B 05.2 INFORMATIONSSÄKERHETSGUIDE (23.11.2018, uppdat. 12.12.2019, 24.9.2021 och 14.12.2023)

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) samt 14.12.2023 (punkterna Bakgrund, punkterna 1–3, 6–8, 10, 11, 13–15 samt bilagorna 3 och 4). Denna guide gäller från 1.1.2024.

Bakgrund (14.12.2023)

Advokaterna har en omfattande allmän tystnadsplikt som kallas advokathemlighet i fråga om sina klienters angelägenheter och uppgifter som de fått i sitt uppdrag. Advokaterna ska se till att advokathemligheten tryggas, eftersom det är en grundläggande rättighet för advokatens klient som baserar sig bl.a. på artikel 6 i Europakonventionen om rätten till en rättvis rättegång och artikel 8 som skyddar respekten för privatlivet och familjelivet. Bestämmelser om innehållet i advokathemligheten finns i Finland bland annat i lagen om advokater (5 c § i lagen om rättegång i brottmål) och i Vägledande regler om god advokatsed som är förpliktande för advokater (VR 3.4 och 4.3). I finsk lagstiftning har brott mot advokathemligheten straffrättsligt sanktionerats.

I advokatverksamheten behandlas stora mängder konfidentiell information som omfattas av advokathemlighet och andra sekretessplikter, såsom företagshemligheter. Enligt punkt 11.6 i Vägledande regler om god advokatsed ska en advokat sörja för informationssäkerheten vid byrån så att inte utomstående olovligen kan skaffa sig tillgång till konfidentiella uppgifter om klienterna. För att precisera informationssäkerhetsskyldigheterna har delegationen godkänt en informationssäkerhetsanvisning som är förpliktande för advokater. (B 05.1, 24.1.2019, ändr. 16.1.2020 och 9.6.2023, gäller fr.o.m. 1.1.2024).

Informationssäkerhetens betydelse accentueras ytterligare när största delen av det material och den kommunikation som hänför sig till advokatverksamheten har blivit elektronisk, processerna digitaliseras, användningen av artificiell intelligens ökar riskerna i anslutning till behandlingen av konfidentiella uppgifter och risken för attacker mot informationssäkerheten inom branschen 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.

När en advokat i advokatverksamhet använder till exempel system som baserar sig på artificiell intelligens, ska advokaten se till att klienternas konfidentiella uppgifter inte röjs eller förs till utomstående för behandling. Kopiering av data till allmänna

molnbaserade plattformar kan äventyra denna konfidentialitet, vilket innebär att advokaten måste försäkra sig om hur information om advokatverksamhet hanteras i olika system och tjänster.

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, men är också en kompletterande kommentar till den bindande anvisningen om informationssäkerhet. Det bör dessutom noteras att denna guide är av rekommendationskaraktär, dvs. om en åtgärd som är förbjuden i denna guide i ett visst fall eller under vissa omständigheter kan genomföras på ett informationssäkert sätt, behöver advokaten inte avstå från detta informationssäkra förfarande endast på grund av den rekommendation om undvikande som anges i denna guide.

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. Dataskyddet ska beaktas som en egen helhet, men en hög informationssäkerhet är en viktig del av fullgörandet av dataskyddsförpliktelserna. 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 (14.12.2023)

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, som denna guide kompletterar, och en eventuell informationssäkerhetspolicy som upprättats för byrån.

Som stöd för planeringen kan användas en utbildningsplan som till exempel fastställer: de kunskaper och färdigheter som behövs för att genomföra en informationssäker verksamhet, den utbildning som behövs, registreringar om genomförandet av utbildningen samt förvärvade kunskaper och färdigheter. Utbildningskraven kan variera mellan olika personalgrupper. På begäran ska det läggas fram en utredning om utbildningen, såsom om fortbildning (B 9).

2 Informationssäkerhetspolicy (14.12.2023)

En advokatbyrå med minst 10 anställda har en informationssäkerhetspolicy som godkänts av byråns högsta ledning.

I informationssäkerhetspolicyn presenteras de principer som styr informationssäkerheten och de centrala frågor som byråns ledning vill uppnå i fråga om informationssäkerheten och hur man bedömer om de önskade målen har uppnåtts. Informationssäkerhetsprinciperna har godkänts av byråns högsta ledning. Informationssäkerhetsprinciperna styr de informationssäkerhetsåtgärder som utförs vid byrån.

I policyn kan man beskriva byråns viktigaste informationssäkerhetsmål och sätten att ställa upp mer detaljerade informationssäkerhetsmål och bedöma hur de uppnås. Det lönar sig att beskriva de tekniska och detaljerade informationssäkerhetsåtgärderna i andra informationssäkerhetsanvisningar och -praxis, så att informationssäkerhetspolicyn vid behov också kan informera externa intressentgrupper om byråns informationssäkerhetsprinciper.

