B 05.2 INFORMATIONSSÄKERHETSGUIDE (23.11.2018, uppdat. 12.12.2019 och 24.9.2021)

Finlands Advokatförbunds styrelse har 23.11.2018 gett följande guide i anslutning till informationssäkerhet vid advokatverksamhet. En uppdatering av guiden har godkänts av styrelsen på styrelsemötet 12.12.2019 (punkterna 1 och 2) och 24.9.2021 (bilagorna 1 och 2).

Bakgrund

I advokatverksamhet hanteras stora mängder konfidentiell information. En advokat ska enligt punkt 11.6 i de vägledande reglerna sörja för datasäkerheten (informationssäkerheten) vid byrån så att inte utomstående olovligen kan skaffa sig tillgång till uppgifter om klienterna. Dessutom har en advokat många andra skyldigheter, vilkas verkställande kräver en tillräcklig nivå på informationssäkerheten. Informationssäkerhetens betydelse understryks ytterligare, då största delen av materialet och kommunikationen i anslutning till advokatverksamheten har blivit elektronisk, processerna har digitaliserats och risken för datatekniska informationsläckage därigenom har ökat.

Med informationssäkerhet avses i denna guide att information, datasystem och kommunikation ska skyddas på ett behörigt sätt. Informationens konfidentialitet, integritet och tillgänglighet skyddas mot fel av olika slag, naturföreteelser samt hot och skador orsakade av uppsåtligt eller oaktsamt handlande.

I denna guide genomgås exempel på olika risker som riktar sig mot informationssäkerheten och som i advokatverksamhet ska beaktas. Med de tekniska lösningar som används, byråns rutiner och utbildning av personalen kan informationssäkerheten påverkas. Guiden fungerar som grund för planering av advokatens egna informationssäkerhetsförfaranden. Dessutom bör det observeras att om exempelvis någon åtgärd är förbjuden i denna guide, men om åtgärden i vissa fall eller under vissa omständigheter kan genomföras på ett informationssäkert sätt, så behöver inte advokaten lämna detta informationssäkra förfarande ogjort endast på grund av att man i denna guide rekommenderat att åtgärden ska undvikas.

Vid bedömningen av kraven på en tillräcklig informationssäkerhet ska särskilt typen och arten av de uppdrag som denna advokatbyrå sköter, betydelsen och känsligheten av informationen i anslutning till uppdragen samt verksamhetens omfattning och den bredare informationssäkerhetsorganisationen som denna eventuellt möjliggör beaktas. För en byrå som sköter privatpersoners ärenden kan det viktiga gällande informationssäkerheten vara att skydda sig mot felsituationer och eventuella inbrottsförsök

i lokalerna, medan en byrå som sköter stora uppdrag inom affärsjuridiken också ska vara beredd på mer professionella försök till dataintrång.

1 Utbildning av personalen och revision

Advokaten ska se till att byråpersonalen får en uppdaterad och tillräcklig utbildning för en informationssäker användning av utrustning och ICT-tjänster samt för informationssäker elektronisk kommunikation. Vid utbildningen ska också informationssäkerhetsanvisning (B 5.1) beaktas utöver denna guide.

Med en informationssäkerhetsrevision identifierar en utomstående bedömare ifall information som är viktig med tanke på affärsverksamheten har skyddats tillräckligt med tanke på risker och bevarandet av advokatsekretessen. Vid revisionen utreds brister i anslutning till administrationen och genomförandet av informationssäkerheten för datasystem samt utvecklingsbehov för dessa. Vid revisionen ska förpliktande informationssäkerhetskrav, såsom den ovan nämnda informationssäkerhetsanvisningen och denna guide samt även allmänna principer och allmän praxis inom informationssäkerhet beaktas. Informationssäkerhetsrevisionen ska göras tillräckligt ofta med beaktande av byråns storlek och affärsrörelsens omfattning samt de förändringar som skett i byråns informationssäkerhetsomgivning – exempelvis lansering av nya system eller en flyttande av lokalerna. Den kan genomföras exempelvis som en del av revisionen eller som en separat konsultering.

Kunder eller andra utomstående parter kan inte utföra en revision av advokatbyrån till exempel genom att direkt eller via mellanhänder beställa en revision, där revisionsrapporten överlåts till kunden eller annan utomstående part, eftersom detta kan äventyra andra kunders konfidentiella uppgifter samt advokatbyråns informationssäkerhet. En rapport av allmän karaktär som upprättats på basen av en revision som beställts av advokatbyrån eller annan framställning som beskriver nivån av informationssäkerheten, kan enligt advokatbyråns bedömning överlåtas eller presenteras för kunden eller på annat vis hållas synlig för allmänheten. (12.12.2019)

2 Externa granskningar och begäran om information (12.12.2019)

Granskningar eller begäran om information som angår advokatbyrån eller advokatverksamheten och som avser uppgifter som samlas och överlåts till kunder, serviceleverantörer eller andra utomstående parter och som gäller praktikaliteter kring advokatverksamheten, kundrelationer eller uppdrag, kan inte utföras. Detta betyder inte, att kunden inte kunde begära information eller dokument som gäller kundens egna kundrelation och uppdrag. Också en av kunden begärd granskning, eller bredare

informationsbegäran angående praktikaliteter kring advokatverksamheten, kan äventyra den konfidentiella behandlingen av andra kunders uppgifter. För att trygga information som omfattas av advokatens tystnadsplikt, ska samtycke till denna typs begäranden inte ges. (12.12.2019)

3 Lokaler

3.1 Planering av lokalerna och besökares möjlighet att röra sig i dem

Inbrotts-, brand- och andra liknande skador på lokalerna bör förebyggas. Lokalernas låssystem ska skötas med bedömning av helheten på ett lämpligt sätt och med beaktande av annan verksamhet som försiggår i byggnaden och de risker som den förorsakar. Ett enskilt arbetsrum behöver inte nödvändigtvis vara låsbart, om exempelvis gångarna till den delen av kontoret eller byggnaden som arbetsrummet ligger i är låsta. Byrån ska ha ett larmsystem som dimensionerats med beaktande av storleken på lokalerna. Larmsystemet kan utgöra en del av byggnadens allmänna larmsystem. I kontorsbyggnaden kan det dessutom finnas behov av att ordna separat bevakning beroende på bland annat byråns eller verksamhetsställets totalareal och läge.

