsbiträdet informeras om incidenten.

Oavsett om en personuppgiftsincident är anmälningspliktig eller inte ska den alltid diarieföras av personuppgiftshandläggaren eller den som handlägger verksamhetens avvikelserapporteringar för den ansvariga verksamheten. Diarieföring sker i det särskilda diariet för dataskyddsfrågor. Om en personuppgiftsincident anmälts ska inkommande handlingar i ärendet från Integritetsskyddsmyndigheten diarieföras av personuppgiftshandläggaren eller den som handlägger verksamhetens avvikelserapporteringar i samma diarium som anmälan.

4.När ska de registrerade informeras?

Enligt dataskyddsförordningen 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 Integritetsskyddsmyndighetens webbplats, När ska vi informera de registrerade? - Integritetsskyddsmyndigheten (imy.se), finns exempel på olika fall av personuppgiftsincidenter. Exempelsamlingen uppdateras löpande.

5.Uppföljning och efterföljande åtgärder

Ansvarig chef tillser att personuppgiftsincidenter följs upp och att behövliga åtgärder vidtas. Uppföljningen sker i samråd med personuppgiftshandläggaren eller den som handlägger verksamhetens avvikelserapporteringar och dataskyddsombudet. Dataskyddsombudet rapporterar till ansvarig nämnd minst en gång per år.

6.Ytterligare information

Information om personuppgiftsincidenter finns på Integritetsskyddsmyndighetens webbplats. Därutöver kan personuppgiftshandläggare och dataskyddsombud ge information om GDPR och hur denna rutin ska tillämpas. Den rättsliga regleringen angående personuppgiftsincidenter finns i GDPR, artikel 33–34 och skäl 85–88. Se vidare Europeiska dataskyddsstyrelsens (EDPB) riktlinjer om anmälan av personuppgiftsincidenter.

7. Intern rapportering av personuppgiftsincident

Nedan finner du Avesta Kommuns mall för intern rapportering av personuppgiftsincidenter. Mallen fylls i av den som upptäckt incidenten och lämnas sedan omgående vidare till förvaltningschef/resultatenhetschef eller VD för verksamheten. Den chef eller VD som erhållit informationen ska omgående göra en bedömning av om händelsen kan utgöra en personuppgiftsincident och om den i så fall ska anmälas till Integritetsskyddsmyndigheten. Dataskyddsombudet bör normalt kontaktas för stöd vid denna bedömning.

Mall för intern rapportering av en personuppgiftsincident

Fyll i nedanstående fält så noggrant som möjligt och e-posta omgående dokumentet till verksamhetens chef/VD med kopia till dso@qbase.se.

Namn:	Avdelning:
Ansvarig chef:	Telefonnummer:

Personuppgiftsincidenten

När inträffade incidenten?
När upptäcktes incidenten?
Vad har hänt vid incidenten? Markera alla alternativ som gäller ☐ **Obehörigt röjande:** Personuppgifter har spridit på ett felaktigt sätt ☐ **Obehörig åtkomst:** Någon inom eller utanför organisationen har tagit del av information som den saknar behörighet till ☐ **Förslut:** Information har gått förlorad på något sätt, till exempel genom att en dator eller mobil blivit stulen ☐ **Förstöring:** Någon eller något har förstört information, till exempel genom att en dator har gått sönder ☐ **Ändring:** Personuppgifter har ändrats på något sätt
Lämna en kort beskrivning av incidenten.
Hur upptäcktes incidenten? ☐ **Genom en automatiserad process:** tekniska säkerhetsåtgärder ☐ **Genom organisatoriska rutiner:** till exempel en återkommande kontroll ☐ **En anställd informerade oss**

- ☐ **Vårt personuppgiftsbiträde informerade oss**
- ☐ **En utomstående eller registrerad informerade oss**
- ☐ **Annat:**

Varför inträffade incidenten enligt er uppfattning?

- ☐ **Mänskliga faktorn: fel i det enskilda fallet**
- ☐ **Brist i organisatoriska rutiner eller processer:** systematiskt fel
- ☐ **Tekniskt fel:** till exempel fel i mjukvara, programinställningar
- ☐ **Medvetet angrepp från någon i organisationen**
- ☐ **Antagonistiskt angrepp:** angrepp utifrån
- ☐ **Okänd orsak**
- ☐ **Övrigt:**

Inträffade incidenten inom ett område där personuppgifterna hanteras av ett anlitat personuppgiftsbiträde?

- ☐ **Ja**
- ☐ **Nej**

Om ja, ange vem som utgör personuppgiftsbiträdet?

Uppgifter om de registrerade

Hur många registrerade har påverkats?

Vilka grupper tillhör de registrerade? Till exempel elever, fackliga företrädare, förtroendevalda osv.

Vilka sorts personuppgifter har incidenten drabbat?

- ☐ **Etniskt ursprung**
- ☐ **Politiska åsikter**
- ☐ **Religiös eller filosofisk övertygelse**
- ☐ **Medlemskap i fackförening**
- ☐ **Genetiska uppgifter:** till exempel DNA
- ☐ **Biometriska uppgifter:** till exempel fingeravtryck
- ☐ **Hälsa**
- ☐ **Sexualliv eller sexuell läggning**
- ☐ **Uppgift om brott**

- ☐ **Personnummer**
- ☐ **Ekonomisk eller finansiell information**
- ☐ **Lokaliseringsuppgifter**
- ☐ **Kommunikationsloggar**
- ☐ **Födelsedatum**
- ☐ **Identifierande information:** till exempel för- och efternamn
- ☐ **Kontaktinformation**
- ☐ **Okänt vilka uppgifter som är drabbade**
- ☐ **Övrigt:**

Var personuppgifterna krypterade?

- ☐ **Ja**
- ☐ **Nej**

Vad kan bli konsekvenserna av incidenten för den registrerade?

- ☐ **Den registrerade förlorar kontrollen över de egna personuppgifterna**
- ☐ **Diskriminering**
- ☐ **Identitetsstöld eller bedrägeri**
- ☐ **Ekonomisk förlust**
- ☐ **Obehörigt hävande av pseudonymisering**
- ☐ **Skadat anseende**
- ☐ **Förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt**
- ☐ **Annan ekonomisk eller social nackdel**
- ☐ **Övrigt:**

Hur allvarlig bedömer ni incidenten?

- ☐ **Obetydlig**
- ☐ **Begränsad**
- ☐ **Betydande**
- ☐ **Mycket allvarlig**