

Anmälan av gränsöverskridande personuppgiftsincident

enligt artikel 33 i dataskyddsförordningen

Har ni inte svar på alla frågor när ni fyller i anmälan, kan ni komplettera anmälan när ni har ytterligare information om incidenten. Kompletteringen ska i så fall ske skyndsamt. Fält märkta med asterisk (*) bör dock fyllas i innan ni skickar in anmälan.

Vid ändring eller komplettering av en tidigare gjord anmälan behöver bara de fält som ska ändras eller kompletteras fyllas i.

Undvik uppgifter som ni inte vill röja.

All information ni lämnar här kommer att bli allmän handling. Det innebär att informationen kan komma att behöva lämnas ut om någon begär det, och det inte finns någon bestämmelse om sekretess som hindrar ett utlämnande. Vi rekommenderar därför att ni inte lämnar fler uppgifter än vad som är nödvändigt i fritextfälten. Om ni ändå väljer att skriva något som ni anser bör omfattas av sekretess, använd fritextfältet sist i formuläret för att beskriva vad som i så fall enligt er bör vara sekretessbelagt. Oavsett detta är det Datainspektionen som slutligen avgör om en handling kan lämnas ut eller inte.

Information om hur Datainspektionen hanterar de personuppgifter ni anmäler finns på Datainspektionens webbplats.

Detta formulär ska användas av personuppgiftsansvariga, inte av registrerade (privatpersoner). Om du som registrerad anser att du har blivit drabbad av en personuppgiftsincident kan du skicka in ett klagomål till oss. I annat fall har du möjlighet att enbart tipsa oss om att en misstänkt personuppgiftsincident har skett.

Läs mer om personuppgiftsincidenter på vår webbplats:

www.datainspektionen.se/pui

Version 1.5 – 2019-01-03



Ska incidenten anmälas till Datainspektionen?

1. Är det här en ny anmälan, eller en ändring eller komplettering av en tidigare gjord anmälan? Markera endast ett alternativ.

- Ny anmälan
 Ändring eller komplettering, ange dnr för tidigare anmälan:

Internt referensnummer:

2. Felaktig incidentanmälan?

Om en tidigare gjord anmälan visat sig inte röra en personuppgiftsincident ska du ange anledningen här.

3. Är det osannolikt att incidenten medfört en risk för de registrerades fri- och rättigheter? Markera endast ett alternativ.

- Ja
 Nej

Om ni svarat ja på frågan ovan är detta inte en incident som behöver anmälas till Datainspektionen. Ni ska i så fall inte skicka in formuläret till Datainspektionen. Ni ska däremot dokumentera incidenten internt.

Att riskera de registrerades fri- och rättigheter kan till exempel vara att de förlorar kontrollen över sina uppgifter, att rättigheter inskränks, att de utsätts för diskriminering, identitetsstöld eller bedrägeri, finansiell förlust, skadlig ryktes-spridning och brott mot sekretess eller tystnadsplikt.

4. Har incidenten inträffat i Sverige eller i ett annat land? Markera endast ett alternativ.

- a. Incidenten har inträffat i Sverige och påverkar inte registrerade personer i andra länder
 b. Incidenten har inträffat i Sverige men påverkar registrerade personer i andra länder
 c. Incidenten har inträffat i minst ett annat land utöver Sverige

Om ni har fyllt i alternativ a ska ni inte fylla i detta formulär. Ni ska i stället fylla formuläret för icke-gränsöverskridande personuppgiftsincidenter.

5. Har ni ert huvudsakliga verksamhetsställe i Sverige?

Markera endast ett alternativ.

- a. Ni har er centrala förvaltning i Sverige och beslut om ändamål och medel för behandlingen fattas inte i något annat land inom EU/EES
- b. Ni har er centrala förvaltning i ett annat land än Sverige men beslut om ändamål och medel för behandlingen fattas i Sverige
- c. Ni har inte er centrala förvaltning i Sverige och beslut om ändamål och medel fattas i ett annat land än Sverige

Om ni har fyllt i alternativ c ska incidenten inte rapporteras till Datainspektionen. Ni ska i stället rapportera incidenten till er "ansvariga tillsynsmyndighet".

Den ansvariga tillsynsmyndigheten är tillsynsmyndigheten för den personuppgiftsansvariges huvudsakliga verksamhetsställe eller enda verksamhetsställe. Det huvudsakliga verksamhetsstället är: den plats i unionen där den personuppgiftsansvarige har sin centrala förvaltning, om inte besluten om ändamålen och medlen för behandlingen av personuppgifter fattas vid ett annat av den personuppgiftsansvariges verksamhetsställen i unionen och det sistnämnda verksamhetsstället har befogenhet att få sådana beslut genomförda, i vilket fall det verksamhetsställe som har fattat sådana beslut ska betraktas som det huvudsakliga verksamhetsstället.