Möjligheten för klienter och andra utomstående personer att röra sig och vistas i lokalerna ska planeras så att inte byråns informationssäkerhet äventyras. Detta måste även beaktas vid planeringen av konferensrum. Klienter och andra utomstående personer ska tas emot när de anländer till byrån och personalen ska visa dem till rätt ställe, så att de inte under besöket på egen hand kan bekanta sig med material som omfattas av advokatsekretessen. Man bör särskilt kunna identifiera personer som utför serviceuppgifter och vid behov ska serviceåtgärderna övervakas. Med externa tjänsteleverantörer, t.ex. städare, servicepersoner eller tjänsteleverantörer ska ett skriftligt sekretessavtal ingås.

Om byrån har många anställda kan till exempel passersedlar eller andra ID-kort användas för att identifiera dem. Passertillstånd, nycklar och elektroniska passerrätter ska samlas in genast när anställningen upphör.

3.2 Placering av utrustning och hantering av post

Byråns utrustning ska placeras så att utomstående inte kommer åt att läsa exempelvis de anställdas skärmar, utskrivna handlingar eller andra meddelanden som kommer till eller skickas ut från byrån. Vid hanteringen av post i pappersform bör man också beakta kraven på informationssäkerhet. Hanteringen av all slags meddelanden och annat material som används inom advokatverksamhet ska helst inte placeras i entréhallar eller mottagningsrum.

Advokatbyråns servrar ska placeras i sådana låsbara rum eller skåp, som endast särskilt utsedda personer har åtkomst till.

3.3 Förvaring av material

Förvaringen av handlingar och annat material ska ordnas så att de inte i onödan kan ses av andra personer. Handlingarnas förvaringsutrymmen ska vara tillräckligt skyddade.

4 Skydd av utrustning som innehåller konfidentiellt material

4.1 Datorer

Eftersom man i advokatverksamhet regelbundet hanterar konfidentiellt och sekretessbelagt material, är regeln att informationen i datorers alla lagringsmedier (t.ex. hårddisken) ska krypteras. Bärbara datorer bär en större risk att bli föremål för stöld än stationära datorer och därför ska informationen i bärbara datorers lagringsmedier alltid krypteras. Krypteringen försvårar åtkomsten till den sparade informationen, om lagringsmediet kommer i fel händer.

Datorerna ska låsa sig automatiskt, om de inte används efter en kort tid. En dator ska också låsas, om datorn blir utan övervakning exempelvis under en paus. I synnerhet datorer i entréhallar och gästrum ska låsas genast om man avlägsnar sig från platsen även om det enbart är för en kort tid. Då datorer eller annan utrustning används utanför byrån ska man se till att förbipasserande eller utomstående personer i närheten inte kan se den information som visas på skärmen. En person som regelbundet hanterar konfidentiell information på allmänna platser eller i kollektivtrafiken ska installera ett sekretessfilter på sin utrustning, som gör att information på skärmen inte syns till andra än användaren av utrustningen eller på annat sätt effektivt skydda den information som visas på skärmen.

En apparat som är avsedd för advokatverksamhet ska alltid i första hand användas för arbetssyften. Av orsaker som har att göra medinformationssäkerhet och sekretess ska man inte tillåta att andra personer, såsom familjemedlemmar, använder datorn. Endast för arbetet nödvändiga och säkra program ska installeras i datorn. Likaså ska man endast besöka för arbetet nödvändiga och säkra webbplatser med datorn.

4.2 Mobila enheter

I telefoner och pekdatorer sparas ofta information som används inom advokatverksamheten eller så kan åtkomst till olika tjänster som används inom

advokatverksamheten fås genom telefonens nätanslutning, dessa innehåller konfidentiell och sekretessbelagd information. Mobila enheter kan innehålla kalenderanteckningar, information om kundrelationer, adressböcker, telefonloggar och annan information som omfattas av advokatsekretessen. Mobil enheten ska vara en sådan modell som har tillräckliga informationssäkerhetsfunktioner för advokatbruk.

En mobil enhet ska förvaras omsorgsfullt och den ska låsa sig automatiskt, om den inte används på en kort tid. Användningen av den mobila enheten ska vara möjlig endast efter en tillförlitlig identifiering (se punkt 6). Utöver att den mobila enheten ska vara låsbar ska även den information som sparas i den krypteras. I den mobila enheten ska även aktiveras möjligheten att radera information, att lokalisera telefonen och att låsa den på distans, om telefonen bjuder på denna möjlighet. Dessa funktioner kan också tas i bruk i mobila enheter med en tredje parts programvara och detta rekommenderas särskilt i större byråer.

4.3 Uppdatering av operativsystem och program

Operativsystem för datorer och mobila enheter samt annan utrustning som används ska utan onödigt dröjsmål uppdateras alltid när det finns tillgång till nya uppdateringar. I operativsystemen ingår en automatisk uppdateringsfunktion, som bör hållas påkopplad och genom vilken tillverkaren ofta även distribuerar informationssäkerhetsuppdateringar. I stället för automatisk uppdatering av operativsystemet kan uppdateringar också installeras genom byråns centraliserade underhåll av datasystem. Uppdateringar ökar operativsystemets säkerhet i datorn. Uppdateringar ska endast skaffas av den ursprungliga leverantören av programmen och från en säker källa. En enskild uppdatering kan emellertid framskjutas, om det inte äventyrar informationssäkerheten och det är nödvändigt för att säkerställa en kontinuerlig funktionalitet exempelvis vid väntan på att andra program uppdateras.

Utöver operativsystemen ska program och applikationer som används uppdateras, då nya uppdateringar är tillgängliga för dem. Uppdateringar kan ofta installeras så att de uppdateras automatiskt.

Om det inte längre kan fås uppdateringar till det operativsystem som är i användning eller till ett sådant program som kan utgöra en informationssäkerhetsrisk ska det bytas mot ett nyare eller vid behov till ett annat program.

4.4 Externa lagringsmedier

Externa lagringsmedier (t.ex. extern hårddisk eller minnespinne) används numera exempelvis vid överföring av stora materialmängder, i synnerhet om materialet inte lätt kan överföras via en internetförbindelse. Det finns allvarliga

informationssäkerhetsrisker i samband med externa lagringsmedier, som advokaten ska beakta. Externa lagringsmedier kan bli föremål för stöld eller förkomma. Vid användning och förvaring av lagringsmedier ska man se till att konfidentiell information i dem är skyddat.

Vid användning av externa lagringsmedier rekommenderas att man väljer ett sådant lagringsmedium som innehåller en krypteringsmöjlighet och andra eventuella informationssäkerhetsegenskaper, såsom möjlighet att förstöra informationen. Alternativt ska de filer som överförs till lagringsmediet krypteras separat.

