# Datainspektionen informerar

# Nr 8/2018

# Allmänna råd

Datainspektionen ger ut allmänna råd i syfte:

1) att öka personuppgiftsansvarigas och personuppgiftsbiträdens medvetenhet om sina skyldigheter enligt EU:s dataskyddsförordning samt

2) att öka allmänhetens medvetenhet om och förståelse för risker, regler, skyddsåtgärder och rättigheter i fråga om behandling av personuppgifter.

De allmänna råden är inte bindande, utan innehåller rekommendationer om hur de bindande kraven i dataskyddsförordningen kan uppnås. Detta dokument är en **allmän vägledning gällande hantering av personuppgiftsincidenter.**

Datainspektionen

Den 21 maj 2018

di.ax datainspektionen

Datainspektionen • Elverksgatan 10, AX-22100 Mariehamn, Åland • Besöksadress: Kvarteret iTiden
+358 (0)18 25 550 • +358 (0)457 34 320 81 • inspektion@di.ax • www.di.ax

# 1. Inledning

Ifall en personuppgiftsansvarig på grund av en säkerhetsincident inte längre kan garantera att principerna för behandling av personuppgifter följs kan detta innebära risker för personers integritet och människors friheter och rättigheter. Sådana incidenter benämns **personuppgiftsincidenter** och dataskyddsförordningen reglerar närmare hur sådana situationer ska hanteras. Enligt dataskyddsförordningen ska personuppgiftsincidenter anmälas till tillsynsmyndigheten, vilket för åländska myndigheter innebär Datainspektionen. Detta ska göras inom 72 timmar efter att incidenten upptäcktes. Beroende på arten och omfattningen kan även de registrerade, vars personuppgifter drabbats av incidenten, behöva informeras.

# 2. Vad är en personuppgiftsincident?

En personuppgiftsincident definieras i artikel 4.12 i dataskyddsförordningen som en ”säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats”.

Personuppgiftsincidenter kan alltså vara av ytterst varierande art. Några exempel på personuppgiftsincidenter:

- Förlust eller stöld av en USB-sticka, en mobiltelefon eller en dator som innehåller personuppgifter.
- Personuppgifter har skickats till fel mottagare.
- Ett fel har uppstått i koden som kontrollerar användaridentifikation vilket leder till att användarna får tillgång till varandras konton.
- Någon har ändrat personuppgifter utan tillstånd.

Det spelar ingen roll ifall det inträffande har skett oavsiktligt eller med avsikt för att det ska vara fråga om en personuppgiftsincident. Av skäl 87 till dataskyddsförordningen framgår att den personuppgiftsansvarige måste vidta alla lämpliga tekniska skyddsåtgärder och alla lämpliga organisatoriska åtgärder för att omedelbart fastställa om en personuppgiftsincident ägt rum, för att sedan skyndsamt kunna informera ansvarig myndighet och i förekommande fall, de registrerade (mer om detta nedan). Här är det alltså viktigt att inte ”vänta och se” ifall det är fråga om en personuppgiftsincident, utan fastställa detta så fort som möjligt.

# 3. Anmälan till Datainspektionen

En personuppgiftsincident **ska anmälas** till Datainspektionen om den **medför en risk för personers rättigheter och friheter**. Vilka riskerna är och hur stora de är beror givetvis på vad som har inträffat och vilken sorts personuppgifter det berör. När en personuppgiftsincident ägt rum ska den personuppgiftsansvarige bedöma hur sannolika och allvarliga risker för individers rättigheter och friheter som incidenten medför. Riskerna kan vara exempelvis diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning, finansiell förlust eller brott mot sekretess och tystnadsplikt.

Om bedömningen visar att den inträffade personuppgiftsincidenten kan medföra risker för de registrerades rättigheter och friheter **måste detta anmälas till Datainspektionen**. Mer detaljerad information om hur anmälan ska göras finns på Datainspektionens hemsida.

