Advokatrådet

ADVOKAT SAMFUNDET

Ministeriet for Fødevarer, Landbrug og Fiskeri - Fødevarestyrelsen
Mørkhøj Bygade 19
2860 Søborg

32@fvst.dk + smsa@fvst.dk

KRONPRINSESSEGADE 28
1306 KØBENHAVN K
TLF 33 96 97 98
FAX 33 36 97 50

DATO: 1. august 2013
SAGSNR.: 2013 - 1962
ID NR : 245990

Høring - over forslag til lov om ændring af forskellige lovbestemmelser om obligatorisk digital kommunikation, klager mv.

Ved e-mail af 19-06-2013 har Ministeriet for Fødevarer, Landbrug og Fiskeri - Fødevarestyrelsen anmodet om Advokatrådets bemærkninger til ovennævnte udkast/forslag.

Advokatrådet har følgende bemærkninger:

I det omfang lovforslaget vedrører kommunikation med borgere, er det Advokatrådets generelle holdning, at der fortsat er en ikke ubetydelig gruppe af borgere, som ikke anvender IT. Borgere bør derfor som udgangspunkt modtage korrespondance i papirform medmindre de positivt har meddelt, at de kun ønsker at modtage korrespondance elektronisk, se Advokatrådets tidligere høringssvar herom. Det er efter Advokatrådets opfattelse en af de største aktuelle retssikkerhedsmæssige udfordringer, at staten forudsætter, at alle borgere er i stand til at kommunikere elektronisk med det offentlige, når alt tyder på, at en stor del af borgerene - herunder ældre - herved risikerer at blive ladt i stikken.

Herudover har Advokatrådet bemærkninger til lovforslagets forhold til Persondataloven. Persondataloven regulerer behandling af personoplysninger, som sker elektronisk eller som vil blive indeholdt i et register. En personoplysning er enhver form for information om en identificeret eller identificerbar fysisk person (persondatalovens § 3, nr. 1). Det betyder, at oplysninger om juridiske personer falder uden for lovens almindelige regulering, mens oplysninger om enkeltmandsejede virksomheder falder inden for lovens anvendelsesområde. Virksomhedsoplysninger, som kan identificere fysiske personer, er omfattet af definitionen på en personoplysning. De typer af personoplysninger, som er relevante i forhold de ændrede regler om obligatorisk digital kommunikation, vil typisk være almindelige, fortrolige eller semi-følsomme (oplysninger om strafbare forhold). Denne sondring har betydning for, hvornår der skal anvendes hhv. kryptering eller stærk kryptering, når oplysningerne sendes over åbne netværk (internettet).

Almindelige personoplysninger kan sendes over internettet, blot der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke får adgang til de sendte personoplysninger.

Behandling er enhver operation eller række af operationer – med eller uden brug af edb – som personoplysninger gøres til genstand for (persondatalovens § 3, nr. 2). Behandlingsbegrebet skal forstås bredt og omfatter således også den videregivelse af personoplysninger, som sker ved fremsendelse af e-mails mellem Fødevareministeriet og borgere eller virksomheder, som indeholder personoplysninger, som identificerer fysiske personer.

Det fremgår af bemærkningerne til udkastet til lovforslag, at bestemmelserne om obligatorisk digital kommunikation alene vedrører kommunikation om forhold, som er reguleret af de love, som er omfattet af udkastet til lovforslag. Kommunikation om forhold, som er omfattet af andre love, fx persondataloven, forvaltningsloven eller offentlighedsloven, berøres derimod ikke af udkastet til lovforslag (pkt. 3.2).

Meningen med disse bemærkninger forekommer ikke klar. Hvis en virksomhed eller en borger kommunikerer med Fødevarestyrelsen, og kommunikationen indebærer behandling af personoplysninger, vil den pågældende kommunikation både være omfattet af persondataloven og den relevante lovgivning på Fødevareministeriets område. De citerede uddrag af bemærkningerne til udkast til lovforslag kunne forlede læseren til at tro, at Fødevareministeriet er af den opfattelse, at forhold enten er omfattet af lovgivning, der henhører under ministeriet, eller af anden lovgivning, fx persondataloven. En sådan antagelse er imidlertid ikke – eller behøver ikke at være – korrekt. Det vil således i praksis i vidt omfang kunne forekomme, at information om forhold omfattet af Fødevareministeriets lovgivning tillige indeholder oplysninger, der utvivlsomt er omfattet af – og derfor (tillige) skal overholde – persondatalovens regler. Skriftlige henvendelser til Fødevarestyrelsen om forhold, som er omfattet af en af de love, der omhandles i udkastet til lovforslag, og som indeholder personoplysninger, skal som udgangspunkt overholde reglerne i persondataloven. Det fremgår ikke noget sted i bemærkningerne til udkastet til lovforslag, at der med de ændrede regler om obligatorisk digital kommunikation er tilsigtet en fravigelse af persondatalovens regler. Tilsvarende bemærkninger gør sig gældende i forhold til forvaltningsloven og offentlighedsloven.

Det fremgår af udkastet til lovforslag, at hjemlen i de pågældende love udformes som en bemyndigelse til fødevareministeren til at fastsætte nærmere regler om digital kommunikation. Bemyndigelsen vil blive udmøntet løbende, i takt med at de tekniske løsninger er på plads, og når borgere og virksomheder er parate.

Datatilsynet har behandlet spørgsmålet om kryptering ved fremsendelse af fortroligt materiale i en sag om e-post-kvitteringsmails på www.bibliotek.dk. Datatilsynet gav i 2005 og forlængede undtagelsesvist i 2010 en dispensation, så det var muligt at fremsende reservationskvitteringer ukrypteret, selv om kvitteringerne ideholdt fortrolige oplysninger (2004-082-0188 og 2009-069-0006). Da der endnu ikke er

fremkommet tekniske løsninger, som kan anvendes til kryptering af indholdet i bibliotekernes kvitteringsmails, er dispensationen stadig gældende.

Det fremgår af udkastet til lovforslag, at det er hensigten, at al relevant skriftlig kommunikation mellem Fødevarestyrelsen og virksomheder eller fysiske personer med tiden skal foregå digitalt. Dette skal enten ske via den digitale postløsning Offentlig Digital Post (fx visse afgørelser, herunder forbud eller påbud) eller via e-mail eller digitale selvbetjeningsløsninger.

