



Direktionen

Rådhuset, Torvet 1
5800 Nyborg

Betjen dig selv på
www.nyborg.dk

Sagsansvarlig:
Anders M. Sørensen

Telefon: 6333 7751

Sagsnr.

Email: anso@nyborg.dk

Send altid personfølsomme oplysninger via din digitale postkasse på borger.dk

26-03-2024

Redegørelse for databrud vedrørende sikker mail 2024

Nyborg Kommune har 15. marts 2024 indberettet et brud på persondatasikkerheden til Datatilsynet vedrørende brug af sikker mail til andre offentlige myndigheder.

Nyborg Kommune har tidligere 25. januar 2024 indberettet et brud på persondatasikkerheden, der bevirkede, at et større antal indgående blanketter aldrig nåede frem til rettidig sagsbehandling. I forbindelse med dette brud igangsatte Nyborg Kommune en omfattende undersøgelse af vores mailsystem, herunder afdækning af konsekvenserne for de berørte borgere, der siden er blevet underrettet efter gældende regler.

Der blev også gennemført en teknisk undersøgelse af den del af vores IT-infrastrukturen, der håndterer sikre forsendelser, lokalt og hos leverandørerne. Sideløbende blev der etableret en postkasse (sikkerhedsnettet), der opsamler alle fejlmeddelelser vedrørende sikre mails og blanketter.

Sikkerhedsnettet har haft som formål at fange meddelelser, som ikke blev modtaget i Nyborg Kommunes elektroniske postkasser samt meddelelser, som ikke blev fremsendt korrekt fra Nyborg Kommunes elektroniske postkasser (ud af organisationen).

Alle disse fejlmeddelelserne bliver nu opsamlet i én særlig postkasse, som tjekkes dagligt og kontrolleres i forhold til, om der er systemiske fejl, der skal reageres på internt og/eller blandt de mange IT-leverandører, der sender og modtager sikre mails til og fra Nyborg Kommune.

Implementeringen af dette nye sikkerhedsnet har medført, at man har konstateret, at en større mængde udgående sikre mails ikke er kommet frem til modtager, hvilket indeværende notat nærmere redegøre for.

Årsagen hertil er, at Nyborg Kommune tidligere har indført et filter på udgående sikre mails, som blokerer for sikre mails indeholdende CPR-numre i emnefeltet (da emnefeltet ikke bliver krypteret). Forbuddet mod at tilføje CPR-nr. i emnefeltet fremgår også af Nyborg Kommunes interne retningslinjer.

Hvordan blev det opdaget?

I forbindelse med denne systematiske overvågning dukkede, der onsdag 13. marts 2024 en fejlmeddelelse op på en sikker mail, der var blevet stoppet af Nyborg Kommunes filter, der bremser mails, der indeholder CPR-nr. i mailen eller emnefeltet.

Det drejede sig om en mail, hvor en medarbejder - på trods af, at det ikke er tilladt - havde skrevet borgerens CPR-nr. i mailens emnefelt, der *ikke* kan krypteres.

På den måde virkede det opsatte CPR-filter efter hensigten, men medarbejderen havde imidlertid *ikke* fået besked om, at mailen ikke blev afsendt. Dvs., at:

- Medarbejderen havde fået en kvittering om, at mailen var udsendt korrekt.
- Mailen lå i vedkommendes "Sendt Post".
- Og sikker-mail loggen viste, at mailen var sendt korrekt.

En nærmere undersøgelse viste, at der desværre er et større antal mails af samme karakter – dvs. sikre mails, hvor CPR-nummer er indsat i emnefeltet – som er blevet stoppet af et CPR-filter, men hvor medarbejderen troede, at mailen var afsendt korrekt.

Det drejer sig både om mails, hvor medarbejdere i Nyborg Kommune "aktivt" har skrevet CPR-nummeret i emnefeltet, men også besvarelser af indgående mails, hvor andre myndigheder har sendt et ukrypteret CPR-nummer i emnefeltet, og som vores medarbejder ikke får fjernet i forbindelse med, at vedkommende besvarer mailen.