Informationssäkerhetspolicyn ska beskriva hur de informationssäkerhetskrav som gäller advokatverksamhet, särskilt med tanke på klienterna uppgifter, ska beaktas. Informationssäkerhetskrav kan utöver advokatverksamhet komma från klienternas ansvarsområden (t.ex. finansbranschen, hälso- och sjukvården, börsbolag som tillämpar insiderlagstiftningen, internationella aktörer). Dessutom hur man bedömer de risker som hotar byråns informationssäkerhet och hur man bemöter dem samt hur kontinuiteten i byråns verksamhet och informationssystem tryggas.

I policyn kan man beskriva de ansvariga aktörerna när det gäller planering, genomförande och underhåll av informationssäkerheten. Dessutom kan det antecknas att ledningens eller advokatbyråns delägare förbinder sig att genomföra, förbättra och resursera informationssäkerheten. I policyn kan man också beskriva informationssäkerhetsutbildningens principer, ansvar och hur man ska informera t.ex. andra tjänsteleverantörer om policyn så att de kan förbinda sig till samma nivå av informationssäkerhet.

3 Revision av informationssäkerheten (14.12.2023)

En advokatbyrå med minst 10 anställda ska regelbundet ordna en extern revision av informationssäkerheten. Dessutom ska en revision utföras om det görs ändringar i informationssäkerhets- eller kontorsmiljön eller i centrala system. Det ska föras bok över revisionerna.

Med hjälp av revision av informationssäkerheten identifierar en extern utvärderare om de uppgifter som är viktiga med tanke på affärsverksamheten är tillräckligt skyddade med tanke på riskerna och för att bevara advokathemligheten. Vid revisionen utreds brister i hanteringen och genomförandet av informationssystemens informationssäkerhet samt deras utvecklingsbehov. Vid revisionen ska man beakta de förpliktande informationssäkerhetskraven, såsom ovan nämnda informationssäkerhetsanvisning och denna guide, även de allmänna principerna och praxis för informationssäkerheten. Revisionen av informationssäkerheten ska utföras tillräckligt ofta med beaktande av byråns storlek och affärsverksamhetens omfattning samt med beaktande av förändringar i byråns informationssäkerhetsmiljö – exempelvis vid

lanseringen av nya system eller efter en flyttning av lokalerna. Den kan genomföras till exempel som en del av revisionen eller som separat konsultation.

Advokatbyråns klienter eller andra utomstående aktörer kan inte revidera en advokatbyrå till exempel så att klienten eller någon annan utomstående beställer en revision direkt eller via mellanhänder och rapporten om revisionen lämnas ut till klienten eller någon annan utomstående, eftersom detta kan äventyra andra klienters konfidentiella uppgifter samt advokatbyråns informationssäkerhet. En allmän rapport över en revision som advokatbyrån själv beställt eller något annat slutresultat som beskriver informationssäkerhetsnivån kan dock enligt advokatbyråns prövning lämnas ut eller visas för klienten eller annars hållas offentligt framlagt.

4 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, klientrelationer eller uppdrag, kan inte utföras. Detta betyder inte, att klienten inte kunde begära information eller dokument som gäller klientens egna klientrelation eller uppdrag. Också en av klienten begärd granskning, eller bredare informationsbegäran angående praktikaliteter kring advokatverksamheten, kan äventyra den konfidentiella behandlingen av andra klienters uppgifter. För att trygga information som omfattas av advokatens tystnadsplikt, ska samtycke till denna typs begäranden inte ges. (12.12.2019)

5 Lokaler

5.1 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 advokathemligheten. 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 passerkort eller andra ID-kort användas för att identifiera dem. Passerkort, nycklar och elektroniska passerrätter ska samlas in genast när anställningen upphör.

5.2 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.

5.3 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.

6 Programvara och tjänster för företagsändamål (14.12.2023)

Programvara och tjänster som används i advokatverksamhet ska vara avsedda för företagsbruk. Detta säkerställer för det första att programvaran och tjänsterna används i enlighet med licensvillkoren för dem. För det andra har programvara och tjänster på företagsnivå vanligen en högre informationssäkerhetsnivå, och detta bör särskilt beaktas vid valet av programvara.

Andra tjänster kan användas endast med klientens särskilda samtycke. Detta är ett undantag från den huvudregel som skrivits in ovan och kan t.ex. på konsumentklientens begäran innebära att klientens uppgifter lagras i den molntjänst som klienten anvisat. Advokaten ska dock se till att tjänsternas konfidentialitet och advokathemligheten inte därigenom äventyras.

7 Hantering av utrustning och åtkomst (14.12.2023)

De anordningar som används i advokatverksamhet vid en advokatbyrå med minst 10 anställda ska omfattas av utrustningshantering. Dessutom måste en lösning för hantering av åtkomst införas.

Vid utrustningshantering görs en förteckning över de anordningar som byrån använder och på dem kan centraliserat ställas in inställningar enligt anordningarna. Utrustningshanteringen ska omfatta de anordningar som används för advokatverksamheten, såsom bärbara datorer, telefoner och pekdatorer. Inom utrustningshanteringen bildar dessa anordningar en förteckning av anordningar med hjälp av vilket man kan följa de anordningar som används och deras livscykel.

