Vår referens: Dnr 25–5000, **Aktbilaga** 18

Beslut om sanktionsavgift

Part

Tele2 Sverige AB, org.nr 556267–5164

Sanktionsavgift enligt 12 kap. 1 § 8 och 10 lagen (2022:482) om elektronisk kommunikation (LEK)

Post- och telestyrelsens avgörande

Post- och telestyrelsen (PTS) beslutar att Tele2 Sverige AB (Tele2) ska betala en sanktionsavgift om åtta miljoner etthundra tusen (8 100 000) kronor.

Bakgrund

Redogörelse för tillsynsärendet

I januari och februari 2025 tog PTS emot tre rapporter från Tele2 om inträffade integritetsincidenter. Av incidentrapporterna framgår att Tele2 har lämnat ut för- och efternamn, telefonnummer och adresser för abonnenter med skyddad folkbokföring till företag som bedriver abonnentupplysning. PTS beslutade därför att inleda ett tillsynsärende för att granska Tele2:s efterlevnad av ett urval av bestämmelser i LEK, PTS föreskrifter och allmänna råd (PTSFS 2022:11) om säkerhet i nät och tjänster (säkerhetsföreskrifterna) och 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 (EU-förordning nr 611/2013). PTS inledde tillsynsärendet den 16 april 2025 genom att ställa skriftliga frågor till Tele2.

Den 16 september 2025 underrättade PTS, med stöd av 11 kap. 5 § LEK, Tele2 om misstanke att bolaget har brustit i efterlevnaden av

- 5 kap. 3 § 1 säkerhetsföreskrifterna,
- 6 kap. 2 § säkerhetsföreskrifterna, och
- artikel 3 samt 4 och 6 i bilaga II till EU-förordning nr 611/2013.

I genomförda riskanalyser har Tele2 inte inkluderat hot avseende oavsiktligt utlämnande av uppgifter om abonnenter med skyddad folkbokföring till abonnentupplysning. En av de misstänkta bristerna var därför att Tele2 inte har uppfyllt kraven i 5 kap. 3 § 1 säkerhetsföreskrifterna på att riskanalyser ska innefatta identifiering av relevanta hot mot aktuella informationsbehandlingstillgångar.

Den misstänkta överträdelsen av 6 kap. 2 § säkerhetsföreskrifterna var att Tele2 inte har vidtagit tekniska och organisatoriska åtgärder för att hantera en risk som bolaget borde ha bedömt skulle undvikas eller reduceras.

Vad gäller EU-förordning nr 611/2013 har Tele2 inte lämnat den information som ska lämnas till abonnenter som drabbas av ett personuppgiftsbrott enligt artikel 3 samt 4 och 6 i bilaga II till förordningen. Enligt dessa punkter ska en anmälan innehålla uppskattat datum för incidenten och förmodade konsekvenser av personuppgiftsbrottet för berörda abonnenter.

Av underrättelsen framgår att PTS ska besluta att ta ut sanktionsavgift av Tele2 vid överträdelser av ovan bestämmelser.

Tele2 gavs tillfälle att yttra sig över underrättelsen och inkom med ett yttrande den 6 oktober 2025.

Tele2:s uppgifter om incidenterna i incidentrapporter och yttranden

Tele2 har lämnat ut namn och mobilnummer för 1 229 Comviq-kunder och 119 Tele2-kunder med skyddad folkbokföring till tre abonnentupplysningsföretag. I förhållande till 1 310 av dessa mobiltelefonikunder har även postadressen till Skatteverkets förmedlingsuppdrag delats för personer med skyddad folkbokföring. För resterande 38 kunder delades de folkbokföringsadresser som abonnenterna hade innan de fick skyddad folkbokföring.

Det varierar hur länge de tre abonnentupplysningsföretagen hade tillgång till berörda uppgifter. Vad gäller de 38 kunderna där folkbokföringsadressen röjdes hade företagen tillgång till namn, telefonnummer och adress som längst från december 2024 fram till dess att Tele2 upptäckte incidenten i februari 2025. För de andra 1 310 kunderna var uppgifterna tillgängliga som längst från maj 2024 fram till februari 2025. Mediantiden för samtliga drabbade abonnenter var 50–60 dagar som uppgifterna om dem delades med abonnentupplysningsföretagen.

I vart fall en del av de delade abonnentuppgifterna har varit sökbara och synliga för allmänheten på abonnentupplysningsföretags webbplatser. Tele2 saknar närmare insyn i hur abonnentupplysningsföretagen har hanterat de mottagna abonnentuppgifterna.

Den oavsiktliga uppgiftsdelningen orsakades av en programvarubugg i samband med migrering av abonnentuppgifter till ett CRM-system (customer relationship management). Programvarubuggen återställde flaggningen som styr vilka uppgifter som skickas till abonnentupplysning.

Innan migreringen till CRM-systemet genomförde Tele2 bland annat tester kring om en tidigare flaggning för skyddade personuppgifter behölls. Bolaget testade dock inte huruvida flaggningen fick genomslag i informationsflödena till abonnentupplysningsföretagen.

Tele2 underrättade de drabbade abonnenterna om det inträffade per sms den 8 februari 2025. Tele2 kontaktade dessutom två av abonnenterna per telefon eftersom de fortfarande hade sina uppgifter synliga på en av abonnentupplysningsföretagens webbplatser. Tele2 har i incidentrapporteringen till PTS inkluderat innehållet i två olika sms. Det som skiljer sms:en åt är informationen om vilken typ av uppgifter som har delats med abonnentupplysningsföretagen. I sms:en uppmanas abonnenterna att ta kontakt med kundservice på ett särskilt nummer för att få mer information. Inom ramen för incidentrapporteringen bifogade Tele2 manus, ”FAQ” (frequently asked questions), för kundtjänstagenterna.

