ERHVERVSSTYRELSEN

Telenor
Frederikskaj 8
2450 København SV

07. maj 2020
Sag 2020-1390
/Chtoch

ERHVERVSSTYRELSEN
Dahlerups Pakhus
Langelinie Allé 17
2100 København Ø

Tlf. 35 29 10 00
CVR-nr 10 15 08 17
E-post erst@erst.dk
www.erst.dk

ERHVERVSMINISTERIET

Afgørelse i Telenors sag om udlevering af modpartsnumre til politiet på baggrund af retskendelser

Erhvervsstyrelsen blev i slutningen af januar 2020 via medierne gjort opmærksom på, at Telenor tilsyneladende har oversendt for mange oplysninger i form af modpartsnumre til politiet som en del af de data, der oversendes efter politiets anmodning og på baggrund af retskendelser. Telenor har redegjort for sagen, herunder at selskabet har udleveret oplysninger til politiet i overensstemmelse med den kendelse, de har modtaget fra politiet. Erhvervsstyrelsen har foretaget en vurdering af, om der er sket brud på persondatasikkerheden i forbindelse med Telenors udlevering af oplysninger til politiet.

1. Afgørelse

Erhvervsstyrelsen træffer hermed afgørelse i medfør af telelovens[1] § 20 om, at Telenor har oversendt for mange oplysninger til politiet som en del af de signaleringsdata, der oversendes efter politiets anmodning, og at denne oversendelse dermed udgør et brud på persondatasikkerheden, jf. bekendtgørelse nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.

På baggrund af Telenors redegørelser, og idet Telenor nu har omlagt proceduren for udtræk af data til politiet, og at bruddet dermed ifølge Telenor er stoppet, samt på baggrund af, at det er Erhvervsstyrelsens forståelse, at ordlyden af kendelser nu er ændret, og Telenor derfor ikke udleverer modpartsnumre, medmindre dette fremgår af kendelsen, foretager styrelsen sig på det foreliggende grundlag ikke yderligere i den konkrete sag.

Erhvervsstyrelsen har den 4. marts 2020 startet et tilsyn på tværs af branchen med foranstaltninger omkring udlevering af personoplysninger til politiet på baggrund af politiets kendelser. Telenor har den 19. marts 2020 fremsendt en redegørelse til Erhvervsstyrelsen om dette. Erhvervsstyrelsen behandler dette som en selvstændig sag.

2. Sagens omstændigheder

Erhvervsstyrelsen anmodede den 28. januar 2020 Telenor om enten at indberette et sikkerhedsbrud eller redegøre for, hvorfor der ikke var tale om oversendelse af for meget information til politiet og dermed et sikkerhedsbrud.

[1] Lovbekendtgørelse nr. 128 af 7. februar 2014 om elektroniske kommunikationsnet og -tjenester

2.1 Telenors redegørelse af 29. januar 2020

Erhvervsstyrelsen modtog en redegørelse fra Telenor den 29. januar 2020, hvoraf det fremgår, at selskabet siden september 2018 har udleveret oplysninger til politiet på baggrund af retskendelser, som lyder på udlevering af *signaleringsdata*.

Det fremgår af Telenors redegørelse, at information om, hvorvidt et givet telefonnummer er afsendende part (A-nummer) eller modtagende part (B-nummer), er en integreret del af signaleringsdata. Telenor mener på den baggrund, at selskabet har udleveret oplysninger til politiet i overensstemmelse med den kendelse, som Telenor har modtaget om udlevering af signaleringsdata. Telenor mener derfor ikke, at der er sket et brud på persondatasikkerheden i den pågældende sag. Dette har Telenor ifølge deres oplysninger også anført over for politiet ved mail af 8. august 2019.

