D3 - Zabezpečenie minimálnej bezpečnosti na ochranu údajov na notárskom úrade

Interný predpis prijatý prezídiom Notárskej komory Slovenskej republiky (ďalej len NK SR) o zabezpečení minimálnej bezpečnosti na ochranu údajov na notárskom úrade.

PREAMBULA

Prezídium Notárskej komory Slovenskej republiky (ďalej len „prezídium“) podľa § 12 ods. 1 písm. d/ a ods. 3 zákona č. 323/1992 Zb. o notároch a notárskej činnosti v znení neskorších predpisov (ďalej len „Notársky poriadok“) vydáva predpis o zabezpečení minimálnej bezpečnosti na ochranu údajov na notárskom úrade v nasledovnom rozsahu:

- Zabezpečenie ochrany údajov uložených na notárskych úradoch (ďalej len NÚ) tak v papierovej, ako aj v elektronickej forme s dôrazom na osobné údaje proti ich strate, zneužitiu, odcudzeniu a poškodeniu.
- Zabezpečenie ochrany údajov v Centrálnom informačnom systéme Notárskej komory SR (ďalej len CIS).
- Zabezpečenie bezpečného prenosu elektronických údajov.
- Zabezpečenie bezpečného archivovania týchto údajov na NÚ tak v elektronickej ako aj papierovej forme.
- Zabezpečenie bezpečného spracúvania údajov na NÚ.
- Zabezpečenie fyzickej a objektovej bezpečnosti pre ochranu osobných údajov. V rámci fyzickej a objektovej bezpečnosti dodržiavať podmienky vstupu a výstupu osôb do chránených objektov (priestorov), pohybu citlivých informácií v objekte, opatrenia určujúce činnosti pri narušení objektu.
- Zabezpečenie personálnej bezpečnosti na NÚ.

Čl. 1
Predmet úpravy

(1) Cieľom tohto interného predpisu je stanoviť postupy a pravidlá súvisiace s bezpečným správaním používateľov CIS pri zabezpečovaní činností NÚ.

(2) Tento vnútorný predpis sa vzťahuje na všetky NÚ (notárov a ich zamestnancov) a v relevantnom rozsahu aj na tretie strany.

Čl. 2
Základné práva a povinnosti používateľov

(1) Každý používateľ CIS má právo využívať funkcionalitu CIS v rozsahu jemu pridelených prístupových oprávnení a v závislosti od svojej pracovnej pozície.

(2) Technické a programové vybavenie NÚ musí byť využívané len v súlade s pravidlami uvedenými v tomto vnútornom predpise a v súlade s bezpečnostnou politikou CIS na NK SR a ďalšími internými predpismi upravujúcimi informačnú a kybernetickú bezpečnosť v prostredí CIS na NK SR.

(3) Notár poučí svojich zamestnancov o pravidlách bezpečnosti, ochrane osobných údajov a fyzickej či kybernetickej bezpečnosti v prostredí NÚ. O poučení vyhotovuje záznam, ktorý podpíše notár aj zamestnanec. Vzor takéhoto záznamu je prílohou č. 1 tohto predpisu.

(4) Používanie technického a programového vybavenia na NÚ na iné ako pracovné účely sa neodporúča a musí byť odsúhlasené notárom.

(5) Každý používateľ CIS je povinný:
   a) dodržiavať pokyny uvedené v tomto vnútornom predpise, ako aj inštrukcie administrátorov NK SR týkajúce sa bezpečného používania technického a programového vybavenia a CIS,
   b) zabrániť odcudzeniu, zneužitiu, strate alebo poškodeniu používaného technického a programového vybavenia ako aj iných citlivých informácií súvisiacich s CIS,
   c) umožniť prístup určenému zmluvnému poskytovateľovi servisu k IT technológiám za účelom vykonania potrebného servisného zásahu, ak tento servis notár nevykonáva svojpomocne,
   d) pri elektronickom spracovaní údajov dodržiavať požiadavky relevantných vnútorných predpisov.

Čl. 3
Prideľovanie a používanie IT prostriedkov

(1) Notár pre plnenie notárskej činnosti vybaví NÚ takou výpočtovou technikou, ktorá spĺňa minimálne technické požiadavky CIS, požiadavky na bezpečnú komunikáciu, bezpečné uchovávanie a spracovanie dát.

(2) Notár na plnenie pracovných úloh zamestnancom NÚ zverí do používania IT prostriedky a zariadenia, ktoré sú oprávnení používať len v rámci svojho poverenia (§ 22,25,27 ods.2 Notárskeho poriadku), ak notár nerozhodne inak. Používatelia sú povinní ochraňovať ich pred poškodením, stratou, zničením alebo zneužitím a využívať povolené vybrané služby počítačových sietí iba v rámci pravidiel stanovených notárom, bezpečnostnou politikou CIS a týmto predpisom.

(3) Bez vedomia notára je používateľom zakázané svojvoľne robiť akékoľvek zásahy do hardvéru ako montáž, demontáž, vyberanie dielov, otváranie a rozoberanie zariadení, zmenu konfigurácie hardvéru, poškodzovanie a znečisťovanie prostriedkov IT, prepojovanie počítačov, tlačiarní a manipulácia s prepojovacími káblami siete, vrátane všetkých ostatných sieťových komponentov a podobne, okrem úkonov realizovaných zmluvným poskytovateľom servisu pre NÚ alebo okrem úkonov súvisiacich s doplnením a výmenou štandardného spotrebného materiálu určeného pre daný druh hardvéru.

