



Garant: Útvar rektora

Košice, 22. 05. 2018
Č. j.: REK000/2018-UPA/3287

Rozhodnutie rektora č. 9/2018

na zabezpečenie bezpečnosti spracúvania osobných údajov na Univerzite Pavla Jozefa Šafárika v Košiciach a jej súčastiach

V súlade s ust. § 15 ods. 1 písm. l) zákona č. 131/2002 Z. z. o vysokých školách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov v nadväznosti na čl. 4 odsek 3 Organizačného poriadku Univerzity Pavla Jozefa Šafárika v Košiciach v platnom znení a v nadväznosti na čl. 32 Nariadenia Európskeho parlamentu a Rady EÚ č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica č. 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „GDPR“) a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ochrane osobných údajov“)

v y d á v a m

nasledovné rozhodnutie na zabezpečenie bezpečnosti spracúvania osobných údajov na Univerzite Pavla Jozefa Šafárika v Košiciach a jej súčastiach.

Čl. 1

Všeobecné ustanovenia

- (1) Toto rozhodnutie stanovuje pravidlá pre bezpečné spracúvanie osobných údajov na Univerzite Pavla Jozefa Šafárika v Košiciach (ďalej len „UPJŠ“).
- (2) Cieľom je zabezpečiť ochranu a bezpečnosť osobných údajov, ktoré sú spracúvané úplne alebo čiastočne automatizovanými prostriedkami spracúvania alebo inými ako automatizovanými prostriedkami spracúvania, ktoré sú súčasťou informačného systému alebo sú určené na spracúvanie v informačnom systéme a eliminovať a minimalizovať hrozby a riziká pôsobiace na tieto informačné systémy.
- (3) Toto rozhodnutie je záväzné pre všetkých zamestnancov Univerzity Pavla Jozefa Šafárika v Košiciach v rozsahu zodpovednosti, ktorá vyplýva z ich pracovného zaradenia.
- (4) Záväzne sa stanovujú povinnosti pre prevádzkovateľa, všetky oprávnené osoby, ktoré spracúvajú osobné údaje a pre zodpovednú osobu, ktorá dozerá na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov.

Čl. 2

Základné pojmy a definície

- (1) Osobnými údajmi sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba“), identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.
- (2) Spracúvanie osobných údajov je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonáva automatizovanými alebo neautomatizovanými prostriedkami.
- (3) Informačným systémom je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe.
- (4) Dotknutou osobou je každá fyzická osoba, ktorej osobné údaje sa spracúvajú.
- (5) Prevádzkovateľom je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov. Pre účely tohto rozhodnutia prevádzkovateľom je Univerzita Pavla Jozefa Šafárika v Košiciach.
- (6) UPJŠ ako prevádzkovateľ určuje účel a prostriedky spracúvania. Účel každého spracúvania osobných údajov v prostredí UPJŠ musí zodpovedať postaveniu a činnosti univerzity. Spracúvanie nesmie byť v protiklade s poslaním univerzity.
- (7) Oprávnenou osobou je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru alebo obdobného pracovného vzťahu a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení.
- (8) Zodpovednou osobou je osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa GDPR.
- (9) Prijemca je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov. Spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania.
- (10) Tretia strana fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov.
- (11) **Porušením ochrany osobných údajov** je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim.

Čl. 3

Zásady zákonného a bezpečného spracúvania osobných údajov

- (1) Pri spracúvaní osobných údajov musia byť dodržané minimálne tieto zákonné pravidlá:
 - a) osobné údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom;
 - b) spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú;
 - c) musí byť zabezpečená správnosť a aktuálnosť osobných údajov, ich prípadná oprava, doplnenie alebo vymazanie;
 - d) osobné údaje musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú.

- (2) Pri spracúvaní osobných údajov musia byť dodržané minimálne tieto bezpečnostné pravidlá:
 - a) osobné údaje dotknutých osôb musia byť zabezpečené pred neoprávneným spracúvaním, nezákonným spracúvaním, odcudzením, stratou, výmazom, poškodením, ako aj pred akýmkoľvek inými neprípustnými formami spracúvania;
 - b) pred opustením alebo vzdialením sa z pracoviska je oprávnená osoba povinná vypnúť alebo zamknúť zariadenie, na ktorom spracúva osobné údaje;
 - c) pred opustením alebo vzdialením sa z pracoviska je oprávnená osoba povinná uložiť všetky nosiče obsahujúce osobné údaje do uzamykateľnej skrine, aby k nim nemala prístup iná neoprávnená osoba.

