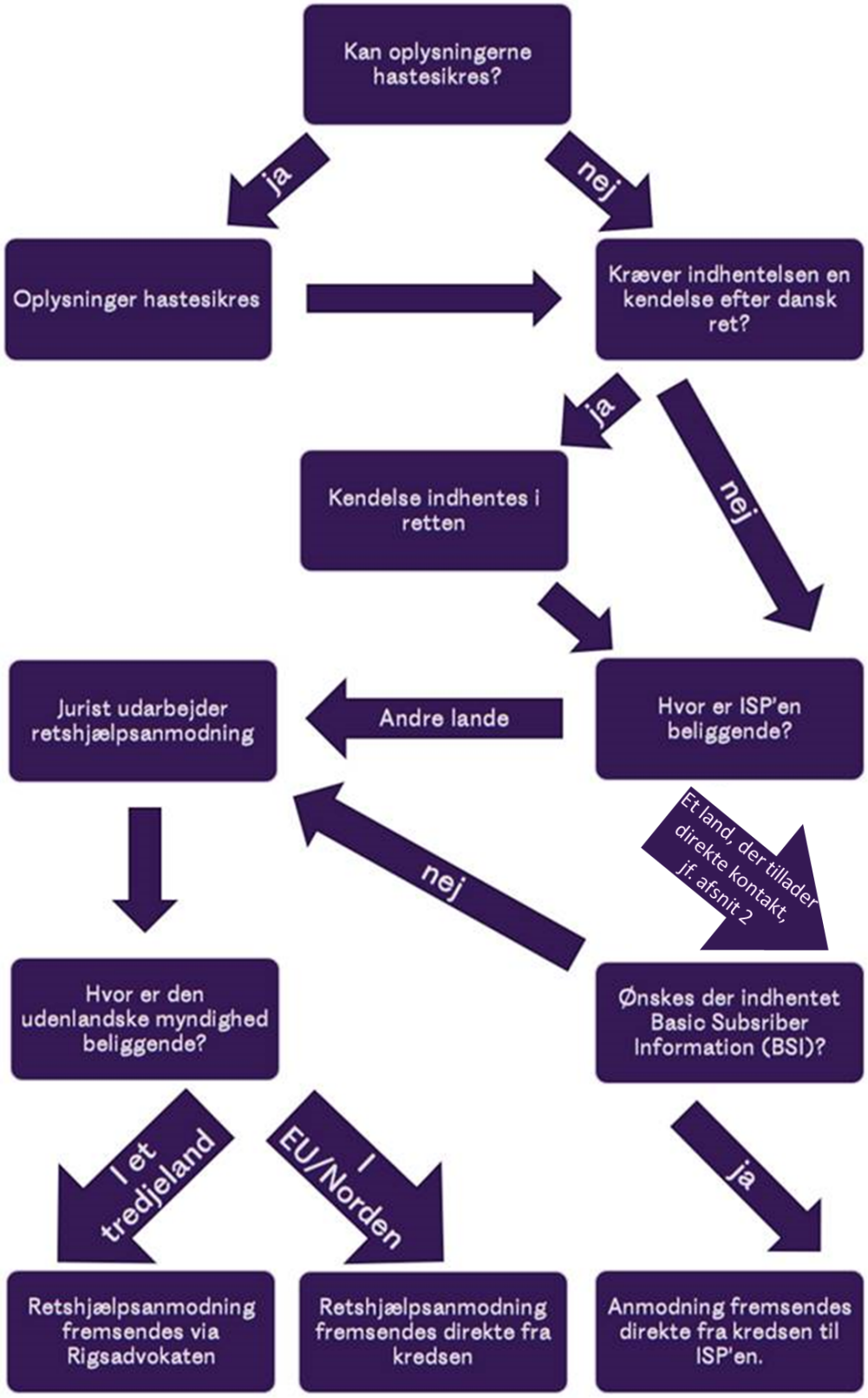
Indhentelse af elektroniske beviser fra internationale internetserviceudbydere mv. (Facebook, Google mv.)