6. Vilka andra länder berörs av incidenten? Markera alla som gäller.

- | | |
|--|---|
| <input type="checkbox"/> Belgien | <input type="checkbox"/> Malta |
| <input type="checkbox"/> Bulgarien | <input type="checkbox"/> Nederländerna |
| <input type="checkbox"/> Cypern | <input type="checkbox"/> Norge (EES) |
| <input type="checkbox"/> Danmark | <input type="checkbox"/> Polen |
| <input type="checkbox"/> Estland | <input type="checkbox"/> Portugal |
| <input type="checkbox"/> Finland | <input type="checkbox"/> Rumänien |
| <input type="checkbox"/> Frankrike | <input type="checkbox"/> Slovakien |
| <input type="checkbox"/> Grekland | <input type="checkbox"/> Slovenien |
| <input type="checkbox"/> Irland | <input type="checkbox"/> Spanien |
| <input type="checkbox"/> Island (EES) | <input type="checkbox"/> Storbritannien |
| <input type="checkbox"/> Kroatien | <input type="checkbox"/> Sverige |
| <input type="checkbox"/> Lettland | <input type="checkbox"/> Tjeckien |
| <input type="checkbox"/> Liechtenstein (EES) | <input type="checkbox"/> Tyskland |
| <input type="checkbox"/> Litauen | <input type="checkbox"/> Ungern |
| <input type="checkbox"/> Luxemburg | <input type="checkbox"/> Österrike |

En tillsynsmyndighet är en "berörd tillsynsmyndighet" om något av följande är uppfyllt:
– ni har ett verksamhetsställe i det land där tillsynsmyndigheten finns
– de registrerade i det land där tillsynsmyndigheten finns i väsentlig grad påverkas eller sannolikt i väsentlig grad kommer att påverkas av incidenten.

Personuppgiftsansvarig

7. Organisationens namn *	Skriv namnet på den personuppgiftsansvarige där incidenten har inträffat.
8. Organisationsnummer *	Skriv organisationsnummer för den personuppgiftsansvarige där incidenten har inträffat.
9. Organisationens postadress *	Postadress till personuppgiftsansvarige (dvs. inte besöksadress).

Kontaktperson/er för anmälan

10. Kontaktpersonens/ernas namn *	Namnet på den/de person/er som Datainspektionen kan kontakta.
11. Kontaktpersonens/ernas roll * Markera endast ett alternativ.	
<input type="checkbox"/> Dataskyddsombud <input type="checkbox"/> Annan roll	
12. Kontaktpersonens/ernas e-postadress*	
13. Kontaktpersonens/ernas postadress	
14. Kontaktpersonens/ernas telefonnummer *	

Incidenten	
15. När inträffade incidenten? *	(År, månad, & dag)
16. Pågår incidenten fortfarande?	
<input type="checkbox"/> Ja <input type="checkbox"/> Nej Om ni har fyllt i Ja ovan, se fråga 18. Om ni har fyllt i Nej, se fråga 17.	
17. När upphörde incidenten?	(År, månad, dag & klockslag)
18. När upptäckte ni incidenten? Klockslag obligatoriskt	(År, månad, dag & klockslag)
19. Er anmälan kommer in senare än 72 timmar efter att ni upptäckte incidenten. Beskriv varför.	
20. Vad har hänt vid incidenten?	Markera det alternativ som bäst stämmer överens med det som inträffade.
<input type="checkbox"/> Obehörigt röjande genom felaktigt utskick av mejl/brev/sms <input type="checkbox"/> Obehörigt röjande: övrigt <input type="checkbox"/> Obehörig åtkomst: Någon inom eller utanför organisationen har tagit del av information som den saknade behörighet till. <input type="checkbox"/> Förlust: Information har gått förlorad på något sätt, till exempel genom att en dator blivit stulen. <input type="checkbox"/> Förstöring: Någon eller något har förstört information, till exempel genom att en dator har gått sönder. <input type="checkbox"/> Ändring: Personuppgifter har ändrats på något sätt.	

