Lisa nr 1

Elektrooniliste vahendite ja interneti kasutamise juhend

ABIMATERJAL ELEKTROONILISTE VAHENDITE JA INTERNETI KASUTAMISE JUHENDI JUURDE

SISUKORD

1. SISSEJUHATUS

Käesolev abimaterjali eemärk on mittekohustuslike soovituste ja näidislahenduste andmisega abistada advokaate Eesti Advokatuuri juhatuse 14. detsembri 2010. a otsusega kinnitatud „Elektrooniliste vahendite ja interneti kasutamise juhend“ (edaspidi „Juhend’’) nõuete täitmisel.

Advokaadid ja advokaadibürood võivad kasutada nii Juhendis kui ka käesolevas abimaterjalis kirjeldatust erinevaid lahendusi, kui need lahendused tagavad konkreetsele olukorrale vastaval tasemel turvalisuse, konfidentsiaalsuse või muude kutsetegevuse nõuete täitmise.

Järgnevas tekstis hõlmab mõiste „advokaat“ sõltuvalt kontekstist ka nii advokaadibürood, advokaadiühingut ja advokaadibüroo pidajat advokatuuriseaduse tähenduses kui ka muid advokaadibüroo töötajaid.

Juhend ja alljärgnev tekst põhinevad CCBE vastavatel suunistel[1]. Lisaks Juhendile ja käesoleva abimaterjali soovitustele peab advokaat oma tegevuses arvestama ka muid õigusakte ning Eesti Advokatuuri juhendeid[2].

2. ELEKTROONILISE KOMMUNIKATSIOONI ÜLDNÕUDED

Advokaadi vastutus kutsetegevuse nõuete rikkumise eest võib tuleneda ka elektroonilise vahendi kaudu osutatud õigusteenusest või elektroonilisel teel peetud kommunikatsioonist. Seetõttu tuleb elektroonilise vahendi kaudu toimuvas kommunikatsioonis olla sama hoolikas kui muus vormis kommunikatsioonis ning veenduda, et kommunikatsiooni oleks täpne, kaasajastatud ja vastavuses kutsetegevuse nõuetega.

[1] http://www.ccbe.org/fileadmin/user_upload/NTCdocument/ccbe_guidelines_ecom1_1182260654.pdf

[2] Nt Eesti Advokatuuri juhatuse otsusega kinnitatud „Ärilise teavitamise juhend“

2.1. Avaldatavatele andmetele esitatavad põhinõuded

2.1.1. Advokaadi kommunikatsioonis peavad olema märgitud mh eestikeelsena advokaadibüroo ärinimi, tegevuskoha aadress ja äriregistri kood.

2.1.2. Advokaadibüroo töötajad, kes ei ole advokaadid, peavad elektroonilises kommunikatsioonis kasutama selgesti eristuvat muud ametinimetust.

2.2. Soovitused avaldatavatele andmetele esitatavate põhinõuete järgimiseks

2.2.1. Nõutud andmed peavad veebilehel olema avaldatud selgelt eristuvana.

2.2.2. Nõutud andmete igakordseks täielikuks edastamiseks e-kirjavahetuses on soovitav luua ja kasutada vastavat e-kirja malli[3], mis sisaldab kogu nõuetekohast informatsiooni. Mallide loomist võimaldab enamik e-kirja tarkvarasid.

2.2.3. Kui advokaadibüroo lubab kasutada ametlikke elektronposti aadresse kutsetegevusega mitteseotud e-kirjavahetuseks, siis selliseks e-kirjavahetuseks on soovitatav kasutada alternatiivset e-kirja malli või signatuuri, kus on sõnaselgelt deklareeritud, et kommunikatsioon ei seondu saatja kutsetegevusega.

2.2.4. Kutsetegevusega mitteseonduvas e-kirjavahetuses ei ole soovitatav kasutada konfidentsiaalsuse või kommunikatsiooni kutsesaladusega kaitstuse hoiatusi, sest nende asjakohatu kasutamine võib kahandada hoiatuste mõju.

3. ÕIGUSTEENUSE JA INFORMATIIVSETE TEADETE ERISTAMINE

3.1. Õigusteenuse ja informatiivse teabe eristamise nõue

3.1.1. Elektroonilises kirjavahetuses tuleb tagada, et adressaadil oleks võimalik eristada õigusteenuse osutamist ning informatiivse teabe edastamist.

3.2. Soovitused õigusteenuse ja informatiivsete teabe eristamiseks

3.2.1. Informatiivsete teadete avaldamisel või edastamisel peab advokaat selgitama, et edastatav teave ei ole õigusteenuse osutamine.

3.2.2. Veebilehel või informatiivsetes teadetes on advokaadibüroodel soovitatav selgelt eraldiseisva teatisega deklareerida, et avaldatav või edastatav teave on üksnes informatiivne. Veebilehel või informatiivsetes teadetes võib soovitada õigusteenuse saamiseks advokaadi poole pöördumist.

3.2.3. Vastava teatise näide on järgimine: „Veebilehe või teate sisu on ette nähtud vaid üldiseks informatsiooniks. See ei kujuta endast õigusteenuse osutamist ega asjatundja arvamust ja seda ei tohi sellena kasutada. Me ei võta endale vastutust sellise informatsiooni kasutamise tagajärgede eest”.

3.3. Lingid ja viited kolmandatele isikutele

3.3.1. Soovitatav on hoiduda tundmatute või potentsiaalselt ohtlike hüperlinkide ja viidete edastamisest ja avamisest.

3.3.2. Kui veebileht või e-kirjavahetus sisaldab hüperlinke või viiteid kolmandate isikute materjalidele, siis võib veebilehekülje külastajal või e-kirja saajal tekkida eeldus, et advokaadibüroo või advokaat kiidab heaks viidatud teenused ja informatsiooni.

[3] Mall on dokumendi näidisvormingut esitav fail või vorm, mis dokumendi koostamisel täidetakse sisulise informatsiooniga.

3.3.3. Tuleb tagada, et edastatavad hüperlingid ja viited ning nende kasutamise kontekst ei oleks (mh mitmetimõistetavuse tõttu) vastuolus kutsetegevuse üldnõuetega.