2.2. Erhvervsstyrelsens møde med Telenor samt supplerende redegørelse

Telenor præsenterede på et møde i Erhvervsstyrelsen den 4. februar 2020 en supplerende redegørelse vedrørende de verserende sager (se afsnit 2.2.1 nedenfor). På mødet oplyste Telenor, at Rigspolitiet kontaktede selskabet den 28. maj 2019 og underrettede selskabet om, at politiet kunne se SMS-indhold (jf. Telenors sag om udlevering af SMS-indhold, sagsnr. 2019-8232). Ifølge Telenor, nævnte Rigspolitiet i samtalen også, at politiet modtog mere data, end de havde behov for, når de modtog signaleringsdata. Telenor oplyste på mødet, at de på tidspunktet for samtalen med Rigspolitiet antog, at omtalen af "mere data, end de havde behov for" henviste til SMS-indhold. Primo august 2019 vendte Rigspolitiet tilbage til Telenor for at præcisere, at der var tale om oplysninger om, at et telefonnummer er modtagende part (et såkaldt B-nummer).

Telenor oplyste endvidere, at Telenor herefter forsøgte at indgå i en dialog med Rigspolitiet for at afklare, hvad politiet i så fald ønskede udleveret, når de anmodede om udlevering af 'signaleringsdata'.

Af den supplerende redegørelse fremgår det, at Telenor mener, at selskabet har udleveret den data, som selskabet var retligt forpligtet til at udlevere på baggrund af dommerkendelser – og der derfor ikke er tal om et sikkerhedsbrud.

Telenor oplyste desuden, at selskabet i mangel af input fra Rigspolitiet i februar 2020 havde sammensat et datasæt, som var selskabets bud på, hvad politiet reelt efterspørger, når de anmoder om signaleringsdata. På baggrund af en fornyet vurdering formoder selskabet, at politiet ønsker information om, hvilke telefonnumre der har været til stede på et givet tidspunkt i et givet område, men uden information om, hvorvidt der er sket kommunikation til og fra de pågældende telefonnumre. Telenor oplyser, at de derfor fremadrettet vil levere nye datasæt uden den pågældende information.
Telenor oplyste videre, at de ville sende en skrivelse til politiet omkring det nye datasæt og bede om deres kommentarer.

2.3 Rigspolitiets bemærkninger til Telenors redegørelser

Erhvervsstyrelsen modtog den 26. februar 2020 Rigspolitiets bemærkninger til Telenors redegørelser. Heraf fremgår det, at spørgsmålet om fortolkningen af retsplejelovens regler om udlevering (edition) vil blive drøftet i et telebrancheforum i den nærmeste fremtid, herunder særligt med fokus på fortolkningen af begrebet "signaleringsdata".

Rigspolitiet gennemgår i deres bemærkninger ligeledes relevante regler i retsplejeloven samt henviser til retspraksis omkring disse regler, herunder særligt landsrettens udtalelse i U.2017.1934Ø, jf. nedenfor.

2.3.1 Landsrettens udtalelse i U.2017.1934Ø

Østre Landsret har i 2017 afsagt kendelse i en sag om udlevering af signaleringsdata. I den konkrete sag ønskede politiet signaleringsdata vedrørende en større ubestemt mængde telefoner for at finde ud af, hvilke telefoner der på et givet tidspunkt befandt sig inden for rækkevidden af de master, der dækker gerningsstedet. Tre teleselskaber (Telenor var ikke omfattet af den konkrete kendelse) pålægges i kendelsen at udlevere signaleringsdata for en given dato i et givent tidsrum, for masteceller, som dækker en given adresse.

Østre Landsret lægger det af anklagemyndigheden oplyste om signaleringsdata til grund for sin kendelse. Af kendelsen fremgår, at anklagemyndigheden har anført følgende om signaleringsdata: "*Der er alene tale om bagudrettede oplysninger, og signaleringsdata giver kun adgang til oplysninger om, hvorvidt en telefon har været tændt, og i givet fald om brugeren er tilknyttet et af de tre [i dag fire] teleselskaber, der gemmer signaleringsdata. Der vil således ikke fremgå oplysninger om, hvorvidt telefonerne har været brugt, og hvilke apparater de eventuelt har været i kontakt med.*"

Det fremgår i øvrigt at ved retten i første instans (Byretten, Glostrup), har teleselskaberne oplyst, at de vil udlevere oplysningerne, og at de ikke ønsker at møde i retten.