I begge af disse situationer overholder medarbejderne ikke gældende interne retningslinjer, men får omvendt heller ikke besked om, at mailen blokeres, og dermed ikke når frem til modtager.

Kortlægning af omfanget

I erkendelsen af, at de manglende udsendte mails har været ramt af et CPR-filter, der blev etableret 6 år tilbage, har vi undersøgt perioden 2018 til 2024 med henblik på at afdække om, der er andre lignende eksempler.

Resultatet er, at der er identificeret i alt 913 mails, som ikke er sendt ud. I nedenstående tabel ses fordelingen over år.

Tabel 1: Blokerede mails med CPR-nr. i emnefeltet

Periode	Antal
2023-2024	119
2022	212
2021	212
2020	142
2019	130
2018	98
I alt	913

Det drejer sig udelukkende om mails omhandlende borgere og sendt mellem Nyborg Kommune og andre offentlige myndigheder (tunnelmails). De ramte mails er udsendt af medarbejdere i alle afdelinger i Nyborg Kommune.

Medarbejdere i Digitalisering og I-sikkerhed har siden fejlen blev opdaget påbegyndt arbejdet med at spore alle de berørte mails og kontaktet de sagsbehandlere, der stadig er ansat.

Dette arbejde har til formål at afklare konsekvenserne for de berørte borgere. I nedenstående tabel 2 ses fordelingen af blokerede mails fordelt på fire kategorierne:

- Sagsbehandler ikke længere ansat.
- Endnu ikke kontaktet sagsbehandler.
- Ikke genfremsendt (afsluttet på anden vis).
- Genfremsendt.

Tabel 2: Blokerede mails med CPR-nr. i emnefeltet fordelt på kategorier

Mails ikke afsendt	2018		2019		2020		2021		2022		2023-2024		I alt	
Sagsbehandler ikke længere ansat	55	56%	57	44%	50	35%	89	42%	31	15%	28	24%	310	34%
Endnu ikke kontakt til sagsbehandler	21	21%	19	15%	40	28%	15	7%	47	22%	18	15%	160	18%
Ikke genfremsendt (afsluttet på anden vis)	0	0%	2	4%	1	2%	1	1%	10	8%	15	13%	29	7%
Genfremsendt	22	22%	52	40%	51	36%	107	50%	124	58%	58	49%	414	45%
I alt	98	100%	130	100%	142	100%	212	100%	212	100%	119	100%	913	100%

Hvor alvorlige er sagerne?

Som det fremgår af tabel 2, så er området ikke fuldt belyst, idet en række sagsbehandlere af tidsmæssige grunde endnu har kunne kontaktes eller ikke længere er ansat.

Ved sidstnævnte kontaktes lederen af afdelingen med henblik på at få den konkrete hændelse nærmere belyst.

Langt de fleste mails er blevet genfremsendt eller håndteret på anden vis, og der er relativt få sager med risiko for "alvorlige" hændelser.

Tabel 3: Foreløbig oversigt i sager med risiko for "alvorlige hændelse"

Periode	Antal	Sager med risiko for "alvorlige hændelser"
2018	0	Ingen bemærkninger
2019	(1)	Potentielt et tilfælde vedr. en samværssag vedr. 2 søskende, som formodes være løst. Sagsbehandler undersøger.
2020	3	Et tilfælde vedr. en selvskadende person, hvor sagsbehandling blev forsinket. Herudover 2 sager vedr. politianmeldelser, der måske ikke er kommet frem til politiet (undersøges).
2021	0	Ingen bemærkninger
2022	2	Disse to tilfælde er der en formodning om, at det kan have haft konsekvens for den registrerede. Sagsbehandler kan ikke i tilfredsstillende grad beskrive sagens afslutning, men vi ved, at der er tale om et barn (født i 2011), og at der ikke er sket genfremsendelse. Sagsbehandler undersøger sagen nærmere.
2023-2024	1	1 vedrører manglende refusion af udgift til borger på herberg.