Kommunikation via den digitale postløsning Offentlig Digital Post vil overholde sikkerhedskravene i persondataloven, fordi der ved brug af løsningen ikke sendes oplysninger i åbne netværk. Der er derfor ikke krav om kryptering, når der sendes fortrolige, semi-følsomme eller følsomme oplysninger. Det er mere problematisk i en persondataretlig kontekst, når der er tale om kommunikation via mail af fortrolige, semi-følsomme eller følsomme oplysninger (behandling af personoplysninger, hvor der skal ske anmeldelse til Datatilsynet efter reglerne i persondatalovens kap. 12). Det fremgår direkte af den såkaldte anmeldelsesbekendtgørelses § 7, at syv nærmere opregnede former for behandling af personoplysninger, som foretages i forbindelse med kontrol i henhold til landbrugs-, fiskeri-, veterinær- og fødevarelovgivningen, er undtaget fra anmeldelse til Datatilsynet. De opregnede former er bl.a. oplysninger om autorisationer, bevillinger, tilladelser og lignende (nr. 4) samt oplysninger om meddelte påbud og forbud eller lignende (nr. 5). I forhold til reglerne om kryptering har det den konsekvens, at de opregnede former for behandling anses for fortrolige og derfor kun må sendes over åbne net, som f.eks. internettet, hvis oplysningerne er krypteret, jf. vejledningen til sikkerhedsbekendtgørelsen pkt. 15.

Det vil ifølge bemærkningerne i udkastet til lovforslag fremgå af den bekendtgørelse, som udmønter bemyndigelsen, hvem der bliver omfattet af pligten til at kommunikere digitalt med ministeriet, om hvilke forhold og på hvilken måde. I den forbindelse bemærkes, at det vil være hensigtsmæssigt, hvis det bestemmes, at den primære digitale kommunikation skal foregå via den digitale postløsning Offentlig Digital Post. Dette skyldes, at fortrolige, semi-følsomme eller følsomme oplysninger ikke må sendes ukrypteret via e-mail. Borgere og virksomheder (og herunder rådgivere) skal derfor i forbindelse med den enkelte implementering informeres om, at de ikke må sende fortrolige, semi-følsomme eller følsomme oplysninger til Fødevareministeriet, hvis de ikke anvender en kryptering, som svarer til den, der kræves i henhold til sikkerhedsbekendtgørelsen med tilhørende vejledning. Det bemærkes i den forbindelse, at Datatilsynet i flere afgørelser har understreget, at den registrerede, hvorom der behandles fortrolige, semi-følsomme eller følsomme oplysninger, ikke kan samtykke til, at sikkerhedsniveauet forringes.

Med venlig hilsen

Lars Økjær Jørgensen

DANSK ERHVERV
BØRSEN
DK-1217 KØBENHAVN K
WWW.DANSKERHVERV.DK

T. +45 3374 6000
F. +45 3374 6080
–
INFO@DANSKERHVERV.DK

Fødevarestyrelsen
Stationsparken 31-33
2600 Glostrup

Sendt pr. e-mail: 32@fvst.dk og smsa@fvst.dk

2. august 2013

Høring over forslag til lov om ændring af forskellige lovbestemmelser om obligatorisk digital kommunikation, klager m.v.
Dansk Erhverv har modtaget ovennævnte høring og har følgende kommentarer.

Generelle bemærkninger
Dansk Erhverv støtter generelt den igangværende digitalisering af den offentlige sektor, som vil understøtte vækst og fremgang for dansk erhvervsliv i en stadig mere global og digital verden samt sikre størst mulig ressourceudnyttelse i den offentlige sektor.

Således støtter Dansk Erhverv også den aktuelle indsats med at indføre Digital Post i danske virksomheder, så de bliver klar til at modtage post via den digitale kanal i takt med, at de enkelte myndigheders løsninger bliver taget i brug, jf. Dansk Erhvervs høringssvar den 1. juli 2013 om udkast til bekendtgørelse m.v. om fritagelse af juridiske enheder med CVR-nummer samt fysiske personer med erhvervsaktiviteter for tilslutning til Digital Post.

Der er en række omstillingsomkostninger forbundet med digitaliseringen, men Dansk Erhverv forventer, at virksomheder efterfølgende vil drage fordel af nemmere indberetning og samspil med det offentlige.

Det er dog helt afgørende, at de digitale løsninger er af en kvalitet, der sikrer tilstrækkelig adgang til hjælp i overgangsperioden og rettidig kommunikation til virksomhederne, samt at de digitale løsninger er tiltrækkeligt fleksible og understøtter forretningsprocesserne i virksomhederne.

Dansk Erhverv finder det vigtigt, at obligatorisk digital kommunikation i videst mulig udstrækning implementeres på samme måde overalt i det offentlige, da de samme virksomheder vil møde det offentlige digitalt gennem en række forskellige myndighedskontakter. Genkendelighed og ensartethed på tværs af offentlige myndigheder er derfor en forudsætning for at høste de potentielle frugter af ressourceudnyttelse i offentlig kontakt med virksomheder.

Forslaget forventes at træde i kraft den 1. januar 2014, og de tilhørende bekendtgørelser, der skal udmønte og dermed iværksætte digitaliseringen konkret, udstedes løbende. Dansk Erhverv mener, at det vil være hensigtsmæssigt med en løbende udrulning af den digitale kommunikation i takt med, at de tekniske systemer kommer på plads, og kan levere den nødvendige forretningsunderstøttelse

DANSK ERHVERV

LEL
lel@danskerhverv.dk

Specifikke bemærkninger

Overgangsordninger
Dansk Erhverv lægger vægt på betydningen af forslagets bemærkning om, at der vil kunne fastsættes overgangsordninger, så det i en periode fortsat vil være frivilligt at indberette digitalt eller evt. søges om dispensation. Digital kommunikation vil være helt nyt for mange virksomheder, og det er derfor helt afgørende, at der fra offentlig side afsættes de nødvendige ressourcer til oplysning, support og løbende drift.

Uændret praksis i kommunikation
Det er efter Dansk Erhvervs opfattelse afgørende, at virksomheders nuværende kommunikation med det offentlige også fremadrettet følger samme principper som hidtil, samt at overgangen til digital kommunikation ikke ændrer virksomheders nuværende kommunikation med fødevaremyndighederne.
Digital Post m.v. er et medie som ikke i sig selv bør få indflydelse på indholdet eller nuværende praksis (regler, tidsfrister eller andet) af kommunikationen mellem fødevaremyndighederne og virksomhederne.

