Sådan behandler vi personfølsom data i Reach Psykologer ApS

Kryptering og sikker mail

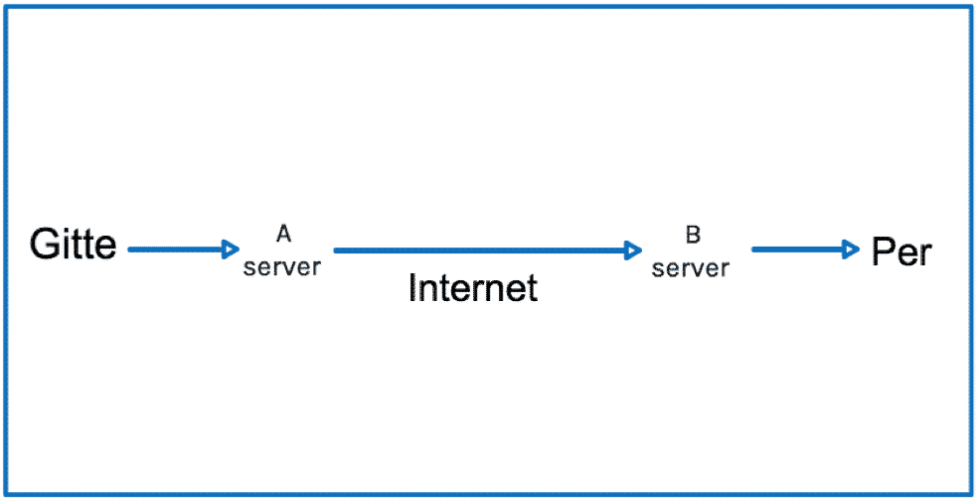
Hvad er en sikker mail og hvordan krypterer du den?

Datatilsynet kræver, at virksomheder, der sender fortrolige personoplysninger via internettet, gør dette via en sikker mail. Så når vi kommunikerer med klienter eller potentielle klienter, skal vi anvende kryptering.

Endvidere er *al* kontakt til psykologer kategoriseret som personfølsomme oplysninger, da alle personoplysninger, der medfører en identificering af en person i *en personfølsom sammenhæng*, kategoriseres som personfølsom data.

Hvad er en mail?

Når du sender en E-mail, så foregår det lidt, som når du sender et brev. Gitte trykker send og postbudet, eller i denne forbindelse, vores mailudbyder ZOHO, modtager mailen i posthuset (A server). Herfra afleverer de via internettet mailen til et andet posthus (B server), som sender Per sin mail.