Version 20. februar 2026

1. Overblik og tjekliste

FLOW CHART - Indhentelse af oplysninger fra internetserviceudbydere (ISP/OSP)



2. Retshjælpsanmodning eller frivillig udlevering af oplysninger?

Det følger af folkerettens almindelige regler om jurisdiktion, at staten har eneret til at udøve myndighed på sit territorium. Det betyder som udgangspunkt, at dansk politi udelukkende kan foretage efterforskning i Danmark. Såfremt et efterforskningsskridt skal foretages i udlandet, er det således som

udgangspunkt nødvendigt at anmode om udenlandske myndigheders bistand gennem en international retshjælpsanmodning.

Indhentelse af elektroniske beviser fra internetserviceudbydere mv. beliggende i udlandet skal derfor som udgangspunkt indhentes ved en international retshjælpsanmodning om edition.

2.1. Hvornår kan der rettes direkte henvendelse?

Nogle lande tillader, at dansk politi må kontakte serviceudbydere mv. beliggende i deres land med en anmodning om frivillig udlevering af visse elektroniske beviser – fx basic subscriber information (BSI). Politiet eller anklagemyndigheden kan i disse tilfælde rette direkte henvendelse til den relevante udenlandske virksomhed.

De lande, der tillader, at dansk politi må rette direkte henvendelse til serviceudbydere mv. beliggende i deres land er: **USA**, **Irland**, **Belgien**, **Cypern**, **Estland**, **Sverige**, **Østrig** samt **Ungarn**. Hvilke typer af anmodninger dansk politi må sende til virksomheder i de forskellige lande fremgår af følgende oversigt:

Direkte kontakt er tilladt til:						
Land:	**ISP:**	**OSP:**	**VASP:**	**Fysiske banker/ Pengeinstitutter:**	**VASPs med anm. om foreløbig "indefrysning" af midler:**	**VASPs med anm. om overførsel af crypto-midler til dansk politis "wallet", pba. en dansk beslaglæggelseskendelse:**
USA	**JA**	**JA**	**JA**	**NEJ**	**NEJ**	**NEJ**
Irland	**JA**	**JA**	**JA**	**JA**	**JA**	**JA**
Belgien	**JA**	**JA**	**JA**	**JA***	**JA**	**JA**
Cypern	**JA**	**JA**	**JA**	**JA**	**NEJ**	**NEJ**
Estland	**JA**	**JA**	**JA**	**JA**	**NEJ**	**NEJ**
Sverige	**JA**	**JA**	**JA**	**JA**	**JA**	**JA**
Østrig	**JA***	**JA***	**JA***	**NEJ**	**JA***	**JA***

Ungarn	**JA**	**JA**	**JA**	**NEJ**	**NEJ**	**NEJ**
Litauen	**NEJ**					
Malta	**NEJ**					
Luxembourg	**NEJ**					
De Britiske Jomfruøer	**NEJ**					
Frankrig	**NEJ**					
Tyskland	**NEJ**					
Grækenland	**NEJ**					
Letland	**NEJ**					
Slovenien	**NEJ**					
Rumænien	**NEJ**					
Polen	**NEJ**					
Holland	**NEJ**					
Bulgarien	**NEJ**					

Tjekkiet	**NEJ**
Kroatien	**NEJ**
Slovakiet	**NEJ**

ISP: Internet Service Provider - OSP: Online Service Provider - VASP: Virtual Asset Service Provider

*På baggrund af oplysninger fra de respektive landes myndigheder er der en stærk formodning imod, at de udenlandske virksomheder efterkommer sådanne anmodninger, hvorfor fremsendelse af en retshjælpsanmodning til de kompetente myndigheder anbefales.

Det er som beskrevet udgangspunktet, at danske myndigheder ikke kan rettes direkte henvendelse til en serviceudbyder mv. med det formål at få udleveret oplysninger. De tilladelser, som de nævnte lande har givet, omhandler som udgangspunkt samtykke til at dansk politi må sende en anmodning om frivillig udlevering af basisoplysninger. Læs mere om de forskellige typer oplysninger under pkt. 3 og i bilag 1.