Der udestår desuden en afklaring af den fremtidige praksis med håndtering af P-numre i forhold til Offentlig Digital Post, det gælder både i forhold til den snarlige udrulning af Offentlig Digital Post og af den efterfølgende obligatoriske digitale kommunikation på Fødevareministeriets område.
I tilfælde hvor virksomheder med flere butikker med særskilte P-numre (butikskæder) i dag modtager post fra det offentlige til den centrale administration, bør dette fortsat være muligt. Det indebærer, at kommunikation og kontakt med kæder, der har flere butikker med særskilte P-numre, fortsat skal kunne forgå centralt og ikke til de enkelte butikker.

Dansk Erhverv uddyber naturligvis gerne ovenstående.

Med venlig hilsen

Lotte Engbæk Larsen

DATATILSYNET

Ministeriet for Fødevarer, Landbrug og Fiskeri
Fødevarestyrelsen
Stationsparken 31-33
2600 Glostrup

Sendt til: smsa@fvst.dk med kopi til:
32@fvst.dk

2. august 2013

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2013-112-0208
Sagsbehandler
Mette Hansen
Direkte 3319 3212

Vedrørende høring over udkast til forslag til lov om ændring af forskellige lovbestemmelser om obligatorisk digital kommunikation, klager mv.

Ved e-mail af 18. juni 2013 har Fødevarestyrelsen anmodet om Datatilsynets eventuelle bemærkninger til ovennævnte lovforslag.

Lovforslaget giver umiddelbart Datatilsynet anledning til følgende bemærkninger:

2. Datatilsynet henviser til sine generelle betragtninger om obligatorisk brug af digitale løsninger i tilsynets høringssvar af 13. februar 2012 til Digitaliseringsstyrelsen vedrørende forslaget om digital post og tilsynets høringssvar af 10. februar 2012 til Digitaliseringsstyrelsen vedrørende lovforslaget om obligatorisk digital selvbetjening. Kopi vedhæftes.

3. Af afsnit 3.2. i de almindelige bemærkninger til det fremsendte lovforslag fremgår det bl.a., at:

> *"Lovforslagets bestemmelser om obligatorisk digital kommunikation vedrører alene kommunikation om forhold, som er reguleret af de af lovforslaget omfattede love. Kommunikation om forhold, som er omfattet af andre love, f.eks. persondataloven, forvaltningsloven eller offentlighedsloven berøres derimod ikke af lovforslaget. Dvs. at der ikke tilsigtes ændringer i f.eks. persondatalovens § 31, indsigelser imod, at oplysninger om vedkommende gøres til genstand for databehandling, jf. § 35, eller krav om berigtigelse m.v. af oplysninger, jf. § 37."*

Tilsynet går herefter umiddelbart ud fra, at persondataloven[1] – inden for dens anvendelsesområde – fuldt ud skal finde anvendelse også i forhold til kommunikation, der omfattes af lovforslaget.

Hvis der tilsigtes fravigelse af persondataloven, skal dette fremgå klart, og der må tillige indgå en vurdering af, hvorvidt den tiltænkte fravigelse er forenelig med databeskyttelsesdirektivet[2]. Hertil kommer, at eventuelle bestemmelser, der fraviger persondataloven, skal fastsættes i selve loven og ikke i bekendtgørelsesform.

3.1. I øvrigt skal tilsynet pege på, at forholdet til persondatalovens § 39 omtales i afsnit 5.1.2.1. Det kunne evt. være hensigtsmæssigt at samle forholdet til persondataloven i afsnit 3.2.

---

[1] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.
[2] Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

Datatilsynet har i øvrigt noteret sig, at Fødevarestyrelsen har vurderet, at persondatalovens § 39 ikke finder anvendelse på de maskinelle afgørelser, som er omfattet af lovforslaget, da de foreslåede bestemmelser ikke omfatter afgørelser, der har retsvirkninger for eller i øvrigt berører den pågældende i væsentlig grad, og som alene er truffet på grundlag af elektronisk databehandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold.

4. Af afsnit 3.4. i de almindelige bemærkninger til det fremsendte lovforslag fremgår det bl.a., at:

> *"Offentlige myndigheder skal, når det er relevant, imidlertid anvende en offentlig digital signatur, der baserer sig på den nationale offentlige OCES (Offentlige Certifikater til Elektronisk Service) standard. Det er et krav, at den digitale signatur har et sikkerhedsniveau svarende til OCES-standarden eller højere. Standarden er fastlagt i certifikatpolitikker, der administreres og reguleres af Digitaliseringsstyrelsen."*

Tilsynet er enigt i, at offentlige myndigheders behandling af personoplysninger i en række tilfælde vil medføre behov for at anvende digitale signaturer med et sikkerhedsniveau svarende til OCES-standarden eller højere. Kvalificerede certifikater med et højere niveau kan i princippet også bruges.

Det står imidlertid ikke umiddelbart Datatilsynet klart, hvad der menes med, at offentlige myndigheder, *når det er relevant*, skal anvende en offentlig digital signatur, der baserer sig på den nationale offentlige OCES standard.

Tilsynet lægger i den forbindelse til grund, at der i dag på en række områder foregår digital kommunikation mellem myndigheder og borgere eller virksomheder, uden at anvendelse af digital signatur er et krav efter persondataloven. F.eks. hvor de personoplysninger, der udveksles, ikke er af fortrolig eller følsom karakter.

Hvis hensigten er at kræve højere sikkerhed, end hvad der i praksis kræves efter persondataloven, bør dette fremgå tydeligere. Der bør i den forbindelse foretages en vurdering af dels de ulemper og omkostninger, som et krav om øget anvendelse af digital signatur vil medføre for myndigheder, borgere og virksomheder, dels forholdet til databeskyttelsesdirektivets regler om datasikkerhed, herunder direktivets artikel 17, hvoraf bl.a. følgende fremgår:

> *"Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelser af oplysninger i et net, samt mod enhver anden form for ulovlig behandling."*
>
> *Disse foranstaltninger skal under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes."*

Tilsynet skal således anmode om, at afsnittet præciseres.

5. Af afsnit 5.1 i de almindelige bemærkninger til det fremsendte lovforslag fremgår det bl.a., at:

> *"Det er i den forbindelse uden betydning, at den pågældende oplever, at den pågældendes egen computer ikke fungerer, at den pågældende har mistet koden til sin digitale signatur eller oplever lignende hindringer, som det er op til den pågældende at overvinde. I så fald må vedkommende f.eks. anvende en computer på et bibliotek eller anmode en rådgiver om at varetage kommunikationen på den pågældendes vegne."*

Datatilsynet skal her til bemærke, at det er tilsynets opfattelse, at såfremt borgerne/virksomhederne henvises til at anvende bibliotekernes PC´ere, bør det af afsnittet om persondataloven fremgår, hvorledes det er muligt at fremsende oplysninger via en PC på et bibliotek og samtidig leve op til persondatalovens sikkerhedskrav.