Externa lagringsmedier kan också vara riskutsatta för virus och skadliga program. Ett lagringsmedium som ägs eller används av en utomstående ska inte kopplas till utrustning som används inom advokatverksamheten, utan att man först säkerställer att det kan göras tryggt.

En advokat ska särskilt försäkra sig om att ett externt lagringsmedium tas ur bruk på ett informationssäkert sätt (se punkt 13 nedan)

5 Skydd av nätförbindelser

Endast sådan utrustning som används inom advokatverksamheten ska ha åtkomst till advokatbyråns interna nätverk. Detta kan verkställas med olika slags utrustning eller genom metoder som verifierar användaren, exempelvis med register över apparater som finns i katalogtjänsten (AD), genom användning av personifierande enhetsadresser (MAC-adress) som fastställts i nätverksenheten, med certifikat eller genom att förhindra anslutning till nätanslutningar genom att täcka över anslutningarna (i allmänna rum). En advokatbyrås nätverk kan också vara trådlöst, ifall det har skyddats på ett behörigt sätt.

I en advokatbyrå kan det också finnas ett separat öppet nätverk som är avsett för att ge besökare nätförbindelse. Det nätverk som är avsett för klienter ska hållas åtskilt från det nätverk som byrån själv använder och utomstående får inte ha åtkoms till byråns interna information eller system via anläggningen.

Nätförbindelse kan också skapas via nätverk utanför advokatbyrån och offentliga nätverk, exempelvis hemma eller på hotell. Om nätförbindelsen är personalens egen och den används regelbundet i arbetet, ska den i regel ha samma informationssäkerhetsnivå som byråns nätverk. Vid användning av ett utomstående nätverk och sporadisk användning av ett eget nätverk ska informationssäkerheten säkerställas genom användning av krypterad förbindelse. En krypterad förbindelse kan bildas exempelvis som Virtual Private Network (VPN) eller Secure Shell (SSH) -förbindelse. Vid behov

ska mer information om skyddslösningar som lämpar sig för byrån inhämtas av tekniska experter.

Av ett trådlöst nätverk som är avsett för både internt och klienters bruk förutsätts åtminstone lösenordsbaserad identifiering och krypterad nättrafik.

6 Användarnamn och lösenord

En användare kan identifiera sig i advokatbyråns system och utrustning genom att använda användarnamn och lösenord, biometrisk identifiering, ID-kort, autentiseringsnycklar eller annan säker identifikationsmetod. Om möjligt ska i de lösningar och tjänster som är i bruk användas en tvåfaktorsautentisering (eller annan metod för ytterligare autentisering), så att man utöver ett lösenord eller annat användarspecifikt certifikat ytterligare använder ett annat identifikationssätt.

Det lösenord som används ska vara tillräckligt informationssäkert. Det är allmänt att datorstyrda program försöker knäcka lösenord och på grund av detta är ett långt lösenord som består av olika tecken som inte innehåller teckensträngar eller ord som är lätta gissa (såsom byråns namn eller det egna födelseåret), i allmänhet det mest informationssäkra. Samma lösenord ska inte användas på nytt. Lösenordet för den egna arbetsstationen och de viktigaste tjänsterna i advokatverksamheten ska bytas ut regelbundet.

Ett lösenord kan också avslöjas för en utomstående genom att personen ser lösenordet då det matas in eller om det används i någon annan tjänst som har utsatts för dataintrång. Lösenordet ska vid behov skyddas fysiskt vid inmatning och det får inte avslöjas för någon. Av ovan nämnda orsak får ett lösenord som används i advokatbyråns nätverk eller arbetsstationer inte användas som lösenord i internettjänster och skall olika lösenord användas i samtliga tjänster där man hanterar material med nära anknytning till advokatverksamheten.

6.1 Nätfiske

Nätfiske (phishing) betyder att någon på olaglig väg försöker få uppgifter, såsom nätbanks- eller användarlösenord, genom att locka mottagaren att ge dem, exempelvis genom bluffwebbplatser som ser äkta ut eller per telefon.

Avsändarinformationen i meddelandet kan vara förfalskat, dvs. meddelandet har inte nödvändigtvis skickats av den nämnda avsändaren. En bilaga eller en länk kan vara något helt annat än vad som anges i meddelandet eller filens namn.

Undvik att svara på alla ovanliga kontakt- eller inloggningsuppmaningar, som du inte själv begärt om. Ge aldrig dina identifieringsuppgifter eller ditt lösenord genom en nättjänst, ett okrypterat meddelande eller per telefon.

7 Informationssäkerhetsprogram och brandvägg

7.1 Virusbekämpning och förhindrande av skadliga program

Det finns många typer av virus och skadliga program. De största riskerna orsakas av virus som avsiktligt förstör eller låser information så att den blir otillgänglig för användaren, ger utomstående tillgång till informationen eller som samlar in information och skickar den till sin värd. Vissa skadliga program kan också kräva betalning för att informationen ska återställas.

En advokatbyrå ska ha ett fungerande och uppdaterat antivirusprogram som förhindrar att virus och andra skadliga program smittar ner byråns system och datorer. Programmet ska uppdateras automatiskt. Virusbekämpningen ska vid behov också installeras på mobila enheter. Ett antivirusprogram ska gå igenom inkommande e-postmeddelanden samt filer och program innan de öppnas eller åtgärdas. Dessutom ska advokatbyråernas utrustning kontrolleras regelbundet mot virus och skadliga program.

Det är viktigt att inte ens öppna e-postmeddelanden från okända avsändare, i synnerhet om rubriken eller innehållet ser misstänkt ut, och framför allt inte öppna länkar eller bilagor till meddelandena.

Man ska undvika att med datorer som används i advokatverksamhet besöka sådana webbsidor där risken för att smittas av skadliga program är större. Om skötseln av ett uppdrag kräver besök på sådana webbsidor, ska advokaten särskilt noggrant försäkra sig om sin informationssäkerhet, exempelvis genom att för åtgärden använda en dator eller mobil enhet som är åtskild från uppdragsarbetet.

Det finns också skäl att vara kritisk till reklam, länkar och program som erbjuds på webbsidor som i och för sig är sakliga. Advokatbyrån ska också se till att de datorer och den utrustning som personalen använder utanför byrån vid skötsel av uppdrag i anslutning till advokatverksamheten har ett ändamålsenligt antivirusskydd.

Vid misstanke om skadliga program eller virus i utrustning ska den omedelbart kopplas bort, tills den är rengjord eller man säkrat att den är ren.