Digitalisering og I-sikkerhed fortsætter arbejdet med at kontakte de medarbejdere, der har udsendt de berørte mails med henblik på at kortlægge omfang og konsekvens.

Hvordan kunne det ske?

Som beskrevet er der en række årsager til, at fejlen sker, såvel menneskelige som tekniske.

I nedenstående redegøres for de årsager, der har haft betydning, herunder en beskrivelse af den tekniske opsætning i Nyborg Kommunes infrastruktur.

Det skal indledningsvist understreges, at det tidligere omtalte sikkerhedsnet har sikret, og vil i fremtiden sikre at lignende fejl lokaliseres og håndteres straks de meldes ind.

Teknisk redegørelse

IT-afdelingen har haft en mail-scanningsløsning siden 2015 og har siden benyttet samme løsning/leverandør til at scanne og stoppe store mængder af spam, virus og andet, der sendes til brugerne i Nyborg Kommune, dvs. med fokus på indgående mails.

I forbindelse med implementering af GDPR indfører IT-afdelingen i 2018 et filter, DLP (data loss prevention) for at stoppe brugerne i at sende mails indeholdende CPR-nummer ud af Nyborg Kommune via almindelig mail.

Begge aftaler fra 2015 og 2018 blev oprindeligt indgået med Comendo, i dag Vipre Security.

Mails med følsomme og fortrolige personoplysninger skal derimod sendes via Send Sikkerknappen i Outlook, der blev indkøbt og implementeret tilbage i 2004 i samarbejde med leverandøren Logiva. Når mails sendes via den sikre løsning fra Logiva, krypteres alt indhold – dog undtaget emnefeltet. Dette er standard-opsætning i alle løsninger.

Årsagen til at emnefeltet ikke krypteres, skyldes at det er en integreret del af mailens *header*. Headeren er den del af mailen, der indeholder tekniske oplysninger om meddelelsen. Den indeholder oplysninger som f.eks. afsenderens mailadresse, modtagerens mailadresse og emnelinjen. Kryptering af emnefeltet kan hindre dets læsbarhed, hvilket kan forringe brugeroplevelsen og funktionaliteten af mailklienter (eksempelvis Outlook).

Hvis en bruger sender en sikker-mail via Logivas løsning indeholdende et CPR-nummer i emnefeltet, så vil Logiva kryptere mailens indhold, dog undtaget emnefeltet. Når mail forsøges videresendt til modtager, vil den blive stoppet af DLP (pga. af CPR-nummer i emnefeltet), som forsøger at sende et fejl-svar retur. Dette svar lander i Logivas miljø, som sender en såkaldt NDR (non-delivery report) til en konkret opsat postkasse (tidligere omtalte "sikkerhedsnet"), således at der følges op på disse mails og afsender kan modtage besked om, at mail ikke er nået frem. Den del monitoreres nu af medarbejdere, der har indsigt i området.

Udfordringen har indtil for nylig været, at denne NDR aldrig blev "samlet op" grundet manglende/forkert opsætning i 2004, hvor løsningen fra Logiva oprindeligt blev implementeret. Løsningen er implementeret på basis af det daværende mail-setup. IT-afdelingen formoder, at løsningen dengang i forbindelse med implementering blev testet, men det kan ikke bekræftes.

Kortfattet beskrivelse af processen:

- Bruger sender en mail via Outlook Send Sikker-funktionen.
- Bruger medsender et CPR-nummer i emnefeltet.
- Logiva krypterer mailens indhold – undtaget emnefeltet – godkender og sender mailen videre.
- Medarbejder modtager kvittering for korrekt afsendelse.
- Spamfilter stopper mailen og forsøger at sende svar retur, som lander i Nyborg Kommunes sikker-mailløsning.
- Sikker-mail kan ikke levere mail retur til afsender, men heller ikke levere mail korrekt til modtager.
- Derfor sendes der (i dag) en NDR til en postkasse ("sikkerhedsnet") i Nyborg Kommune, som der kan handles på.

