



Rapportering av integritetsincident från tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster

Ni kan rapportera integritetsincidenter via denna blankett till incidentrapport@pts.se. Integritetsincidenter och rapporteringen av dessa regleras i EU Kommissionens förordning (EU) nr 611/2013¹ samt 1 kap 7 § samt 8 kap 8 § Lagen (2022:482) om elektronisk kommunikation (LEK). Med blanketten avser PTS att underlätta för tillhandahållare att rapportera integritetsincidenter till myndigheten enligt lag och EU-förordning och skapa enkelhet, smidighet och likabehandling i incidenthanteringen vid PTS. För rapportering av säkerhetsincidenter i allmänt tillgängliga elektroniska kommunikationstjänster finns en annan blankett och andra regler gäller.

En inledande rapport ska vara Post- och telestyrelsen till handa inom 24 timmar från det att integritetsincidenten upptäcktes.

Grundläggande uppgifter

1. Kontaktuppgifter och organisation ²	2. Datum
3. Ert referensnummer för ärendet	4. PTS diarienummer (vid komplettering)
5. Detta är en: ☐ en fullständig rapport (allt rapporteras på en gång och avses inte följas av fler rapporter) ☐ en inledande rapport (kommer att kompletteras) ☐ en kompletterande rapport (kommer att kompletteras) ☐ en kompletterande och slutlig rapport (avses inte att följas av fler rapporter)	
6. Denna incident rapporteras även helt eller delvis som en säkerhetsincident ³ Ja ☐ Nej ☐	
7. Vad var tillhandahållarens roll i samband med incidenten? ⁴	
8. Önskas sekretess på uppgifter i rapporten? Ja ☐ Nej ☐	

¹ EU Kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation

² PTS lämnar alltid ut kontaktuppgifter om någon begär att få ta del av handlingen då den är allmän. Skriv därför bara uppgifter som kan lämnas ut. En kontaktväg eller kontaktpunkt ska alltid anges, men behöver inte innehålla personuppgifter.

³ Uppgiften behövs för att säkerställa att en och samma händelse som rapporterats till PTS enligt två olika regelverk för rapportering av säkerhetsincidenter respektive rapportering av integritetsincidenter handläggs samordnat, effektivt och smidigt.

⁴ T.ex. nätägare, tjänsteleverantör, kommunikationsoperatör, internetknutpunktsleverantör eller tillhandahållare av nummberoende interpersonella kommunikationstjänster, s.k. NI-ICS, m.fl.

Om ja; sekretess önskas på grund av:

- ☐ Affärspartners ekonomiska eller personliga förhållanden
- ☐ Affärsförhållanden som kan antas skada bolaget om de offentliggörs
- ☐ Driftsförhållanden som kan antas skada bolaget om de offentliggörs
- ☐ Uppgift om säkerhets- eller bevakningsåtgärd om syftet med åtgärden motverkas om uppgiften röjs

- ☐ Annat. Ange:

Inledande rapport

9. När inträffade integritetsincidenten? ⁵

10. När upptäcktes integritetsincidenten?

11. Hur upptäcktes integritetsincidenten?

12. Vad har hänt? Beskriv omständigheterna, t.ex. tekniska och/eller organisatoriska orsaker samt händelseförloppet.

13. Ange om händelsen rörde sig om otillåtet (ange en eller flera) ⁶:

- ☐ avslöjande
- ☐ förlust
- ☐ ändring
- ☐ åtkomst
- ☐ utplåning

av uppgifter som behandlas i samband med tillhandahållande av tjänster.

☐ Händelsen var oavsiktlig.

14. Vilka behandlade uppgifter ⁷ har berörts?

⁵ Om exakt tidpunkt eller tidsrymd inte kan fastställas, gör en uppskattning. Ange om det är en uppskattning.

⁶ Begreppet integritetsincident definieras i 1 kap. 7 § LEK. Ange de omständigheter enligt definitionen som talar om vad det är för slags säkerhetsincident som rapporteras.