(4) Používateľ CIS musí pri používaní IT prostriedkov a zariadení dodržiavať nasledovné zásady:
   a) prístup k uloženým údajom dôsledne chrániť pomocou vstupného mena a hesla, prípadne vhodného bezpečnostného biometrického prostriedku (napr. rozpoznávanie tváre, odtlačku prsta a pod.), ktoré v plnej miere nahrádzajú meno a heslo), zariadenia musia byť nastavené tak, aby pri nečinnosti užívateľa boli automaticky odhlásené z operačného systému,
   b) počas práce zabezpečiť, aby sa k informáciám na zariadení nedostali neoprávnené osoby (napr. nahliadaním ponad plece),
   c) ubezpečiť sa, že zariadenie je vhodne zabezpečené tak v kancelárii, ako aj počas prípadného prenosu,
   d) v prípade potreby odkladať prenosné zariadenie na miesto, kde nie je nápadné, predovšetkým ho nenechávať na viditeľnom mieste,
   e) v prípade použitia vzdialeného prístupu, chrániť prístupové údaje do vnútorného prostredia NÚ,
   f) zabezpečiť, aby citlivé informácie neboli sprístupnené osobám, ktoré na to nemajú oprávnenie, v prípade potreby používať na ochranu citlivých informácií šifrovací softvér,
   g) stratu alebo krádež IT vybavenia oznámiť okamžite notárovi. Ten následne udalosť oznámi zamestnancom CIS na NK SR,
   h) zamestnancom NÚ je bez vedomia notára zakázané kopírovať existujúce programové vybavenie a údaje z CIS, lokálnych diskov pracovných staníc, sieťových diskov a pamäťových médií okrem prípadov zálohovania údajov,
   i) je zakázané pripájať k pracovnej stanici alebo do počítačovej siete pamäťové médiá získané z neznámeho zdroja (napr. USB kľúč, externý disk a pod.),
   j) je zakázané vyvíjať činnosti smerujúce k prelomeniu bezpečnostných mechanizmov chrániacich CIS.

(5) Do siete NÚ je zakázané pripájať zariadenia, ktoré nie sú majetkom notára, výnimku môže povoliť len notár.

(6) V prípade používania IT prostriedkov a zariadení mimo priestorov NÚ je používateľ povinný chrániť IT techniku, vybavenie, dáta a informácie pred neoprávneným prístupom.

(7) Pre prácu s IT prostriedkami sú realizované prvotné štandardné nastavenia pre operačný systém a softvér, ktoré zohľadňujú bezpečnostné, prevádzkové a ďalšie požiadavky CIS. Používatelia nemôžu svojvoľne bez súhlasu notára meniť nastavenia operačného systému alebo používaného softvéru. Tieto nastavenia vykonávajú pracovníci zmluvného poskytovateľa servisu pre NÚ (ak túto činnosť notár nezabezpečuje svojpomocne).

(8) V prípade vyradenia IT prostriedku alebo zariadenia NÚ z majetku notára zabezpečiť výmaz a odstránenie všetkých prístupových údajov do CIS a dokumentov obsahujúcich osobné údaje.

Čl. 4
Zásady práce na diaľku a používanie mobilných zariadení

(1) Práca na diaľku znamená, že IT prostriedky a zariadenia NÚ sú používané na výkon práce zamestnancov mimo priestorov NÚ.

(2) Práca zamestnanca NÚ na diaľku musí byť schválená notárom.

(3) Pri práci na diaľku, t. j. mimo kancelárie notára (§ 16 ods. 2 NP), sú používatelia CIS povinní dodržiavať nasledujúce zásady:
   a) používanie verejných alebo súkromných počítačov a zariadení na prístup k sieťam, údajom alebo informačným systémom NÚ či NK SR je zakázané, používatelia CIS môžu pre účely práce na diaľku používať iba zariadenia, ktoré sú majetkom notára a tak je predpoklad, že spĺňajú minimálne bezpečnostné požiadavky,
   b) na prístup do internej siete NÚ je možné používať iba schválené technológie a zariadenia na zabezpečené vzdialené pripojenie,
   c) v prípade vzdialeného pripojenia sú používatelia po dokončení práce povinní odpojiť sa od siete NÚ,
   d) používanie notebookov alebo mobilných zariadení NÚ inými osobami ako sú notár a poverení zamestnanci je zakázané, okrem zmluvných poskytovateľov servisu na NÚ pre výkon svojej činnosti,
   e) ak sa notebook alebo mobilné zariadenie práve nepoužívajú, musia byť bezpečne uložené mimo dohľadu nepovolaných osôb a zabezpečené proti odcudzeniu, strate, poškodeniu a zničeniu,
   f) notebook alebo iné mobilné zariadenie nesmie byť nikdy ponechané bez dozoru, najmä pri cestovaní verejnou dopravou, na verejnom priestranstve alebo v zaparkovanom vozidle,

g) v prípade cestovania sú používatelia CIS povinní nosiť notebook alebo mobilné zariadenia vždy ako príručnú batožinu a nenechávať ju bez dozoru,
h) ak má používateľ CIS prístup k osobným údajom alebo dôverným informáciám, nesmie ich pri práci na diaľku nikdy tlačiť, kopírovať, presúvať alebo ukladať na lokálne pevné disky alebo vymeniteľné médiá, pokiaľ na to nemá výslovné oprávnenie ako súčasť svojej pracovnej úlohy,
i) v prípade, ak je nevyhnutné pristupovať k osobným údajom alebo citlivým informáciám prostredníctvom notebooku alebo mobilného zariadenia na verejných miestach (napr. vo vlaku, v hale hotela, v kaviarni, na letisku a pod.), sú používatelia CIS povinní zabezpečiť, aby obrazovku zariadenia a informácie na nej zobrazené nemohli vidieť neoprávnené osoby,
j) používať elektronickú poštu v doméne notar.sk alebo takú elektronickú poštu, ktorej používanie je spravované zmluvnými podmienkami, ktoré sú v súlade so Zákonom o ochrane osobných údajov a aktuálnych všeobecných nariadení Európskeho parlamentu a Rady o ochrane údajov, (ďalej len GDPR),
k) používanie nezabezpečeného verejného bezdrôtového pripojenia do internetu (WIFI) je neprípustné.

