EXTERNA IT-TJÄNSTER VID ADVOKATVERKSAMHET

Till Sveriges advokatsamfunds styrelse

Genom beslut den 3 december 2010 uppdrog Advokatsamfundets styrelse åt presidiet att tillsätta en arbetsgrupp med uppdrag att närmare analysera frågan om advokats möjlighet att använda sig av olika externa IT- och webbaserade tjänster.

Den tillsatta arbetsgruppen har bestått av advokaterna Björn Gustavsson, Lars Perhard, Henrik Bengtsson 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 9 juni 2011

Björn Gustavsson Lars Perhard Henrik Bengtsson

Johan Sangborn

INNEHÅLLSFÖRTECKNING

1. Sammanfattning

Arbetsgruppen har fått i uppdrag att analysera frågan om advokaters möjligheter att inom ramen för advokatverksamheten använda sig av olika externa IT- och webbaserade tjänster, dvs. IT-lösningar som ligger utanför advokatbyråns ”egna väggar”. Arbetsgruppens överväganden och praktiska rekommendationer finns sammanfattade i avsnitt 2.

Arbetsgruppen gör sammantaget bedömningen att det inte finns något hinder mot att använda externa IT-lösningar, under förutsättning att advokatens tystnadsplikt och övriga yrkesplikter upprätthålls och efterlevs. Enligt arbetsgruppen finns det vidare 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 säkerheten. Om IT-leverantörens personal kan komma åt konfidentiella uppgifter måste deras diskretion och tystnadsplikt säkerställas, genom upprättande av sekretessavtal el. dyl. 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 och 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 överväga att informera klienten

om – och om så anses nödvändigt även inhämta klientens samtycke till – att ärenderelaterade handlingar och uppgifter hanteras genom extern IT-leverantör. 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 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.

Sammantaget kan konstateras att användningen av datateknik erbjuder advokater en möjlighet att förbättra standarden och snabbheten på juridiska tjänster. Särskilt användandet av externa IT-lösningar kan dock innebära problem i förhållande till de regler som gäller för advokater. Denna promemoria innehåller en rad rekommendationer och praktiska råd, avseende hur sådana problem kan undvikas.

Användandet av externa IT-lösningar aktualiserar dessutom frågan om i vilken utsträckning myndigheter och andra utomstående organ kan få åtkomst – genom processuella tvångsåtgärder eller på annat sätt – till inom advokatverksamheten elektroniskt lagrad information som finns utanför advokatbyråns ”egna väggar”. Här är rättsläget i dag inte helt klarlagt och några säkra slutsatser kan därför inte dras. Arbetsgruppens bedömning är dock (se avsnitt 4.3) att samma skydd för externt lagrad elektronisk information gäller som för information som finns på advokatbyrån. Detta innebär bl.a. att beslagsförbudsreglerna avseende information som omfattas av advokatsekretess, liksom skydd mot edition, anses gälla även om informationen är lagrad/befinner sig utanför advokatbyråns egna väggar, t.ex. på en extern dataserver. Eftersom rättsläget emellertid inte är helt klarlagt i fråga om beslagsförbudets omfattning för externt lagrad elektronisk information, måste varje advokat vara medveten om att sådan information ändå skulle kunna bli föremål för tvångsåtgärder. Nogsamma överväganden bör därför göras innan känslig information anförtros en extern IT-leverantör.

I fråga om vad en advokat specifikt bör beakta vid elektronisk kommunikation, hänvisas till den rekommendation som antagits av Rådet för advokatsamfunden i Europeiska unionen, CCBE (*Guidance for European Lawyers on Electronic Communication and the Internet*), vilken i dess fullständiga lydelse biläggs denna promemoria.

Ledning i fråga om advokats elektroniska kommunikation kan även hämtas från Advokatsamfundets promemoria *e-post och annan digital teknik i advokatverksamhet – några punkter att tänka på*, som 21 oktober 2004 tillställts ledamöterna genom cirkulär nr 22/2004 (se nedan avsnitt 6).

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 utnyttjande av s.k. tredjepartsleverantörer som sköter trafiken och lagrar informationen på sina servrar belägna i datacenter inom och utom Sverige, dvs. utanför advokatbyråns egna väggar.

2.2 Teknikfrågor m.m.

Ett teknikområde som förväntas kraftigt påverka användningen av IT är s.k. *Cloud Computing* eller molntjänster. Vad som avses med detta är IT- eller webbtjänster som tillhandahålls användaren, t.ex. en advokatbyrå, av tredje man 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*, ASP *Application Service Provider*, *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 ökad bandbredd och överkapacitet 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[1] följda av ett stort antal medelstora och mindre aktörer, gör för närvarande betydande investeringar på detta teknikområde. Exempel på molntjänster för advokater är Internetbaserad e-mail, datalagringstjänster *on line* och olika applikationstjänster (”Software as a Service” eller ”SaaS”) som kan användas på distans, från kontoret eller plats

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

utanför kontoret. En sådan 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 t.ex. en *browser*, en *tunn klient*, dvs. i princip endast skärm, datormus och tangentbord, en *smartphone* eller en pekplatta.

Användningen av den nya datatekniken exponerar 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. Mobilt bredband, uppkoppling via *WiFi* (s.k. *hot spots*) är ett par exempel på tekniker som medger åtkomst till både advokatbyråns interna och externa nätverk, varmed stora mängder information skickas fram och tillbaka, ibland helt oskyddat.

Ett annat teknikområde som för advokater idag är vanligare förekommande än molntjänster, 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 alla tjänster och produkter som erbjuds av marknaden från ett advokatperspektiv. Utvecklingen är dessutom under en 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 faror, 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 advokaten bestämmer sig för att kommunicera eller lagra data med hjälp av externa tjänsteleverantörer måste han eller hon således förvissa sig om att informationen därmed också skickas och förvaras på ett lika betryggande sätt som om advokaten 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 advokat 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 advokater 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 ut-

tömmande och utgör endast en exemplifiering av överväganden som advokaten bör göra inför användning av externa IT-tjänster i sin advokatverksamhet.

Ett samarbete med en leverantör av externa IT-tjänster handlar till stor del om förtroende. Advokaten bör förvissa sig om att den tilltänkta leverantören har en sådan ställning (både 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 advokaten 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. Detta är också sådant som lämpligen bör återspeglas i form av krav i avtalet med leverantören.

1. **Åtkomst:** Advokaten ska vid varje given tidpunkt snabbt och utan inskränkningar kunna komma åt all sin information i ett för advokaten hanterbart format; för att underlätta överföring vid t.ex. flytt till annan leverantör eller hemtagning av data. Advokaten 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, varken 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 personal måste komma åt konfidentiella uppgifter, måste deras tystnadsplikt och diskretion säkerställas genom avtal. 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* på den lagrade informationen och även spara e-mail 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. **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 och om aktivering av skalskydd på advokatens datorer, *smartphones* och pekplattor.

6. **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 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.

7. **Äganderätten till data:** Advokatens äganderätt till sina (och klientens) data måste säkerställas i avtalet med leverantören, inklusive information som uppkommer under hand, t.ex. metadata och trafikdata. Det bör framgå av avtalet att äganderätt till advokatens data inte under några omständigheter kan övergå till leverantören.

8. **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 (se avsnitt 4.3.2 och 4.3.3).

9. **Leverantörens policies:** Leverantören bör ha riktlinjer/policies i vart fall för nedan angivna områden. Krav om att leverantören ska ha sådana policies kan antingen tas in i avtalet eller så kan advokaten nöja sig med att leverantören verifierar att denne har och tillämpar sådana policies.
   a) Policy för att informera advokaten om eventuellt uppdagade säkerhets-brister och incidenter;
   b) Policy för att informera om att leverantören blir föremål för utländsk domstols eller myndighets åtgärder som – oaktat vad som anges ovan under 8. – kan resultera i att leverantören tvingas lämna ut information;
   c) Policy för permanent radering av eventuellt kvarvarande data (t.ex. dubbletter pga. backup) efter flytt samt för partiella lösningar, t.ex. i de fall en enskild advokat, av flera, lämnar advokatbyrån; samt
   d) Policy beträffande advokatens rätt till insyn i leverantörens säkerhets-åtgärder.

10. **Kryptering:** Leverantören bör verifiera i vilken omfattning denne använder kryptering beträffande data, såväl i transit och bearbetning som i

vila. Advokaten kan i detta sammanhang behöva överväga om krav på mer avancerad kryptering bör ställas.

