UPPDATERAD VÄGLEDNING OM ANVÄNDNINGEN AV EXTERNA IT-TJÄNSTER I ADVOKATVERKSAMHET

Till Sveriges advokatsamfunds styrelse

Advokatsamfundets styrelse har uppdragit åt en arbetsgrupp att uppdatera den vägledning om externa IT-tjänster i advokatverksamhet som beslutades den 9 juni 2011.

Arbetsgruppen har bestått av advokaterna Björn Gustavsson, Lars Perhard, samt Johan Sangborn, stf. chefsjurist vid Advokatsamfundets kansli.

I denna rapport redovisar arbetsgruppen sina överväganden, rekommendationer och praktiska råd. Arbetsgruppen anser sig härmed ha slutfört sitt uppdrag.

Stockholm den 20 mars 2019

Björn Gustavsson Lars Perhard Johan Sangborn

INNEHÅLLSFÖRTECKNING

1. Sammanfattning

Arbetsgruppen har fått i uppdrag att uppdatera de bedömningar och analyser som gjordes i rapporten från 9 juni 2011 om advokaters möjligheter att inom ramen för advokatverksamheten använda sig av olika externa IT- och webbaserade tjänster. Frågan om advokaters IT-lösningar och informationslagring utanför advokatbyråns ”egna väggar” har aktualiserats av den kontinuerliga tekniska utvecklingen, det tilltagande hotet mot advokatetiska kärnvärden (främst i fråga om advokatsekretess) samt nya lagstiftningsåtgärder som avser dataskydd och personlig integritet liksom tvångsmedelsanvändning och uppgiftslämning avseende elektroniska dokument och digitaliserade uppgifter. Av särskilt intresse är EU:s dataskyddsförordning (GDPR) som trädde i kraft den 25 maj 2018.

Vad gäller GDPR har Advokatsamfundets styrelse den 9 mars 2018 (cirkulär nr 6/2018) antagit en *Vägledning för tillämpningen av EU:s dataskydds-förordning i advokatverksamhet*. Dataskyddsvägledningen täcker även in en rad frågeställningar som måste beaktas i samband med att en advokat upphandlar externa IT-tjänster och teknisk utrustning.

Även eventuella lagstiftningsförslag om moderniserade straffprocessuella tvångsmedel avseende bland annat digitalt lagrad information till följd av beslagsutredningens förslag i december 2017 (SOU 2017:100) kan komma att få betydelse för elektroniskt lagrad information i advokatverksamhet.[1] I dagsläget har regeringen dock ännu inte presenterat några lagförslag om förändrad tvångsmedelsanvändning i IT-miljö.

Den bedömning som gjordes i 2011 års rapport om att det inte finnas något hinder mot att använda externa IT-lösningar (främst s.k. molntjänster) i advokatverksamhet, under förutsättning att advokatens tystnadsplikt och skydd av

[1] Se Beslagsutredningens betänkande Beslag och husrannsakan – ett regelverk för dagens behov (SOU 2017:100).

klientinformation, liksom övriga yrkesplikter upprätthålls och efterlevs, gäller alltjämt.

Enligt arbetsgruppen finns det emellertid numera ytterligare ett antal förhållanden som särskilt måste uppmärksammas när en advokatbyrå väljer att låta en extern leverantör ansvara för byråns ärendedokumentation och klientinformation. Avgörande är att det finns en tydlig hantering av dataskyddsfrågor, säkerhet kring information och skydd av känsliga uppgifter. Om IT-leverantörens personal kan komma åt konfidentiella uppgifter måste deras diskretion och tystnadsplikt säkerställas, genom upprättande av sekretessavtal eller dylika åtgärder samt genom information om insiderlagstiftning, m.m. Åtkomstmöjligheten för den externa IT-leverantören bör under alla förhållanden begränsas så mycket som möjligt. Den externa leverantören måste å sin sida dessutom ha en utarbetad och väl fungerande säkerhetspolicy, syftande till att säkerställa att inga obehöriga kan få tillgång till systemen med advokatbyråns ärendematerial och klientinformation.

När advokatbyråer använder sig av externa IT-lösningar för sin kontorsorganisation måste det vidare säkerställas att den elektroniska hanteringen av ärenden, klientinformation och annan information, sker på ett sådant sätt att det även i övrigt är förenligt med det advokatetiska regelverket och att klienternas rättigheter och skydd därmed upprätthålls. Särskilt aktualiserar frågan om externa IT-lösningar för advokater den så viktiga frågan om skyddet för informationsutbytet mellan advokat och klient. När det kan förutses att särskilt känslig information kan komma att hanteras, bör därför advokatbyrån informera klienten om – och om så anses nödvändigt även inhämta klientens samtycke till – att ärenderelaterade handlingar och uppgifter hanteras genom extern IT-leverantör.[2]

Förvaring av klientinformation i egna lokaler i traditionell mening kan aldrig bli helt säker mot stöld, brand, inbrott och andra tänkbara incidenter. Det krav som finns är att advokaten ska förvara klientinformationen på ett så betryggande sätt

[2] Se vidare sid. 20 under överväganden om behovet i vissa fall av att informera klienten om advokatbyråns IT-lösning, m.m. (punkten 9).

som möjligt, enligt principen om det tekniskt möjliga och ekonomiskt rimliga. Denna princip får anses gälla samtliga typer av klientrelaterad information, oavsett om den finns i pappersform eller i elektronisk form. Det finns därför ingen anledning att göra någon annan bedömning i de fall informationen förvaras genom externa IT-tjänster.

Sammantaget konstateras att användningen av datateknik erbjuder advokatbyråer en möjlighet att förbättra standarden och snabbheten på juridiska tjänster. Externa IT-tjänster erbjuder advokatbyråer en flexibel och kostnadseffektiv hantering av elektroniskt lagrad information. Användandet av externa IT-lösningar innebär dock även utmaningar, risker och praktiska problem i förhållande till krav på dataskydd och de särskilda professionella skyldigheter och etiska regler som gäller för advokater. Det finns även särskilda risker förenade med att använda externa IT-lösningar av extraterritoriellt slag, innebärande att data lagras på servrar i länder som inte svarar upp mot den regelnivå i fråga om dataskydd, konfidentialitet och skydd mot utlämnande av uppgifter som råder inom EU. Denna promemoria innehåller en rad rekommendationer och praktiska råd, avseende hur sådana risker och problem kan hanteras och i bästa fall undvikas.[3]

Användandet av externa IT-lösningar aktualiserar dessutom frågan om i vilken utsträckning myndigheter kan kräva åtkomst – genom processuella tvångsåtgärder eller på annat sätt – till inom advokatverksamheten elektroniskt lagrad information som finns utanför advokatbyråns ”egna väggar”. Arbetsgruppens bedömning är mot bakgrund av befintlig domstolspraxis (se främst NJA 2015 s. 631 och NJA 2010 s. 122), uttalanden av JK och JO, doktrin på området, samt i

[3] Även om teknikutvecklingen under senare år har gått mycket snabbt framåt, finns fortfarande viss ledning att hämta i fråga om advokats elektroniska kommunikation från Advokatsamfundets promemoria *e-post och annan digital teknik i advokatverksamhet – några punkter att tänka på*, som den 21 oktober 2004 tillställdes ledamöterna genom cirkulär nr 22/2004. I fråga om vad en advokat specifikt bör beakta vid användning av externa IT-tjänster hänvisas även till den vägledning som år 2012 antagits av Rådet för advokatsamfunden i Europeiska unionen, CCBE, *CCBE Guidelines on the Use of Cloud Computing Services by Lawyers*, liksom till den rekommendation som CCBE år 2008 antagit rörande elektronisk kommunikation (*Guidance for European Lawyers on Electronic Communication and the Internet*).

frånvaro av idag befintlig lagstiftning som skulle tyda på motsatsen (se nedan avsnitt 4.3),[4] att samma skydd för externt lagrad elektronisk information gäller som för information som finns internt på advokatbyrån.

Beslagsförbudsreglerna avseende uppgifter som omfattas av advokatsekretess och skydd mot edition, m.m. får därmed anses gälla även om informationen är lagrad eller på annat sätt finns utanför advokatbyråns egna väggar, t.ex. på en extern dataserver här i landet.[5]

Eftersom externt lagrad information emellertid också kan förvaras på dataservrar utanför Sverige, innebär det att även den lagstiftning som gäller i det land där informationen finns lagrad avgör vilket skydd som finns för advokatbyråns digitala uppgifter. Det är därför viktigt att nogsamma överväganden görs i fråga om placeringen av de externa dataservrar som advokatbyråer avser att använda för sin datahantering och informationslagring.[6] Såsom framgår av denna vägledning finns det även en rad andra omständigheter som grundligt måste analyseras innan känslig information anförtros en extern IT-leverantör.

[4] Se Beslagsutredningens betänkande Beslag och husrannsakan – ett regelverk för dagens behov (SOU 2017:100).
[5] Enligt gällande rätt tillämpas beslagsförbudsreglerna analogiskt på elektroniskt lagrad information (NJA 2015 s. 631).
[6] Se särskilt rörande risker förknippade med dataservrar utanför EU sid. 4 f. i CCBE:s vägledning om advokaters användning av molntjänster (*CCBE Guidelines on the Use of Cloud Computing Services by Lawyers*).
.

2. Arbetsgruppens överväganden och rekommendationer

2.1 Inledning

Utövningen av advokatyrket sker i allt högre utsträckning med hjälp av digital teknik, ofta genom överföring och lagring av information i elektronisk form (data). Informationsflödena är också ofta gränsöverskridande. Datatrafik och lagring sker mer och mer genom användande av externa leverantörer som sköter trafiken och lagrar informationen på sina servrar belägna i datacenter inom eller utom Sverige.

2.2 Teknikfrågor m.m.

Ett teknikområde som kraftigt påverkat användningen av IT är s.k. molntjänster. Vad som avses med detta är IT- eller webbtjänster som tillhandahålls användaren, t.ex. en advokatbyrå, av en extern leverantör över *internet* (servrar, applikationer, data, m.m.). Förenklat kan sägas att det förhållandevis nya med molntjänster, jämfört med tidigare kända IT-företeelser (som traditionell s.k. *Outsourcing*, *Application Service Provider*, *ASP*, *hosting* och andra liknande lösningar), är att marknaden nu erbjuder prismässigt mycket attraktiva och konkurrenskraftiga IT-tjänster, vilka har blivit möjliga genom en allt billigare tillgång till bandbredd och datalagring, delvis betingad av överskottskapacitet i stora datacenter världen över. Detta medför emellertid att användaren oftast inte vet var eller på vilken eller vilka servrar data hanteras, lagras och behandlas.

Flera av de ledande leverantörerna i IT-branschen[7] följda av ett stort antal medelstora och mindre aktörer, har investerat och fortsätter investera i betydande omfattning på detta teknikområde. Exempel på molntjänster för advokater är internetbaserad e-mail, datalagringstjänster *on line* och olika applikationstjänster som kan användas på distans, från kontoret eller plats utanför kontoret. En sådan

[7] Exempelvis *Google*, *Microsoft*, *Amazon*, *IBM* och *HP*.

tjänst i molnet kan exempelvis omfatta funktionalitet för konfliktkontroll, dokumenthantering, tidredovisning och fakturering samt lagring av data. Tjänsterna kan nyttjas av användaren med hjälp av egen utrustning (t.ex. *PC*, *Mac*, pekplatta eller *smartphone*).