2.4 Telenors svar på Erhvervsstyrelsens opfølgende spørgsmål

Erhvervsstyrelsen har den 4. marts 2020 – bl.a. på baggrund af Rigspolitiets bemærkninger – stillet en række supplerende spørgsmål til Telenor med henblik på yderligere oplysning af sagen. Styrelsen modtog Telenors svar den 11. marts 2020.

Telenor oplyser, at det hidtil har fremgået af de til politiet oversendte datasæt, hvilke numre der er henholdsvis A- og B-numre, idet numrene fremgår som hhv. calling/called eller from/to. Telenor oplyser hertil endvidere, at et fokusnummer – dvs. det nummer der er genstand for en konkret kendelse – sagtens kan være et B-nummer i en given kommunikation.

Telenor oplyser yderligere, at lokaliseringsdata udgør en mindre del af den samlede mængde indsamlede signaleringsdata, og at indsamling af signaleringsdata sker til brug for selskabets fejlretning. Lokaliseringsdata omfatter oplysninger om lokalisering og ikke andet end dette. Oplysning om, hvorvidt et

telefonnummer er afsendende eller modtagende part er således ikke en del af lokaliseringsdata.

Telenor oplyser endvidere, at selskabets signaleringsdata indeholder alle signaleringer i netværket, herunder informationer om modpartsnumre (dvs. telefonnumre, der sættes i forbindelse med det telefonnummer, der er genstand for kendelsen), uanset om modparten befinder sig inden for eller uden for det givne fokusområde, dvs. det område, der er genstand for en konkret kendelse.

Endelig skriver Telenor, at selskabet ikke længere udleverer signaleringsdata til politiet. Telenor har bedt Rigspolitiet om, at kendelser fremadrettet skal lyde på lokaliseringsdata frem for signaleringsdata. Selskabet oplyser videre, at politiet nu har ændret kendelsernes ordlyd til at angå "lokaliseringsdata".

2.5 Telenors kommentarer til Rigspolitiets bemærkninger

Telenor sendte den 27. marts selskabets kommentarer til Rigspolitiets bemærkninger. Heraf fremgår det, at Telenor er af den holdning, at Rigspolitiets bemærkninger tager udgangspunkt i, hvad der teoretisk *kan* kræves udleveret, og ikke hvad der reelt *ønskes* udleveret.

Rigspolitiet bemærker, at fortolkning af kendelser beror på retspraksis. Telenor skriver hertil, at telenors forpligtelse og hjemmel defineres af kendelsens indhold. Indholdet må som udgangspunkt findes ved en ordlydsfortolkning.
Telenor skriver ligeledes, at retsplejeloven definerer hvilke oplysninger der *kan* udleveres på baggrund af en kendelse, men at det er den konkrete kendelses ordlyd, der definerer, hvad der *skal* udleveres.

Telenor er således ikke enig i Rigspolitiets bemærkninger om, at en kendelses indhold både kan og skal afgøres ud fra en fortolkning af ordlyden af den bestemmelse i retsplejeloven, der hjemler kendelsen, da dette vil gøre ordlyden af kendelsen overflødig.

Telenor henviser ligeledes til den relevante bestemmelses brede karakter (retsplejelovens § 804, stk. 1), og at det derfor er helt centralt, at kendelsens ordlyd klart og præcist definerer, hvilken data som skal udleveres.

Telenor oplyser endelig, at de ikke mener, at Landsrettens udtalelse i U.2017.1934Ø definerer "signaleringsdata", som Rigspolitiet henviser til i deres bemærkninger. Telenor skriver, at anklagemyndighedens udlægning af signaleringsdata er en sandhed med modifikationer, idet retten ikke tager selvstændigt stilling til spørgsmålet, men uden videre lægger hvad Telenor kalder en upræcis oplysning fra anklagemyndigheden til grund.

3. Regelgrundlag

Erhvervsstyrelsen fører tilsyn med overholdelse af reglerne i teleloven[2], jf. telelovens § 20.