11. **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. Advokaten kan även utifrån samma bedömningsgrunder i vissa fall behöva överväga nödvändigheten av att inhämta samtycke från klienten innan en molntjänst tas i användning för hantering av klientens data.

12. **Personuppgiftslagens krav**: Avtal med leverantör ska vara förenliga med personuppgiftslagens krav, vilket bl.a. innebär att personuppgiftsbiträdesavtal måste upprättas eller ingå som del av ett avtal om externa IT-tjänster (se närmare om detta i avsnitt 4.5) och att särskilda krav måste vara uppfyllda för att personuppgifter ska få överföras till länder utanför EES-området eller andra länder med adekvat skyddsnivå.

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 för att administrera klientakter och annat 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, köpa externa resurser i form av olika sorters Internettjänster, s.k. molntjänster eller *Cloud Computing*, vilket innebär en möjlighet att hantera program, datalagring, kapacitet och processorkraft på en extern resurs (se närmare beskrivning nedan i avsnitt 3.2). En annan viktig aspekt med denna typ av molntjänster 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 han eller hon befinner sig, genom uppkoppling på en dator. På så sätt slipper advokaten/advokatbyrån att direkt själv behöva sköta byråns IT-administration och många gånger kan den tredjepartsleverantör som förvarar all information i skyddade datahallar upprätthålla långt bättre säkerhet än vad många advokatbyråer själva klarar av att upprätthålla med interna lösningar.

Sådana externa IT-lösningar för dock med sig en rad olika frågeställningar. En viktig sådan fråga är säkerheten. Eftersom det inom advokatverksamhet finns ytterst känslig information, måste denna typ av externa IT-lösningar kunna säkerställa högsta möjliga säkerhet, genom att hårdvaran omgärdas av robusta brandväggar och att hanteringen säkras med lösenord, kryptering, etc.

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.

Advokaters möjlighet att utnyttja olika externa IT- och webbaserade lösningar inom ramen för sin advokatverksamhet 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 förstone 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 och klientprivilegier, 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 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. kan arbeta utanför kontoret och komma åt i princip samma information som om man befann sig på kon-

toret. Mobilt bredband, uppkoppling via *WiFi*, etc. är ett par exempel på tekniker som medger åtkomst till nätverk samt att stora mängder information skickas fram och tillbaka, på ett ofta oskyddat sätt.

Ett exempel på teknik som nu snabbt påverkar användningen av IT är alltså *Cloud Computing* eller ”molntjänster”. Starkt förenklat kan sägas att molntjänster

- innebär nya möjligheter till billigare, mer flexibel och mer kraftfull datahantering – advokatens data behandlas således utanför kontoret;
- bygger på att processorkraft, lagring eller funktioner tillhandahålls som tjänster på Internet till användare som inte behöver ha teknisk kunskap eller kontroll över infrastrukturen;
- är en variant av outsourcing – någon annan sköter uppgiften eller del därav;
- har blivit möjliga genom billig tillgång till ökad bandbredd och överkapacitet i stora datacenter; samt
- sannolikt har kommit för att stanna, då de stora leverantörerna i IT-branschen för närvarande satsar stort på detta teknikområde.

Det förekommer en mängd förkortningar för att beskriva olika molntjänster[2]. Produkter och tjänster som innebär nya möjligheter även för advokatbyråer utvecklas i snabb takt. Nya affärsmodeller innebär att man kan slippa stora investeringar och i stället betala för den faktiska användningen av datorkraft eller programvaror, något som är intressant för advokatbyråer oavsett storlek och verksamhetsinriktning. I flera fall kan dessa tjänster göra särskild nytta på de något mindre advokatbyråerna. Det mesta av en advokatbyrås IT-stöd kommer att kunna köpas som tjänster genom uppkoppling mot Internet och dagens rutiner kommer att påverkas av nya tekniska möjligheter. Det kan handla om e-post, tidredovisning, elektronisk lagring av akter och annan information, bokföringsprogramvara, m.m.

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

3.3 Probleminventering

Den ovan beskrivna tekniska utvecklingen innebär att många advokatbyråer som använder molntjänster och liknande IT-lösningar, 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 anges ett antal exempel på frågeställningar som behöver beaktas i samband med att advokatbyrån anlitar utomstående eller skaffar IT-lösningar som innebär att information hanteras eller lagras utanför advokatbyrån. Beroende på svaret på respektive fråga kan området ifråga innebära ett problem i förhållande till tillämpliga regelverk.

1. Risk för obehörig åtkomst till information? Leverantörer och deras anställda kan utgöra en typ av risk. Så kallade *hackers* kan vara en annan typ av risk.

2. Vet man säkert var information 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.

3. Om leverantören hanterar personuppgifter, finns då tydlig (skriftlig) reglering av leverantörens ansvar som personuppgiftsbiträde?

4. Har leverantören erforderliga rutiner för tagning av *backup*?

5. Har leverantören erforderliga rutiner för att säkerställa att bara sådana anställda som behöver tillgång till information för att kunna utföra sina

uppgifter får tillgång till informationen? Är berörd personal genom sekretessavtal eller på annat sätt informerad om sekretesskrav, insiderlagstiftning och liknande regler?

6. Finns det en tydlig reglering i avtalet av vem som äger data?

7. Snabb och smidig tillgång till data, under löpande avtalsperiod respektive när avtalet upphör? Även obeståndssituationer måste 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. Finns tydlig reglering av hur leverantören ska agera om myndigheter begär att information härstammande från advokatbyrån ska lämnas ut?

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

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 bestämmelser som direkt tar sikte på IT-frågor och Advokatsamfundet har inte heller i övrigt utfärdat några vägledande uttalanden eller rekommendationer i dessa frågor. Advokatsamfundet utarbetade dock i oktober 2004 en promemoria under rubriken ”E-post och annan digital teknik i advokatverksamhet – några punkter att tänka på”, vilken tillställdes ledamöterna genom Cirkulär nr 22/2004.

Inte heller i annan författning eller för andra liknande verksamhetsutövare finns reglering kring denna typ av frågor. Tidigare fanns av Datainspektionen utfärdade föreskrifter 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. Dessa föreskrifter är dock sedan länge upphävda (DIFS 1998:1).[3]

Avsaknaden av uttrycklig reglering i fråga om IT-tjänster är inte unikt för Sverige, utan gäller även i vårt närområde (se nedan avsnitt 5) 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.

[3] Det kan dock uppmärksammas att datainspektionens föreskrifter om undantag från förbudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser m.m. i (DIFS 2010:1) träffar advokattjänster såvitt gäller behandlingen av personuppgifter som är nödvändig för kontroll av att jävssituation inte föreligger i advokatverksamhet eller annan juridisk verksamhet.

4.2 Allmänt om advokatens plikter med bäring på IT-användning

Som bekant framgår de plikter som åvilar en advokat 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 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 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. Även om, som kommer beskrivas i det följande, det är svårt att säkert säga var skyddet för elektroniskt lagrad information går i det fall informationen finns på själva advokatkontoret i egna dataservrar etc., är det än svårare att avgöra vad som gäller när denna information finns hos externa IT-leverantörer.

Utgångspunkten från ett advokatperspektiv måste dock vara reglerna om tystnadsplikt, vittnesplikt och frågeförbud för advokater, beslagförbudsregleringens

och editionspliktens omfattning, liksom det förhållandet – såsom slagits fast i praxis och rättstillämpningen i övrigt (JO- och JK-beslut etc.) – att elektroniskt lagrad information får anses vara att jämställa med skriftliga handlingar.

Vad som här tillkommer är sedan en bedömning av vilket skydd som gäller för advokatsekret information som finns elektroniskt lagrad utanför advokatbyråerna.

4.3.1 Utgångspunkterna för advokatens tystnadsplikt

Att människor i förtroende ska kunna vända sig till advokat och därvid 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 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.[4]

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

[4] Se 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).

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

Av 36 kap. 5 §[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). För försvarare gäller således ett orubbligt frågeförbud och en försvarare kan 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.

[5] I dess senaste lydelse SFS 2010:1056.

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 reglering som särskilt tar sikte på information i elektronisk form finns emellertid inte.

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.[6] 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. Detta för att inte advokatsekretessen skulle bli alltför urholkad. Sammantaget fann Högsta domstolen att handlingarna var skyddade mot beslag enligt 27 kap. 2 § RB.[7]

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.[8]

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.