<p>21. Kort beskrivning av incidenten</p>	
<p>22. Vad är det för typ av incident?</p> <ul style="list-style-type: none"> <input type="checkbox"/> Digital enhet har förlorats <input type="checkbox"/> Dokument har förlorats/skadats <input type="checkbox"/> E-post har förlorats eller öppnats av obehörig person <input type="checkbox"/> Hackning <input type="checkbox"/> Skadlig kod (malware) <input type="checkbox"/> Nätfiske (phishing) <input type="checkbox"/> Fysiskt dokument har gallrats på felaktigt sätt <input type="checkbox"/> E-avfall har inte rensats på personuppgifter <input type="checkbox"/> Personuppgifter har publicerats av misstag <input type="checkbox"/> Personuppgifter har avslöjats muntligen av misstag <input type="checkbox"/> Övrigt: 	
<p>23. Hur upptäckte ni incidenten? Markera endast ett alternativ.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Genom en automatiserad process: tekniska säkerhetsåtgärder <input type="checkbox"/> Genom organisatoriska rutiner, till exempel en återkommande kontroll <input type="checkbox"/> En anställd informerade oss <input type="checkbox"/> Vårt personuppgiftsbiträde informerade oss <input type="checkbox"/> En utomstående eller registrerad informerade oss. 	
<p>24. Varför inträffade incidenten enligt er uppfattning? Markera endast ett alternativ.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Mänskliga faktorn: fel i det enskilda fallet <input type="checkbox"/> Brist i organisatoriska rutiner eller processer: systematiska fel <input type="checkbox"/> Tekniskt fel, till exempel fel i mjukvara, programinställningar <input type="checkbox"/> Medvetet angrepp från någon i organisationen: angrepp inifrån <input type="checkbox"/> Antagonistiskt angrepp: angrepp utifrån <input type="checkbox"/> Okänd orsak 	

25. Inom vilket verksamhetsområde inträffade incidenten?

Markera endast ett alternativ.

- Hälsa- och sjukvård
- Socialtjänst
- Skola: förskola, grundskola, gymnasium
- Universitet eller högskola
- Annan eftergymnasial utbildning
- Forskning
- Finansiell sektor eller försäkring
- Kreditupplysning
- Inkasso
- Näringslivet i övrigt
- Polis
- Rättsväsendet i övrigt
- Ideell organisation eller ekonomisk förening
- Kommun
- Statlig myndighet
- Övrigt:

Biträden

26. Gäller incidenten en personuppgiftsbehandling som hanteras av anlitade personuppgiftsbiträden eller underbiträden?

- Ja
 Nej

27. Organisationens namn och organisationsnummer.

Organisationens namn och organisationsnummer:

Organisationens namn och organisationsnummer:

Organisationens namn och organisationsnummer:

Uppgifterna och de registrerade

28. Hur många registrerade har påverkats?

Exakt antal:

Om ni inte känner till det exakta antalet kan ni uppskatta antalet genom att fylla i något av de angivna intervallen. Markera endast ett alternativ.

- 1–10
- 11–100
- 101–1 000
- 1 001–10 000
- 10 001–100 000
- 100 001–500 000
- 500 001–1 miljon
- Över 1 miljon
- Okänt/kan inte ange

29. Hur många uppgifter om registrerade personer har påverkats?

Exakt antal:

Om ni inte känner till det exakta antalet kan ni uppskatta antalet och fylla i något av de angivna intervallen. Markera endast ett alternativ.

- 1–10
- 11–100
- 101–1 000
- 1 001–10 000
- 10 001–100 000
- 100 001–500 000
- 500 001–1 miljon
- Över 1 miljon
- Okänt/kan inte ange

30. Vilka grupper tillhör de registrerade?

Markera alla alternativ som gäller.

- Anställda hos den personuppgiftsansvarige
- Användare av den personuppgiftsansvariges tjänster
- Kunder hos den personuppgiftsansvarige
- Prenumeranter
- Medlemmar, till exempel i en förening eller en kundklubb
- Militär, det vill säga anställda inom totalförsvaret
- Patienter
- Barn
- Skolelever i förskola, grundskola eller gymnasium
- Studerande i eftergymnasial utbildning
- Utsatta personer, till exempel personer som lever med skyddad identitet
- Övriga personer som enligt er bedömning drabbas särskilt hårt om personuppgifter sprids
- Kan inte ange för närvarande
- Övrigt:

31. Vilken sorts personuppgifter har incidenten drabbat?

Markera alla alternativ som gäller.

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Genetiska uppgifter
- Biometriska uppgifter
- Hälsa
- Sexualliv eller sexuell läggning
- Uppgift om brott
- Personnummer
- Ekonomisk eller finansiell information
- Officiella dokument
- Lokaliseringsuppgifter (till exempel GPS-position, ej adressuppgifter)
- Kommunikationsloggar
- Metadata om kommunikation
- Födelsedatum
- Identifierande information (till exempel för- och efternamn)
- Kontaktinformation
- Okänd
- Övrigt:

32. Var personuppgifterna krypterade? Markera endast ett alternativ.

- Ja, samtliga uppgifter
- Ja, men inte alla uppgifter
- Nej
- Vet inte

Konsekvenser

33. Vad kan bli konsekvenserna av incidenten?

Markera alla alternativ som gäller.