⁷ Med behandlade uppgift avses uppgifter som har behandlats i samband med tillhandahållande av elektroniska kommunikationstjänster.

15. Vilka åtgärder har ni vidtagit eller ska ni vidta för att avhjälpa eller begränsa incidenten? Ange både tekniska och organisatoriska åtgärder? ⁸

16. Har någon annan leverantör varit inblandad i incidenten?⁹ Ange i så fall vilken.

Tillhandahållaren ska lämna en kompletterande rapport till PTS inom tre dagar från den inledande rapporten.¹⁰ Det går alltid bra att lämna samtliga uppgifter i en fullständig rapport inom 24 timmar från upptäckten, eller att fylla i fält avsedda för kompletterande rapport även i en inledande rapport.

Kompletterande rapport / fortsättning

17. Vad har hänt? Lägg till sådant som tillkommit efter den inledande rapporten om detta är en kompletterande rapport.

18. Ange antal berörda användare och/eller aktiva anslutningar. ¹¹

19. Ange potentiella konsekvenser och potentiell menlig inverkan för användare och/eller aktiva anslutningar. ¹²

20. Vilka åtgärder har ni vidtagit för att minska skada eller negativa konsekvenser för drabbade användare och/eller aktiva anslutningarna? Ange både tekniska och organisatoriska åtgärder. ¹³

⁸ De åtgärder som efterfrågas här rör tekniska och organisatoriska åtgärder med fokus på att begränsa eller stoppa incidenten från att fortgå.

⁹ Ange om någon annan leverantör, affärspartner eller dylikt varit inblandad i, medverkat till eller orsakat incidenten.

¹⁰ Om leverantören, trots sin utredning, inte kan tillhandahålla alla uppgifter inom tre dagar från den ursprungliga anmälan ska leverantören lämna så många uppgifter som den förfogar över inom den tidsfristen och till den behöriga myndigheten lämna en välgrundad motivering till den sena anmälan av de återstående uppgifterna. Leverantören ska snarast möjligt lämna de återstående uppgifterna till den behöriga myndigheten och, om det är nödvändigt, snarast möjligt uppdatera redan lämnade uppgifter.

¹¹ Vet ni ännu inte vid den kompletterande rapporten hur många som har drabbats, ange detta. Ange även hur lång tid ni bedömer för att en komplett rapport ska kunna ges in.

¹² Om ni inte kan komma på vilka konsekvenser händelsen kan få för användaren, så ange i vart fall att abonnenten själv bör tänka igenom vilka konsekvenserna kan bli.

¹³ De åtgärder som efterfrågas här är åtgärder med fokus på att minska skadan eller potentiell skada för abonnent och/eller användare eller att annars hjälpa berörd abonnent eller användare i anledning av incidenten. T.ex. att operatören bett den felaktiga mottagaren av en uppgift radera uppgiften eller begärt återkallelse av en felaktig kreditupplysning.

21. Finns det drabbade i andra EU-länder?

☐ Ja

☐ Nej

22. Har ni anmält eller ska ni anmäla händelsen till andra myndigheter? I så fall vilka.

Information om innehållet i underrättelser till användare och/eller abonnenter

23. Hur många drabbade användare och/eller aktiva anslutningar har underrättats?

24. Hur och när har de drabbade underrättats?

25. Bifoga bilaga eller infoga underrättelsens innehåll här.¹⁴

PTS behandling av personuppgifter

PTS behandlar personuppgifter som inkommit inom ramen för incidentrapportering för att kommunicera och handlägga ärendet. Den rättsliga grunden för behandlingen är att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i PTS myndighetsutövning.

För mer information om PTS personuppgiftsbehandling, se [Behandling av personuppgifter | PTS](#)

Incidentrapporten skickas till incidentrapport@pts.se.

¹⁴ Det är inte tillräckligt att ange att en underrättelse har skett i enlighet med förordningen. Det faktiska innehållet i underrättelsen ska redogöras för, exempelvis genom kopia på skrivelsen eller talmanus från telefonsamtal.