3.4. Elektronposti ja veebiserverid

3.4.1. Tähelepanu tuleb pöörata asjaolule, et veebiserveri operatsioonisüsteemile ning veebitarkvarale oleks alla laaditud värskeimad parandused ning turvauuendused. See aitab ära hoida pahatahtlikke rünnakuid, mis ühel või teisel moel võivad põhjustada veebilehe sisu tahtmatut muutumist või andmete kadu.

3.4.2. Tuleb tagada, et veebilehest ning e-maili serveritest tehakse varukoopiaid ja et need on taastatavad (sh logid).

3.4.3. Juhul kui veeb/elektronpost on majutatud teenusepakkuja serveris, tuleks veenduda, et teenusepakkuja ja majutusteenus vastavad eelnevatele nõuetele.

4. ADVOKAADI ELEKTROONILINE KOMMUNIKATSIOON

4.1. Põhinõuded advokaadi elektroonilisele kommunikatsioonile

4.1.1. Advokaat peab oma elektroonilise kommunikatsiooni kaitstuse ja konfidentsiaalsuse tagamiseks kasutusele võtma ja uuendama adekvaatseid ja ajakohaseid meetmeid.

4.2. E-kirjavahetuse tahtlik jälgimine ning pahatahtlik rünne

4.2.1. Advokaadil on soovitatav kaitsta oma elektroonilist kommunikatsiooni sisu igasuguse kuritahtliku modifikatsiooni vastu. Seda nii kliendi kui ka omaenda huvide kaitseks.

4.2.2. Advokaadil on soovitatav kasutada vahendeid, mis on mõistlikes piirides kättesaadavad, et tagada oma e-kirjavahetuse töökindlus ja kaitstus. Kuigi e-kirjavahetus on tehniliselt ja juriidiliselt kaitstud kolmandate isikute jälgimise vastu, võib selle konfidentsiaalsus siiski olla mitmesuguste vahenditega rünnatav. Advokaadid peavad seetõttu pidevalt hindama e-kirjavahetusega seonduvaid riske.

4.2.3. Kliendi või adressaadi nõudel tuleb kasutada mõistlikult kättesaadaval olevaid krüpteerimisvõtteid. Võimalik on kasutada ID kaardi vms tehnilise lahenduse pakutavaid võimalusi e-kirjavahetuse sisu pahatahtliku modifitseerimise vastu digitaalallkirjastamise või jälgimise vastu krüpteerimise näol. Advokaat peab enne vastavate abivahendite kasutusele võtmist selgitama välja nende abivahendite kasutamise seonduvad riskid.

4.2.4. Kolmandate isikute pakutavate elektronposti teenuste, kiirvestlustarkvara (MSN, Skype) ja mobiilsete seadmete kasutamisel tuleb hoolikalt kaaluda, kas need on piisavalt kaitstud e-kommunikatsiooni jälgimise või pahatahtliku ründe vastu ning kas kasutusele on võetud piisavad meetmed, mis hoiavad ära vastava kommunikatsiooni ja selle sisu avalikuks tulemise.

4.2.5. Vajadusel tuleb kliente ja muid e-kirjade adressaate või saatjaid informeerida riskidest, millega puututakse kokku elektroonilise kommunikatsiooni vahendite kasutamisel.

4.3. Konfidentsiaalsuse teade eksliku edastamise juhuks

4.3.1. Soovitatav on e-kirjadele lisada konfidentsiaalsuse teade koos nõudega eksliku edastamise korral teavitada sellest e-kirja saatjat ning kustutada ekslikult saadud e-kiri ja selle manused.

4.3.2. Kuigi e-kirjale lisatud konfidentsiaalsuse teade ei pane enamasti e-kirja ekslikule saajale õiguslikult siduvat kohustust, võib eeldada, et paljud saajad järgivad

instruktsiooni ja seeläbi on võimalik vältida ekslikust adresseerimisest tuleneva kahju tekkimist.

4.3.3. Advokaadid võivad kasutada järgmist soovituslikku konfidentsiaalsuse teadet: „Käesolev e-kiri on saadetud advokaadi kutsetegevuses ning selle sisu on konfidentsiaalne. E-kirjas sisalduvat informatsiooni võib kasutada vaid isik, kellele see on adresseeritud. Kui te pole sihipärane saaja, palun teavitage saatjat ja kustutage e-kiri koos manustega kohe ja lõplikult oma süsteemist."

4.3.4. Advokaatidel on soovitatav lisada näidisteade või analoogne modifitseeritud teade oma e-kirja malli või signatuuri.

4.4. Viirused ja ründetarkvara

4.4.1. E-kirjad võivad sisaldada viiruseid või muud pahatahtlikku tarkvara, mis võivad ebateadliku tegutsemise ning puuduliku tehnilise kaitse korral kahjustada advokaadi tööjaama, arvutivõrgu või veebilehe toimimist. Sellised viirused ja tarkvara võivad omavoliliselt edastada konfidentsiaalset informatsiooni kolmandatele isikutele või lubada sellele volitamata juurdepääsu.

4.4.2. Advokaadibüroodel on soovitatav omada IT ohutusstrateegiat ja rakendada selliste riskide vastu kaasaegseid tehnilise kaitse ettevaatusabinõusid. Samuti peaksid advokaadibürood tagama, et advokaadid ja muud töötajad oleksid teavitatud ja järgiksid ohutusprotseduure. Alljärgnevalt on lisatud mõned peamised soovitatavad ohutusprotseduurid:

