Vår referens: 23–978 **Aktbilaga:** 21

Beslut angående sanktionsavgift

Parter

WhatsApp Ireland Limited (WhatsApp), med säte i Irland, org. nr 607470

Ombud: Cirio Advokatbyrå AB, anna.hovstadius@cirio.se

Saken

Sanktionsavgift enligt 12 kap. 1 § 5 lagen (2022:482) om elektronisk kommunikation (LEK)

Post- och telestyrelsens avgörande

Post- och telestyrelsen (PTS) avstår från att ta ut sanktionsavgift från WhatsApp Ireland Limited (WhatsApp) och avslutar ärendet utan ytterligare åtgärd.

Bakgrund

Reglerna om skyldighet att rapportera in säkerhetsincidenter till PTS i 8 kap. 3 § LEK trädde i kraft i juni 2022. I augusti 2022 började även Post- och telestyrelsens föreskrifter och allmänna råd om säkerhet i nät och tjänster (PTSFS 2022:11) (PTS säkerhetsföreskrifter) att gälla, vilka bl.a. anger tidsfrister för incidentrapportering samt vilka uppgifter rapporterna ska innehålla. Under månaderna närmast efter att de nya reglerna om säkerhetsincidenter trädde ikraft förde PTS dialoger med ett flertal tillhandahållare kring vad som utgör rapporteringspliktiga säkerhetsincidenter enligt LEK och PTS säkerhetsföreskrifter. PTS har sett ett särskilt behov av att informera och föra dialog med de nya aktörstyper, till vilka WhatsApp hör, som sedan juni 2022 omfattas av rapporteringskraven.

Bakgrunden till detta beslut och den dialog som PTS har haft med WhatsApp efter det avbrott i tjänsten som inträffade den 25 oktober 2022 framgår av den underrättelse som PTS skickade till WhatsApp den 30 mars 2023, se aktbilaga 12. Av utredningen i ärendet framgår även följande. PTS ställde i november 2022 i dialogen med WhatsApp frågan om det kunde vara av intresse för WhatsApp med ett möte för att prata om exempelvis skillnader i

Post- och telestyrelsen
Postadress: Box 6101, 102 32 Stockholm
Besöksadress: Hälsingegatan 38
Telefon: 08-678 55 00
E-post: pts@pts.se
www.pts.se

regelverken vad gäller rapportering av säkerhets- respektive integritetsincidenter och frågor om handlingars offentlighet i Sverige och svenska sekretessregler. PTS uppgav att syftet med mötet skulle vara att underlätta en bra och smidig fortsatt rapporteringsrutin. WhatsApp var positiva till ett sådant möte men mötet blev inte av. När bolaget återkopplade till PTS att ett möte skulle vara intressant fanns det fortfarande en legal frist för att lämna in en kompletterande säkerhetsincidentsrapport.

WhatsApps yttrande över PTS underrättelse

WhatsApp har den 26 april 2023 yttrat sig över underrättelsen och i samband med detta inkommit med samtliga de uppgifter som tidigare saknades för att utgöra en komplett incidentrapportering. I sitt yttrande anför WhatsApp bl.a. följande.

WhatsApp har utvecklat grundliga interna rutiner för att identifiera och hantera säkerhetsincidenter genom hela sin globala organisation. Enligt dessa rutiner och direktivet om inrättande av en europeisk kodex för elektronisk kommunikation bedömdes inte den aktuella incidenten utgöra en anmälningspliktig incident. Vidare anför WhatsApp att bolaget är angeläget om att vara transparent och samarbeta med PTS och ber därför PTS att betrakta det aktuella yttrandet, som innehåller den erforderliga informationen enligt LEK, PTS säkerhetsföreskrifter samt punktuppställningen i PTS underrättelse, som en formell anmälan.

Skäl

Tillämpliga bestämmelser

Krav avseende incidentrapportering

Av 1 kap. 7 § LEK framgår att med säkerhetsincident avses en händelse med en faktisk negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster, eller på förmågan att motstå sådana händelser.

Av 8 kap. 3 § LEK framgår bl.a. att den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst utan onödigt dröjsmål ska rapportera säkerhetsincidenter till PTS som har haft en betydande påverkan på nät och tjänster.

Av bestämmelsens andra stycke framgår att PTS har bemyndiganden att meddela ytterligare föreskrifter om rapportering av säkerhetsincidenterna och föreskrifter om undantag från rapporteringsskyldigheten.