[2] Lovbekendtgørelse nr. 128 af 7. februar 2014 om elektroniske kommunikationsnet og -tjenester

Det følger af telelovens § 8, at ministeren fastsætter regler om minimumskrav for udbydere af offentlige elektroniske kommunikationsnet eller -tjenesters behandling af persondata i elektroniske kommunikationsnet og -tjenester. Bestemmelserne i § 8, stk. 1–4, lyder således:

> ”*Erhvervs- og vækstministeren fastsætter regler for udbydere af offentlige elektroniske kommunikationsnet eller -tjenester om minimumskrav til behandling af persondata i elektroniske kommunikationsnet og -tjenester.*
>
> *Stk. 2. Regler fastsat i medfør af stk. 1 skal bl.a. omfatte krav om følgende:*
>
> 1. *Passende tekniske og organisatoriske foranstaltninger med henblik på at styre risici for persondatasikkerheden i elektroniske kommunikationsnet og -tjenester og sikre et sikkerhedsniveau, der står i forhold til risici.*
> 2. *Underretning af Erhvervsstyrelsen ved brud på persondatasikkerheden. Pligten kan omfatte underretning af andre end Erhvervsstyrelsen under særlige omstændigheder.*
>
> *Stk. 3. Regler fastsat i medfør af stk. 1 kan endvidere af hensyn til persondatabeskyttelse bl.a. omfatte krav om følgende:*
>
> 1. *A-nummer-visning, automatisk viderestilling og forbrugsopgørelser.*
> 2. *Opbevaring og behandling af trafikdata og lokaliseringsdata i forbindelse med elektronisk kommunikation.*
>
> *Stk. 4. Erhvervs- og vækstministeren fastsætter nærmere regler om tilsyn med overholdelsen af regler, der fastsættes i medfør af stk. 1, herunder om kontrol med persondatasikkerheden.”*

Bestemmelsen i telelovens § 8, stk. 1, er udmøntet ved bekendtgørelse nr. 462 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester. Om risikostyring anføres følgende i bekendtgørelsens § 3:

> *”Udbydere af offentlige elektroniske kommunikationstjenester skal løbende træffe passende tekniske og organisatoriske foranstaltninger med henblik på at styre risici for persondatasikkerheden i forbindelse med udbud af elektroniske kommunikationstjenester. Udbyderne skal gennem disse foranstaltninger sikre et sikkerhedsniveau, der, under hensyn til teknologiens aktuelle stade og omkostningerne i forbindelse med gennemførelsen af foranstaltningerne, står i forhold til risici.*
>
> *Stk. 2. De foranstaltninger, der er nævnt i stk. 1, skal som minimum*

> 1. *sikre, at kun autoriserede personer får adgang til persondata til lovlige formål,*
> 2. *beskytte lagrede eller sendte persondata mod hændelig eller ulovlig tilintetgørelse, hændeligt tab eller ændring og ubeføjet eller ulovlig lagring, behandling, adgang eller videregivelse, og*
> 3. *gennemføre en sikkerhedspolitik for persondatasikkerheden i forbindelse med udbud af elektroniske kommunikationstjenester."*

Om tilsyn med styring af risici anføres følgende i bekendtgørelsens § 7:

> *"Erhvervsstyrelsen fører tilsyn med de foranstaltninger, som udbydere af offentlige elektroniske kommunikationstjenester skal træffe efter § 3.*
>
> *Stk. 2. Erhvervsstyrelsen kan i forbindelse med tilsyn efter stk. 1 påbyde udbydere af offentlige elektroniske kommunikationstjenester at gennemføre de tiltag, som, Erhvervsstyrelsen vurderer, er nødvendige for at sikre, at kravene i § 3 er overholdt."*

Overtrædelse af bestemmelserne i § 3 kan straffes med bøde, jf. bekendtgørelsens § 10, stk. 1.

4. Vurdering og begrundelse

På baggrund af de oplysninger, Erhvervsstyrelsen har modtaget fra Telenor og Rigspolitiet samt Landsrettens kendelse i U.2017.1934Ø, er det Erhvervsstyrelsens vurdering, at der har været et sikkerhedsbrud hos Telenor siden selskabet begyndte at udlevere den i sagen omhandlede datatype til politiet i september 2018, frem til selskabet i februar 2020 får implementeret foranstaltninger, der skal hindre lignende brud.