Tele2 har vidtagit åtgärder genom att rätta flaggningarna i CRM-systemet som gjorde att abonnentuppgifterna felaktigt lämnades ut. Sedan incidenterna rapporterades till PTS har Tele2 även infört en manuell kontroll som ett sista steg innan abonnentuppgifter skickas till abonnentupplysning. Kontrollen ska upptäcka och i förekommande fall rätta eventuella diskrepanser mellan flaggning och status enligt Skatteverket, där Skatteverkets information om skyddade personuppgifter alltid ska anses vara korrekt. Arbete pågår med att automatisera denna process.

Tele2 har tidigare bedömt att några hot avseende felaktigt utlämnande av abonnentuppgifter om abonnenter med skyddade personuppgifter inte har varit relevanta att inkludera i riskanalyserna. Incidenterna som Tele2 rapporterade till PTS i januari och februari 2025 visar att denna bedömning var felaktig. Bedömningen gjordes med utgångspunkt i att det endast är Skatteverket som ska ha adressuppgifter om personer med skyddade personuppgifter och att Tele2 endast ska ha tillgång till nummer- och namnuppgifter. Någon hänsyn togs inte till förhållandena att Tele2 kan ha adressuppgifter från tidpunkten innan kunden erhöll skyddade personuppgifter. Hänsyn togs inte heller till att uppdateringar som ska ta bort tidigare uppgifter om kunder med skyddade personuppgifter kan misslyckas. I Tele2:s riskanalyser avseende utlämnande av uppgifter till abonnentupplysningsföretag som ska uppdateras under 2025 kommer dessa nya hot, hänförliga till skyddade personuppgifter, att inkluderas.

Tele2:s yttrande över underrättelsen

Tele2 anser att PTS underrättelse om misstanke om att bolaget har brustit i efterlevnaden av 5 kap. 3 § säkerhetsföreskrifterna saknar grund. PTS bedömning att Tele2 borde ha inkluderat hotet om oavsiktlig delning av uppgifter hänförliga till personer med skyddade personuppgifter med abonnentupplysning motsägs av och är oförenligt med säkerhetsföreskrifterna. I föreskrifterna ställs krav på att operatörer lär sig av historien och löpande uppdaterar sina hotbeskrivningar och riskanalyser med beaktande av de incidenter som har inträffat. Operatörerna förutsätts emellertid inte kunna förutspå framtiden. Att det finns tidigare okända hot som en operatör inte har anledning att inkludera i sina riskanalyser förrän efter det att de har materialiserats och orsakat en incident är alltså ett grundantagande i PTS föreskrifter. PTS bedömning i denna del är även oförenlig med och motsägs av ett tidigare beslut att avsluta ett tillsynsärende avseende Tele2 under 2023 utan åtgärd. Det finns inga formuleringar i avslutsbeslutet som antyder att Tele2 borde ha inkluderat hot i riskanalyserna som adresserar frågan om oavsiktlig delning av uppgifter hänförliga till personer med skyddade personuppgifter.

Tele2 anser att misstanken om överträdelse av 6 kap. 2 § säkerhetsföreskrifterna saknar grund. PTS bedömning i denna del motsägs av och är oförenligt med säkerhetsföreskrifterna. Eftersom Tele2 inte har identifierat aktuellt hot i sina riskanalyser har det inte funnits någon risk att hantera genom säkerhetsåtgärder.

Tele2 anser att bolaget hade goda, legitima och rimliga skäl att utelämna de uppgifter som ska lämnas enligt punkt 4 i bilaga II till EU-förordning nr 611/2013 i meddelandena till de drabbade abonnenterna. När sms:en skickades kunde Tele2 inte med säkerhet ange något eller några datum för incidenten. Antalet dagar som informationen felaktigt var exponerad varierar mellan abonnenterna. En uppskattning av datumet för incidenten hade riskerat att innehålla en felmarginal på sex månader för vissa abonnenter. Med en sådan potentiellt betydande felmarginal kan en uppskattning inte länge anses fylla något rimligt syfte.

Tele2 hade även goda, legitima och rimliga skäl att utelämna de uppgifter som ska lämnas enligt punkt 6 i bilaga II till EU-förordning nr 611/2013. Tele2 informerade abonnenterna om att deras personuppgifter felaktigt varit exponerade. Det fanns inget behov av att förklara för en abonnent vad detta innebär särskilt då det endast är abonnenterna och berörda offentliga myndigheter, och inte Tele2, som vet på vilka grunder som abonnenterna har begärt och erhållit skyddade personuppgifter. Det kan inte finnas något som Tele2 kan delge i detta sammanhang som abonnenterna inte redan vet.

Skälen för avgörandet

Tillämpliga bestämmelser

Sanktionsavgift

Enligt 12 kap. 1 § 8 LEK ska PTS besluta att ta ut en sanktionsavgift av den som inte vidtar åtgärder för att säkerställa skydd av uppgifter som behandlas i samband med tillhandahållandet av en tjänst i enlighet med 8 kap. 6 § LEK eller föreskrifter som har meddelats med stöd av den paragrafen. Vidare ska PTS enligt 12 kap. 1 § 10 LEK besluta att ta ut en sanktionsavgift av den som inte underrättar om integritetsincidenter i enlighet med 8 kap. 8 § eller EU-förordning nr 611/2013.

Av 12 kap. 2 § LEK följer att en sanktionsavgift ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor. 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.

PTS får 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.

En sanktionsavgift ska enligt 12 kap. 5 § LEK betalas till PTS inom 30 dagar från det att beslutet om att ta ut avgiften vunnit laga kraft eller inom den längre tid som anges i beslutet.

Skydd av uppgifter vid tillhandahållande av tjänster

Enligt 8 kap. 6 § första, tredje och fjärde styckena LEK ska den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas. Åtgärderna ska vara ägnade att säkerställa en nivå på säkerheten som, med hänsyn till tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsincidenter. Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om sådana skyddsåtgärder.

Begreppet integritetsincident definieras i 1 kap. 7 § LEK som en händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster.

Riskanalyser

Enligt 5 kap. 1 § säkerhetsföreskrifterna ska tillhandahållaren genomföra riskanalyser. I en riskanalys ska tillhandahållaren analysera risken för att tillgångar, informationsbehandlingstillgångar eller förbindelser orsakar eller drabbas av säkerhets- eller integritetsincidenter. Riskanalyser ska göras för varje tillgång, informationsbehandlingstillgång och förbindelse.

