Digitaliserings-
styrelsen

TDC Net A/S,
CVR 40075267

27. april 2026
KDRT/SISMIK
J. nr. 2025-19877

Digitaliseringsstyrelsen
Landgreven 4
1301 København K

Afslutning af tilsyn vedr. filtrering af SMS-beskeder

Digitaliseringsstyrelsen vender hermed tilbage til sagen, hvor styrelsen den 31. oktober 2025 har anmodet teleselskaberne TDC Net A/S, CVR 40075267 (herefter TDC Net) og TDC Brands A/S, CVR 40075291 (herefter TDC Brands) om en redegørelse for håndteringen af den SMS-filtrering, selskaberne har foretaget med henblik på at forebygge "svindel", herunder en redegørelse for selskabernes lagring af SMS-beskeder og medarbejderes adgang til indholdet af sådanne beskeder.

TDC Net og TDC Brands har i et fælles høringssvar oplyst, at løsningen er blevet håndteret samlet og er implementeret, anvendt og administreret i TDC-koncernen, og at TDC Brands udførte den operative gennemgang af kampagner. Digitaliseringsstyrelsen har på den baggrund udarbejdet enslydende afgørelser, som er sendt til de respektive selskaber.

1. Sammenfatning

Digitaliseringsstyrelsen har på det foreliggende grundlag besluttet at afslutte tilsynssagen, som angår den allerede foretagne og nu ophørte filtrering af SMS-beskeder.

Beslutningen om at afslutte tilsynet sker på baggrund af mødet den 12. september 2025 mellem Digitaliseringsstyrelsen, Teleindustrien og en række teleselskaber, den efterfølgende generelle redegørelse af 31. oktober 2025 fra Teleindustrien og TDC Net og TDC Brands samlede høringssvar, der efter omstændighederne ikke giver Digitaliseringsstyrelsen anledning til at foretage yderligere i forhold til filtreringen.

Nedenfor følger en kort redegørelse for de væsentligste omstændigheder, der danner baggrund for Digitaliseringsstyrelsens beslutning.

2. Sagsfremstilling

Regeringen og Teleindustrien blev den 13. november 2023 enige om en række initiativer til imødegåelse af digital svindel i telenettene, herunder etableringen af en løsning for SMS-filtrering. Som led i dette udarbejdede Digitaliseringsministeriet i samarbejde med telebranchen en initiativbeskrivelse dateret den 4. oktober 2024, hvori løsningen blev beskrevet og vurderet til – efter de daværende forudsætninger – at kunne gennemføres inden for rammerne af telelovens §§ 7–9.

SMS-filtreringen blev i den oprindelige beskrivelse, der lå til grund for Digitaliseringsstyrelsens vurdering af sagen, jf. initiativbeskrivelserne af 4. oktober 2024, beskrevet som et AI- eller robotdrevet filtreringssystem, som ved tydelige tegn på svindel kunne blokere beskeder fra at nå frem til modtageren. Denne filtrering skulle som hovedregel fungere uden, at fysiske personer fik kendskab til indholdet af enkelte SMS-beskeder, da det alene var en algoritme, der skulle finde og blokere den videre fremsendelse af SMS-beskeder med tydelige tegn på svindel.

Digitaliseringsstyrelsen lagde ved sin vurdering særligt vægt på, at der i vid udstrækning allerede eksisterede spam-filtre, at ingen fysiske personer ville få kendskab til indholdet af SMS-beskederne, at udbyderne i etableringen af systemet ikke begrænsede beskyttelsen af deres abonnenters og brugeres kommunikationshemmelighed mere end, hvad der var nødvendigt for at sikre et passende sikkerheds-niveau, at behandlingen ville stå i rimeligt forhold til alvoren af truslen, der blev forebygget, og at det ikke var muligt at opnå formålet på en for privatlivets fred mindre indgribende måde.

TDC Net og TDC Brands begyndte at lagre beskeder fra den 16. oktober 2024 og fra den 14. november 2024 fik TDC Brands medarbejdere adgang til systemet, og fra den 22. november 2024 begyndte medarbejderne praktisk at anvende kampagnevisning. Selskaberne har redegjort for erfaringerne med effektiviteten af filtreringen, og i varierende grad for de forskellige kriterier, som selskaberne har benyttet som grundlag for denne.