Med hjälp av en åtkomsthanteringslösning kan man t.ex. begränsa tillgången till byråns informationssystem och uppgifter för annan utrustning än byråns egen samt ställa gemensamma specifikationer i inställningarna för byråns utrustning. Åtkomsthantering kan oftast definieras per enhet (enhetshantering, certifikat), per IP-adress (t.ex. kontorets IP-adressrymd) och per användare (användarförteckning). Åtkomsten kan begränsas inte bara till byråns omgivning utan också endast till de uppgifter som behövs i arbetsuppgifterna enligt personens befattningsbeskrivning, till exempel genom att användaren placeras i en viss användargrupp eller roll. I en åtkomsthanteringslösning kan trappor fastställas till exempel på basis av atypiskt beteende (en användare försöker kontakta en atypisk adress med en godkänd enhet, vilket kräver till exempel ytterligare verifiering, till exempel en advokats dator försöker logga in på nätet till exempel från utlandet, varvid användaren för att kunna logga in måste använda tvåfaktorsautentisering).

8 Skydd av utrustning som innehåller konfidentiell information (14.12.2023)

8.1 Datorer och servrar

Eftersom konfidentiella och sekretessbelagda uppgifter regelbundet behandlas i advokatverksamheten, ska utgångspunkten vara kryptering av uppgifterna i alla lagringsmedier (såsom hårddiskar). I fråga om bärbara datorer är risken för att bli utsatt för stöldbrott större än för stationära datorer eller servrar, och därför ska uppgifterna på lagringsmedierna alltid krypteras. Kryptering gör det svårare att få tillgång till den lagrade informationen om lagringsmediet hamnar i fel händer. Krypteringen skyddar innehållet i datamediet, oavsett om lagringsmediet missbrukas på grund av stöld eller på grund av att datorn återvinns. Därför måste även serverdiskarna krypteras.

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 med informationssäkerhet och sekretess ska

man inte tillåta att andra personer, såsom familjemedlemmar, använder datorn eller annan utrustning. Endast för arbetet nödvändiga och säkra program ska installeras i datorn. Likaså ska man endast besöka för arbetet nödvändiga och säkra webbplatser med datorn.

8.2 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 advokathemligheten. Som mobil enhet ska väljas 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.

Även i fråga om mobila enheter ska uppmärksamhet fästas vid de uppgifter som syns på skärmen. Man kan installera ett sekretessfilter på mobila enheter för att skydda den information som visas på skärmen.

8.3 Molntjänster, databaser och andra sammanställda datamaterial (t.ex. tabeller)

De uppgifter som lagrats i de molntjänster och databaser som används i advokatverksamhet ska vara krypterade. Redan vid upphandlingen av tjänster är det bra att säkerställa möjligheten att kryptera uppgifter och att den tas i bruk på rätt sätt.

Vid användning och anskaffning av molntjänster ska uppmärksamhet fästas vid att tjänsten erbjuder en tillräcklig nivå av informationssäkerhet, dvs. att uppgifterna är krypterade så att utomstående inte får tillgång till dem. I typiska kommersiella tjänster har man presenterat funktioner för kryptering av information som är mer avancerade än de applikationer som är avsedda för konsumenter, och även företagen strävar efter att på sina servrar skydda information som är avsedd för yrkesmässigt bruk betydligt effektivare än konsumentinformation. Om det finns en version av molntjänsten, till exempel med en AI-lösning, som innehåller mer omfattande säkerhetsfunktioner och som skiljer uppgifterna från andra användares uppgifter, ska en sådan version tas i bruk.

Tabeller, databaser och molntjänster som sammanställer klientuppgifter ska också skyddas med kryptering. I praktiken ska det i de tabeller som behandlar klientuppgifter anges ett lösenord för att förhindra att uppgifterna blir tillgängliga. De mest typiska tabellkalkylprogrammen använder stark kryptering för att blockera åtkomsten

till data och när lösenordsskydd har aktiverats blockeras åtkomsten till data om tabellen hamnar i fel händer. Databaser som hanterar klientdata ska krypteras. Beroende på databasen kan kryptering genomföras på olika sätt, men vid kryptering av databaser måste särskild uppmärksamhet fästas vid att de nycklar som frigör krypteringen också är tillräckligt skyddade, eftersom databaserna kan öppnas när nycklarna förenas med databaserna på samma sätt som okrypterade databaser.

8.4 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.

8.5 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 skyddad.

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 omsorgsfullt 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).

9 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 åtkomst 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.

10 Användarnamn och lösenord (14.12.2023)

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.

Enligt nuvarande uppfattning är det inte tryggare att regelbundet byta lösenord än att välja och hålla fast vid ett starkt lösenord. Detta beror på att behovet av att byta lösenord till slut torde leda till ett lösenord som är lätt att byta och komma ihåg.

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 olika ska lösenord användas i samtliga tjänster där man hanterar material med nära anknytning till advokatverksamheten.

10.1 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.

11 Informationssäkerhetsprogram, brandvägg och åtkomsträttigheter (14.12.2023)

11.1 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.

För att förhindra virus och skadliga program ska man inte öppna e-postmeddelanden från okända avsändare, om rubriken eller innehållet ser misstänkt ut, och framför allt ska man inte öppna länkar eller bilagor i meddelandena.