Den "menneskelige" faktor

Nyborg Kommune har en række retningslinjer, som medarbejderne introduceres for ved ansættelsesstart. De sidste fire år har medarbejdere, ledere og politikere modtaget løbende undervisning i GDPR og awareness samt via 2 årlige e-learningkurser.

I "Retningslinjen for anvendelse mails og anden digital kommunikation" fremgår det bl.a. markeret med kursiv:

...Send sikkert til borgere

Opret din mail som du plejer, men skriv borgerens cpr.nr. i "til-feltet" i stedet for en mailadresse. Benyt knappen "Send sikkert" i stedet for den almindelige "Send" knap i Outlook. Når der sendes mail til borgerens cpr.nr., havner mailen i borgerens digitale postkasse på Borger.dk. *Bemærk, at emnefeltet ikke krypteres - skriv derfor aldrig borgeres navn eller cpr-nummer i emnefeltet.* Borgeren kan se og besvare fra Borger.dk.

Send sikkert til virksomheder

Opret din mail som du plejer, men skriv virksomhedens cvr. nr. i "til-feltet" i stedet for en mailadresse. Benyt knappen "Send sikkert" i stedet for den almindelige "Send" knap i Outlook. Når der sendes mail til virksomhedens cvr. nr., havner mailen i virksomhedens digitale postkasse på Virk.dk. *Bemærk, at emnefeltet ikke krypteres - skriv derfor aldrig personfølsomme oplysninger i emnefeltet.* Virksomheden kan se og besvare mailen fra Virk.dk...

Digitalisering og I-sikkerhed udsender løbende SPOT's med vejledende information og opmærksomhedspunkter inden for informationssikkerhed til alle medarbejdere i Nyborg Kommune.

Der er ført statistik på udsendte SPOT's siden 2020. I den forbindelse kan det oplyses, at der er udsendt SPOT vedrørende Sikker Mail den 2. november 2020, 1. oktober 2021, 27. marts 2023 og 18. marts 2024.

Eksempel på løbende information til alle medarbejdere fremgår af bilag 1.

IT-revision, NSIS-revision DPO-tilsyn

BDO gennemfører hvert år en ekstern IT-revision og NSIS-revision. Næste revision er planlagt til 3. og 4. juni 2024.

IT-revisionen omfatter en revision af kommunens generelle it-kontroller for de it-systemer, der har betydning for kommunens regnskabsføring og regnskabsafklæggelse.

NSIS-revisionen omfatter en revision af om kommunen lever op til alle krav i den nationale sikkerhedsstandard (certificering), herunder kommunens lokale IdP-løsning samt kontrollerens udformning og implementering.

Kommunens DPO (Bech-Bruun) gennemfører løbende tilsyn med kommunen lever op til GDPR-reglerne og lovgivningen vedrørende håndtering og sikring af personoplysninger, herunder persondatapolitikker og –procedurer.

Den løbende eksterne revision og DPO-tilsyn har ikke givet anledning til bemærkninger vedrørende opsætning eller håndteringen af sikker mails.

Der gennemføres årligt ledelsestilsyn vedrørende I-sikkerhed, hvor der bl.a. spørges ind til om alle medarbejdere er bekendt med, at følsomme og/eller fortrolige personoplysninger skal sendes sikkert (fx sikker mail eller digital post) i henhold til gældende retningslinjer.

Har der ikke været henvendelser fra medarbejderne gennem årene?

Man kan måske undre sig over, hvorfor indeværende hændelse kan finde sted over 6 år uden, at nogen har reageret. Der har højst sandsynligt været henvendelser fra medarbejderne gennem årene, der primært har kontaktet IT-afdelingens support.