Efter det oplyste, stod det hen over sommeren klart for TDC Net og TDC Brands, at en effektiv filtrering af SMS-beskeder ikke kunne ske inden for rammerne af den oprindelige initiativbeskrivelse. Nærmere bestemt forudsatte filtreringen både lagring af beskedindhold i en kortere periode og en vis menneskelig involvering med henblik på at verificere systemets identifikation af SMS-beskeder, der i bred forstand kunne

kategoriseres under den bredere betegnelse "digital svindel". På den baggrund ophørte selskaberne fra den 4. juli 2025 dels med at lagre nyt beskedindhold, dels med at foretage manuel gennemgang af sådanne SMS-beskeder og kampagner, der potentielt set udgjorde forsøg på svindel.

Digitaliseringsstyrelsen blev på et møde den 12. september 2025 med Teleindustrien og de fem deltagende selskaber, herunder TDC Net og TDC Brands, orienteret om sagsforløbet med SMS-filtrering, samt om de praktiske erfaringer selskaberne havde gjort sig med idriftsættelsen og håndteringen af systemet. Selskaberne gjorde i denne forbindelse opmærksom på, at det ikke stod dem klart, hvorvidt SMS-filtrering fremover ville kunne ske inden for rammerne af initiativbeskrivelsen og telelovens § 7.

Den 24. september 2025 modtog Digitaliseringsstyrelsen – efter aftale med Teleindustrien – en kopi af Teleindustriens redegørelse af samme dato til Digitaliseringsministeren. Redegørelsen indeholder en generel beskrivelse af selskabernes håndtering af SMS-filtreringen.

SMS-filtreringen er i Teleindustriens redegørelse beskrevet som et system, der anvender maskinlæring til at identificere masseudsendte SMS-beskeder med enslydende indhold baseret på mønstre, links og definerede nøgleord. Når de nærmere fastsatte udvælgelseskriterier er opfyldt, grupperes de udvalgte beskeder som en mulig svindel-kampagne, der præsenteres for en medarbejder hos operatøren. Medarbejderen vurderer, hvorvidt der er tale om legitim kommunikation eller svindel. Hvis der er tale om en svindelkampagne noteres dette i systemet, som uden yderligere involvering af medarbejdere fremover kan screene og blokere SMS-beskeder af tilsvarende karakter.

Digitaliseringsstyrelsen anmodede den 31. oktober 2025 TDC Net og TDC Brands om at besvare en række spørgsmål om selskabernes konkrete håndtering af SMS-filtreringen. Styrelsen har efterfølgende modtaget et samlet svar fra selskaberne og har i den forbindelse noteret sig følgende,

- at selskaberne ikke havde implementeret systemet inden for rammerne af den oprindelige beskrivelse, der lå til grund for Digitaliseringsstyrelsens vurdering af sagen, jf. initiativbeskrivelserne af 4. oktober 2024,

- at selskaberne i forlængelse heraf havde implementeret et system til overvågning af SMS-beskeder, uden at have et fuldstændigt klart billede af, hvordan systemet skulle fungere,

- at beskederne generelt blev lagret i kortere perioder, og at selskaberne undervejs i implementeringsfasen aktivt havde forholdt sig til lagringsperioden med henblik på at reducere denne,

- at selskabernes filtrering var baseret på varierende kriterier for identifikation af potentielle svindel-SMS/-kampagner, f.eks. [redacted]

- at kun masseudsendte beskeder med ensartet indhold blev grupperet og præsenteret for udvalgte medarbejdere som potentielle såkaldte svindelkampanger med henblik på at minimere risikoen for, at en medarbejder blev præsenteret for beskeder, som måtte karakteriseres som private,

- at masseudsendte beskeder med ensartet indhold var karakteriseret ved omfatte en bestemt mængde af enslydende beskeder og et eller flere supplerende kriterier, for eksempel at [redacted],

- at der var implementeret en række forskellige foranstaltninger herunder anonymisering af A- og B-numre (afsender- og modtagernummer), med henblik på ikke at kunne henføre kommunikationen til konkrete personer,

- at der hos selskaberne var ni tekniske/understøttende medarbejdere, som efter behov havde adgang til at yde teknisk bistand til løsningen og derfor havde haft adgang til at læse indholdet af beskeder og kampagner,

- at det var fire [redacted] medarbejdere, som havde håndteret den daglige drift af løsningen, og dermed havde adgang til at læse indholdet af kampagner med henblik på at vurdere, hvorvidt de kunne kategoriseres som svindel-kampagner,

- at de pågældende medarbejdere efter det oplyste karakteriseres som enten betroede medarbejdere, der var

underlagt tavshedspligt i medfør af deres stilling og/eller sikkerhedsgodkendte medarbejdere,

- at der som led i SMS-filtreringen var frasorteret et ganske betydeligt antal svindel-SMS-beskeder på omkring 13,3 mio.,

- at selskaberne havde foretaget logning af medarbejdernes aktiviteter i løsningen, men at der ikke var foretaget kontrol med logningen i implementerings- eller driftsfasen.