5.1. Af afsnit 5.1. i de almindelige bemærkninger til det fremsendte lovforslag fremgår det endvidere, at:

> *"Ved kommunikation via e-mail kan der stilles krav om sikker identifikation, således at mailen afsendes med digital signatur for at sikre, at afsenderen er den, vedkommende giver sig ud for at være. Er der tale om udveksling af følsomme oplysninger, bør dette enten ske ved krypterede mails (dette forudsætter typisk et certifikat til den pågældende myndigheds e-postadresse) eller den offentlige digitale postløsning. Der vil således også kunne fastsættes regler om, at visse oplysninger sendes til myndighederne ved krypterede mails eller via den offentlige digitale postløsning."*

Datatilsynet skal hertil bemærke, at det ikke klart fremgår, at det ikke alene er ved transmission af følsomme oplysninger, men også ved transmission af *fortrolige* oplysninger, at der stilles krav om kryptering. Hvad angår fortrolighed kan denne sikres ved forsvarlig kryptering af de transmitterede oplysninger. Hvis der er tale om transmission af fortrolige oplysninger, herunder personnummer, skal der som minimum foretages en kryptering.

Hvis de transmitterede oplysninger er af følsom karakter (omfattet af persondatalovens § 7, stk. 1 og § 8, stk. 1), skal der anvendes en stærk kryptering, baseret på en anerkendt algoritme.

Sikkerhed for autenticitet (afsenders og modtagers identitet) og integritet (de transmitterede oplysningers ægthed) må sikres i fornødent omfang ved anvendelse af passende sikkerhedsforanstaltninger, f.eks. elektronisk signatur eller individuelle, fortrolige adgangskoder. Datatilsynet skal på denne baggrund anmode om, at afsnittet præciseres.

Afsluttende bemærkninger

Det bemærkes for en god ordens skyld, at det følger af persondatalovens § 57, at der ved udarbejdelse af bekendtgørelser, cirkulærer eller lignede generelle retsforskrifter, der har betydning for beskyttelse af privatlivet i forbindelse med behandling af personoplysninger, skal indhentes en udtalelse fra Datatilsynet.

Kopi af dette høringssvar er sendt til Justitsministeriets lovafdeling til orientering.

Med venlig hilsen

Birgit Kleis
Kommitteret

Bilag: Datatilsynets høringssvar af 13. februar 2012 til Digitaliseringsstyrelsen vedrørende lovforslaget om digital post.
Datatilsynets høringssvar af 10. februar 2012 til Digitaliseringsstyrelsen vedrørende lovforslaget om obligatorisk digital selvbetjening.

DATATILSYNET

Digitaliseringsstyrelsen
Landgreven 4
Postboks 2193
1017 København K

Sendt til: bil@digst.dk

13. februar 2012

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2012-112-0011
Sagsbehandler
Trine Cseh-Lessel
Direkte 3319 3219

Vedrørende høring over forslag til lov om Offentlig Digital Post

Hermed fremsendes Datatilsynets bemærkninger til ovennævnte høring, hvor Digitaliseringsstyrelsen ved e-post af 27. januar 2012 har bedt om tilsynets bemærkninger.

1. Datatilsynet finder det uklart, hvorvidt borgerne og virksomhederne stadig har ret til at henvende sig ved krypteret e-post til myndighederne og krav på også at få svar via sikker e-post, hvis det ønskes. Der henvises til eDag2 aftalen. Kopi af meddelelse af 2. april 2004 om eDag2 vedlægges.

Datatilsynet bemærker i den forbindelse, at der i lovforslaget ikke er krav om, at myndighederne skal sende svar digitalt til de borgere, der måtte ønske det. I forhold til borgerne synes løsningen på dette punkt ringere.

Den foreslåede obligatoriske ordning, som indebærer omfattende håndtering og lagring af borgernes og virksomhedernes breve hos en udvalgt privat virksomhed, må efter Datatilsynets opfattelse give anledning til visse principielle og i den sidste instans politiske overvejelser om hensynet til de berørte personers privatliv.

Hensynet til brugerne kan således efter tilsynets vurdering tale for, at der fortsat gives adgang til at vælge mellem forskellige løsninger til sikker digital kommunikation.

2. Det anføres flere steder, at postløsningen opfylder de relevante krav i persondataloven og sikkerhedsbekendtgørelsen. Medmindre Digitaliseringsstyrelsen er i besiddelse af en nylig revisionsrapport, hvor løsningen er gennemgået i alle detaljer i forhold til persondataloven, skal tilsynet foreslå, at teksten ændres, så det i stedet fremgår, at løsningen *skal opfylde* de omtalte krav.

3. I bemærkningerne til § 3 anføres i sidste afsnit, at "Finansministeren påser ved udpegning af den systemansvarlige, at denne også i relation til opbevaring af juridiske enheders kommunikation mv., efterlever bestemmelserne i § 41, stk. 3 -5, i lov om behandling af personoplysninger."

Datatilsynet foreslår, at sætningen omformuleres til: *Finansministeren påser ved udpegning af den systemansvarlige og i kontraktens løbetid, at den systemansvarlige og eventuelle databehandlere, som denne anvender, også i*

relation til opbevaring af juridiske enheders kommunikation mv., efterlever bestemmelserne i § 41, stk. 3 -5, i lov om behandling af personoplysninger. Finansministeriet skal orienteres om og godkende alle kontrakter med databehandlere og skal til stadighed vide, hvor oplysningerne behandles, herunder også hvor backup af data og standby-beredskab befinder sig.

4. Efter Datatilsynets opfattelse bør ansvaret for, at datasikkerheden i forbindelse med den digitale post løsning er tilstrækkeligt høj, ligge hos såvel Digitaliseringsstyrelsen som den udpegede systemansvarlige.

Datatilsynet går i den forbindelse ud fra, at Digitaliseringsstyrelsen ved fastlæggelse af sikkerhedsniveauet for den digitale post løsning har foretaget en samlet risikovurdering omfattende alle elementer i løsningen.