Det finns alltså ingen rättspraxis som uttryckligen uttalar vad som gäller i fråga om tillämpningen av beslagsförbud på datalagrad information. Frågan om behovet av att anpassa husrannsakans- och beslagsreglerna som en följd av den

---

[6] I målet var den ifrågavarande advokaten och advokatbyrån dessutom styrelseledamot i det aktiebolag som berördes av beslaget. Högsta domstolen ansåg att handlingarna trots detta kundes anses ha anförtrotts advokaten i hans egenskap av advokat och påtalade att det i sammanhanget var av betydelse om bolaget kunde anses vara advokatens klient eller ej.

[7] 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).

[8] 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.

tekniska utvecklingen har dock länge varit föremål för diskussion i en mängd utredningar tillsatta av regeringen, liksom överväganden på regeringskansliet.

Tvångsmedelskommittén föreslog att bestämmelsen skulle upphävas och att beslagsfrågan i stället skulle avgöras efter en intresseavvägning i det enskilda fallet (SOU 1984:54 s. 96 ff.). Förslaget ledde inte till någon ändring. Data-straffrättsutredningen föreslog år 1992 omfattande ändringar i dessa bestämmelser (SOU 1992:110). Polisrättsutredningen, som såg över reglerna i 27 och 28 kap. RB, ansåg att polisens sökande efter information i datorer saknar lagstöd och att det fanns behov av att lagreglera detta (SOU 1995:47 s. 184, 366 ff. och s. 493 ff.). Motsatt bedömning gjordes nästföljande år av IT-utredningen, som menade att reglerna i 27 och 28 kap. RB är direkt tillämpliga på datainformation (SOU 1996:40 s. 209). I promemorian Brott och brottsutredning i IT-miljö (Ds 2005:6), som behandlar frågan om vilka lagändringar som krävs för att Sverige ska kunna ratificera Europarådets konvention om IT-relaterad brottslighet och dess tilläggsprotokoll, föreslås att en uttrycklig reglering ska införas genom vilken bestämmelsen i 27 kap. 2 § RB om begränsningar i rätten att lägga beslag på skriftliga handlingar görs direkt tillämplig på elektronisk information. Förslagen har inte lett till lagstiftning.

Av den ovan nämnda departementspromemorian Brott och brottsutredning i IT-miljö (Ds 2005:6), framgår att det råder skilda meningar om huruvida reglerna om husrannsakan och beslag i sig är tillämpliga på den information som finns lagrad i datorer och hur reglerna ska tillämpas (s. 281 ff.). Vidare framgår att vissa anser att reglerna om beslagsförbud ska tillämpas analogt medan andra anser att det inte behövs. Enligt promemorian innebär detta att skyddet för exempelvis en advokats klienthandlingar som är lagrade på datamedium blivit betydligt bräckligare än vad lagstiftaren avsett, eftersom regeln om beslagsförbud inte anpassats till den numera dominerande tekniska formen för framställning och lagring av text. Konsekvensen av detta blir enligt utredaren att regeln om beslagsförbud i 27 kap. 2 § RB, ger ett betydligt sämre skydd för elektroniskt lagrade handlingar.

Frågan om beslag i IT-miljö har nu senast varit föremål för Förundersökningsutredningens överväganden (Ju 2009:07).[9] Utredningen överlämnade helt nyligen sitt slutbetänkande.[10] Utredningen anger att utgångspunkten är att skyddet för innehållet i en handling bör vara lika starkt oavsett om det finns i ett pappersdokument eller i en elektronisk handling. Ett sätt att uppnå samma skydd skulle enligt utredningen vara att uttryckligen göra beslagsförbudsreglerna direkt tillämpliga även på elektroniska handlingar. Enligt utredningens mening skulle dock en sådan lösning medföra en påtaglig risk för att de brottsutredande myndigheternas arbete i samband med verkställigheten av beslag i IT-miljö skulle försvåras. Ett uttryckligt förbud mot beslag av vissa elektroniska handlingar skulle nämligen kunna innebära att myndigheterna redan före ett beslag av en informationsbärare måste försäkra sig om att det digitala lagringsutrymmet inte innehåller uppgifter som omfattas av beslagsförbudet. Ett krav på sådan förhandsgranskning skulle i många fall vara orimligt med hänsyn till informationsmängden. Bestämmelserna om beslagsförbud bör därför enligt utredningens uppfattning inte göras direkt tillämpliga på elektroniska handlingar eller uppgifter. Enligt utredningen är det ett bättre alternativ att uppställa särskilda regler för hur genomsökningen av datorer och andra informationsbärare ska gå till när beslaget väl skett. Utredningen föreslår bl.a. att det i vissa fall och för vissa berörda personer, bl.a. advokater, ska införas en närvarorätt vid genomsökning av digitala informationsbärare. I betänkandet finns en utförlig redovisning av praxis, doktrin, JO- och JK-beslut och andra överväganden som gjorts i fråga om beslagsförbudets tillämpning och omfattning i fråga om elektroniska handlingar m.m.[11] Framtiden får utvisa om förslagen denna gång leder till lagstiftning i dessa frågor.

I ljuset av nu anförd rättspraxis och utredningsarbeten är det av största vikt att säkerställa att skyddsreglerna för informationsutbyte mellan advokat och klient inte kringgås genom resonemang om att elektroniskt lagrad information inte utgör

[9] Förstärkt rättssäkerhet och effektivitet i förundersökningsförfarandet, dir. 2009:35 och 2010:94.
[10] Den 19 maj 2011 lämnade Förundersökningsutredningen sitt slutbetänkande Förundersökning – *objektivitet, beslag, dokumentation m.m.*, SOU 2011:45.
[11] Se Förundersökningsutredningens slutbetänkande, SOU 2011:45, särskilt sid. 284-298 samt 352- 360.

en handling eller liknande, och därmed inte skulle omfattas av tystnadsplikts- och beslagsförbudsregleringen.

Advokatsamfund har i olika sammanhang också framfört att det finns behov av att förtydliga lagstiftningen på området till skydd för informationsutbytet mellan en advokat och dennes klient. Förhållandet att rättsläget är oklart får t.ex. inte innebära att uppgifter som är avsedda att omfattas av beslagsförbudet skulle åtnjuta ett sämre skydd om de finns upptagna i elektronisk form än om de finns i en skriftlig handling.

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 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[12] liksom av JK i två beslut år 2007[13] – 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

[12] I det ärendet gällde beslaget en brottsmisstänkt persons dator i vilken lagrats bl.a. e-postkorrespondens 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 beskriv si SOU 2011:45 s. 293 ff.

[13] 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.

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 delat bedömningen 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 är tillämpliga även på elektroniska handlingar.

Advokatsamfundet har också ansett 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).

JO anser 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 textmeddelanden, 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.

Det har i ljuset av vad som nu anförts från åklagarhåll i olika sammanhang anförts att nuvarande reglering i 27 kap. 2 § RB medför begränsningar i möjligheterna att ta handlingar – och även elektroniska sådana – i beslag, som från saklig synpunkt är alltför långtgående. En sådan formell tolkning av begreppet "skriftlig handling" i 27 kap. 2 § RB som anvisas i Högsta domstolens praxis i förening med bl.a. teknikutvecklingen leder enligt Åklagarmyndigheten till effekter som kan vara menliga för brottsbekämpningen eftersom det skulle vara olyckligt om den som är misstänkt för ett allvarligt brott kan undanskaffa bevisningen genom att t.ex. överlämna en dator till sin försvarare med en upplysning att de kan innehålla något av intresse. Det torde endast vara i undantagsfall som hela syftet bakom ett samarbete mellan en advokat och hans eller hennes uppdragsgivare skulle vara brottslig eller enbart bestå i att advokatens aktiva medverkan ska dölja ett brott och det på den grunden inte är frågan om sådan yrkesutövning som avses i 36 kap. 5 § RB (se NJA 2010 s. 122).

Advokatens tystnadsplikt och omfattningen av skyddet mot beslag och andra processuella tvångsåtgärder har även prövats i flera avgöranden i Europadomstolen. I exempelvis domstolens avgörande i *Petri Sallinen mot*

Finland[14] 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.

Arbetsgruppen gör sammantaget följande bedömning i fråga om skyddet mot beslag beträffande information som finns elektroniskt lagrad utanför advokatbyrån via en extern IT-tjänst.