Användningen av tekniken medför ett kostnadseffektivt sätt att lagra advokatbyråns data, men exponerar också advokatbyråer för problem från säkerhetssynpunkt, bl.a. eftersom advokater därmed i ökande utsträckning använder lösningar som medger fjärråtkomst av information oavsett om informationen finns hos externa leverantörer eller om advokaten har en egenhantering med servrar inom byråns väggar. Advokaten kan arbeta utanför kontoret och komma åt i princip samma information som om denne befann sig på kontoret. Bredbandskapacitet via fiber, mobilt bredband och uppkoppling via *WiFi* är några exempel på tekniska lösningar som medger åtkomst till både advokatbyråns interna och externa nätverk, varmed stora mängder information skickas fram och tillbaka, ibland helt oskyddat. Säkerheten påverkas i hög grad av vald teknik och vilka säkerhetsrutiner den valda leverantören tillämpar. Exempel är kryptering av e-posttrafik och s.k. *redundans*, dvs. att informationen vid problem kan kommas åt på annan teknisk eller fysisk plats. Det är, som nämns nedan, emellertid inte ovanligt att säkerheten till och med ökar vid användning av externa IT-tjänster.

Ett annat teknikområde som för advokater idag är vanligt förekommande är de delvis nya redskap som används i verksamheten, såsom allt mindre och kraftfullare bärbara datorer, s*martphones*, pekplattor, usb-minnen, *flash-drives* m.m. Trådlösa *scanners* och skrivare med direkt access till *internet* och med hög lagringskapacitet kan också nämnas.

Det är i detta sammanhang inte möjligt att kartlägga, kommentera eller auktorisera specifika tjänster och produkter som erbjuds av marknaden från ett advokatperspektiv. Utvecklingen är dessutom under ständig och snabb förändring, vilket gör att en utvärdering under alla förhållanden skulle få ett kort ”bäst före

datum”. I detta dokument redovisas därför endast övergripande, liksom märkes- och teknikneutrala, synpunkter i syfte att vägleda eller medvetandegöra de advokater som redan använder eller har för avsikt att använda externa IT-lösningar för sin advokatverksamhet; i fråga om risker, lämpliga skyddsåtgärder, beaktande av yrkesplikter, m.m.

2.3 Etiska regler

Såsom utvecklas i avsnitt 4.2 nedan finns en rad etiska regler som har bäring på advokaters användning av externa IT-lösningar. I det etiska regelverket regleras först och främst den så viktiga tystnads- och diskretionsplikten, avseende det som anförtrotts advokaten inom ramen för advokatverksamheten.

Vidare finns regler om arkivhållning (tio år eller den längre tid som ärendet påkallar), liksom om skyldighet att se till att advokatens kontorsorganisation är i god ordning och att klientens information förvaras på ett betryggande sätt med hänsyn till dess innehåll och omständigheterna i övrigt.

Denna reglering tar primärt sikte på traditionell (analog) information. De etiska reglerna är dock teknikneutrala och det ställs därför samma krav på upprätthållande av yrkesplikterna när det gäller klientrelaterad digital information.

Innan en advokatbyrå bestämmer sig för att kommunicera eller lagra data med hjälp av externa tjänsteleverantörer måste man således förvissa sig om att informationen därmed också skickas och förvaras på ett lika betryggande sätt som om advokatbyrån hade hanterat sina data på egen server inom kontorets väggar, med de erforderliga och rimliga säkerhetsåtgärder som en sådan hantering föranleder.

2.4 Överväganden och rekommendationer

Det är som ovan nämnts inte möjligt att i detalj ange vilka externa IT-tjänster en advokatbyrå bör kunna anlita. Som så ofta annars i advokatverksamhet handlar det om att använda sunt förnuft, iaktta viss försiktighet samt vidta rimliga åtgärder till skydd av information och upprätthållande av yrkesplikter.

I syfte att underlätta för advokatbyråer inför anlitande av leverantörer som tillhandahåller externa IT-tjänster, har nedan listats ett antal punkter med övergripande praktiska råd och andra rekommendationer. Listan är inte uttömmande och utgör endast en exemplifiering av överväganden som advokatbyråer bör göra inför användning av externa IT-tjänster i sina advokatverksamheter.

Ett samarbete med en leverantör av externa IT-tjänster handlar till stor del om förtroende. Advokatbyrån bör förvissa sig om att den tilltänkta leverantören har en sådan ställning (både kompetens- och erfarenhetsmässigt, finansiellt och i övrigt) att leverantören kan förväntas fullgöra de åtaganden som får anses nödvändiga när det gäller handhavandet av elektroniskt lagrad information tillhörig en advokatbyrå. Därutöver bör advokatbyrån göra sådana kontroller och ta sådana referenser, som man normalt alltid bör göra innan man ingår affärsförbindelser, exempelvis beträffande marknadsposition, försäkringsskydd och leverantörens förmåga att leva upp till befintliga standarder.

Utöver nämnda kommersiella överväganden bör advokatbyrån särskilt beakta följande aspekter innan en molntjänst eller annan form av extern IT-lösning införskaffas.[8] Detta är också sådant som lämpligen bör återspeglas i form av krav i avtalet med leverantören.

[8] Ytterligare överväganden kan även vid behov göras utifrån CCBE:s rekommendationer i *CCBE Guidelines on the Use of Cloud Computing Services by Lawyers*.

1. **Åtkomst:** Advokatbyrån ska vid varje given tidpunkt snabbt och utan inskränkningar kunna komma åt all sin information i ett för advokatbyrån hanterbart format; för att underlätta överföring vid t.ex. flytt till annan leverantör eller hemtagning av data. Advokatbyrån bör därför vara särskilt uppmärksam på exempelvis verksamhetsförändringar hos leverantören som kan tänkas försvåra eller på sikt omöjliggöra fullgörandet av tjänsten.

2. **Säkerhet:** Leverantören ska bedriva ett fortlöpande säkerhetsarbete så att inte informationen, vare sig i transit eller i vila, obehörigen kan åtkommas av tredje man, t.ex. genom s.k. *hackers* på *internet* eller andra typer av attacker.

3. **Sekretess:** Det ska i avtalet regleras att advokatens/kundens information inte får lämnas ut till tredje man eller användas av leverantören för andra ändamål än att leverera tjänsten. Leverantörens anställda och eventuella underleverantörer får inte beredas möjlighet att ta del av konfidentiell klientinformation i större utsträckning än vad som är nödvändigt för uppdragets utförande. Om IT-leverantörens, eller eventuella underleverantörers, personal måste komma åt konfidentiella uppgifter, måste deras tystnadsplikt och diskretion säkerställas genom avtal. Här ska noteras att leverantörerna ofta i sina anställningsavtal har sekretessåtaganden som är adekvata, att det – beroende på leverantörens rutiner – ofta är så att de anställda normalt inte har åtkomst till information på sådant sätt att den kan läsas i klartext samt att det ofta finns rigorösa rutiner kring hanteringen när sådan åtkomst undantagsvis krävs. Den externa personalen bör vidare informeras om tystnadsplikt i förhållande till insiderlagstiftning och liknande regleringar. Se även vad som nedan anges om kryptering.

4. **Skydd:** Åtkomst till data måste säkerställas och data måste skyddas mot förvanskning. Leverantören ska bl.a. fortlöpande ta *backup* eller på annat sätt säkerställa att den lagrade informationen inte går förlorad och även

spara e-post korrespondens under viss tid i avvaktan på lagring. Leverantören måste ha erforderliga brandväggar och annat skydd, mot informations(för-)störande åtgärder (t.ex. virus, *spyware*, trojaner och annan s.k. *malware*), etc.

5. **Driftavbrott:** Många av de molntjänster som blir aktuella för en advokatbyrå är viktiga för den dagliga verksamheten, varför längre driftavbrott kan få stora konsekvenser. Leverantören bör i avtal eller på annat sätt därför klargöra vilka åtgärder leverantören vidtagit för att minimera risken för avbrott och hur snabbt driften kan återupptas om något allvarligt händer med de aktuella servrarna (t.ex. brand eller sabotage). Det kan handla om alternativa datacenter på olika platser, speglade diskar eller andra lösningar.

6. **Intern användarreglering:** Det måste finnas en tydlig reglering av hur advokatbyråns anställda ska ha tillgång till IT-miljön, t.ex. genom tydliga anvisningar om användande av erforderligt säkra lösenord, eventuell kryptering och aktivering av skalskydd på advokatbyråns datorer, *smartphones* och pekplattor.

7. **Gränsöverskridande tjänster:** Om informationen kan komma att lagras på servrar belägna i länder som har en annan legal skyddsnivå för elektroniskt lagrad data än vad vi har i Sverige, måste advokatbyrån beakta detta. Det kan t.ex. bli fråga om att i avtalet med leverantören reglera att data inte får lagras utanför en viss region (t.ex. EU) eller utanför ett visst land. Typiskt sett kan det vara svårt eller opraktiskt att inhämta samtycke från klienten i dylika frågor. Det är därför lämpligt att föra en dialog direkt med leverantören för att säkerställa att erforderlig skyddsnivå gäller för advokatbyråns data.[9]

[9] Se även Dataskyddsvägledningen sid. 9 (avsnitt 1.3.13) och sid. 57 f. (avsnitt 10.1).

8. **Äganderätten till data:** Advokatbyråns äganderätt till sin (och klientens) data måste säkerställas i avtalet med leverantören, inklusive – när detta krävs – information som uppkommer under hand, t.ex. metadata och trafikdata. Det bör framgå av avtalet att äganderätt till advokatbyråns klientdata inte under några omständigheter kan övergå till leverantören. I detta sammanhang noteras att det är lämpligt att med leverantören diskutera användningen av metadata och trafikdata. Leverantören behöver tillgång till metadata för att kunna tillhandahålla tjänsten och har ofta ett intresse av att även efter avtalets upphörande kunna använda aggregerad (anonymiserad) trafikdata. Advokatbyrån har dock mycket sällan något intresse av vare sig metadata eller trafikdata, utan advokatbyråns primära intresse är att data som leverantören även efter avtalets upphörande har tillgång till inte kan kopplas till advokatbyrån eller dess klienter.