7.2 Skydd av nättrafik

En brandvägg behövs för att skydda advokatbyråns nätverk och datorer från angrepp som kommer utifrån (internet). Syftet med en brandvägg är att den bara släpper igenom önskad nättrafik och förhindrar skapandet av otillåtna förbindelser med utrustning som är kopplad till det interna nätet.

En advokatbyrå ska ha en brandvägg. Brandväggen kan vara en programvara eller inbyggd i utrustningen. Ofta är det tillrådligt att bygga ett brandväggssystem som kombinerar båda alternativen. Programvaran och utrustningen ska hållas funktionsdugliga och uppdaterade.

8 Lagring av handlingar och åtkomsten till information

Advokater är skyldiga att spara och förvara korrespondens som gäller deras uppdrag. Skyldigheten kan också uppfyllas genom att korrespondensen lagras i elektronisk form på ett informationssäkert och säkrat sätt. Det är mer informationssäkert att lagra filer på en server än på särskilda anordningar. Gällande bevaringstider läs också B 10 Anvisning gällande bevarande av handlingar.

Bara de personer som behöver eller som kan behöva den konfidentiella informationen för sina arbetsuppgifter ska ha tillgång till handlingarna i fråga. Inom byrån ska åtkomsten till handlingar även vid behov begränsas; detta är nödvändigt speciellt när det gäller om insiderärenden.

9 Säkerhetskopiering

Genom säkerhetskopiering kan man kontrollera risker som orsakas av att information förstörs, förändras (som kan bero t.ex. på att utrustningen går sönder eller förstörs), att utrustningen stjäls, att virus eller skadlig programvara installeras eller att användaren av misstag raderar informationen. Säkerhetskopiering ersätter inte en behörig arkivering av handlingar, eftersom arkivet med handlingar också ska säkerhetskopieras.

9.1 Information som ska säkerhetskopieras

Central information som gäller advokatverksamheten ska säkerhetskopieras. Det rekommenderas att åtminstone följande uppgifter säkerhetskopieras:

- Information som uppkommit i arbetet med all slags utrustning, inkl. mobila enheter, och som ännu inte arkiverats
- ärendehanteringssystem och faktureringsuppgifter
- e-postmeddelanden och eventuella andra kommunikationslösningar som används
- elektroniska kalendrar och kontaktinformation
- arkiverade handlingar och annan arkiverad information

Om informationen har lagrats i externa tjänster av olika slag eller molntjänster, ska man se till att det i den köpta tjänsten ingår tillräcklig säkerhetskopiering. Vid behov ska fysiska säkerhetskopior tas av dessa tjänster eller så ska informationen säkerhetskopieras mellan de olika tjänsterna.

9.2 Metoder för säkerhetskopiering och förvaring av information

För säkerhetskopiering finns ett flertal olika tekniska verktyg och applikationslösningar. Ett alternativ är externa säkerhetskopieringstjänster som innebär att informationen skickas via nätet till tjänsteleverantörens server. Fördelen med en sådan tjänst kan anses vara att informationen förvaras utanför byrån på ett annat ställe än den information som ska säkerhetskopieras. Då avtalet ingås ska alla de aspekter beaktas som i regel är förenade med användningen av externa tjänster och behovet av att kunna skicka information på ett säkert sätt. Om säkerhetskopior inte görs i en molntjänst, rekommenderas det att säkerhetskopior förvaras på ett säkert ställe utanför byrån eller den egentliga lagringsplatsen ifall det inte finns en separat lämplig och trygg bevaringsplats.

9.3 Frekvens för säkerhetskopieringen

Man bör se till att informationen säkerhetskopieras regelbundet. Säkerhetskopieringen ska i regel ske automatiskt, så att den inte är beroende av arbetssituationen eller personalens egen aktivitet. Om säkerhetskopieringen endast gäller ändringar som gjorts efter föregående säkerhetskopiering, ska man regelbundet också ta en komplett säkerhetskopia på hela materialet för att säkerställa att säkerhetskopiorna är fullständiga.

Advokaten ska säkerställa att säkerhetskopieringen av byråns information fungerar såsom avsett och att informationen snabbt och problemfritt kan återställas.

10 Köp och utläggning av ICT-tjänster

I advokatverksamhet är det ofta nödvändigt att anlita externt ICT-stöd för att säkerställa teknisk kompetens men också för att köpa IT-tjänster (såsom molntjänster) av en extern leverantör. I båda fallen aktualiseras informationssäkerhets- och dataskyddsfrågor, som advokaten måste beakta.

10.1 Externt tekniskt stöd

När en advokatbyrå anlitar externt tekniskt stöd ska behöriga sekretssavtal ingås med tjänsteleverantören. Stöd kan användas för exempelvis advokatbyråns maskinvarumiljö och för att bygga upp de system som används, för underhåll, service, bedömning av nivån på informationssäkerheten, användarstöd och annat arbete som kräver tekniskt stöd.

Leverantören av det tekniska stödet ska inte ha onödigt omfattande åtkomst till den information som används inom advokatverksamheten. Åtkomsten ska begränsas så att den är så knapphändig och kortvarig som möjligt.

10.2 Köp av ICT-tjänster

Vid köp av ICT-tjänster bevaras, hanteras och överförs information som omfattas av advokatsekretessen med servrar el-ler tjänster som advokaten inte uteslutande besitter. Många företag erbjuder tjänster, där advokatbyråernas sekretessbelagda information används och bevaras på tjänsteleverantörens server. Typiska tjänster som utnyttjar extern serverkapacitet är e-post, webbsidor, säkerhetskopiering, elektroniska kalendrar, fakturering, klient- och uppdragsregister eller lagringsutrymme på nätet. Anlitandet av externa servrar är i vissa fall, t.ex. för webbsidor, en förnuftig lösning och ibland också den enda fungerande lösningen. Tjänsterna kallas ofta molntjänster eller SaaS-tjänster (Software as a Service).

Vid anskaffningen av tjänster ska advokaten särskilt uppmärksamma frågan om dels de krav som sekretessen ställer, dels hur advokatbyrån ska organiseras på ett ändamålsenligt sätt. När man väljer tjänsteleverantör är det absolut nödvändigt att försäkra sig om att tjänsteleverantören till fullo förbinder sig att iaktta sekretessen. Bara den advokat som skaffar tjänsten samt advokatbyråns personal ska ha tillgång till informationen.