Förundersökningsutredningen har i sitt slutbetänkande ansett det olämpligt att göra beslagsförbudsreglerna direkt tillämpliga även i fråga om elektroniska handlingar och att skyddet för advokatsekret elektroniskt lagrad information i stället bör säkerställas genom särskilda regler för genomsökningen av informationsbäraren och att advokater ska ges en närvarorätt vid sådan genomsökning.[15] Om det vid en sådan genomsökning av den digitala informationsbäraren visar sig ha sådant innehåll som skyddas av regleringen i 36 kap. 5 § RB, är det inte tillåtet att ta ytterligare del av innehållet och materialet får inte användas i förundersökning eller användas som bevisning. Skyddet för själva informationen kvarstår oförändrat.

[14] Dom den 27 september 2005.
[15] Se a.a. SOU 2011:45 s. 355 ff.

Trots Förundersökningsutredningens bedömning om att beslagsförbudsreglerna inte kan göras direkt tillämpliga även på elektroniskt lagrad information, finns tillräckligt auktoritativa uttalanden, praxis och doktrin som talar för att det, *i dagsläget*, får anses finnas ett skydd mot intrång i advokatsekret information med stöd av beslagsförbudsreglerna i rättegångsbalken. Inte heller utredningen föreslår ju någon utvidgning av beslagsmöjligheten, även om informationen finns i elektronisk form. Det går heller inte att förutse i vilken omfattning förslagen i denna del kommer att leda till lagstiftning.

I avsaknad av uttrycklig reglering görs därför i nuläget 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 överlämnades till polis eller åklagare.[16] En advokat bör alltså i dagsläget kunna utgå ifrån att beslagsförbudsreglerna gäller även för elektronisk information.

Arbetsgruppen gör, under samma förutsättningar, bedömningen att detsamma får anses gälla i fråga om advokatsekret information som finns på externa servrar eller 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). Enligt svensk rätt[17] får alltså

[16] 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.
[17] Beroende på var den elektroniskt lagrade informationen befinner sig geografiskt bör det observeras att andra jurisdiktioner kan ha annan reglering kring sekretesskyddet.

advokatsekret digital information anses åtnjuta samma sekretesskydd oavsett om informationen finns lagrad inom eller utanför advokatbyråns egna väggar.[18]

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.

4.3.3 Civilrättsliga bevissäkrings- och säkerhetsåtgärder

Som ovan påpekats finns inga rättsfall där HD uttalat sig om tillämpningen av beslagsförbuden på datalagrad information. Däremot har HD tolkat tillämpligheten av reglerna om edition i 38 kap. RB när det gäller sådan information. Dessa bestämmelser 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

[18] Se även nedan avsnitt 4.3.3 där samma bedömning görs i fråga om editionsplikt.

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.[19] Editionsplikten har här ansetts gälla för den som på grund av 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.[20] 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

---

[19] Se Vänbok till Bertil Södermark, s 218f., 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 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.

[20] 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.

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 regelverket, liksom enligt 15 kap. 3 § RB.[21] 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.

[21] 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.

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 räkning. Intrångsundersökningar får inte omfatta handlingar som omfattas av beslagsförbudet och vid civilrättsliga beslag bör beslagsförbudet ges motsvarande tillämpning.

4.4 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 ad-

vokats 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.

4.5 Personuppgiftslagen

En advokat som behandlar personuppgifter är enligt 1 § personuppgiftslagen (1998:204) att anse som personuppgiftsansvarig. Om advokaten väljer att anlita en IT-leverantör som för advokatens räkning behandlar personuppgifter är denne att betrakta som personuppgiftsbiträde. Mot bakgrund av att begreppet ”behandling” i personuppgiftslagen omfattar snart sagt varje befattning med personuppgifter i en dator (lagring, radering, kopiering, vidarebefordran) kan det

presumeras att en advokats anlitande av en IT-leverantör för tillhandahållande av IT-tjänster kommer att innefatta personuppgiftsbehandling på vilken personuppgiftslagen blir tillämplig.

Enligt 30 § andra stycket personuppgiftslagen ska det finnas ett skriftligt avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet, ett s.k. personuppgiftsbiträdesavtal.[22] I avtalet ska det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldig att vidta sådana lämpliga tekniska och organisatoriska säkerhetsåtgärder till skydd för de personuppgifter som behandlas. Det är den personuppgiftsansvarige som har ansvaret för att instruktionerna är så tydliga att otillåten behandling inte kommer att utföras.

Om personuppgiftsbiträdesavtalet tillåter att personuppgiftsbiträdet anlitar ett annat företag såsom underentreprenör för någon viss behandling av personuppgifterna, är även underentreprenören normalt att betrakta som personuppgiftsbiträde till den personuppgiftsansvarige, eftersom även denne behandlar personuppgifter för den personuppgiftsansvariges räkning. Detta innebär att den personuppgiftsansvarige är skyldig att se till att dessa båda personuppgiftsbiträden träffar ett inbördes avtal.

Enligt 31 § personuppgiftslagen är den personuppgiftsansvarige skyldig att säkerställa att lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda de personuppgifter som behandlas. Den personuppgiftsansvarige ska genom åtgärderna åstadkomma en säkerhetsnivå som är lämplig med beaktande av

(i) de tekniska möjligheter som finns,
(ii) vad det skulle kosta att genomföra åtgärderna,
(iii) de särskilda risker som finns med behandlingen av personuppgifterna, samt
(iv) hur känsliga de behandlade personuppgifterna är.

[22] Ett sådant avtal kan utgöra en del av ett avtal om externa IT-tjänster och behöver inte utgöra ett separat dokument.

Den personuppgiftsansvarige har en skyldighet att utöva tillsyn över personuppgiftsbiträdets säkerhetsåtgärder, att dessa är tillräckliga enligt personuppgiftslagen och att de genomförs. Om behandlingen innefattar känsliga personuppgifter uppställs särskilt stränga säkerhetskrav. Datainspektionen har i tillsynsbeslut tillämpat en sträng syn vilket innebär att en personuppgiftsansvarig som behandlar och kommunicerar känsliga personuppgifter bl.a. är skyldig att införa rutiner för säker identifiering av mottagare, se till att det loggas vem som fått del av uppgifter och att kommunikation ska vara krypterad.

Om IT-leverantören är etablerad i ett land inom EES-området eller i något av de länder som anses ha en adekvat skyddsnivå, uppstår inga problem. Är emellertid IT-leverantören etablerad på annat ställe, omfattas den personuppgiftsansvariges överföring av personuppgifter till en sådan IT-leverantör av exportförbudet i 33 § personuppgiftslagen. Enligt 13 § 2 personuppgiftsförordningen, får personuppgifter föras över till tredje land om personuppgifterna förs över med tillämpning av ett avtal som innehåller sådana standardavtalsklausuler som kommissionen enligt artikel 26.4 i dataskyddsdirektivet (dir. 95/46/EG) har beslutat erbjuder tillräckliga garantier för att privatliv och enskilda personers grundläggande fri- och rättigheter skyddas samt för utövningen av motsvarande rättigheter.[23]

[23] I Kommissionens beslut av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG, anges hur sådana klausuler ska utformas för att exporten ska vara tillåten. En personuppgiftsansvarig som anlitar ett personuppgiftsbiträde i tredje land kan därmed säkerställa att exporten är tillåten enligt personuppgiftslagen genom att utforma avtalet med IT-leverantören (personuppgiftsbiträdet) i enlighet med kommissionens beslut.

5. Reglering av IT-tjänster i andra länder

Såsom tidigare angetts har Rådet för advokatsamfunden i Europa, CCBE, tagit fram riktlinjer till hjälp för advokater att se över säkerheten i sin elektroniska kommunikation. Rekommendationen om elektronisk kommunikation och Internet innehåller en rad icke bindande, men viktiga praktiska råd för advokater i fråga om säkerhet och sekretess vid elektronisk kommunikation m.m. Även om den inte direkt behandlar frågan om externa IT-tjänster vid advokatverksamhet, har den bedömts vara av sådan betydelse att den bilagts denna rapport. Någon reglering eller annan dokumentation specifikt rörande externa IT-tjänster har inte tagits fram inom CCBE. Inte heller nationellt i Europa finns – såvitt efter en översiktlig genomgång har kunnat bedömas – i någon större utsträckning någon uttrycklig reglering eller annan dokumentation kring frågor om externa IT-tjänster. Såsom framgår av avsnitt 6 finns dock omfattande sådan reglering och dokumentation i exempelvis USA.