(4) Na zaistenie bezpečnosti mobilných zariadení sú NÚ povinné dodržiavať nasledujúce zásady:
a) každý používateľ CIS, ktorý používa prenosné zariadenie (napr. notebook, mobilný telefón, tablet a pod.) je plne zodpovedný za bezpečnosť a ochranu citlivých a dôverných informácií v ňom a v CIS uložených,
b) každý používateľ CIS, ktorý používa prenosné zariadenie, je zodpovedný za jeho ochranu pred krádežou, zneužitím, stratou alebo poškodením a pre tento účel je povinný dodržiavať zásady podľa čl. 5 tohto dokumentu,
c) pri pripájaní mobilných zariadení do CIS je nutné dodržiavať všetky zásady ochrany pred infiltráciami škodlivým kódom tak, aby nedošlo k prenosu infiltrácie do infraštruktúry NK SR po ich znovu pripojení,
d) odporúča sa aby mobilné zariadenie pri pripojení do iných sietí spustené skenovanie prostredníctvom antivírusového programu a nastavený personálny firewall tak, aby bolo dostatočne ochránené pred napadnutím škodlivým kódom,
e) mobilné zariadenie pre prácu s CIS nesmie byť v rovnakom čase pripojené do inej siete, alebo internetu tak, aby sa tieto siete vzájomne prepojili,
f) pri využívaní mobilných telefónov alebo smartfónov pre prácu s CIS a účtom elektronickej pošty NK SR je používateľ povinný použiť automatické blokovanie zariadenia s potrebou odblokovania,
g) používateľ mobilného zariadenia vybaveného kryptografickými nástrojmi musí šifrovať dáta na lokálnom disku.

Čl. 5
Zásady fyzickej bezpečnosti

(1) V oblasti fyzickej bezpečnosti NÚ je potrebné dodržiavať nasledovné zásady:
a) NÚ má pozostávať najmenej z troch miestností, a to z kancelárie notára, kancelárie zamestnanca (ov) a z predsiene (čakárne). Miestnosti majú byť od seba oddelené pevnou stenou a uzamykateľnými dverami,

b) prístupový vchod do NÚ má byť vybavený pevnými dverami, v prípade potreby bezpečnostnými dverami, najlepšie však dverami certifikovanými Národným bezpečnostným úradom na stupeň utajenia Dôverné alebo Tajné. V prípade viacerých prístupových vchodov, všetky vchody majú byť vybavené vyššie uvádzanými dverami,
c) okná NÚ majú byť zabezpečené proti vniknutiu podľa potreby a to mrežami, alebo bezpečnostnými fóliami, alebo inými mechanickými, prípadne elektronickými spôsobmi. Okná umiestnené na neprístupných miestach (umiestnené vo výške a pod.) nemusia byť vyššie uvedenou ochranou zabezpečené, ak miestnosť v ktorom je okno umiestnené, je chránená iným bezpečnostným systémom proti vniknutiu (detektor pohybu a pod.),
d) všetky priestory NÚ musia byť vybavené poplachovým systémom narušenia (PSN) s akustickou alebo svetelnou signalizáciou a s prepojením na príslušný útvar polície, alebo bezpečnostnej služby, prípadne s možnosťou hlásenia narušenia objektu prostredníctvom telekomunikačného zariadenia zodpovedným osobám. Monitorovanie priestorov môže notár zabezpečiť aj vlastnými bezpečnostnými technológiami (inteligentné mobilné kamerové riešenia).
e) o potrebe hlásiť prípadné narušenie priestorov NÚ na NK SR rozhoduje notár,
f) používateľ CIS nesmie nechávať miestnosť, v ktorej sú umiestnené prvky IT bez dozoru odomknutú (voľne prístupnú v prípade neprítomnosti zamestnancov),
g) v prípade dlhšieho vzdialenia sa z miestnosti musí používateľ CIS uložiť výsledky svojej práce, odložiť médiá obsahujúce dôverné informácie (CD disky, DVD disky, USB kľúče), ako aj citlivé dokumenty na bezpečné miesto alebo miestnosť zamknúť,
h) pred odchodom z práce musí používateľ CIS korektným spôsobom ukončiť prácu v jednotlivých aplikáciách, odhlásiť sa z CIS a z operačného systému,
i) interné dokumenty alebo médiá sa nesmú vyhadzovať do bežných odpadkových košov, ale musia byť bezpečným spôsobom zlikvidované (skartované, viacnásobne bezpečne sformátované resp. fyzicky zlikvidované a pod.),
j) počítačové vybavenie (pracovné stanice, notebooky, tlačiarne, skenery) sa nesmie bez súhlasu notára vynášať z priestorov NÚ.

Čl. 6
Bezpečné používanie hesiel a ďalších autentifikačných prostriedkov

(1) Všetci používatelia, správcovia informačných systémov ako aj tretie strany sú zodpovední za svoje prihlasovacie údaje.

(2) V prípade využívania autentifikačných prostriedkov, ako je napr. čipová karta s certifikátom, USB kľúč, či pridelená SIM karta na prístup z mobilných zariadení, sa postupuje podľa postupov stanovených k danému zariadeniu.

(3) V prípade využívania biometrických vlastností na účely autentifikácie musí byť tento spôsob v súlade s legislatívnymi požiadavkami o kybernetickej bezpečnosti.

(4) Pri prihlasovaní do CIS každý používateľ povinne používa dvojitú autentifikáciu.

(5) V prípadoch, kedy nie je možné pre používateľa zvoliť vlastné heslo napr. pri vytváraní nového používateľského účtu, dostane používateľ pri prvotnom prihlásení bezpečné prechodné heslo. Všetci užívatelia sú povinní zmeniť si prechodné heslo pri prvom prihlásení.

(6) Nové používateľské heslo musí spĺňať nasledujúce podmienky:
   a) minimálna dĺžka hesla do CIS je stanovená administrátorom NK SR,
   b) heslo musí obsahovať minimálne 1 malé písmeno,
   c) heslo musí obsahovať minimálne 1 veľké písmeno,
   d) heslo musí obsahovať minimálne jednu číslicu a špeciálny znak.

(7) Pre všetkých používateľov CIS vrátane zamestnancov tretích strán je zakázané:
   a) zdieľať heslá k personalizovaným účtom s inými osobami,
   b) uchovávať heslá v nešifrovanej podobe, bez ohľadu na to, či sú uchované na elektronickom alebo fyzickom médiu,
   c) používať rovnaké heslo do rôznych systémov,
   d) pri zadávaní hesla kontrolovať svoje okolie a zabezpečiť, aby nikto nemohol fyzicky odpozorovať heslo.