9. **Extern åtkomst (tvångsåtgärder, m.m.):** Förutom en uttrycklig reglering av sekretess bör det även utformas skriftliga instruktioner om hur leverantören ska agera i de fall denne av svensk eller utländsk domstol eller myndighet blir ålagd att lämna ut information. Utgångspunkten i ett sådant fall är normalt att informationen eller de elektroniskt lagrade handlingarna tillhör advokaten och att samma reglering som gäller för skydd av advokatsekret skriftlig information därmed ska tillämpas på den hos leverantören elektroniskt lagrade informationen. Utlämnande får därmed inte ske utan advokatbyråns eventuella godkännande (se närmare avsnitt 4.3.2 och 4.3.3).[10]

10. **Leverantörens riktlinjer:** Leverantören bör ha tydliga riktlinjer (policy) i fråga om säkerhet och dataskydd. Krav på att leverantören ska ha sådana

[10] I detta sammanhang noteras att det pågår en diskussion om räckvidden av den amerikanska lagstiftningen *the US Cloud Act*, som anses kunna innebära att amerikansk domstol kan ålägga ett amerikanskt företag (eller dess koncernbolag) att lämna ut information, även om informationen lagras på servrar t.ex. inom EU. Det skulle föra för långt att i detta dokument gå in på detaljer kring detta, men om en advokatbyrå avser att för externa IT-tjänster anlita en leverantör som ingår i en amerikansk grupp av företag, bör advokatbyrån beakta denna risk. CCBE har analyserat the US Cloud Act och dess implikationer på och förenlighet med europeisk rätt; se *CCBE Assessment of the U.S. CLOUD Act*.

riktlinjer kan antingen tas in i avtalet eller så kan advokatbyrån nöja sig med att leverantören verifierar att denne har och tillämpar sådana riktlinjer.[11] Sådan policy bör finnas i vart fall

a) för att informera advokatbyrån om eventuella incidenter rörande säkerhet (normalt åtgärdar leverantören brister när de uppdagas utan att informera kunderna och detsamma gäller försök till angrepp som, om de lyckats, skulle leda till en säkerhetsincident);

b) för att informera advokatbyrån för det fall leverantören skulle bli föremål för utländsk domstols eller myndighets åtgärder som innefattar krav på utlämnande av information (se ovan p. 8 och 9);

c) för permanent radering av eventuellt kvarvarande data (t.ex. dubbletter p.g.a. *backup* eller på s.k. speglade diskar) efter flytt samt för partiella lösningar (t.ex. i de fall en enskild advokat, av flera, lämnar advokatbyrån), om inte detta framgår av avtalet, där det ofta anges att all kunddata raderas viss tid efter avtalets upphörande samt att kunden själv när som helst kan radera sin egen data; samt

d) beträffande advokatens rätt till insyn i leverantörens säkerhetsåtgärder.

11. **Kryptering:** Leverantören bör verifiera i vilken omfattning denne använder kryptering beträffande data, såväl i transit och bearbetning som i vila. Advokatbyrån kan i detta sammanhang behöva överväga om krav på mer avancerad kryptering bör ställas.

12. **Klientinformation och samtycke:** Klienten kan – när så, beroende på uppdrag, klient och andra omständigheter, bedöms lämpligt – behöva informeras om byråns användning av externa IT-tjänster. Advokatbyrån kan även utifrån samma bedömningsgrunder i vissa fall behöva överväga

[11] Se även Dataskyddsvägledningen sid. 50 ff. (avsnitt 7.3) för information av vilka krav m.m. som ska ställas på leverantören vid anlitande av denne som personuppgiftsbiträde.

nödvändigheten av att inhämta samtycke från klienter innan en molntjänst tas i användning för hantering av klienternas data. Huvudregeln bör dock vara att samtycke inte ska behöva inhämtas för själva personuppgifts-behandlingen, eftersom behandlingen av klientens uppgifter är en nödvändig åtgärd för att fullgöra ett avtal.[12]

13. **GDPR**: Avtal med en leverantör ska vara förenliga med GDPR:s krav, vilket bl.a. innebär att personuppgiftsbiträdesavtal måste upprättas eller ingås som del av ett avtal om externa IT-tjänster och att särskilda krav måste vara uppfyllda för att personuppgifter ska få överföras till länder utanför EES-området eller andra länder med annan legal skyddsnivå (se ovan p. 7).

[12] Se vidare avsnitt i Dataskyddsvägledningen sid 30 ff. om lagliga grunder för behandling (avsnitt 2.2).

3. Externa IT-tjänster

3.1 En användning förenad med vissa frågor och problem

Under en längre tid har frågor dykt upp kring advokaters möjligheter att använda sig av externa IT-lösningar inom ramen för advokatverksamheten. Ett allt vanligare förekommande fenomen har blivit att, i stället för att investera stora pengar för att skapa bra och säkra datalösningar internt på advokatbyrån, i stället köpa relativt billiga externa resurser i form av olika slags internettjänster, s.k. molntjänster, vilket innebär en möjlighet att hantera program, datalagring, kapacitet och processorkraft på en extern resurs (se närmare beskrivning nedan i avsnitt 3.2). En viktig aspekt med denna typ av molntjänst är den tillgänglighet som det innebär att slippa hålla datalagring och filer på en enskild plats. I IT-molnet får kunden enkelt tillgång till sitt material oberoende av var denne befinner sig, genom uppkoppling på en dator. På så sätt slipper advokaten/advokatbyrån att själv ombesörja byråns IT-administration. Många gånger kan den tredjepartsleverantör som förvarar all information i skyddade datahallar dessutom upprätthålla långt bättre fysisk säkerhet (”skalskydd”) än vad många advokatbyråer själva klarar av att upprätthålla med interna lösningar.

Externa IT-lösningar för emellertid även med sig en rad olika risker. Förutom skalskyddet, är informationssäkerhet (”teknisk säkerhet”) en viktig fråga. Eftersom det inom advokatverksamhet ofta finns ytterst känslig information, måste denna typ av externa IT-lösningar kunna säkerställa högsta möjliga säkerhet, t.ex. genom att hårdvaran omgärdas av robusta brandväggar och att hanteringen innefattar säker inloggning (t.ex. högkvalitativ s.k. tvåstegs-autentisering)[13], kryptering, etc.

[13] Tvåstegsautentisering av lägre kvalitet kan ofta hackas genom återställningsfunktionen. Återställning via sms och mobilnummer innehåller säkerhetsbrister p.g.a. teleoperatörers låga säkerhetskrav på registrering av vidarekoppling m.m.

En annan viktig fråga i detta sammanhang är självfallet hur en sådan extern IT-lösning måste vara utformad för att svara upp mot de etiska krav som ställs på advokater och advokatbyråer till skydd för klienterna. I detta hänseende uppstår också frågan om ägande-/förfoganderätten till den elektroniskt externt lagrade informationen. Eller annorlunda uttryckt; om sådan information med åberopande av advokatsekretess är skyddad mot annans åtkomst – genom processuella tvångsåtgärder el. dyl. – trots att den fysiskt befinner sig utanför advokatkontorets väggar.

Advokatbyråers möjlighet att använda sig av olika externa IT- och webbaserade lösningar inom ramen för sin verksamhet har aktualiserats allt mer och allt eftersom den IT-tekniska utvecklingen gått framåt. Frågan om vilka IT-lösningar som är tillåtna utanför advokatbyråns egna väggar, rymmer alltså en rad frågeställningar av såväl juridisk/regulatorisk som teknisk natur.

Externa lösningar i form av s.k. *IT-hosting*, *webbhotell* och användandet av molntjänster och andra system, måste i första hand alltid bedömas i förhållande till det etiska regelverk som omgärdar advokatverksamheten. Användande av externa tjänster som innebär att advokatens data transporteras och lagras externt – ofta i andra länder – innebär alltså att advokaten måste analysera vad detta innebär, bland annat i fråga om tystnadsplikt, skydd mot tvångsåtgärder av såväl straffprocessuell som civilrättslig natur, liksom frågor kring arkivering och utlämnande av handlingar.

3.2 Den tekniska utvecklingen

Många advokatbyråer har länge använt sig av IT-lösningar som på olika sätt aktualiserat risker för obehörig åtkomst till information, t.ex. användning av okrypterad e-post för känslig information och olika former av outsourcing, där utomstående hanterat advokatens klientinformation.

På senare tid har den tekniska utvecklingen inneburit att dessa frågor blivit än mer aktuella, därav behovet av att nu analysera om, och i så fall på vilket sätt, de regler som gäller för advokater begränsar deras möjligheter att utnyttja vissa IT-lösningar.

En sådan teknisk utveckling är att även advokater i ökande utsträckning använder lösningar som medger fjärråtkomst av information, dvs. möjligheten att utanför kontoret komma åt i princip samma information som om man befann sig på kontoret. Mobilt bredband, uppkoppling via *WiFi*, etc. är ett par exempel på teknik som medger åtkomst till nätverk, där stora mängder information skickas fram och tillbaka på ett ofta oskyddat sätt, trots att det finns allmänt tillgängliga tekniska lösningar för att skydda sådan information, t.ex. genom kryptering.

Ett exempel på teknik som etablerat sig väl och fortsätter att påverka användningen av IT är alltså olika typer av molntjänster. Förenklat kan nämnas att molntjänster

- innebär möjligheter till billigare, mer flexibel och mer kraftfull datahantering,
- bygger på att processorkraft, lagring eller funktioner tillhandahålls som tjänster på *internet* till användare som inte behöver ha teknisk kunskap eller kontroll över infrastrukturen; advokatens data behandlas således utanför kontoret,
- är en variant av *outsourcing* – någon annan sköter, oftast automatiserat, den elektroniska datan eller delar därav, samt
- är möjliga genom billig tillgång till ökad bandbredd för kommunikation och lagrings- och processorkapacitet i stora datacenter.

Det förekommer en mängd förkortningar för att beskriva olika molntjänster[14].

[14] Exempelvis ”SaaS” (*Software as a Service*), ”PaaS” (*Platform as a Service*) samt ”IaaS” (*Infrastructure as a Service*).

Produkter och tjänster som innebär nya möjligheter även för advokatbyråer utvecklas i snabb takt. Nya affärsmodeller innebär att man kan slippa stora initiala investeringar och i stället genom ett särskilt abonnemang eller prenumeration betala periodvis för den faktiska användningen av datorkraft eller programvaror, något som är intressant för advokatbyråer oavsett storlek och verksamhetsinriktning. Det mesta av en advokatbyrås IT-stöd kan idag köpas som tjänster genom uppkoppling mot *internet* och dagens rutiner kommer att förändras ytterligare till följd av nya tekniska möjligheter. Det kan handla om olika typer av program för kontorsstöd, såsom ordbehandling, kalkyl, e-post, tidredovisning, liksom elektronisk lagring av akter och annan information och bokföring, m.m. En konsekvens av detta är att även en liten advokatbyrå, utan stora initiala investeringar, kan skaffa sig tillgång till moderna och säkra IT-lösningar.

3.3 Exempel på nödvändiga överväganden

Den ovan beskrivna tekniska utvecklingen innebär att många advokatbyråer som använder molntjänster och liknande IT-lösningar, i viss mening helt eller delvis avhänder sig kontrollen över information som genereras av advokatbyrån eller på annat sätt har anknytning till advokatbyråns verksamhet, vilket i sin tur innebär att advokatbyrån måste överväga hur de yrkesplikter som gäller för advokater ska kunna efterlevas.

Nedan ges ett antal exempel på frågeställningar som behöver beaktas i samband med att advokatbyrån anlitar utomstående IT-leverantörer eller skaffar IT-lösningar som innebär att information hanteras eller lagras utanför advokatbyrån, utöver mer sedvanliga kommersiella frågeställningar som t.ex. tjänstens funktionalitet (egenskaper) och tillgänglighet med anknytande servicenivågarantier och prestanda. Uppräkningen är inte uttömmande. Beroende på svaret på respektive fråga kan området ifråga innebära ett problem i förhållande till tillämpliga regelverk.