Det bemærkes, at det afhænger af det omhandlede lands nationale regler, om det er tilladt for en serviceudbyder at udlevere oplysninger. Hvis det er tilladt, for en serviceudbyder at udlevere oplysninger til dansk politi, er det op til den enkelte udbyder, om den ønsker at udlevere oplysningerne uden et pålæg fra dets nationale kompetente myndigheder. Om en udbyder vil udlevere oplysninger på frivillig basis, afhænger i nogle tilfælde af typen af kriminalitet, sagen drejer sig om. Det kan derfor være relevant at konsultere den enkelte udbyders guidelines (law enforcement guide's) med henblik på at vurdere om det kan forventes, at denne udbyder vil udlevere oplysningerne på frivillig basis, eller om der i stedet skal sendes en retshjælpsanmodning til de kompetente myndigheder i det pågældende land. Læs mere herom under pkt. 7.

Der kan, uanset udbyderens geografiske placering, rettes direkte henvendelse til en udbyder med henblik på, at udbyderen sikrer oplysninger til senere udlevering. Du kan læse mere om hastesikring under pkt. 2.2.

I alle andre tilfælde skal der fremsendes en retshjælpanmodning til de kompetente myndigheder i det land, hvor oplysningerne befinder sig. Læs mere herom under pkt. 3.

2.1.1. USA - Virtual Asset Service Providers (VASPs)

USA har oplyst, at Virtual Asset Service Providers (VASPs) betragtes som finansielle institutioner og bliver behandlet på samme måde som en bank. Dog kan dansk politi desuagtet rette direkte henvendelse til en VASP med henblik på at få udleveret basisoplysninger. Det er frivilligt om en VASP vil udlevere sådanne oplysninger uden en amerikansk retskendelse, på baggrund af en dansk retshjælpsanmodning.

2.1.2. Belgien – EDSR / Telegram

Udover, at Belgien accepterer, at dansk politi- og anklagemyndighed retter direkte henvendelse til internetserviceudbydere beliggende i Belgien, accepterer Belgien endvidere, at dansk politi- og

anklagemyndighed retter direkte henvendelse til EDSR, der er Telegrams retlige repræsentant i Belgien.

Det bemærkes i den forbindelse, at Danmark ikke deltager i nogle af de internationale aftaler, der regulerer retlige repræsentanters udlevering af oplysninger til judicielle myndigheder. EDSR kan således alene anmodes om frivilligt at udlevere oplysninger.

2.2. Hastesikring

Elektroniske beviser på en konto kan blive slettet af brugeren, ligesom beviserne kan blive overskrevet eller på anden vis løbende slettet af udbyderen. Det er vigtigt at bemærke, at en udbyder sjældent gemmer data i mere end 3 måneder. Nogle udbydere tilbyder derfor at fastfryse (hastesikre) de oplysninger, der findes på en brugers konto, således at disse ikke bliver slettet permanent, imens anmodningen om udlevering af oplysninger udfærdiges og behandles.

For at sikre eventuelle beviser bør politiet derfor hurtigst muligt undersøge, hvorvidt den relevante serviceudbyder tilbyder hastesikring, og i givet fald anmode udbyderen herom. En anmodning om hastesikring kan sendes direkte til udbyderen.

Bemærk, at omfanget af de elektroniske beviser, som udbyderen kan **hastesikre**, går videre end de oplysninger, som kan **udleveres** på frivillig basis.

Det følger af amerikansk ret, at politiet og anklagemyndigheden i visse tilfælde skal sandsynliggøre, at de elektroniske beviser fortsat befinder sig hos serviceudbyderen på tidspunktet for rettens behandling af retshjælpsanmodningen. Derfor er en hastesikring af de ønskede oplysninger afgørende for, at retshjælpsanmodningen behandles og senere accepteres og opfyldes, jf. nedenfor under pkt. 3.2.2.3.

En udbyders hastesikring af elektroniske beviser sker på frivillig basis, og fremgangsmåden kan derfor variere hos de enkelte udbydere. Det er i denne forbindelse vigtigt at bemærke, at en eventuel hastesikring typisk alene vil gælde for en periode på 90 dage, og at kun nogle enkelte udbydere accepterer en forlængelse af den nævnte periode. En forlængelse af perioden sker ved fremsendelse af en ny anmodning til den relevante udbyder. Du kan finde henvisning til fremgangsmåden hos de enkelte udbydere under pkt. 7.