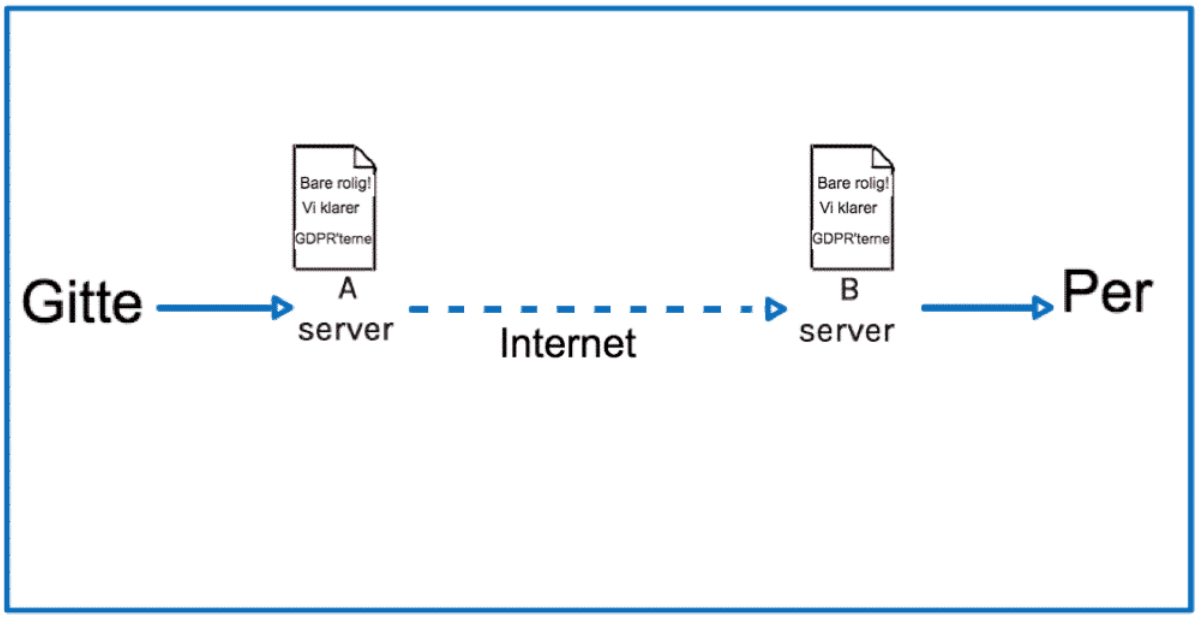


Sikker mail

Grundlæggende bruger vi to løsninger for at passe på vores klienters data.

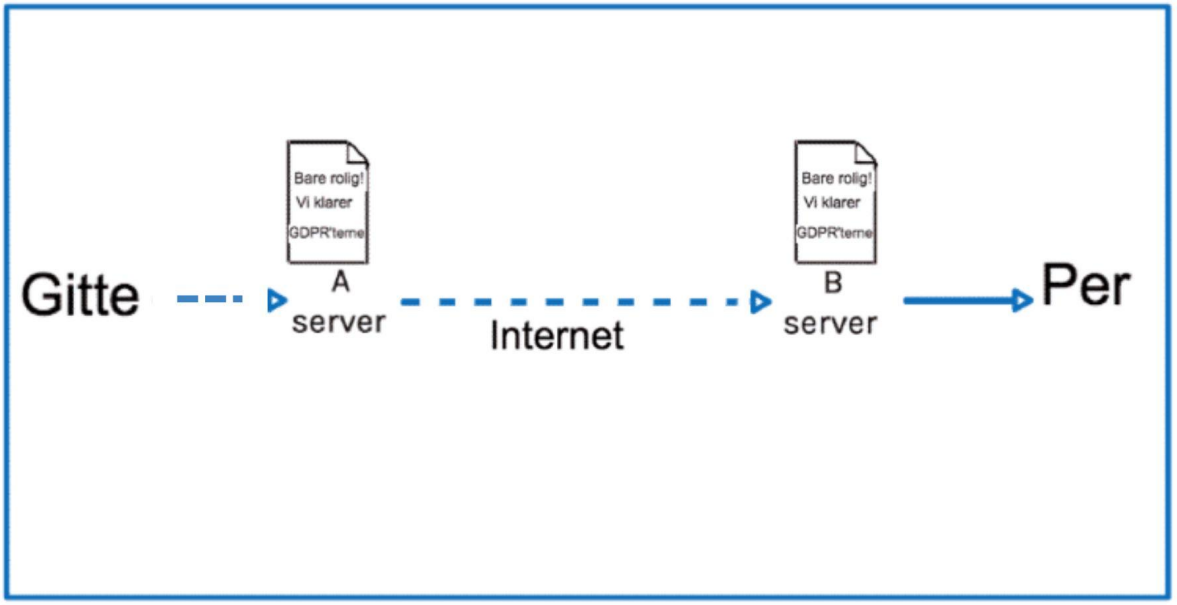
For det første bruger vi Transport Layer Security 1.2 (TLS) som krypterer vores mails. Kryptering betyder, at oplysninger eller data ændres til en hemmelig kode, som uvedkommende ikke kan tyde.

Denne løsning sørger for at vores mail ikke bliver snuppet på vejen til modtageren fordi den krypterer selve overførslen af mailen, fra “A server”, over internettet, til “B server”. Med TLS vil mailen fremkomme ukrypteret på modtagerens server, hvis modtagerens “mail-service” også understøtter TLS.



Denne løsning er nemmest at anvende i praksis, da de fleste mailudbydere har TLS som standard. Figuren viser hvordan TLS kryptering virker. Den stiplede pil indikerer, at det er selve vejen over internettet, der bliver krypteret. Indholdet af mailen er altså ikke krypteret.