1. **Hur ser skyddet mot externa angrepp ut?**

Hur bedöms risken för obehörig åtkomst till information? Intrång från så kallade hackers kan vara en sådan typ av risk. En annan risk kan vara s.k. överbelastningsattacker eller ”DDoS” (*Distributed Denial of Service*) attacker. Ännu ett exempel på risker är s.k. *Ransomware*, som innebär att advokatbyråns datorer infekteras med ett virus som låser/krypterar information som bara blir åtkomlig igen om betalning erläggs. Angriparnas avsikt är att hindra kunder och användare att få tillgång till tjänster som IT-leverantören tillhandahåller (på *internet*).

2. **Hur ser leverantörens skydd mot interna angrepp ut?**

Först måste givetvis advokatbyrån se över förhållandena för sin egen personal och verksamhet. Upprättande av sekretessförbindelser i anknytning till anställningsavtal och av personalen kvitterad policy avseende den egna verksamheten är ett måste. Vidare kan utöver brandväggar mot omvärlden olika typer av interna ”skott” läggas upp, så att alla medarbetare inte har tillgång till andra ärenden än de som det finns verksamhetsmässig anledning att ha tillgång till. Leverantörer och deras anställda utgör också en typ av risk. Har leverantören erforderliga rutiner för att säkerställa att enbart sådana anställda som behöver tillgång till information för att kunna utföra sina uppgifter har tillgång till informationen? Är berörd personal genom sekretessavtal eller på annat sätt informerad om sekretesskrav, insiderlagstiftning och liknande regler? Ofta har leverantörerna avtal med sina anställda som på ett adekvat sätt reglerar dessa frågor, liksom rutiner som säkerställer att endast behöriga personer har absolut nödvändig åtkomst till information. Det är dock viktigt att verifiera att så är fallet även med den dataleverantör som advokatbyrån avser att anlita. Enligt uppgift innebär rutinerna hos de större välkända leverantörerna att det endast i extrema undantagsfall blir aktuellt att kunna ha sådan åtkomst till data att data kan läsas i klartext. Flera av dessa leverantörer brukar låta någon av de stora revisionsbyråerna verifiera att säkerhetsrutinerna är tillfyllest och upprätthålls.

3. **Vet advokaten säkert var informationen lagras?**

I vissa länder kan exempelvis myndigheter ta sig rätten att kräva tillgång till information på ett sätt som vi inte är vana vid. En annan aspekt på lagring utomlands är att lagstiftningen avseende personuppgifter ställer krav på om personuppgifter ska överföras till och/eller lagras utanför EES (se ovan 2.4).

4. **Hanterar leverantören personuppgifter?**

Om leverantören hanterar personuppgifter måste det finnas en tydlig, skriftlig, reglering av leverantörens ansvar som personuppgiftsbiträde.

5. **Har leverantören erforderliga rutiner för att säkerställa att advokatens data inte försvinner?**

Här måste kontrolleras vilka säkerhetsarrangemang och metoder som tillämpas. Förvaras advokatbyråns information på olika servrar på olika orter (s.k. distribuerad säkerhet) och tas i förekommande fall t ex. backup av kundens data, måste det finnas tydliga rutiner för backup-tagningen.

6. **Regleras det i avtalet vem som äger advokatens data?**

Det måste tydligt regleras i avtal att advokatbyrån äger den data som enligt uppdraget ska lagras externt. Äganderätten ska då lämpligen även omfatta s.k. metadata (data om data) och trafikdata (in- och utloggning).

7. **Finns en tillräckligt snabb och smidig tillgång till data, under löpande avtalsperiod respektive när avtalet upphör?**

Detta måste uppmärksammas. Även obeståndssituationer bör beaktas.

8. **Lagras data i ett format som utan konverteringsåtgärder kan användas av andra leverantörer?**

Om så inte är fallet, kan det i praktiken bli en inlåsningseffekt, som gör det svårt att byta leverantör.

9. **Behövs medgivande från klienter för att använda IT-lösningen ifråga och i vilken utsträckning bör klienten i övrigt informeras om byråns IT-lösning?**

Erforderliga kontroller och bedömningar måste göras. I vissa fall kan det vara lämpligt att klienten informeras om advokatbyråns användande av externa IT-tjänster t.ex. genom att information härom tas in i uppdragsavtalet med klienten. Rör det sig om behandling av särskilt känslig klientinformation kan det i vissa fall till och med finnas anledning att inhämta klientens samtycke till den externa databehandlingen.

10. **Sker överföring av information på ett säkert sätt?**

Tillräcklig kryptering eller annan lösning som ger motsvarande skydd bör användas vid all överföring av känslig information.

11. **Finns tydlig reglering av hur leverantören ska agera om myndigheter begär att information härstammande från advokatbyrån ska lämnas ut?**

Överväganden måste göras om vad som händer med data om brottsbekämpande myndigheter skulle begära ut information och t.o.m. göra husrannsakan och ta lagrad information i beslag (se ovan avsnitt 2.4 punkterna 8 och 9).

12. Använder sig leverantören av samma servrar för flera kunder?

I så fall måste överväganden även göras (se ovan 11) i fråga om andra kunders data ligger på samma server och om det finns risk för att advokatbyråns data skulle kunna omfattas av straffprocessuella åtgärder avseende annan kund till den externa leverantören och hur detta skulle kunna påverka advokatbyråns löpande verksamhet.

Överväganden i fråga om GDPR:

I det följande sammanfattas några av de problem- eller frågeställningar som föranleds av det nya regelverket i GDPR. En mer komplett analys och beskrivning återfinns i Dataskyddsvägledningen, där det även finns mallar och checklistor som underlättar förståelsen för och tillämpningen av GDPR.

a) Säkerställ att leverantörens roll som personuppgiftsbiträde är klar genom avtalet och att leverantören inte har någon rätt att för egen räkning använda advokatens data, vilket inte är ovanligt, t.ex. i samband med olika gratistjänster, i syfte t.ex. att profilera användaren för marknadsföring.

b) Säkerställ att leverantören endast använder advokatbyråns data enligt byråns dokumenterade instruktioner.

c) Säkerställ att leverantörens personal som kommer i kontakt med advokatbyråns data har gjort en lämplig form av sekretessåtagande, jfr ovan.

d) Klargör att leverantören måste inhämta advokatbyråns samtycke i de fall underleverantörer ska engageras för behandling av kundens data.

e) Leverantören måste också ha erforderliga rapport- och säkerhetssystem på plats och mekanismer och funktionalitet för att bereda advokatbyrån

möjlighet att i sin tur i tid underrätta vederbörande tillsynsmyndighet om incidenter.[15] Leverantören måste vidare göra åtaganden om att assistera advokatbyrån vad gäller tillgodoseendet av registrerades rättigheter enligt GDPR, bl.a. rätten att bli ”glömd”, rätten till portabilitet[16] samt rätten att behandlingen ska begränsas.

f) Advokatbyrån bör analysera vilka risker som kan finnas i förhållande till GDPR utifrån den verksamhet advokatbyrån bedriver och den typ av tjänst leverantören tillhandahåller. Såsom framgår av Dataskyddsvägledningen är det en stor skillnad mellan GDPR och tidigare gällande reglering när det gäller omfattningen av och nivån på sanktionsavgifter (offentligrättslig påföljd som tillfaller staten) och skadestånd (individuellt utkrävt ansvar som riktar sig mot den personuppgiftsansvarige och/eller personuppgiftsbiträdet, i förhållande till deras respektive brott mot bestämmelserna i GDPR). Det ska här särskilt noteras att det finns viss osäkerhet vad gäller fördelningen av ansvaret enligt GDPR mellan en leverantör (personuppgiftsbiträde) och den som anlitar leverantören (personuppgiftsansvarig), bl.a. vad gäller regressrätt och eventuellt solidariskt ansvar för skadestånd. Om advokatbyråns verksamhet innefattar omfattande hantering av personuppgifter, är det därför viktigt att sätta sig in i såväl GDPR:s reglering i dessa avseenden som de villkor som leverantören tillämpar (där man i standardavtal t.ex. ofta försöker begränsa regressrätten). Det skulle föra för långt att här gå in på detaljer om just dessa frågeställningar.

[15] Se Dataskyddsvägledningen (avsnitt 1.3).
[16] I korta drag innebär detta att den som lämnat sina personuppgifter till ett företag, under vissa förutsättningar, har rätt att få ut och överföra sina personuppgifter till ett annat, konkurrerande företag. Se Datainspektionens särskilda riktlinjer om rätten till dataportabilitet.

4. Reglering med bäring på IT-tjänster vid advokatverksamhet

4.1 Avsaknad av specifik reglering av IT-tjänster vid advokatverksamhet

Det etiska regelverket innehåller inga uttryckliga bestämmelser som tar sikte på IT-frågor. Advokatsamfundet har i huvudsak inte heller i övrigt utfärdat några vägledande uttalanden eller rekommendationer i dessa frågor – utöver tidigare vägledning om användningen av externa IT-tjänster från år 2011 – och de allmänna rekommendationer som i oktober 2004 lämnats i promemorian *E-post och annan digital teknik i advokatverksamhet – några punkter att tänka på* (cirkulär nr 22/2004) samt tidigare nämnda Dataskyddsvägledning och Advokatsamfundets integritetspolicy.[17]

Den huvudsakliga avsaknaden av uttrycklig reglering i fråga om IT-tjänster är inte unikt för Sverige, utan gäller även i flertalet övriga europeiska länder (se avsnitt 6) och hänger bland annat samman med att det är fråga om användning av teknik som är under kontinuerlig och snabb utveckling och som hela tiden förändrar förutsättningarna för användandet av elektronisk information inom advokatverksamheten. En annan orsak är självfallet utgångspunkten att det regelverk som omgärdar advokatverksamheten är teknikneutral och att yrkesplikterna ska upprätthållas oavsett om dessa tar sikte på information som finns i traditionell skriftlig form eller i elektronisk form.

4.2 Allmänt om advokatens plikter med bäring på IT-användning

Plikter som åvilar en advokat framgår av rättegångsbalken (RB), Stadgar för Sveriges advokatsamfund, Vägledande regler om god advokatsed (VRGA) och den europeiska advokatorganisationen CCBE:s etiska regler *Code of Conduct for*

[17] Inte heller i annan författning eller för andra till advokater jämförbara verksamhetsutövare finns någon uttrycklig reglering kring denna typ av frågor. De tidigare av Datainspektionen utfärdade föreskrifterna för uppdragsregister inom advokatverksamhet (DIFS 1996:5), vari bl.a. angavs att överföring av personuppgifter inom ramen för advokatverksamhet inte får ske utan att uppgifterna är krypterade, är sedan länge upphävda (DIFS 1998:1).

European Lawyers, vilka är tillämpliga och bindande för svenska advokater vid gränsöverskridande verksamhet, samt i viss annan författning. Vidare utvecklas innebörden av god advokatsed genom vägledande uttalanden av styrelsen och genom disciplinnämndens avgöranden.