Efter Datatilsynets opfattelse er det endvidere nødvendigt, at der ved indretningen af de it-løsninger, som skal anvendes, er opmærksomhed på personers ret til privatliv og databeskyttelse. Beskyttelse af personoplysninger og privatliv bør efter Datatilsynets opfattelse indgå som en integreret del af ethvert digitaliseringsprojekt.

Datatilsynet skal i den forbindelse opfordre til, at der gennemføres en såkaldt privatlivsimplikationsanalyse (PIA).

Datatilsynet skal endvidere opfordre til brug af såkaldte privatlivsfremmende teknologier eller "Privacy Enhancing Technologies".

I forbindelse med tilsynets tidligere dialog med Økonomistyrelsen er det oplyst, at der udformes en form for (light) PIA (Privacy Impact Assessment) vedrørende den fællesoffentlige dokumentboks løsning. Tilsynet har imidlertid aldrig modtaget den udarbejdede PIA.

5. Persondataloven i § 41, stk. 4, indeholder en særlig regel, hvorefter der for oplysninger, der behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, skal træffes foranstaltninger, der gør det muligt at bortskaffe eller tilintetgøre oplysningerne i tilfælde af krig eller lignende forhold.

Denne regel indebærer bl.a., at visse større landsdækkende administrative systemer og specialregistre ikke må føres i udlandet.

Reglen finder efter sin ordlyd alene direkte anvendelse, når det er en offentlig myndighed, der er dataansvarlig.

Datatilsynet finder, at Finansministeriet i lyset af de hensyn, der ligger bag den omtalte bestemmelse, bør overveje, hvor digital post løsningen fysisk må afvikles og supporteres.

6. Datatilsynet skal gøre opmærksom på, at "personfølsomme oplysninger", som er anvendt i lovforslaget på side 7, ikke er et begreb, som anvendes i lovgivningen. Det er endvidere tilsynets erfaring, at udtrykket i praksis ofte giver anledning til misforståelser, da der ikke findes en entydig definition. I stedet

kan f.eks. anføres "følsomme personoplysninger", hvilket omfatter de kategorier af oplysninger af følsom karakter, som er omfattet af persondatalovens §§ 7 og 8.

7. Datatilsynet skal i øvrigt henholde sig til tilsynets udtalelse af 5. januar 2012 i forbindelse med prøhøringen over lovforslaget.

8. For god ordens skyld skal Datatilsynet bemærke, at ved udarbejdelse af bekendtgørelser, cirkulærer eller lignende generelle retsforskrifter, der har betydning for beskyttelsen af privatlivet i forbindelse med behandling af oplysninger, skal der indhentes en udtalelse fra Datatilsynet, jf. persondatalovens § 57.

Kopi af dette brev er dags dato sendt til Justitsministeriets Lovafdeling.

Med venlig hilsen

Lena Andersen
Kontorchef

Bilag: Meddelelse af 2. april 2004 om eDag2

DATATILSYNET

Digitaliseringsstyrelsen
Landgreven 4
Postboks 2193
1017 København K

Att.: Katrine Neregaard Rasmussen
Sendt til: knera@digst.dk samt jabaj@digst.dk

10. februar 2012

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2012-112-0012
Sagsbehandler
Lasse May
Direkte 3319 3214

Vedrørende høring over forslag til lov om ændring af lov om Det Centrale Personregister, lov om dag-, fritids- og klubtilbud mv. til børn og unge, lov om folkeskolen og sundhedsloven

Ved e-mail af 27. januar 2012 har Digitaliseringsstyrelsen anmodet om Datatilsynets bemærkninger til ovennævnte lovforslag.

1. I afsnit 3.2 i de almindelige bemærkninger om "persondatabeskyttelse" omtales kravet om de fornødne sikkerhedsforanstaltninger i persondatalovens § 41, stk. 3, samt sikkerhedsbekendtgørelsen, herunder bestemmelsen i bekendtgørelsens § 14.

Datatilsynet skal i tilknytning dertil påpege, at persondataloven i sin helhed skal iagttages, når der udvikles og implementeres digitale selvbetjeningsløsninger. Tilsynet skal særligt fremhæve følgende elementer:

- Grundbetingelserne om god databehandlingsskik, saglighed og proportionalitet.
- Krav om behandlingshjemmel, herunder evt. behov for samtykke. Der kan bl.a. være behov for, at borgeren i visse situationer klikker ja til, at oplysninger indhentes fra en anden myndighed f.eks. med henblik på automatisk udfyldelse af formularer.
- Iagttagelse af de registrerede personers rettigheder. Selvbetjeningsløsninger må bl.a. tage hånd om oplysningspligten, således at de oplysninger, som skal gives til borgeren, gives i forbindelse med udfyldningen af formularer og lignende online.
- Datasikkerhed: Krav om de fornødne sikkerhedsforanstaltninger, instruktion, skriftlig kontrakt med eventuelle databehandlere og kontrol med disse, sikkerhedsbekendtgørelsen.

2. Af afsnit 4.2 i de almindelige bemærkninger fremgår bl.a. følgende:

"[...] Allerede i dag er der således borgere, der får hjælp til at ansøge, anmelde, indberette mv., uanset om dette er ved udfyldelse af en blanket eller en mere digitalt baseret løsning. På tilsvarende vis er det forventningen, at der vil være borgere, som vil have behov for hjælp til at bruge digital selvbetjening. Andre institutioner som for eksempel bibliotekerne vil også være et oplagt sted at tilbyde borgerne hjælp til digital selvbetjening. De kommunale borgerservicecentre og eksempelvis bibliotekerne vil således kunne tilbyde adgang til computere og

medarbejdere, der kan hjælpe borgerne med de digitale løsninger. På den måde bliver også de mindre it-kyndige borgere efterhånden mere digitalt selvhjulpne.

Hjælp til digital selvbetjening ligger i forlængelse af den almindelige vejledningsopgave overfor borgerne, som de kommunale borgerservicecentre varetager. De offentlige myndigheder er således fortsat underlagt den sædvanlige vejledningspligt samt pligt til i givet fald at henvise en borger til rette myndighed, jf. forvaltningsloven § 7.

I kommuner, frivillige organisationer og oplysningsforbund foregår der en række aktiviteter i såvel offentligt som privat regi, som støtter op om borgernes behov for hjælp og kompetencer. Heriblandt kan nævnes kommunernes Digitale Ambassadører, ældreorganisationernes datastuer og oplysningsforbundenes itundervisning.
[...]
Det er hensigten, at borgerne fortsat skal tilbydes hjælp således, at det eksempelvis vil være muligt for en borger, der ikke selv har en PC, at møde op på borgerservice eller det lokale bibliotek og her udfylde en flytteanmeldelse eller skrive sit barn op til skolestart digitalt på kommunens PC."