3. Det retlige grundlag

Beskyttelse af kommunikationshemmeligheden er reguleret i telelovens § 7[1], som har følgende ordlyd:

> "**§ 7.** Ejere af elektroniske kommunikationsnet og udbydere af elektroniske kommunikationsnet eller -tjenester og nummeruafhængige interpersonelle kommunikationstjenester og deres ansatte og tidligere ansatte må ikke uberettiget videregive eller udnytte oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf, som de får kendskab til i forbindelse med det pågældende udbud af elektroniske kommunikationsnet eller -tjenester og nummeruafhængige interpersonelle kommunikationstjenester. De nævnte ejere og udbydere skal træffe de foranstaltninger, der er nødvendige for at sikre, at oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf ikke er tilgængelige for uvedkommende."

Telelovens § 7 er en implementering af e-databeskyttelsesdirektivets art. 5, stk. 1[2] , som har følgende ordlyd:

> "1. Medlemsstaterne sikrer kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, både for så vidt angår selve kommunikationen og de dermed forbundne trafikdata, via nationale forskrifter. De forbyder især aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges af andre end brugerne, uden at de pågældende brugere har indvilget heri, bortset fra tilfælde, hvor det er tilladt ifølge lovgivningen, jf. artikel 15, stk. 1. Dette stykke er ikke til hinder for teknisk

[1] Lovbekendtgørelse nr. 681 af 16. juni 2025 om elektroniske kommunikationsnet og -tjenester (teleloven)
[2] Europa- Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (e-databeskyttelsesdirektivet)

lagring, som er nødvendig for overføring af en kommunikation, forudsat at princippet om kommunikations-hemmelighed ikke berøres heraf."

Persondatasikkerhedsbekendtgørelsen[3] § 3 regulerer risikostyring i forbindelse med udbud af bl.a. elektroniske kommunikationstjenester, og har følgende ordlyd:

"**§ 3.** Udbydere af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester skal løbende træffe passende tekniske og organisatoriske foranstaltninger med henblik på at styre risici for persondatasikkerheden i forbindelse med udbud af elektroniske kommunikationstjenester og nummeruafhængige interpersonelle 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 og nummeruafhængige interpersonelle kommunikationstjenester."

4. Digitaliseringsstyrelsens vurdering

4.1. Spørgsmålet om *lagring af kommunikation* skal behandles i medfør af reglerne om kommunikationshemmeligheden i telelovens § 7, som har til formål at beskytte fortroligheden af brugernes kommunikation.

Telelovens § 7 implementerer e-databeskyttelsesdirektivets art. 5. Direktivets art. 5 er formuleret forskelligt fra telelovens § 7, for så vidt angår reglerne om lagring i relation til kommunikationshemmeligheden.

Efter sin ordlyd kan telelovens § 7 – efter Digitaliseringsstyrelsens opfattelse – danne grundlag for en videre adgang til lovlig anvendelse af oplysninger (*"må ikke uberettiget … udnytte oplysninger"*), end det synes at være udgangspunktet efter ordlyden af e-databeskyttelsesdirektivets art. 5 (*"forbyder især…, lagring"*). Ordlyden

[3] Bekendtgørelse nr. 1882 af 4. december 2020 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige interpersonelle kommunikationstjenester

af § 7 udelukker efter styrelsens vurdering således ikke, at et teleselskab kortvarigt kan lagre SMS-beskeder til varetagelse af saglige formål.

Det er i den forbindelse Digitaliseringsstyrelsens vurdering, at lagring af beskeder med henblik på filtrering må anses for at være et sagligt formål, der principielt kan rummes inden for ordlyden af telelovens § 7. Det er imidlertid styrelsens opfattelse, at lagringen af SMS-beskeder med henblik på filtrering, som det er sket i den konkrete sag, er af så indgribende karakter, at det forudsætter klar og tydelig hjemmel. Styrelsen finder i den forbindelse, at telelovens § 7 ikke i sig selv udgør en sådan klar og tydelig hjemmel. Styrelsen lægger herved vægt på den usikkerhed, der er forbundet med ordlyden af telelovens § 7 sammenholdt med e-databeskyttelsesdirektivets art. 5.

