FÖRVALTNINGSRÄTTEN I STOCKHOLM

Avdelning 31

DOM
2021-03-18
Meddelad i Stockholm

Mål nr
15589-20

KLAGANDE
Tele2 Sverige AB, 556267-5164

Ombud: [redacted]

MOTPART
Post- och telestyrelsen

ÖVERKLAGAT BESLUT
Post- och telestyrelsens beslut 2020-06-25, se bilaga 1

SAKEN
Tillämpning av lagen om elektronisk kommunikation

FÖRVALTNINGSRÄTTENS AVGÖRANDE

1. Förvaltningsrätten bifaller överklagandet delvis och ändrar tidpunkten för när åtgärderna enligt det överklagade beslutet ska vara uppfyllda till den 30 juni 2021.

2. Förvaltningsrätten avslår överklagandet i övrigt.

Postadress	Besöksadress	Telefon	Telefax	Expeditionstid
115 76 Stockholm	Tegeluddsvägen 1	08-561 680 00 **E-post**: avd31 fst@dom.se www.domstol.se/forvaltningsratten-i-stockholm/	-	måndag–fredag 08:00–16:00

YRKANDEN M.M.

Post- och telestyrelsen (PTS) beslutade den 25 juni 2020, med stöd av 7 kap. 5 § lagen (2003:389) om elektronisk kommunikation (LEK), att förelägga Tele2 Sverige AB (Tele2) att senast den 31 mars 2021 införa en teknisk lösning som säkerställer att kunder som ringer in till kundtjänst är korrekt autentiserade innan kundtjänstmedarbetaren kan lämna ut uppgifter eller göra ändringar i abonnemang. I beslutet angavs bl.a. vidare att en korrekt skyddsåtgärd ska omöjliggöra att information som behandlas i samband med tillhandahållandet av den elektroniska tjänsten kan avslöjas eller ändras på uppmaning av obehörig person via telefonkundtjänst och att den tekniska lösningen ska innebära att autentisering av kunder inte kan ske via en manuell bedömning av kundtjänstpersonal, utan avgörandet om autentiseringen blir godkänd eller ej ska ligga hos den tekniska lösningen. Skälen för beslutet framgår av bilaga 1.

Tele2 yrkar i första hand att förvaltningsrätten upphäver beslutet. I andra hand yrkar bolaget att förvaltningsrätten ändrar det överklagade beslutet och fastställer rättelsetidpunkten till den 30 juni 2021 i stället för den 31 mars 2021.

PTS bestrider bifall till överklagandet.

VAD PARTERNA ANFÖR

Tele2 anför bl.a. följande.

Förstahandsyrkandet

Föreläggandet uppfyller inte gällande krav på tydlighet och precision och går längre än vad som är lagligt möjligt enligt bestämmelsen i 6 kap. 3 § LEK

Ett förvaltningsbeslut måste vara så tydligt utformat att adressaten förstår vad som krävs för att följa detta. Detta gäller såväl beslut om vitesföreläggganden som beslut om förelägganden och förbud som inte är förenade med ett vite. Högsta förvaltningsdomstolen har uttalat att ett vitesföreläggande ska vara formulerat så att adressaten ”måste vidta just de åtgärder som anges i föreläggandet” och att adressaten måste kunna ”säkert ... avgöra om åtgärden innebär att föreläggandet följs eller inte”. Av Högsta förvaltningsdomstolens praxis följer vidare att adressaten ”måste ... få tydliga uppgifter om vad denne ska göra eller underlåta för att följa föreläggandet” och att ”Denna information måste i allt väsentligt framgå av själva föreläggandet.” Högsta förvaltningsdomstolen har sammanfattat kravet på tydlighet och precision avseende vitesförelägganden som att ”den som ett föreläggande riktar sig till måste få helt klart för sig vad som fordras för att det fastställda vitesbeloppet inte ska dömas ut. Vitet måste således vara knutet till en klart definierad prestation eller underlåtenhet.”

Det överklagade föreläggandet lever inte upp till de högt ställda krav på tydlighet och precision som uppställts i praxis. Det kan till att börja med konstateras att enligt vad som anges i första meningen under rubriken ”Post- och telestyrelsens avgörande” i föreläggandet krävs att en kundtjänstmedarbetare inte i något fall får ”lämna ut uppgifter eller göra ändringar i abonnemang” utan att den kund som kontaktar kundtjänsten först autentiserats i en teknisk lösning såsom t.ex. BankID. Föreläggandet går i denna del längre än vad som är lagligt möjligt enligt bestämmelsen i 6 kap. 3 § lagen LEK, eftersom nämnda lagbestämmelse endast avser uppgifter ”som överförs, lagras eller på annat sätt behandlas i samband med tillhandahållandet av en elektronisk kommunikationstjänst” medan

föreläggandets första mening alltså reglerar uppgifter i allmänhet utan någon som helst anknytning till om uppgifterna överförts, lagrats eller på annat sätt behandlats i samband med tillhandahållandet av en elektronisk kommunikationstjänst. I föreläggandets andra mening finns i och för sig en referens till de specifika uppgiftstyper som avses i 6 kap. 3 § LEK, men ingenstans framgår av föreläggandet att andra meningen i föreläggandet är avsedd att begränsa omfattningen av föreläggandets första mening.

PTS har i målet hos förvaltningsrätten uppgett att föreläggandet avser ”uppgifter operatören har tystnadsplikt för enligt LEK”. Vilka uppgifter som omfattas av tystnadsplikt enligt LEK framgår dock inte av 6 kap. 3 § LEK, utan av 6 kap. 20 § LEK. Det är därför även oklart om PTS menar att föreläggandets omfattning regleras av vad som följer av 6 kap. 3 § LEK eller av vad som följer av 6 kap. 20 § LEK.

Med beaktande av föreläggandets mycket ingripande effekter måste denna typ av oklarheter ses som allvarliga, eftersom de innebär att Tele2 inte utan förtydliganden från PTS sida har möjlighet att korrekt efterkomma föreläggandet. Det är t.ex. oklart om Tele2 enligt föreläggandet kan påbörja en försäljning till en inringande kund, oavsett om kunden är existerande eller tillkommande, för att först senare under det påbörjade samtalet begära en autentisering av kunden. Första meningen i föreläggandet skulle kunna anses ge uttryck för att detta inte är tillåtet medan andra meningen synes ge utrymme för detta.