2.1. Datatilsynet er enig i, at der er behov for vejledning og evt. undervisning i brug af digitale løsninger. Efter tilsynets opfattelse er der desuden behov for, at undervisning og instruktion kan ske, uden at borgerens eller underviserens egne personoplysninger anvendes. Datatilsynet skal på den baggrund opfordre til, at der bliver udarbejdet fiktive datasæt, som kan anvendes, når borgere skal have undervisning i digital selvbetjening.

2.2. I forhold til den omtalte vejledning i borgerservicecentre og på bibliotekerne skal Datatilsynet opfordre til, at det tydeliggøres, at såvel bibliotekets som borgerservicecentres medarbejdere handler som ansatte i en offentlig forvaltningsmyndighed (kommunen), og at kommunen er ansvarlig for den vejledning, der gives, og for medarbejdernes håndtering af oplysninger om borgerne, som de måtte blive bekendt med.

Forpligtigelsen efter persondataloven og sikkerhedsbekendtgørelsen til at give instruktion til medarbejdere, der håndterer personoplysninger, er ligeledes relevant i denne sammenhæng. Kommunens instrukser om håndtering af personoplysninger i forbindelse med vejledning i brug af selvbetjeningsløsninger kan indgå i de uddybende sikkerhedsregler, som kræves efter sikkerhedsbekendtgørelsen.

2.3. Datatilsynet skal endvidere påpege vigtigheden af, at sikkerheden på de computere, der stilles til rådighed på eksempelvis borgerservicecentre og biblioteker, til enhver tid har et tilstrækkeligt niveau. For eksempel med hensyn til antivirus-beskyttelse, firewall, web-filtrering (URL-filter) og lignende. Det vil endvidere være relevant at opsætte pc'erne således, at der ikke er administratorrettigheder for borgerne, det sidstnævnte for at beskytte mod, at utilsigtede eller tilsigtede handlinger udført af én borger kan have indflydelse på sikkerheden for en anden borger, der benytter samme pc.

Som minimum bør kommunen fastlægge procedurer til sikring af, at de pc'er, der stilles til rådighed, konstant er sikkerhedsmæssigt opdaterede, her tænkes på antivirus, operativsystem og al anden software. Procedurerne bør indgå i de uddybende sikkerhedsregler. For at sikre, at der tages hånd om dette, foreslår

Datatilsynet, at Digitaliseringsstyrelsen overvejer, om det kan være hensigtsmæssigt og formålstjentligt, at styrelsen udsteder mere formelle regler herom.

3. I de almindelige bemærkninger omtales NemID flere steder. Under overskriften "Identifikation af brugeren" er det i afsnit 4.2. bl.a. anført, at det på langt hovedparten af områderne må forventes, at der stilles krav om anvendelse af en sikker identifikation af borgeren i form af den nødvendige digitale signatur som eksempelvis NemID. Det er videre anført, at ved anvendelse af digital signatur skal der være tale om en digital signatur baseret på den til enhver tid gældende OCES-standart, som er fastlagt i certifikatpolitik for OCES-personcertifikater og certifikatpolitik for OCES-medarbejdercertifikater, såsom NemID.

Tvungen brug af selvbetjeningsløsninger baseret på NemID aktualiserer en problemstilling, som tilsynet tidligere har påpeget overfor IT og Telestyrelsen omkring opbevaring af borgernes private nøgle.

Datatilsynet udtalte bl.a. følgende i brev af 3. marts 2009 til IT og Telestyrelsen:

"[...] Det er endvidere Datatilsynets opfattelse, at et generelt hensyn til brugernes privacy taler for, at brugerne skal have et valg med hensyn til, hvor deres nøgle opbevares.

Datatilsynet skal derfor opfordre til, at der hurtigst muligt skabes mulighed for egen opbevaring af den private nøgle.

Datatilsynet skal endvidere anbefale, at det overvejes, om ikke muligheden for egen opbevaring af den private nøgle bør være gratis, eller at prisen i det mindste bliver så lav som muligt og alene kommer til at afspejle omkostningerne. [...]"

Datatilsynet bekendt er der endnu ikke etableret mulighed for egen opbevaring af den private nøgle. På Datatilsynets forespørgsel har Digitaliseringsstyrelsen (IT og Telestyrelsen) den 22. august 2011 oplyst, at løsningen med decentral opbevaring af den private nøgle er udskudt til udgangen af 2012, og det i medierne er det efterfølgende blevet oplyst, at løsningen nu er udskudt på ubestemt tid.

4. I de almindelige bemærkninger i lovforslagets afsnit 4.4 er bl.a. anført at, det ikke anses fornødent at fastsætte særlige krav om digital sikkerhed i form af eksempelvis digital signatur i lovforslaget.

Datatilsynet er for så vidt enig, men skal understrege, at der er behov for sikre løsninger. Tilsynet har set flere eksampler på, at myndigheder mv. har udviklet deres egen login til mobile enheder som smartphones og lignende. Tilsynet har i brev af 29. november 2011 rettet henvendelse til Digitaliseringsstyrelsen og gjort opmærksom på, at der er et aktuelt behov for et sikkerhedsmæssigt forsvarligt login til selvbetjeningsløsninger på smartphones og lignende.

Med venlig hilsen

Lena Andersen
Kontorchef

Ref Morten Damkjær Nielsen
Dato 7. August 2013
Side 1 af 2

Fødevarestyrelsen
Stationsparken 31-33
2600 Glostrup

Landbrug & Fødevarer

Axelborg, Axeltorv 3
DK 1609 København V

T +45 3339 4000
F +45 3339 4141
E info@lf.dk
W www.lf.dk

CVR DK 25 52 95 29

Vedr.: Høring – forslag til lov om ændring af forskellige lovbestemmelser om obligatorisk digital kommunikation, klager m.v.

Med henvisning til Fødevarestyrelsens skrivelse af 18. juni 2013 om ovenstående, Deres j. nr.: 2013-32-2320-00077/SMSA, skal Landbrug & Fødevarer bemærke følgende:

Landbrug og Fødevarer bemærker med tilfredshed, at Fødevarestyrelsen i det fremsendte høringsbrev skriver, at de foreslåede hjemler til at stille krav om at skriftlig kommunikation skal foregå digitalt, først vil blive udmøntede, når de tekniske løsninger er på plads, og når borgere og virksomheder er parate.

