B 5.1 INFORMATIONSSÄKERHETSANVISNING (24.1.2019, ändrad 16.1.2020)

Finlands Advokatförbunds delegation har 24.1.2019 gett följande anvisning gällande informationssäkerhet vid advokatverksamhet. Anvisningen träder i kraft 1.6.2019. *Förändringarna, som godkänts av delegationen 16.1.2020, träder i kraft 1.2.2020*.

Advokaten ska se till att

1. advokatens egen och byråpersonalens kompetens gällande informationssäkerhet är på tillräckligt hög nivå så att denna anvisning och informationssäkerhetsguiden (B 5.2) kan tillämpas vid ordnandet av verksamheten. En advokatbyrå med minst 10 arbetstagare ska ordna en extern informationssäkerhetsrevision med jämna mellanrum.

2. granskningar eller begäran om information som angår advokatbyrån eller advokatverksamheten och som avser uppgifter som samlas och överlåts till kunder, serviceleverantörer eller andra utomstående parter och som gäller praktikaliteter kring advokatverksamheten, kundrelationer eller uppdrag, kan inte utföras. (16.1.2020, i kraft 1.2.2020)

3. de fysiska lokaler som är i användning är låsta och även i övrigt skyddade. Allt material som omfattas av advokatsekretessen, oavsett hur informationen har sparats eller förvarats, är skyddat.

4. information i utrustning och redskap som används inom advokatverksamheten är krypterad. Denna utrustning och dessa redskap får inte ges i utomståendes användning. För bevarandet av advokatsekretessen ska man undvika att använda främmande personers utrustning eller att ansluta sådan till egen utrustning. Man ska beakta utrustningens livscykel så att utrustning som inte längre får uppdateringar, tas ur bruk och byts mot ny.

5. de trådlösa nätverken som byrån eller advokaten använder i sin utrustning är skyddade. Besökare i byrån ska inte ha tillgång till byråns interna nätverk (ett eget trådlöst nätverk har exempelvis ordnats för besökare). Vid användning av allmänna nätverk ska en krypterad anslutning användas (VPN eller motsvarande).

6. de lösenord som används är tillräckligt komplicerade, de byts ut tillräckligt ofta och andra får tillgång till dem. Extra identifieringsmetoder används om möjligt för att uppnå en högre informationssäkerhetsnivå.

7. informationssäkerhetsprogramvaror och brandväggar är i skick. Uppdateringar av utrustning, operativsystem, program och applikationer installeras utan obefogat dröjsmål.

8. endast sådana personer ska ha tillgång till handlingar som behöver eller kan behöva konfidentiell information eller åtminstone åtkomst till dessa filer för att sköta sina arbetsuppgifter.

9. säkerhetskopiering görs regelbundet. Utrustning och medier som innehåller säkerhetskopior har krypterats och förvarats omsorgsfullt. Man ska se till att säkerhetskopiorna testas regelbundet.

10. samtliga avtal som ingås med utomstående tjänsteleverantörer uppfyller kraven på informationssäkerhet, dvs. innehåller i synnerhet villkor som gäller sekretess (särskilt när det gäller externa IT-tjänster, parter som har tillträde till lokalerna).

11. allt material som skickas med e-post eller på annat elektroniskt sätt är vid behov krypterat. Advokaten ska se till att materialet krypteras, om innehållet är särskilt känsligt eller klienten kräver krypterad kommunikation, samt vid behov instruera sin klient att leverera materialet med skyddad metod.

12. handlingar och annat material sparas, förvaras, arkiveras och förstörs på ett säkert sätt.

13. all utrustning som innehåller information tas ur bruk och töms på ett informationssäkert sätt (*datorer, mobila enheter, lagringsmedier osv.)*. Detsamma gäller lagrings- och nättjänster.

14. kontinuiteten i verksamheten har ombesörjts så att nödvändig information som är viktig med tanke på byråns kontinuitet har dokumenterats i samlad form och att denna dokumentering är tillgänglig för de parter som svarar för kontinuiteten.