Pedagogická fakulta Univerzity Jana Evangelisty Purkyně v Ústí nad Labem

Metodický pokyn děkana PF k ochraně osobních dat *(metodika GDPR)*

AKTUALIZACE K 1. 8. 2018

A. Úvod

Osobní údaje jsou jakékoli informace o identifikovaném nebo identifikovatelném subjektu údajů. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména **odkazem na určitý identifikátor** (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Klasická výzkumná data mohou být zpracována bez omezení (pokud neobsahují data osobní či citlivá).

Mezi obecné osobní údaje řadíme **jméno, pohlaví, věk a datum narození, osobní stav, ale také IP adresu a fotografický záznam.** Vzhledem k tomu, že se ochrana osobních údajů vztahuje i na podnikající fyzické osoby, řadíme mezi osobní údaje i tzv. organizační údaje, kterými jsou například e-mailová adresa, telefonní číslo či různé identifikační údaje vydané státem.

Citlivé osobní údaje jsou speciální kategorií podle systému ochrany osobních dat, která zahrnuje **údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob, ale také genetické a biometrické údaje.** Tyto údaje mohou subjekt údajů zapříčinit diskriminaci nositele údajů.

Pravidla politiky GDPR jsou na UJEP konkretizována směrnicí rektora **2/2018 účinné od 1. 7. 2018**.

B. Obecná doporučení ke všem typům uložení osobních údajů

a) Osobní údaje je potřeba **ukládat** pouze do složek a programů k tomu určených - nelze např. přenášet na flash-disku v nezabezpečené podobě.
b) Při **zasílání** e-mailem doporučujeme soubor zaheslovat a heslo sdělit příjemci jinou cestou (např. formou sms).
c) Při každém **opuštění počítače**, na kterém probíhá práce s osobními údaji, musí dojít k jeho "uzamknutí" tak, aby při návratu k počítači bylo nutné opět zadat heslo.
d) Používat svěřené zařízení výpočetní techniky **pouze pro pracovní účely** (tj. nestahovat soubory pro soukromé účely (např. filmy, dokumenty apod.) na disk počítače.
e) Fyzická data (tj. složky, papírové dokumenty) s osobními údaji **MUSÍ** být uloženy pod uzamčením.
f) Fyzická ochrana se týká docházek a prezenčních listin.
g) Souhlas se zpracováním osobních údajů nemůže být obecný, vyžadovaný „předem", neurčitě

a „pro jistotu“.

h) Omezení předávání osobních údajů mimo EU, do USA jen certifikovaným osobám – týká se údajů spojených s Erasmem a předávaných výzkumných dat.

C. Přístup k osobním údajům

Doporučené zabezpečení osobních údajů podle jejich způsobu uložení	
Osobní údaje jsou uloženy přímo na pevném disku daného počítače	• počítač musí být přístupný pouze na heslo, resp. uživatelské jméno, které je individuální pouze pro osobu oprávněnou k přístupu k osobním údajům (tj. nikoliv např. sdílené heslo pro všechny učitele), • počítač musí být v době, kdy je nepoužívaný/vypnutý, v uzamčené místnosti.
Osobní údaje jsou uloženy na serveru (ve sdílené složce) - tedy potenciálně dostupné z jakéhokoliv počítače v síti UJEP	• musí být zajištěno, že osobní údaje jsou dostupné pouze oprávněným osobám (tj. do sítě je potřeba se hlásit na konkrétní uživatelský účet/jméno nebo složka musí být dostupná pod heslem, které je známé pouze příslušné oprávněné osobě), • server by měl být ve speciální zamčené místnosti s přístupem pouze pro nezbytný okruh osob (ředitel, IT technik), • data na serveru by měla být šifrovaná (zajišťuje CI UJEP).
Osobní údaje jsou uloženy v cloudu (potenciálně dostupné z jakéhokoliv počítače či mobilního zařízení)	• všechny počítače či mobilní zařízení, která jsou využívána pro přístup k osobním údajům, musí být řádně zabezpečena - musí vyžadovat heslo pro přístup, • přístup k souborům by měl být chráněn heslem, které je potřeba zadat při každém novém přihlášení do cloudové služby (tj. nikoliv “zapamatovat heslo”), • je potřeba mít s poskytovatelem cloudové služby uzavřenou dohodu/smlouvu dle požadavků GDPR, • tento způsob ukládání doporučujeme maximálně eliminovat.
Osobní údaje jsou uloženy ve speciálním software (např. IS STAG, účetní systém FIS apod.)	• všechny počítače či mobilní zařízení, která jsou využívána pro přístup k osobním údajům, musí být řádně zabezpečena - musí vyžadovat heslo pro přístup, • systém by měl umožňovat individualizovaný přístup pro jednotlivé uživatele a nastavení práv tak, aby bylo možné nastavit každému práva pouze na určitou oblast (tj. nikoliv jedno společné heslo a přístup pro všechny) – řeší CI UJEP.