(8) Všetci používatelia CIS vrátane zamestnancov tretích strán musia dodržiavať nasledovné bezpečnostné zásady:
   a) v informačných systémoch vyžadujúcich autentifikáciu môže používateľ pracovať iba pod používateľským účtom, ktorý mu bol oficiálne pridelený,
   b) chrániť svoje identifikačné, autentifikačné a kryptografické prostriedky (heslo, prístupovú kartu, podpisový kľúč a pod.) pred zneužitím, odcudzením, stratou alebo prezradením neoprávnenej osobe,
   c) uchovávať svoje heslá v tajnosti, za vhodný výber hesla je vždy zodpovedný používateľ,
   d) nenechávať svoje heslo na všeobecne dostupnom mieste pri pracovnej stanici,
   e) v prípade podozrenia, že heslo bolo prezradené, okamžite o tom informovať notára a zabezpečiť si zmenu hesla. Ak heslo nemôže byť bezodkladne zmenené, požiada sa administrátor NK SR o blokovanie konta.
   f) pri ukončení pracovného pomeru so zamestnancom notár v CIS vyznačí dátum ukončenia, čím zabráni zamestnancovi ďalší prístup do CIS,
   g) obmieňať heslá v pravidelných intervaloch,
   h) odporúča sa nevčleňovať heslá do automatických procesov prihlasovania (napr. nezaklikávať automatické zapamätanie si hesla),
   i) odporúča sa nepoužívať heslo zložené z mena zamestnanca, dátumu jeho narodenia alebo iného ľahko uhádnuteľného slova, resp. číslic,
   j) používať prednostne silné heslo, ktoré je ťažko uhádnuteľné,
   k) v prípade, ak je potrebné bezpečné ukladanie a management hesiel sa pre tento účel vyžaduje používanie na to určených softvérových produktov,
   l) umožniť iným ako oprávneným osobám (napr. zmluvnému poskytovateľovi servisu pre NÚ) prístup na PC a to len v prípade nevyhnutnosti (napr. v prípade servisného zásahu). Zamestnanci NÚ o takomto prístupe vždy informujú notára,

m) pri ukončení činnosti notára administrátor NK SR bezodkladne zablokuje všetky používateľské účty v CIS na danom NÚ.

Čl. 7
Používanie internetu

(1) Prístup na internet sa na NÚ využíva na pracovné činnosti NÚ.

(2) Aktivity zamestnancov môžu byť pri prístupe k internetu monitorované a zaznamenané, v prípade bezpečnostného incidentu možno túto evidenciu použiť na ďalšie konanie, podozrenie zo zneužívania internetu sa môže stať predmetom šetrenia a vyústiť až do disciplinárneho konania alebo pracovnoprávnej zodpovednosti. O potrebe monitorovania pripojenia NÚ do internetu rozhoduje notár, ktorý pre prípad realizácie takéhoto monitorovania bude postupovať v súlade s § 13 ods. 4 Zákonníka práce[1], aktualizuje primerane svoje podmienky ochrany súkromia o nový účel „aplikovanie kontrolných mechanizmov zamestnávateľa“ a vykoná vlastné posúdenie prevahy oprávneného záujmu pre súvisiace spracúvanie osobných údajov svojich zamestnancov formou tzv. balančného testu, pričom monitorovanie svojich zamestnancov bude vykonávať iba za podmienky, že balančný test poskytne akceptovateľné závery o dostatočne legitímnych, nevyhnutných a proporcionálnych zásahoch NÚ do práv a slobôd zamestnancov NÚ.

(3) Za nevhodné a neprijateľné využívanie prístupu na internet sa považuje najmä:
a) akékoľvek použitie internetu, ktoré bolo na NÚ notárom výslovne zakázané,
b) odosielanie, opätovné zasielanie, opakované prehliadanie akýchkoľvek materiálov, ktoré sú alebo by mohli byť v akomkoľvek zmysle považované za porušenie zákonov SR, medzinárodných dohôd, ktorými je SR viazaná alebo neetické (pornografické, obscénne, urážlivé alebo hanlivé z hľadiska sexuálneho, rasového, politického, náboženského alebo iného), prípadne by mohli mať kriminálnu povahu,
c) akékoľvek používanie internetu, ktoré by mohlo poškodiť dobré meno NK SR, notára, či NÚ, alebo by sa mohlo kvalifikovať ako inak škodlivé.

(4) Používatelia CIS na NÚ využívajúci služby internetu sú povinní najmä:
a) využívať služby internetu v súlade so svojimi pracovnými povinnosťami,
b) v prípade zamestnancov NÚ informovať notára o akýchkoľvek aktivitách, ktoré môžu mať za následok narušenie informačnej a kybernetickej bezpečnosti,
c) využívať pri pracovnej činnosti iba pripojenie do internetu, prípadne mobilné pripojenie prevádzkované zmluvným poskytovateľom pripojenia do internetu pre NÚ a žiadne iné,
d) dbať na to, aby svojím konaním nevystavili CIS, prípadne aj prostredie NÚ bezpečnostnému riziku.

(5) Je zakázané sprístupňovať materiály obsahujúce interné informácie v elektronickej forme prostredníctvom internetu (najmä bez náležitých kryptografických opatrení), ak nie sú v súlade so zásadami NÚ odsúhlasené notárom.

[1] Zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov

(6) Je zakázané, aby NÚ na pripojenie do CIS používal také pripojenie do internetu, ktoré je zdieľané s inou právnickou či fyzickou osobou (napr. spoločné pripojenie do internetu pre celú budovu, ktoré využívajú aj iné osoby mimo NÚ).

(7) Pri používaní služby internet je zakázané:
   a) sťahovať súbory, ktoré priamo nesúvisia s pracovnou činnosťou,
   b) sťahovať a inštalovať neoficiálne počítačové programy,
   c) spúšťať ľubovoľné programy nachádzajúce sa na internete (zábavný softvér, multimediálne aplikácie a pod.),
   d) zúčastňovať sa diskusných skupín, sociálnych sietí (okrem spravovania oficiálnej stránky NÚ) internetových zoznamovacích portálov a podobných stránok, slúžiacich na zábavu vo voľnom čase.