Den allmänna bestämmelsen om advokats skyldigheter finns i 8 kap. 4 § RB. Av denna följer att en advokat i sin verksamhet redbart och nitiskt ska utföra de uppdrag som anförtrotts honom och iaktta god advokatsed. Motsvarande bestämmelse finns även i 34 § Stadgar för Sveriges advokatsamfund. Advokatens roll och främsta skyldigheter utvecklas ytterligare i 1 VRGA.

Vad angår advokatens roll och främsta skyldigheter kan särskilt framhållas att det i 1 VRGA bl.a. framgår att en advokat ska uppträda sakligt och korrekt samt så att förtroendet för advokatkåren upprätthålls.

Enligt 2.1.1 VRGA ska en advokat utföra ett uppdrag med omsorg, noggrannhet och tillbörlig skyndsamhet. Advokaten ska se till att klienten inte förorsakas onödiga kostnader. Bakgrunden till denna regel är bland annat att det i alla sammanhang bör vara omsorgen om klienten som sätts i förgrunden.

I 2.2 VRGA regleras den så viktiga tystnads- och diskretionsplikten. Enligt 2.2.1 har en advokat tystnadsplikt avseende det som anförtrotts advokaten inom ramen för advokatverksamheten, eller som advokaten i samband därmed fått kännedom om. Undantag från tystnadsplikten gäller i vissa särskilt angivna fall. I fråga om tystnadsplikten är det advokatverksamheten som utgör ramen för tystnadsplikten. Verksamheten är en vidare ram än uppdraget och innebär exempelvis att även information som advokaten får från en presumtiv klient, där något uppdrag ännu inte föreligger, kan omfattas av tystnadsplikten.

Enligt 2.2.2 VRGA är en advokat skyldig att iaktta diskretion om sina klienters angelägenheter. En advokat får inte utan skäl göra sig underrättad om ärenden som förekommer på den byrå där advokaten är verksam, men som advokaten inte

själv arbetar med. Den preciserade diskretionsplikten avser att förbjuda ”snokande” i ärenden som advokaten inte själv arbetar med. Däremot är regeln inte avsedd att träffa de många situationer där det föreligger ett godtagbart skäl för advokaten att i sin professionella verksamhet ta reda på uppgifter rörande en klient eller uppgifter i ett ärende som advokaten själv inte arbetar med. Enligt 2.2.3 VRGA är en advokat skyldig att ålägga sin personal samma tystnadsplikt och diskretionsplikt som gäller för advokaten själv.

I 2.3 VRGA regleras vad som gäller i fråga om information till klienten och här anges att klienten ska hållas underrättad om vad som förekommer vid utförandet av uppdraget och att frågor från klienten om uppdraget ska besvaras skyndsamt.

Enligt 6.2.2 VRGA får en advokat inte medverka till att bevis undertrycks eller förvanskas. Vidare föreskrivs att en advokat dock inte är skyldig att förete eller åberopa bevis eller lämna uppgift som talar till klientens nackdel, om det inte finns en laglig skyldighet för advokaten att göra detta.

I 7.3 VRGA regleras hur en advokat ska organisera sin kontorsverksamhet. Enligt 7.3.1 är en advokat skyldig att se till att kontorsorganisationen är i god ordning och har en för verksamheten anpassad utrustning och bemanning samt att alla klientuppdrag bevakas. En väl fungerande kontorsorganisation är normalt en förutsättning för att klientintresset ska kunna bevakas på bästa sätt. Det åligger därför advokaten att skaffa sig sådan bemanning och utrustning att advokaten på bästa sätt kan tillvarata klienternas intressen.

I 7.11 VRGA finns en bestämmelse som tar sikte på tillhandahållande av kännetecken åt annan. Enligt denna regel får en advokat inte tillåta att annan använder brevpapper eller kännetecken på sätt som oriktigt förmedlar intrycket av att advokaten och dennes verksamhet är avsändare, har skapat dokumentet eller på annat sätt ansvarar för dess innehåll. Regeln innebär inte att advokaten till exempel är förhindrad att skicka olåsta Word-dokument till klienten. Advokaten får

dock inte tillåta klienten att ändra i dokumenten och därefter presentera dem som om de kom från advokaten.

I 7.12 VRGA regleras frågor om utlämnande och arkivering av handlingar. Enligt 7.12.1 VRGA ska advokaten, när ett uppdrag slutförts eller på annat sätt upphört, utan dröjsmål till klienten lämna ut sådana handlingar som tillhör denne om inte klienten särskilt begär att handlingar fortsatt ska förvaras av advokaten och denne accepterar detta. I 7.12.2 VRGA stadgas att en advokat är skyldig att i original eller kopia arkivera de handlingar som ansamlats under utförandet av ett uppdrag. Detta gäller dock inte dubbletter, tryckta handlingar och liknande material som utan större svårigheter kan tas fram från annat håll. Arkivhållning ska ske under tio år eller den längre tid som uppdragets natur påkallar. Handlingar, andra än klienten tillhöriga originalhandlingar, får arkiveras i form av fotografiska eller elektroniska kopior.

4.3 Advokatens tystnadsplikt och skyddet mot tvångsåtgärder

Externa IT-lösningar aktualiserar naturligt frågan om skyddet för de uppgifter som inom ramen för advokatverksamheten förvaras utanför advokatbyråns egna väggar. Det är dock svårt att entydigt och säkert säga var skyddet för elektroniskt lagrad information går, oavsett om informationen finns på själva advokatkontoret i egna dataservrar etc. eller lagrade på dataservrar hos externa IT-leverantörer.

Utgångspunkterna för skyddet av elektroniskt lagrad klientinformation är lagbestämmelserna om tystnadsplikt, vittnesplikt och frågeförbud för advokater, beslagförbudsregleringens och editionspliktens omfattning, liksom det förhållandet – såsom slagits fast i praxis och rättstillämpningen i övrigt (t.ex. i beslut av JO och JK) – att elektroniskt lagrad information får anses vara att jämställa med skriftliga handlingar. Till detta kommer sedan en bedömning av vilket skydd som gäller för verksamhetsinformation som finns elektroniskt lagrad utanför advokatbyråerna.

4.3.1 Utgångspunkterna för advokatens tystnadsplikt

Att människor i förtroende ska kunna vända sig till advokat och vara garanterade att vad de anförtror advokaten – skriftligen eller muntligen – inte kommer till utomståendes kännedom är en grundval i en demokratisk rättsstat. Skälen är flera. För att rättsutredningar och processer ska kunna bygga på ett riktigt material måste advokaten erhålla fullständiga uppgifter från klienten. Det kan endast bli fallet om klienten är övertygad om att vad han anförtror advokaten inte förs vidare utan klientens medgivande. Också mera allmänt har det ansetts vara av vikt att människor i förtroende ska kunna diskutera och redovisa sina personliga och ekonomiska angelägenheter med advokater.

Principerna om konfidentialitet och lojalitet utgör hörnstenar i de vägledande reglerna om god advokatsed. En advokats främsta plikt är att visa trohet och lojalitet gentemot klienten. En advokat har tystnadsplikt avseende det som anförtrotts advokaten inom ramen för advokatverksamheten, om inte klienten samtyckt till att information får lämnas ut. Advokatens tystnadsplikt omfattar även klientens identitet.[18]

4.3.2 Skydd mot straffprocessuella tvångsmedel

Av 27 kap. 1 § första stycket RB, följer bl.a. att föremål som skäligen kan antas ha betydelse för utredning om brott får tas i beslag. I bestämmelsens andra stycke anges att vad som sägs om föremål också – om inte annat är särskilt föreskrivet – gäller om skriftliga handlingar.

I 27 kap. 2 § RB regleras det s.k. beslagsförbudet. I denna bestämmelse anges att beslag får inte läggas på sådan skriftlig handling vars innehåll kan antas vara så-

[18] Se Advokatsamfundets vägledning om advokatens tystnadsplikt från september 2012 (cirkulär nr 15/2012). Se även t.ex. vägledande uttalanden den 15 oktober 2010 angående advokats lagliga skyldighet att till Skatteverket ange klientens VAT-nummer (cirkulär nr 18/2010) samt den 13 november 2009 angående advokats skyldighet att uppge referenser vid upphandling (cirkulär nr 25/2009) samt vägledande uttalande den 20 juni 2013 angående omfattningen av advokatens tystnadsplikt m.m. (cirkulär nr 21/2013).

dant att befattningshavare eller annan som avses i 36 kap. 5 § RB inte får höras som vittne om.

Av 36 kap. 5 § andra stycket RB framgår att advokater får höras som vittnen om något som i denna deras yrkesutövning har anförtrotts dem eller som de i samband därmed har erfarit, endast om det är medgivet i lag eller den, till vars förmån tystnadsplikten gäller, samtycker till det. Vidare stadgas i tredje stycket att ett rättegångsombud, biträden eller försvarare får höras som vittnen om vad som anförtrotts dem för uppdragets fullgörande endast om parten medger det. Detta gäller oavsett om ombudet är advokat eller inte och omfattar även vad huvudmannen i angivet syfte meddelat ombudet innan denne åtog sig uppdraget (se NJA II 1943 s. 468). I fråga om advokater och deras biträden, dock ej försvarare, gäller enligt bestämmelsens fjärde stycke alltid en skyldighet att vittna i mål angående brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år (den s.k. genombrottsregeln). Beträffande försvarare gäller således ett orubbligt frågeförbud och en försvarare kan därmed aldrig tvingas vittna rörande sådan information som anges i bestämmelsens andra stycke.

Utgångspunkten är alltså att en advokat inte får höras som vittne angående omständigheter som advokaten anförtrotts i sin yrkesutövning enligt 36 kap. 5 § andra stycket RB. Inte heller en handling som innehåller sådan information får, om den innehas av advokaten eller klienten, tas i beslag enligt 27 kap. 2 § RB. Av bestämmelsen i 27 kap. 2 § första meningen RB framgår att skriftliga handlingar inte får tas i beslag om de kan antas innehålla uppgifter som exempelvis en advokat med stöd av 36 kap. 5 § RB inte kan höras som vittne om.

Detta innebär att allt som advokaten erfarit som ett resultat av skyddad kommunikation omfattas av denna reglering. Allt som klienten har uppgett i förtroende till advokaten och de intryck och den information som advokaten har fått med anledning av sitt uppdrag omfattas av det s.k. frågeförbudet i 36 kap. 5 § RB.

I bestämmelsen om beslagsförbud i 27 kap. 2 § RB finns enbart en hänvisning till frågeförbudet i 36 kap. 5 § RB. Bestämmelsen innehåller inte någon beskrivning av vilka skriftliga meddelanden som är undantagna från beslag. Reglerna om beslag i 27 kap. RB tar vidare sikte på fysiska föremål. Den särskilda bestämmelsen i 1 § andra stycket tillkom, eftersom det vid beslag av handlingar normalt inte är handlingen som sådan, utan den information handlingen innehåller, som är av intresse för brottsutredningen. På samma sätt kan man beträffande dataservrar, mobiltelefoner och andra bärare av elektronisk information, som ju i och för sig är ett föremål, säga att det som regel inte är föremålet som sådant utan den information som detta innehåller som är av intresse för brottsutredningen. Någon lagreglering som uttryckligt tar sikte på information i elektronisk form finns emellertid inte (dock finns prejudikat och andra auktoriserade uttalanden, se nedan).