PTS har i målet anfört att med begreppet ”kund” i föreläggandet endast avses befintliga kunder och inte potentiella eller tidigare kunder till Tele2. Detta är dock inget som framgår av föreläggandet utan där talas generellt om ”kunder” utan någon närmare precisering. Tele2 ställer sig också frågande till om PTS verkligen menar att föreläggandet endast tar sikte på befintliga kunder hos Tele2 och t.ex. inte även på tidigare kunder hos Tele2

som i och för sig avslutat sina tjänster hos Tele2 men som t.ex. kanske ringer in till Tele2:s kundtjänst med frågor om en avslutande faktura som kunderna erhållit. På samma sätt framgår det inte av föreläggandet huruvida begreppet kunder omfattar sådana enskilda kunder med vilka Tele2 saknar direkt avtalsrelation, men där kundernas fastighetsägare har ingått ett avtal med Tele2 om tjänstetillhandahållande till kunderna.

Dessa frågor kan synes vara detaljfrågor i sammanhanget, men har i själva verket en mycket stor betydelse för Tele2:s möjligheter att efterkomma föreläggandet. Att föreläggandet inte ger tydligt besked om vilka exakta grupper av personer som är att betrakta som kunder i föreläggandets mening innebär dessutom att det för Tele2 är omöjligt att förstå vad som krävs för att följa föreläggandet. Detta innebär i sin tur att föreläggandet inte lever upp till de högt ställda krav på tydlighet och precision som redogjorts för i det föregående och att föreläggandet därför inte är rättsenligt utan bör upphävas. Detta gäller även om PTS under rättsprocessens gång försöker tydliggöra innebörden av föreläggandet (se RÅ 1990 ref. 39 och RÅ 1994 ref. 29). Enligt Tele2:s mening är det uppenbart att det överklagade föreläggandet inte uppfyller de krav på precision och tydlighet som gäller beslut av denna karaktär vilket är en mycket allvarlig brist eftersom även små förändringar av kravens omfattning (avseende antingen vilka kunder som omfattas eller vilka uppgiftskategorier som omfattas) får mycket stor påverkan på Tele2:s möjligheter och aktiviteter för att efterkomma föreläggandet.

Föreläggandet saknar rättslig grund

Vad sedan gäller kraven enligt föreläggandet på sådana uppgifter som de facto överförts, lagrats eller på annat sätt behandlats i samband med tillhandahållandet av en elektronisk kommunikationstjänst så är det Tele2:s bestämda uppfattning att föreläggandet saknar rättslig grund. Det ska här till

att börja med noteras att, såsom framgår av föreläggandet, bristande autentisering för Tele2:s del har konstaterats vid endast två fall totalt. Detta ska sättas i relation till att Tele2 årligen hanterar cirka två miljoner kundkontakter, dvs autentiseringsbrister har förekommit vid cirka 0,000001 procent av samtliga ärenden. Denna extremt låga procentsats visar att Tele2 i själva verket har vidtagit sådana lämpliga tekniska och organisatoriska åtgärder som krävs för att säkerställa att de uppgifter som överförs, lagras eller på annat sätt behandlas i samband med tillhandahållandet av Tele2:s tjänster skyddas på det sätt som avses i 6 kap. 3 § LEK, dvs. det finns om man ser på Tele2 isolerat ingen legal grund för ett ingripande enligt 7 kap. 5 § LEK.

PTS synes även ha lagt brister hos andra tjänstetillhandahållare till grund för föreläggandet mot Tele2 och synes mena att föreläggandet adresserar ett branschproblem. Detta är en rättstillämpning som Tele2 vänder sig starkt mot. Det enda som är relevant vid bedömningen av om ett föreläggande lagligen kan riktas mot Tele2 är eventuella identifierade brister hos just Tele2. Att låta eventuella brister hos andra tjänstetillhandahållare ligga till grund för ett föreläggande mot Tele2 kan aldrig anses vara acceptabelt. Då det av det överklagade föreläggandet - och med beaktande av det mycket begränsade antalet identifierade fall avseende Tele2 specifikt – dock är uppenbart att PTS agerat just på det sättet i förhållande till Tele2 utgör även detta grund för att upphäva det överklagade föreläggandet, eftersom det helt enkelt saknas rättslig grund för ett ingripande enligt 7 kap. 5 § LEK mot Tele2 specifikt.

Föreläggandet uppfyller inte kraven på proportionalitet

När det sedan gäller kravet i föreläggandet på att en teknisk lösning alltid ska användas för autentisering så bör det till att börja med noteras att Tele2 redan idag har vidtagit en rad säkerhetsåtgärder för att säkerställa en korrekt autentisering av bolagets kunder. PTS synes dock mena att endast en teknisk

lösning av det slag som följer av föreläggandet är god nog. PTS förklarar dock ingenstans i föreläggandet varför det t.ex. inte är tillräckligt med en rutin som säkerställer att känsliga uppgifter endast skickas till en kunds folkbokföringsadress. PTS synes inte heller tillmäta det faktum att Tele2 redan infört krav på BankID-identifiering för sådana processer som kan betraktas som särskilt känsliga någon betydelse. En sådan analys av redan vidtagna åtgärder måste naturligtvis genomföras och redovisas för att en bedömning ska kunna göras i fråga om ytterligare krav är rimliga och det kan i avsaknad av en sådan analys inte anses vara proportionellt att införa den typen av ingripande krav som föreläggandet medför. Sådana krav står i direkt strid med 1 kap. 2 § LEK.

I fråga om rimligheten och proportionaliteten av de tekniska krav som PTS förelagt Tele2 att uppfylla så synes PTS dessutom i föreläggandet ha förbisett en rad problem som införandet av den förelagda tekniska lösningen skulle ge upphov till. Listan på problem kan göras lång, men Tele2 väljer att fokusera på de mest allvarliga bristerna som har det gemensamt att vissa kundgrupper överhuvudtaget inte kommer att kunna få hjälp per telefon med sina tjänster utan kommer att vara hänvisade till att besöka en Tele2-butik, vilket framstår som högst beklagligt särskilt under en pågående pandemi.

De kundgrupper som kommer att drabbas av ovanstående problem är de som av olika skäl inte har möjlighet att legitimera sig med BankID eller en liknande tjänst. Hit hör företrädesvis äldre personer, men även personer som förlorat eller fått sin mobiltelefon med tillhörande mobilt BankID stulen och som ringer in för att spärra sina tjänster mot obehörigt användande. Inte heller kommer enskilda kunder hos en fastighetsägare med vilken Tele2 har avtal (t.ex. kunder som har ett grundutbud av TV-tjänster) kunna ringa in till Tele2:s kundtjänst för att få hjälp med sina tjänster, eftersom Tele2 saknar en direkt avtalsrelation med dessa och därför inte kan legitimera dem via BankID eller liknande lösningar. Vidare kommer problem uppstå för gode

män och förvaltare som saknar BankID eller liknande för de kunder som de representerar. Att avsluta abonnemang för avlidna personer kommer inte heller att fungera per telefon.