Genom ett sekretessavtal med tjänsteleverantören ska man säkerställa att informationen hålls hemlig. Tjänsteleverantörens personal ska vid normala situationer förhindras åtkomst till advokatens uppgifter. Tjänsteleverantören ska kunna erbjuda en teknisk informationssäkerhet av tillräckligt hög standard. Utomståendes möjlighet att komma åt informationen ska förhindras med hjälp av tekniska lösningar och

bevarandet av informationen ska säkras. Avtal ska ingås gällande tillräcklig nivån på servicen så att advokaten har en tillräckligt tillförlitlig tillgång till sitt material när som helst. Om advokatens IT-kunskaper inte är tillräckliga för att bedöma nivån på informationssäkerheten, ska en extern teknisk expert anlitas för att bedöma tjänsten.

Vid valet av tjänsteleverantör bör vikt fästas bland annat vid tjänsteleverantörens referenser, certifikat, bakgrund och soliditet samt servrarnas etableringsland. Tjänsteleverantörens servrar kan finnas i olika delar av världen och den teknik som tillämpas inom tjänsten kan grunda sig på delning och kopiering av informationen till flera serverfarmer som eventuellt finns i olika länder eller världsdelar. Läs också anvisningarna som gäller behandling av personuppgifter i advokatverksamhet, ifall personuppgifter överförs utanför EES-området.

En del av molntjänsterna är mycket lätta att ta i bruk. Tjänsteavtalet om att börja använda en nättjänst ingås ofta exempelvis genom att användaren klickar på en länk eller skapar användarnamn, varvid användaren meddelar att han eller hon godkänner tjänsteleverantörens villkor. Vid advokatverksamhet går det emellertid inte att börja använda vilken molntjänst som helst, utan tjänstens lämplighet – även med beaktande av informationssäkerheten och dataskyddet – ska bedömas från fall till fall.

Å andra sidan kan en molntjänst vara en mer informationssäker lösning än att en advokatbyrå själv börjar skapa den serverinfrastruktur som informationssäkerheten kräver. Fördelen med molntjänster är att det bara kostar en bråkdel att anlita experter på IT-teknik och informationssäkerhet jämfört med vad underhållet av tjänsterna skulle kosta om det erbjöds för egna datorer.

Med ändamålsenlig kryptering av nättrafiken och tillförlitlig identifiering i molntjänsten, är det möjligt att förvara all konfidentiell information i tjänsten, utan att knappast alls behöva spara någon konfidentiell information i t.ex. en mobil enhet eller i datorn. Därigenom kan informationssäkerhetsskador minimeras, om en enskild apparat förkommer. Genom att använda molntjänster slipper man också de skador som orsakas av att utrustning går sönder.

Vid användning av molntjänster ska tjänsteleverantörens säkerhetskopiering motsvara det som byrån inom advokatverksamhet i punkt 9 förutsätter av sin egen säkerhetskopiering. Vid användning av molntjänster ska man emellertid också beakta risken att åtkomsten till molntjänsten överraskande kan upphöra eller att tjänsteleverantören slutar att tillhandahålla tjänsten.

10.3 Hot man bör förbereda sig på

Det kan hända att myndigheterna riktar en eventuell begäran eller ett eventuellt krav om information till den som tillhandahåller molntjänster och på detta sätt även får tillgång till advokatens konfidentiella information. Genom avtalsarrangemang och genom att försäkra sig om att tjänsteleverantörens tjänster har ett tillräckligt tekniskt genomförande samttjänsteleverantörens kompetens bör tjänsteleverantörens tjänsts förmåga att hålla isär information som hör till olika instanser säkerställas.

Omfattningen av hur tjänsteleverantören ger myndigheter och andra utomstående tillgång till uppgifterna kan bero på serverns etableringsland eller tjänsteleverantörens hemort.

11 Elektronisk kommunikation

Elektronisk kommunikation har även inom advokatverksamhet blivit den huvudsakliga kommunikationsformen. Elektronisk kommunikation förutsätter i regel klientens samtycke, vilket man emellertid numera ofta kan utgå ifrån på grundval av att klienten har kontaktat advokaten per e-post. Det rekommenderas att det i de avtalsvillkor som advokaten använder ingår ett omnämnande om att elektronisk kommunikation används vid skötseln av uppdraget.

Advokaten ska emellertid beakta att det är möjligt att olovligt följa elektronisk kommunikation eller att dekryptera deras krypteringssystem. Det är i praktiken omöjligt att heltäckande skydda elektronisk kommunikation från det att ett meddelande skapas tills mottagaren läser det samt arkiverar det efter läsningen. Detta ska advokaten beakta vid all elektronisk kommunikation och bedöma från fall till fall, när det går att använda e-post och när det inte kommer i fråga.

Vid behov ska advokaten handleda klienten att använda krypteringsmetoder för att skicka känsligt material.

11.1 Skydd av konfidentiellt meddelande

I lagen är elektronisk kommunikation skyddat på samma sätt som annan konfidentiell kommunikation. Nivån av skydd för konfidentialiteten är inte beroende av nivån på det tekniska skyddet eller ett meddelandes eventuella krypteringssystem eller avsaknaden av ett sådant.

Ett e-postmeddelande är konfidentiellt, om det inte uttryckligen är avsett för allmänheten, och en felaktig mottagare får inte på något sätt utnyttja innehållet i

meddelandet, även om det felaktigt har adresserats till honom eller henne. Meddelande om sekretess i samband med meddelanden är en praxis som rekommenderas advokater och det understryker meddelandets konfidentialitet för mottagaren, men ensidigt framställt kan det inte ålägga felaktiga mottagare skyldigheten att agera eller frånta avsändaren ansvaret för att informationen skickats till fel mottagare. (Lag om tjänster inom elektronisk kommunikation 136 §)

Modell för sekretessmeddelande:

Tämä viesti on luottamuksellinen ja tarkoitettu ainoastaan vastaanottajalle. Mikäli ette ole viestissä tarkoitettu vastaanottaja, olkaa hyvä ja ilmoittakaa siitä lähettäjälle ja tuhotkaa viesti välittömästi.

–-

Detta meddelande är konfidentiellt och avsett endast för mottagaren. I fall Ni inte är den avsedda mottagaren, vänligen informera avsändaren om detta och förstör meddelandet omedelbart.

This e-mail is confidential and is meant for the recipient only. If you are not the intended recipient, please inform the sender of this and destroy the message immediately.