Av den information som inhämtats från våra nordiska grannländer i fråga om befintliga regler, riktlinjer, rekommendationer eller annan typ av dokumentation kring IT-tjänster vid advokatverksamhet, har det framkommit att det inte i något av dessa länder finns närmare reglerat eller utrett vad som ska gälla i fråga om advokaters användning av externa IT-tjänster. I Norge finns ingen reglering alls och inga åtgärder är enligt uppgift planerade.[24]

Såväl i Finland som i Danmark har det tagits fram vissa, allmänna, riktlinjer i fråga om datasäkerhet. Danska advokatsamfundet har även angett att de vid interna diskussioner kring klientsekretessen vid externa IT-lösningar, bedömer att det avgörande för sekretessen är huruvida materialet/informationen är hänförligt till advokatverksamhet och inte var materialet/informationen fysiskt finns tillgängligt (jfr arbetsgruppens bedömning i avsnitt 4.3).

[24] I fråga om Norge kan dock tilläggas att rättsväsendet i Norge i maj 2011 beslutat att köpa server, lagring och externa nätverkslösningar av en privat leverantör. Ramavtalet omfattar bl.a. norska justitiedepartementet, polisen, kriminalvården och domstolsadministrationen.

Danska advokatsamfundet har även tagit fram en broschyr om datasäkerhet, i vilken det ifråga om externt lagrad information görs summariska överväganden som motsvarar vad som anges i denna rapport . Även Finlands advokatsamfund har tagit fram ett dokument med rekommendationer rörande elektronisk kommunikation och Internet, vilket helt och hållet bygger på CCBE:s framtagna rekommendationer (se bilaga). I övrigt har finska advokatsamfundet bara konstaterat att försiktighet är påkallad för advokater och advokatbyråer vid användning av externa IT-lösningar och att tystnadsplikten och andra yrkesplikter alltid måste upprätthållas.

6. Övrigt

För ytterligare information i frågor som rör externa IT-tjänster och andra elektroniska frågor, liksom för den som önskar fördjupa sig i tekniska aspekter och risker, finns här exempel på ett antal länkar.

- Advokatsamfundets promemoria *e-post och annan digital teknik i advokatverksamheten – några punkter att tänka på*, cirkulär nr 22/2004: http://www.advokatsamfundet.se/Documents/Advokatsamfundet_sv/Cirkulär/137451_20060830164852.pdf
- Övervägande och analyser kring etiska frågor och säkerhetsfrågor i en artikel från American Bar Association (ABA): http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/law_office_technology/saas.html
- American Bar Association har i september 2010 författat ett White Paper i ämnet där remisstiden gick ut strax före jul, se http://www.docstoc.com/docs/55095677/ABA-Ethics-Commission-2020-For-Comment-Issues-Paper-Concerning-Client-Confidentiality-and-Lawyers%E2%80%99-Use-of-Technology
- Om man tittar ytterligare mot USA, har exempelvis North Carolina Bar Association, Arizona State Bar Committee, New York State Bar Association och Alabama State Bar Association ställts inför motsvarande frågor och meddelat opinions beträffande användning av Cloud-tjänster, se http://www.docstoc.com/docs/35532924/NC-Bar-FEO-2010-7, http://www.myazbar.org/Ethics/opinionview.cfm?id=704, http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&CONTENTID=42697&TEMPLATE=/CM/ContentDisplay.cfm respektive http://www.alabar.org/ogc/PDF/2010-02.pdf
- Finansinspektionens föreskrifter FFFS 2005:1 (kapitel 7) som anger förutsättningarna för outsourcing av finansiell verksamhet, se http://www.fi.se/upload/30_Regler/10_FFFS/2005/FFFS0501.pdf
- Queen Mary University of London: Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374

- EU om molnet, se rapporten: 2010.http://cordis.europa.eu/fp7/ict/ssai/events-20100126-cloud-computing_en.html
- ENISA Cloud Computing Risk Assessment http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
- The NIST Definition of Cloud Computing (National Institute of Standards and Technology, Information Technology Laboratory), http://www.google.se/#hl=sv&source=hp&biw=897&bih=347&q=nist+definition+cloud+computing&aq=0&aqi=g2&aql=&oq=nist+definition+&fp=64b670166e0b0061
- Dataföreningen och Cloud Sweden, se: http://natverk.dfs.se/riks/cloudsweden

Représentant les avocats d'Europe
Representing Europe's lawyers

ELECTRONIC COMMUNICATION AND THE INTERNET

Conseil des barreaux européens – Council of Bars and Law Societies of Europe
association internationale sans but lucratif
Avenue de la Joyeuse Entrée 1-5 – B 1040 Brussels – Belgium – Tel.+32 (0)2 234 65 10 – Fax.+32 (0)2 234 65 11/12 – E-mail ccbe@ccbe.org – www.ccbe.org

ELECTRONIC COMMUNICATION AND THE INTERNET

Summary of guidance

I. Content of e-mail and Internet sites

1. Data

- Keep it accurate and updated
- Comply with professional rules (a basic requirement is usually the name and address of the firm as well as the name of its partners or a statement about where this information can be obtained)

2. Nature of the on-line legal service

- Explain the nature of the legal advice being provided so as to avoid misunderstandings and possible claims against lawyers for inaccurate or incorrect advice

3. Links and references to third parties

- Care must be taken to ensure that these sites do not appear offensive to the profession, or incompatible with the profession's underlying principles

II. Lawyer correspondence

1. Deliberate interception and hacking

- Consider to use and offer appropriate means to protect the content of correspondence against any fraudulent modification, such as digital signatures or encryption, or both digital signatures and encryption
- Consider to use and offer a means of electronic communication, in particular when using web-mail service providers, online messengers or mobile devices, which is reasonably protected against any interception and hacking which could result in the disclosure of the existence and content of communications
- Use encryption techniques which are reasonably available every time clients or correspondents request them
- Inform clients and correspondents, if necessary, of the risks encountered by the use of electronic communications

2. Inadvertent access

- Include automated confidentiality warnings

3. Viruses and malicious software

- Develop a security strategy and basic security procedures

4. Electronic mail correspondence between lawyers

- Bear in mind the professional rules applicable to correspondence between lawyers when using e-mail

III. Safeguarding professional secrecy and personal data

- Sending, receiving and holding e-mail correspondence may involve the processing of personal data requiring sufficient data protection measures in order to comply with professional secrecy obligations and other applicable laws and legislation, which must be dealt with in accordance with relevant data protection legislation
- Display a confidentiality notice

IV. Safeguarding copyright

- Verify copyright protection and use copyright notices if required by legislation

V. Best practice

- Verify the identity of an on-line client
- Give a timely response to an on-line client
- Keep records of electronic correspondence
- Maintain user privacy and monitor standards for electronic correspondence
- Comply with professional rules regarding on-line cross-border disputes

VI. Archiving of electronic documents and e-mails

- Develop policies regarding the archiving of electronic documents and e-mails, not only on what should be archived, but how it should be archived, in order to preserve accessibility to the electronic documents and e-mails for the appropriate time
- Be aware that saving electronic documents and e-mails in one program might have consequences for the possibility to retrieve them for the appropriate time
- Archive electronic documents and e-mails using a generally accepted format, ensuring their legibility in the future, and the safeguarding of the original version

VII. Awareness of hidden data in files and documents

- Be aware that files and documents may include hidden data that are not visible or which renders information about the document and is in addition to the main body of the text (often called "metadata")
- There might be meta data that it is useful or even vital for the lawyer to keep and other data that it is important to erase depending on where it is to be sent (eg the lawyer's file, to the client for tracking changes, or to the lawyer for the other party).
- Hidden data may be tied to visible data in such way, that copying and pasting visible data will also bring along the hidden data
- Always check whether "Track Changes" is used in electronic documents
- If using "Track Changes", make sure they are visible and "accept" or "reject" the changes before distributing the document unless the other party has intended to receive the document with such track changes visible.
- Check that no other version of the document is stored in the file
- Check "Document Properties" or similar before sending a document to see that it does not include information not intended for the recipient
- Use specific programs that permits the analysis of and to strip out hidden data
- Consider installing a system that automatically checks outgoing electronic documents and removes hidden data

ELECTRONIC COMMUNICATION AND THE INTERNET

Guidance for Lawyers
CCBE

FOREWORD

1. The electronic provision of legal services, via electronic mail ("e-mail"), the Internet or any other new technology, offers lawyers an opportunity to enhance the quality of their services and the speed at which these can be delivered to their clients. Without proper guidance, however, e-services can result in serious losses for which a firm, and lawyer, may be held liable.