Til gengæld fungerer det sådan hos vores mailudbyder ZOHO at vores mails, vedhæftninger mv. krypteres på vores server. Så modsat de fleste udbydere, ser vores situation således ud:



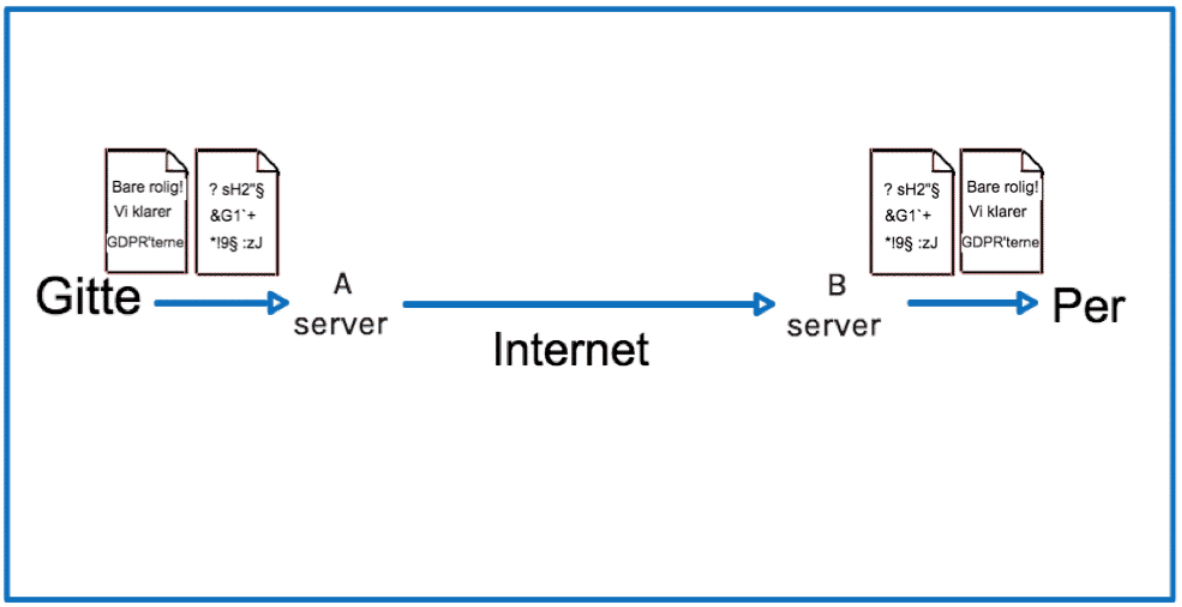
Mailen er altså kun dekrypteret i modtagerens inbox. Derfor er det ganske ansvarligt - og inden for persondatalovens retningslinjer - at vores hverdags-korrespondance mv. foregår almindeligt gennem ZOHO.

Til gengæld skal du være opmærksom på, aldrig at lave sikkerhedskopier af dine mails, videresende dem til en anden udbyder mv..

Ligesom du skal oplyse din klient om at han eller hun skal passe på sin data på sin ende, ved bl.a. at slette vores korrespondance løbende og bruge en udbyder der understøtter TLS 1.2 (Hvilket både Google, Outlook, Proton og Zoho gør - *hvis* klienten bruger et opdateret styresystem og en opdateret browser). Herudover sendes en automatisk mail fra Reach Psykologer til alle klienter, der informerer klienter om hvordan de kan og bør sikre deres data.

Kryptering af indholdet (End-to-End kryptering)

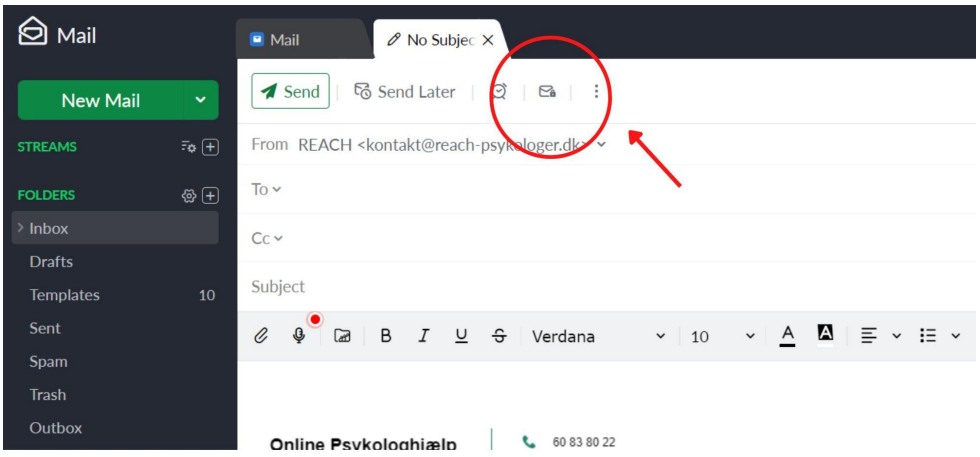
Vores anden og mere omfattende løsning er at kryptere selve indholdet af mailen, ofte kendt som end-to-end kryptering. Figuren viser en typisk end-to-end kryptering. Mailen bliver sendt fra Gitte til (A server), der krypterer indholdet. Her vil Per modtage et link til et sted, hvor beskeden kan læses sikkert.