11.2 Betydelsen av omsorgsfull verksamhet

Advokater ska lägga stor vikt vid att omsorgsfullt skydda kommunikationen i synnerhet när ett meddelande innehåller klientens eller motpartens personuppgifter eller om uppdraget är särskilt känsligt eller betydande. Inte ens om klienten godkänt användningen av ett kommunikationsmedium befrias advokaten från ansvaret för skyddet av personuppgifter och i regel ska ett meddelande som innehåller känsliga personuppgifter alltid skickas krypterat (se anvisningar om behandling av personuppgifter vid advokatverksamhet).

Merparten av felen i kommunikationen orsakas av avsändaren eller mottagaren själv exempelvis genom att skicka eller vidareförmedla meddelandet med fel sändlista. Vid elektronisk kommunikation ska advokaten handla med eftertanke och alltid försäkra sig om att ett meddelande skickas till rätta och på förhand kontrollerade e-postadress. Advokatens skyldighet att handla omsorgsfullt sträcker sig ända till att säkerställa val av rätt mottagare.

En advokat ska alltid då ett meddelande skickas försäkra sig om att mottagaren är den rätta. Dessutom är det bra att försäkra sig om att det i dokumenten inte innehåller metadata, som avslöjar exempelvis en annan klients namn eller uppgifter. Avlägsnandet av metadata kan automatiseras innan meddelandet skickas.

11.3 Tekniskt skydd vid elektronisk kommunikation

I nätverket överförs e-postmeddelanden ofta okrypterade och lagras i olika mellansystem, vilket gör att ett oidentifierat antal utomstående har möjlighet att behandla meddelandena.

För att verifiera egna e-postmeddelanden rekommenderas det att advokater skaffar ett eget domännamn (t.ex. advokatbyrå.fi), med vilken den egna kommunikationen skiljer sig från tjänster av allmän natur (såsom de vanligaste tillgängliga e-posttjänsterna).

E-postmeddelanden kan skickas mer informationssäkert i krypterad form. Då förmedlas meddelandet i krypterad form och endast mottagaren kan omvandla den till en läsbar text med en krypteringsnyckel. Det finns många slags krypteringstekniker och detta kräver olika former av beredskap hos mottagaren. En advokat är inte skyldig att enbart skicka krypterade e-postmeddelanden i sin verksamhet, men en advokat bör beakta begränsningarna gällande okrypterad kommunikation. Det rekommenderas att en advokat har den tekniska beredskapen och kompetensen att skicka och ta emot krypterade e-postmeddelanden.

De filer som skickas kan också separat skyddas med ett lösenord oavsett krypteringen av e-postmeddelandet. Lösenordsskyddet beror på filtypen och vilket program filen har skapats med.

11.4 Andra kommunikationskanaler

En advokat kan kommunicera i realtid med olika kommunikations- och direktmeddelandetjänster, som allt oftare är tillgängliga också via mobila enheter. En advokat ska ha en mycket omsorgsfull inställning till kommunikation och alltid försäkra sig om att mottagaren av meddelandet är korrekt identifierad och kontrollera om meddelanden som skickas via denna kanal är krypterade.

Det bör observeras att det även finns informationssäkerhetsrisker i samband med användandet av traditionella verktyg. Faxmeddelanden kan inte anses vara ett mer säkert sätt att skicka meddelanden än e-post. I faxmeddelanden kombineras ofta risken med elektronisk trafik och problem med informationssäkerheten hos pappersutskrifter. Även textmeddelanden kan användas i advokatverksamheten, men att skicka

konfidentiell information eller personuppgifter som ett textmeddelande rekommenderas inte. Textmeddelanden överförs i mobilnätet i allmänhet i okrypterad form.

12 Arkivering och förstöring av handlingar

Advokaten ska se till att handlingar arkiveras och förstörs på ett lämpligt sätt (se B 10 Anvisning för bevarande av handlingar).

Förstöringen av hemlig och konfidentiell information är lika viktigt som dess skyddande och annan behandling av den. Handlingar ska förstöras på ett informationssäkert sätt till exempel genom att anlita en utomstående tjänsteleverantör. Konfidentiella handlingar får aldrig kastas i en vanlig papperskorg, utan ska läggas i särskilda låsta kärl, från vilka de sedan tas och förstörs på ett säkert sätt. Advokaten ska ge byråns personal, städare och andra utomstående som hanterar byråns material anvisningar om hur handlingar behandlas på ett lämpligt sätt.

Handlingar förstörs antingen genom fysisk destruktion med till exempel en dokumentförstörare eller genom att försätta dem i en sådan form att innehållet i dem inte längre kan användas. Om man själv gör destruktionen, är det bra att kontrollera att handlingarna förstörs på rätt sätt, t.ex. att handlingarna strimlats tillräckligt fint.

13 Urdrifttagning av utrustning som innehåller information

Datorer, mobila enheter, externa lagringsmedier och annan utrustning som används inom advokatverksamhet kan innehålla konfidentiell information. Information som finns i utrustning som tas ur drift ska raderas på ett informationssäkert sätt, oavsett om utrustningen ska skrotas eller återanvändas.

Radering av alla filer från utrustning som tas ur bruk eller formatering av lagringsmedier är inte en tillräcklig åtgärd för trygga informationssäkerheten. Fysisk förstöring av lagringsmedier utgör inte heller en garanti för att informationen inte skulle kunna återställas. En säker radering av information ska göras med ett separat raderingsprogram, som säkerställer att informationen inte kan återställas. Information och utrustning kan också lämnas för att förstöras till företag som är specialiserade på området, i synnerhet om byrån inte är säker på hur information förstörs på ett säkert sätt. Destruktion av information kan också ingå i hyresavtal för leasingutrustning, men då ska man se till utrustningen inte exempelvis tillfälligt förvaras på ett sätt som är olämpligt med tanke på informationssäkerheten.

När en advokat tar ur bruk datorer, mobila enheter, externa lagringsmedier och annan utrustning ska informationen i dem alltid förstöras fullständigt. Detta gäller

- vid återlämning av leasad utrustning,
- utrustning som är avsedd för återanvändning/försäljning och
- utrustning som lämnas till destruktion.

14 Kontinuiteten i verksamheten

Advokaten ska se till att information som är nödvändig med tanke på kontinuiteten i byrån har dokumenterats i samlad form och att denna dokumentation finns tillgänglig för de parter som svarar för kontinuiteten. Se mer detaljerat B 10 Anvisning för arkivering, punkt 5.

BILAGA 1

ÅTGÄRDER FÖR ATT SKYDDA TJÄNSTEN OFFICE 365 / MICROSOFT 365 FÖR DATAINTRÅNG (24.9.2021)

Office 365/Microsoft 365 ger åtkomst till kontorstjänster av många olika slag och är därför intressant för datafiskare och knäckare. En advokat ska sköta om följande omständigheter för att förhindra datafiske och skydda tjänsten Office 365/Microsoft 365 ("365-abonnemang").