Man ska undvika att med datorer som används i advokatverksamhet besöka sådana webbsidor där risken för att datorer 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.

11.2 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. Brandväggsprogramvaran och -utrustningen ska hållas funktionsdugliga och uppdaterade.

11.3 Åtkomsträttigheter

Användarnamn för de programvaror och administratörer som påverkar hanteringen av informationssäkerheten är de viktigaste åtkomsträttigheter som ska skyddas. I fel händer ger dessa åtkomsträttigheter missbrukaren eller angriparen ett sätt att undvika att bli upptäckt och att legitima användare stängs av från sina egna system. De flesta angripare och sabotageprogram behöver systemadministratörsrättigheter för att kunna sprida sig eller installera sig i systemen. Om användarna använder användarnivåkoder kan skadliga åtgärder begränsas effektivt.

Det lönar sig att särskilja användarkoderna åtminstone enligt nivåerna administratör och användare, men även i större organisationer till exempel för huvudanvändare kan man införa användarnivåkoder som finns mellan dem.

12 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 enskilda anordningar. Gällande bevaringstider läs också B 10 Anvisning för 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 är fråga om insiderärenden.

13 Säkerhetskopiering (14.12.2023)

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.

13.1 Planering av säkerhetskopiering

I fråga om system som är viktiga med tanke på advokatverksamheten ska byrån bedöma för hur lång tid man högst har råd att förlora uppgifter? Och fastställa säkerhetskopieringens frekvens utifrån bedömningen.

Man bör också bedöma hur länge byrån kommer att klara sig utan systemet, med beaktande av rusningstoppar? Och fastställa en tidsplan för att återställa det system som ska säkerhetskopieras.

Dessutom ska det bedömas hur länge säkerhetskopierade uppgifter kan behövas, dvs. hur länge ska säkerhetskopierade uppgifter förvaras? I bedömningen bör det beaktas att det kan uppstå situationer där man till exempel inte på lång tid märker att viktiga uppgifter har raderats eller på grund av ett sabotageprogram blir tvungen att återställa filer långt tillbaka i tiden.

13.2 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.

13.3 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 informationssäkert 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.

13.4 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.

14 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.

14.1 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. Åtkomsten bör ses över med jämna mellanrum så att rättigheter som blivit onödiga kan tas bort. Distansförbindelser till byråns system ska ges separat och övervakas.

14.2 Köp av ICT-tjänster

Vid köp av ICT-tjänster bevaras, hanteras och överförs information som omfattas av advokathemligheten med servrar eller 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 information. Dessutom är det skäl att efter att tjänsten har avslutats försäkra sig om att informationen raderas och vid behov överförs till en annan tjänst. 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 en tillräcklig nivå 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 med 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 informationssäkerhetsrisker 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.

14.3 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 säkerställande av ett tillräckligt tekniskt genomförande av tjänsteleverantörens tjänster och även av kompetensen ska man försäkra sig om att den information som hör till olika aktörer hålls åtskild.

Hur myndigheter eller andra utomstående kan få tillgång till uppgifter av tjänsteleverantören kan bero på det land där servern är belägen eller tjänsteleverantörens hemort.

15 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.

15.1 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.

15.2 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-postadresser. 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.

15.3 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.

15.4 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.

16 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.

17 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.

18 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 bevarande av handlingar, 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. Flerfaktorsautentisering 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 tvåfaktorsautentisering 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 365-abonnemangets informationssäkerhet. Användaren bör minst vara förtrogen med följande: identifiering av den rätta inloggningssidan, genom vilken man kan identifiera 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 berörda parter, 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 moln-tjänster 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.

BILAGA 3 (14.12.2023)

[Organisationens logotyp]

[XX Advokatbyrå Ab]

INFORMATIONSSÄKERHETSPOLICY

Version:	
Versionsdatum:	
Upprättats av:	
Godkänts av:	
Sekretessnivå:	Intern

Ändringshistorik

Datum	Version	Upprättats av	Beskrivning av ändring

Innehållsförteckning

Syfte, omfattning och användare

Syftet med denna informationssäkerhetspolicy är att fastställa informationssäkerhetens mål eller syfte, riktlinjer samt ansvar och organisation.

Praxis inom policyn tillämpas på verksamheten vid [XX Advokatbyrå Ab].

Användare av detta dokument är alla anställda vid [XX Advokatbyrå Ab] och av relevanta externa intressenter.

Referensdokument

- Förteckning över rättsliga, reglerande och avtalsmässiga krav
- Riskhanteringspolicy
- Riskhanteringsplan
- Kontinuitetsplan
- Utbildningsplan
- Revisionsplan
- [Återhämtningsplan]
- [Förteckning över datatillgångar]
- [Förfarande för hantering av informationssäkerhetsstörningar]

Basterminologi inom informationssäkerhet

Konfidentialitet – kännetecknande för information som endast är tillgänglig för behöriga personer eller system.

Tillgänglighet – kännetecknande för information som behöriga personer kan använda vid behov.

Integritet – kännetecknande för information som endast behöriga personer eller system kan ändra på ett tillåtet sätt.