Normalt ved denne metode skal både afsender og modtager have et nøglepar, der kan kryptere og dekryptere indholdet af mailen – derfor navnet “End-to-End” kryptering. Men fordi vores inbox i forvejen er krypteret, får kun modtager en nøgle. Denne løsning giver en høj sikkerhed for hvem der modtager mailen, og for hvem der sender, da kun disse personer kan læse mailens indhold - endvidere vil mailen automatisk slettes efter en uge (en uge som standard, men du kan selv indstille tidsrummet).

Denne metode bruger vi til alle mails som indeholder særlige sårbare informationer, såsom cpr. nr. - i psykologerklæringer -, bankoplysninger eller andet, der netop vurderes særligt sensitivt.

Du sender mailen ved at bruge ikonet med en nøgle på brevet ved siden af vores almindelige “send” knap i ZOHO



Det er lige nu ikke muligt for klienten at downloade vores end-to-end krypterede mails, hvorfor vi skal kommunikere til dem, at de skal tage et screenshot hvis der fx

er tale om en psykologerklæring. Vi ved dog at ZOHO arbejder på denne tjeneste også, så forhåbentligt snart.

Hvis du er nysgerrig på ZOHOs kryptering, så kan du læse mere her: https://www.zoho.com/encryption.html

OBS. mange mailudbydere såsom google tilbyder end-to-end krypterede mails på samme måde som ZOHO. Når du beder din klient sende personfølsom data til dig, så send samtidigt et link til en guide der viser dem hvordan de gør dette sikkert. Du kan bare søge på Google: "how to send an end-to-end encrypted email with …."

Så hvad siger Datatilsynet?

Ifølge datatilsynet, skal vi som minimum bruge TLS version 1.2, hvis vi overfører fortrolige eller følsomme oplysninger (Lovkrav). Vi skal anvende end-to-end kryptering, hvis der er en særlig høj risiko for de implicerede, f.eks. helbredsoplysninger og lignende (god praksis).

Hvad siger Dansk Psykologforening?

DP er grundlæggende enige i, hvordan vi forvalter ansvaret for datasikkerheden hos Reach Psykologer ApS, men de har også lidt ekstra råd.

1) Privatpraktiserende psykologer er ikke forpligtet til at tilmelde sig Datatilsynet i forbindelse med behandling af personfølsomme oplysninger.
2) Ansvaret for den personfølsomme data ligger hos psykologen og kan ikke samtykkes væk af den, der er i behandling.
3) Når du kontaktes af en klient/potentiel klient, kan du ikke være sikker på at forbindelsen er krypteret, hvorfor du ikke skal svare direkte på den oprindelige mail, men i stedet oprette en ny mailtråd.
4) Sådan holder du en kalender
    a) Sikker dig at synkronisering ikke sker til en usikret internetserver
    b) Brug initialer, listenummer eller lignende i din kalender, og hav en faktisk liste med navne over for listenummer i et sikkert opbevaret sted
    c) Brug ikke en privat enhed til din elektroniske kalender, da eksterne aktører fra andre apps ofte vil have tilladelse til at tilgå den data, der måtte være på din telefon.
5) Du må kun sikkerhedskopiere din smartphone/iPad/tablet hvis du gør det til en sikret computer eller server. Du må f.eks. ikke gemme på en ukrypteret "cloud".
6) Kommuniker aldrig med klienter på sociale medier, da denne data vil gemmes hos en tredjepart, der så ejer den.