- Viirusevastase, nuhkvaravastase tarkvara rakendamine ja jooksev uuendamine ning seire;
- Sülearvutite kõvaketaste, mälupulkade krüpteerimine (vältimaks konfidentsiaalsuse riski nt kaotamise puhul);
- Vältida programmide käivitamist nn „Administraatori" õigustes (viirused ja muu pahavara töötavad kõige paremini kui nad käivitatakse priviligeeritud õigustes);
- Elektronposti serverite ja e-kirja tarkvara konfigureerimine selliselt, et manused saadetise saamisel automaatselt ei avaneks. Selline lähenemine tagab, et viiruseid ei saa automaatselt importida teistesse süsteemidesse. Soovitatav ei ole avada kahtlusi tekitava pealkirjaga ja/või kahtlustäratavalt elektronposti aadressilt saabuvat e-kirja ning käivitada e-kirjade manuses olevaid programme või skripte;
- Tagada, et kutsetegevuses kasutatavat elektronposti aadressi ei kasutataks tarbijamängude mängimiseks, isiklike kommertsteadete tellimiseks, foorumite kasutamiseks ning muudeks tegevusteks, mis võivad põhjustada hulgalise kommertsteadete ja rämpsposti saatmise mõnele elektronposti aadressile;
- Läbimõeldud salasõnapoliitika (piisav parooli keerukustase, selle vahetamine teatud aja tagant);
- Tööjaamades „Auto-Run" funktsionaalsuse väljalülitamine, vältimaks pahatahtlike programmide automaatset käivitamist, mis nt võivad edastada konfidentsiaalset informatsiooni kolmandatele isikutele;
- Kasutatav tarkvara on soovitatav hoida ajakohasena. Soovitav on jälgida, et kriitilised uuendused ning turvapaigad on alla laaditud;
- Tagamine, et advokaadibüroo arvutivõrk oleks adekvaatselt kaitstud rünnete, viiruste või muude Internetist kui ka sisevõrgust lähtuvate ohtude vastu. Advokaadibürool on oma tööjaamade ja neis sisalduva informatsiooni kaitseks

soovituslik paigaldada tarkvaraline või riistvaraline tulemüür, ründetuvastussüsteem kui ka ründe blokeerimise süsteem (Intrusion Detection & Intrusion Prevention Systems);

- Klientidele internetiühenduse pakkumiseks nõupidamisruumides on soovitatav kasutada sisevõrgust eraldatud külalisvõrku, kust pääseb ainult internetti. Selleks võib kasutada 801.1x põhist autentimist. WIFI e. traadita võrgud peaksid olema kaitstud tänapäevaste autentimis- ning krüpteerimisvõimalustega nagu näiteks WPA2/AES 256;
- Kui advokaadibüroo IT seadmete hooldus või muud IT teenused tellitakse teenusepakkujalt, siis on soovitatav, et advokaadibüroo:
    - veenduks teenusepakkuja ja tema personali kõrgendatud usaldusväärsuses ning kvalifikatsioonis;
    - teostaks adekvaatset järelevalvet teostatavate tööde ja osutatavate teenuste üle;
    - tagaks teenusepakkuja ja tema personali poolt konfidentsiaalsuse ja muude kutsetegevuse nõuete järgimise (nt konfidentsiaalsuslepingute sõlmimise kaudu).

4.5. Elektrooniline kommunikatsioon advokaatide vahel

4.5.1. Advokaatide vahelises elektroonilises kommunikatsioonis tuleb kinni pidada advokaatide vahelist suhtlust puudutavatest kutseeetika nõuetest ja muudest professionaalsetest reeglitest.

5. KLIENDI ERAELU JA ISIKUANDMETE KAITSE

5.1. E-kirjade saatmise, saamise ja hoidmisega võib kaasneda isikuandmete töötlemine, mis nõuab piisavate andmekaitse meetmete kasutamist, täitmaks lisaks kutsetegevuse nõuetele ka isikuandmete kaitset reguleerivaid õigusakte.

6. ELEKTROONILISE KOMMUNIKATSIOONI HEAD TAVAD

6.1. Kliendi tundmine ja tahte väljaselgitamine

6.1.1. Advokaat peab veenduma elektrooniliste vahendite kaudu kontakteeruva kliendi või muu isiku isikusamasuses.

6.1.2. Isikusamasuse kontrollimine on lihtsam digitaalallkirja kasutamise korral. Digitaalallkirja puudumisel on advokaadil soovitatav veenduda saatja isikusamasuses kommunikatsiooni konteksti kaudu. Kui elektroonilise kommunikatsiooni teel ei ole võimalik kahtlusi kõrvaldada, siis on vajalik väidetava saatja isikusamasuses veendumine telefoni või vahetu kohtumise kaudu.

6.1.3. Elektroonilise kommunikatsiooniga kaasneda võiv anonüümsus võib osutuda atraktiivseks petturite ja rahapesijate jaoks. Advokaadid peavad olema tähelepanelikud, et elektroonilises kommunikatsioonis oleks tagatud vastavas valdkonnas advokaatidel lasuvate kohustuste täitmine.

6.1.4. Kui advokaadil tekkib kahtlus kliendi isikusamasuses, tema tegelikus tahtes, vastastikuses arusaamises või ebakohaste mõjutuste puudumises, siis on soovitatav rakendada kõrgendatud hoolsust või võimalusel loobuda elektroonilise kommunikatsiooni kasutamisest ja kliendiga kohtuda.

6.2. Õigeaegne vastus

6.2.1. Advokaadibürool on soovitatav rakendada organisatoorseid või tehnilisi vahendeid, mis tagavad, et advokaadi äraolekul ei jääks temale saabunud e-kirjad tähelepanuta ning neile vastamine toimuks õigeaegselt ja kohaselt.

6.2.2. Soovitatav on mitte rakendada või loobuda automaatsest kinnitustest e-kirja kättesaamise kohta. Advokaadi jaoks on oluline saata teade e-kirja kättesaamise kohta vaid siis, kui saatja soov või tahe õigusteenuse või informatsiooni kohta on advokaadile täiel määral mõistetav.

6.2.3. Advokaadi äraolekul on soovitatav kasutada automatiseeritud „büroost väljas“ (out of office) vastuseid, kui advokaat on advokaadibüroost eemal päeva või kauem.

6.2.4. Soovitatav on tagada mõne advokaadi või advokaadibüroo töötaja juurdepääs eemalviibiva advokaadi sissetulevate kirjade kausta, et kontrollida regulaarselt kausta sisu ja tagada õigeaegne vastus kiiretele päringutele.