Men en kombination af, at der ikke har været opsat et "sikkerhedsnet" samt at medarbejderen fik en kvittering, kunne se mailen i sin "Sendt Post" samt loggen også viste en korrekt afsendt mail, så har vi i de situationer, hvor andre myndigheder har klaget over manglende mails fra Nyborg Kommune henholdt os til, at alt tydede på, at det var myndighedens fejl og ikke Nyborg Kommune som afsender.

Det er samtidigt meget få medarbejdere i IT-afdelingen, som har haft adgang til og viden om den tekniske systemopsætning vedrørende det særlige filter, som stopper mails, hvor borgernes CPR-nr. er skrevet i emnefeltet.

Indberetning til Datatilsynet og videre opfølgning

Nyborg Kommune har 15. marts 2024 indberettet et brud på persondatasikkerheden til Datatilsynet vedrørende brug af sikker mail til andre offentlige myndigheder.

Nyborg Kommune har tidligere 25. januar 2024 indberettet et tilsvarende brud på persondatasikkerheden, der bevirkede at et større antal indgående blanketter aldrig nåede frem til rettidig sagsbehandling.

På trods af sammenhængen til det tidligere brud, så har Digitalisering og I-sikkerhed på baggrund af rådgivning fra vores DPO valgt at indberette det som et nyt brud til Datatilsynet.

Der arbejdes sideløbende på at få et yderligere overblik over konsekvenserne for borgerne, og der påbegyndes et arbejde med at underrette de registrerede, hvor det er muligt og under hensyntagen til gældende lovgivning på området. Det foreløbige resultat indikerer, at der indtil videre er relativt få "alvorlige" hændelser. Langt de fleste sager er håndteret på anden vis.

Nyborg Kommune har på baggrund heraf implementeret et sikkerhedsnet, som skal fange meddelelser som ikke bliver modtaget i Nyborg Kommunes elektroniske postkasser samt meddelelser, som ikke bliver fremsendt korrekt fra Nyborg Kommunes elektroniske postkasser (ud af organisationen).

Den opsatte overvågning har sikret, at vi nu får information om fejlede mailhændelser, som vi kan handle på straks. Men har også haft den konsekvens, at fejl tilbage i tiden nu er sporbare, hvilket der følges op på nu.

Det skal understreges, at hvis kommunen ikke havde implementeret IT-systemer til håndtering af send sikkert/filter ville alle mails kunne have medført et sikkerhedsbrud i sig selv, hvor borgernes CPR-nr. var blev kompromitteret.

Sammenfatning og konklusion

Databrudet skyldes, at medarbejdere i Nyborg Kommune i enkelte tilfælde har forsøgt at sende sikker mail til andre offentlige myndigheder, hvor borgernes CPR-nr. var skrevet i emnefeltet, hvilket er i strid med kommunens retningslinjer for brug af sikker mail.

Indholdet og bilag i sikker mail bliver sendt krypteret, men tekst i emnefeltet bliver ikke krypteret og må derfor ikke indeholde personfølsomme oplysninger, herunder CPR-nr.

For at undgå at borgernes data bliver kompromitteret, er der i forbindelse med ny GDPR lovgivning i 2018 indført et særligt filter, som stopper mails, hvor borgernes CPR-nr. er skrevet i emnefeltet.

Filtret har korrekt blokeret afsendelsen af mails og forhindret databrud, men afsenderen har ikke fået besked herom og i stedet fået en kvittering på, at mailen var sendt, hvilket også kunne ses i "Sendt post" i Outlook.

Den tekniske fejl er nu elimineret, og der er oprettet en særlig postkasse "sikkerhedsnet", hvor alle fejl og sikkerhedsbrud vedrørende sikker mail bliver opsamlet og kontrolleret dagligt. Dermed får medarbejderne nu besked om, at en sikker mail ikke er sendt, fordi mailen indeholder fortrolige oplysninger i emnefeltet.