- (3) Pri spracúvaní osobných údajov prostredníctvom úplne alebo čiastočne automatizovaných prostriedkov spracúvania oprávnená osoba najmä:
 - a) využíva služby Internetu povolené za účelom plnenia pracovných úloh, pričom dodržiava bezpečnostné opatrenia prijaté prevádzkovateľom za účelom zabezpečenia ochrany osobných údajov,
 - b) informačnú techniku (počítače, notebooky, USB kľúč, a pod.) umiestňuje iba v uzamykateľných priestoroch; miestnosť, v ktorej sa nachádza informačná technika, musí byť pri každom odchode oprávnenej osoby uzamknutá a po skončení pracovného času je oprávnená osoba povinná vypnúť počítač a uzamknúť skrine s materiálmi obsahujúcimi osobné údaje,
 - c) dbá na antivírusovú ochranu pracovných staníc sledovaním toho, či správne funguje primárne určený softvérový systém, ktorý je automaticky pravidelne aktualizovaný,
 - d) berie do úvahy zákaz odinštalovania, zablokovania alebo zmenu konfigurácie antivírusovej ochrany,
 - e) prístup do informačného systému spracúvajúceho osobné údaje musí byť chránený minimálne menom a heslom;
 - f) dôsledne dodržiava pravidlá ochrany prístupových práv a odhlasuje sa z programov, resp. z operačného systému na svojom počítači,
 - g) všetky spracúvané osobné údaje v pravidelných intervaloch zálohuje, aby bolo možné v prípade potreby údaje v informačnom systéme nanovo obnoviť.

- (4) Pri spracúvaní osobných údajov prostredníctvom neautomatizovaných prostriedkov spracúvania (listová forma spracúvaných osobných údajov) oprávnená osoba najmä:
- a) zachováva obozretnosť pri podávaní chránených informácií, vrátane osobných údajov pred návštevníkmi prevádzkovateľa alebo inými neoprávnenými osobami,
 - b) neponecháva osobné údaje voľne dostupné na chodbách a v iných neuzamknutých miestnostiach alebo na iných miestach, vo verejne prístupných miestach a pod.,
 - c) odkladá spisy a iné listinné materiály na určené miesto a neponecháva ich po skončení pracovného času, resp. opustení pracoviska voľne dostupné (napr. na pracovnom stole),
 - d) zaobchádza s tlačnými materiálmi obsahujúcimi osobné údaje podľa ich citlivosti; je potrebné aplikovať všetky relevantné opatrenia, ktoré zabezpečia ochranu vytlačených informácií obsahujúcich osobné údaje pred neoprávnenými osobami,
 - e) v prípade tlače dokumentov obsahujúcich osobné údaje zabezpečuje, aby sa počas tlačenia neoboznámila s nimi neoprávnená osoba; tlačené materiály obsahujúce osobné údaje musia byť ihneď po ich vytlačení odobraté oprávnenou osobou a uložené na zabezpečené miesto; to sa uplatňuje aj pri kopírovaní dokumentov - nadbytočné a chybné dokumenty oprávnená osoba bez zbytočného odkladu zlikviduje skartovaním,
 - f) pri skončení pracovného pomeru alebo obdobného pracovného vzťahu oprávnená osoba je povinná odovzdať prevádzkovateľovi pracovnú agendu vrátane spisov obsahujúcich osobné údaje.

Čl. 4

Rozsah oprávnení, povinností a zodpovedností oprávnenej osoby

- (1) Všetky oprávnené osoby musia byť poučené o právach a povinnostiach ustanovených zákonom o ochrane osobných údajov a GDPR a o zodpovednosti za ich porušenie pred uskutočnením prvej operácie s osobnými údajmi. Záznam o poučení/pokyn oprávnenej osoby je súčasťou osobného spisu zamestnanca.
- (2) Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení pracovného pomeru alebo obdobného pracovného vzťahu.
- (3) Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona, alebo vo vzťahu k Úradu na ochranu osobných údajov Slovenskej republiky (ďalej len „úrad“) pri plnení jeho úloh podľa zákona o ochrane osobných údajov, ustanovenia o povinnosti mlčanlivosti podľa osobitných predpisov tým nie sú dotknuté.
- (4) Oprávnená osoba môže spracúvať osobné údaje pre potreby UPJŠ len na základe platných zákonov, právnych predpisov a interných dokumentov a v súlade s nimi.
- (5) Oprávnená osoba môže spracúvať len také osobné údaje, ktoré svojím rozsahom a obsahom zodpovedajú ich účelu spracúvania a sú nevyhnutné na jeho dosiahnutie.
- (6) Oprávnená osoba je povinná:
 - a) spracúvať osobné údaje takým spôsobom, aby nedošlo k ich poškodeniu, nechcenej modifikácii alebo zničeniu,
 - b) spracúvať osobné údaje iba v priestoroch, ktoré sú na to určené,
 - c) spracúvať osobné údaje iba na schválených technických prostriedkoch,
 - d) **bezodkladne informovať** zodpovednú osobu o každom porušení ochrany osobných údajov na email zodpovedna-osoba@upjs.sk,
 - e) dodržiavať všetky požiadavky na kvalitu hesiel,