Av 17 kap. 1 § PTS säkerhetsföreskrifter framgår att tillhandahållaren bl.a. ska rapportera sådana säkerhetsincidenter som anges i 5 §.

Av 17 kap. 2 § PTS säkerhetsföreskrifter framgår att tillhandahållaren vid incidentrapportering ska lämna en inledande och en kompletterande rapport.

Av 17 kap. 3 § PTS säkerhetsföreskrifter framgår att den inledande rapporten ska vara Post- och telestyrelsen till handa inom 72 timmar från det att säkerhetsincidenten upptäcktes och att den ska innehålla uppgifter om

1. när säkerhetsincidenten inträffade,
2. hur länge säkerhetsincidenten har pågått,
3. antal aktiva anslutningar eller användare som har drabbats av säkerhetsincidenten,
4. berört geografiskt område, i de fall det är relevant,
5. vilka säkerhetsaspekter (tillgänglighet, autenticitet, riktighet eller konfidentialitet) som har berörts av säkerhetsincidenten,
6. vilka kommunikationsnät, kommunikationstjänster, lagrade, överförda eller behandlade uppgifter eller närliggande tjänster som har berörts av säkerhetsincidenten,
7. säkerhetsincidentens påverkan på kommunikationsnätet eller kommunikationstjänsten eller påverkan på funktioner i samhället,
8. tillhandahållarens preliminära bedömning av orsaken till säkerhetsincidenten,
9. hur säkerhetsincidenten har påverkat berörda aktiva anslutningar eller användare i Sverige,
10. huruvida säkerhetsincidenten har medfört begränsningar i möjligheten till nödkommunikation via det kommunikationsnät eller den kommunikationstjänst som berörts av säkerhetsincidenten, och
11. tillhandahållarens kontaktuppgifter och referensnummer för ärendet.

Allmänt råd till 3 §

Tillhandahållaren bör göra en uppskattning av tidpunkten för när säkerhetsincidenten har inträffat i de fall en exakt tidpunkt inte kan fastställas med stöd av system för övervakning eller loggning. Uppskattningen bör göras med utgångspunkt från kända fakta om incidenten.

Redogörelsen enligt 3 § 6 bör innehålla såväl uppgifter om de berörda nätteknologierna som uppgift om berörda slutanvändartjänster, till exempel rösttelefoni, meddelandetjänst eller internetanslutning.

Av 17 kap. 4 § PTS säkerhetsföreskrifter framgår att den kompletterande rapporten ska vara Post- och telestyrelsen till handa inom två veckor från det att den inledande rapporten

lämnades och att anstånd kan beviljas. Vidare framgår att rapporten ska innehålla uppgifter om

1. komplettering och uppdatering av uppgifterna som lämnats i den inledande rapporten,
2. orsakerna till säkerhetsincidenten,
3. vilken information som har lämnats till allmänheten och berörda personer samt vid vilken tidpunkt och på vilket sätt denna information lämnades,
4. de åtgärder som har vidtagits för att minimera effekterna av säkerhetsincidenten inför slutligt avhjälpande,
5. de åtgärder som har vidtagits för att avhjälpa de fel och brister som orsakat säkerhetsincidenten och vid vilken tidpunkt åtgärderna vidtogs,
6. de åtgärder som har vidtagits och som planeras för att undvika liknande säkerhetsincidenter samt vid vilken tidpunkt dessa åtgärder vidtogs eller när de bedöms vara genomförda, och
7. referensnummer för ärendet.

Allmänt råd till 4 §

Tillhandahållarens redogörelse för orsakerna till säkerhetsincidenten bör beskriva samtliga kända omständigheter som har eller kan ha bidragit till att incidenten inträffade.

Av 17 kap. 5 § PTS säkerhetsföreskrifter följer att säkerhetsincidenter som innebär störning eller avbrott (tillgänglighet) i tillhandahållna kommunikationsnät eller kommunikationstjänster alltid ska rapporteras under förutsättning att vissa tröskelvärden är uppfyllda, se tabell nedan.

