



Borgerforslag - støtterblanket

Du kan bruge denne blanket til at støtte et borgerforslag, hvis du ikke kan bruge den digitale løsning på borgerforslag.dk.

Der er ingen forpligtelser forbundet med at være støtter af et forslag.

Dine personoplysninger bliver ikke offentliggjort, når du er støtter af forslaget. Vi henviser i øvrigt til politikken for, hvordan vi behandler personoplysninger, på borgerforslag.dk. Du kan se et uddrag af persondatapolitikken med de relevante afsnit for støttere nedenfor.

Sådan støtter du ikkedigitalt et borgerforslag

1. Når du har udfyldt blanketten og underskrevet den, skal du sende den som fysisk post til Christiansborg, Folketinget, Rigsdagsgården 4, 1218 København K, att.: Borgerforslag.
2. Når Folketingets Administration har modtaget blanketten, kontrollerer administrationen ved at slå op i Det Centrale Personregister (CPR), at du har stemmeret til folketingsvalg. Herefter registrerer vi din støtte i systemet, og du modtager en bekræftelse pr. brev eller e-mail på, at din støtte er registreret.

Titel

Danmark skal afvise chatkontrol og beskytte privat digital kommunikation

Id: FT-24513

Forslag

Folketinget skal pålægge regeringen at arbejde aktivt imod og stemme nej til enhver EU-regulering, der muliggør generel eller automatiseret scanning af borgeres private digitale kommunikation.

Det skal gælde både obligatorisk scanning og ordninger, hvor scanning beskrives som frivillig, midlertidig, risikobaseret eller teknisk begrænset, hvis resultatet i praksis er, at private beskeder, e-mails, chats, billeder, videoer, links eller filer kan gennemgås uden konkret mistanke og uden forudgående retskendelse.

Danmark skal ikke støtte regler, der svækker eller omgår end-to-end-kryptering, herunder client-side scanning, hvor indhold kontrolleres på brugerens enhed før kryptering. Danmark skal heller ikke støtte regler, der skaber en permanent teknisk infrastruktur til masseovervågning af lovlige borgere.

Folketinget skal samtidig pålægge regeringen at arbejde for en alternativ europæisk indsats mod seksuelt misbrug af børn online. Den indsats skal bygge på målrettet efterforskning, domstolskontrol, hurtig fjernelse af kendt ulovligt materiale, styrket internationalt politisamarbejde, bedre ressourcer til politiets specialenheder, hjælp til ofre og forebyggelse af grooming og sextortion.

Regeringen skal desuden fremlægge en offentlig juridisk redegørelse for, hvordan forslag om chatkontrol forholder sig til Grundlovens § 72, retten til privatliv, kommunikationshemmelighed, databeskyttelse og kravet om proportionalitet.

Bemærkninger til forslaget

Chatkontrol rejser et grundlæggende spørgsmål om, hvor grænsen går mellem målrettet kriminalitetsbekæmpelse og generel overvågning af befolkningen.

Forslaget stilles ikke for at svække beskyttelsen af børn. Seksuelt misbrug af børn er en af de mest alvorlige former for kriminalitet, og gerningspersoner skal efterforskes og retsforfølges effektivt. Men kampen mod



FT-24513 - Danmark skal afvise chatkontrol og beskytte privat digital kommunikation

alvorlig kriminalitet må ikke føre til, at alle borgeres private beskeder gøres til genstand for automatiseret kontrol.

Private digitale beskeder har i dag samme samfundsmæssige funktion som breve og telefonsamtaler. De bruges til samtaler med familie, venner, læger, advokater, journalister, arbejdspladser, myndigheder og andre nære relationer. Når kommunikationen flytter fra brev og telefon til digitale tjenester, bør beskyttelsen ikke blive svagere.

Grundlovens § 72 beskytter bl.a. mod undersøgelse af breve og brud på post-, telegraf- og telefonhemmeligheden, medmindre der er lovhjemmel og som udgangspunkt retskendelse. Bestemmelsen blev skrevet før moderne chat apps, men dens princip er stadig klart: private meddelelser skal ikke kunne undersøges vilkårligt eller generelt. Folketinget bør derfor kræve, at digital kommunikation behandles med mindst samme alvor som ældre kommunikationsformer.

Chatkontrol vender et centralt retsstatsprincip på hovedet. Normalt bør indgreb i privat kommunikation kræve konkret mistanke, nødvendighed, proportionalitet og uafhængig kontrol. Ved generel scanning undersøges derimod store mængder kommunikation fra mennesker, der ikke er mistænkt for noget. Det betyder, at den lovlige borger i praksis behandles som et muligt efterforskningsobjekt.