Enligt 5 kap. 3 § säkerhetsföreskrifterna ska riskanalyserna innefatta åtminstone

1. identifiering av relevanta hot mot den aktuella tillgången, informationsbehandlingstillgången eller förbindelsen som kan leda till att en säkerhets- eller integritetsincident inträffar,
2. en bedömning av vilka konsekvenser som kan uppstå i händelse av att identifierade hot realiseras,
3. en bedömning av sannolikheten för att identifierade hot realiseras, och
4. en sammanvägd bedömning av sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra om de realiseras (riskbedömning).

Begreppet informationsbehandlingstillgång definieras i 2 kap. 2 § säkerhetsföreskrifterna som system, databaser och fysiska resurser som används för informationsbehandling.

Riskhantering och åtgärder efter riskbedömning

Enligt 6 kap. 1 § säkerhetsföreskrifterna ska tillhandahållaren utifrån riskbedömningen besluta hur respektive risk ska hanteras genom att avgöra om riskerna ska undvikas, reduceras eller accepteras. Sådana beslut ska dokumenteras. Beslut om att acceptera en risk ska motiveras.

Enligt 6 kap. 2 § första stycket säkerhetsföreskrifterna ska tillhandahållaren vidta tekniska och organisatoriska åtgärder för att hantera de risker som ska undvikas eller reduceras. Åtgärderna ska vidtas på en nivå som är anpassad till den risk som föreligger, med beaktande av tillgänglig teknik och kostnaderna för åtgärderna.

Upplysning om bestämmelser om rapportering av integritetsincidenter

I 17 kap. 7 § säkerhetsföreskrifterna anges att bestämmelser om rapportering av integritetsincidenter finns i EU-förordning nr 611/2013.

EU-förordning nr 611/2013

Av artikel 3.1 i EU-förordning nr 611/2013 följer att om ett personuppgiftsbrott kan antas inverka menligt på en abonnents eller en enskild persons personuppgifter eller integritet ska leverantören av den allmänt tillgängliga elektroniska

kommunikationstjänsten underrätta abonnenten eller den enskilda personen om personuppgiftsbrottet.

När det ska fastställas om ett personuppgiftsbrott kan antas inverka menligt på en abonnents eller enskild persons personuppgifter eller integritet ska enligt artikel 3.2 i synnerhet följande omständigheter beaktas:

a) De berörda personuppgifternas art och innehåll, i synnerhet när de avser finansiell information, särskilda kategorier av uppgifter enligt artikel 8.1 i direktiv 95/46/EG samt lokaliseringsdata, internetloggar, webbläsarhistorik, uppgifter om e-post och specificerade samtalslistor.
b) Personuppgiftsbrottets troliga konsekvenser för den berörda abonnenten eller enskilda personen, i synnerhet om brottet skulle kunna medföra identitetsstöld eller bedrägeri, fysisk skada, psykiska men, förödmjukelse eller skadat rykte.
c) Omständigheterna för personuppgiftsbrottet, i synnerhet om uppgifterna har stulits eller om leverantören vet att uppgifterna finns hos en obehörig tredje part.

Av bilaga II till förordningen framgår att anmälan till en drabbad abonnent ska innehålla följande information.

1. Leverantörens namn.
2. Identitet och kontaktuppgifter för personuppgiftsombudet eller andra kontaktpunkter där mer information kan erhållas.
3. Sammanfattning av den incident som orsakade personuppgiftsbrottet.
4. Uppskattat datum för incidenten.
5. De berörda personuppgifternas art och innehåll enligt artikel 3.2.
6. Förmodade konsekvenser av personuppgiftsbrottet för den berörda abonnenten eller enskilda personen enligt artikel 3.2.
7. Omständigheterna kring personuppgiftsbrottet enligt artikel 3.2.
8. Åtgärder som leverantören vidtagit för att åtgärda personuppgiftsbrottet.
9. Åtgärder som leverantören rekommenderar för att mildra den tänkbara menliga inverkan.

Begreppet personuppgiftsbrott definieras i artikel 2 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation som ett brott mot säkerhetsbestämmelserna som leder till oavsiktlig eller olaglig utplåning, förlust, ändring, otillåtet avslöjande eller åtkomst av personuppgifter som överförs, lagras eller på annat sätt behandlas i samband med tillhandahållandet av allmänt tillgänglig elektronisk kommunikationstjänst inom unionen.

PTS bedömning

Tele2 har brustit i regelefterlevnaden

Allmänt om skyddsåtgärder

Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster har ett ansvar att skydda de uppgifter som behandlas i samband med tillhandahållandet. Integritetsincidenter som kan uppstå när sådana uppgifter inte skyddas kan leda till allvarliga konsekvenser för enskilda abonnenter. Dessutom kan integritetsincidenter försvaga allmänhetens tillit till elektroniska kommunikationstjänster. PTS har meddelat föreskrifter om sådana skyddsåtgärder (säkerhetsföreskrifterna).

Tele2 har inte identifierat relevanta hot i riskanalyserna

Det har framkommit att de namn, telefonnummer och adresser som lämnades ut till abonnentupplysningsföretagen hämtades från Tele2:s CRM-system. Det har också framkommit att Tele2 vid tidpunkten för de inträffade incidenterna hade riskanalyser avseende utlämnande av uppgifter till abonnentupplysningsföretag. Dessa riskanalyser innefattade dock inte några hot hänförliga till personer med skyddade personuppgifter, inbegripet oavsiktlig delning av uppgifter om sådana abonnenter med abonnentupplysning.

Enligt 5 kap. 3 § 1 säkerhetsföreskrifterna ska de riskanalyser som ska genomföras enligt 1 och 2 §§ samma kapitel innefatta identifiering av relevanta hot mot varje informationsbehandlingstillgång, i det här fallet aktuellt CRM-system med abonnentuppgifter. Att relevanta hot identifieras är en förutsättning för att en tillhandahållare ska kunna göra adekvata riskbedömningar och vidta lämpliga skyddsåtgärder.