Čl. 8
Zásady používania prenosných médií

(1) V prostredí NÚ sa zakazuje používanie prenosných médií tretích strán, ak notár nestanoví inak.

(2) Pred použitím prenosného média (USB kľúč, CD/DVD, prenosný disk a pod.) je potrebné ho skontrolovať na prítomnosť vírusov alebo iných škodlivých programov prostredníctvom antivírusovej a malwarovej ochrany.

(3) Pred zapnutím pracovnej stanice odpojiť všetky cudzie externé médiá, ktoré sú pripojené k počítaču (napr. CD/DVD médiá, USB kľúče, externé disky).

(4) Likvidáciu prenosných médií zabezpečuje NÚ tak, aby sa citlivé informácie na nich uložené zlikvidovali bezpečným spôsobom.

(5) Pevné disky a iné médiá obsahujúce interné informácie je nevyhnutné bezpečne vymazať pred tým, ako sa odstránia z pracoviska.

(6) Citlivé informácie na prenosných médiách sú zničené vhodným spôsobom (napr. viacnásobným preformátovaním pevného disku špecializovaným softvérom alebo fyzickou likvidáciou).

Čl. 9
Používanie elektronickej pošty

(1) Pri používaní elektronickej pošty je potrebné dodržiavať nasledovné zásady:
   a) elektronickú poštu používať na zabezpečenie pracovných činností,
   b) pre zabezpečenie požadovanej úrovne bezpečnosti informácií sú používatelia povinní pri komunikácii s externým prostredím prostredníctvom elektronickej pošty obsahujúce osobné

údaje podľa GDPR , prípadne iné citlivé informácie, tie zabezpečiť proti zneužitiu neoprávnenými osobami (napr. zabezpečenie heslom, šifrovaním a pod.)

c) pri zasielaní elektronickej pošty používateľ uvádza predmet (subject) elektronickej pošty v jeho príslušnej časti určenej na tento účel. Pred odoslaním správy je povinný skontrolovať rozsah zvolených adresátov,
d) neodosielať a nešíriť správy, ktoré môžu niekoho urážať, šíriť neoverené a poplašné informácie,
e) neodosielať a nerozposielať nevyžiadanú elektronickú poštu typu SPAM, ktorá nesúvisí s pracovnou činnosťou a ktorá môže adresáta obťažovať. V prípade opakovaného doručenia nevyžiadanej elektronickej pošty od iného zamestnanca túto skutočnosť oznámiť notárovi,
f) interné informácie neodosielať mimo NÚ bez súhlasu notára,
g) zabezpečiť informovanie odosielateľa akejkoľvek správy v elektronickej pošte, ktorá bola zaslaná omylom, že správa bola prijatá a kópia vymazaná. V prípade, ak takáto elektronická pošta bola zaslaná viacerým adresátom (hromadná pošta), treba informovať iba odosielateľa, nie všetkých adresátov uvedených v zozname,
h) pri plánovanej neprítomnosti na pracovisku (dovolenka, pracovná cesta a podobne) sa odporúča nastaviť v klientovi elektronickej pošty „Automatické odpovede (mimo pracoviska)“. Poskytnutie hesla neoprávneným osobám z dôvodu kontroly elektronickej pošty, príp. iných dôvodov je neprípustné.
i) na komunikáciu používať také schránky elektronickej pošty a riešenia pri ktorých poskytovateľ služby elektronickej pošty dostatočne zabezpečuje zmluvné podmienky pre ochranu súkromia v súlade so Zákonom o ochrane osobných údajov a GDPR, (napr. v doméne @notar.sk).

Čl. 10
Používanie softvéru, aplikácií

(1) Na výkon pracovných činností notár pre svoj NÚ zabezpečí softvér s legálne nadobudnutou licenciou.

(2) Inštalovať a konfigurovať softvér na PC sú oprávnení iba zamestnanci zmluvného poskytovateľa servisu pre NÚ (ak notár si túto činnosť nezabezpečuje svojpomocne). Meniť svojvoľne konfiguráciu softvéru používateľmi je zakázané, všetky zmeny musia byť schválené notárom.

(3) Používaný softvér v PC na NÚ musí byť v pravidelných intervaloch aktualizovaný, rozhodnutie o intenzite aktualizácií je v kompetencii notára, alebo zmluvného poskytovateľa servisu. Kontrola potreby aktualizácií sa odporúča na dennej báze.

(4) Testovať alebo zavádzať taký softvér, o ktorom sa predpokladá, že by mohol ohroziť dôvernosť, dostupnosť alebo integritu informačných technológií, dát, informácií a informačných procesov CIS je prísne zakázané.

(5) Vlastniť, distribuovať, reprodukovať alebo používať počítačové programy na odpočúvanie komunikácie alebo inú neautorizovanú činnosť v počítačovej sieti NÚ je prísne zakázané.

(6) Je zakázané vykonávať akúkoľvek aktivitu, ktorá by mohla rušiť alebo ohrozovať integritu a bežnú prevádzku informačných technológií, dát, informácií alebo informačných procesov CIS.

Čl. 11
Ochrana pred škodlivým kódom

(1) Používateľ CIS je povinný sa vždy presvedčiť, že nainštalovaný softvér na ochranu pred škodlivým kódom je funkčný, prípadne nebol úmyselne alebo omylom zablokovaný.

(2) Systém na ochranu pred škodlivým kódom musí byť na zariadení nakonfigurovaný tak, že umožní najmä:
   a) automatizovanú kontrolu spúšťaných, resp. otváraných programov,
   b) automatizované aktualizácie od výrobcu, alebo centralizovaného systému riešenia ochrany pred škodlivým kódom ihneď, ako budú výrobcom sprístupnené,
   c) bezodkladné sprístupnenie notifikácie o bezpečnostných incidentoch zachytených systémom na ochranu pred škodlivým kódom.

(3) Každé koncové IT zariadenie pripojené do siete NÚ (napr. PC, tablet, smartfón) musí byť vybavené legálnou verziou systému na ochranu pred škodlivým kódom, ktorý je pravidelne aktualizovaný a má podporu od výrobcu.