6.3. Rämpspost

6.3.1. Kuna ilma nõusolekuta saadetavate kommertsteadaannete ja muude massiliste e-kirjade (rämpspost) voog võib e-kirjavahetuse kasutajatele olla tõsiseks probleemiks, siis on soovituslik kasutada spetsiaalset filtreerivat tarkvara (rämpspostifiltrid), mis vähendab saajani jõudva rämpsposti kogust.

6.3.2. Rämpspostifiltrite kasutamisest on soovitatav kliente teavitada, vältimaks ohte, mis kaasnevad oluliste teadete advokaadini mittejõudmisega. Klientidele on soovitatav selgitada, et tähtsale elektroonilisele kommunikatsioonile peaks alati järgnema telefonikõne, faks või trükitud eksemplar posti teel.

6.3.3. Rämpspostifiltrite seadistamisel tuleb jälgida, et seadistus ei oleks liiga range, kuna sellisel juhul võivad kutsetegevusega seonduvad e-kirjad advokaadini mitte jõuda. Soovitatav on teatava regulaarsusega kontrollida rämpspostifiltrisse jäänud e-kirju veendumaks, et kutsetegevusega seonduvad e-kirjad ei oleks rämpspostifiltrisse jäänud.

7. SOOVITUSED ELEKTROONILISTE DOKUMENTIDE HALDAMISEKS

7.1. Elektrooniliste dokumentide loomist ja hilisemat haldamist, sh säilitamist hõlbustab kinnipidamine järgmistest soovitustest:

- Kasutage dokumentide loomiseks malle;
- Alustage dokumentide loomist tühimalliga või tühja dokumendiga. Teise dokumendi aluseks võtmisel säilivad esialgse dokumendi metaandmed[4], mis võib olla eksitav või seonduda teisele kliendile õigusteenuse osutamisega;
- Kontrollige, kas informatsioon „Atribuutide“[5] ekraanil on uuendatud ja õige;
- Kasutage dokumentides selget struktuuri (nt profiile ja pealkirju);
- Kopeerige ja kleepige nii vähe kui võimalik, selleks et vältida ebaõigete metaandmete lisamist;

[4] Vaata punkti 10.1. metaandmete kohta

[5] Selle funktsiooni leiate tekstitöötlusprogrammi menüüvalikust „File” / „Fail” funktsioonina „Properties” / „Atribuudid”. See funktsioon sisaldab näiteks informatsiooni dokumendi loomise aja, autori, muutmise aja jms kohta.

- Ärge kasutage dokumentide muutmise vältimiseks paroole, sest parooli kadumisel on dokumenti võimatu avada; kasutage selle asemel valikut „vaid lugemiseks“ (Read only);
- Kasutage standardseid kirjatüüpe (nt Arial, Times New Roman), kuna neid kirjatüüpe tunnistavad ja kuvavad korrektselt enamik programme;
- Kasutage dokumendi päiseid ja jaluseid metaandmete sisestamiseks, näiteks dokumendi nimi ja versiooninumber;
- Ärge kasutage automaatse kuupäeva ja aja välju, kuna need muutuvad iga kord, kui dokumenti avatakse või trükitakse;
- Kasutage tabeleid või tabeldusmärke, kui vajalik, ja mitte tühikuklahvi. See tagab dokumendi küljenduse säilimise;
- Salvestage dokument keskses serveris ja mitte tööjaama kõvakettal. Nii saab iga advokaadibüroo töötaja leida dokumendi viimase versiooni.

8. SOOVITUSED E-KIRJADE HALDAMISEKS

8.1. E-kirja adresseerimisel on soovitatav järgida järgnevaid juhiseid:

- Kontrollige enne e-kirja saatmist (veelkordselt), et sisestatud või aadressiraamatust valitud saaja ja tema aadress on kavatsetud saaja ja kasutusel on õige aadress;
- Olge hoolikas, kui kasutate postiloendit (mailing list), sest nende tellijate ring võib sageli muutuda; kuna muutuste kohta informatsiooni ei säilitata, siis on tagantjärgi keeruline või võimatu kindlaks teha postiloendi kaudu e-kirja saanud isikute ringi;
- Isegi kui see tundub enesestmõistetav: andke alati oma e-kirjale teema. See aitab e-kirju leida ja sorteerida;
- Kasutage e-kirja teatevalikuid, nagu „kiire“ vaid siis, kui see on absoluutselt vajalik, kuna kõik e-kirja rakendused ei suuda neid korrektselt taasesitada.

8.2. E-kirja koostamisel on soovitatav järgida järgnevaid juhiseid:

- Kus võimalik, koostage ja saatke e-kirjad lihtteksti või HTML formaadis, kuna kõik e-kirjade programmid ei suuda korrektselt kuvada muid formaate või kirjatüüpe;
- E-kirjale on soovitatav vastata kirja saatja poolt kasutatud formaadis s.t kui kiri saabus lihtteksti kujul, tuleb vastus saata samuti lihtteksti kujul. Vastasel juhul ei pruugi saatja e-kirjade programm vastust õigesti kuvada;
- Kasutage manuseid mõistlikult (saatke pilte üldlevinud formaadis manustena ja mitte kleebitult e-kirja või teistesse dokumentidesse);
- E-kirjale vastates ärge lisage oma kommentaare esialgsesse e-kirja teksti sisse, vaid sisestage oma kommentaarid esialgse e-kirja kohale ja jätke esialgse e-kirja päise ja oma allkirja vahele teie teadet ja esialgset teadet eristav tühik või muu märgend;

- Kasutage saatja olulisi kontaktandmeid sisaldavat signatuuri, mis hõlbustab saatjaga ühenduse võtmist.