Med utgångspunkt i de inträffade integritetsincidenterna får det anses uppenbart att oavsiktligt utlämnande av abonnentuppgifter för personer med skyddade personuppgifter är ett relevant hot i den mening som avses i 5 kap. 3 § 1 säkerhetsföreskrifterna. Att det handlar om ett relevant hot och ett hot som Tele2:s riskanalyser därmed ska innefatta förefaller även vara ostridigt eftersom Tele2 har uppgett att bolagets riskanalyser ska uppdateras med ett sådant hot under 2025.

Nästa fråga som PTS ska ta ställning till är om Tele2 borde ha insett att det var ett relevant hot att inkludera i riskanalyserna tidigare och innan det att röjandet av abonnentuppgifter inleddes i maj 2024.

PTS konstaterar att detta inte är första gången som Tele2 felaktigt har delat uppgifter om sina kunder med abonnentupplysningsföretag. Under 2023 granskade PTS bland annat Tele2:s skyddsåtgärder vid uppgiftsdelning med abonnentupplysning. Bakgrunden till tillsynen var att PTS 2021–2023 hade mottagit incidentrapporter från

flera tillhandahållare om att abonnentuppgifter felaktigt lämnats ut. För Tele2:s del handlade det om att en migrering av kunder från ett tidigare varumärke 2021 och en intern systemförändring 2023 hade resulterat i att uppgifter delats med abonnentupplysning utan kunders samtycken. Visserligen grundade sig dessa integritetsincidenter i avsaknaden av samtycke och det handlade inte om abonnenter med skyddade personuppgifter. PTS framhöll dock i 2023 års tillsynsärende att det i incidentrapporter från andra tillhandahållare hade framkommit att abonnentuppgifter rörande personer med skyddade personuppgifter hade röjts med potentiellt allvarliga konsekvenser. PTS lyfte dessa omständigheter både i begäran om uppgifter som skickades till Tele2 och i myndighetens beslut att avsluta tillsynen. PTS frågade även Tele2 specifikt om bolagets riskarbete kopplat till utlämnande av uppgifter till abonnentupplysning för kunder med skyddade personuppgifter.

Av ovan framgår sammanfattningsvis att Tele2 tidigare felaktigt har delat abonnentuppgifter med företag som bedriver abonnentupplysning. Inom ramen för PTS tillsyn under 2023 uppmärksammades Tele2 på att andra tillhandahållare hade röjt uppgifter om personer med skyddade personuppgifter och allvarligheten i det inträffade. Tele2 ombads då även att redogöra för bolagets riskhantering i förhållande till just personer med skyddade personuppgifter i aktuell kontext. PTS konstaterar att Tele2 mot bakgrund av dessa omständigheter haft förutsättningar att inse att oavsiktlig delning av namn, telefonnummer och adresser för personer med skyddade personuppgifter kunnat inträffa och att det därmed är ett relevant hot att ta med i riskanalysen Aktuella omständigheter borde också ha fått Tele2 att i ett tidigare skede identifiera oavsiktligt röjande av abonnentuppgifter hänförliga till personer med skyddade personuppgifter som ett relevant hot i bolagets riskanalyser.

När den oavsiktliga delningen av uppgifter påbörjades i maj 2024 hade Tele2 flaggningar för personer med skyddade personuppgifter avsedda att hindra uppgiftsdelning till abonnentupplysning. Tele2 tog emot informationen från Skatteverket om vilka abonnenter som hade skyddade personuppgifter. Även innan aktuella incidenter inträffade verkar Tele2 alltså ha känt till att bolaget behandlade uppgifter om personer med skyddade personuppgifter. Vidare tolkar PTS flaggningarna i CRM-systemet som att Tele2 betraktar uppgifter hänförliga till denna abonnentgrupp som särskilt skyddsvärda. Sammantaget tycks det ha funnits en medvetenhet hos Tele2 både om att bolaget behandlade denna typ av uppgifter och deras behov av skydd i kontexten uppgiftsdelning med abonnentupplysning. PTS anser att detta är en ytterligare omständighet som gör att Tele2 borde inkluderat hotet i bolagets riskanalyser i ett tidigare skede.

Tele2 har förklarat att bolaget missat att ta hänsyn till att de kunde ha kvar adressuppgifter från tidpunkten innan en kund fick skyddade personuppgifter. Någon hänsyn togs inte heller till att uppdateringar som ska ta bort gamla adressuppgifter

kan misslyckas. Tele2:s uppgifter om förbiseenden kring vilka adressuppgifter bolaget behandlar förändrar inte PTS bedömning att Tele2:s riskanalyser borde ha innefattat oavsiktligt utlämnande av abonnentuppgifter för personer med skyddade personuppgifter. PTS noterar också att det inte bara var adressuppgifter som lämnades ut till de tre abonnentupplysningsföretagen utan även namn och telefonnummer.

Tele2 har uppgett att PTS bedömning är oförenlig med myndighetens beslut att avsluta ovan berört tillsynsärende under 2023 utan åtgärd. Det är i sig riktigt att PTS förra granskning av Tele2:s arbete med skydd av abonnentuppgifter vid uppgiftsdelning med abonnentupplysning avslutades utan några fastställda regelöverträdelser. På PTS frågor i det ärendet uppgav dock Tele2 att bolaget saknade de uppgifter som efterfrågas av abonnentupplysningsföretag i förhållande till personer med skyddade personuppgifter. Vidare beskrev Tele2 att bolaget därmed inte kan lämna ut de uppgifter som efterfrågas av abonnentupplysningsföretagen. Detta har visat sig inte stämma då Tele2 nu har röjt uppgifter som bolaget behandlat just om personer med skyddade personuppgifter. PTS bedömning i denna del i tillsynsärendet 2023 utgick således från felaktiga uppgifter som Tele2 hade lämnat.