Allt det ovanstående visar på orimligheten i PTS generella krav i föreläggandet på införande av en generell teknisk autentiseringslösning. Kravet är helt enkelt alltför ingripande för att det ska kunna anses som rimligt och är direkt oproportionellt med hänsyn till LEK:s syften enligt 1 kap. 1 § LEK. Tele2 har svårt att se hur PTS förslag kan betraktas som rimligt och lagenligt eftersom det går rakt emot Tele2:s kunders intressen och kommer att driva kunder till fysiska butiker under pågående pandemi.

Andrahandsyrkandet

Tele2 har endast medgetts tid till den 31 mars 2021 att efterleva det överklagade föreläggandet. Detta är en orimligt kort tid eftersom Tele2:s kundtjänstmedarbetare arbetar med drygt 20 system avseende bolagets olika varumärken och produkter. Att bygga om dessa dryga 20 system på det sätt föreläggandet kräver är ett mycket stort och tidskrävande IT-projekt. Ett sådant IT-projekt kan inte heller forceras eftersom det riskerar att äventyra möjligheterna för kunderna att på ett fungerande sätt hantera sina tjänster framöver. De sagda tidsmässiga problemen gäller särskilt om föreläggandet ska tolkas som att inte ens Tele2:s kundtjänstmedarbetare får ha access till underliggande system med viss basfakta avseende en kund som inte dessförinnan autentiserat sig (dvs. att systemen då i sin helhet ska vara tekniskt låsta) och att medarbetarna därmed ska vara förhindrade att tex svara på basala frågor från en kund i fråga om dennes tjänst t.ex. fungerar, är avstängd eller spärrad. Tele2 bedömer dock under alla förhållanden att det inte finns faktisk möjlighet för Tele2 att efterkomma PTS meddelade föreläggande i alla delar innan den 30 juni 2021. För det fall förvaltningsrätten skulle avslå

Tele2:s förstahandsyrkande i målet så måste således i vart fall andrahandsyrkandet bifallas. Detta framstår för övrigt som det enda rimliga med hänsyn till den pågående pandemin eftersom det inte rimligen kan vara eftersträvansvärt att under densamma ställa tekniska krav som medför att flera typer av ärenden kommer att behöva hanteras vid fysiska kundbesök i butiker snarare än från distans.

PTS anför bl.a. följande.

Föreläggandet är tydligt

PTS har förelagt Tele2 att senast den 31 mars 2021 införa en teknisk lösning som säkerställer att kunder som ringer in till kundtjänst är korrekt autentiserade innan kundtjänstmedarbetaren kan lämna ut uppgifter eller göra ändringar i abonnemang. En korrekt skyddsåtgärd ska omöjliggöra att information som behandlas i samband med tillhandahållandet av den elektroniska tjänsten kan avslöjas eller ändras på uppmaning av obehörig person via telefonkundtjänst. Den tekniska lösningen ska innebära att autentisering av kunder inte kan ske via en manuell bedömning av kundtjänstpersonal, utan avgörandet om autentiseringen blir godkänd eller ej ska ligga hos den tekniska lösningen. Det ska därmed inte heller vara möjligt att från- eller kringgå rutiner för autentisering.

Av föreläggandets lydelse framgår tydligt att det handlar om kunder som ringer in till kundtjänst. Således avses inte eventuellt blivande kunder, utan någon som redan är kund. Ordet kund i föreläggandet är tillräckligt tydligt för att föreläggandet ska kunna efterlevas av Tele2. Enligt den allmängiltiga definitionen av ordet är en kund till Tele2 en person som köper eller utnyttjar Tele2:s tjänster. Blivande eller tidigare roller som kund omfattas inte av ordet kund.

PTS föreläggande omfattar de uppgifter som faller inom ramen för regleringen i 6 kap. 3 § LEK och 4 § Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter. Föreläggandet är inte heller otydligt i detta avseende. Det finns inte något motsatsförhållande, eller något tolkningsutrymme, mellan mening ett och mening två i föreläggandet. I enlighet med vad som anges i 6 kap. 3 § LEK är det uppgifter som behandlas i samband med tillhandahållandet av tjänsten som ska skyddas bl.a. mot oavsiktlig eller olaglig förstörelse, förlust eller ändring. Skyddsåtgärden i föreläggandet är nödvändig för att skydda dessa uppgifter och för att därmed undvika integritetsincidenter. Det torde stå synnerligen klart för Tele2 att föreläggandet riktar in sig på uppgifter operatören har tystnadsplikt för enligt LEK, som berör en viss kund, och t.ex. inte allmän information om att en viss typ av tjänst ligger nere för ett visst antal kunder i södra Sverige eller dylikt.

Föreläggandet har rättslig grund

Den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst har enligt LEK en skyldighet att vidta nödvändiga skyddsåtgärder för att undvika integritetsincidenter. Tillhandahållaren har också en skyldighet att genomföra åtgärden på en nivå som är lämplig för att hantera en identifierad risk. PTS har genom mottagandet av anmälan om integritetsincidenter 2018 och första halvan 2019 från förelagda tillhandahållare, och därefter vid efterföljande tillsyn under 2019 och första halvan 2020, konstaterat att det finns en identifierad och hög risk för integritetsincidenter som består i otillåtet avslöjande och otillåten ändring av kunders abonnemangsuppgifter och tjänster i abonnemangen. Denna form av integritetsincidenter kan leda till mycket allvarliga konsekvenser för enskilda abonnenters liv, då den skyddsvärda informationen används i brottsligt syfte t.ex. för att skada abonnenten.

Det är den mänskliga bedömningen som sker i varje enskilt fall som skapar risker för att integritetsincidenter ska kunna uppstå. Det är korrekt att Tele2 har gett in två incidentrapporter till PTS under 2018 och första halvan av 2019. PTS noterar dock att ytterligare en rapport inkommit 2019 (dvs. efter att tillsynen startat) där samtalsspecifikation obehörigen har beställts ut via telefonkundtjänst och att en rapport inkommit till PTS den 12 juni 2020 (dvs. efter att Tele2 underrättats) där personal i kundtjänst frångått rutiner och fem abonnenter/personer drabbats av försök till bedrägeri. De två sistnämnda rapporterna låg inte till grund för PTS föreläggande, men visar väl på att det finns risk för att kundtjänst vid Tele2 frångår rutiner. Antalet rapporter till PTS är inte heller ett säkert mått på hur många incidenter som faktiskt förekommit. Antalet incidentrapporter beror i stor utsträckning på tillhandahållarens förmåga att upptäcka incidenter, antingen av kundtjänstmedarbetare, genom att kunden tar kontakt, eller i uppföljande interna kontroller.