1. För advokatverksamhet ska förvärvas ett 365-abonnemang som är avsett för företagsanvändning i enlighet med licensvillkoren.

2. Flerstegsautentisering ska tas i bruk för alla som använder 365-abonnemanget, och autentiseringen ska ställas in så att den är tidsbestämd. Dessutom gäller det att säkerställa att det är möjligt att logga in i tjänsten om det uppkommer ett fel i autentiseringstjänsten (till exempel genom att skapa en byrålådeanvändare för vilken tvåstegsautentisering inte har införts).

3. 365-abonnemangets inloggningssida ska anpassas i enlighet med företagets visuella framtoning. På detta sätt är det svårare att vilseleda användare att mata in uppgifter på eventuella falska webbplatser.

4. Administratörskoder till 365-abonnemanget (systemadministratör) ska endast beviljas efter behov, och det gäller att utfärda så få administratörskoder som möjligt (t.ex. 1–2 st.) När personer inte längre behöver administratörskoder och andra användarkoder, ska dessa koder avlägsnas.

5. Användarna ska ges utbildning särskilt i syfte att förhindra de vanligaste händelserna som äventyrar 356-abonnemangets informationssäkerhet. Användaren bör minst vara förtrogen med följande: identifiering av den rätta inloggningssidan, identifiering av falska meddelanden, säker hantering av användarnamnet och lösenordet samt åtgärder om användaren blivit utsatt för bedrägeri eller försök till bedrägeri.

6. Lösenordet till 365-abonnemanget ska vara starkt och det ska inte användas i andra tjänster.

7. Möjligheten att nollställa lösenord på eget initiativ bör tas i bruk, om det i anslutning till nollställning av användarens lösenord blir nödvändigt att skicka ett nytt lösenord över en okrypterad förbindelse.

8. Endast administratören ska ha behörighet att skapa regler för vidaresändning av e-postmeddelanden. Syftet med detta är att förhindra att angripare vidaresänder alla e-postmeddelanden från ett användarkonto och följer upp kommunikationen på kontot.

9. Uppgifter som omfattas av förvaringsskyldigheten inom advokatverksamhet ska säkerhetskopieras på ett pålitligt sätt.

10. Åtgärder för att utestänga angripare från 365-abonnemanget ska planeras på förhand. Det är nödvändigt att utarbeta ett systematiskt sätt att komplett utestänga angripare från tjänsterna och att göra upp en kontrollista över åtgärder som eventuellt behövs (såsom avbrytande av förbindelserna till alla tjänster, anmälan till dataskyddsombudsmannen och andra instanser, kontroll av att byråns fakturor och kundernas kontouppgifter är oförändrade efter attacken).

11. Åtgärderna för att skydda mobilutrustning som tillhör dem som använder 365-abonnemanget ska vidtas åtminstone i enlighet med det som meddelas i Advokatförbundets informationssäkerhetsanvisning och -guide (kryptering av utrustningen, automatisk låsning osv.).

De skyddsåtgärder som beskrivs i denna bilaga kan också tillämpas på andra molntjänster som används i advokatverksamhet.

I fråga om mer tekniska detaljer se Cybersäkerhetscentrets guide Skydd mot nätfiske och dataintrång i Microsoft Office 365, som är avsedd för personer som ansvarar för dataadministrationen och informationssäkerheten i organisationer.

Denna bilaga till Informationssäkerhetsguiden har beretts i Finlands Advokatförbunds IT-utskott, som godkände innehållet 23.8.2021. Advokatförbundets styrelse godkände nya bilagor till guiden vid sitt sammanträde 24.9.2021.

BILAGA 2

Sekretessavtal (24.9.2021)

1. **Parter**

   Beställare:

   [Advokatbyrå Ab]

   [FO-nummer]

   [Adress]

   Avtalspart:

   _____

   _____

   _____

2. **Bakgrund och syfte**

   Beställaren är medlem i Finlands Advokatförbund och bedriver advokatverksamhet i enlighet med lagen om advokater (496/1958), nedan "Advokatlagen"). Advokat är en skyddad yrkesbeteckning och endast medlemmar i Finlands Advokatförbund får använda yrkesbeteckningen advokat.

   En advokat ska redbart och samvetsgrant utföra anförtrodda uppdrag och i all sin verksamhet iaktta god advokatsed (Advokatlagen 5 § 1 mom. och Finlands Advokatförbunds stadgar 33 §). En advokat har en sådan absolut och i tid obegränsad tystnadsplikt som avses i Advokatlagen 5 c §. Föreskrifter om sekretess finns också i andra lagar. Enligt punkt 11.5 i Finlands Advokatförbunds vägledande regler om god advokatsed ska advokaten se till att byråpersonalen liksom andra personer som regelmässigt eller tillfälligt utför tjänster för byrån iakttar sekretess- och tystnadsplikten.

Avtalsparten är villig att tillhandahålla Beställaren sina tjänster på ett sätt som avtalas separat. Beställaren kan i enlighet med bestämmelser som är förpliktande för Beställaren inte beställa eller använda Avtalspartens tjänster utan att Avtalsparten åtar sig att iaktta motsvarande sekretess- och tystnadsplikt som Beställaren själv är skyldig att iaktta. Avtalsparten är medveten om betydelsen av denna omständighet. För att fullgöra dessa åligganden avtalar Parterna om följande:

3. Avtalsvillkor

1. Beställaren och Avtalsparten har avtalat, avtalar eller avser att avtala om ordinarie eller tillfälliga tjänster (nedan "**Tjänsten**" eller "**Tjänsterna**") som Avtalsparten tillhandahåller Beställaren eller en part som Beställaren anvisat. Ett separat avtal ingås om produktionen av Tjänsten, och detta Avtal är en oskiljbar del av villkoren som gäller produktionen av Tjänsten. Detta Avtal tillämpas på alla Tjänster som beställs hädanefter, oberoende av vilka tjänster de är.

2. Alla uppgifter eller delar av uppgifter som gäller Beställarens klienter eller uppdrag, oberoende av vilka uppgifter de är och oberoende av i vilken form de presenteras eller har kommit till Avtalspartens kännedom i anslutning till genomförandet av Tjänster, är utan undantag absolut konfidentiella och sekretessbelagda (dessa uppgifter kallas nedan "**Advokathemligheter**"). För klarhets skull konstateras att även uppgifter som i övrigt är offentliga är Advokathemligheter.