(4) Pokiaľ nie je nastavená automatická kontrola ochrany pred škodlivým kódom, je potrebné skontrolovať všetky USB kľúče, DVD/CD alebo iné externé médiá, vrátane médií používaných naposledy na inom PC a médií od externých firiem, vzdelávacích agentúr, servisných technikov, dodávateľov, prípadne iných subjektov.

(5) Po prijatí elektronickej pošty bez popisu prílohy od neznámeho odosielateľa prílohu neotvárať (môže obsahovať neznámy vírus). Zamestnanec NÚ o tom informuje notára.

Čl. 12
Zásady čistej obrazovky a prázdneho stola

(1) Každý PC musí byť chránený mechanizmami uzamknutia PC. Po určitej dobe nečinnosti je na každom PC vo vlastníctve NÚ nastavené automatické spustenie do úsporného režimu.

(2) Pred opustením kancelárie v pracovnom čase je každý používateľ povinný uzamknúť svoj PC, aby sa zamedzilo prístupu neoprávnených osôb k prihláseným používateľským účtom.

(3) Používateľ je povinný pred odchodom z práce vypnúť PC, ak neexistujú príčiny, pre ktoré je potrebné nechať ho zapnutý (príčiny súvisiace s pracovnou činnosťou, servisom pracovnej stanice a podobne).

(4) Tak notár, ako zamestnanci NÚ musia zabezpečiť, aby sa pred odchodom z pracoviska na jeho pracovnom mieste nenachádzali voľne dostupné materiály a dokumenty, ktoré sú citlivé z hľadiska dôvernosti, tieto je potrebné vždy umiestniť do uzamykateľných skríň, prípadne iných zariadení na to určených.

Čl. 13
Povinnosti súvisiace s reakciou na bezpečnostné incidenty

(1) Používatelia CIS sú povinní pomáhať odhaľovať a oznamovať možné porušenia bezpečnosti, čo má zásadný význam pre ochranu bezpečnosti informácií spracúvaných v prostredí CIS.

(2) Akékoľvek známe problémy alebo problémy, o ktorých má používateľ podozrenie, že by mohli znamenať ohrozenie informačných technológií, dát, informácií a informačných procesov, je povinný bezodkladne oznámiť notárovi, ktorý incident nahlasuje administrátorom NK SR a to najmä:
   a) stratu alebo krádež počítačových zdrojov alebo informácií,
   b) výskyt vírusu alebo otvorenie rizikovej elektronickej pošty,
   c) všetky ostatné záležitosti súvisiace s narušením informačnej a kybernetickej bezpečnosti.

(3) Pri podozrení, že na počítači bola vykonávaná neoprávnená činnosť, resp. akákoľvek činnosť bez vedomia používateľa CIS, je v prípade zamestnancov potrebné okamžite informovať notára, ktorý zváži ďalší postup.

(4) O bezpečnostnom incidente notár vyhotoví písomný záznam, ktorého náležitosťou sú hlavne dátum a čas incidentu, podrobný popis incidentu, rozsah spôsobených škôd. V prípade, že sa incident týka CIS, kópiu záznamu zasiela administrátorom NK SR.

(5) Kybernetické bezpečnostné incidenty sa v prostredí CIS ohlasujú nasledovným spôsobom:
   a) manažérovi kybernetickej bezpečnosti NK SR na TČ: 02 556 423 12 alebo
   b) na adresu cis@notar.sk

Čl. 14
Používanie tlačových služieb

(1) Pri používaní tlačiarní a iných zariadení umožňujúcich tlač dokumentov sú používatelia CIS povinní dodržiavať nasledovné zásady:
   a) používateľ môže vytvárať tlačové výstupy len v rozsahu určenom jeho povereni, v prípade výstupov obsahujúcich citlivé informácie musí používateľ zabezpečiť, aby k príslušnej tlačiarni nemala počas tlačenia výstupov nekontrolovaný prístup neoprávnená osoba,
   b) chybné a neaktuálne tlačové výstupy je potrebné zlikvidovať v skartovacom zariadení,
   c) zamestnanec NÚ nemôže svojvoľne meniť konfigurácie tlačiarní bez vedomia notára a zodpovedá za škody spôsobené neodbornou manipuláciou.

Čl. 15
Bezpečnostné zásady súvisiace so zálohovaním

(1) Za priebežné zálohovanie lokálnych pracovných údajov NÚ je zodpovedný notár, ktorý určí potrebný rozsah a intenzitu záloh.

(2) Zálohovať sa môžu iba súbory súvisiace s pracovnými činnosťami, na tieto potreby je potrebné využívať oficiálne médiá odsúhlasené notárom (napr. USB disky, USB kľúče) a pridelené konkrétnym používateľom.

(3) Súbory, ktoré NÚ pre svoju prácu nepotrebuje, ale je nutné ich uchovávať na archívne účely, sa ukladajú na príslušné dátové médiá podľa pokynu notára, prípadne administrátora CIS a podľa postupov definovaných vo vnútorných predpisoch NK SR.

(4) Používané zálohovacie médiá (najmä USB kľúče, CD/DVD) musia byť vždy označené tak, aby bolo zrejmé, aké údaje obsahujú a kto je ich vlastníkom.

(5) Zálohovacie médiá musia byť uložené v bezpečnom prostredí (minimalizácia rizika neautorizovaného prístupu, krádeže, porušenia v dôsledku vplyvu prostredia).

(6) Údaje z CIS sa na NÚ nezálohujú. Ich zálohovanie sa vykonáva centrálne v cloude NK SR.

Čl. 16
Zásady dodržiavania právnych a regulačných požiadaviek

(1) Používatelia CIS sú povinní dodržiavať relevantné právne predpisy týkajúce sa ochrany dát a ochrany práv duševného vlastníctva z oblasti autorského práva a práv súvisiacich s autorským právom. Tieto právne predpisy sa vzťahujú aj na používanie počítačových programov (softvéru, aplikácií) vytvorených pre NK SR, rozmnožovanie počítačového programu bez licencie znamená porušenie autorských práv podľa zákona č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom (autorský zákon) v znení neskorších predpisov.