Genom de incidentrapporter som PTS har mottagit och genom den tillsyn som har följt, har PTS förstått att andra personer än abonnenten, utan identifiering, har kunnat få ut uppgifter om kunden, om dennes samtal, och kunnat ändra abonnemangsuppgifter. Antalet anmälda incidenter skiljer sig åt mellan de tillhandahållare som PTS granskat, men metoderna för autentisering skiljer sig inte åt i någon större utsträckning. Brister i autentiseringen av personer som ringer till kundtjänst är ett generellt problem hos alla tillhandahållare som ingått i tillsynen. Bristerna behöver kraftigt begränsas för att minimera riskerna för kunderna att utsättas för brott, såsom bedrägerier, identitetskapning, eller brott i nära relation.

Föreläggandet är proportionerligt och i överensstämmelse med LEK:s syften

Den förelagda skyddsåtgärden rör svårigheter med att säkert identifiera kunder i kundtjänst. Syftet är att begränsa utrymmet för mänskliga felbedömningar i kundtjänst. Genom att kräva en tvingande teknisk lösning som säkerställer att befintliga kunder som ringer in till kundtjänst är korrekt identifierade, innan kundtjänstmedarbetaren kan lämna ut uppgifter eller göra ändringar i abonnemang, säkerställs en minskad risk för fel. Den förelagda lösningen innebär att kundtjänstmedarbetaren inte kan välja bort den säkra identifieringen/autentiseringen, något som är möjligt och som förekommer i dagsläget.

De säkerhetsåtgärder som Tele2 har idag är inte tillräckliga, eftersom de baseras på mänskliga bedömningar och de tekniska lösningar som finns kan väljas bort. Tele2 saknar därmed en tekniskt tvingande och säker identifiering av sina kunder i kundtjänst. Den avsaknaden leder till alltför höga risker för integritetsincidenter av ett slag som kan medföra konsekvenser som identitetsstöld, bedrägeri, fysisk skada, psykiska men, förödmjukelse eller skadat rykte. Det finns således en identifierad risk för allvarliga konsekvenser varför den förelagda åtgärden är proportionerlig och inte allt för ingripande.

Beträffande vad Tele2 har anfört om att det uppstår problem för bl.a. gode män och förvaltare vill PTS peka på att möjligheten för en kund att ge fullmakt till en annan person inte kommer att påverkas av genomförandet av en teknisk lösning. Föreläggandet är även proportionerligt med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna för Tele2. Den tekniska lösning som PTS har förelagt Tele2 att vidta, syftar till att hindra kundtjänstpersonal från att kringgå Tele2:s rutiner för autentisering av kunder som ringer in till kundtjänst. Tele2 menar att skyddsrutinen att

enbart skicka känsliga uppgifter till kunds folkbokföringsadress skulle vara tillräckligt som skyddsrutin. PTS kan inte se att den rutinen som Tele2 beskriver, med att utskick görs till kunds folkbokföringsadress t.ex. när samtalsspecifikationer beställs av någon obehörig, tillräckligt minskar risken för kunden att råka ut för skada. Är kunden inte korrekt autentiserad kan någon annan ha beställt samtalsspecifikation medan kunden inte vet om att en sådan beställning har gjorts, och en obehörig kan vittja kundens postlåda för att hämta upp specifikationen.

Tele2 har uppgett att man har möjlighet att bevilja en kund en sekretesskod som kunden måste uppge till kundtjänstmedarbetaren innan denne får tillgång till kundens uppgifter. Detta tyder på att Tele2 redan idag delvis använder en sådan skyddsåtgärd som föreläggandet avser. Ett införande av en heltäckande teknisk lösning som inte kan kringgås av kundtjänstmedarbetaren kan därför inte anses vara så kostsam att föreläggandet ska anses vara oproportionerligt med hänsyn till kostnaderna eller den teknik som finns att tillgå. Det ska också tilläggas att den skyddsåtgärd som förelagts av PTS inte behöver vara BankID, utan en icke specifik teknisk lösning som syftar till att en manuell bedömning inte ska kunna göras av kundtjänstpersonal. Avgörandet om autentiseringen/identifieringen av kunden blir godkänd eller ej ska ligga hos den tekniska lösningen.

Sammanfattningsvis är den förelagda åtgärden nödvändig för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas. Dessutom är den ägnad att säkerställa en säkerhetsnivå, med beaktande av tillgänglig teknik och kostnaderna, väl avvägd mot risken för integritetsincidenter och allvarsgraden i dessa.

Den förelagda åtgärden syftar till att tillgodose ett gott integritetsskydd. PTS har konstaterat att det finns risk för allvarliga integritetsincidenter och har funnit att en åtgärd för att minimera risken utgörs av en teknisk lösning för

autentisering i kundtjänst. Det torde stå synnerligen klart att föreläggandet är helt i linje med lagens syfte och därtill utgör en åtgärd som grundas på det fastställda problemets art. Dessutom är det så väl rimligt som proportionerligt. Föreläggandet är därmed förenligt även med 1 kap. 1 § LEK och 1 kap. 2 § LEK.

Tele2:s andrahandsyrkande

PTS har vid fastställandet av tiden varit mycket generös med genomförandetiden. PTS har under tillsynen inhämtat information från tjänstetillhandahållarna angående bl.a. tiden för genomförande. PTS har tagit den längsta tid som angetts av tjänstetillhandahållarna för genomförande och lagt till ytterligare tre månader för testning och utbildning av personal. Av vad som framkommit i tillsynsärendena är det PTS uppfattning att Tele2 inte har sämre förutsättningar än övriga tjänstetillhandahållare vad gäller möjligheten att genomföra skyddsåtgärden inom den angivna tiden. PTS bedömer att Tele2, som redan idag använder sig av en del av den tekniska lösningen, har faktisk möjlighet att efterkomma föreläggandet inom den väl tilltagna tiden, den 31 mars 2021. Det kan även här noteras att övriga förelagda tjänstetillhandahållare inte har klagat vare sig på föreläggandet eller på tiden för genomförande.

SKÄLEN FÖR AVGÖRANDET

Tillämpliga bestämmelser framgår av det överklagade beslutet.

Förvaltningsrättens bedömning

Tele2 har i första hand yrkat att förvaltningsrätten ska upphäva det överklagade beslutet och i andra hand att rättelsetidpunkten ska ändras från den 30 mars 2021 till den 30 juni 2021.