8.3. E-kirjade haldamisel on soovitatav järgida järgnevaid juhiseid:

- Tagage, et sissetulevate e-kirjade kausta hallatakse hoolikalt ja regulaarselt;
- Soovitatav on otsustage kohe e-kirja saamisel või saatmisel, kas e-kiri väärib salvestamist ning kui e-kiri kuulub salvestamisele, siis tõstke see koheselt õigesse kausta;
- Kui puudub dokumendihaldussüsteem või muu spetsiaalne e-kirjade süstematiseerimise lahendus, siis looge säilitamisele kuuluvate e-kirjade jaoks eraldi kataloogid nende leidmise hõlbustamiseks;
- Säilitamisele kuuluvate e-kirjade kataloogidest tuleb teha regulaarselt varukoopiad. Aegajalt on soovitatav kontrollida ja veenduda varukoopiate sisu korrektsuses.
- Säilitage ja arhiveerige alati originaalne e-kiri; ärge säilitage säilitamisele kuuluvaid e-kirju kopeerituna teise rakendusega salvestatavasse faili, kuna selline meetod kahjustab tõsiselt dokumendi autentsust ja terviklikkust (mh metaandmed[6] lähevad kaduma);
- Advokaadibürood võivad kehtestada erinevaid nõudeid advokaadibüroo sisesele ja välisele e-kirjavahetusele. Advokaadibüroo sisesele e-kirjavahetusele võib rakendada leebemaid nõudeid (nt ei lisata erinevaid välistele saatjatele mõeldud teateid ja signatuure);
- E-kiri, mille advokaat saadab või saab osana oma kutsetegevusest on ametlik e-kiri. E-kiri, mille advokaat saadab või saab eraisikuna ja mis pole saadetud seoses ametiülesannetega, on isiklik e-kiri;
- Soovitatav on e-kirjale lisatavate spetsiaalsete märgete või teatistega selgelt eristada isiklik e-kiri ametlikust e-kirjast;
- Kaalumist väärib ka advokaadi kutsetegevuseks kasutatava e-postiaadressi mittekasutamine isiklikuks kirjavahetuseks.

9. ELEKTROONILISTE DOKUMENTIDE JA E-KIRJADE ARHIVEERIMINE

9.1. Elektrooniliste dokumentide arhiveerimine

9.1.1. Kutsetegevusega seonduvate elektrooniliste dokumentide säilitamisel kehtivad samad sisulised nõuded nagu kirjalikus vormis dokumentide säilitamise suhtes.

9.1.2. Advokaadibüroodel on soovitatav rakendada sisemisi reeglid elektrooniliste dokumentide ja e-mailide ja e-kirjade säilitamise kohta. Juhend võib määrama selle, millised elektroonilised dokumendid ja e-kirjad, millises formaadis ja kus säilitamisele kuuluvad.

9.1.3. Soovitatav on kliendiga kokku leppida, kas ja kui kaua õigusteenuse osutamise ajal ja peale õigusteenuse osutamist säilitab advokaadibüroo õigusteenuse osutamisega seonduvaid dokumente ja elektroonilist kommunikatsiooni.

[6] Vt punkti 10

9.2. Elektroonilise kommunikatsiooni säilitamise põhinõuded

9.2.1. Kutsetegevusega seonduvad elektroonilised dokumendid või e-kirjad tuleb säilitada kas paberkandjal kliendi toimikus või eelistatult digitaalses arhiivis.

9.2.2. E-kirjade säilitamisväärtuse hindamisel on soovitatav lähtuda vähemalt samadest kriteeriumitest, nagu paberkandjal dokumentide säilitamisel. Arvestades e-kirjade arhiveerimise lihtsust ja kommunikatsiooni konteksti väärtuslikkust on soovitav säilitada kutsetegevusega seonduv e-kirjavahetus täies ulatuses.

9.2.3. Elektrooniliste dokumentide arhiveerimiseks salvestamisel on soovitatav kasutada üldiselt aktsepteeritud formaate ning kasutada sama formaati kõigi dokumentide ja e-kirjade jaoks. Elektroonilisi dokumente ja e-kirju arhiveerides tuleb meeles pidada, et oluline on nii nende loetavuse kui ka originaalkujul säilimise tagamine.

9.2.4. Elektroonilise kommunikatsiooni pikaajalise säilitamise korral tuleb tagada, et säilivad ka elektroonilise kommunikatsiooni sisuga tutvumiseks vajalikud programmid ja seadmed.

9.2.5. Isegi kui e-kiri on kustutatud, võib seda siiski veel taastada. Vastavas küsimuses tuleb pöörduda IT-spetsialisti poole.

9.2.6. Elektroonilise kommunikatsiooni paberkandjal säilitamise korral on säiliku autentsuse kontrollimise võimaldamiseks soovitatav samal viisil säilitada ka vastava kommunikatsiooni metaandmed. Siiski on soovitatav lisaks paberkandjatele või paberkandja asemel säilitada e-kirjad digitaalsel kujul.

9.3. Digitaalallkiri

9.3.1. Digitaalallkirjastatud dokumendid tuleb salvestada ja säilitada digitaalallkirjastatud kujul (.ddoc). Kuna .ddoc ei ole tarkvaratootjate poolt üldlevinult tunnustatud, siis võib olla otstarbekas digitaalselt allkirjastatud dokumentide salvestamine ka digitaalselt allkirjastamata kujul. Viimasel juhul tuleb tagada allkirjastamata faili digitaalselt allkirjastatud originaali säilitamine ja leitavus.

9.3.2. Lisaks Eestis seadustatud digitaalallkirja formaadile on (muudes riikides) levinud teistsugused digitaalallkirjastamise viisid ja formaadid. Mõnes välisriigis kasutatavale digitaalse allkirjastamise vahendile on omistatud võrdne õiguslik tähendus Eesti digitaalse allkirjaga. Vähemlevinud digitaalallkirjastamise meetoditega kokkupuutumisel peab advokaat kontrollima vastava digitaalallkirjastamise meetodi usaldusväärsust ja õiguslikku tähendust.

9.3.3. Eestis vähemlevinud meetodil digitaalallkirjastatud dokumentide säilitamisel tuleb juhinduda digitaalselt allkirjastatud dokumentide säilitamise üldistest soovitustest, kuid täiendavalt on soovitatav lisada digitaalallkirja usaldusväärsuse kontrollimise tulemused, saadud lisaandmed (nt vastused päringutele) või ülevaade usaldusväärsuse veendumiseks tehtud toimingutest.