2. As a communication tool, e-mail is easy to use and many users tend to regard it as if it were a spoken medium rather than a written one. As a result, the content of some e-mails may well be regarded as defamatory or offensive if it is read by an unintended recipient. Both the lawyer sending the message, and the firm employing him/her, may be held liable.

3. Internet sites (or websites) are increasingly being used by law firms for advertising, but also as a means of disseminating legal advice and information. Many lawyers feel that providing legal services on-line offers the opportunity to obtain access to a much wider client base, to decrease overheads (the lawyer no longer needs an office), to have flexible working hours and to streamline case work procedures by downloading Internet tools such as case-management software. But the Internet also presents clear dangers for lawyers. The absence of a face to face meeting with a client could make it more difficult for a lawyer to assess a case and to provide complete advice, an on-line client could usurp the identity of another person (for a will, for example), and a person could wrongly portray him/herself as a lawyer, as has occurred in the physical world.

4. The archiving of electronic documents and e-mails is an issue of great importance. The CCBE therefore consider it necessary to make the national Bars and Law Societies aware of the fact that both digital and paper records must meet the same legal requirements when sent and archived. It recommends the adoption of policies regarding the archiving of electronic documents and e-mails.

5. To reap the benefits of on-line technology while minimising its dangers, firms need to consider how legal professional standards and best practice can be translated into the electronic world. The CCBE believes the most effective way to do this is by drafting an Internet and electronic mail policy.

6. To assist law societies, bars and firms in producing their own policy, the CCBE has drafted a model Internet and e-mail policy. This may need to be adapted to a country's own professional rules and to the firm's particular circumstances. It is recommended that, once adopted, the policy be disseminated among all the firm's staff together with other suitable advice.

I. Content of e-mail and Internet sites

A lawyer and firm's liability for wrong or misleading information can be engaged when providing advice or information electronically or on paper. Care must therefore be taken to check that data is accurate, updated and in compliance with professional rules.

1. Data: Complying with Professional Rules

a) Principles:

The information required in lawyer correspondence may vary from country to country. Generally, all professional rules require basic information which will allow a client to verify the firm's credentials and file a complaint against the firm. The latter will comprise: the name of the firm, its address, the name of the firm's partners, or a statement about where this information can be obtained, and any other information on the registration of the service provider in accordance with the EU Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)[1].

b) Guidance:

For Internet sites, law firms are advised to provide this information in a clearly visible notice on the home page.

For electronic mail correspondence, law firms may wish to introduce templates, as described below.

E-mail software can provide its users with one or more standard templates incorporating the information they must provide in their correspondence.

When firms permit users to send private e-mail, they are recommended either to ask solicitors to write private e-mails on an alternative template that expressly states that the communication is from the user alone and not the firm, or to require that lawyers apply a different signature block for private communications.

When firms permit users to take part in public discussions on mailing lists by e-mail, confidentiality or privilege warnings are obviously inappropriate, and their inclusion can detract from the effect of the message. Firms may wish to consider adopting a specific template for such purposes.

2. Nature of an on-line legal service

a) Principles

Many of those who contact a law firm through its website or via e-mail have little or no legal knowledge. In order not to mislead the client, it is therefore imperative that the lawyer clearly explain when his/her communication constitutes legal information and when it constitutes advice.

Generally, "information" can be defined as material which will be the same, irrespective of the person requesting the legal service. If, on the other hand, material will depend on the person requesting the service, then the service can be defined as "advice".[2]

b) Guidance:

In e-mail correspondence, the lawyer will need to clarify when information provided constitutes legal advice and when it is only information. The context of the e-mail correspondence can assist in establishing the nature of the service.

---

1 http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf

2 As an example: a person enquiring about the tax rate for France in a given year will receive information. If, on the other hand, a person enquires about his/her tax duties for a particular year, he/she will receive advice.

For Internet sites, firms are advised to state clearly on the home page that the services provided by the site are for information only. Without minimal contact, it is impossible for a firm to offer advice, which is why many sites will state that legal advice can be obtained from a lawyer by using the site's e-mail link. A sample disclaimer is provided below.

Sample disclaimer for an Internet site:

"The content of this site is for general information purposes only. It does not constitute professional advice (legal or otherwise) nor should it be used as such. We cannot accept responsibility for actions based on the material contained herein".

3. Links and references to third parties

If a site provides links and references, the user of the site is likely to think the firm approves of the services and information provided on affiliate sites. Care must be taken to ensure that these sites do not appear offensive to the profession, or incompatible with the profession's underlying principles (e.g. if a law firm's website posts an advertisement or a link to an insurance company, it may give the impression that its independence is being jeopardised).

II. Lawyer correspondence

Professional lawyer correspondence is generally confidential. To protect the correspondence from being accessed by unauthorised parties, the CCBE suggests the following:

1. Deliberate interception and hacking

Lawyers have to protect the content of their electronic correspondence against any fraudulent modification, in particular to preserve their own interests.

To this end, it is recommended that lawyers use a means of electronic communication that is reasonably available to ensure the integrity of their electronic communications.

Although electronic communications are technically and legally protected against interception by third parties, their confidentiality might be in danger through various means. Lawyers have therefore to assess the risks encountered by their electronic correspondence (in particular when using web-mail service providers, online messengers or mobile devices) and take appropriate measures, such as the use of encryption techniques according to the situation, and to inform their clients and correspondents of the risks encountered through electronic communications. Lawyers should not abstain from using encryption that is reasonably available every time their client or correspondents request them.

2. Inadvertent access

Many firms already include a confidentiality warning on fax messages because of the risk that these will be sent to the wrong person by mistake. Firms should consider adopting similar confidentiality warnings for e-mail.

Automated confidentiality warnings

While automated confidentiality warnings are unlikely to impose any legally binding duty on an unintended recipient, many recipients may be expected to heed them, and the warnings may therefore help prevent a mistake from causing loss.

The following specimen warning is offered for adaptation:

"Information in this message is confidential. It is intended solely for the person to whom it is addressed. If you are not the intended recipient, please notify the sender, and please delete the message from your system immediately and thoroughly."

Firms can usefully attach this sample warning message to e-mail correspondence by using a template or a signature block.

Firms may feel that attaching such a warning to all e-mail correspondence is unnecessarily burdensome and may depreciate the importance of the warning. Nevertheless, unless lawyers consider whether to include the warning every time they send a message, it is recommended that the warning be attached to all e-mail correspondence.

Lawyers should note that legally confidential information in lawyer correspondence may cease to be confidential if the message is sent to others (for example, if the message is accidentally sent to a mailing list).

3. Viruses and malicious software

Electronic mail correspondence can be infected by viruses which can affect a firm's Internet site and entire network. In addition, such viruses and software can distribute confidential information or allow unauthorised access to it.

Firms are encouraged to have a security strategy and to maintain up-to-date technical precautions against such risks. They are also encouraged to ensure that users remain alert to the importance of security procedures. Some basic security procedures are included below:

(a) Adoption of anti-virus software.

(b) Configuring e-mail servers that attachments cannot open automatically upon receipt. This will ensure that viruses cannot be automatically imported into other systems.

(c) Ensuring the firm's computer network is adequately protected from incursions or viruses from the Internet.

If a firm is linked to the Internet through a permanent open line, it is strongly recommended that they install firewalls to ensure their systems are protected.

If a firm has a dial-in connection, it is recommended that it considers installing a firewall. If the expense is too high, the firm should at least consider isolating the computers which obtain access to the Internet from the firm's network. This will ensure that an incursion or virus from the Internet will not affect the firm's entire network.

(d) If the maintenance of a firm's network and computers is outsourced, it is recommended that the firm

- conducts appropriate security checks of the personnel who will be completing the maintenance work and ensures that the personnel have adequate technical qualifications;
- conducts adequate supervision of the work being carried out;
- agrees on measures to be taken for compliance with confidentiality and other ethical rules.

4. Electronic mail correspondence between lawyers

When sending an electronic mail correspondence, lawyers have to bear in mind the professional rules applicable to lawyers' correspondence in general. These professional rules may include rules on the form of the correspondence, or on the storage or archiving of the correspondence for a certain period of time, or the confidentiality. Lawyers who send correspondence by electronic mail to a lawyer in

another Member State and who wish that it remains confidential or without prejudice should clearly express his/her intention when communicating the document.