Informationssäkerhet – bevarande av informationens konfidentialitet, integritet och tillgänglighet.

Hantering av informationssäkerheten – en del av en övergripande hanteringsprocess som sköter planeringen, genomförandet, underhållet, granskningen och förbättringen av informationssäkerheten.

Hantering av informationssäkerhet

Mål och mätning

De allmänna målen för hanteringen av informationssäkerheten [i XX Advokatbyrå Ab] är följande: sekretess för klientuppgifter (konfidentialitet), iakttagande av kraven i lagstiftningen och bestämmelserna om advokatverksamhet, säkerställande av att de uppgifter som behövs i advokatverksamheten är användbara (tillgänglighet, integritet, användbarhet), upprätthållande av en tillförlitlig advokattjänstleverantörs anseende genom att förbättra kunnandet och medvetenheten om informationssäkerhet, upprätthållande av en tillförlitlig advokattjänstleverantörs anseende genom att minska och förhindra eventuella informationssäkerhetsstörningar. Informationssäkerhetspolicyn skapar en grund för affärsverksamheten [i XX Advokatbyrå Ab] och för säkerställandet av informationssäkerheten.

[Uppgiftsbenämning] svarar för uppställandet och uppföljningen av dessa allmänna mål för hanteringen av informationssäkerheten. Alla mål ska ses över minst [en gång per år] eller om informationssäkerheten eller kontorsmiljön eller centrala system ändras.

Uppnåendet av målen ska följas upp regelbundet. På basis av resultaten av uppföljningen ska avhjälpande åtgärder utarbetas. [Uppgiftsbenämning] ansvarar för uppföljningen och för att detaljerna i dess resultat rapporteras till [uppgiftsbenämning].

Krav på informationssäkerhet

Denna informationssäkerhetspolicy och hanteringen av hela informationssäkerheten ska överensstämma med de rättsliga, regleringsmässiga samt avtalsmässiga och andra väsentliga skyldigheter som är väsentliga för organisationen i fråga om informationssäkerhet.

En detaljerad förteckning över alla avtalsmässiga och rättsliga krav finns i dokumentet Förteckning över rättsliga, regleringsmässiga och avtalsmässiga krav [inkl. en förteckning över författningar och normer på lägre nivå som gäller advokatverksamhet, regleringskrav (såsom en förpliktande informationssäkerhetsanvisning som kompletterar Vägledande regler om god advokatsed), krav i anslutning till avtalet (klienters krav, olika avtal med intressentgrupper) och andra väsentliga informationssäkerhetskrav (t.ex. interna krav).].

Riskhantering inom informationssäkerhet och hanteringsmetoder

Informationssäkerhetsriskerna bedöms och analyseras regelbundet utifrån deras konsekvenser för affärsverksamheten. En riskbedömning ska göras också när kontors- eller informationssäkerhetsmiljön förändras t.ex. när nya system fastställs och i samband med betydande förändringar som påverkar verksamhetens kritiska karaktär.

Kontinuiteten i verksamheten

Det primära syftet med informationssäkerheten är att trygga kontinuiteten i advokatverksamheten under alla förhållanden. [Hantering av kontinuiteten i verksamheten definieras i Kontinuitetsplanen [och Återhämtningsplanen].]

Utbildning i informationssäkerhet

Den kompetens som hänför sig till informationssäkerheten säkerställs genom regelbundna utbildningar i informationssäkerhet. Utbildningarna har dokumenterats [metod eller system].

Tillsyn över informationssäkerheten

Tillsynen över informationssäkerheten utförs som regelbundna externa revisioner av informationssäkerheten. Det förs bok över revisionerna. Revisionen definieras närmare i Revisionsplanen (bilaga x), som fastställer revisionsperioderna, revisionskriterierna, revisionens omfattning och revisorn. Revisionen kan utföras i en helhet på en gång eller i delar så att helheten täcks. Revisionsplanen kan användas för att verifiera genomförda och framtida revisioner.

Ansvar

Ansvarsområdena för hantering av informationssäkerheten är följande:

- [uppgiftsbenämning] ansvarar för att säkerställa att hanteringen av informationssäkerheten genomförs och upprätthålls i enlighet med denna policy och att alla nödvändiga resurser finns tillgängliga.

- [uppgiftsbenämning] ansvarar för samordningen av hanteringen av informationssäkerheten och för rapporteringen av resultaten [incidenter, störningssituationer och respons från intressentgrupper]

- [den högsta ledningen] ska granska hanteringen av informationssäkerheten minst en gång om året eller varje gång en betydande förändring sker och upprätta protokoll över granskningsmötet. Syftet med ledningens granskning är att utreda lämpligheten, tillräckligheten och effektiviteten i hanteringen av informationssäkerheten [i förhållande till riskerna]

- [uppgiftsbenämning] genomför en utbildningsplan i informationssäkerhet för de anställda

- ansvaret för att skydda informationstillgångarnas integritet, användbarhet och konfidentialitet ligger hos varje ägare av informationstillgångarna

- varje fel eller svaghet i informationssäkerheten ska rapporteras till [uppgiftsbenämning]

- [uppgiftsbenämning] bestämmer vilka informationssäkerhetsrelaterade uppgifter som ska kommuniceras till olika intressentgrupper (både interna och externa), av vem och när

- [uppgiftsbenämning] ansvarar för att godkänna och genomföra en utbildnings- och upplysningsplan som ska tillämpas på alla personer som har en roll i hanteringen av informationssäkerheten.