Vad gäller Tele2:s uppgifter om att bolaget inte kan förutsättas förutspå framtiden vill PTS understryka följande. Det framgår av 5 kap. 1 § säkerhetsföreskrifterna att i en riskanalys ska tillhandahållaren analysera risken för att bland annat informationsbehandlingstillgångar orsakar eller drabbas av säkerhets- eller integritetsincidenter. Av 5 kap. 3 § 1 säkerhetsföreskrifterna framgår vidare att tillhandahållaren ska identifiera relevanta hot mot informationsbehandlingstillgången som kan leda till att en säkerhets- eller integritetsincident inträffar. PTS säkerhetsföreskrifter ställer således krav på att riskanalysen ska vara framåtblickande.

Mot bakgrund av det som anförts ovan är PTS samlade bedömning följande. Oavsiktligt utlämnande av abonnentuppgifter för personer med skyddade personuppgifter har under aktuella omständigheter varit ett relevant hot i den mening som avses i 5 kap. 3 § 1 säkerhetsföreskrifterna. Tele2 borde ha insett att det var ett relevant hot att inkludera i riskanalyserna tidigare och innan det att röjandet av abonnentuppgifter inleddes i maj 2024. Tele2 har därmed brustit i efterlevnaden av 5 kap. 3 § 1 säkerhetsföreskrifterna.

Tele2 har inte vidtagit tekniska och organisatoriska åtgärder för att skydda abonnentuppgifterna

Enligt 5 kap. 3 § 4 säkerhetsföreskrifterna ska en tillhandahållares riskanalyser också innefatta en riskbedömning. Riskbedömningen är en sammanvägd bedömning av

sannolikheten för att identifierade hot inträffar och de konsekvenser det kan medföra om de realiseras. Enligt 6 kap. 1 och 2 §§ säkerhetsföreskrifterna ska riskbedömningen sedan ligga till grund för tillhandahållarens riskhantering och skyddsåtgärder.

Eftersom Tele2 inte har tagit upp ett relevant hot i riskanalysen följer det naturligt att det inte finns en anknytande riskbedömning eller dokumenterad bedömning av vilka åtgärder som ska ha vidtagits. Om Tele2 däremot hade identifierat hotet och gjort en riskbedömning ser PTS det som uteslutet att en risk som innebär att skyddade personuppgifter kan delas obehörigen skulle ha accepterats av Tele2. Under aktuella omständigheter har Tele2 haft en skyldighet att genomföra tekniska och organisatoriska åtgärder för att adressera risken. Den bristfälliga riskanalysen har med andra ord inte befriat Tele2 från skyldigheten att skydda aktuella abonnentuppgifter. Den fråga PTS har att ta ställning till är om Tele2 ändå kan anses ha gjort vad som rimligen kan efterfrågas för att hantera risken att skyddade personuppgifter röjs.

Av 6 kap. 2 § säkerhetsföreskrifterna framgår att åtgärderna ska vara på en nivå som är anpassad till den risk som föreligger, med beaktande av tillgänglig teknik och kostnaderna för åtgärderna. Beträffande risken kan det konstateras att PTS inledde tillsynen 2023 efter att Tele2 och andra tillhandahållare rapporterat om integritetsincidenter i samband med delning av uppgifter med abonnentupplysning. Därefter har Tele2 i incidentrapporterna från 2025 uppgett att uppgifter om 1 348 abonnenter med skyddade personuppgifter oavsiktligt delades med och var tillgängliga hos abonnentupplysningsföretag under perioden maj 2024 – februari 2025. Det faktum att incidenter återkommande inträffat under flera års tid visar på en förhållandevis hög risk för integritetsincidenter vid utlämnande av uppgifter till abonnentupplysning. Att Tele2 som huvudregel är skyldiga att lämna ut vissa abonnentuppgifter med hög frekvens till abonnentupplysning är också en omständighet som enligt PTS innebär en förhöjd risk.[1] Att abonnentuppgifterna avser utsatta individer är ytterligare en högriskfaktor.

Det förhållandet att abonnentuppgifter om 1 348 personer med skyddade personuppgifter delades med flera abonnentupplysningsföretag under flera månaders tid utgör en stark indikation på att Tele2 inte har haft skyddsåtgärder som varit anpassade till risken. Vid en granskning av Tele2:s redogörelse för det inträffade kan PTS också se brister i säkerhetsarbetet.

Det har framkommit att Tele2 inte testade huruvida en tidigare flaggning för skyddade personuppgifter fick genomslag i informationsflödena till

[1] Se 7 kap. 38 § LEK och Post- och telestyrelsens föreskrifter (PTSFS 2022:2) om skyldighet att lämna ut abonnentuppgifter.

abonnentupplysningsföretagen. Eftersom syftet med flaggningen just var att styra uppgiftsdelningen var det en brist att Tele2 inte testade om flaggningen fick avsedd effekt efter migreringen av abonnentuppgifter till CRM-systemet. Dessutom har Tele2 själva medgett att de genomförda testerna var bristfälliga.

Det har också framkommit att Tele2 nu har infört en kontroll som ska upptäcka och rätta eventuella diskrepanser mellan flaggningen i Tele2:s system och Skatteverkets information om skyddade personuppgifter. Det framstår som att det inträffade inte hade behövt ske om en jämförande kontroll av detta slag tidigare hade varit implementerad i Tele2:s verksamhet. Hade till exempel en programvarubugg resulterat i att flaggningen felaktigt ändrades i Tele2:s CRM-system med abonnentuppgifter borde en kontroll gentemot Skatteverkets uppgifter ha hindrat ett felaktigt utlämnande. Tele2 verkar istället ha förlitat sig på bolagets systems förmåga att bibehålla korrekt flaggning angående skyddade personuppgifter vid migreringen av abonnentuppgifterna till CRM-systemet. Avsaknaden av åtgärd för att säkerställa att dessa särskilt skyddsvärda uppgifter inte delades med abonnentupplysning utgjorde även det enligt PTS en brist i Tele2:s säkerhetsarbete. PTS kan inte heller se att tillgänglig teknik eller kostnader kan ha utgjort ett hinder mot att vidta denna typ av skyddsåtgärder i ett tidigare skede.