Såfremt en udbyder efter anmodning har hastesikret de ønskede oplysninger, skal dette fremgå af den efterfølgende anmodning til den udenlandske myndighed eller udbyder, ligesom udbyderens kvittering/ID-nummer for sikring bør vedlægges. Hvis udbyderen ikke har ønsket eller haft mulighed for at hastesikre de elektroniske data, skal dette ligeledes fremgå af en eventuel retshjælpsanmodning til den udenlandske myndighed.

3. Forberedelse

3.1. Generelle overvejelser

3.1.1. Hjemmel i Danmark

Inden der rettes henvendelse til udlandet, enten via retshjælpsanmodning eller direkte til udbyderen, skal der tages stilling til, hvorvidt der er hjemmel til at indhente de ønskede elektroniske beviser efter dansk ret. Retskendelser, herunder **kendelser om edition**, skal indhentes forud for fremsendelse af en

retshjælpsanmodning til en udenlandsk myndighed. For nogle udbydere er det en betingelse for frivillig udlevering af oplysninger, at der er indhentet en dansk kendelse.

3.1.2. Beskyttelse af efterforskningen

Endvidere skal det overvejes, om efterforskningen vil blive kompromitteret ved at indhente de elektroniske beviser. Efterforskningen kan blandt andet blive kompromitteret i tilfælde, hvor udbyderen agter at orientere den pågældende om anmodningen, eller hvor udbyderen vil slette den pågældendes konto som følge af, at denne er blevet anvendt i strid med udbyderens interne retningslinjer.

En dansk domstol kan ikke pålægge den udenlandske udbyder tavshedspligt efter retsplejelovens regler herom, men politiet og anklagemyndigheden kan i stedet anmode den udenlandske myndighed eller udbyder om at behandle henvendelsen fortroligt. En sådan anmodning om fortrolighed bør begrundes. Det kan også være hensigtsmæssigt at anmode den udenlandske myndighed eller udbyder om at kontakte politiet eller anklagemyndigheden i Danmark forud for fuldbyrdelsen af en anmodning, såfremt myndigheden eller udbyderen ikke agter at holde henvendelsen fortrolig[1].

3.1.3. Udvis forsigtighed

Markedet for internetserviceudbydere er kun reguleret i begrænset omfang, og nogle udbydere drives af kriminelle personer. Vær derfor varsom med at fremsende en anmodning samt fortrolige oplysninger direkte til ukendte udbydere.

3.1.4. Omfanget af oplysninger

Lovens betingelser for at pålægge en udbyder at udlevere oplysninger er sjældent ens i Danmark og udlandet. Særligt i USA stilles langt højere krav til mistankegrundlag mv. Derfor bør det overvejes, hvilke og hvor mange elektroniske oplysninger der ønskes udleveret, herunder om det foreliggende efterforskningsmateriale lever op til de udenlandske myndigheders krav for indhentelse af oplysningerne, jf. nedenfor pkt. 3.2.2.

De udenlandske myndigheders krav til efterforskningsmaterialet kan betyde, at de elektroniske oplysninger må indhentes ad flere omgange, f.eks. ved først at indhente identitetsoplysninger og på den baggrund skabe grundlag for at indhente indholdsdata.

Endvidere kan sagsbehandlingstiden variere ud fra mængden og arten af de oplysninger, der ønskes indhentet. Det vil således typisk tage 6-18 mdr. at indhente oplysninger fra USA via en international retshjælpsanmodning, hvorimod oplysninger indhentet direkte fra udbyderen typisk vil tage 14-30 dage. Politiet og anklagemyndigheden bør derfor inddrage tidsestimatet i vurderingen af nødvendigheden af retshjælpen, ligesom en eventuel retshjælpsanmodning bør udfærdiges på et så tidligt stadie af efterforskningen som muligt.

3.2. Udarbejdelse af en retshjælpsanmodning

[1] Eksempel: "If it is not possible to preserve confidentiality in the above manner, please notify me prior to executing this Letter of Request".

Samtidig med eller straks efter fremsendelse af en eventuel anmodning om hastesikring bør en anmodning om udlevering af oplysningerne udarbejdes.

Det afgørende for, om anklagemyndigheden skal fremsende en formel international retshjælpsanmodning til en udenlandsk myndighed, eller om der undtagelsesvist kan rettes direkte henvendelse til udbyderen, er udbyderens fysiske placering (idet enkelte lande har accepteret, at der rettes direkte henvendelse) og typen af oplysninger, som ønskes udleveret. Alle retshjælpsanmodninger udarbejdes som udgangspunkt af anklagemyndigheden, medmindre andet aftales konkret.