Det er ikke tilstrækkeligt at kalde scanning frivillig. Hvis EU-lovgivning gør det muligt eller forventeligt, at store platforme scanner private beskeder, skabes der alligevel en overvågningsinfrastruktur. Når først en sådan infrastruktur findes, kan den senere udvides til andre formål, andre typer indhold og andre politiske prioriteter. Det er en reel risiko for formålsudvidelse.

Chatkontrol er også et cybersikkerhedsproblem. End-to-end-kryptering virker, fordi kun afsender og modtager skal kunne læse indholdet. Hvis en tjeneste skal scanne beskeder før eller under afsendelse, skal indholdet gøres tilgængeligt for software uden for den private samtale. Det kan ske gennem client-side scanning på brugerens enhed eller andre tekniske løsninger, men resultatet er det samme: fortroligheden omgås.

Et sådant system vil skabe nye angrebsflader. Software, der kan gennemgå private beskeder, bliver et oplagt mål for cyberkriminelle, fremmede stater, spywareproducenter og andre aktører. Sårbarheder, fejlkonfigurationer eller misbrug kan få langt større konsekvenser, netop fordi systemet er bygget til at få adgang til følsomt indhold.

Derudover kan automatiske scanningssystemer tage fejl. Falske positive kan ramme uskyldige borgere og føre til, at private billeder, familie billeder eller anden følsom kommunikation bliver markeret, gemt, videresendt eller vurderet af andre. Jo større mængder kommunikation der scannes, desto større bliver antallet af fejl i praksis, selv hvis fejlprocenten på papiret er lav.

Danmark bør ikke støtte EU-regler, der presser udviklere til at bygge overvågning ind i kommunikationstjenester. Sikker kommunikation er ikke kun vigtig for almindelige borgere. Den beskytter også børn, journalister, advokater, whistleblowere, virksomheder, offentlige myndigheder og personer i udsatte situationer. Svækkes den digitale sikkerhed for alle, bliver samfundet samlet set mindre sikkert.

Der findes bedre alternativer. Indsatsen bør rettes mod gerningspersoner, kendt ulovligt materiale og konkrete risikomiljøer. Det kræver flere ressourcer til politiets specialiserede enheder, bedre behandling af anmeldelser, hurtigere internationalt samarbejde, mere effektiv fjernelse af materiale ved kilden, bedre støtte til ofre og stærkere forebyggelse af grooming og sextortion. Det er målrettede tiltag, som kan styrke børns beskyttelse uden at indføre masseovervågning.

Danmark bør også være åben om sin EU-position. Borgerne skal kunne se, om regeringen arbejder for eller imod regler, der påvirker privatliv, kryptering og kommunikationshemmelighed. Et så vidtgående indgreb må



FT-24513 - Danmark skal afvise chatkontrol og beskytte privat digital kommunikation

ikke behandles som en teknisk detalje i EU-forhandlinger.

Hvis en EU-retsakt måtte være uforenelig med Grundloven, følger det af dansk forfatningsret, at Grundloven skal gå forud. Folketinget bør derfor ikke vente på, at problemet først opstår efter vedtagelse. Regeringen bør pålægges allerede nu at afvise chatkontrol og fremlægge en juridisk vurdering af forholdet til Grundlovens § 72 og øvrige grundlæggende rettigheder.

Et frit samfund skal kunne bekæmpe alvorlig kriminalitet uden at gøre alle borgeres private samtaler søgbare. Danmark bør stå fast på, at børns sikkerhed og borgernes grundlæggende rettigheder ikke er modsætninger. Begge dele kræver målrettede, retssikre og teknisk ansvarlige løsninger.

Forslag stillet af

Sigurd Philip Krag Berthel
Danmark Fax

Kontaktoplysninger

kpbs1280@protonmail.com

Medstillere

Sean Chapman Lindquist
Tårnby

Anders Kildahl Johansen
København

Tim Løvegaard Lagermann
Tårnby

Daniel Meier Sørensen
Nordfyns

Josefine Krag Yaqoob
København

Kontaktoplysninger

seanchapman111@gmail.com
53274811

anders@kildahl.me

timlagermann@gmail.com

daoos9661@gmail.com

josefine.yaqoob@gmail.com



Støtteerklæring

For borgere der ikke kan bruge den digitale løsning på borgerforslag.dk.

Jeg ønsker at være støtter for det borgerforslag, der fremgår af denne blanket.

Fulde navn (skal udfyldes)

Adresse (skal udfyldes)

Postnummer (skal udfyldes)

By (skal udfyldes)

Cpr-nummer (skal udfyldes)

E-mail (hvis du ønsker en kvittering for registreringen af din støtte pr. e-mail)

Dato

Underskrift

Med min underskrift bekræfter jeg, at jeg har læst forslaget, og at jeg har læst og accepteret samtykkeerklæringen nedenfor.