Tele2:s tolkning av PTS föreskrifter tycks vara att om ett hot inte har identifierats i genomförda riskanalyser så existerar ingen risk som ska hanteras. Vidare har Tele2 invänt att det inte går att ställa krav på tekniska och organisatoriska åtgärder för att skydda exempelvis konfidentaliteten hos behandlade abonnentuppgifter om ett hot inte har identifierats i en riskanalys. Med anledning av detta vill PTS framhålla att 6 kap. 2 § säkerhetsföreskrifterna handlar om de tekniska och organisatoriska åtgärder som enligt 8 kap. 6 § LEK ska vidtas för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av kommunikationstjänster skyddas. Avsikten med 6 kap. säkerhetsföreskrifterna är att konkretisera och precisera arbetet en tillhandahållare ska vidta för att leva upp till bland annat denna lagstadgade skyldighet att vidta skyddsåtgärder. PTS föreskrifters struktur och innehåll inskränker inte denna skyldighet. Det vore dessutom orimligt om en tillhandahållare kunde undslippa ansvar att vidta tekniska och organisatoriska skyddsåtgärder enligt 6 kap. 2 § säkerhetsföreskrifterna enbart på den grunden att tillhandahållaren valt eller missat att inkludera ett visst hot i sina riskanalyser.

Mot bakgrund av det som anförts ovan är PTS samlade bedömning följande. Om Tele2 hade identifierat aktuellt hot i riskanalysen i enlighet med 5 kap. 3 § 1 säkerhetsföreskrifterna hade Tele2 i den anknytande riskbedömningen kommit fram till att risken skulle undvikas eller reduceras i enlighet med 6 kap. 1 § säkerhetsföreskrifterna. Under sådana omständigheter innebär Tele2:s bristfälliga riskanalys inte att bolaget undantas från skyldigheten att skydda aktuella

abonnentuppgifter i enlighet med 6 kap. 2 § säkerhetsföreskrifterna. När incidenterna inträffade maj 2024–februari 2025 hade Tele2 inte vidtagit tillräckliga tekniska och organisatoriska åtgärder för att skydda uppgifterna från att lämnas vidare till abonnentupplysningsföretagen. Detta resulterade i att de 1 348 abonnenterna med skyddad folkbokföring fick sina uppgifter utlämnade. Tele2 har därmed brustit i efterlevnaden av 6 kap. 2 § säkerhetsföreskrifterna.

Tele2 har inte lämnat information om uppskattat datum för incidenten i anmälan till de drabbade abonnenterna

PTS bedömer det inträffade som ett personuppgiftsbrott som kunde antas inverka menligt på abonnenternas personuppgifter eller integritet. Enligt artikel 3 i EU-förordning nr 611/2013 var Tele2 därmed skyldiga att underrätta de drabbade abonnenterna. Tele2:s SMS till abonnenterna visar att bolaget delar den bedömningen.

I bilaga II till förordningen finns nio punkter som specificerar vilken information Tele2 hade att lämna. Enligt punkten 4 ska informationen till abonnenterna innefatta uppskattat datum för incidenten. Det är ostridigt att sms:en som Tele2 skickade till de drabbade abonnenterna inte innehöll någon sådan information. Det är också ostridigt att FAQ:n som Tele2:s kundtjänst använde inte innehöll någon information om uppskattat datum för incidenten. Den enda informationen om tidsaspekten var att det i FAQ:n stod att omfattningen av problemet uppdagades den 7 februari 2025. Att lämna information om när Tele2 upptäckte omfattningen av det inträffade är inte samma sak som att informera om ett uppskattat datum för incidenten. PTS konstaterar således att informationen som Tele2 lämnade till de 1 348 drabbade abonnenterna inte motsvarar informationskravet i punkten 4 i bilaga II EU-förordning nr 611/2013.

I bilaga I till EU-förordning nr 611/2013 anges vilken information som ska lämnas till PTS vid inträffade integritetsincidenter. PTS har tagit fram ett formulär för rapportering av integritetsincidenter som är baserat på bilaga I. I bilaga I till förordningen och i PTS formulär görs en distinktion mellan när incidenten inträffade och när incidenten upptäcktes. Tele2 har vid rapporteringen av incidenterna som ligger till grund för aktuellt tillsynsärende, och vid tidigare rapportering av integritetsincidenter till PTS, fyllt i detta formulär. Det borde därmed ha varit tydligt för Tele2 att informationen som bolaget lämnade till abonnenterna inte var förenlig med kravet i punkten 4 i bilaga II till EU-förordning nr 611/2013.

PTS noterar att Tele2 skickade sms:en till de berörda abonnenterna den 8 februari 2025. Dagen efter, dvs. den 9 februari 2025, rapporterade Tele2 till PTS att vissa av uppgifterna hade lämnats ut till abonnentupplysningsföretagen redan i maj 2024. Tele2 har förklarat att vid tillfället för utskicket av sms:en kunde bolaget inte

med säkerhet ange något eller några datum för incidenten. Av punkten 4 bilaga II till EU-förordning nr 611/2013 framgår emellertid att det är tillräckligt att göra en uppskattning av datum för incidenten.

Tele2 anser vidare att bolaget hade skäl att utelämna aktuell information då en uppskattning hade riskerat att innehålla en felmarginal på sex månader för vissa abonnenter. PTS bedömer dock att Tele2 hade kunnat lämna information till abonnenterna om uppskattat datum för incidenten i form av ett tidsintervall. Tele2 hade då också, precis som i incidentrapporteringen till PTS, kunnat precisera att det förekommer individuella variationer kring hur länge uppgifterna var exponerade. På så sätt hade Tele2 kunnat uppfylla informationskravet utan att behöva lämna felaktig information.