Uanset dette, finder Digitaliseringsstyrelsen, at der ikke er grundlag for at udtale kritik af TDC Net og TDC Brands hidtidige lagring af SMS-beskeder. Baseret på sagens forløb lægger styrelsen i den forbindelse særligt vægt på, at ordlyden af telelovens § 7 har været forbundet med usikkerhed, at selskaberne har søgt at begrænse lagringen mest muligt i forhold til at kunne forfølge et sagligt formål og at selskaberne af egen drift ophørte med lagringen, da der opstod tvivl om, hvorvidt lagringen gik ud over rammerne i lovens § 7.

4.2. Medarbejdernes *adgang til indholdet* af kommunikationen i SMS-beskeder er reguleret af reglerne om kommunikationshemmelighed i telelovens § 7, hvorefter oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf ikke må være tilgængelige for uvedkommende.

Det er i den forbindelse Digitaliseringsstyrelsens opfattelse, at telelovens § 7 ikke er til hinder for, at TDC Net og TDC Brands (og deres medarbejdere) efter omstændighederne kan få adgang til (dele af) indholdet af kommunikationen, hvis behandlingen i øvrigt sker til nødvendige og saglige formål. I lighed med det ovenfor under afsnit 4.1. anførte, er det imidlertid ligeledes styrelsens vurdering, at adgang til indholdet af beskeder med henblik på filtrering af svindel-SMS-beskeder, som det er sket i det konkrete tilfælde, ikke kan rummes inden for telelovens § 7, men forudsætter klar og tydelig hjemmel.

Digitaliseringsstyrelsen har imidlertid noteret sig, at selskabet har tilrettelagt medarbejdernes involvering i filtreringen med henblik på at minimere risikoen for, at medarbejderne er blevet præsenteret for SMS-

beskeder med indhold af personlig karakter, og som i øvrigt ikke har kunnet karakteriseres som svindel-beskeder.

I den forbindelse har Digitaliseringsstyrelsen lagt vægt på, at filtreringen har været implementeret på en sådan måde, at den manuelle gennemgang af beskederne har været begrænset til en såkaldt "kampagnevisning". Kampagnevisningen har bl.a. været implementeret på en sådan måde, at automatiske anonymiseringsmekanismer har fjernet eller maskeret udvalgte typer af personhenførbare oplysninger i de viste beskeder. En type information, der er anonymiseret, er telefonnummeret på afsender- og modtagernummer (A- og B-nummer), så de beskedeksempler, der blev vist, ikke umiddelbart kunne henføres til den afsendende eller modtagende abonnent.

Kampagnevisningen har været begrænset til beskedkategorier med ensartet indhold, der enten har været masseudsendt eller har været masseudsendt og i øvrigt opfyldte mindst ét andet kriterie som [redacted] for at mindske risikoen for, at selskabets medarbejdere blev præsenteret for private beskeder mellem to parter.

Digitaliseringsstyrelsen har endvidere noteret sig, at TDC Net og TDC Brands – i takt med at der er opnået erfaring med effekten af filtreringen – løbende har forholdt sig til og tilpasset kriterierne for udvælgelse af mulige svindelkampagner.

Det fremgår endelig af sagens oplysninger, at adgangen til beskedindhold har været begrænset til et snævert antal autoriserede medarbejdere, der har været underlagt tavshedspligt, samt at adgangen har været funktionsbetinget og knyttet til udførelsen af en konkret arbejdsopgave, der har haft til formål at beskytte TDC Net og TDC Brands brugere mod svindel.

Det er på den baggrund Digitaliseringsstyrelsens samlede vurdering, at der ikke er grundlag for at udtale kritik af den nu ophørte manuelle gennemgang af kampagner.

4.3. For så vidt angår spørgsmålet om etablering af andre *organisatoriske og sikkerhedsmæssige rammer* for SMS-filtrering, følger det af persondatasikkerhedsbekendtgørelsen § 3, at det påhviler teleudbyderne løbende at træffe passende tekniske og organisatoriske foranstaltninger med henblik på at styre risici for persondatasikkerheden.