Erklæring om samtykke for støttere

Jeg har læst og er indforstået med Politikken for behandling af personoplysninger i ordningen om borgerforslag. Du kan læse et uddrag af politikken på følgende side.

Jeg er indforstået med

- at personoplysninger om mig behandles som beskrevet, når jeg benytter ordningen,
- at jeg som støtter af et borgerforslag ikke kan trække min støtte tilbage, når jeg har givet den, og
- at jeg kun kan støtte det samme borgerforslag én gang.



Sådan behandler vi dine personoplysninger på borgerforslag.dk

Når du anvender hjemmesiden borgerforslag.dk som hovedstiller af et borgerforslag, medstiller af et borgerforslag eller støtter af et borgerforslag, behandler vi nogle oplysninger om dig. Dette er nærmere beskrevet i det følgende.

Derfor behandler vi dine personoplysninger

Vores formål med at behandle dine personoplysninger på borgerforslag.dk er at varetage de opgaver, der følger af:

- Lov nr. 1672 af 26. december 2017 om en ordning for borgerforslag med henblik på behandling i Folketinget. Loven er ændret ved lov nr. af 698 af 24. maj 2022.
- Bekendtgørelse nr. 843 af 8. juni 2022 om en ordning for borgerforslag med henblik på behandling i Folketinget.

De oplysninger, vi indsamler i forbindelse med borgerforslagsordningen, bruger vi ikke til andre formål, og vi videregiver dem ikke til andre.

Særligt for ikkedigitale borgere

Borgere, som ikke benytter den digitale løsning på borgerforslag.dk, og som vi herefter kalder ikkedigitale borgere, kan i stedet benytte en papirbaseret løsning. De kan tilkendegive, at de ønsker at være hovedstiller, medstiller eller støtter af et borgerforslag, ved at indsende en blanket med de relevante oplysninger til Folketingets Administration med fysisk post.

Når vi modtager en blanket fra en ikkedigital borger, undersøger vi ved at slå op i Det Centrale Personregister, om borgeren har stemmeret til folketingsvalg. Det er en betingelse for at benytte borgerforslagsordningen, at man har stemmeret til folketingsvalg, og oplysningerne om stemmeret bruger vi til at sikre, at borgeren opfylder denne betingelse.

Det Centrale Personregister indeholder ikke oplysninger om valgret for personer med fast bopæl på Færøerne. Disse skal derfor afgive en erklæring om, at de har stemmeret til Folketinget. Erklæringen træder i stedet for Folketingets Administrations opslag af, at den pågældende har valgret, ved at slå personen op i Det Centrale Personregister. Hvis de ikke har et cpr-nummer, skal de i stedet oplyse deres færøske p-tal.

Hvis betingelsen om stemmeret er opfyldt, indtaster Folketingets Administration oplysningerne fra blanketten i systemet. Vi behandler de indtastede oplysninger på samme måde som de tilsvarende oplysninger om borgere, der har brugt den digitale løsning.

Læg mærke til, at vi gemmer korrespondance pr. post eller e-mail mellem Folketingets Administration og ikkedigitale borgere i Folketingets Administrations almindelige journal- og sagsbehandlingssystemer. Formålet er navnlig at sikre dokumentation af sagsbehandlingen, f.eks. for at kunne rekonstruere hændelsesforløb, hvis der skulle opstå uenighed mellem Folketingets Administration og borgere om administrationen af ordningen.

De blanketter, vi modtager fysisk, gemmer vi i et afgrænset tidsrum. Vi opbevarer dem bag lås, og de er kun tilgængelige for medarbejdere i Folketingets Administration, som har brug for at få adgang til oplysningerne i blanketterne for at varetage arbejdsopgaver i relation til borgerforslagsordningen.

Sikkerhed og logning i den digitale løsning på borgerforslag.dk

Kommunikation mellem brugerne og systemet foregår via en krypteret og sikker forbindelse.

Systemet er hostet eksternt, og Folketingets Administration har indgået en databehandleraftale, som vi løbende kontrollerer.

Vi opbevarer data, som vi behandler i systemet, på servere, der fysisk befinder sig i EU.



Dataansvarlig myndighed og kontakt

Folketinget er den dataansvarlige myndighed for borgerforslagsordningen.

Du kan kontakte Folketingets Administration med spørgsmål om, hvordan vi i Folketingets Administration behandler personoplysninger i forbindelse med borgerforslagsordningen. Du kan sende en e-mail til os på borgerforslag@ft.dk, eller du kan ringe til os på telefon 3337 5500.

Du kan også sende et brev til os:

Christiansborg, Folketinget
Att.: Borgerforslag
Rigsdagsgården 4
1218 København K

Du kan også kontakte Folketingets Administrations databeskyttelsesrådgiver på e-mail dpo@ft.dk eller på telefon 3337 5500 eller ved at sende et brev att. databeskyttelsesrådgiveren.