Tele2:s förstahandsyrkande

Tele2 har till stöd för sitt förstahandsyrkande bl.a. anfört att föreläggandet går längre än vad som är lagligt möjligt och att föreläggandet är otydligt. Bolaget har vidare anfört att beslutet, med beaktande av det mycket begränsade antalet identifierade autentiseringsbrister som förekommit hos Tele2, saknar rättslig grund. Enligt Tele2 är kraven i föreläggandet inte heller proportionerliga eller i överensstämmelse med LEK:s syften.

Går föreläggandet längre än vad som är lagligt möjligt och är föreläggandet tydligt?

Tele2 menar att föreläggandet kan tolkas som att en kundtjänstmedarbetare inte i något fall får lämna ut uppgifter eller göra ändringar i abonnemang utan att den kund som kontaktar kundtjänsten först autentiserats via en teknisk lösning. Tele2 menar att föreläggandet därmed går utöver vad som anges i 6 kap. 3 § LEK om skyddsåtgärder. Enligt Tele2 uppfyller föreläggandet inte heller gällande krav på tydlighet och precision. Bolaget menar att det inte är tydligt vad PTS har avsett med begreppet ”kund” som används i föreläggandet eller vilken typ av uppgifter som omfattas av föreläggandet.

För att kunna ta ställning till om beslutet går längre än vad som är möjligt enligt 6 kap. 3 § LEK måste förvaltningsrätten kunna fastställa innebörden av det som anges i föreläggandet. Enligt Tele2 är det oklart om endast befintliga kunder omfattas av föreläggandet, eller om även tidigare och nya kunder omfattas. Tele2 menar vidare att det är oklart om föreläggandet gäller även för uppgifter för enskilda kunder med vilka bolaget saknar direkt avtalsrelation med.

Av den första meningen i föreläggandet under rubriken ”Post- och telestyrelsens avgörande” framgår att Tele2 ska införa en teknisk lösning som säkerställer att kunder som ringer in till kundtjänst är korrekt autentiserade innan kundtjänstmedarbetaren kan lämna ut uppgifter eller göra ändringar i abonnemang. Förvaltningsrätten anser att det är tydligt att föreläggandet avser att skydda uppgifter om enskilda personers abonnemang. Föreläggandet ska därför tillämpas för uppgifter avseende en viss kunds abonnemang; andra mer generella frågor om abonnemang berörs dock inte av föreläggandet. Enligt förvaltningsrättens mening är det vidare tydligt att föreläggandet gäller uppgifter om en enskild kunds abonnemang oavsett vad det är för slags elektronisk kommunikationstjänst som abonnemang tecknats för. Förvaltningsrätten anser därför att PTS inte har använt ordet ”kund” i föreläggandet på ett sådant sätt att det inte framgår hur föreläggandet ska efterlevas.

Tele2 har även ansett att det inte är tydligt vilka uppgiftskategorier som omfattas av föreläggandet. Enligt bolaget ger de två första meningarna i föreläggandet under rubriken ”Post- och telestyrelsens avgörande” upphov till olika tolkningar av vilken typ av uppgifter som omfattas av föreläggandet och bolaget menar därför att det är oklart vilken typ av uppgifter som en kundtjänstmedarbetare inte får lämna ut enligt föreläggandet utan att ha vidtagit de skyddsåtgärder som anges i föreläggandet. Enligt Tele2 ger den första meningen intryck av att föreläggandet gäller för uppgifter i allmänhet och inte enbart för sådana ”uppgifter som överförs, lagras eller på annat sätt behandlas i samband med tillhandahållandet av en elektronisk kommunikationstjänst”.

Enligt förvaltningsrättens mening är det dock tydligt att det som anges i meningarna efter den första meningen i det överklagade beslutet under rubriken ”Post- och telestyrelsens avgörande” utgör ett förtydligande av det som anges i den första meningen. Av föreläggandets andra mening framgår att

”En korrekt skyddsåtgärd ska omöjliggöra att informationen som behandlas i samband med tillhandahållandet av den elektroniska tjänsten kan avslöjas eller ändras på uppmaning av obehörig person via telefonkundtjänst”. Med beaktande av det som anges i denna mening och med hänsyn till vad som anges i 6 kap. 3 § LEK, som PTS har hänvisat till i det överklagade beslutet, anser förvaltningsrätten att det är tydligt att föreläggandet omfattar sådana uppgifter som behandlas i samband med tillhandahållandet av en elektronisk kommunikationstjänst, men inte andra uppgiftskategorier. Förvaltningsrätten anser därmed att föreläggandet inte går utöver vad som är lagligt möjligt enligt 6 kap. 3 § LEK. Förvaltningsrätten anser vidare att föreläggandet är tillräckligt preciserat för att Tele2 ska ha möjlighet att efterkomma det. Föreläggandet uppfyller därmed gällande krav på tydlighet och precision.

Har PTS haft rättslig grund för att meddela föreläggandet?

Tele2 har gjort gällande att PTS inte har haft fog för att meddela föreläggandet med hänsyn till det mycket begränsade antalet identifierade autentiseringsbrister som förekommit hos Tele2. Enligt bolaget har PTS låtit brister hos andra tjänstetillhandahållare ligga till grund för föreläggandet.

Förvaltningsrätten konstaterar att det följer av 6 kap. 3 § LEK att den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas.

Av utredningen i målet framgår att PTS vid tillsyn av Tele2 och andra tillhandahållare av elektroniska kommunikationstjänster har funnit att rutiner för att använda skyddsåtgärder vid autentisering av personer som ringer till kundtjänst inte följs. Enligt PTS tyder resultaten på en brist i Tele2:s och andra företags åtgärder för att skydda uppgifter vid personalens

hantering av telefonsamtal till kundtjänsten om ändringar i kunders abonnemang och utlämnande av information om kunders abonnemang.

Vid PTS tillsyn av Tele2 har det framkommit att bolaget har haft dokumenterade rutiner för hur en person som ringer till kundtjänsten ska identifieras, men trots detta har det förekommit att information har lämnats ut till obehöriga personer. Orsaken till detta har av Tele2 uppgetts vara att obehöriga personer som ringt till kundtjänst inte har identifierats enligt rutin och att kundtjänstmedarbetare ändå har gjort beställningar av samtalsspecifikationer som endast den som är behörig ska kunna göra.

Förvaltningsrätten konstaterar att det vid PTS tillsyn av Tele2 har framkommit att det har förekommit integritetsincidenter vid hantering av ärenden av Tele2:s kundtjänstpersonal. Även om antalet fall av incidentrapporter vid tidpunkten för PTS tillsyn har varit begränsade hos Tele2 anser förvaltningsrätten att det som framkommit vid PTS tillsyn ger stöd för att bolaget inte har vidtagit tillräckliga åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av en elektronisk kommunikationstjänst skyddas. Även om det av föreläggandet framgår att det även har förekommit brister hos andra tillhandahållare av elektroniska kommunikationstjänster anser förvaltningsrätten inte att det framkommit att PTS har låtit brister hos andra tjänstetillhandahållare ligga till grund för föreläggandet. Förvaltningsrätten anser mot denna bakgrund att PTS har haft rättslig grund för att meddela ett föreläggande mot bolaget.