Anmälan ska göras utan onödigt dröjsmål och **inom 72 timmar** efter att den personuppgiftsansvarige fått vetskap om personuppgiftsincidenten.

Ifall anmälan inte görs inom 72 timmar måste den personuppgiftsansvarige i sin anmälan ge en motivering till förseningen. Det ska dock noteras, att det är endast i ytterst speciella situationer som en försenad anmälan kan godtas och att gränsen på 72 timmar i de allra flesta fall måste följas.

I anmälan ska information ges om

- personuppgiftsincidentens art,
- vilka kategorier av registrerade personer och personuppgifter som berörs,
- det ungefärliga antalet personer och personuppgifter som berörs
- namn och kontaktuppgifter till dataskyddsombudet och andra som kan lämna information om personuppgiftsincidenten
- de sannolika konsekvenserna av personuppgiftsincidenten
- de åtgärder som vidtagits eller vilka åtgärder som föreslås för att åtgärda personuppgiftsincidenten, samt åtgärder som mildrar dess potentiella negativa effekter

I vissa situationer kan det vara svårt för den personuppgiftsansvarige att ha tillgång till all information som krävs för en anmälan inom 72 timmar. Detta kan vara fallet till exempel vid större nätattacker, där mer ingående undersökningar krävs för att fastställa personuppgiftsincidentens art och omfång.

I artikel 33.4 i dataskyddsförordningen stadgas därför att om det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt dröjsmål. Det rekommenderas att den personuppgiftsansvarige i sådana fall tydligt anger ifall denne avser att komplettera anmälan senare.

*Personuppgiftsincidenter som inte måste anmälas*

Alla personuppgiftsincidenter behöver inte anmälas till Datainspektionen. I vissa fall är det osannolikt att den inträffade incidenten innebär risker för personers rättigheter och friheter. Till exempel kanske en laptop innehållande dokument med personuppgifter har stulits, men laptopen är försedd med så säkra mekanismer och lösenord för att förhindra obehörig åtkomst att det i praktiken inte är möjligt att få tillgång till personuppgifterna. Förutsatt att en backup av personuppgifterna i laptopen finns lättillgängliga för den personuppgiftsansvarige eller personuppgiftsbiträdet (så att personuppgifterna alltså inte är förlorade) skulle denna incident osannolikt medföra risker för personers friheter och rättigheter och skulle alltså inte behöva anmälas till Datainspektionen. Observera dock att dataskyddsförordningen kräver att den personuppgiftsansvarige ska **dokumentera** alla personuppgiftsincidenter, även de som inte anmäls till Datainspektionen. Se punkt 6 nedan.

# 4. Information till de registrerade

I vissa situationer är det inte bara Datainspektionen som ska informeras om personuppgiftsincidenten, utan även de personer som drabbats av incidenten. Detta är fallet i situationer där risken som personuppgiftsincidenten leder till för personernas friheter och rättigheter är hög, vilket stadgas i artikel 34 i dataskyddsförordningen. Tröskeln för att informera de registrerade är alltså högre än för att anmäla till Datainspektionen, då en anmälan ska ske om en risk finns – även om det inte är en hög risk. Den personuppgiftsansvarige måste bedöma dels hur allvarliga konsekvenserna kan bli för de registrerade och dels hur sannolikt det är att enskilda personer drabbas. Risken är högre om konsekvenserna är allvarliga, och om sannolikheten för konsekvenser är stor är risken också högre. Detta är en bedömning som görs från fall. Ifall Datainspektionen anser att det finns en hög risk för individers friheter och rättigheter har Datainspektionen befogenhet att kräva att personuppgiftsansvariga informerar berörda personer om detta inte gjorts.