Anklagemyndighedens dokumentsamling indeholder koncepter til internationale retsanmodninger.

Find flere oplysninger på fagsiden Internationalt samarbejde på Vidensbasen (kræver login).

Se pkt. 8 – tjekliste til USA.

3.2.1. Typer af oplysninger

De elektroniske beviser kan typisk inddeles i 3 kategorier alt efter, hvor sensitive de er:

1. ”Basic Subscriber Information” – BSI (abonnementsoplysninger, herunder IP-adresser)
2. ”Transactional Information” – TI (trafikdata)
3. ”Content” (indholdsdata, fx indholdet af billeder eller beskeder)

Du kan læse mere om de forskellige typer oplysninger i bilag 1.

Alene oplysninger i den første kategori kan forventes udleveret på frivillig basis. Oplysninger i de sidste to kategorier kan således typisk alene udleveres på baggrund af en formel international retshjælpsanmodning sendt via den kompetente udenlandske myndighed.

3.2.2. Krav til mistankegrundlag mv.

Vær opmærksom på, at der særligt i USA stilles langt højere krav til det foreliggende efterforskningsmateriale, før domstolene pålægger udbydere at udlevere oplysninger, jf. pkt. 3.1.4.

3.2.2.1. BSI

Såfremt udbyderen er beliggende i USA, skal politiet og anklagemyndigheden i anmodningen redegøre for, at oplysningerne er relevante for og relateret til efterforskningen. Det er ikke tilstrækkeligt blot at anføre, at den mistænkte f.eks. har en e-mailkonto.

Såfremt anmodningen vedrører udlevering af IP-adresser i en bestemt tidsperiode, er det vigtigt at anføre det præcise tidspunkt og tidszone samt redegøre for, hvorfor oplysningerne er relevante i hele den anførte periode.

3.2.2.2. TI

Såfremt udbyderen er beliggende i USA, skal anklagemyndigheden i retshjælpsanmodningen anføre konkrete grunde til, at oplysningerne er relevante og væsentlige for efterforskningen.

3.2.2.3. Content

Såfremt udbyderen er beliggende i USA, skal anklagemyndigheden fremsende tilstrækkelige oplysninger til, at anklagemyndigheden i USA kan indhente en retskendelse. Det betyder, at der i retshjælpsanmodningen grundigt skal redegøres for, at der er særligt bestyrket mistanke om, at den pågældende har begået forbrydelsen, samt bestemte grunde til at antage, at beviser til brug for straffesagen kan findes i de ønskede oplysninger. Endvidere skal anklagemyndigheden redegøre for, at de faktiske oplysninger, der ligger til grund for vurderingen, er aktuelle, og at det er sandsynligt, at beviserne fortsat er iblandt de ønskede oplysninger. Det har i den forbindelse stor betydning, om der er sket hastesikring af oplysningerne.

I det omfang kravene til indhentelse af oplysninger i kategori 3 (Content) er opfyldt, er kravene til indhentelse af oplysninger i kategori 1 (BSI) og kategori 2 (TI) tillige opfyldt. Såfremt kravene til indhentelse af oplysninger i kategori 3 ikke er opfyldt, kan det overvejes at indhente de øvrige oplysninger med henblik på at styrke efterforskningsmaterialet, således at anklagemyndigheden efterfølgende kan anmode om oplysninger omfattet af kategori 3. Se endvidere pkt. 3.2.3 om oplysninger om omfanget af relevant materiale.

3.2.3. Oplysninger om omfanget af relevant materiale

Selvom udlevering af oplysninger kræver fremsendelse af en international retsanmodning til de udenlandske myndigheder, er visse udbydere villige til at udlevere informationer om omfanget af relevant materiale ved direkte henvendelse. Det kan eksempelvis være oplysninger om, at der findes et bestemt antal chatbeskeder i den periode, som politiet har oplyst som gerningstidspunkt, eller at der findes et bestemt antal billedfiler med en nærmere angivet datastørrelse med relation til efterforskningen.