Kilde: https://www.dp.dk/wp-content/uploads/spoergsmaal-om-datasikkerhed-1.pdf

Sådan forstår vi god praksis hos Reach Psykologer ApS

Hos Reach Psykologer ApS opbevarer vi personfølsomme data på følgende lokationer: ZoHo, Wix, Aidaform, WhatsApp, Jyske Bank og betalingsudbyder (Stripe) samt i vores journal. Hver af disse udbydere forsikrer os om den absolut bedste udgave af datasikkerhed, der findes. Men vi skal også selv være mindfulde om, hvordan vi behandler den data i vores hænder. Her er vores udgave af god praksis:

1) Opsæt altid to-trins-godkendelse til alle vores platforme
2) Brug almindelig mailkorrespondance til hverdagsmails.
3) Brug end-to-end kryptering, når dine mails indeholder særlige sensitive informationer.
4) Når vi beder klienten sende særlige sensitive informationer vedhæfter vi en guide til hvordan de skal gøre dette med sikkerhed for deres data.
5) Vores interne mailkorrespondance, er krypteret hele vejen og vi kan derfor frit skrive internt
6) Svar ikke direkte på en henvendelse når en klient/potentiel klient skriver til dig, men start en ny mailtråd
7) Efter x antal sessioner sendes en automatisk e-mail ud til klienter, der informerer dem om, at når vores mails ligger i deres inbox, kan vi ikke længere stå for sikkerheden af indholdet, hvorfor vi i denne mail opfordrer klienten til at slette vores samtaler løbende.
8) Selvom vores inbox er krypteret, arbejder vi med en god praksis om at slette alle mails efter 6 mdr. uden kontakt fra klienten. Hvis mailen er relevant for journalisering, kopieres den til en sikker ekstern harddisk. Eller printes.
9) Når en klient færdiggør deres forløb hos os, skal klientens kontaktinformationer slettes på alle platforme, dvs. Zoho, WhatsApp og Wix.
    a) Da det dog er et lovkrav (for autoriserede psykologer og god praksis for uautoriserede psykologer), at inkludere navn, adresse og alder på klienten i deres journal, skal du sørge for at kopiere kontaktinformationer ned i din journal på en sikker, ekstern harddisk.
    På den måde har vi både lovhjemmel og et legitimt formål med at opbevare klientens data - i *minimum* 5 år.
    b) Når en klients profil slettes, skriver vi altid til klienten og informerer dem om dette, således at hvis de vender tilbage på et senere tidspunkt, at de er klar over at de skal oprette en ny profil.
6) Når du gør brug af WhatsApp som kommunikationsmiddel med dine klienter
    a) da sørg altid for at du ikke laver backups af samtalen lokalt på din telefon
    c) sørg for at der er en kode (på telefonen) for at få tilgang til din WhatsApp
    d) Hav ikke notifikationer slået til, så man kan læse noget af teksten (i pop-up notifikationer) uden af have tilgang til din WhatsApp
    e) brug en arbejdstelefon uden andre Apps installeret.
    f) slet samtalen når forløbet ender.
    g) download samtalen til en ekstern og sikker harddisk hvis relevant for journal.

7) Aidaform skriver at de vil holde vores data sikker, men fordi de har server uden for EU så har vi nogle ekstra foranstaltninger for datasikkerheden.
   Bl.a. bruger vi altid svar-ID frem for personfølsom data såsom navn.
   Svar-ID generes vilkårligt af psykologen og opbevares i klientens journal.
   I vores intromail, beder vi dem kun gøre brug af deres fornavn som identifikation af besvarelsen.
8) Vores hjemmesideudbyder Wix er iøvrigt helt up to date med alle sikkerhedsforanstaltninger, og har certifikater i ISO, PCI og TLS
   Læs mere her:
   https://support.wix.com/en/article/security-of-wixs-billing-services-and-pci-compliance#iso-compliance
   Datasikkerheden her ligger hos WIX
   Hvis man gør brug af synkronisering til googlekalender, kan man efter opstart af forløb redigere klientens navn til kun at indeholde deres initialer. Dette kan gøres under kontakter i WIX. I så tilfælde informeres klienten herom.
9) Opbevaring af journal
   a) skal være på en sikker ekstern harddisk, hvis journalen er digital.
   b) der skal ikke være adgang til denne journal fra internettet.
   c) adgang til denne journal skal være igennem kode.
   d) hvis den ikke er digital, er det et lovkrav at den opbevares bag lås i dit hjem.