I praxis finns ett antal avgöranden som behandlar beslagsförbudet när det gäller advokater. I rättsfallet NJA 1977 s. 403 prövades frågan om vilken sorts handlingar som omfattas av beslagsförbudet. Högsta domstolen (HD) ansåg här sammanfattningsvis att beslagsförbudsregeln får anses gälla skriftliga handlingar utan begränsning. HD uttalade att det – särskilt eftersom det var fråga om skydd för enskild mot tvångsingripande från det allmännas sida – möta hinder att tillämpa bestämmelsen i 27 kap. 2 § RB i strid med dess ordalydelse. HD uttalade även att regeln måste antas ha kommit att bli betydligt vidsträcktare än som föranleds av ändamålet att tillgodose behovet av sekretess i förhållandet mellan advokat och klient.

I NJA 1990 s. 537 hade vissa handlingar rörande ett aktiebolag tagits i beslag i en advokatbyrås lokaler. När det gällde frågan vilket stöd domstolen borde kräva för en advokats påstående att hinder för beslag föreligger, uttalade Högsta domstolen att det måste anses tillräckligt med ett blygsamt mått av bevisning för att visa att något har anförtrotts en advokat i dennes yrkesutövning (jfr även RH 1996:121). Detta för att inte advokatsekretessen skulle bli alltför urholkad. Sammantaget

fann Högsta domstolen att handlingarna var skyddade mot beslag enligt 27 kap. 2 § RB.[19]

I NJA 2010 s. 122 har HD återigen prövat frågan om beslagsförbud av handlingar som förvarats i en advokatbyrås lokaler. En advokat som var delägare i byrån var misstänkt för bl.a. grovt skattebrott. Enligt HD hade dock detta inte någon betydelse för skyddet mot beslag på advokatkontoret, eftersom beslagsförbudet är avsett att skydda klientens intressen. Detta befogade intresse behövde enligt HD inte vara mindre av det skälet att advokaten är misstänkt för brott. HD upphävde beslagen.[20]

Även Regeringsrätten (idag Högsta förvaltningsdomstolen), har i två avgöranden prövat begränsningen i advokaters vittnesplikt enligt 36 kap. 5 § RB när det gäller utlämnande av handlingar och uppgifter i skatteärenden (RÅ 2001 ref. 67 I och II). Domstolen har intagit samma ståndpunkt som HD i fråga om tillämpningen av beslagsförbudet.

Som framgått är beslagsförbudsregeln i 27 kap. 2 § RB enligt sin ordalydelse direkt tillämplig endast på skriftliga handlingar. Även om lagen i sig inte ger någon ledning i fråga om omfattningen av beslagsförbudsreglerna i förhållande till elektroniskt lagrad information och elektroniska handlingar, har emellertid beträffande just beslagsregleringens tillämpning på annat än skriftliga handlingar, Justitieombudsmannen (JO) och Justitiekanslern (JK) uttalat att starka skäl talar för att i

[19] Den omständigheten att en handling är lagrad elektroniskt hindrar i och för sig inte att den kan bli föremål för edition (se NJA 1998 s. 829 samt nedan avsnitt 4.3.3).

[20] Enligt HD uteslöt inte klientförhållandet att vissa handlingar ändå skulle kunna tas i beslag, om de inte kunde anses ha lämnats i förtroende. I det aktuella målet hade dock inte presenterats något underlag för att det skulle finnas anledning att göra skillnad på de olika handlingar som tagits i beslag. Riksåklagaren hade invänt att beslagsförbudet inte var tillämpligt eftersom advokaten i detta fall själv var misstänkt för brott och därmed inte kunde höras som vittne enligt 36 kap. 5 § RB. Liksom i 1990 års fall, där en liknande invändning gjordes, ansåg dock HD att detta inte hade någon betydelse, eftersom beslagsförbudet är avsett att skydda klientens intressen. Detta befogade intresse behöver enligt HD inte vara mindre av det skälet att advokaten är misstänkt för brott. HD anmärkte dock att för det fall hela syftet bakom ett samarbete mellan en advokat och hans uppdragsgivare skulle vara brottsligt eller enbart bestå i att advokatens aktiva medverkan ska dölja ett brott, det som regel inte kan anses vara fråga om sådan yrkesutövning som anges i 36 kap. 5 § RB. Underlag för att göra en sådan bedömning fanns enligt HD inte i det aktuella fallet och HD upphävde därför beslagen.

beslagsförbudssammanhang hantera elektroniska handlingar på samma sätt som skriftliga handlingar.

I beslut den 22 december 2010 (dnr 140-2010) konstaterar JO att beslagsreglerna i RB i och för sig tar sikte på fysiska föremål och att uttrycklig reglering som tar sikte på information i elektronisk form saknas. JO ansåg dock – i likhet med vad som framhölls i JO 2009/10 s. 80[21] liksom av JK i två beslut år 2007[22] – att starka skäl talar för att behandla elektroniskt lagrad information på samma sätt som man skulle ha behandlat informationen om den hade återfunnits i en skriftlig handling.

Av betydelse i sammanhanget är vidare att det t.ex. av NJA 1977 s. 403 framgår att förbudet mot beslag enligt 27 kap. 2 § 1 RB inte är begränsat till handlingar som är att betrakta som meddelanden från klienten till advokaten eller i allt fall har upprättats i samband med och föranletts av klientens kontakt med advokaten. I stället omfattar beslagsförbudet i princip varje skriftlig handling som anförtrotts en advokat inom ramen för dennes yrkesutövning (se också bl.a. NJA 2010 s. 122). Detta slås också fast i ovan angivna JO-beslut från 2010.

Advokatsamfundet har i olika sammanhang framfört ståndpunkten att det är korrekt att beslagsförbudet beträffande handlingar (inklusive elektroniska textmeddelanden) som anförtros en advokat inom ramen för dennes yrkesutövning gäller oavsett när handlingen upprättats. Det har alltså ingen betydelse att handlingarna upprättats i tiden före det att ett visst uppdrag för advokaten har uppstått (t.ex. såsom förordnande av domstol som någon form av rättsligt biträde).

---

[21] I det ärendet gällde beslaget en brottsmisstänkt persons dator i vilken lagrats bl.a. e-post-korrespondens mellan honom och hans f.d. hustru (se 27 kap. 2 § 2 RB angående beslagsförbud på skriftliga meddelanden mellan närstående). Beslaget gjordes hos den misstänkte, dvs. datorns ägare. Se även JO:s beslut 2008-12-04 dnr 2138-2007, vilket utförligt beskrivs i SOU 2011:45 s. 293 ff.
[22] Justitiekanslerns beslut den 19 december 2007, dnr 6372-07-31 och 6373-07-31. Dessa beslut rörde frågor som aktualiserades i samband med ett beslag av en dator hos en person med anknytning till ett medieföretag. Justitiekanslern ansåg bl.a. att förutsättningarna för genomsökande av en dator tillhörande någon inom den skyddade krets som avses i 27 kap. 2 § RB bör författningsregleras. Se om dessa JK-beslut även i SOU 2011:45 s. 293.

Advokatsamfundet har också i olika sammanhang framfört uppfattningen att elektroniska handlingar såsom elektroniskt lagrad information i exempelvis dataservrar, i mobiltelefoner o. dyl. är att jämställa med vanliga handlingar i pappersform och att beslagsförbudsbestämmelserna därför får anses vara tillämpliga även på elektroniska handlingar.

JO har ansett att det i vissa fall måste vara tillåtet att ta bäraren av information, t.ex. en dator eller mobiltelefon, i beslag även om den innehåller skyddad information som omfattas av beslagsförbudet. JO anser att det är en sak att som i JO 2009/10 s. 80, ta en informationsbärare i beslag hos en misstänkt för att utröna om den innehåller information som omfattas av ett beslagsförbud för visst slag av kommunikation. Enligt JO är det något helt annat att ta själva informationsbäraren i beslag hos en försvarare som anförtrotts denne eller snarare dess innehåll. I en sådan situation omfattas enligt JO beslagsförbudet samtlig information som klienten anförtrott sin försvarare. JO har därför ansett att all den information som fanns elektroniskt lagrad i en mobiltelefon som fanns i en försvarsadvokats besittning omfattades av beslagsförbudet (inte endast text-meddelanden, utan även t.ex. uppgifter om när meddelanden och samtal ägt rum).

Advokatsamfundet har instämt i denna JO:s bedömning. Skulle bärare av information kunna beslagtas hos en advokat, trots att den innehåller skyddad information som anförtrotts advokaten, skulle detta i praktiken innebära att även skyddad information ofrånkomligt löper avsevärd risk att röjas. Här är Högsta domstolens uttalande om att det ska räcka med blygsamt mått av bevisning kring ett påstående om att en dator innehåller skyddad information för att den inte ska kunna tas i beslag av största vikt (NJA 1990 s. 537). Det är i praktiken omöjligt att sålla bort eller bortse ifrån information som uppenbarligen är skyddad. Även om sådan information givetvis inte ska få användas som bevisning, skulle det innebära en urgröpning av hela intresset och syftet med skyddad information, sekretess och förtrolighet mellan klient och advokat.

Frågan om behovet av att anpassa husrannsakans- och beslagsreglerna som en följd av den tekniska utvecklingen har dock länge varit föremål för diskussion i en mängd utredningar tillsatta av regeringen, liksom överväganden på regeringskansliet.[23] Dessa utredningar har dock inte föranlett några lagändringar i här aktuella avseenden.[24] Även om det av JO och JK, liksom av ett antal utredningar har framhållits att det måste vara ändamålet bakom beslagsförbudsbestämmelsen som måste avgöra dess tolkning så att även elektroniskt lagrad information av skyddsvärd karaktär skulle falla inom bestämmelsens tillämpningsområde, har rättsläget inte klarlagts förrän Högsta domstolens avgörande i frågan den 18 augusti 2015.