3. Avtalsparten ska hemlighålla och behandla alla Advokathemligheter som konfidentiella ("**Avtalspartens Sekretess- och tystnadsplikt**"). Avtalspartens Sekretess- och tystnadsplikt gäller också alla de Advokathemligheter som eventuellt kommit till Avtalspartens kännedom i anslutning till Tjänster som genomförts innan detta Avtal undertecknades.

4. Avtalspartens Sekretess- och tystnadsplikt är evig och kan inte sägas upp på något sätt.

5. Om en lag som är direkt förpliktande för Avtalsparten, en bestämmelse på lägre nivå än lag som är förpliktande för Avtalsparten eller någon annan myndighetsföreskrift som är förpliktande för Avtalsparten eller ett serviceavtal mellan Avtalsparten och Beställaren ålägger Avtalsparten en mer omfattande sekretess- eller handlingsskyldighet än vad som avtalas i detta Avtal, inskränker detta Avtal inte Avtalspartens skyldigheter till någon del.

6. Om Avtalsparten och Beställaren i ett annat avtal avtalat om en sekretess- eller handlingsskyldighet som är mer begränsad än den skyldighet som avtalas i detta Avtal, iakttas detta Avtal till denna del.

7. Avtalsparten är skyldig att se till att varje enskild person som tillhör Avtalspartens personal, varje enskild person som deltar i genomförandet av de Tjänster som Avtalsparten levererar till Beställaren och varje annan person

som har åtkomst till Advokathemligheter personligen åtar sig att iaktta en sekretess- och tystnadsplikt som motsvarar Avtalspartens sekretess- och tystnadsplikt, om inte avtal om motsvarande sekretess- och tystnadsplikt ingåtts i personens arbetsavtal. Avtalsparten är skyldig att på Beställarens begäran uppvisa en kopia av ett sådant åtagande eller en annan redogörelse för fullgörandet av skyldigheten i enlighet med detta villkor.

8. Avtalsparten ska med nödvändiga tekniska och arbetsorganisatoriska lösningar se till att endast de personer som av nödvändighet och i syfte att genomföra Tjänster behöver åtkomst till Advokathemligheter har sådan åtkomst. Avtalsparten ska se till att ett tillförlitligt och aktuellt register förs över varje enskild person som har fysisk, informationsteknisk eller annan åtkomst till Advokathemligheter. Avtalsparten ska i den omfattning det är möjligt också se till att förbindelser som tas till Advokathemligheter övervakas med tillämpliga, bestående loggdata. Avtalsparten ska vägleda, informera och utbilda sin personal om vad Avtalspartens Sekretess- och tystnadsplikt innebär. Avtalsparten ska på Beställarens motiverade begäran ge Beställaren en kopia, ett utdrag eller en annan redogörelse över de register som förs och de logguppgifter som registreras.

9. Avtalsparten får inte återge, kopiera eller reproducera Advokathemligheter på annat sätt än vad som är nödvändigt för att genomföra en Tjänst som Avtalsparten tillhandahåller eller vad som uttryckligen och separat avtalats med Beställaren. Avtalsparten ska se till att alla kopior på Advokathemligheter förstörs efter att Tjänsten genomförts eller när kopiorna inte längre behövs för att genomföra Tjänsten, om inte Avtalsparten och Beställaren separat avtalat om att kopiorna ska arkiveras för Beställarens räkning.

10. Avtalsparten är inte berättigad att överlåta Advokathemligheter till tredjeparter, såsom till Avtalspartens underleverantörer eller Avtalspartens egna serviceleverantörer utan separat skriftligt avtal om detta med Beställaren. En sådan tredjepart ska dessutom åta sig att iaktta en sekretess- och tystnadsplikt som motsvarar den sekretess- och tystnadsplikt som avtalas i detta Avtal.

11. Avtalsparten ska vid genomförandet av tjänster och vid all behandling av Advokathemligheter iaktta en för sitt verksamhetsområde lämplig omsorg samt allmänt accepterade förfaranden.

12. Avtalsparten ska så snabbt som möjligt underrätta Beställaren om alla sådana omständigheter som Avtalsparten får kännedom om eller som Avtalsparten misstänker, såsom om brister, avvikelser, risker och motsvarande omständigheter som kan ha betydelse för fullgörandet av Avtalspartens Sekretess- och tystnadsplikt, oavsett om de gäller Avtalsparten, Avtalspartens personal eller tredjeparter.

13. Om husrannsakan eller annan inspektion som utförs av myndighet eller annan övervakande instans görs i Avtalspartens lokaler, informationssystem eller andra ställen där det finns eller kan finnas kopior av Advokathemligheter, ska Avtalsparten omedelbart informera den som utför inspektionen om att Advokathemligheter är befintliga och kontakta Beställaren så snart det är tillåtet.

14. Om Avtalsparten eller dess anställda eller något annat biträde bryter mot detta Avtal har Beställaren ensidig rätt att häva Avtalet om produktion av Tjänster med omedelbar verkan oberoende av bestämmelser om tidsbestämd tjänst. Beställaren är endast skyldig att erlägga betalningar som gäller Tjänster som levererats fram till hävningen av Avtalet.

15. Avtalsparten är medveten om att även en ringa försummelse av Avtalspartens Sekretess- och tystnadsplikt kan förorsaka Beställaren eller Beställarens klient eller andra instanser omätbart stor och överraskande skada. Avtalsparten är skyldig att ersätta Beställaren, Beställarens klient eller annan skadelidande för alla skador som Avtalsparten eller dess biträden förorsakar genom att bryta mot Avtalspartens Sekretess- och tystnadsplikt. Advokathemligheterna kan innehålla uppgifter vilkas röjande är straffbart enligt strafflagen.

16. Detta Avtal kan endast ändras skriftligen.

17. På detta Avtal tillämpas Finlands lag.

18. Tvister som föranleds av detta Avtal avgörs i den tingsrätt i vars domkrets Beställaren har sin hemvist.

[Återstoden av sidan har lämnats tom med avsikt. Underskrifterna görs på nästa sida.]

4. Underskrifter

Beställare

_____

Datum och ort

_____

Underskrift

_____

Namnförtydligande

Avtalspart

_____

Datum och ort

_____

Underskrift

_____

Namnförtydligande

Denna bilaga till Informationssäkerhetsguiden har beretts i Finlands Advokatförbunds IT-utskott, som godkände innehållet 17.9.2021. Advokatförbundets styrelse godkände nya bilagor till guiden vid sitt sammanträde 24.9.2021.