L&F mener, at øget digitalisering er en vigtig forudsætning for fortsat effektivisering af den offentlige sektor. Landbrug og fødevarer er derfor generelt positivt indstillet overfor øget digital kommunikation mellem det offentlige og landets virksomheder og borgere.

I den forbindelse er det imidlertid vigtigt at påpege, at tilfredsstillende digital kommunikation forudsætter tilstedeværelse af effektive bredbåndsforbindelser. I dagens Danmark findes der fortsat områder, hvor det er vanskeligt at skaffe internetforbindelser, der har tilstrækkelig kapacitet til, at digital kommunikation mellem virksomheder og myndigheder kan finde sted på tilfredsstillende vis. Eksempelvis kræver det op imod 4-5 Mbit at klare de krav, som Fødevareministeriet stiller til landbrugserhvervet i forbindelse med indberetninger, download af markkort mv.

Hvis ikke virksomhederne og producenterne har adgang til internetforbindelser med tilstrækkelig kapacitet, vil regler om tvungen digital kommunikation føre til øgede administrative byrder, idet indberetninger og kommunikation med Fødevarestyrelsen bliver vanskelig og tidskrævende. Det er vores indtryk, at brugeroplevelsen ved lav hastighed opleves som om at det pågældende system ikke fungerer, således at systemet i praksis bliver uanvendeligt.

I bemærkningerne til de af lovforslagets enkelte paragraffer, der bemyndiger ministeren til at fastsætte regler om, at skriftlig kommunikation skal foregå digitalt, anfører Fødevarestyrelsen, at det med den forslåede udformning af bestemmelserne er muligt på bekendtgørelsesniveau at fastsætte regler om, at visse grupper i en overgangsperiode ikke skal være omfattet af kravet om pligtmæssig digital kommunikation. Herudover nævner lovforslaget, at borgere eller virksomheder efter ansøgning undtagelsesvist kan opnå dispensation, Ifølge bemærkningerne kunne det for eksempel være relevant for personer, der bor i dele af Danmark, hvor det ikke er teknisk muligt at koble sig på internettet. Landbrug & Fødevarer finder af ovennævnte årsager, at lovbemærkningerne på dette punkt lægger op en for restriktiv linje for undtagelser og dispensationer, idet dispensation også bør kunne opnås af personer og virksomheder i områder, hvor der ikke på almindelige vilkår kan skaffes en fastnet internetforbindelse med beregnet downstreamhastighed på mindst 3 Mbit/s.

Landbrug & Fødevarer ser frem til at blive inddraget i forbindelse med udarbejdelse af bekendtgørelserne på de enkelte lovområder.

Lovforslaget rummer desuden bemyndigelse til at fastsætte regler om klager mv. for en række områder vedrørende dyrevelfærdslovgivningen, således at disse underlægges samme procedurer som gælder for hovedparten af den øvrige lovgivning under Fødevareministeriet. Landbrug & Fødevarer finder, at de foreslåede bemyndigelser følger naturligt af overførslen af ressortansvaret for dyrevelfærd fra justitsministeren til fødevareministeren.

Med venlig hilsen

Morten Damkjær Nielsen
Chefkonsulent

Fødevare-, veterinær- og forskningspolitik

D +45 3339 4295
M +45 3017 8857
E mdn@lf.dk

Søren Mark Sandorff (FVST)

Fra: Dennis Jensen <deje@food.dtu.dk>
Sendt: 27. juni 2013 13:04
Til: KundeUDV Jura 32
Cc: Søren Mark Sandorff (FVST); DTU-Fødevareinstituttet
Emne: Høringssvar til høring vedr. forslag til lov om ændring af forskellige lovbestemmelser om obligatorisk digital kommunikation, klager m.v., FVST j.nr. 2013-32-2320-00077

docId: http://fvstcaptia/fvstcapprd11/DOK1895388
SJ: -1

j.nr. 13/06381

FVST j.nr. 2013-32-2320-00077

DTU Fødevareinstituttet takker for invitationen til at deltage i høring vedr. forslag til lov om ændring af forskellige lovbestemmelser om obligatorisk digital kommunikation, klager m.v.

Det er imidlertid vores vurdering, at emnet for høringen ligger uden for instituttets kompetence og ansvarsområde, hvorfor vi afstår fra nærmere kommentarer til det modtagne materiale.

Venlig hilsen
Dennis Jensen

Dennis Jensen
Koordinator
Kommunikations- og Ledelsessekretariatet
DTU Fødevareinstituttet

Danmarks Tekniske Universitet
DTU Fødevareinstituttet
Mørkhøjgård, lokale 102
Mørkhøj Bygade 19
2860 Søborg
DTU Fødevareinstituttet
Direkte telefon 35 88 77 04
deje@food.dtu.dk
www.food.dtu.dk

Fra: Søren Mark Sandorff (FVST) [mailto:SMSA@fvst.dk]
Sendt: 18. juni 2013 16:31
Til: Beskæftigelsesministeriet; Erhvervs- og Vækstministeriet; Finansministeriet; Forsvarsministeriet; Justitsministeriet; Ligestillings- og Kirkeministeriet; kebmin@kebmin.dk; Kulturministeriet; Miljøministeriet; Ministeriet for By, Bolig og Landdistrikter; Ministeriet for Børn og Undervisning; Ministeriet for Sundhed og Forebyggelse; Ministeriet for Forskning, Innovation og Videregående uddannelse; Skatteministeriet; Social- og Integrationsministeriet; Statsministeriet; Transportministeriet; Udenrigsministeriet; oim@oim.dk; A/S Mortalin; A-consult a/s; Advokatrådet; ALECTIA; Alimentas ApS; Alternativfondet; Anticimex; Arbejderbevægelsens Erhvervsråd; Arbejdsgiverforeningen for konditorer_ bagere og chokolademagere (AKBC); Bager- og Konditormestre i Danmark; Biodania; Biodynamisk Forbrugersammenslutning; Brancheforeningen for farmaceutiske industrivirksomheder i Danmark; Brancheforeningen for Lægemiddelvirksomheder i Danmark (LIF); Bryggeriforeningen (Ann Louise Nielsen); Bryggeriforeningen (kontakt); Bureau Veritas Denmark; CIBIS-Fødevarerådgivning; Coop Danmark - Karin