Eftersom de drabbade abonnenterna hade skyddad folkbokföring får det antas att de vid tillfället för incidenterna hade en hotbild mot sig. Dessa abonnenter fick ett sms från Tele2 om att deras namn, telefonnummer, och i vissa fall adress, under en tid kan ha varit tillgängliga på olika söktjänster. När det handlar om en särskilt utsatt kundgrupp är det extra viktigt att abonnenterna får all den information som ska lämnas i enlighet med regelverket. PTS uppfattning är också att abonnenterna hade kunnat skapa sig en bättre bild av det inträffade om de hade fått en uppskattning av tidsomfånget för incidenten, om än ett intervall på flera månader, jämfört med att inte få någon sådan information alls.

Mot bakgrund av ovanstående resonemang är PTS samlade bedömning att Tele2 har brustit i efterlevnaden av artikel 3 och punkten 4 i bilaga II till EU-förordning nr 611/2013.

Tele2 har inte lämnat information om förmodade konsekvenser av personuppgiftsbrottet i anmälan till de drabbade abonnenterna

Enligt punkten 6 i bilaga II till EU-förordning nr 611/2013 ska informationen även inbegripa de förmodade konsekvenserna för abonnenterna. Enligt artikel 3.2 i EU-förordning nr 611/2013 ska det i synnerhet beaktas om det inträffade skulle kunna medföra identitetsstöld eller bedrägeri, fysisk skada, psykiska men, förödmjukelse eller skadat rykte.

I formuläret som ska användas vid rapportering av integritetsincidenter till PTS ska tillhandahållaren ange potentiella konsekvenser och potentiell menlig inverkan för de drabbade abonnenterna. I incidentrapporterna som ligger till grund för detta tillsynsärende skrev Tele2 att personer som lever med skyddad folkbokföring i regel har en hotbild riktad mot sig. Tele2 skrev även att ett avslöjande av namn, folkbokföringsadress och telefonnummer i ett offentligt register därför kan medföra fara för liv och hälsa.

Det är ostridigt att Tele2 emellertid inte har inkluderat någon information om förmodade konsekvenser för de drabbade abonnenterna i sms:en eller FAQ:n. PTS förstår att Tele2 inte har haft möjlighet att förutse konsekvenserna av att aktuella uppgifter har läckt till abonnentupplysning på en individnivå. Samtidigt anser PTS alltjämt att det är viktigt att aktuella informationskrav i bilaga II efterlevs särskilt när den inträffade incidenten kan få allvarliga konsekvenser. Tele2 hade kunnat uppfylla informationskravet i punkten 6 genom att lämna samma information till abonnenterna som de lämnade i incidentrapporteringen till PTS. Tele2 hade också exempelvis kunnat komplettera informationen med att det är abonnenten själv som bäst kan bedöma vilka konsekvenser uppgiftsdelningen kan få och att abonnenten därför själv bör tänka igenom detta och vidta relevanta åtgärder. Enligt PTS kan Tele2 dock inte välja att helt hoppa över ett informationskrav med motiveringen att informationen skulle vara överflödig.

Sammantaget bedömer PTS att Tele2 har brustit i efterlevnaden av artikel 3 och punkten 6 i bilaga II till EU-förordning nr 611/2013.

Sanktionsavgift

Påförande av sanktionsavgift

PTS ska ta ut en sanktionsavgift av den som inte uppfyller kraven uppräknade i 12 kap. 1 § LEK. Föreskrifter meddelade med stöd av 8 kap. 6 § LEK och EU-förordning nr 611/2013 ingår i uppräkningen. Tele2 ska därmed påföras en sanktionsavgift för samtliga i ärendet aktuella överträdelser. Intervallet för storleken på avgiften är 5 000 – 10 000 000 kronor. Beloppsgränserna är avsedda att ge utrymme för proportionella, effektiva och avskräckande sanktioner.[2]

Faktorer som PTS ska ta särskild hänsyn till vid bedömningen av avgiftens storlek

Enligt 12 kap. 2 § andra stycket LEK ska PTS vid bedömningen av avgiftens storlek ta särskild hänsyn till den skada eller risk för skada som har uppstått, tidigare överträdelser och kostnader som aktören har undvikit till följd av överträdelsen.

Skada och risk för skada har uppstått

Tele2:s bristfälliga riskanalys och riskhantering har resulterat i en skada. Skadan består i att namn, telefonnummer och i vissa fall tidigare adressuppgifter hänförliga till 1 348 personer med skyddad folkbokföring har delats med och varit tillgängliga hos tre abonnentupplysningsföretag under perioden maj 2024-februari 2025. Det har framkommit att i vart fall en del av de läckta uppgifterna varit synliga på några av de

[2] Prop. 2021/22:136 s. 361 f.

mest använda webbplatserna med söktjänster avseende namn, nummer och adresser.

Aktuella överträdelser har även medfört en risk för skada med allvarliga konsekvenser. Allvarlighetsgraden i det inträffande kan belysas med exempel från Skatteverkets webbplats om när beslut om skyddad folkbokföring kan bli aktuellt. Ett exempel är att en person har utsatts för eller riskerar att utsättas för våld, hot eller liknande. Det kan också handla om att ett beslut om kontaktförbud inte ger tillräckligt skydd. Ett annat exempel är att personen har vittnat angående ett grovt brott.[3]

PTS känner inte till att någon av de drabbade abonnenterna ska ha utsatts för hot, våld eller liknande på grund av de läckta uppgifterna. Med utgångspunkt i vad som kan krävas för beslut om skyddad folkbokföring får dock läckan av abonnentuppgifterna anses ha medfört en risk för skada med allvarliga konsekvenser. Om den eller de som orsakat skyddsbehovet för abonnenten får tag i dennes personuppgifter så kan hotbilden förvärras och leda till skada. Det skulle kunna handla om uppsökande av kontakt med psykisk eller fysisk skada som konsekvens, eller i värsta fall fara för liv.