9.4. Autentsus

9.4.1. Autentsus on nii elektrooniliste kui ka mitteelektrooniliste dokumentide säilitamise võtmekontseptsioon, mis võimaldab tõendada dokumendi säilimist esialgsel kujul, dokumendi looja või saatja isikut ja dokumendi loomise või saatmise aega.

9.4.2. Kontekst, milles dokument on valmistatud ja kasutatud ning muudatused, mis on tehtud dokumendi haldamise ja säilitamise käigus, on sageli kirjeldatud metaandmetes. Metaandmed teevad võimalikuks arhiveeritud dokumendi autentsuse kontrollimise ja tõendamise.

9.4.3. Elektroonilise dokumendi terviklikkuse säilitamiseks ja autentsuse kontrollimise võimaluste tagamiseks on soovitatav:

- dokument arhiveerida võimalikult originaalsel kujul (nt e-kirjad säilitada koos manusega);
- elektroonilise dokumendi konverteerimisel teise formaati säilitada ka originaalformaadis elektrooniline dokument;
- kirjeldada ja säilitada dokumendi originaalne kontekst ja säilitada dokumendiga tehtud kõigi toimingute ja sellega seotud isikute katkematut nimekirja.

9.4.4. Kui elektroonilist dokumenti taasesitatakse selle loomise arvutikeskkonnast erinevas keskkonnast, siis võib see dokument kuvada ja toimida esialgsest erinevalt. Kui dokumendi ülekandmine või konverteerimine teise arvutikeskkonda pole teostatud teadlikult ja õigesti valitud viisil, siis võib elektroonilise dokumendi autentsus saada kahjustatud.

10. PEIDETUD ANDMETE (METAANDMETE) HALDAMINE

10.1. Peidetud andmed (metaandmed)

10.1.1. Elektroonilised dokumendid ja muud arvutifailid sisaldavad tihti täiendavat informatsiooni, mis edastab teavet dokumendi või selle väidetava autori kohta ja mis võib olla avatud või peidetud, näiteks autor, loomise kuupäev ja aeg ja viimane muudatus, kasutatud mall ja muu selline.

10.1.2. Sõltuvalt informatsiooni loomusest ja kontekstist, milles viimane ilmub võib informatsioon olla kasulik, kahjutu või piinlik, potentsiaalselt ohtlik või viia juhusliku konfidentsiaalse ja saajale mittemõeldud informatsiooni avalikustamiseni. Teisest küljest võivad sellised andmed olla advokaadi jaoks kasulikud või isegi eluliselt vajalikud. Seetõttu peab advokaat olema teadlik metaandmete olemasolust ning astuma samme metaandmete säilitamiseks ja hoiduma mittesoovitavate metaandmete edastamisest teistele pooltele.

10.1.3. Advokaadid loovad sageli uue dokumendi varem loodud sarnase dokumendi põhjale. Kui advokaat ei ole teadlik metaandmete olemasolust ja õigest kasutuselevõtust, siis on võimalik, et varasema dokumendi põhjal loodud dokumendi saaja võib peidetud andmetega tutvudes saada informatsiooni selle kohta, millise kliendi jaoks oli loodud algdokument ja milliseid muudatusi või parandusi tehti algdokumenti erinevate isikute poolt, kes seda läbi vaatasid.

10.1.4. Dokumendi sisu kopeerimine ja selle kleepimine uude dokumenti pole alati piisav, et vältida metaandmete uude dokumenti kandumist, kuna mõnda tüüpi metaandmed on seotud tekstiga ning sellise teksti kleepimine uude dokumenti kopeerib uude dokumenti ka algse teksti metaandmed.

10.2. Sisu multiversioonid

10.2.1. „Jälita muudatusi" („Track changes") funktsioon programmis Microsoft Word on kasulik, et näha muudatusi, mis on erinevate kasutajate poolt tehtud erinevatesse dokumendi versioonidesse, kuid seda funktsiooni peab kasutama kohase ettevaatusega.

10.2.2. „Jälita muudatusi" funktsiooni kasutatakse enamasti selliselt, et kõik muudatused on ekraanil nähtavad („Lõplik koos märgistusega"). Rohkelt muudatusi sisaldava dokumendiga töötades võib olla mugavam kasutada „Jälita muudatusi" funktsiooni režiimis, kus muudatusi jälgitakse, kuid neid ei näidata ekraanil („Lõplik"). Sellises režiimis töötades võib mitte märgata, et „Jälita muudatusi" funktsioon on sisse lülitatud ning edastada saajale dokument, millesse tehtud muudatused ja kommentaarid on saaja jaoks nähtavad või leitavad.

10.2.3. Seetõttu tuleb peale dokumendi muutmist dokumendi edastamiseks salvestamisel igakordselt veenduda, et „Jälita muudatusi“ funktsioon on välja lülitatud ning kõik muudatused kas aktsepteeritud või hüljatud (v.a kui jälitatud muudatuste saajale saatmine on teadlik).

10.2.4. Kui advokaatide vahel on kokku lepitud elektroonilise dokumendi erinevate versioonide vahetamine „Jälita muudatusi“ funktsiooni kasutades, siis peab advokaat tagama, et kõik tema poolt tehtud muudatused on dokumendi saaja jaoks nähtavad. Tehtud muudatuste (osaline) varjamine on vastuolus kutseeetika nõuetega.

10.3. PDF kasutus dokumentide edastamiseks

10.3.1. PDF formaadis (.pdf) dokumendid on hea alternatiiv Microsoft Word formaadis (.doc / .docx) dokumentidele.

10.3.2. Enamasti ei kaasne PDF formaadis dokumentidega eelnevalt märgitud probleeme metaandmete ning muudatuste jälitamisega, sest PDF formaat esitab dokumenti üldiselt nii, nagu seda kuvatakse või prinditakse. Pange tähele, et PDF dokumendis tekstile või selle osale valge või musta kasti lisamine varjab, kuid ei kustuta kasti alla jäävat teksti. Kasti eemaldamise korral muutub tekst jälle nähtavaks. PDF dokumendid toetavad mitmeid kasutaja-spetsiifilisi peidetud andmeid, kuid praktikas on selliste andmete kasutus väga ebaharilik. Kindluse mõttes on siiski soovitatav enne dokumendi edastamist ,,Atribuute” kontrollida.