Kommunikation om informationssäkerhetspolicyn

[Uppgiftsbenämning] ska säkerställa att alla anställda hos [organisationens namn] och relevanta externa intressenter känner till denna Informationssäkerhetspolicy.

Stöd för genomförande av hanteringen av informationssäkerheten

[Styrelsen/ledningsgruppen] meddelar att genomförandet och den fortsatta förbättringen av hanteringen av informationssäkerheten kommer att stödjas med tillräckliga resurser för att uppnå alla de mål som fastställs i denna policy och för att uppfylla alla identifierade krav.

Giltighet och dokumenthantering

Detta dokument gäller från [datum].

Ägaren till denna informationssäkerhetspolicy är [uppgiftsbenämning], som ska granska och vid behov uppdatera detta dokument [minst en gång om året].

[uppgiftsbenämning]

[namn]

_____

[underskrift]

BILAGA 4 REVISIONSGUIDE (14.12.2023)

Informationssäkerhetsanvisningen (B 05.1) förpliktar advokatbyråer med över 10 anställda att ordna en extern informationssäkerhetsrevision regelbundet och när vissa ändringar genomförs samt att föra bok över revisionerna.

Bakgrund

Syftet med denna revisionsguide är att fastställa omfattningen av revisionen vid en advokatbyrå, om verksamheten inte omfattas av någon annan allmänt godtagen informationssäkerhetsstandard (t.ex. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001). Allmänt vedertagna standarder för informationssäkerhet omfattar utarbetande och regelbunden revision av ett separat revisionsprogram som en del av upprätthållandet av standarden för informationssäkerhet.

Informationssäkerhetsrevisionen är en praxis som syftar till att förbättra hanteringen av informationssäkerheten vid en byrå. Vid revisionen kan man hitta dolda utvecklingsobjekt som kan äventyra advokatverksamheten och avslöja konfidentiella uppgifter som omfattas av advokathemligheten. Oönskade förändringar och fel i informationssäkerhetsmiljön är naturliga händelser som inte helt kan undvikas. Revisionen kan användas som ett av de effektivaste sätten att hitta och rätta till dem.

Det lönar sig att utnyttja den regelbundna revision som informationssäkerhetsanvisningen förpliktar till som ett sätt att kontinuerligt förbättra byråns informationssäkerhetsverksamhet.

Revisionsplan och revisionsrapport

Revisionsplanen fastställer normalt revisionsperioderna, revisionskriterierna, revisionens omfattning och revisorn. Det rekommenderas att revisionen utförs årligen. Revisionen kan utföras i en helhet på en gång eller i delar så att helheten täcks. Revisionsplanen kan användas för att verifiera genomförda och framtida revisioner.

Revisionsrapporten beskriver iakttagelser som gjorts under revisionen och avvikelser från den verksamhet som strider mot kraven. En avvikelse registreras vanligen när verksamheten inte alls uppfyller det krav som ställs på den. Iakttagelsen kan beskriva en partiell underlåtenhet att uppfylla kraven eller en positiv iakttagelse av verksamheten. Revisionsberättelsen kan verifiera resultaten av revisionen och de åtgärder som kräver korrigering.

Revisorn

Revisorn ska vara behörig att utföra revisionen, även om det inte har ställts några egentliga kriterier för revisorn. Revisorn ska känna till kraven, i praktiken Advokatförbundets informationssäkerhetsanvisning (B 05.1) utifrån vilken revisionen utförs och den allmänna verksamhetsmiljö där kraven uppfylls.

Revisorn ska ha erfarenhet av revisionsprocessen för att iakttagelserna i revisionen och rapporten om dem ska kunna utnyttjas för att utveckla verksamheten.

Det väsentliga är att revisionen utförs av en aktör som inte ansvarar för upprätthållandet och förvaltningen av den befintliga ICT-miljön.

Revisionens förlopp

Revisionen är i allmänhet indelad i faser där varje fas omfattar särskilda uppgifter, såsom granskning av informationssäkerhetsdokumentation, upprättande av revisionschecklista, genomförande av den egentliga revisionen, rapportering och uppföljning av korrigerande åtgärder.

Informationssäkerhetsrevisionen av advokatverksamhet utförs minst enligt Advokatförbundets krav i informationssäkerhetsanvisningen (B 05.1). I praktiken beaktar revisorn dock också de övriga krav som byråns egen informationssäkerhetsmiljö ställer.

I det första skedet, vid granskningen av informationssäkerhetsdokumentationen, sammanställs den dokumentation som behövs (såsom Advokatförbundets informationssäkerhetsanvisning (B 05.1) och byråns egen informationssäkerhetsanvisning) för genomgången och ur dokumentationen uppgörs en lista över de ärenden som man vill granska.