(2) Používatelia CIS sú povinní dodržiavať aj relevantné právne predpisy týkajúce sa informačnej a kybernetickej bezpečnosti a z nich vyplývajúce bezpečnostné opatrenia definované v interných predpisoch NK SR.

(3) Akékoľvek podozrenie z porušovania vnútorných alebo právnych predpisov súvisiacich s používaním IT sú používatelia povinní okamžite oznámiť notárovi, ktorý následne rozhodne o potrebe oznámiť udalosť administrátorom NK SR.

Čl. 17
Ochrana osobných údajov

(1) Tento interný predpis slúži na zabezpečenie súladu Nariadenia Európskeho parlamentu a Rady (EÚ) z 27. apríla 2016 č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (v texte aj len ako „**GDPR**“) a zákonom č. 18/2018 Z. z. o ochrane osobných údajov (v texte aj len „**Zákon o ochrane osobných údajov**“). Akýmkoľvek odkazom na GDPR je zároveň myslené relevantné ustanovenie Zákona o ochrane osobných údajov, ak by sa na spracúvanie a/alebo časť spracúvania osobných údajov regulovaného týmto interným predpisom vzťahoval Zákon o ochrane osobných údajov a naopak.

(2) Tento interný predpis používa primárne pojmy definované v čl. 4 GDPR.

(3) Notár poučí svojich zamestnancov o pravidlách ochrany osobných údajov na NÚ, prípadne pre zamestnancov NÚ zabezpečí odborné školenie.

(4) Notár a jeho zamestnanci dbajú na to, aby sa pri spracúvaní osobných údajov dodržiavali požiadavky GDPR a Zákona o ochrane osobných údajov a práva dotknutých osôb.

(5) NÚ, ktoré vedenie a evidenciu svojho účtovníctva, mzdovej a personálnej agendy zabezpečujú prostredníctvom externého dodávateľa, sú povinné z dôvodu ochrany osobných údajov svojich zamestnancov uzatvárať s týmto dodávateľom zmluvu o spolupráci, do ktorej inkorporujú všetky relevantné požiadavky pre úpravu právneho vzťahu prevádzkovateľa a sprostredkovateľa podľa čl. 28 ods. 3 GDPR ako klauzulu o mlčanlivosti a o ochrane osobných údajov podľa GDPR. Obdobne bude NÚ pristupovať aj k akýmkoľvek ďalším externým dodávateľom, ktorí pri poskytovaní služieb pre potreby NÚ budú potrebovať pristupovať k osobným údajom NÚ alebo budú inak vykonávať akékoľvek spracovateľské operácie s takýmito osobnými údajmi, ktoré NÚ spracúva ako prevádzkovateľ v kontexte dosahovania vlastných účelov spracúvania osobných údajov, ktoré vymedzil vo svojich Podmienkach ochrany súkromia (napr. s poskytovateľmi cloudových služieb, poskytovateľmi služieb externej správy a likvidovania registratúrnych záznamov a pod.).

(6) NÚ vymenuje zodpovednú osobu podľa čl. 37 GDPR, ktorá dohliada na zákonnosť a bezpečnosť spracúvania osobných údajov na NÚ. Zodpovedná osoba sa určí na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany osobných údajov a na základe spôsobilosti plniť úlohy podľa GDPR.

Čl. 18
Zverejňovanie osobných údajov

(1) Notár a jeho zamestnanci nezverejňujú osobné údaje žiadnych dotknutých osôb mimo prípadov, ktoré určuje platná legislatíva a ku ktorým má NÚ zrejmý právny základ na vykonanie takejto citlivej spracovateľskej operácie podľa čl. 6 ods. 1 GDPR (napr. NÚ zverejňuje osobné údaje v nevyhnutnom rozsahu v prípade potreby zverejňovania na úradnej tabuli NÚ na základe takých právnych skutočností, o ktorých to ustanoví zákon, ak je to nevyhnutné pre riadne splnenie zákonných povinností NÚ).

(2) Notár je povinný vyškoliť svojich zamestnancov a používateľov CIS, aby pri zverejňovaní akýchkoľvek osobných údajov postupovali veľmi obozretne a na základe pokynov notára. NÚ je povinný presadzovať, aby všetci jeho zamestnanci a používateľa CIS dbali na to, aby počas registrácie údajov do registrov CIS neboli zadané osobné údaje, ktoré by mohli byť automaticky zverejnené vo verejnej časti Notárskych centrálnych registrov na internetovej stránke NK SR, okrem údajov ktorých zverejňovanie stanovuje platná legislatíva a ktoré sú zverejňované v súlade s podmienkou podľa čl. 18 ods. 1 tohto interného predpisu.

(3) NÚ je povinný osobitne znemožniť vlastnými vhodnými opatreniami a individuálne uloženými pokynmi, aby jeho zamestnanci a používatelia CIS v rozpore s platnou legislatívou nezverejnili o žiadnej dotknutej osobe i) všeobecne použiteľný identifikátor podľa osobitného predpisu[2], resp. rodné číslo, ii) osobitné kategórie osobných údajov podľa čl. 9 ods. 1 GDPR bez existencie minimálne jednej výnimky podľa čl. 9 ods. 2 GDPR, iii) údaje týkajúce sa uznania viny za trestné činy alebo priestupky, ak takéto zverejnenie nie je výslovne povolené zákonom, ktorý obsahuje primerané záruky pre ochranu práv a slobôd dotknutých osôb.

(4) NÚ je povinný zabezpečiť prostredníctvom vlastných opatrení, postupov a vhodne vyškoleného a poučeného personálu anonymizáciu akýchkoľvek osobných údajov, ktoré sú obsiahnuté v listinách a dokumentoch určených na zverejnenie ešte pred ich zverejnením naskenovaním do CIS alebo úradnej tabule NÚ, a to v prípadoch, ak je nevyhnutné takýto dokument alebo listinu zverejniť, ale neexistuje právny základ pre zverejnenie osobných údajov v zmysle čl. 18 ods. 1 tohto vnútorného predpisu a/alebo prípadne dodatočné podmienky v zmysle čl. 18 ods. 3 tohto vnútorného predpisu.