Tid som incidenten pågått	*Incidentens uppskattade omfattning*
≥ 1 timme	≥ 150 000 användare eller aktiva anslutningar i Sverige, ≥ 50 procent kapacitetsbortfall eller ≥ 15 000 km² sammanhängande berört område
≥ 2 timmar	≥ 30 000 användare eller aktiva anslutningar i Sverige, ≥ 30 procent kapacitetsbortfall eller ≥ 5 000 km² sammanhängande berört område
≥ 6 timmar	≥ 5 000 användare eller aktiva anslutningar i Sverige, ≥ 20 procent kapacitetsbortfall eller ≥ 2 500 km² sammanhängande berört område
≥ 24 timmar	≥ 2 000 användare eller aktiva anslutningar i Sverige, ≥ 10 procent kapacitetsbortfall eller ≥ 1 000 km² sammanhängande berört område

Allmänt råd till 5 §

Berört område för kommunikationstjänster som tillhandahålls över mobila nätanslutningar bör normalt vara det sammanlagda täckningsområdet för berörda celler eller motsvarande i mobilnätet.

Kapacitetsbortfall bör till exempel kunna beräknas som andelen berörda användare eller aktiva anslutningar i förhållande till det totala antalet användare eller aktiva anslutningar för kommunikationstjänsten, eller, andel misslyckade samtalsförsök.

Åläggande av sanktionsavgift

Av 12 kap. 1 § 5 LEK framgår att tillsynsmyndigheten ska besluta att ta ut en sanktionsavgift av den som inte rapporterar om säkerhetsincidenter i enlighet med 8 kap. 3 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen.

En sanktionsavgift ska enligt 12 kap. 2 § LEK bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

Av bestämmelsens andra stycke framgår att när avgiftens storlek bestäms ska särskild hänsyn tas till

1. den skada eller risk för skada som har uppstått till följd av överträdelsen,
2. om aktören tidigare har begått en överträdelse, och
3. de kostnader som aktören har undvikit till följd av överträdelsen.

Tillsynsmyndigheten får enligt tredje stycket avstå från att ta ut en sanktionsavgift helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

PTS bedömning

En regelöverträdelse har skett

Baserat på de uppgifter WhatsApp har lämnat till PTS, bedömer PTS att den inträffade händelsen i WhatsApp-tjänsten den 25 oktober 2022 når upp till trösklarna i 17 kap. 5 § PTS säkerhetsföreskrifter eftersom avbrottet i WhatsApp-tjänsten varade i mer än två timmar och uppskattningsvis påverkade cirka 1,1 miljoner WhatsApp-användare i Sverige. Därmed var händelsen rapporteringspliktig till PTS. WhatsApp är en stor tillhandahållare av

kommunikationstjänster och har många användare i Sverige. Det finns därmed en risk att eventuella framtida avbrott och störningar i WhatsApp-tjänsten potentiellt kan drabba många svenska användare. Vid utebliven rapportering av faktiska säkerhetsincidenter avseende avbrott och störningar (tillgänglighet) i enlighet med PTS rapporteringströsklar finns det således risk att PTS inte får vetskap om allvarliga händelser och att PTS inte får del av viktig information kring incidenten. PTS har även en skyldighet att vidarerapportera större incidenter till ENISA[1] varje år i enlighet med gällande EU-rättsakter.

I WhatsApps yttrande över PTS underrättelse, uppger WhatsApp bl.a. att bolaget har utvecklat grundliga interna rutiner för att identifiera och hantera säkerhetsincidenter genom hela sin globala organisation och att den aktuella incidenten inte bedömdes utgöra en anmälningspliktig incident enligt dessa rutiner och direktivet om inrättande av en europeisk kodex för elektronisk kommunikation. PTS delar inte denna bedömning. Incidenten borde därmed ha rapporterats till PTS i enlighet med regelverket.

I bolagets yttrande över PTS underrättelse vill WhatsApp att PTS ska betrakta svaren i yttrandet som en formell anmälan. Det är därmed enligt PTS uppfattning ostridigt att ett antal av de obligatoriska uppgifterna har kommit in för sent till PTS.

PTS konstaterar därmed att WhatsApp inte har rapporterat den inträffade säkerhetsincidenten i enlighet med 8 kap. 3 § LEK samt 17 kap. 1 – 5 §§ PTS säkerhetsföreskrifter. Uppgiftslämnandet var inte komplett utifrån de regler som gäller för rapportering av säkerhetsincidenter och skedde inte inom den föreskrivna tiden för rapportering av säkerhetsincidenter. Regelöverträdelsen består i att såväl den inledande rapporten som den kompletterande rapporten enligt vad som beskrivits ovan saknade en rad uppgifter som enligt 17 kap. 3–4 §§ ska finnas med i rapporterna.