- f) dodržiavať zásadu „čistého pracovného stola“ (nosiče obsahujúce osobné údaje musí pred odchodom z pracoviska uložiť a uzamknúť),
 - g) nepotrebné nosiče dát obsahujúce citlivé informácie (listinné dokumenty, médiá) bezpečne zlikvidovať (listinné dokumenty skartovaním, médiá bezpečne fyzicky zničiť),
 - h) raz ročne podrobiť sa školeniu z oblasti bezpečnosti informačných systémov a z oblasti ochrany osobných údajov.
- (7) Oprávnená osoba je zodpovedná:
- a) za plnenie informačnej povinnosti podľa čl. 13 a 14 GDPR vo vzťahu k dotknutej osobe v mene prevádzkovateľa,
 - b) za správnosť osobných údajov pri ich získavaní,
 - c) za to, že rozsah získaných osobných údajov zodpovedá účelu, na ktorý sú osobné údaje spracúvané,
 - d) za ochranu osobných údajov počas ich spracúvania,
 - e) za neoprávnené sprístupnenie svojho hesla inej osobe, následne i za jeho zneužitie a spôsobné škody,
 - f) za bezpečnú likvidáciu osobných údajov.
- (8) Oprávnená osoba nesmie:
- a) modifikovať programové vybavenie, na ktorom spracúva osobné údaje,
 - b) zasielať osobné údaje prostredníctvom nezabezpečenej siete/prostredia bez toho, aby zabezpečila ochranu ich dôvernosti (ochrana pred vyzradením),
 - c) využívať osobné údaje na iné ako stanovené účely.

Popis povolených činností oprávnených osôb

Čl. 5

Získavanie osobných údajov

- (1) Oprávnená osoba je povinná získavať na základe svojho pracovného zaradenia len nevyhnutné osobné údaje výlučne na zákonom ustanovený alebo vymedzený účel. Je neprípustné, aby oprávnená osoba získavala osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti.
- (2) Pri získavaní osobných údajov je oprávnená osoba povinná overiť správnosť a aktuálnosť predkladaných osobných údajov.
- (3) Získavanie osobných údajov kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií možno len vtedy, ak
 - a) je to nevyhnutné na dosiahnutie účelu spracúvania a dotknutá osoba s tým písomne súhlasí (súhlas so spracúvaním kópie musí byť v zrozumiteľnej a ľahko dostupnej forme, formulovaný jasne a jednoducho a vlastnoručne podpísaný priamo na vyhotovenej kópii),
 - b) to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby.

Čl. 6

Zverejňovanie osobných údajov

- (1) Je neprípustné zverejňovať:
 - a) na web sídle fakúlt rozvrh (čas a miestnosť) na príslušný semester s uvedením mien a priezvisk študentov, študijného programu a ročníka;

- b) výsledky skúšok na internete, resp. v inom zozname uverejnenom na verejne prístupnom mieste v budove vysokej školy v rozsahu študijný program, ročník, predmet študijného plánu, meno, priezvisko študenta, počet kreditov;
- c) na web sídle fakúlt zoznamy ich absolventov v rozsahu meno a priezvisko, rok ukončenia štúdia, študijný program, resp. študijný odbor bez predchádzajúceho súhlasu absolventov.

Čl. 7

Uchovávanie, archivovanie a likvidácia osobných údajov

- (1) Uchovávanie a archivovanie osobných údajov musí byť v súlade so zákonom o archívoch a registratúrach.
- (2) Likvidáciu osobných údajov môže vykonať iba osoba oprávnená spracúvať tieto údaje.
- (3) Nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné, zreteľne označiť a bez zbytočného odkladu zlikvidovať.
- (4) Oprávnená osoba je povinná vykonať likvidáciu osobných údajov, ktoré sú súčasťou už nepotrebných pracovných dokumentov (napr. rôzne pracovné súbory, pracovné verzie dokumentov v listinnej podobe) rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať; to neplatí vo vzťahu k osobným údajom, ktoré sú súčasťou obsahu registratúrnych záznamov prevádzkovateľa.