III. Safeguarding lawyer client privilege and personal data

Lawyers should be aware that sending, receiving and holding e-mail correspondence may involve the processing of personal data, requiring sufficient data protection measures to be in place in order to comply with professional secrecy obligations and other applicable laws and legislation. .

IV. Safeguarding copyright

Before downloading a file, a lawyer should ensure that there will be no infringement of copyright.

Example of a copyright notice:

"The content of this site is protected by copyright [© name of firm]. It cannot be copied, in part or in full, and in any form, unless it is done for the following purposes:

1) Personal use
Content of this site may be copied, in part or full, if the information is intended for personal use only.

2) Other purposes
The content of this site may be copied, in part or in full, for the benefit of a third party if all of the following conditions are met:

a) the copy indicates this site as its source and provides the site's complete address and copyright information;
b) the copy indicates that it is protected by copyright restrictions which must be respected by the third party;
c) the copy, in part or in full, must not be inserted into another text or publication, in whatever form, without prior permission;
d) the copy, in part or in full, must not be stored, on another website or on any other electronic system, without prior permission;
e) the copy, in part or in full, must never be disseminated for commercial purposes without prior permission.

No part of this site may be copied, transmitted or stored on another Web site or on any form of electronic system without prior permission, except for indexing and updating all search engines and similar services aimed at directing users to this website."

Other exemptions may also apply in accordance with local circumstances.

V. Best Practice Principles

There is no reason why firms should not give and receive professional undertakings by e-mail, but firms may wish to exercise caution when accepting any undertakings through this medium.

It is difficult to decide from the face of an e-mail message whether it was really sent by its purported sender, although its context may often put the matter beyond doubt.

In time, digital signatures (eventually in connection with biometrics) may provide much better evidence of the authenticity of e-mail, and the widespread adoption of encryption will bring with it the additional benefit of improved authentication.

In the meantime, firms given a professional undertaking by e-mail are recommended to check that the context provides reasonable assurance of its authenticity, and/or to check by telephone or fax that it came from its purported sender should there be any doubts about this.

E-mail: Automated confirmation of receipt: Firms are cautioned not to use automatic confirmation of the receipt of e-mails. It is important for the lawyer to send a confirmation only if the request for advice or information has been fully understood. He/she may well wish to ask the client for further information and agree on a timeframe in which the advice will be provided. Firms should be aware that it may be necessary to positively disable this function in the e-mail program options.

1. Knowing the Client

Firms may accept instructions by e-mail and via a website, but they should apply the same checks and make the same enquiries as they would for traditional client-lawyer communication (paper and face to face meetings).

The potential of the Internet for anonymous communications may prove attractive to fraudsters and money launderers, and firms must be alert to their duties in this area.

Some areas of practice, such as the making of wills and/or divorce on-line, present special risk when conducted remotely (impersonation or undue influence, for example), and e-mail may increase those risks and the need for caution.

2. Timely Response

a) Principles:

Firms already know (or should know) how to handle incoming letters, faxes and telephone calls in the absence of the intended recipient.

E-mail presents new problems because it can arrive unperceived by other members of staff. Firms are recommended to make effective technical and practical arrangements to ensure that e-mails receive a timely and appropriate response.

b) Guidance:

It is recommended that firms use automated out-of-office responses when members of staff are away from the office for a day or more provided that, in the same way, firms arrange for incoming e-mail, mails and faxes to be checked when the lawyer is absent. A limited number of people (a secretary and a colleague, for instance) should have access to an absent lawyer's inbox with a view to checking the contents regularly and ensuring that any urgent enquiries are dealt with promptly.

Systematically sending out-of-office messages in response to every e-mail received may be both annoying and a discredit to the firm, especially if an absent lawyer has subscribed to mailing lists and remains subscribed while on holiday. To avoid this, it is recommended that firms should, if possible, arrange for all automated out-of-office messages to be sent only once to every e-mail correspondent.

3. Spam

Unsolicited bulk e-mail or, as it is generally known, 'spam' can be a significant problem for firms using e-mail. Filtering software is available to reduce the amount of spam. However, if firms use spam filters they should warn clients in order to avoid the blocking of legitimate correspondence. They should explain that important communications should always be followed up with a telephone call, fax or printed copy by post. Firms that run their own mail-servers should consider returning unsolicited e-mail to the sender with a message along the specified lines

4. Records

Just as paper files are used to retain copies of outgoing letters and notes of telephone conversations, so copies of e-mail messages (other than those with no legal significance) should be kept on file. In respect to authenticity, the metadata of e-mail messages should be recorded as well. At this time, it is recommended that paper files be used although this view may change when the truly electronic office arrives.

Lawyers should be aware that even if an e-mail is deleted, it may still be capable of being retrieved. In disputes, even deleted e-mails may well be subject to disclosure.

For more detailed guidelines, please see paragraph VI.

5. User privacy

a) Principles:

Firms need to monitor the correspondence and communications of their fee-earners and other staff to ensure that their professional standards are maintained. If advice is given by members of staff by e-mail, firms will need to be able to check the accuracy of the advice.

Normally, this will be done by a review of paper files, but cases may arise where firms will wish to check communications on their way to or from a member of staff.

Where the use of the firm's system for private communications is permitted, such a check may intrude on the privacy of members of a firm's staff. In certain jurisdictions, such checks may not be lawful.

b) Guidance for lawyers using e-mail:

If users are permitted to send private e-mail on the firm's system, it will be impractical to isolate it from other messages for monitoring purposes.

It should be part of the firm's terms of service that members of staff agree to such monitoring, and the possibility of this occurring should be made clear.

6. Cross Border on-line: professional rules

If a lawyer provides his/her services via e-mail, the rules which apply to the lawyer - client relationship depends on the location of the lawyer[3]:
As an example:

- An Irish lawyer gives advice, via e-mail, to a client in Belgium.
- The lawyer-client relationship is, in accordance with the E-Commerce Directive, governed by professional rules in Ireland.

If a lawyer provides his/her services, via e-mail, to a client who resides outside the EU, it is recommended that both parties agree on the rules to be applied to their relationship.

VI. Archiving of electronic documents and E-mails

Developments in information technology go fast and it is increasingly common not to keep a paper copy of every document, but it remains legally necessary to archive certain documents and e-mail for several years. As is mentioned previously, lawyers should be aware that in disputes, even deleted e-mails may well be subject to disclosure.

---

[3] Directive 2000/31/EC of 8 June 2000 of the European Parliament and of the Council on certain legal aspects of Information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"): http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf

1. Archiving e-mails

E-mail is an outstanding example of a distributed means of communication that is therefore difficult to control. Many people believe that e-mail has no official status. Employees often decide for themselves what should and should not be kept and save or delete their e-mail messages at their own discretion as they wrongly view electronic mail as part of their own personal working domain. Firms need to have fixed policies as to the choice of which e-mail messages need to be considered for preservation. In principle, the same criteria as for 'normal' paper post will apply. The requirements set out in law that apply to documents in paper format will also apply to documents in electronic format. The format of the document is irrelevant. There should also be guidelines for using and organising e-mail, as people tend to print them out and therefore they are not preserved correctly. Part of the context or other information is thus lost and the accessibility lessens.

2. Electronic signature[4]

As the use of digital signatures in documents and e-mails increases, the question of preserving the signatures also comes to the fore. Some of the data on which digital signatures are based and which to a large degree determine the trust that can be placed in a digital signature, is held by the accredited certification-service-providers in the sense of the EU Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures. This data is mainly data that proves the certification is genuine (data on consulted identity documents, application forms and signed conditions) and historical data about cancelled certificates. This data may be highly significant in the event of a dispute about the authenticity and applicability of a digital signature.

3. Authenticity

It is also important that the characteristics of the digital document be preserved so that the integrity of the document is safeguarded. This can be accomplished largely by developing a strategy in which the important aspects of the content, structure, appearance and the behaviour of the document can be preserved. The preservation of the characteristics of digital documents archived is very important. Finally, authentication is the important point. The context in which the document is made and used, and any changes that have been made as a result of management and preservation activities, are described in the metadata[5]. This makes it possible to demonstrate or verify the extent to which the document which has been archived is authentic in creation and contemporary use.