Digitaliseringsstyrelsen har i den forbindelse noteret sig, at medarbejdernes aktiviteter i systemet har været logget. Det fremgår imidlertid af sagen, at TDC Net og TDC Brands efterfølgende ikke har kontrolleret logfiler med henblik på at vurdere, hvorvidt medarbejderne har tilgået og anvendt oplysninger i videre omfang end forudsat. Det er styrelsens opfattelse, at kravet i persondatasikkerhedsbekendtgørelsens § 3 indebærer, at kontrolkravene skærpes, når der er tale om adgang til oplysninger, der potentielt er omfattet af kommunikationshemmeligheden. En sådan skærpet kontrol kan bestå i fx løbende kontrol af logfiler.

Uagtet at TDC Net og TDC Brands således har truffet en række foranstaltninger med henblik på at begrænse medarbejdernes adgang til indholdet af kommunikationen og viden om modtagere, se pkt. 4.2, finder Digitaliseringsstyrelsen, at selskaberne som minimum burde have foretaget løbende stikprøvekontrol af logfilerne. Styrelsen udtaler derfor kritik af, at selskabernes manglende kontrol af logfiler ikke har været i overensstemmelse med persondatasikkerhedsbekendtgørelsens § 3.

4.4. For så vidt angår TDC Net og TDC Brands *styring af risici i projektet*, skal Digitaliseringsstyrelsen bemærke, at det i tilknytning til udarbejdelsen af initiativbeskrivelserne af oktober 2024 blev lagt til grund, at SMS-filtreringen hverken forudsatte lagring af beskedindhold eller menneskelig involvering med henblik på at verificere systemets identifikation af SMS-beskeder. Den efterfølgende implementering og drift af filtreringen viste imidlertid, at disse forudsætninger ikke holdt stik, og at selskaberne i en periode herefter lagrede SMS-beskeder og tilgik dele af indholdet heraf.

Det følger som nævnt ovenfor af persondatasikkerhedsbekendtgørelsens § 3, at der skal træffes passende tekniske og organisatoriske foranstaltninger med henblik på at styre risici for persondatasikkerheden. Dette indebærer efter Digitaliseringsstyrelsens opfattelse bl.a. en generel forpligtelse til, at TDC Net og TDC Brands ved implementeringen af nye løsninger løbende påser, at der ikke etableres en utilsigtet behandling af personoplysninger.

Det er Digitaliseringsstyrelsens vurdering, at TDC Net og TDC Brands faktiske implementering af SMS-filtreringen har medført en behandling af personoplysninger, der utilsigtet er sket i videre omfang end oprindeligt forudsat af selskaberne. Det er endvidere styrelsens vurdering, at dette skred er sket utilsigtet og uden en forudgående

stillingtagen til, om den faktiske implementering fortsat fandt sted inden for rammerne af teleloven.

Det er på denne baggrund Digitaliseringsstyrelsens vurdering, at TDC Net og TDC Brands ikke har haft det fornødne fokus på, hvorvidt implementeringen og driften af løsningen til stadighed var i overensstemmelse med de oprindelige og godkendte rammer for projektet. Styrelsen lægger i den forbindelse særligt vægt på, at projektet forudsatte en omfattende og potentiel indgribende behandling af fortrolige oplysninger, hvilket efter styrelsens opfattelse skærper kravene til løbende risikostyring af projektet.

Digitaliseringsstyrelsen finder derfor, at TDC Net og TDC Brands– ved at implementere en løsning uden at have et klart billede af, hvordan løsningen ville fungere i relation til lagring og menneskelig adgang til indholdet af kommunikation – ikke har truffet passende foranstaltninger med henblik på at styre risici for persondatasikkerheden. Styrelsen udtaler derfor kritik af, at selskabernes projektstyring ikke er sket i overensstemmelse med persondatasikkerhedsbekendtgørelsens § 3.

Digitaliseringsstyrelsen offentliggør en kopi af dette brev på styrelsens hjemmeside, men foretager sig herefter ikke yderligere i anledning af TDC Net og TDC Brands hidtidige – og nu ophørte – filtrering af SMS-beskeder.

5. Klagevejledning

Digitaliseringsstyrelsens 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 Digitaliseringsstyrelsen 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.

Digitaliserings-
styrelsen

Med venlig hilsen

Signe S. Mikkelsen
Fuldmægtig