Froeidt; Dacopa; DAKA; DAKOFO; Danish Seafood Association; Dankost (Jonna Kokholm); Danmarks Aktive Forbrugere; Danmarks Apotekerforening; Danmarks Farve- og Lakindustri; Danmarks fiskehandlere; Danmarks Fiskeriforening (mail); Danmarks Krebseavlerforening (Birthe Lindberg; Danmarks Skibsmægierforening; adm-ahr-DTU; Dansk Akvakultur; Dansk Elite Smiley; Dansk Erhverv (høring); Dansk Erhverv (info); Dansk Erhverv (tsk); Dansk Fåreavl; Dansk Galop; Dansk Gede Union; Dansk Hunderegister; Dansk Isindustri; Dansk Kennel Klub; Dansk Kvæg; Dansk Landbrugsrådgivning; Dansk Rideforbund; Dansk Skalddyrcenter; Dansk Supermarked (JRB); Dansk Travsports Centralforbund; Dansk Åleproducentforening; Danske Advokater; Danske Fugleforeninger (formand); Danske Lammeproducenter; Danske Læskedrik Fabrikanter (info); Danske Regioner; Danske Slagtermestre (Hovedpostkasse); Danske Speditører; DAZA (Danske Zoologiske Haver og Akvarier); DCA - Nationalt Center for Fødevarer og Jordbrug; De Samvirkende Købmænd (Kirsten Jacobsen); Den Danske Brancheorganisation for Vitalmidler; Det danske Fjerkræråd (JNL); Det dyreetiske Råd; Det Sundhedsvidenskabelige Fakultet; Det veterinære Sundhedsråd (FVST); DFO, Dansk Flavour Organisation; DHI, Center for Miljø og Toksologi; DI Fødevarer; DI Handel; Diabetesforeningen; Diagnostica ApS; DOSO-DyreværnsOrganisationernes SamarbejdsOrganisation; FOOD-Institut postkasse; VET Institut postkasse; Dyrefondet; Dyreforsøgstilsynet (FVST); Dyrenes Beskyttelse; Dyreværnsforeningen Alle Dyrs Ret; E-Branchekoden ApS; ECSCOM/Kim Iversen; EFSA – Effektiv Food Safety Advise; Elite Food Aps; Emballageindustrien; EMCON; Erhvervsstyrelsen; Erhvervsstyrelsen; Erhvervsstyrelsen CKR; Eurofins Steins Laboratorium A/S; Faglig Fælles Forbund 3F; Fair Dog; Fairtrade Mærket; FEHA; Felis Danica; Fokus på Dyr; Food Diagnostics ApS; Foodcare; FoodEfficiency; Forbrugerrådet 1; Force Technology; Foreningen Aktive Dyrerettigheder; Foreningen for Biodynamisk Jordbrug (biodynamisk); Foreningen Muslingeerhvervet (FME); Forsvarets Bygnings - & Etablissementstjeneste; FS-C.dk (Food Safety Consult); FS-C.dk (Food Safety Consult),; FødevareExperten,; Fødevaregruppen; Fødevarekonceptet; Gigtforeningen; Greenpeace; Grønhverdag; Hatting-KS A/S; HELSAM; Hesteinternatet af 1999; Hestens Værn; Hjerteforeningen; Horesta; Horesta (Tine Skriver); Hygiejnegruppen; Højmarkslaboratoriet A/S; Håndværksrådet; International Transport Danmark; Kantineledernes Landsklub; KGH CUSTOMS SERVICES Danmark; KGH CUSTOMS SERVICES Sverige; Kobenhagenfur; Konsumfiskeindustriens Arbejdsgiverforening; Kontrolgruppen; Kost & Ernæringsforbundet; Kost, Motion & Sund fornuft (KMS); Kræftens Bekæmpelse Høring EH; Kræftens Bekæmpelse Høring GLH; Kuluk consult ApS; Landbrug og Fødevarer (Mie Nielsen Blom); Landbrug og Førevarer; Landsforeningen af Danske Mælkeproducenter; Landsforeningen for Bæredygtigt Landbrug; Landsforeningen Komitéen mod Dyreforsøg; Landsforeningen til Oplysning om og Afskaffelse af Vivisektion i; Landskontoret for Heste; Lolex ApS; Lynges E.Kontrol; Møllers Fødevarerådgivning; NaturErhvervstyrelsen; naturerhvervstyrelsen- reception; Ninkovich Consult ApS; NOAHs Sekretariat (noah); NOPALAX; Nærbutikkernes Landsforening; OASA; Plastindustrien i Danmark; Postkasse, Dyreværnsrådet; Postkasse, FKC; Q-food ApS; QMS - Consult; Rigsadvokaten; Rigspolitichefen; Rådet for Dyreforsøg; Rådet vedrørende Hold af Særlige Dyr; SAMMARK; sf@lykkeberg.com; Sills & Løndal Rådgivning ApS; SKAT (Helle Ferm); Smiley-One; SPF-Danmark; SPT; Stop Spild Af Mad; Styrelsen for Universiteter og Internationalisering; Sundhedsrådet; Sundhedsstyrelsen; Teknologisk Institut; V & S Distillers; Videncenter for Svineproduktion; Videncentret For Landbrug; WSPA Danmark; Økologisk Landsforening
Cc: Anette Haurum (FVST); Susanne Rosbach (FVST); Birthe Schubart Haabegaard (FVST)
Emne: Høring over udkast til forslag til lov om ændring af forskellige lovbestemmelser om obligatorisk digital kommunikation

Til Fødevarestyrelsens høringsparter

Vedhæftet fremsendes høring over udkast til forslag til lov om ændring af forskellige lovbestemmelser om obligatorisk digital kommunikation, klager m.v. samt høringsbrev og høringsliste.

Høringen er tillige lagt på Høringsportalen og kan ses på følgende link:
https://hoeringsportalen.dk/Hearing/Details/16818.

Eventuelle bemærkninger til udkastet til lovforslag skal være Fødevarestyrelsen i hænde **senest fredag den 2. august 2013**, og sendes til smsa@fvst.dk med kopi til 32@fvst.dk.

Eventuelle spørgsmål vedrørende udkastet til lovforslaget kan rettes til undertegnede.

Med venlig hilsen

Søren Mark Sandorff
Cand.jur I JURA
smsa@fvst.dk

Ministeriet for Fødevarer, Landbrug og Fiskeri
Fødevarestyrelsen I Stationsparken 31-33 I 2600 Glostrup I Tlf. +45 72 27 67 74 I fvst.dk/kontakt I www.fvst.dk