I rättsfallet **NJA 2015 s. 631** klargjordes det slutligen, att förbudet mot husrannsakan och beslagsförbudet även gäller om den skyddade handlingen är lagrad i elektronisk form i en informationsbärare, såsom en dator. Trots att bestämmelsen enligt ordalydelsen tar sikte på skriftliga handlingar ansåg Högsta domstolen i detta prejudicerande avgörande att beslagsförbudet gäller för såväl information av annat slag än skrift som för andra bärare av information än papper. Även i de fall en skriftlig handling innehåller skyddad information, men det inte är den skyddade informationen som eftersöks, omfattas handlingen av beslagsförbudet. Motsvarande synsätt bör därför intas då den eftersökta informationen finns lagrad i en elektronisk fil och det kan antas att filen innehåller någon form av information som träffas av beslagsförbudet. Högsta domstolen utgick i sin tolkning från handlingsbegreppet i 2 kap. 3 § tryckfrihetsförordningen vilken omfattar så väl framställningar i skrift som sådana vilka kräver tekniska hjälpmedel för framställan. Mot bakgrund av detta konstaterade således Högsta domstolen att beslagsförbudet är analogiskt tillämpligt även på elektroniskt lagrad information. Det har härmed äntligen klargjorts i praxis att beslagsförbudsreglerna enligt gällande rätt tillämpas

[23] Se närmare rättsläget efter NJA 2015 s. 631 i Beslagsutredningens betänkande Beslag och husrannsakan – ett regelverk för dagens behov (SOU 2017:100) s. 458 ff.
[24] Under avsnitt 4.3.2 i 2011 års vägledning om externa IT-tjänster i advokatverksamhet har de utredningsarbeten som berört frågor om beslagsmöjligheter av elektroniskt lagrad information behandlats utförligt, till vilket det här hänvisas.

analogiskt på elektroniskt lagrad information.[25] Detta garanterar således den enskilde samma skydd mot brottsutredande myndigheters tillgång till integritetskänslig information i vissa handlingar oavsett i vilken form de aktuella handlingarna är upprättade.

Advokatens tystnadsplikt och omfattningen av skyddet mot beslag och andra processuella tvångsåtgärder har även prövats i flera avgöranden i Europadomstolen. I exempelvis i målet *Sommer mot Tyskland*[26] ansåg domstolen att åklagarmyndighetens granskning av en brottmålsadvokats klientmedelskonto stod i strid med artikel 8 Europakonventionen. I målet *Petri Sallinen mot Finland*[27] hade polisen gjort husrannsakan hos Sallinen, som var advokat, och beslagtagit datafiler som innehöll information om hans klienter. Europadomstolen fann att nationell lag inte gav tillräckligt skydd mot ingrepp av detta slag och fann därför att Europakonventionens artikel 8 hade kränkts. Domstolen noterade särskilt att bestämmelserna i den finska rätten var oklara avseende vilket skydd advokatsekretessen medgav och att husrannsakan och beslaget sammantaget vidtagits utan tillräckliga rättsliga garantier. Domstolen angav att avsaknaden av regler för vilka dokument som kan bli föremål för husrannsakan och beslag i förhållande till advokatsekretessen kränkte klagandens rättigheter enligt artikel 8. Det är särskilt värt att notera att Europadomstolen hänvisade till *Recommendation (Rec. 2000/21) of the Committee of Ministers* (se ovan), enligt vilken staterna ska vidta alla nödvändiga åtgärder för att tillförsäkra respekt för den konfidentiella relationen mellan advokat och klient. Europadomstolen har alltså ansett att det åligger staten – och därmed dess myndigheter – att tillse att advokatsekretessen skyddas.

[25] I målet – som rörde frågor rörande husrannsakan på en tidningsredaktion i syfte att genom beslag av en elektronisk informationsbärare få tillgång till digitala fotografier – slog HD bl.a. fast att beslagsförbudet i 27 kap. 2 § RB omfattar även annan information än skrift och andra bärare av information än papper och att om en eftersökt fil (eller annan eftersökt informationsenhet) på en elektronisk informationsbärare kan antas innehålla information som omfattas av frågeförbudet i 36 kap. 5 § RB (skyddad information), så gäller enligt beslagsförbudet ett absolut hinder mot beslag.
[26] Dom den 27 april 2017.
[27] Dom den 27 september 2005.

I december 2017 presenterade **Beslagsutredningen** en rad förslag som i vissa delar berör de frågeställningar som behandlas i denna vägledning.[28] Förslagen i betänkandet har remitterats, men tidplanen för det fortsatta lagstiftningsarbetet är enligt uppgift oklar. Det går heller inte att förutse i vilken omfattning förslagen i denna del kommer att leda till lagstiftning.

Sammantagen bedömning

Mot bakgrund av vad som nu har redovisats görs sammantaget följande bedömning i fråga om skyddet mot beslag beträffande information som finns elektroniskt lagrad utanför advokatbyrån via en extern IT-tjänst.

I avsaknad av uttrycklig reglering och med stöd av förevarande praxis görs bedömningen att dataservrar, mobiltelefoner och andra bärare av elektronisk information, med stöd av bestämmelserna i 27 kap. 2 § 1 RB, får anses vara fredat från beslag, såvida inte klienten medger att föremålet överlämnas till polis eller åklagare.[29] En advokat bör alltså i dagsläget kunna utgå ifrån att beslagsförbudsreglerna gäller även för elektroniskt lagrad information.

I avvaktan på eventuella lagstiftningsåtgärder till följd av Beslagsutredningens förslag rörande beslag av elektroniskt lagrad data får det därmed i dagsläget anses finnas ett skydd mot intrång i advokatsekret information som lagras elektroniskt på advokatbyrån med stöd av beslagsförbudsreglerna i rättegångsbalken och förevarande prejudikat (NJA 2015 s. 631 och NJA 2010 s. 122).

Arbetsgruppen gör, under samma förutsättningar, bedömningen att detsamma får anses gälla i fråga om advokatsekret information som finns på externa servrar el-

[28] Se beslagsutredningens betänkande Beslag och husrannsakan – ett regelverk för dagens behov (SOU 2017:100).
[29] Jfr t.ex. NJA 1977 s. 403, JO 1977/78 s. 19, Fitger, Rättegångsbalken, En kommentar på Internet, 28 kap. 1 § RB, och Lindberg, Straffprocessuella tvångsmedel, 2:a uppl., s. 636. Se även NJA 1981 s. 791 NJA 1990 s. 537 NJA 1992 s. 307 NJA 1998 s. 829 NJA 2003 s. 107 NJA 2010 s. 122 samt uppsatsen Beslag i IT-miljö – en dragkamp mellan integritet och effektivitet, examensarbete i processrätt vårterminen 2018 Uppsala universitet, författare Sandra Johansson.

ler i annan IT-miljö utanför advokatkontorets egna väggar. Enligt RB får handlingar som innehåller förtrolig information mellan advokat och klient inte tas i beslag (eller för den delen editeras, se nedan 4.3.3) och detta måste anses gälla oavsett var informationen fysiskt befinner sig. Vidare är det ju advokaten och advokatbyrån som faktiskt råder över och har äganderätten till informationen i databasen eller vilken extern IT-lösning det nu är fråga om. Det är därmed advokaten och inte IT-leverantören som förfogar över den elektroniskt lagrade informationen. Härtill kommer att det är klientens intresse som skyddas genom beslagsförbudsregleringen och att detta skydd inte påverkas av att informationen är lagrad elektroniskt (jfr NJA 2010 s. 122 och 2015 s. 631). Enligt svensk rätt[30] får alltså advokatsekret digital information anses åtnjuta samma sekretesskydd oavsett om informationen finns lagrad inom eller utanför advokatbyråns egna väggar.[31]

Som flera gånger påtalats bör, mot bakgrund av den osäkerhet som ändå råder i fråga om beslagsförbudets omfattning för externt lagrad elektronisk information, varje advokat vara medveten om att sådan information dock kan komma att bli föremål för tvångsåtgärder. Nogsamma överväganden bör därför göras innan känslig information anförtros en extern IT-leverantör. Detta gäller särskilt om den externa IT-leverantören är ett utomeuropeiskt bolag eller använder sig av servrar lokaliserade i ett land utanför EU som inte uppfyller de krav på dataskydd, konfidentialitet och skydd mot utlämnande av uppgifter som gäller i Sverige eller övriga EU-stater. Risken ökar då betydligt för att utlämnande av konfidentiell information kan krävas av behöriga myndigheter i det land där servrarna finns eller IT-leverantören har sin hemvist i enlighet med där gällande lagstiftning.

[30] Beroende på var den elektroniskt lagrade informationen befinner sig geografiskt bör det observeras att andra jurisdiktioner kan ha annan reglering kring sekretesskyddet.
[31] Se även nedan avsnitt 4.3.3 där samma bedömning görs i fråga om editionsplikt.

4.3.3 Civilrättsliga bevissäkrings- och säkerhetsåtgärder

Som ovan påpekats har HD i NJA 2015 s. 631 uttalat sig om tillämpningen av beslagsförbuden på datalagrad information. HD har även tolkat tillämpligheten av reglerna om edition i 38 kap. RB när det gäller sådan information. Dessa bestämmelser (2 och 4 §§) gäller, i likhet med 27 kap. 2 § RB, enligt sin ordalydelse bara skriftliga handlingar. I avgörandet NJA 1998 s. 829 har dock HD slagit fast att editionsreglerna, trots ordalydelsen, är tillämpliga även på datalagrad information.

En leverantör av IT-tjänster till en advokat eller advokatbyrå kan därmed tänkas bli föremål för civilrättsliga bevissäkrings- och säkerhetsåtgärder i form av editionsföreläggande, intrångsundersökning och förvarstagande enligt 15 kap. 3 § RB. En editionssökande har enligt 38 kap. 2 § RB rätt att ansöka om edition avseende svarandens, eller tredje parts, handlingar som kan antas äga betydelse som bevis. Av 38 kap. 2 § andra stycket RB följer att befattningshavare eller annan, som avses i 36 kap. 5 § RB (däribland advokater och deras biträden) inte är skyldiga att lämna ut handlingar om handlingens innehåll kan antas vara sådant, att advokaten inte får höras som vittne om innehållet. Befrielsen från editionsskyldighet kan således åberopas av en advokat som innehar handlingar som inte omfattas av vittnesplikten.

Om en editionssökande skulle rikta en editionsansökan mot en IT-leverantör till en advokat, oavsett om denne är part i rättegången, är frågan om IT-leverantören på samma vis som en advokat kan åberopa befrielse från editionsskyldigheten.

I doktrinen har det analyserats om tredje man som har faktisk tillgång till handlingar, såsom arkivföretag eller IT-leverantörer, kan bli föremål för editionsplikt.[32] Editionsplikten har här ansetts gälla för den som på grund av

[32] Se Vänbok till Bertil Södermark, s 218 f., där Lars Heuman i sin uppsats *Skyldighet för en part att lämna en förteckning över de skriftliga bevis han innehar*, adresserar frågeställningen. Om ett bolag är part och innehar en omfattande dokumentation kan, enligt Heuman, inte företagsledarna åläggas editionsplikt. Om parten är ett moderbolag, men ett dotterbolag har förfoganderätten över

äganderätt förfogar över handlingarna och deras innehåll. Andra personer som har tillgång till materialet ska inte kunna förfoga över dem genom att medge ett yrkande om edition.

Arbetsgruppen instämmer i denna bedömning och anser att reglerna om editionsplikt och undantagen från desamma inte bör tolkas formalistiskt, utan med beaktande av ändamålet med undantaget från vittnes- eller editionsplikten, nämligen att en advokat inte ska kunna tvingas att vittna om innehållet i sin kommunikation med klienten eller lämna ut handlingar som kommunicerats med klienten.[33] Var advokaten i en sådan situation faktiskt förvarar de elektroniska handlingarna kan inte inskränka advokatsekretessen. Det ska dock noteras att vad som sagts ovan gäller endast editionssvaranden som omfattas av svenska editionsregler. Reglerna beträffande ”*attorney–client privilege*” skiljer sig från land till land och en editionsansökan riktad mot en IT-leverantör i syfte att åtkomma advokat/klient-korrespondens eller en advokats arbetsmaterial kan, beroende på bl.a. var IT-leverantören har sitt säte eller lagrar materialet, komma att ges in i domstol i en annan jurisdiktion där reglerna om undantag från editionsplikt inte nödvändigtvis också omfattar en IT-leverantör som levererar tjänster åt en advokat.