I revisionschecklistan antecknas de ärenden som granskas vid revisionen: källan till kravet och det ärende som ska granskas, de system som ska granskas, intervjufrågor, tidsschema osv.

Vid den egentliga revisionen väljer revisorn källan till kravet, föremålet för revisionen och kontrollerar att kraven uppfylls. Detta kan göras genom observationer och intervjuer. Resultaten och anteckningarna om dem kan antecknas i checklistan för att verifiera saken.

I revisionsrapporten antecknas de avvikelser och iakttagelser som upptäckts vid revisionen. Anteckningen av en avvikelse ska göras med sådan noggrannhet att man utifrån den kan vidta korrigerande åtgärder. Registreringen av avvikelsen bör därför basera sig på de anteckningar som gjorts vid den egentliga revisionen.

Frågor på revisionschecklistan

Avsikten är att frågorna i checklistan nedan ska stödja bedömningen av informationssäkerheten i byråns egen verksamhet till exempel när man förbereder sig för en revision. Genom frågorna på checklistan kan man bedöma läget för byråns informationssäkerhet utifrån de förpliktande punkterna i Advokatförbundets informationssäkerhetsanvisning (B 05.1).

I frågorna på checklistan har man fastställt det krav på verksamheten som punkten i informationssäkerhetsanvisningen ställer och en exempelfråga som definierar överensstämmelse med kraven.

Checkfrågor vid revision

Checkfrågor i enlighet med Advokatförbundets informationssäkerhetsanvisning (B 05.1).

Anvisningspunkt	Krav	Överens-stämmelse med krav Ja / Nej	Autentisering av överens-stämmelse
1. Utbildning	Har en utbildningsplan utarbetats för byrån?		
	Finns det uppteckningar om de kvalifikationer som erhållits genom utbildningarna?		
2. Informationssäkerhetspolicy	Har byrån en beskrivning över informationssäkerhetspolicyn?		
	Har de principer för informationssäkerhet som beskrivs i policyn godkänts av den högsta ledningen?		
3. Revision av informationssäkerheten	Har byrån genomfört en informationssäkerhetsrevision där informationssäkerheten har bedömts utifrån kraven i Advokatförbundets informationssäkerhetsanvisning B 05.1, utifrån kraven i		

	lagstiftningen och utifrån byråns egna krav på informationssäkerhet?		
	Har revisionen av informationssäkerheten genomförts regelbundet?		
	Har revisionen av informationssäkerheten genomförts efter ändringar i de centrala systemen? [inriktning av kravet/verifieringsgrund för kravet?]		
	Har revisionen av informationssäkerheten genomförts efter ändringar i informationssäkerhetsmiljön? [inriktning av kravet /verifieringsgrund för kravet?]		
	Har revisionen av informationssäkerheten genomförts efter ändringar i byråmiljön? [inriktning av kravet/verifieringsgrund för kravet?]		
4. Granskningar	Har uppgifterna om ordnande av advokatverksamhet, klientrelationer och uppdrag skyddats, åtskilts och hemlighållits under granskningar som gäller byrån?		
5. Principer för informationssäkerhet	Har byrån de principer för informationssäkerhet som beskrivs?		
	Har de beskrivna principerna godkänts av den högsta ledningen som verksamhetsprinciper? [genom vilka den förbinder sig att uppfylla kraven >]		
	Har de krav som lagstiftningen och regleringen ställer på advokatverksamhet beaktats i principerna för informationssäkerhet?		

	Har man i principerna för informationssäkerhet beaktat de krav som de avtal som ingåtts vid byrån ställer på byrån?		
	Styr principerna för informationssäkerhet verksamheten på praktisk nivå?		
6. Säkerheten i lokalerna	Är lokalens dörrar och andra ingångar låsta så att endast behöriga personer kan passera genom dem?		
	Har allt material som omfattas av advokathemligheten (såsom pappersmaterial, lagringsmedier) förvarats på ett skyddat sätt i lokalerna?		
7. Programvara och tjänster	Är den programvara som används i advokatverksamheten sådan programvara som är avsedd för företagsändamål?		
	Är de tjänster som används i advokatverksamheten, såsom molntjänster, tjänster som är avsedda för företagsändamål?		
	Har man verifierbart kommit överens med klienten om användning av annan programvara eller tjänst än sådan som är avsedd för företagsändamål vid skötseln av ärenden?		
8. Lösningar för enhets- och åtkomsthantering (för byråer med fler än 10 anställda)	Är de datorer och mobila enheter som används i advokatverksamheten enheter som styrs genom enhetshantering?		
	Är åtkomsthanteringen av datorer och mobila enheter som används i advokatverksamheten sådan att endast behöriga användare kan använda dem?		