Är föreläggandet proportionerligt och i överensstämmelse med LEK:s syften?

Tele2 anser att kravet i föreläggandet på att en teknisk lösning alltid ska användas för autentisering är oproportionerligt. Bolaget anser även att föreläggandet inte är i överensstämmelse med LEK:s syften. PTS har i målet anfört

att syftet med den tekniska lösning, som Tele2 har förelagts att vidta, är att hindra kundtjänstpersonal från att kringgå Tele2:s rutiner för autentisering av kunder som ringer in till kundtjänst.

Enligt förvaltningsrättens mening är kravet på en teknisk lösning ändamålsenligt och nödvändigt för att uppå syftet att undvika att det sker integritetsincidenter i samband med att personer ringer till Tele2:s kundtjänst för att få ut uppgifter om abonnemang eller göra ändringar i abonnemang. Förvaltningsrätten bedömer att kravet behövs för att säkerställa att enskilda kundtjänstmedarbetare inte frångår de rutiner som finns angående autentisering. Med hänsyn till att kravet på en teknisk lösning inte måste uppfyllas genom krav på BankID anser förvaltningsrätten att kravet inte går längre än vad som är nödvändigt för att uppnå det eftersträvade syftet. Med beaktande av de konsekvenser som en integritetsincident kan få för en enskild kund bedömer förvaltningsrätten att kravet på en teknisk lösning får anses rimligt även om kravet i vissa fall gör att det blir besvärligare för de som ringer till kundtjänst för att få ut uppgifter om sitt abonnemang eller för att göra ändringar i sitt abonnemang. Vad Tele2 har anfört om att antalet inrapporterade incidentrapporter är få föranleder inte någon annan bedömning i fråga om kravets rimlighet. Med beaktande härav och med hänsyn till att det framkommit att Tele2 för vissa kunder redan i dag använder en sådan skyddsåtgärd som föreläggandet avser bedömer förvaltningsrätten att föreläggandet får anses förenligt med proportionalitetsprincipen. Förvaltningsrätten anser vidare att föreläggandet är i överensstämmelse med LEK:s syften.

Sammanfattning

Förvaltningsrätten anser sammanfattningsvis att det inte finns skäl att upphäva det överklagade beslutet. Tele2:s förstahandsyrkande ska därför avslås.

Tele2:s andrahandsyrkande

Med hänsyn till vad Tele2 har anfört om det arbete som krävs för att kunna efterleva föreläggandet och med beaktande av tidsåtgången för en rättslig prövning av föreläggandet anser förvaltningsrätten att det finns skäl att ändra slutdatum för när de förelagda åtgärderna ska ha vidtagits. Förvaltningsrätten anser att en rimlig tidpunkt för när åtgärderna enligt det överklagade beslutet ska vara uppfyllda är den 30 juni 2021. Mot bakgrund härav finner förvaltningsrätten att Tele2:s andrahandsyrkande ska bifallas.

HUR MAN ÖVERKLAGAR

Detta avgörande kan överklagas. Information om hur man överklagar finns i bilaga 2 (FR-03).

[redacted]
Rådman

I avgörandet har även deltagit nämndemännen [redacted], [redacted] och [redacted] har varit föredragande.

Tele2 Sverige AB, 556267-5164

Föreläggande att vidta skyddsåtgärder vid autentisering i kundtjänst

Saken

Föreläggande enligt 7 kap. 5 § lagen (2003:389) om elektronisk kommunikation (LEK); fråga om att vidta skyddsåtgärder vid autentisering i kundtjänst.

Post- och telestyrelsens avgörande

Post- och telestyrelsen (PTS) förelägger Tele2 Sverige AB (Tele2) att senast den 31 mars 2021 införa en teknisk lösning som säkerställer att kunder som ringer in till kundtjänst är korrekt autentiserade innan kundtjänstmedarbetaren kan lämna ut uppgifter eller göra ändringar i abonnemang. En korrekt skyddsåtgärd ska omöjliggöra att information som behandlas i samband med tillhandahållandet av den elektroniska tjänsten kan avslöjas eller ändras på uppmaning av obehörig person via telefonkundtjänst. Den tekniska lösningen ska innebära att autentisering av kunder inte kan ske via en manuell bedömning av kundtjänstpersonal, utan avgörandet om autentiseringen blir godkänd eller ej ska ligga hos den tekniska lösningen. Det ska därmed inte heller vara möjligt att från- eller kringgå rutiner för autentisering.

Detta föreläggande gäller enligt 8 kap. 22 § LEK omedelbart.

Bakgrund

Under 2018 och 2019 har PTS tagit emot rapporter från flera tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster (tillhandahållare) om integritetsincidenter kopplade till kundtjänst. Dessa incidenter tyder på att medarbetare i tillhandahållarens kundtjänst brustit i sin autentisering av personer som ringer kundtjänst, vilket inneburit att obehörig person har kunnat ändra eller komma åt uppgifter om en kunds abonnemang. Detta är en av de

Post- och telestyrelsen

Postadress:
Box 5398
102 49 Stockholm

Besöksadress:
Valhallavägen 117 A
www.pts.se

Telefon: 08-678 55 00
Telefax: 08-678 55 05
pts@pts.se

vanligaste integritetsincidenter som rapporteras till PTS. I och med att flera tillhandahållare rapporterat in liknande händelser har PTS funnit anledning att misstänka brister i tillhandahållares metod för att skydda behandlade uppgifter vid autentisering i kundtjänst.

PTS beslutade därför i maj 2019 att granska ett antal tillhandahållare, däribland Tele2, vad gäller företagets metod att autentisera personer som ringer till kundtjänsten för att få information om eller göra ändringar i en kunds abonnemang. Tillsynen avgränsades till kundtjänst som tillhandahålls via telefon.

PTS har begärt in dokumentation från Tele2 om rutinerna för autentisering av personer som ringer företagets kundtjänst samt även en övergripande beskrivning av hur Tele2 tillämpar dessa rutiner. PTS har vid möte med Tele2 gått igenom rutiner och processer samt ställt frågor till medarbetare i kundtjänst.