En IT-leverantör kan vidare bli föremål för civilrättsliga skydds- och säkerhetsåtgärder enligt reglerna om intrångsundersökning i det immaterialrättsliga

---

handlingarna, kan man inte anse att moderbolaget innehar handlingarna”. Heuman finner stöd för sin uppfattning i NJA 2007 s. 309 där frågan var om en tidning som lagrade artiklar hos en annan juridisk person omfattades av den s.k. databasregeln i 1 kap 9 § YGL. Databasregeln är enligt sin lydelse endast tillämplig när en redaktion för en periodisk skrift eller för radioprogram, ett företag för yrkesmässig framställning av tryckta eller därmed enligt tryckfrihetsförordningen jämställda skrifter eller av tekniska upptagningar eller en nyhetsbyrå med hjälp av elektromagnetiska vågor på särskild begäran tillhandahåller allmänheten information ur en databas. Tredje man omfattas således inte enligt lagtexten av databasregeln. Högsta domstolen konstaterade att ”avgörande för bedömningen bör därför inte vara var databasen kan sägas vara placerad eller om databasverksamheten är förlagd till en särskild juridisk person. I stället får anses mest förenligt med de intressen som grundlagarna bygger på, inte minst intresset av att källskyddet bevaras, att den som faktiskt råder över informationen i databasen också betraktas som den som tillhandahåller den.” Tidningens artiklar ansågs därför omfattas av skyddet i yttrandefrihetsgrundlagen oaktat att tredje man lagrade materialet. Heuman menar att det finns goda skäl att göra motsvarande bedömning när det gäller parts uppgiftsskyldighet.

[33] En sådan tolkning är också mest förenlig med *Recommendation (Rec. 2000/21) of the Committee of Ministers Principle I (6),* rörande nödvändigheten av att tillförsäkra respekt för den konfidentiella relationen mellan advokat och klient.

regelverket, liksom enligt 15 kap. 3 § RB.[34] En IT-leverantör kan på motsvarande vis bli föremål för säkerhetsåtgärder i form av förvarstagande, även det enligt 15 kap. 3 § RB. En intrångsundersökning kan enbart riktas mot den som misstänks ha begått ett immaterialrättsligt intrång och får, olikt edition, inte riktas mot tredje man. En intrångsundersökning får enligt 56 f § andra stycket upphovsrättslagen inte omfatta handlingar som omfattas av beslagsförbudet i 27 kap. 2 § RB. Om en intrångsundersökning genomförs hos en leverantör av IT-tjänster till en advokat i anledning av att denne misstänks ha begått immaterialrättsligt intrång ska intrångsundersökningen inte omfatta handlingar som omfattas av beslagsförbudet.

Mot bakgrund av att Kronofogdemyndighetens verkställighet av en intrångsundersökning ofta sker skyndsamt och det material som blir föremål för verkställigheten ofta kan vara omfattande, kan det protokoll som upprättas efter intrångsundersökningen i praktiken komma att omfatta handlingar som omfattas av beslagsförbudet. När det gäller reglerna om civilrättsligt beslag (”annan åtgärd” enligt 15 kap. 3 § RB) saknas det uttryckligt undantag för handlingar som omfattas av beslagsförbudet. Arbetsgruppens uppfattning är att Kronofogdemyndigheten vid verkställighet av ett civilrättsligt beslag bör gå tillväga på samma vis som vid en intrångsundersökning och undanta handlingar som omfattas av beslagsförbudet.

Sammanfattningsvis bör en IT-leverantör som blir editionssvarande i en svensk rättegång kunna åberopa dels att handlingarna inte omfattas av editionsplikt eftersom de inte innehas av IT-leverantören med äganderätt, dels att IT-leverantören är befriad från editionsskyldigheten eftersom denne innehar handlingar för advokats/advokatbyrås räkning. Intrångsundersökningar får inte omfatta handlingar som omfattas av beslagsförbudet och vid civilrättsliga beslag bör beslagsförbudet ges motsvarande tillämpning (se ovan).

[34] Ett exempel på denna situation var när internetleverantören *Bahnhof* i egenskap av svarande blev föremål för en intrångsundersökning och det efterföljande beslaget kom att omfatta tredje mans datorfiler, se Stockholms tingsrätts beslut 2005-03-09 i mål nr T 8991-05.

5. Arkivering och utlämnandefrågor

Som ovan redovisats regleras frågor om arkivering och utlämnande av handlingar i 7.12 VRGA och som angetts gäller enligt 7.12.1 VRGA att advokaten, när ett uppdrag slutförts eller på annat sätt upphört, utan dröjsmål till klienten ska lämna ut sådana handlingar som tillhör denne om inte klienten särskilt begär att handlingar fortsatt ska förvaras av advokaten och denne accepterar detta.

Enligt 7.12. 2 VRGA är vidare en advokat skyldig att i original eller kopia arkivera de handlingar som ansamlats under utförandet av ett uppdrag. Detta gäller dock inte dubbletter, tryckta handlingar och liknande material som utan större svårigheter kan tas fram från annat håll. Arkivhållning ska ske under tio år eller den längre tid som uppdragets natur påkallar. Handlingar, andra än klienten tillhöriga originalhandlingar, får arkiveras i form av fotografiska eller elektroniska kopior. Advokatens skyldighet att hålla handlingarna arkiverade under minst tio år gäller även om klienten begär att tiden ska förkortas eller att någon handling ska förstöras tidigare. Alla meddelanden som innehåller rådgivning eller som vidarebefordrar materiell information ska sparas antingen i utskrift i för ärendet upplagd akt eller elektroniskt. Arkivering elektroniskt ska ske på ett sådant sätt att alla användare har åtkomstmöjlighet men redigering omöjliggörs.

I anslutning till denna bestämmelse har styrelsen den 28 januari 2011 (cirkulär nr 5/2011) antagit ett vägledande uttalande angående advokaters skyldighet att lämna ut handlingar i ärendet till klient m.m., där följande slogs fast. Frågan om advokats skyldighet att, sedan ett uppdrag upphört, utlämna handlingar i ärendet till klienten har besvarats av styrelsen för Sveriges advokatsamfund i ett vägledande uttalande av den 17 mars 1995. Den omständigheten att advokatens uppdrag har omfattat mer än en klient påverkar inte advokatens skyldigheter enligt detta uttalande. Inom ramen för ett pågående gemensamt uppdrag har advokaten, såvitt annat inte gemensamt överenskommits, en skyldighet att på begäran från någon av klienterna lämna ut samtliga handlingar oavsett från vem handlingarna härrör. Detta gäller även sedan uppdraget upphört. Skyldigheten

innefattar även elektroniskt sparade dokument och gäller oberoende av om någon av klienterna motsätter sig detta.

I fråga om omhändertagande och arkivering av digitalt lagrat material gör sig samma allmänna synpunkter gällande som i fråga om annat material. I den delen kan hänvisas till den rapport om arkivläggning av handlingar som utarbetades av Advokatsamfundets arkivkommitté (se TSA 1973 s. 329) och styrelsens ställningstagande till rapporten (TSA 1974 s. 85). Rapporten är något ålderstigen, men kan ändå tjäna till vägledning. I fråga om en advokats allmänna arkivhandlingar, dvs. sådana handlingar som inte till följd av bestämmelser om bokföring måste arkiveras viss tid, rekommenderades en generell arkiveringstid på tjugo år.

Skyldigheten att bevara material torde även innebära en skyldighet att ha erforderliga ”backup-rutiner” för digital information. En stöld eller brand får inte medföra att viktig klientinformation går förlorad.

Arkivering och utlämnandefrågor som omfattas av EU:s dataskyddsförordning (GDPR) behandlas, såsom tidigare sagts, utförligt i Advokatsamfundets *Vägledning för tillämpningen av EU:s dataskyddsförordning i advokatverksamhet*, till vilken hänvisas i tillämpliga delar.

Det erinras i detta sammanhang även om att särskilda förpliktelser vad gäller skyldighet att arkivera elektroniska handlingar och uppgifter samt behandla personuppgifter också kan föreligga i vissa ärenden enligt lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism (PTL).[35]

[35] Se för ytterligare information avsnitt 15 i 2017 års *Vägledning för advokater och advokatbyråer beträffande lagstiftningen om åtgärder mot penningtvätt och terroristfinansiering* (cirkulär nr 19/2017).

6. Europeisk utblick

Utöver de riktlinjer som Rådet för advokatsamfunden i Europa, CCBE, tagit fram rörande advokaters elektroniska kommunikation och användning av *internet* (vilken bilades 2011 års vägledning om externa IT-tjänster),[36] har CCBE år 2012 tagit fram en särskild vägledning om advokaters användning av externa IT-tjänster (*CCBE Guidelines on the Use of Cloud Computing Services by Lawyers*), till vilken det särskilt hänvisas. CCBE har även tagit fram vissa andra dokument som kan vara av intresse.[37]

Av den information som inhämtats från våra nordiska grannländer och några andra länder i Europa i fråga om befintliga regler, riktlinjer, rekommendationer eller annan typ av dokumentation kring användning av externa IT-tjänster (molntjänster) vid advokatverksamhet, har det framkommit att det endast i vissa länder finns sådan dokumentation.[38] Denna dokumentation har beaktats i relevanta delar vid framtagandet av de rekommendationer och överväganden som gjorts i denna vägledning.

.//.

[36] Se CCBE:s riktlinjer *Electronic Communication and the Internet* från den 24 oktober 2008.
[37] Se www.ccbe.eu och https://www.ccbe.eu/search/?id=17&tx_kesearch_pi1%5Bsword%5D=Cloud+computing&tx_kesearch_pi1%5Bpage%5D=1&tx_kesearch_pi1%5BresetFilters%5D=0&tx_kesearch_pi1%5BsortByField%5D=&tx_kesearch_pi1%5BsortByDir%5D=&x=0&y=0. CCBE har även tagit fram ett dokument om användningen av molntjänster i Europa; *CCBE Response Consultation from the European Commission concerning Trusted Cloud Europe* från den 28 maj 2014, samt en vägledning från den 20 maj 2016 rörande förbättrad IT-säkerhet för advokater mot olovlig övervakning (*CCBE Guidance on Improving the IT Security of Lawyers Against Unlawful Surveillance*).
[38] Se dokumentation från det norska advokatsamfundet; det danska advokatsamfundet; det engelska advokatsamfundet (*Law Society of England and Wales*), det skotska advokatsamfundet (*Law Society of Scotland*); samt det *tyska advokatsamfundet (Deutscher Anwaltverein – DAV)*. I Tyskland finns också uttryckliga regler om att en leverantörs anställda i samband med molntjänster måste ingå sekretessåtaganden i förhållande till uppdragsgivande advokatbyråer.