9. Kryptering	Är datorer, mobila enheter, lagringsmedier som används i advokatverksamhet krypterade?		
	Är de tabeller, databaser och molntjänster som innehåller klientuppgifter krypterade?		
	Används den utrustning som används i advokatverksamheten, såsom datorer, mobila enheter [och skrivare], endast av den person som driver ärendet?		
	Används i advokatverksamheten endast utrustning som uttryckligen fastställts som säker?		
	Har extra utrustning som ska anslutas till säkra enheter fastställts som säkra?		
	Får all utrustning som används i advokatverksamheten regelbundet uppdaterade programuppdateringar som produkttillverkaren lanserat?		
	Raderas uppgifterna i de enheter som ska tas ur bruk, på ett informationssäkert sätt så att det inte längre är möjligt att återställa uppgifterna?		
10. Nätverk	Är det nätverk som används på byrån skyddat så att det endast behöriga enheter kan ansluta sig till det?		
	Är byråns trådlösa nätverk krypterade med modern, kvalificerad kryptering?		
	Har de anslutningar som används via offentliga nätverk krypterats på ett adekvat sätt [version] (t.ex. VPN, TLS)?		

11. Lösenord	Tillämpas en lösenordsprincip?		
	Kräver man vid lösenordsprincipen tillräckligt långa och komplicerade lösenord (versaler och gemener, siffror och specialtecken)?		
	Har man i lösenordsprincipen fastställt när lösenordet ska ändras?		
	Har man i lösenordsprincipen fastställt en säker lagring av lösenord?		
	Har det i lösenordsprincipen fastställts krav på stark autentisering (såsom flerfaktorsautentisering)?		
12. Programvara för informationssäkerhet	Har de enheter som används i advokatverksamheten erforderlig programvara för informationssäkerhet?		
	Har de enheter som används i advokatverksamheten erforderlig brandvägg?		
	Har säkerhetsprogramvara som kan kringgå användarbegränsningar begränsats endast till systemadministratörer?		
	Har systemadministratörernas användarnamn begränsats enligt befattningsbeskrivning och kompetens till personer som behöver dem?		
	Används systemadministratörens koder endast när det krävs en sådan behörighetsnivå (t.ex. åtgärder för systemhantering)?		
	Installeras uppdateringar av all utrustning, operativsystem, programvara och		

	alla applikationer som används i advokatverksamheten planmässigt och efter det att uppdateringen har offentliggjorts utan onödigt dröjsmål?		
13. Åtkomsträttigheter	Begränsas användarnas åtkomsträtt till information, beroende på deras arbetsuppgift, enligt deras behov av information?		
14. Säkerhetskopiering	Säkerhetskopieras allt material som uppfyller kraven i B 10 Anvisning för bevarande av handlingar?		
	Görs säkerhetskopieringen regelbundet?		
	Har säkerhetskopieringen dimensionerats utifrån en uppskattning av den maximala godtagbara förlusten av uppgifter?		
	Har molntjänsterna också säkerhetskopierats i enlighet med lagringskraven?		
	Är lagringstiden för säkerhetskopior tillräcklig?		
	Har säkerhetskopiorna krypterats och bevarats på ett säkert sätt?		
	Har tester för återställning av säkerhetskopierade uppgifter genomförts på ett framgångsrikt sätt		
15. Säkerheten hos leverantörer	Har man med leverantörerna ingått avtal om informationssäkerhet som uppfyller informationssäkerhetskraven?		
	Har man med leverantörerna ingått avtal om sekretess som uppfyller informationssäkerhetskraven?		

	Har man kommit överens med leverantörerna om att begränsa åtkomsträtterna så att de motsvarar arbetsuppgifterna?		
	Har man kommit överens med leverantörerna om att regelbundet kontrollera att åtkomsträtterna är uppdaterade?		
	Har man kommit överens med leverantören om att uppgifterna i behövlig utsträckning kan överföras till en annan tjänst?		
	Har man med leverantören kommit överens om att förstöra uppgifterna när användningen av tjänsten upphör?		
16. Kryptering av kommunikation	Uppfyller den kommunikationskanal som använts i advokatverksamheten informationssäkerhetskraven?		
	Har de kommunikationskanaler som godkänts för sekretessbelagda uppgifter fastställts vid byrån?		
	Används krypterad e-post för sekretessbelagda uppgifter som skickas per e-post?		
	Har man med klienten kommit överens om sätten att sända sekretessbelagda uppgifter?		
	Har man kommit överens med klienten om sätten för sekretessbelagd kommunikation?		
17. Material	Uppfyller materialet för advokatverksamhet de krav som ställs på lagring av materialet?		

	Uppfyller materialet i advokatverksamheten de krav som ställs på förvaring av materialet?		
	Uppfyller materialet i advokatverksamheten de krav som ställs på arkivering av materialet?		
	Uppfyller materialet i advokatverksamheten kraven på hur materialet ska förstöras?		
18. Inaktiverad utrustning	Har all inaktiverad utrustning, såsom datorer, mobila enheter och lagringsenheter raderats från data så att det inte går att återställa data till enheten?		
	Har alla inaktiverade nätverksbaserade lagringsplatser raderats från data så att det inte går att återställa data?		
19. Tryggande av kontinuiteten i verksamheten	Har de uppgifter som är väsentliga med tanke på kontinuiteten i verksamheten noggrant utretts?		
	Har de uppgifter som är väsentliga för kontinuiteten i verksamheten dokumenterats?		
	Finns de dokument som är väsentliga med tanke på kontinuiteten i verksamheten tillgängliga i störningssituationer, för de personer som behöver dem?		