Att ha en hotbild mot sig och sedan informeras om att ens nummer eller tidigare adress varit offentligt sökbara får också bara det i sig antas ha skapat oro, stress eller liknande hos flera av abonnenterna. Det får också antas att i vart fall en del av de drabbade känt ett behov av att vidta åtgärder som byte av nummer eller till och med adress. Det senare är inte helt osannolikt även om de röjda adresserna var platser där berörda abonnenter var folkbokförda innan de fick skyddad folkbokföring. Detta då även sådan information skulle kunna användas som ett led i att försöka nå eller få tag i någon. Att uppgifterna i många av fallen varit exponerade i flera månader har inneburit en ökad risk för att uppgifterna ska hamna i fel händer. Antalet drabbade abonnenter är ytterligare en försvårande omständighet.

Sammantaget bedömer PTS att omfattningen av det inträffade och risken för allvarlig skada motiverar en hög sanktionsavgift.

Inga tidigare fastslagna överträdelser av liknande slag

PTS har inte i beslut fastslagit att Tele2 begått överträdelser av liknande slag tidigare.

Tele2 har undvikit kostnader

Efter inträffade integritetsincidenter vidtog Tele2 åtgärder för att bättre skydda behandlade abonnentuppgifter. En ny process implementerades för att upptäcka och rätta avvikelser mellan flaggningen i Tele2:s CRM-system och Skatteverkets

[3] Skatteverket.se/privat/folkbokforing/skyddadepersonuppgifter.se, besökt 2025-10-29.

information. Avsaknaden av en sådan kontrollåtgärd var en av orsakerna till att abonnentuppgifterna röjdes. Tele2 har undvikit kostnader genom att inte införa en process av detta slag i ett tidigare skede.

Innan migreringen av abonnentuppgifterna till CRM-systemet genomförde Tele2 tester. Testerna omfattade bland annat om en tidigare flaggning för skyddade personuppgifter behölls. Det testades dock inte huruvida flaggningen fick genomslag i informationsflödena till abonnentupplysningsföretagen. Att genomföra tester inriktade på flaggningens avsedda effekt framstår som relativt grundläggande. Enligt PTS har Tele2 även undvikit kostnader genom att inte genomföra tillräckliga tester.

Ju högre besparing, desto högre bör sanktionsavgiften bli. I aktuellt fall gör PTS bedömningen att det bör handla om relativt begränsade besparingar. Det tycks ha gått förhållandevis snabbt och enkelt för Tele2 att få ovan kontrollåtgärd på plats. PTS beaktar även att Tele2 genomfört vissa tester. Vid en sammanvägd bedömning motiverar redogjorda omständigheter endast en begränsad höjning av avgiften.

Det ska tilläggas att Tele2 inte förmodas ha undvikit några kostnader genom att utelämna uppskattat datum för incidenten och förmodade konsekvenser i informationen till de drabbade abonnenterna.

Andra faktorer som PTS beaktar vid bedömningen

Uppräkningen i 12 kap. 2 § andra stycket LEK över omständigheter som ska beaktas när avgiftens storlek bestäms är inte uttömmande, utan hänsyn kan behöva tas till andra omständigheter. Det kan till exempel vara relevant att beakta hur länge en överträdelse har pågått, tillhandahållarens finansiella ställning eller att den avgiftsskyldige har samarbetat med tillsynsmyndigheten för att komma till rätta med överträdelsen.[4]

Vad gäller tidsaspekten har Tele2 till följd av bristfällig riskanalys och riskhantering felaktigt delat skyddsvärda abonnentuppgifter under en period på över ett halvt år. Detta är en lång period.

Tele2 är ett av de största telekombolagen i Sverige. Tele2 Sverige AB:s årsredovisning för 2024 visar att bolaget omsatte cirka 22 852 000 000 kronor det budgetåret. För att framstå som en effektiv, proportionell och avskräckande åtgärd motiverar överträdelserna och Tele2:s finansiella ställning att Tele2 påförs en sanktionsavgift på den övre delen av beloppsintervallet. Ett lägre belopp än så kan inte antas få en kännbar effekt under aktuella omständigheter.

[4] Prop. 2021/22:136 s. 524.

PTS fick kännedom om det inträffade genom Tele2:s incidentrapportering. Det är positivt och viktigt att tillhandahållare följer sin lagstadgade skyldighet att rapportera incidenter av detta slag.

PTS samlade bedömning av sanktionsavgiftens storlek

Det som Tele2:s bristfälliga riskarbete har resulterat i sticker ut i allvarlighetsgrad vid en jämförelse med de integritetsincidenter som PTS normalt sett tar emot. Det gäller såväl antalet drabbade, tidsomfånget, inträffad skada samt risk för skada. För att sanktionsavgiften ska framstå som en effektiv, proportionell och avskräckande åtgärd läggs även betydande vikt vid Tele2:s finansiella ställning. Att Tele2 får antas ha undvikit vissa kostnader motiverar därutöver ett något högre belopp. Motsvarande förmildrande omständigheter föreligger inte. Vid en sammanvägd bedömning anser PTS att sanktionsavgiften för Tele2:s överträdelse av 5 kap. 3 § 1 säkerhetsföreskrifterna, 6 kap. 2 § säkerhetsföreskrifterna samt artikel 3 och punkt 4 och 6 i bilaga II till EU-förordning nr 611/2013, ska bestämmas till 8 100 000 kronor. Av beloppet är 100 000 kronor hänförligt till överträdelsen av EU-förordningen.

Det saknas skäl att avstå från att ta ut en sanktionsavgift

Det saknas skäl att helt eller delvis avstå från att ta ut en sanktionsavgift med stöd av 12 kap. 2 § tredje stycket LEK.

Betalning av sanktionsavgift

Av 12 kap. 5 § LEK framgår att sanktionsavgiften tillfaller staten. Den faktureras av PTS efter det att beslutet vunnit laga kraft. Betalningen ska vara PTS tillhanda senast inom 30 dagar från fakturadatum.

Underrättelse om överklagande

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

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

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 generaldirektören Dan Sjöblom. Föredragande har varit juristen Markus Sjöberg. I ärendets slutliga handläggning har även divisionschefen Catarina Wretman, avdelningschefen Patrik Bystedt, chefsjuristen Karolina Asp, enhetschefen Anders Franzén, verksjuristen Sofie Sandell, juristen Mats Jönsson och ingenjören Timo Lundqvist deltagit.