Rapporteringen är numera komplett då WhatsApp har inkommit med de saknade uppgifterna i samband med sitt yttrande över PTS underrättelse den 26 april 2023.

Mot bakgrund av att WhatsApp inte har rapporterat säkerhetsincidenten i enlighet med 8 kap. 3 § LEK och 17 kap. 1 – 5 §§ PTS säkerhetsföreskrifter, går PTS vidare med en bedömning av om sanktionsavgift ska utgå.

Sanktionsavgift

PTS ska besluta att ta ut en sanktionsavgift av den som inte rapporterar om säkerhetsincidenter i enlighet med regelverket. Av förarbetena till bestämmelsen om

[1] The European Union Agency for Cybersecurity

sanktionsavgifter avseende säkerhet i nät och tjänster framgår att lagstiftaren anser att det är viktigt att det finns tydliga drivkrafter för operatörer att följa gällande regelverk (prop. 2021/22:136 s. 353). Den effekt som sanktionsavgifter har på viljan att följa reglerna där sanktionsavgift kan bli aktuellt, har dessutom bedömts som så viktig av regeringen att PTS *ska* ta ut en sanktionsavgift och inte endast *får* besluta att göra det.

WhatsApp har i det här fallet alltså gjort sig skyldigt till en överträdelse som normalt medför att sanktionsavgift ska påföras. PTS får emellertid avstå från att ta ut en sanktionsavgift helt eller delvis om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften.

PTS har på eget initiativ under den tid då WhatsApp skulle inkomma med rapporter om säkerhetsincidenten inlett en dialog med bolaget och efterfrågat vissa specifika uppgifter från WhatsApp samt i ett senare skede även föreslagit ett möte med bolaget för att bland annat förklara det svenska regelverket. PTS bedömer att den dialog som myndigheten har haft med WhatsApp och som har medfört att ett antal uppgifter har lämnats till myndigheten i tid, i kombination med att myndigheten inte återkom om mötestid till bolaget, kan ha lett till att WhatsApp fått uppfattningen att PTS inte såg behov av ytterligare uppgifter i ärendet. Detta särskilt mot bakgrund av att PTS inte efterfrågade de återstående uppgifterna innan myndigheten underrättade bolaget den 30 mars 2023. PTS bedömer därmed att det med hänsyn till de särskilda omständigheterna i detta specifika ärende, är oskäligt att ta ut någon sanktionsavgift med anledning av överträdelsen. Myndigheten beslutar därför att helt avstå från att ta ut en sanktionsavgift från WhatsApp. I och med att samtliga uppgifter om incidenten har lämnats till PTS finns det inte heller skäl att vidta några ytterligare tillsynsåtgärder.

Underrättelse om överklagande

Om ni vill överklaga detta beslut ska ni skriva till Förvaltningsrätten i Stockholm. Brevet ska dock sändas till Post- och telestyrelsen, Box 6101, 102 32 Stockholm, alternativt till pts@pts.se.

Tala om i brevet vilket beslut ni överklagar genom att ange beslutets nummer. Tala också om vilken ändring av beslutet ni vill ha.

Brevet med överklagandet ska innehålla: ert person-/organisationsnummer, postadress, e-postadress och telefonnummer till bostaden och mobiltelefon. Adress och telefonnummer till er arbetsplats ska också anges samt eventuell annan adress där ni kan nås för delgivning. Om ni anlitar ett ombud, ska ombudets namn, postadress, e-postadress, telefonnummer till arbetsplatsen och mobiltelefonnummer anges.

PTS måste ha fått ert överklagande inom tre veckor från den dag ni fått del av beslutet. Annars kan överklagandet inte prövas.

PTS sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning.

Om något är oklart kan ni vända er till PTS.

Beslutet har fattats av ställföreträdande generaldirektören Catarina Wretman. I ärendets slutliga handläggning har även avdelningschefen Patrik Bystedt, chefsjuristen Karolina Asp, enhetschefen Johanna Eklund, verksjuristen Sofie Sandell, seniora handläggaren Erika Hersaeus och juristen Petra Nilsson (föredragande) deltagit.