- Den registrerade förlorar kontrollen över de egna personuppgifterna
- Begränsning av rättigheter
- 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:

34. Vad för andra konsekvenser kan incidenten leda till?

Konfidentialitetsincidenter

- Större distribution av personuppgifter än vad som var nödvändigt eller vad de registrerade samtyckt till
- Personuppgifter kan komma att samköras med andra uppgifter om de registrerade
- Övrigt:

Riktighetsincidenter

- Personuppgifter som inte är korrekta kan ha behandlats av misstag
- Personuppgifter kan ha behandlats för andra ändamål än de avsedda
- Övrigt:

Tillgänglighetsincidenter

- Förlust av förmågan att tillhandahålla en tjänst som är kritisk/nödvändig för de registrerade
- Påverkan av förmågan att tillhandahålla en tjänst som är kritisk/nödvändig för de registrerade
- Övrigt:

35. Hur allvarlig bedömer ni att incidenten är?	
<p>Uppskatta hur allvarlig incidenten är med hänsyn till de registrerades integritet. 1 är minst allvarlig och 4 mest allvarlig. Markera endast ett alternativ.</p> <p><input type="checkbox"/> 1. Obetydlig</p> <p><input type="checkbox"/> 2. Begränsad</p> <p><input type="checkbox"/> 3. Betydande</p> <p><input type="checkbox"/> 4. Mycket allvarlig</p>	
36. Hur har ni agerat efter incidenten?	Beskriv vad ni har gjort. Har ni vidtagit åtgärder eller avser att vidta åtgärder för att lösa problem, förebygga eller mildra effekterna av incidenten?
Datum och tid: Åtgärd:	
Datum och tid: Åtgärd:	
Datum och tid: Åtgärd:	
Datum och tid: Åtgärd:	

Information till de registrerade	
<p>37. Har ni informerat de registrerade om incidenten? Markera endast ett alternativ.</p> <p><input type="checkbox"/> Ja <input type="checkbox"/> Nej</p> <p>Om ni svarat Ja på frågan ovan, se nästa fråga. Om ni svarat Nej på frågan ovan, se fråga 39.</p>	
<p>38. När informerade ni de registrerade?</p> <p>Datum:</p> <p>Gå vidare till fråga 43.</p>	
<p>39. Kommer ni att informera de registrerade? Markera endast ett alternativ.</p> <p><input type="checkbox"/> Ja <input type="checkbox"/> Nej <input type="checkbox"/> Vi har inte tagit ställning än</p> <p>Om ni svarat Ja på frågan ovan, se nästa fråga. Om ni svarat Nej, gå till fråga 41.</p>	
<p>40. När kommer ni att informera de registrerade?</p> <p>Datum:</p> <p>Se fråga 46.</p>	
<p>41. Varför kommer ni inte att informera de registrerade? Markera alla alternativ som gäller.</p> <p><input type="checkbox"/> a: Incidenten medför inte hög risk för personers fri- och rättigheter <input type="checkbox"/> b: Personuppgifterna var krypterade eller på annat sätt skyddade <input type="checkbox"/> c: Vi har redan vidtagit åtgärder som avhjälper riskerna <input type="checkbox"/> d: Att informera innebär en oproportionell ansträngning, vi har istället informerat allmänheten</p> <p>Om ni svarat a eller b på frågan ovan, se fråga 46. Om ni svarat c, se fråga 42. Om ni svarat d, se fråga 44.</p>	

<p>42. Beskriv de åtgärder ni vidtagit för att avhjälpa riskerna som innebär att ni inte behöver informera de registrerade.</p>	
<p>Se fråga 46.</p>	
<p>43. Hur har ni informerat de registrerade?</p>	
<p>Se fråga 45.</p>	
<p>44. Beskriv hur ni informerat allmänheten eller vilka åtgärder ni vidtagit för att informera de registrerade på ett effektivt sätt.</p>	
<p>45. Vad har ni lämnat för information till de registrerade? Bifoga informationen till anmälan.</p>	

Komplettering/eventuell sekretess

46. Den här anmälan kommer att kompletteras. Om ni ska komplettera anmälan så måste det ske skyndsamt. Markera endast ett alternativ.

- Ja
 Nej

47. Vi anser att viss information i min anmälan bör omfattas av sekretess. Beskriv vilken information som enligt er bör vara sekretessbelagd, och varför.

Har du frågor?

Läs mer om personuppgiftsincidenter på vår webbplats. www.datainspektionen.se/pui

Om du inte hittar svaret där kan du nå oss på e-post personuppgiftsincident@datainspektionen.se eller tel 08-657 61 00.

Kontakt

Blanketten skickar du per brev till:
Datainspektionen
Box 8114
104 20 Stockholm