If the digital document is reproduced in a different computer environment than that in which it was originally made, it may look and behave entirely differently. If the transition to the other computer environment is not controlled, the authenticity of the digital document may be affected. Authenticity is a key concept in the preservation of documents, digital or other ways, and says that the document is what it says it is and that it was made by a specific person. The authenticity of documents can be safeguarded by describing and preserving the original context of the documents and by maintaining a chain of unbroken custody. A document has integrity when it is complete and uninterrupted in all essential aspects, so this means that it is intact and not changed or corrupted in such a way that its meaning is no longer clear. Changes are acceptable to a certain extent, as long as they do not affect the original meaning or function of the document. Basically, it makes no difference whether a document has a digital or a physical form: authentic preservation must be achieved, regardless. The problem that arises with digital documents, however, is that due to changing technology, not all aspects of a document can be preserved as precisely as when it was made. This does not mean, though, that sustainable preservation of authentic digital documents is impossible.

[4] See also directive 1999/92/EC on a Community framework for electronic signatures, OJ L13 of 19 January 2000, page 12.
[5] Not only the text of the document itself contains important data, also metadata is important. Metadata is data about data. Metadata is added to a digital document to describe extra information about the five characteristics of a document mentioned above so that, among other things, checks can be made on whether the document is what it 'says' it is. At the same time, metadata makes it possible to retrieve and use a particular digital document. Examples of such data are the purported author of the document, subject, business process in which it was created and date on which it was created. But metadata is also important in the context of registering that preservation activities have been carried out.

As mentioned previously, archiving electronic documents and e-mails differs from how paper documents are archived. When you keep the next points in mind when you create an e-mail or document, it will be easier to archive documents and e-mails, which need to be saved for several years according to legal requirements.

a) Document

When you keep in mind the next points it will be easier to archive[6] documents afterwards:

- use templates[7] to create documents
- start creating documents with a blank template, otherwise information (metadata[8]) of other documents might be included in the new document and will therefore include wrong information
- check if the information in the properties[9] screen is up-to-date
- instruct users to use explicit structure in documents, which means use of profiles and headings
- copy and paste as little as possible in order to prevent incorrect metadata being included
- do not use passwords to secure documents, because if the password gets lost it is impossible to open the document, use read-only option instead
- use standard letter type fonts like Arial, or Times New Roman, because these fonts will be recognised by other programs
- use headers and footers to insert metadata such as name and version number of document
- do not use automatic date and time fields, because they may change every time you open the document
- use tables or tabs when necessary and not space bar, so the lay-out of the document is fixed
- save the document centrally on the server and not on the hard disk of the workstation, so the newest version can be retrieved by everyone.

b) E-mail

In order to be able to decide if an e-mail needs to be archived, a distinction can be made, taking into account the following comments.

aa) Addressing e-mail messages

- always use the address book, because this contains extra information about the people to whom you are sending your message
- be circumspect when using distribution lists, because they can change often and if when the distribution list changes no information is kept about this, you cannot trace to whom the e-mail was sent to originally
- even if this sounds self-evident: always give your e-mail message a subject, it helps to sort and evaluate messages
- use message options, such as 'urgency' only when absolutely necessary, because not all e-mail applications can reproduce them correctly

bb) Drafting an e-mail message

- where possible make and send messages in plain text or in HTML-format, because not all e-mail programs can read various fonts
- do not use automatically updating fields messages (not stable and may update every time the e-mail is opened)
- use attachments sensibly (send images as bitmap or .JPEG and not pasted in other application)

[6] See paragraph about archiving.
[7] A template is a lay-out model for documents.
[8] See under 4.
[9] This option you will normally find under the heading 'file' of your word processing program. This option contains for example information about when the document has been created, by whom the document has been created and when the document has been adapted.

- do not 'insert' when replying to e-mail, just type your comments above the original message and leave space between headers of original message and your signature
- use a signature block containing important contextual information so it is easier to trace the sender

cc) Managing e-mail messages

- ensure that the inbox is well managed, so when you receive a message decide if it needs to be saved and if so put it in the right folder
- if no special system exists to store messages, create directories for e-mails that have to be preserved to make tracing easier; make sure incoming and outgoing messages are kept in the same directory
- never paste content of message into another application and delete the original message as this would seriously damage both the authenticity and the integrity of the document (metadata[10] will get lost)

dd) Incoming or outgoing e-mail (internal and external)

This distinction has a different character to the classifications below, but is nonetheless relevant to the regulations for dealing with e-mail. A difference between internal and external e-mail can also be made in this category, distinguishing between electronic messages exchanged within an organisation and messages exchanged with outside parties.

ee) Official e-mail versus private e-mail

E-mail that an employee sends or receives as part of his/her job is official e-mail. E-mail that an employee sends or receives as a private individual, which is not related to the fact that the employee holds office in the organisation, is classified as private e-mail.

ff) E-mail to be preserved versus e-mail to be destroyed

If an e-mail message is functional, a decision has to be taken as to whether it is eligible for preservation. In principle, the same criteria as for 'normal' paper post apply here too.

c) Archiving of documents and e-mail

It is advised to save the documents and e-mails in the original version with the program in which it is made, because it is not known what programs can do in the future with 'old' (digitally archived) versions of documents and e-mails. It is also recommended to use a generally accepted format, and to use this same format for all documents and e-mails. When archiving documents and e-mails, it should be kept in mind that both the preservation of their legibility for the future and the safeguarding of the documents and e-mails in their original versions are important.

VII. Awareness of hidden data in files and documents

It is important to be aware that electronic documents and other computer files often carry additional information which renders information about the document or about its purported author, and that may be open or hidden, e.g. author, date and time of creation and last change, template used and such like. Depending on the nature of information and the context in which it later appears, the information may be useful, harmless or embarrassing, potentially dangerous or lead to an accidental disclosure of confidential information or information not intended for the recipient of the document. On the other hand, such data could also be useful or even vital to keep for a lawyer. In this case, the lawyer would need to take steps to preserve the metadata and to not to let it out to other parties.

a) Document re-use and information disclosure

Lawyers are experts in reusing documents, and it is very common to use a document as a starting point when creating another document in another case for another client, and the new document as a

[10] See under 4.

new starting point in yet another case for yet another client. If the lawyer is not aware of the existence of hidden data, it is possible that the recipient of the last version of the document, by analysing the hidden data, can tell who the original document was created for and which changes or amendments have been made by the various individuals having reviewed it. Copying the contents of a document and pasting them into a new document is not a reliable method to avoid that hidden data are following the document, as some hidden data are tied to a text in such way that pasting the text into a new document will also copy the original hidden data.

b) Multiple versions of content

The "Track Changes" function in Microsoft Word is useful to see changes made between document versions, but this feature must be used with due caution. "Track Changes" might be turned on, but the user might have change display switched off and as a result the changes made and by whom may be visible when change display is switched on again.

As a general guideline it is suggested that users always check whether "Track Changes" is used or not. The only way to discard saved changes between document versions is either to accept them or to reject them.

c) Regarding using PDF instead of Microsoft Word for Distributing Documents

PDF documents are a good alternative to documents in Microsoft Word format. For the most part, PDF is immune to the mentioned issues, as PDF documents really represent the document as it will be printed. Note however, that e.g. inserting a black or white box over a text will not remove the text, but place that box over the text and thus hide the text when printed. By removing the box, the text will be visible again. PDF documents do support a number of user-specified hidden data, but in practice use of such data is very unusual. To be on the safe side, however, it's recommended that "Document Properties" are checked before distributing the document.

It should be noted that there are different kinds of PDF document. A PDF document created by scanning text using a scanner or photocopier may contain only an image copy of the markings on the sheet of paper. The text in such a document cannot be searched using word-searching tools and cannot easily be cut and pasted into other documents. On the other hand, a PDF document saved from a word-processing program is usually stored as text and not simply as an image. Documents in this form require less storage space than image PDF documents. For these reasons, documents should generally be saved as text PDF documents (as opposed to image PDF documents) where they are to be stored in a searchable database, or where limiting file sizes (for example in e-mail attachments) is important.

d) Special tools to remove hidden data

There exist special computer software tools that analyse documents and can remove old versions of content or other hidden data. It is recommended that these tools are installed and used when distributing sensitive information in electronic documents. These tools can be downloaded for example from the web-site of Microsoft and be installed in the Office2003/XP version. In the Office 2007 version of Word, this is already a default tool (please see "Office button"/"Inspect Document").