Sådanne oplysninger kan understøtte efterforskningsmaterialet med henblik på at indhente oplysninger omfattet af kategori 2 (TI) og kategori 3 (Content). Derfor kan det allerede i forbindelse med hastesikring eller anmodning om identitetsoplysninger (BSI) være relevant at anmode udbyderen om, ud fra politiets oplysninger om den kriminelle handling, at angive den tidsperiode, der kunne indeholde relevante oplysninger for efterforskningen samt den samlede datastørrelse af det relevante materiale.

3.3. Fremsendelse mv.

For oplysninger om krav til oversættelse og fremsendelse af retshjælpsanmodningen mv. henvises til afsnittet i Rigsadvokatmeddelelsen om International retshjælp.

3.3.1. Hastende sager

Ved sager af hastende karakter, f.eks. terrorsager, kan det være hensigtsmæssigt at have et tæt samarbejde med den udenlandske myndighed. Kontakten til udenlandske myndigheder beliggende i tredjelande sker som udgangspunkt gennem Rigsadvokaten.

Rigsadvokaten kan vejlede om alternative fremsendelseskanaler i hastende tilfælde. Du kan kontakte Rigsadvokatens internationale enhed på tlf.: 7268 9082.

4. Love og andre forarbejder

- Den Europæiske konvention af 23. november 2001 om IT-kriminalitet
- Den Europæiske Konvention af 20. april 1959 om gensidig retshjælp i straffesager
- EU-konventionen af 29. maj 2000 om gensidig retshjælp i straffesager mellem Dem Europæiske Unions Medlemsstater

De største udbydere har deres retshåndhævelsesguidelines liggende online. Vær opmærksom på altid at anvende de nyeste guidelines, som kan findes på udbydernes hjemmeside eller ved google-søgning.

5. Tjekliste til USA

Tjekliste til anmodninger om gensidig retshjælp til USA i forhold til indhentelse af elektroniske beviser (Cybercrime eller info fra fx sociale medier/tjenester)

Retsgrundlag:

- Konvention af 23. november 2001 om IT-kriminalitet
- *Convention on Cybercrime of 23 November 2001*

Bevarelse (preservation):

- Hvis data bevares fra et tidligt tidspunkt, øges sandsynligheden for, at vi kan få resultater af det.
    - Kontakt udbyderen direkte eller brug døgnnetværket (*24/7 Network*).

- Ved bevarelse bedes du anføre datoen for bevarelsen og udbyderens referencenummer i din anmodning om gensidig retshjælp.
- Databevarelsen opretholdes ved fortsat indsendelse af anmodninger om forlængelse.

Oplysninger til anmodningen (denne oversigt er ikke udtømmende, men disse punkter bedes behandlet):

- Lovovertrædelser –
    - Hvad er den konkrete adfærd, som udgør de(t) strafbare forhold?
    - Er ordlyden af de relevante straffelovsbestemmelser medtaget?

- Den ønskede bistand – anfør følgende i anmodningen:
    - Den type oplysninger, der ønskes for hver enkelt konto (dvs. oplysninger om kontoens abonnent og transaktioner eller abonnent- og transaktionsoplysninger samt indholdsmæssige oplysninger for kontoen) samt de(n) periode(r), som der søges oplysninger for, og
    - Forholdet mellem jeres efterforskning og den ønskede bistand (med andre ord, hvorfor ønsker efterforskerne at få fremskaffet disse oplysninger?)

- Identifikation af konti (*account identifiers*) – findes der en entydig identifikation for de enkelte omtalte konti?
    - Tjek for afvigelser i stavemåder i anmodningen og oversættelser heraf.
    - Præcisér, hvis der bruges et tal eller bogstav, hvor det kan være svært at skelne:

        - O (bogstav) eller 0 (tal)
        - (L) eller 1 (et)
    - Muligheder for identifikation af Facebook-konti (medtag alle dem, I har):
        - Den e-mailadresse, der er tilknyttet kontoen
        - Facebook URL – www.facebook.com/brugernavn
        - ID-nummer
    - Hvis et vidne eller en forurettet samarbejder med jer, så overvej at bruge de værktøjer til selvhjælp, som udbyderne tilbyder, til at få data om kontoen (såsom værktøjet "Download My Facebook" eller funktionen "Download Your Data" i Googles Dashboard).