10.3.3. Oluline on märkida, et eksisteerib erinevat tüüpi PDF dokumente. PDF dokument, mis on loodud teksti skaneerimisega skanneri või fotokoopiamasinaga, sisaldab üksnes originaaldokumendi kujutiskoopiat. Sellises dokumendis sisalduvat teksti ei saa sõnaotsingu vahenditega töödelda ja seda ei saa hõlpsasti lõigata ja kleepida teistesse dokumentidesse. PDF dokument, mis on salvestatud sõnatöötluse programmis, on tavaliselt talletatud tekstina ja mitte lihtsalt kujutisena. Dokumendid selles vormis nõuavad vähem talletusruumi kui kujutisena PDF dokumendid. Neil põhjustel peaks PDF formaadis dokumente üldiselt salvestama tekst PDF dokumentidena.

10.4. Spetsiaalsed vahendid metaandmete leidmiseks ja eemaldamiseks

10.4.1. Eksisteerivad spetsiaalsed arvutiprogrammid, mis analüüsivad dokumente ja suudavad eemaldada varjatud sisu, dokumendi eelmised versioonid või muud metaandmed. Soovitatav on selliste vahendite allalaadimine ning kasutamine enne elektrooniliste dokumentide edastamist. Neid vahendeid võib alla laadida näiteks Microsofti veebilehelt ja Office2003/XP versioonis. Wordi Office 2007 versioonis on vastav funktsioon juba vaikimisi lisatud (vt “Office nupp”->“Valmista ette“->“Kontrolli dokumenti”).

11. SOOVITUSED KASUTATAVATELE SALASÕNADELE

11.1. Mistahes kasutatav salasõna peab olema valitud selliselt, et seda on võimalik meelde jätta, kuid pole lihtne ära arvata. Salasõna ei ole soovitatav ühelegi kaitsmata kohas asuvale andmekandjale krüpteerimata kujul jäädvustada või dokumenteerida ega teatavaks teha ühelegi isikule.

11.1.1. Salasõna on soovitatav koostada suur- ja väiketähtede ning numbrite kombinatsioonist. Soovitav on lisaks kasutada kirjavahemärke. Salasõna soovitatav pikkus on vähemalt 9 sümbolit.

11.1.2. Salasõnade parema turvalisuse tagamise hõlbustab järgmistest soovitustest kinnipidamine:

- Salasõnaks ei tohiks olla suvaline nimi, sõnaraamatus leiduv sõna või kuupäev;
- Ärge koostage salasõna vaid ühesugustest sümbolitest ega klaviatuurijärjestuses tähtedest ja numbritest;
- Ärge tuletage salasõna kasutaja isiklikust informatsioonist, mida keegi võib lihtsa vaevaga ära arvata, näiteks kasutajanimi, pereliikme või lemmiklooma nimi, oma telefoni- või autonumber, enda või perekonnaliikme sünnipäev ning aadress jne;
- Püüdke vältida lihtsasti tuletatavat parooli eelnevalt kasutatud salasõna, näiteks muutes paroolis ühte tähte/numbrit.

11.1.3. Salasõna on soovitatav vahetada regulaarselt, soovitatavalt iga 90 päeva tagant. Süsteemidesse ligipääsuks ID-kaardi kasutamisel PIN koodi regulaarselt vahetada ei tule.

11.1.4. Tööjaama juurest lahkudes peaks kasutaja sulgema tööjaama, väljuma arvutivõrgust või lühema pausi korral lukustama tööjaama (näiteks Windows logo klahv + L).

11.1.5. Oma isiklikku salasõna ega PIN koodi ei tohiks kasutaja mitte kunagi mitte kellelegi avalikustada. Administraatoril/IT-s on reeglina olemas eraldi juurdepääsuõigused kasutaja probleemide lahendamiseks ning ta ei pea teadma kasutaja parooli.

12. MOBIILSEADMETE JA ANDMEKANDJATE KASUTAMINE

12.1. Mobiilsideseadmete kasutamine

12.1.1. Kui advokaat kasutab elektronposti ja kalendri haldamiseks mobiiltelefoni või muud mobiilsideseadet, siis vaikimisi on mobiilsideseadmes talletatud e-kirjad ja kalendrikirjed, samuti serverist e-kirjade edasist lugemist võimaldav kasutajatunnus ja salasõna, ilma parooli küsimata ligipääsetavalt.

12.1.2. Kõrvaliste isikute ligipääsu vältimiseks mobiilsideseadmes talletatavale informatsioonile on soovitatav rakendada mobiiltelefonile automaatselt järgmised piirangud:

- Tagage, et telefon lukustuks automaatselt, kui seda pole üle 15 minuti järjest kasutatud;
- Iga telefoni ekraani lahtilukustamise korral küsitakse kasutajalt vähemalt 4-kohalist lukukoodi;
- Vahetage telefoni lukukood regulaarselt ning vahetamise korral kasutage erinevaid lukukoode;
- Seadistage telefon nii, et lukukoodi korduval ebakorrektsel sisestamisel kustutatakse telefonist kõik andmed, failid, sätted ja kontaktid;
- Mobiiltelefoni mälu ja mälukaart on soovitav krüpteerida (kui mobiiltelefon seda toetab) nii, et sinna salvestatud faile ja elektronposti ei oleks võimalik ilma telefoni lukukoodi teadmata kätte saada;
- Mobiilseadmed võivad võimaldada kauglukustust ning andmete distantsilt kustutamist. Soovitatav on vastavad võimalused aktiveerida ning telefoni kadumisel neid võimalusi viivitamatult kasutada;

- Mobiilseadme kadumise korral on soovitatav viivitamatult muuta e-kirjade serverist mobiilseadmesse lugemiseks vajalik kasutajatunnus ning salasõna.