Tele2 har uppgett i huvudsak följande:

Tele2 har rutiner för identifiering, som ska följas av personal i bolagets kundtjänst. Kundtjänst använder bl.a. följande säkerhetsåtgärder för identifiering av personer som ringer:

1. Kontrollfrågor. Kundtjänstmedarbetaren använder enklare kontrollfrågor t.ex. muntlig kontroll att namn och personnummer stämmer, vid icke kundspecifika frågor eller generella tips. Gäller det känsligare frågor där inte BankID ska användas ska kundtjänst ställa kontrollfrågor angående detaljer kring kundens abonnemang som endast kunden kan känna till.
2. Mobilt BankID ska alltid användas vid ett antal ärenden där viktig information om kunden lämnas ut eller där ändringar i abonnemanget görs.
3. Brevutskick till folkbokföringsadress sker t.ex. av samtalsspecifikation, sekretesskod och nytt SIM-kort (vid spärr av det gamla). Som bekräftelse vid ändring i abonnemang och vid de fall kunden inte har BankID skickas skriftligt underlag.
4. Sekretesskod kan beställas av kund via kundtjänst och skickas ut till kunds folkbokföringsadress. Om en kund har sekretesskod måste medarbetare i kundtjänst få denna kod av kund för att kunna öppna kundbilden.
5. Att hänvisa kunden till en butik för att hämta nytt SIM-kort är ett alternativ till att skicka ut kortet till folkbokföringsadressen. Kunden får då visa legitimation i butiken.

Noteringar görs om kunden verkar osäker eller inte har kunnat svara på någon fråga så att andra kundmedarbetare kan se det. Om en kund ber om vidarekoppling av sitt telefonnummer till annat telefonnummer ber kundtjänsten dem att göra det själva på webbportalen, där de loggar in med användarnamn och lösenord. Tele2 har också uppgett att nyanställda kundtjänstmedarbetare får utbildning om bolagets rutiner för autentisering i kundtjänst.

Tele2:s inställning

PTS har den 3 februari 2020, i enlighet med 7 kap. 4 § LEK, underrättat Tele2 om att myndigheten finner skäl att misstänka att Tele2 inte efterlever 6 kap. 3 § LEK och 4 § i PTS föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter, genom att inte ha vidtagit tillräckliga skyddsåtgärder i samband med autentisering vid telefonsamtal med företagets kundtjänst. Tele2 har i yttrande som kom in den 24 februari 2020 och vid möte den 30 mars 2020 sammanfattningsvis framfört följande:

Tele2 vill anföra att bristande autentisering endast har inträffat vid två fall där bägge fallen avsåg beställning av samtalsspecifikation. Utifrån det faktum att Tele2 dels har rutiner som fastställer att autentisering alltid ska ske, dels har rutiner som innebär att särskilt känslig information alltid skickas till abonnentens folkbokföringsadress, är Tele2 av uppfattningen att tillräckliga åtgärder har vidtagits för säkerställa att abonnentspecifik information endast kommer den specifika abonnenten tillhanda. Oavsett vem som initierar en dylik beställning, vare sig denne person är korrekt autentiserad eller inte, förutsätter alltså åtkomst till information att någon annan än abonnenten obehörigen bryter postförsändelsen (under eller efter transport). Ett brott som sker av någon annan part anser Tele2 ligger utanför sina möjligheter att råda över.

Med tanke på att Tele2:s kundservice hanterar ca 2 miljoner kundkontakter årligen utgör dessa fall 0,000001 procent av samtliga ärenden. Tele2:s bedömning är att denna siffra påvisar att gällande rutiner är tillfredsställande.

Tele2 har via e-post till PTS meddelat att BankID-verifikation har införts som enda verifikationsmetod för ett antal ärenden.

Skäl

Tillämpliga bestämmelser

I 7 kap. 4 § LEK anges att om PTS finner skäl att misstänka att den som bedriver verksamhet enligt denna lag inte efterlever lagen eller de beslut om skyldigheter eller villkor eller de föreskrifter som har meddelats med stöd av lagen, inte efterlever en genomförandeåtgärd som avses i 1 § andra stycket eller

inte använder en radiosändare i den utsträckning som villkoren medger, ska myndigheten underrätta den som bedriver verksamheten om detta förhållande och ge denne möjlighet att yttra sig inom skälig tid.

Enligt 7 kap. 5 § LEK får tillsynsmyndigheten meddela de förelägganden och förbud som behövs för rättelse av en överträdelse som avses i 4 § ska ske omedelbart eller inom skälig tid. Följs inte föreläggandet, får tillsynsmyndigheten, efter utgången av den tid som angetts i underrättelsen enligt 4 §, meddela de ytterligare förelägganden eller förbud som behövs för efterlevnaden. Enligt fjärde stycket får förelägganden och förbud förenas med vite.

Enligt 6 kap. 3 § LEK ska den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att de uppgifter som överförs, lagras eller på annat sätt behandlas i samband med tillhandahållandet av tjänsten skyddas. Åtgärderna ska vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsincidenter.

Enligt 4 § Post- och telestyrelsens föreskrifter och allmänna råd (PTSFS 2014:1) om skyddsåtgärder för behandlade uppgifter ska tillhandahållaren vidta de skyddsåtgärder som anges i föreskrifterna samt andra nödvändiga skyddsåtgärder, på den nivå som är lämplig för att hantera de identifierade riskerna.

PTS bedömning

Den som tillhandahåller allmänt tillgängliga elektroniska kommunikations-tjänster har ett ansvar att skydda uppgifter som behandlas i samband med tillhandahållandet. Integritetsincidenter som kan uppstå när sådana uppgifter inte skyddas kan leda till allvarliga konsekvenser för enskilda användare, såsom ekonomisk skada, allvarlig personlig kränkning eller till och med fara för liv och hälsa om en obehörig får tillgång till information. Dessutom kan integritets-incidenter försvaga allmänhetens tillit till elektroniska kommunikationstjänster.

PTS har i sin tillsyn av Tele2 och andra tillhandahållare av elektroniska kommunikationstjänster funnit att rutiner för att använda skyddsåtgärder vid autentisering av kunder som ringer kundtjänsten inte alltid följs. Detta leder typiskt sett till att information om kunden delas med obehörig person eller att en obehörig person kan göra ändringar i en kunds abonnemang. Detta utgör en brist i åtgärderna för att skydda uppgifter som behandlas i samband med tillhandahållande av den elektroniska kommunikationstjänsten.

Antalet anmälda incidenter skiljer sig åt mellan de tillhandahållare som PTS granskat men metoderna för autentisering skiljer sig inte åt i någon större utsträckning. PTS bedömer därför att brister i autentiseringen av personer som ringer till kundtjänst är ett generellt problem hos alla tillhandahållare som ingår i tillsynen.