- Datoer og oplysninger om brug –
    - Er der et afgrænset tidsinterval for brugen af kontoen i forbindelse med den kriminelle aktivitet? Hvis muligt, så anfør den første og den sidste kendte dato, hvor kontoen blev brugt.
    - Indeholder anmodningen andre væsentlige datoer i efterforskningen?
        - Datoen for anmeldelse af forbrydelsen til politiet
        - Datoen hvor den mistænkte blev anholdt
    - Forklares det i anmodningen, hvordan kontoen er forbundet til den kriminelle aktivitet?
    - Forklares det i anmodningen, hvordan myndighederne blev opmærksomme på brugen af kontoen i forbindelse med den kriminelle aktivitet?

- Fortrolighed (confidentiality) – tages der i anmodningen stilling til følgende aspekter vedr. **fortrolighed**?
    - Tavshedspligt – vil det skade efterforskningen, hvis kontohaveren bliver gjort opmærksom på, at der er anmodet om oplysninger? Forklar i givet fald hvorfor.
    - Hemmeligholdelse – vil det skade efterforskningen, eller er der andre interesser, der skal tages hensyn til, og som retfærdiggør, at kendelsen ikke skal offentliggøres og/eller være tilgængelig for offentligheden?

- Ønsket procedure – anføres der i anmodningen eventuelle attestationer, som bevismaterialet skal leveres med, for at det lovligt kan anvendes i jeres straffesag?

- Hastende karakter – er der nogen tidsbegrænsninger, eller er anmodningen af hastende karakter? Er det i så fald tydeligt anført i anmodningen, og er der anført eventuelle tidsfrister (såsom datoer for hovedforhandling)?

Dataenes placering (vedr. indhold):

- Spørg udbyderen:
    - Hvor befinder dataene for de enkelte konti sig?
    - I hvilke(t) land(e) vil udbyderen acceptere retsskridt vedrørende den pågældende konto?
- Medtag disse oplysninger i anmodningen om gensidig retshjælp.

Særligt bestyrket mistanke (retlig standard "probable cause" ved mere end blot BSI):

Såfremt der søges indhold (content-data) fra et firma, serviceudbyder mv., så skal de amerikanske myndigheder møde den retlige standard "probable cause". Det er en væsentlig højere retlig standard end den i retsplejeloven i forbindelse med edition og kan bedst sammenlignes med særlig bestyrket mistanke. Probable cause er den samme standard som skal møde ved anmodning om ransagning. Anmodningen skal derfor indeholde mange flere oplysninger end ved edition i Danmark.

Betingelser for, at der kan etableres *probable cause*:

1. Troværdig information om forbrydelsen
2. Den troværdige information om forbrydelsen, skal kunne få en mand/kvinde af rimelig fornuft til at tro, at der er sket en forbrydelse.

Troværdigheden af informationen øges,

- hvis der er tale om en øjenvidne (førstehånds-vidne)
- Hvis informationen støttes af tekniske beviser.

Lidt simplificeret fortalt kræver den retlige standard, at man kan sandsynliggøre, at det man søger også befinder sig der, hvor man vil søge.

Det betyder, at anmodningen skal være meget omfangsrig med megen beskrivelse af alle relevante fakta.

For hver faktuel information der gives, skal der være angivet kilde til, hvorfra informationen stammer - **altså** – hvor ved vi det fra. Der skal IKKE vedlægges bilag der understøtter informationen. De amerikanske myndigheder lægger det der fremgår af anmodningen til grund.

Det kræver at man kan sandsynliggøre, at det man søger befinder sig der hvor man vil søge.

- Er der pålidelige beviser for, at der er begået et strafbart forhold?
    - Hvilke kilder henholder myndighederne sig til?
    - Hvornår fandt det strafbare forhold sted?

- Er der pålidelige beviser for, at det er sandsynligt, at den pågældende konto indeholder beviser i forbindelse med det strafbare forhold?
    - Hvordan har I fundet frem til kontoen?
    - Hvordan er kontoen forbundet til den mistænkte?
    - Blev kontoen brugt til at fremme den strafbare handling? Beskriv i givet fald hvordan.
    - Blev kontoen brugt til at drøfte den strafbare handling? Hvad ved man i så fald om disse drøftelser?