Udleveringerne af oplysninger til politiet sker som led i politiets efterforskning af sager. Politiet anmoder teleselskaber om oplysninger på baggrund af retskendelser. Retskendelserne lød i en række tilfælde i perioden september 2018 til februar 2020 på udlevering af "signaleringsdata", og Telenor udleverede, hvad selskabet vurderede, var oplysninger til politiet i overensstemmelse med ordlyden i kendelserne.

Det er Erhvervsstyrelsens opfattelse, at Telenor burde have foretaget informationssøgning, herunder i retspraksis, hvis selskabet var i tvivl om ordlyden af kendelserne og dermed omfanget af den data, der skulle udleveres på baggrund heraf.

Om end Landsrettens udtalelse i U.2017.1934Ø ikke har direkte til formål at definere begrebet "signaleringsdata", kan det af denne udtalelse udledes, at kendelser om signaleringsdata alene vedrører udlevering af allerede registrerede lokaliseringsoplysninger, og at kendelser om signaleringsdata således ikke angår oplysninger om, hvilke telefoner eller andre tilsvarende kommunikationsapparater

der sættes i forbindelse med en bestemt telefon eller andet kommunikationsappart (dvs. modpartsnumre). Det er derfor styrelsens vurdering, at selskabet har udleveret for meget data til politiet, når der er sket udlevering af modpartsnumre. En nærmere gennemgang følger nedenfor:

Når Telenor siden september 2018 har udleveret signaleringsdata til politiet, er der i de tilfælde, hvor selskabet har leveret oplysninger om modpartsnumre, således leveret for meget data til politiet.

Det følger af § 3, stk. 1 og 2, i bekendtgørelse nr. 462 23. maj 2016, at Telenor er forpligtet til løbende at træffe passende tekniske og organisatoriske foranstaltninger med henblik på at styre risici for persondatasikkerheden. Det skal bl.a. sikre, at der ikke sker ubeføjet videregivelse af persondata.

Efter Erhvervsstyrelsens opfattelse har der ikke hos Telenor været fastsat passende tekniske og organisatoriske foranstaltninger med henblik på at styre risiciene for persondatasikkerheden, når der oversendes flere oplysninger til politiet, end der anmodes om i medfør af retskendelser, hvilket har medført brud på persondatasikkerheden.

Erhvervsstyrelsen har noteret sig, at Telenor har opsat nye procedurer for udlevering af data til politiet på baggrund af kendelser fra politiet, og at der ikke længere fremgår oplysninger om, hvorvidt et fokusnummer er afsendende eller modtagende part. Det er endvidere Erhvervsstyrelsens forståelse, at der i dialogen mellem Rigspolitiet og telebranchen allerede er sket en tilpasning af begreberne, der understøtter at fremtidige brud forebygges.

Opsamlende finder Erhvervsstyrelsen, at Telenor har oversendt for mange oplysninger til politiet som en del af de signaleringsdata, der oversendes efter politiets anmodning, og at denne oversendelse dermed udgør et brud på persondatasikkerheden, jf. bekendtgørelse nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.

På baggrund af Telenors redegørelser, og idet Telenor nu har omlagt proceduren for udtræk af data til politiet, og at bruddet dermed ifølge Telenor er stoppet, samt på baggrund af, at det er Erhvervsstyrelsens forståelse, at ordlyden af kendelser nu er ændret, og Telenor derfor ikke udleverer modpartsnumre, medmindre dette fremgår af kendelsen, foretager styrelsen sig på det foreliggende grundlag ikke yderligere i den konkrete sag. Erhvervsstyrelsen skal dog bemærke, at det konkrete brud vil indgå i styrelsens løbende overvejelser om, hvorvidt der er behov for at iværksætte et tilsyn på området.

4.1 Underretningspligt

Kommissionens forordning (EU) nr. 2013/611 af 24. juni 2013 gælder for underretning om brud på persondatasikkerheden, der foretages af udbydere af offentligt tilgængelige kommunikationstjenester.

Forordningen indeholder i artikel 2 en forpligtelse for teleudbydere til at underrette den kompetente nationale myndighed, dvs. Erhvervsstyrelsen, om samtlige brud på persondatasikkerheden.