PTS anser att det stora antalet incidenter som rapporterats in av flera tillhandahållare till PTS stödjer bedömningen att risken för att personuppgifter som behandlas i samband med tillhandahållandet av den elektroniska kommunikationstjänsten lämnas ut till obehörig person är hög. Kunder ringer även in till operatörens kundtjänst för att få hjälp med att göra ändringar i sitt abonnemang och sker inte en korrekt autentisering av kunden finns risk att det är en obehörig person som gör ändringar i kundens abonnemang. Om inte de skriftliga eller muntliga rutinerna följs av kundtjänstmedarbetaren är risken stor att ett otillåtet avslöjande eller en otillåten ändring görs av kundens personuppgifter och abonnemang.

Tele2 har anfört att företaget använder mobilt BankID som autentisering vid flertalet ärenden som en kund kan göra via telefonsamtal till kundtjänst. Det finns ingen spärr som hindrar avsteg från rutinen med krav på BankID. Vid de fall kunden inte har BankID använder Tele2 olika typer av kontrollfrågor som är av en sådan art att endast kunden bör känna till svaren. Det finns dock inget som hindrar att kundtjänstpersonalen underlåter att ställa dessa frågor eller att personalen utför det ärende som önskas även vid fel svar på frågorna.

För att hantera risken för att obehöriga får tillgång till kunders personuppgifter eller kan göra ändringar i abonnemang anser PTS att det krävs en teknisk skyddsåtgärd som hindrar detta. Den tekniska skyddsåtgärden ska säkerställa att kunden är korrekt autentiserad innan information om kunden lämnas ut eller förändring av kundens abonnemang eller av kundens uppgifter görs. Det ska därmed inte vara möjligt kringgå rutinerna för autentisering.

Tele2 ska därför föreläggas att införa en teknisk lösning som säkerställer att kunder som ringer in till kundtjänst är korrekt autentiserade innan kundtjänst-medarbetaren kan lämna ut uppgifter eller göra ändringar i abonnemang. En korrekt skyddsåtgärd ska omöjliggöra att information som behandlas i samband med tillhandahållandet av den elektroniska tjänsten kan avslöjas eller ändras på uppmaning av obehörig person via telefonkundtjänst. Den tekniska lösningen ska innebära att autentisering av kunder inte kan ske via en manuell bedömning av kundtjänstpersonal, utan avgörandet om autentiseringen blir godkänd eller ej

ska ligga hos den tekniska lösningen. Det ska därmed inte heller vara möjligt att från- eller kringgå rutiner för autentisering.

Tid för rättelse

Det föreligger inte hinder för Tele2 att vidta tekniska säkerhetsåtgärder för autentisering av kund som ringer in till kundtjänst.

Med hänsyn till åtgärdernas omfattning och behovet av utbildning och test efter implementering ges Tele2 till och med den 31 mars 2021 att genomföra rättelsen.

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 5398, 102 49 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 enhetschefen [redacted] I ärendets slutliga handläggning har även [redacted] (föredragande), [redacted] verksjuristen [redacted] enhetscheferna [redacted] och [redacted] samt chefsjuristen [redacted] deltagit.

PTS Beslutat av: [redacted]

SVERIGES DOMSTOLAR

Hur man överklagar

FR-03

Vill du att beslutet ska ändras i någon del kan du överklaga. Här får du veta hur det går till.

Överklaga skriftligt inom 3 veckor

Tiden räknas oftast från den dag som du fick del av det skriftliga beslutet. I vissa fall räknas tiden i stället från beslutets datum. Det gäller om beslutet avkunnades vid en muntlig förhandling, eller om rätten vid förhandlingen gav besked om datum för beslutet.

För en part som företräder det allmänna (till exempel myndigheter) räknas tiden alltid från den dag domstolen meddelade beslutet.

Observera att överklagandet måste ha kommit in till domstolen när tiden går ut.

Vilken dag går tiden ut?
Sista dagen för överklagande är samma veckodag som tiden börjar räknas. Om du exempelvis fick del av beslutet måndagen den 2 mars går tiden ut måndagen den 23 mars.

Om sista dagen infaller på en lördag, söndag eller helgdag, midsommarafton, julafton eller nyårsafton, räcker det att överklagandet kommer in nästa vardag.

Så här gör du

1. Skriv förvaltningsrättens namn och målnummer.
2. Förklara varför du tycker att beslutet ska ändras. Tala om vilken ändring du vill ha och varför du tycker att kammarrätten ska ta upp ditt överklagande (läs mer om prövningstillstånd längre ner).
3. Tala om vilka bevis du vill hänvisa till. Förklara vad du vill visa med varje bevis. Skicka med skriftliga bevis som inte redan finns i målet.
4. Lämna namn och personnummer eller organisationsnummer.

   Lämna aktuella och fullständiga uppgifter om var domstolen kan nå dig: postadresser, e-postadresser och telefonnummer.

   Om du har ett ombud, lämna också ombudets kontaktuppgifter.
5. Skicka eller lämna in överklagandet till förvaltningsrätten. Du hittar adressen i beslutet.

Vad händer sedan?

Förvaltningsrätten kontrollerar att överklagandet kommit in i rätt tid. Har det kommit in för sent avvisar domstolen överklagandet. Det innebär att beslutet gäller.

Om överklagandet kommit in i tid, skickar förvaltningsrätten överklagandet och alla handlingar i målet vidare till kammarrätten.

Har du tidigare fått brev genom förenklad delgivning kan även kammarrätten skicka brev på detta sätt.

Anvisningar för överklagande **FR-03 – Överklagandetid 3 v - PT** • Producerat av Domstolsverket, Avd. för domstolsutveckling • 2020-05

Prövningstillstånd i kammarrätten

När överklagandet kommer in till kammarrätten tar domstolen först ställning till om målet ska tas upp till prövning.

Kammarrätten ger prövningstillstånd i fyra olika fall.

- Domstolen bedömer att det finns anledning att tvivla på att förvaltningsrätten dömt rätt.
- Domstolen anser att det inte går att bedöma om förvaltningsrätten dömt rätt utan att ta upp målet.
- Domstolen behöver ta upp målet för att ge andra domstolar vägledning i rättstillämpningen.
- Domstolen bedömer att det finns synnerliga skäl att ta upp målet av någon annan anledning.

Om du *inte* får prövningstillstånd gäller det överklagade beslutet. Därför är det viktigt att i överklagandet ta med allt du vill föra fram.

Vill du veta mer?

Ta kontakt med förvaltningsrätten om du har frågor. Adress och telefonnummer hittar du på första sidan i beslutet.

Mer information finns på www.domstol.se.

Anvisningar för överklagande **FR-03 – Överklagandetid 3 v - PT** • Producerat av Domstolsverket, Avd. för domstolsutveckling • 2020-05