Fremsendelse gennem Rigsadvokaten

- Anmodningen og oversættelse – samt i helt særlige tilfælde bilag – samles i én pdf og sendes til Rigsadvokaten til rigsadvokaten@ankl.dk, som sender den til rette myndighed i USA.
    - Vedrørende bilag skal det bemærkes, at de amerikanske myndighede ikke ønsker bilag, idet de alene forlader sig på de informationer der fremgår af anmodningen. Det betyder, at relevant information skal fremgå af anmodningen, og der skal ikke henvises til bilag.
    - Kendelsen har ingen retskraft i USA, så den skal i udgangspunktet ikke med.

Bilag

Bilag 1: Typer af oplysninger

Basic Subscriber Information (BSI)

BSI er oplysninger om en abonnent, eksempelvis:

1. Abonnentens konto eller brugernavn (the subscriber's account or login name).
2. Abonnentens navn og adresse (the subscriber's name and street address).
3. Abonnentens telefonnummer eller numre (the subscriber's telephone number or numbers).
4. Abonnentens e-mailadresse (the subscriber's email address).
5. IP-adresse benyttet af abonnenten ved registrering af kontoen (the Internet Protocol (IP) address used by the subscriber to register the account or otherwise initiate service).
6. Alle IP-adresser benyttet af abonnenten ved tilgåelsen af kontoen (all IP addresses used by the subscriber to log into the account).
7. Tidspunkter og dato for samt varighed af sessioner (session times, dates and duration).
8. Andre oplysninger vedrørende abonnenten med henblik på identifikation af denne, herunder betalingsoplysninger (any other information pertaining to the identity of the subscriber, including, but not limited to billing information (including type and number of credit cards, student identification number, or other identifying information).

Transactional Information (TI) – trafikdata

TI er oplysninger om trafikdata og svarer til historiske teleoplysninger om en telefon. Som eksempel på TI kan nævnes:

1. Forbindelsesoplysninger om andre systemer, som abonnenten har besøgt via e-mailkontoen (connection information for other systems to which the user connected via the email account/web host account), inkl.
    a. Forbindelsesdestinationen eller oprindelsessted for forbindelsen, inkl. tilslutningsport (connection destination or source of connection).
    b. Forbindelsestidspunkt, -dato og tidszone (connection time and date).
    c. Frakoblingstidspunkt, -dato og tidszone (disconnect time and date).
    d. Forbindelsesmetode (eksempelvis telnet, ftp, http) (method of connection to system (e.g. telnet, ftp, http)).
    e. Mængden af dataoverførsel (eksempelvis antal bytes) (data transfer volume (e.g. bytes)).
    f. Andre relevante routerinformationer (any other relevant routing information)
2. Afsender/modtager af en e-mail samt oplysninger om dato, tidspunkt og datastørrelsen (ikke indhold) (source of destination of any electronic mail messages sent from or received by the account, and the date, time, and length of the message).
3. Information vedrørende billeder, videoer eller dokumenter uploadet til kontoen eller hjemmesiden, herunder dato og tidspunkt for upload, samt filens størrelse (ikke indhold) (information pertaining to any image(s) or other documents uploaded to the account/website, including the dates and times of upload, and the size of the files).
4. Navn og andre identifikationsoplysninger på personer, der har besøgt en bestemt hjemmeside, fil, billede eller lignende inden for en bestemt periode (name and other identifying details of indiviuals that accessed a specific image/file/web page in a specified period of time, on a specific date).

Content

Typen af oplysninger om indhold, som anklagemyndigheden kan anmode om at få udleveret, afhænger af kontotypen:

1. For e-mail og web hosting konti: Indholdet af alle e-mails, herunder vedhæftede filer, der er lagret på kontoen, inkl. indholdet af de e-mails, der er afsendt fra kontoen samt udkast (the content of all emails stored in the account, including copies of emails sent from the account and drafts).
2. For sociale medier: Alt indhold, herunder indholdet af chatbeskeder til og fra abonnenten, vennelister, medlemsskaber af grupper og begivenheder (all communications and messages made or recieved by the user, including all private messages, attachments (video, audio and picture), groupmemberships and events).

Bilag 2: Flow chart - Indhentelse af oplysninger fra internetserviceudbydere (ISP/OSP)

Se flow chart under pkt. 1.