Informationen till de registrerade ska ske utan onödigt dröjsmål, formuleras på ett begripligt sätt och innehålla åtminstone:

- en tydlig och klar beskrivning av personuppgiftsincidentens art
- namn och kontaktuppgifter till dataskyddsombudet eller till annan kontakt som är insatt och kan svara på frågor
- en beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten
- en beskrivning av vad som gjorts eller kommer att göras för att hantera personuppgiftsincidenten
- en beskrivning, i förekommande fall, av vad som gjorts för att mildra negativa följder av personuppgiftsincidenten

En av huvudorsakerna till att informera personerna som drabbats är att kunna ge dem information om vilka åtgärder de bör vidta för att skydda sig mot effekterna av en personuppgiftsincident. Till exempel kan de drabbade behöva ändra sina lösenord eller vidta liknande åtgärder, beroende på personuppgiftsincidentens art.

# 5. Personuppgiftsbiträdets roll

Det är alltid den personuppgiftsansvarige som har det huvudsakliga ansvaret för att informera Datainspektionen och de drabbade om en personuppgiftsincident. Dock ställer dataskyddsförordningen vissa krav även på personuppgiftsbiträdet.

Ett personuppgiftsbiträde är enligt artikel 33.2 i dataskyddsförordningen skyldigt att underrätta den personuppgiftsansvarige **utan onödigt dröjsmål** efter att ha fått vetskap om en personuppgiftsincident.

Till skillnad från den personuppgiftsansvarige ska personuppgiftsbiträdet **inte** göra en riskbedömning av incidenten. Det viktiga är att personuppgiftsbiträdet informerar den personuppgiftsansvarige utan onödigt dröjsmål när det står klart att en personuppgiftsincident har inträffat. Det är sedan upp till den personuppgiftsansvarige att utföra en bedömning av risken som personuppgiftsincidenten för med sig. Ifall ett personuppgiftsbiträde är anlitat av flera

personuppgiftsansvariga ska personuppgiftsbiträdet separat informera var och en av de personuppgiftsansvariga som påverkats av en incident.

Förhållandet mellan den personuppgiftsansvarige och personuppgiftsbiträdet regleras genom ett personuppgiftsbiträdesavtal. I ett sådant avtal ska enligt artikel 28.3 f i dataskyddsförordningen ingå skyldigheterna för personuppgiftsbiträdet att bistå den personuppgiftsansvarige med att uppfylla kraven i artikel 33 och 34 gällande rapportering av personuppgiftsincidenter. Avtalet bör alltså tydligt reglera hur underrättandet av en personuppgiftsincident till den personuppgiftsansvarige ska ske.

Det är möjligt att i avtalet reglera att personuppgiftsbiträdet ska ha befogenhet att göra anmälan av en personuppgiftsincident enligt artikel 33 och 34 i den personuppgiftsansvariges ställe. Här är det dock viktigt att notera att det **juridiska ansvaret** för att anmäla personuppgiftsincidenten till Datainspektionen, och i förekommande fall informera de registrerade, alltid **kvarstår hos den personuppgiftsansvarige.**

## 6. Dokumentation

Dataskyddsförordningens artikel 33.5 ställer krav på att den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Kravet på dokumentation gäller alltså varje personuppgiftsincident och **inte endast de incidenter som anmäls** till Datainspektionen. Detta krav är kopplat till den grundläggande principen om ansvarsskyldighet (på engelska: accountability) i artikel 5.2 i dataskyddsförordningen. Det hör också ihop med de krav som ställs på den personuppgiftsansvariges ansvar i artikel 24.

Utöver de krav som ställs i artikel 33.5 rekommenderar Artikel 29-gruppen även att den personuppgiftsansvarige dokumenterar skälen för valet av de åtgärder som vidtagits i samband med personuppgiftsincidenten. Ifall bedömningen har gjorts att en personuppgiftsincident inte ska anmälas till Datainspektionen bör skälen för den bedömningen antecknas. Den personuppgiftsansvarige ska på begäran av Datainspektionen kunna visa upp dokumentationen. Det är upp till den personuppgiftsansvarige att bestämma hur dokumentationen av personuppgiftsincidenterna ska genomföras, men innehållet måste överensstämma med dataskyddsförordningens krav.