Digitalisering og I-sikkerhed har gjort en kæmpe indsats med at afdække og undersøge databrudet, som omfatter 913 mails i perioden 2018-2024.

Langt de fleste mails er blevet genfremsendt eller håndteret på anden vis, og der er relativt få sager med risiko for "alvorlige" hændelser.

Antallet af fejl skal ses i lyset af at der i samme periode er sendt 163.000 sikre mails i Outlook, 5 mio. sikre mails fra fagsystemerne (Nova, Nexus, DUBU m.fl.) og 6,8 mio. almindelige mails i Outlook.

Det er meget få medarbejdere i IT-afdelingen, som har haft adgang til og viden om den tekniske systemopsætning vedrørende det særlige filter, som stopper mails, hvor borgernes CPR-nr. er skrevet i emnefeltet.

Systemopsætningen af "Send Sikkert" funktionen i Outlook og implementeringen af det særlige filter er sket i samarbejde med eksterne IT-konsulenter (Vipre Security, Logiva).

Den løbende eksterne IT-revision, NSIS-revision og DPO-tilsyn har ikke givet anledning til bemærkninger vedrørende opsætning eller håndteringen af sikker mail.

Direktionen finder det beklageligt:

- At medarbejdere i Nyborg Kommune i enkelte tilfælde ikke har fulgt retningslinjerne for brug af sikker mail.
- At der teknisk har været implementeret et filter som forhindre databrud, men som ikke har givet afsenderen besked om, at sikker mail ikke var afsendt.
- At der ikke har været implementeret en særlig postkasse "sikkerhedsnet", hvor alle fejl og sikkerhedsbrud vedrørende sikker mails blev opsamlet og kontrolleret dagligt.
- At den tekniske systemopsætning ikke har været tilstrækkeligt testet og afprøvet i forhold til fejl inden ibrugtagning.

Nyborg Kommune står samtidig overfor stigende og mere komplekse krav til digital understøttelse og IT-support i hele organisationen samtidig med skærpede krav til bl.a. overholdelse af lovgivningen i forhold til GDPR, nationale sikkerhedsstandarder NSIS, IT-revision, IT-beredskabsplaner og cybersikkerhed.

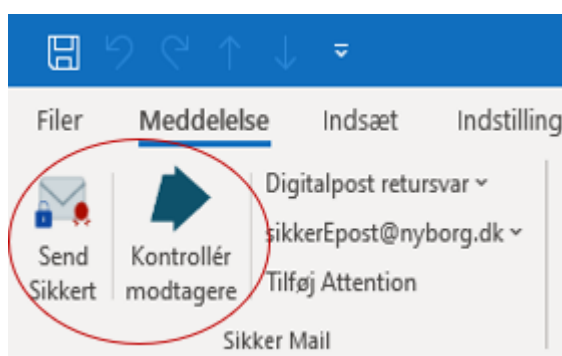
Direktionen har derfor besluttet, at gennemføre en ekstern gennemgang af hele IT-området i Nyborg Kommune.

Dette vil omfatte en ekstern skriftlig konsulentrapport med en 360 graders gennemgang af hele IT-området i Nyborg Kommune, herunder anbefalinger til eventuelle forbedringer i forhold til IT-infrastruktur, I-sikkerhed, support, organisering, kompetencer, driftsøkonomi, investeringer, samarbejde og IT-understøttelse af afdelinger/institutioner i hele organisationer.

Bilag 1: Send sikkert i Outlook (SPOT)

Send sikkert i Outlook

Størstedelen af vores korrespondance med borgere, virksomheder og andre offentlige myndigheder foregår digitalt og skal i udgangspunktet håndteres gennem vores fagsystemer. Denne SPOT har fokus på, hvad du skal være opmærksom på, når du bruger Outlook i kommunikationen med vores digitale omverden.