12.2. Andmekandjate kasutamine

12.2.1. Digitaalseks andekandjaks (edaspidi andmekandjad) loetakse seadmeid, mille peale saab salvestada digitaalset infot (kõvakettad). Eemaldatavateks andmekandjateks loetakse andmekandjatest neid, mida saab ilma tööjaama korpust avamata tööjaama küljest või arvutivõrgust eemaldada või sinna lisada (USB pulgad, mälukaardid, CD/DVD plaadid, telefonide ja fotoaparaatide mälukaardid jne).

12.2.2. Eemaldatavate andmekandjate kasutamisel tuleb arvestada, et nende kasutamine on kõrgendatud ohu allikas. Eemaldatavaid andmekandjaid on lihtne kaotada, varastada, need võivad rikneda ja neid võidakse kasutada tööjaama viirustega nakatamiseks.

12.2.3. Kui töökohustuste tõttu on mõnes tööjaamas vajalik kasutada kolmandate isikute andmekandjaid, siis on soovitav IT-spetsialisti sellest teavitada. Vajadusel on soovitatav tõsta sellise tööjaama turvalisust.

12.2.4. Konfidentsiaalse informatsiooni salvestamine eemaldatavale digitaalsele andmekandjale on soovitatav üksnes erandjuhtumil ning otsese vajaduse korral.

12.2.5. Krüpteerimata konfidentsiaalset informatsiooni sisaldavat andmekandjat tuleb transportida isikliku järelevalve all ja hoida analoogselt konfidentsiaalset informatsiooni sisaldavate paberkandjate suhtes rakendatavatele nõuetele ja hoolsusele.

12.2.6. Konfidentsiaalset informatsiooni sisaldava andmekandja viimisel väljapoole advokaadibürood tuleb andmekandja krüpteerida ID-kaarti kasutades või mõne muu piisavalt turvalise krüptolahendusega.

12.2.7. Kui konfidentsiaalse informatsiooni andmekandjatel hoidmine ei ole enam vajalik, on soovitatav informatsioon andmekandjalt koheselt kustutada või andmekandja hävitada nii, et sellelt pole võimalik informatsiooni taastada.

12.2.8. Digitaalse andmekandja andmisel teise isiku valdusesse on soovitatav eelnevalt veenduda, et andmekandja ei sisalda informatsiooni, millele andmekandja saanud isik juurdepääsu omada ei tohi.

12.2.9. Konfidentsiaalse informatsiooni kopeerimisel eemaldatavale andekandjale või konfidentsiaalse informatsiooniga eemaldatava andmekandja ühendamisel tööjaamaga võib olla soovitatav kasutada juhtmevaba ühenduse (sinihammas, infrapuna) asemel juhtmega ühendust.

12.2.10. Konfidentsiaalset informatsiooni sisaldava andmekandja kadumisest või vargusest on soovitatav koheselt teavitada advokaadibüroo pidajat.

12.3. Sülearvuti kasutamise ja hoidmise kord

12.3.1. Vältimaks sülearvuti varastamist, kaotamist või riknemist on kasutajal soovitatav järgida järgnevaid juhiseid:

- Avalikes kohtades hoidke sülearvutit alati isikliku järelevalve all;
- Ärge jätke sülearvutit valveta kohtadesse, kus on oht selle varastamiseks (auto salongi, lahtise akna alla, avalikku kohta järelevalveta jne);
- Pärast sülearvuti viibimist temperatuuril alla 0^{o} C laske sülearvutil enne käivitamist seista toatemperatuuril, tagamaks, et sülearvuti temperatuur enne kasutamist tõuseks toatemperatuuriga samale tasemele;

- Ärge jätke sülearvutit magnetvälja (näiteks varjestamata kõlarite lähedusse), otsese päikese kiirguse või kõrge temperatuuri kätte, samuti tolmusesse või niiskesse keskkonda;
- Transportige sülearvutit vaid selleks ettenähtud kotis;
- Reisimisel kandke sülearvutit käsipagasina;
- Võimaluse korral laske sülearvutile (koos kotiga) teha röntgeni asemel käsitsi läbivaatus;
- Võimaluse korral hoidke sülearvuti eemal metallidetektorist.

12.3.2. Sülearvuti vargusest, kaotamisest, (ajutisest) kolmanda isiku valdusesse sattumisest või hävimisest on soovitatav viivitamatult teavitada advokaadibüroo pidajat.

12.3.3. Tagamaks sülearvutis olevate andmete turvalisust ja piiramaks viiruste levikut on kasutajal soovitav järgida järgnevaid juhiseid:

- Arvestage muuhulgas, et väljaspool advokaadibüroo sisevõrku (eriti avalikes WIFI võrkudes) võidakse krüpteerimata ühendusi pealt kuulata;
- Sülearvutisse logimiseks eelistage parooli asemel kiipkaardi ja PIN koodi kombinatsiooni;
- Sisestage paroolid ja/või kiipkaardi PIN kood nii, et kõrvalised isikud ei näeks, milline parool/PIN kood sisestati;
- Sülearvuti juurest lahkumisel sulgege sülearvuti ja eemaldage kiipkaart (kui seda kasutati sülearvutisse logimiseks);
- Juhtmeta ühenduste (WIFI, infrapunaliides, sinihammas) kasutamisel vältige nende tarbetut aktiveerimist ning konfidentsiaalsete andmete puhul eelistage kaabelühendust;
- Advokaadibüroo võrgus läbi võrgukaabli olemise ajal lülitage välja kõik sülearvuti juhtmeta (WIFI, infrapunaliides, sinihammas) ühendused (sülearvutil on selleks tavaliselt spetsiaalne nupp);
- Kahtluse või teadmise korral, et sülearvuti tulemüür ja/või viirusetõrjetarkvara ei ole töökorras või on välja lülitatud, ärge ühendage sülearvutit avalikku arvutivõrku, vaid andke sülearvuti võimalikult kiiresti büroo IT-spetsialistile ülevaatamiseks;
- Kahtluse või teadmise korral, et sülearvutis on viirus, ärge ühendage sülearvutit ei advokaadibüroo ega avalikku arvutivõrku, vaid teatage juhtunust IT-spetsialistile, kes organiseerib sülearvuti võimalikult kiire ülevaatamise.