Čl. 8

Spôsob likvidácie nosičov

- (1) Listinný nosič osobných údajov sa zničí pomocou skartovacieho stroja, likvidácia väčšieho množstva listinných nosičov je na základe písomnej zmluvy zabezpečená prostredníctvom tretej strany.
- (2) Likvidácia elektronického nosiča – prenosné média (CD, DVD, páska a pod.) prebieha prostredníctvom fyzického zničenia nosiča (rozlámanie, skartovanie pásky).

Čl. 9

Spôsob identifikácie a autentizácie pri prístupe k informačnému systému

- (1) Každá oprávnená osoba prístupujúca k informačnému systému UPJŠ musí mať pridelené prihlasovacie meno a heslo, ktoré uchováva v tajnosti. Individuálne prihlasovacie účty pomáhajú stanoviť osobnú zodpovednosť. Spoločné používanie prihlasovacích mien a hesiel viacerými oprávnenými osobami je zakázané. V prípade podozrenia, že prišlo k vyzradeniu hesla, je oprávnená osoba povinná si heslo okamžite zmeniť.
- (2) Poskytovanie špecifických informácií o používateľoch informačného systému UPJŠ, ktoré by mohli byť zneužitú pre neoprávnený prístup k údajom a programom (identifikačné a autentizačné údaje) tretím osobám je zakázané.

Čl. 10

Zodpovednosti zodpovednej osoby

- (1) Zodpovedná osoba pri výkone svojich úloh náležite zohľadňuje riziko spojené so spracovateľskými operáciami, pričom berie do úvahy povahu, rozsah, kontext a účel spracúvania osobných údajov.
- (2) Zodpovedná osoba je povinná najmä:
 - a) poskytovať informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa všeobecne záväzných právnych predpisov týkajúcich sa ochrany osobných údajov,
 - b) monitorovať súlad so všeobecne záväznými predpismi týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa alebo sprostredkovateľa súvisiacimi s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných údajov,
 - c) poskytovať na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania podľa čl. 35 GDPR,
 - d) spolupracovať s úradom pri plnení svojich úloh,
 - e) plniť úlohy kontaktného miesta pre úrad v súvislosti s otázkami týkajúcimi sa spracúvania osobných údajov vrátane predchádzajúcej konzultácie uvedenej v č. 36 GDPR a podľa potreby aj konzultácie v iných veciach,
 - f) zabezpečiť realizáciu procesu poučenia/pokynu oprávnených osôb,
 - g) zabezpečiť vybavovanie žiadostí dotknutých osôb pri uplatňovaní ich práv,
 - h) zabezpečovať vedenie záznamov o spracovateľských činnostiach podľa čl. 30 GDPR,
 - i) vyhodnocovať, či porušenie ochrany osobných údajov pravdepodobne povedie k riziku pre práva a slobody fyzickej osoby na účely čl. 33 GDPR,
 - j) vyhodnocovať, či porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva a slobody fyzickej osoby na účely čl. 34 GDPR,
 - k) viesť vnútornú evidenciu všetkých porušení ochrany osobných údajov a prijímať opatrenia na ich predchádzanie a nápravu.

Čl. 11

Oznamovanie porušenia ochrany osobných údajov

- (1) Zodpovedná osoba v mene prevádzkovateľa oznámi úradu také porušenie ochrany osobných údajov, pri ktorom je pravdepodobné, že porušenie povedie k riziku pre práva a slobody fyzickej osoby (ďalej ako „bezpečnostný incident“)
- (2) Zodpovedná osoba je povinná oznámiť bezpečnostný incident podľa ods. 1 vedeniu univerzity bezodkladne a úradu do 72 hodín po tom, ako sa o ňom dozvedela.
- (3) Oznámenie podľa odseku 1 musí obsahovať aspoň:
 - a) opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategórií a približného počtu dotknutých osôb (napr. študenti, zamestnanci), ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
 - b) kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
 - c) opis pravdepodobných následkov porušenia ochrany osobných údajov,

- d) opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

Ak v čase oznámenia nie sú zodpovednej osobe známe všetky informácie, poskytnú ich bezodkladne po tom, čo sa o nich dozvie.

- (4) V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, zodpovedná osoba bez zbytočného odkladu oznámi porušenie ochrany osobných údajov dotknutej osobe.

Čl. 12

Záverečné ustanovenia

- (1) Toto rozhodnutie nadobúda platnosť a účinnosť dňom jeho podpisu rektorom UPJŠ.
- (2) Zároveň sa ruší Rozhodnutie rektora č. 21/2013 ktorým sa vydáva bezpečnostná smernica o ochrane osobných údajov na Univerzita Pavla Jozefa Šafárika v Košiciach a jej súčastiach.

prof. RNDr. Pavol Sovák, CSc.
rektor UPJŠ