Alle medarbejdere i Nyborg Kommune sender sikkert til hinandens "@nyborg.dk"-mailadresser, idet vores interne sikkerhedssystem sikrer, at oplysningerne ikke kan opfanges af uvedkommende.

Når du sender en almindelig mail uden for vores sikkerhedssystem, svarer det til, at du sender et åbent postkort, hvor andre potentielt kan læse med. Hvis du derimod sender mails krypteret (dvs. via "send sikkert" -knappen), svarer det til, at mailen ligger i en lukket kuvert.

Vi kan ikke forhindre f.eks. borgere i, at de sender følsomme oplysninger, så som helbredsoplysninger til os via forbindelser, som ikke er sikrede. I en sådan situation må du svare borgeren tilbage via sikker mail, hvor svaret havner i deres Digital Post og samtidigt opfordre dem til fremadrettet at benytte de sikre kanaler.

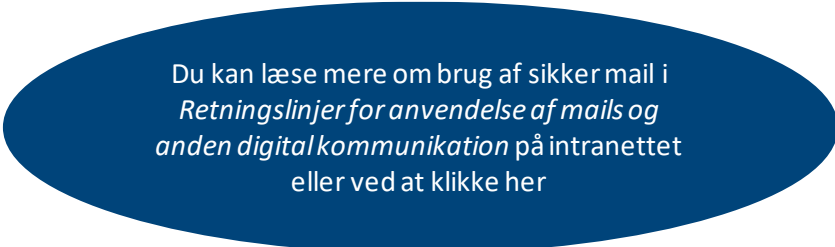
Brug af modtagerfeltet/"til"-feltet

Det er en god ide at vente med at udfylde modtagerfeltet til efter du har skrevet indholdet, for at undgå at få sendt en ufærdig mail ved en fejl eller til en forkert modtager. Det er muligt at kontrollere den modtager du gerne vil sende sikkert til vha. knappen "Kontrollér modtagere".

Borger: Skriv borgerens cpr.nr. i "til"-feltet i stedet for en mailadresse. Benyt knappen "Send sikkert" i stedet for den almindelige "Send" knap. Når der sendes mails til borgerens cpr.nr., havner mailen i borgerens digitale postkasse på Borger.dk. Borgeren kan se og besvare fra Borger.dk.

Virksomheder kan kontaktes ved at skrive deres cvr. nr. i "til"-feltet i stedet for en mailadresse. Benyt "Send sikkert"-knappen og mailen havner i virksomhedens digitale postkasse på Virk.dk. Virksomheden kan se og besvare mailen fra Virk.dk.

Offentlige myndigheder har en sikker mailadresse, hvortil du kan sende krypterede mails. Der kan også sendes sikker mail til offentlige myndigheders cvr. nr. på samme måde som ovenfor beskrevet ved virksomheder, hvor mailen havner i myndighedens digitale postkasse. Mange offentlige myndigheder (og enkelte større virksomheder) er desuden tilsluttet en ordning kaldet "Direkte adressering", hvor du kan sende direkte til medarbejdernes postkasser.



Du kan læse mere om brug af sikker mail i
*Retningslinjer for anvendelse af mails og
anden digital kommunikation* på intranettet
eller ved at klikke her

Uanset hvilken metode du vælger, vil mailen kun blive sendt i fald, der er et validt cpr, cvr eller sikker mailadresse (Direkte adressering).

VIGTIGT vedr. "Emne"-feltet

Mails skal have en præcis overskrift, der dækker indholdet og hjælper til at få meddelelsen placeret hos rette vedkommende. Når du sender sikre mails, skal du dog være opmærksom på, at overskriften i "emne"-feltet ikke krypteres. Dette gælder alle ovennævnte modtagertyper. Skriv derfor aldrig navne, cpr-/cvr-nummer eller andre fortrolige og/eller følsomme oplysninger i "emne"-feltet.