(5) Anonymizáciu osobných údajov je potrebné vykonať v maximálnom možnom rozsahu, pričom je potrebné zabezpečiť trvalé vymazanie všetkých relevantných identifikátorov, ktoré by mohli byť spätne obnovené alebo využité NÚ ako prevádzkovateľom alebo aj treťou stranou na priamu alebo nepriamu identifikáciu dotknutej osoby. Pri anonymizácii zverejňovaných osobných údajov je zodpovedná osoba NÚ povinná zobrať primerane do úvahy tzv. doktrínu primeranej

[2] Zákon č. 301/1995 Z. z. o rodnom čísle v znení neskorších predpisov

pravdepodobnosti interpretovanú v recitály č. 26 GDPR[3] a v rozsudku Súdneho dvora EÚ vo veci Patrick Breyer vs Nemecko (C-582/14) a presadiť v konkrétnych prípadoch takú mieru a spôsob anonymizácie osobných údajov, ktorý pri zachovaní miery primeranej pravdepodobnosti neumožní nikomu spätne identifikovať konkrétne fyzické osoby, ktorých osobné údaje NÚ anonymizoval a zverejnil v anonymizovanej forme.

(6) NÚ sa v otázkach anonymizácie osobných údajov radí so svojou zodpovednou osobou určenou pre ochranu osobných údajov a v druhovo rovnakých prípadoch postupuje pri ich opakovaní sa v budúcnosti v zmysle rád svojej zodpovednej osoby primerane rovnakým spôsobom.

Čl. 19

Zrušuje sa interný predpis prijatý prezídiom Notárskej komory SR o zabezpečení minimálnej bezpečnosti na ochranu údajov na notárskom úrade schválený dňa 5.8.2004.

Čl. 20

Tento interný predpis bol schválený 19.12.2023 a nadobúda účinnosť dňa 1.1.2024.

[3] *„Na určenie toho, či je fyzická osoba identifikovateľná, by sa mali brať do úvahy všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije, napríklad osobitným výberom, na priamu alebo nepriamu identifikáciu fyzickej osoby. Na zistenie toho, či je primerane pravdepodobné, že sa prostriedky použijú na identifikáciu fyzickej osoby, by sa mali zohľadniť všetky objektívne faktory, ako sú náklady a čas potrebný na identifikáciu so zreteľom na technológiu dostupnú v čase spracúvania, ako aj na technologický vývoj.“*

Príloha č. 1

POUČENIE ZAMESTNANCOV NOTÁRSKEHO ÚRADU
O PRAVIDLÁCH BEZPEČNOSTI V PROSTREDÍ NOTÁRSKEHO ÚRADU

V zmysle interných predpisov Notárskej komory SR týkajúcich sa prístupu notárov a ich zamestnancov do Centrálneho informačného systému Notárskej komory SR (ďalej len CIS) a v súlade s požiadavkami zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov som bol poučený, ako zamestnanec Notárskeho úradu ďalej len NÚ), o

a) povinnosti ochrany údajov a záväzku mlčanlivosti o údajoch, s ktorými som počas výkonu prác na NÚ prišiel do styku, ako aj zákaze ich využitia pre osobnú potrebu, zverejnenia, poskytnutia a sprístupnenia, s výnimkou orgánov činných v trestnom konaní, ak som bol zbavený mlčanlivosti podľa platnej legislatívy, a to aj po ukončení pracovného, resp. zmluvného pomeru,

b) povinnosti zachovávať mlčanlivosť o osobných údajoch, s ktorými som počas výkonu prác na NÚ prišiel do styku, ako aj zákaze ich využitia pre osobnú potrebu, zverejnenia, poskytnutia a sprístupnenia, s výnimkou orgánov činných v trestnom konaní a vo vzťahu k Úradu pre ochranu osobných údajov pri plnení jeho úloh, ak som bol zbavený mlčanlivosti podľa platnej legislatívy,

c) povinnosti realizovať zásahy do CIS iba v určenom rozsahu v rámci pracovnej náplne,

d) povinnosti rešpektovať operatívne pokyny notára a vedúceho správcu CIS,

e) povinnosti bezodkladne ohlásiť zistené bezpečnostné nedostatky a bezpečnostné incidenty na NÚ a v CIS,

f) povinnosti realizovať pracovné činnosti tak, aby pri nich nedošlo k poškodeniu alebo zničeniu komponentov IT na Notárskom úrade alebo k neočakávanému prerušeniu ich prevádzky,

g) možnosti pripájať svoje technologické prostriedky (napr. počítač, notebook, meracie prístroje, a pod.) do siete NÚ a k CIS len po predchádzajúcom súhlase notára a to len na nevyhnutne potrebnú dobu a s rešpektovaním podmienok spojených so súhlasom, ako napríklad antivírová kontrola a pod.,

h) možnosti vynášať zariadenia, materiál a údaje patriace NÚ (informačno-komunikačné zariadenia, výsledky zostáv vytvorených na základe skriptov, zbery údajov, poskytované údaje, a pod.) z priestorov NÚ len so súhlasom notára,

i) povinnosti rešpektovať autorské práva k materiálom poskytnutým zo strany NK SR a NÚ,

j) povinnosti vrátiť všetky materiály a údaje vrátane elektronických, ktoré boli poskytnuté zo strany NK SR a NÚ a zlikvidovať všetky ich kópie, ak to nebolo zmluvne dohodnuté inak,

k) o obsahu Interného predpisu NK SR o zabezpečení minimálnej bezpečnosti na ochranu údajov na NÚ.

Svojím podpisom potvrdzujem, že som bol oboznámený s interným predpisom o zabezpečení minimálnej bezpečnosti na ochranu údajov na notárskom úrade, tomuto poučeniu porozumel v plnom rozsahu. Toto poučenie sa podpisuje minimálne dvoch vyhotoveniach. Jedno vyhotovenie sa vkladá do osobného spisu zamestnanca na NÚ a druhé zostáva u zamestnanca.

Meno a priezvisko	Pozícia	Email	Telefón	Podpis