Derudover indeholder forordningen i artikel 3 en central bestemmelse om udstrækningen af teleudbyderens forpligtelse til at underrette en abonnent eller fysisk person.

Erhvervsstyrelsen har i medfør af § 8, stk. 1 og 4, § 80 og § 81, stk. 2, i teleloven udstedt bekendtgørelse om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester[3].

I bekendtgørelsens § 5, stk. 1, er der anført en pligt til at indberette brud på persondatasikkerheden til Erhvervsstyrelsen, og i § 5, stk. 2 er Erhvervsstyrelsen tillagt kompetence til at kunne kræve – efter at have vurderet sikkerhedsbruddets sandsynlige negative virkninger – at udbyderen underretter slutbrugeren eller evt. berørte fysiske personer om sikkerhedsbruddet.

Når styrelsen skal vurdere, hvorvidt der er pligt til underretning af de berørte abonnenter eller personer lægges der vægt på, om sikkerhedsbruddet kan forventes at krænke personoplysninger eller privatlivets fred for en abonnent eller en fysisk person. Ved vurderingen af, om sikkerhedsbruddet kan forventes at krænke personoplysninger eller privatlivets fred, skal der, jf. forordningen, inddrages hensyn til 1) karakteren og indholdet af de pågældende oplysninger, 2) om bruddet kan forventes at medføre identitetstyveri eller svig, fysisk skade, psykologisk forstyrrelse, tort eller skade af omdømme, og 3) omstændighederne ved bruddet – navnlig når oplysninger er blevet stjålet.

Erhvervsstyrelsen har foretaget en sådan vurdering af spørgsmålet om underretningspligt, og det er styrelsens opfattelse, at der ikke er belæg for at påbyde Telenor en pligtmæssig underretning af de berørte personer. I denne vurdering er der bl.a. lagt vægt på, at:

- Karakteren af indholdet vedrører en videregivelse af telefonnumre på modparter. Telefonnumre anses som almindelige personoplysninger. Videregivelsen skete efter anmodning og på baggrund af en retskendelse,
- data er tilgået den ønskede adressat (politiet) – der er således ikke tale om et ubevist læk eller utilsigtet videregivelse til offentligheden eller en anden utilsigtet adressat fx en privat fysisk eller juridisk person,
- det er en særlig omstændighed ved sikkerhedsbruddet, at fremsendelsen af signaleringsoplysninger sker til brug for Rigspolitiets efterforskning af strafbare forhold. Datasættet kan indeholde oplysninger om personer som ikke nødvendigvis er eller må være vidende om, at der pågår politimæssig efterforskning mod dem, og at der i den forbindelse er opnået en retskendelse til, at der må indhentes signaleringsoplysninger.

[3] Jf. Bekendtgørelse om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester (BEK. Nr. 462 af 23/05/2016)

På baggrund af ovenstående finder styrelsen således ikke, at sikkerhedsbruddet kan forventes at krænke personoplysninger eller privatlivets fred for en abonnent eller en fysisk person. Det er dermed styrelsens vurdering, at der ikke er grundlag for at pålægge Telenor at underrette de berørte abonnenter eller personer om bruddet.

På baggrund af det foreliggende grundlag foretager Erhvervsstyrelsen sig således ikke yderligere i den konkrete sag.

5. Klagevejledning

Erhvervsstyrelsens afgørelse kan påklages til Teleklagenævnet, Toldboden 2, 8800 Viborg, tlf.: 72 40 56 00, e-mail: tkn@naevneneshus.dk.

En klage skal være Teleklagenævnet i hænde senest fire uger efter, at Erhvervsstyrelsen har truffet denne afgørelse.

Opmærksomheden henledes på, at der i medfør af § 3, stk. 1, i bekendtgørelse nr. 383 af 21. april 2011 om Teleklagenævnets virksomhed skal betales et gebyr på 4.000 kr. for behandling af klager af denne type i Teleklagenævnet. Beløbet vil blive opkrævet af Teleklagenævnets sekretariat.

Med venlig hilsen

Christina Toft Michelsen