D. Doporučení k tvorbě vstupních hesel

a) Heslo musí obsahovat minimálně 8 znaků.
b) Mělo by se jednat o kombinaci velkých a malých písmen a čísel nebo speciálních znaků.
c) Neměla by obsahovat "slovníková" slova - např. "Skola123".
d) Měla by být nastavena pravidelná změna hesel, minimálně 2 x za rok.
e) Hesla by se neměla psát nikam na papír a ukládat poblíž počítače.
f) Heslo pro přístup do počítače by mělo být jiné než heslo pro přístup do softwaru/aplikace s osobními daty (tak, aby se pro přístup k osobním datům zadávala minimálně 2 různá hesla).
g) Jakýkoliv systém by měl umožnit změnu hesla ze strany uživatele v jakýkoliv okamžik.
h) Hesla by měla být „odolná" vůči celým jménům (uživatele), známým číselným údajům (rok narození, číslo kanceláře, přirozená posloupnost čísel apod.).

E. Používání softwaru

a) Na počítačích je potřeba mít nainstalované pouze legální verze veškerého softwaru.
b) Je nutné vždy mít software aktualizovaný, zejména:
   i. operační systém (aktualizuje se většinou automaticky),
   ii. kancelářský software, např. MS Office (aktualizuje se rovněž automaticky),
   iii. oficiální antivirový program,
   iv. oficiální webový prohlížeč,
   v. popř. software používaný pro práci s osobními údaji.

F. Předávání a zasílání osobních údajů

a) Osobní údaje předávané či zasílané v elektronické podobě by měly být vždy zabezpečené a zaheslované tak, aby v případě ztráty média (např. flash-disk) nebo nabourání se do e-mailu nebylo možné se k osobním údajům dostat bez znalosti přístupového hesla.
b) Osobní údaje nelze posílat přímo e-mailem, ale formou zaheslované přílohy.
c) Doporučujeme zasílat osobní údaje formou datové schránky.

G. Využívání bezdrátová sítě - Wi-Fi

a) Nedoporučujeme používat Wi-Fi zcela nezabezpečenou – tzn. bez přístupového hesla.
b) Heslo by se mělo pravidelně měnit – minimálně 1x ročně.

H. Fotografie, videozáznamy

a) Nesouhlas musí být vždy respektován.
b) Musí být respektována obecná etická pravidla.
c) Lze pořizovat obecné dokumentační záznamy – novinářská licence – netýká se face boku!!!

d) Portrétní a kontaktní fotografie (např. na webu fakulty) – je nutné respektovat nesouhlas, souhlas je při zveřejnění vždy nutný, nelze zveřejňovat automaticky tím, že je někdo zaměstnanec fakulty.
e) Fotografie pro marketingové účely (billboardy, propagační předměty) – musí být pořízen samostatný souhlas.

I. Newslettery

a) Rozesílání dle oprávnění a po udělení souhlasu adresáta.
b) Musí existovat širší souvislost obsahu sdělení se studiem (studentská akce, mimořádné přednášky).
c) Týká se i informačních e-mailů zaměstnancům.
d) Souhlas musí být vždy snadno a zřejmě odvolatelný.

J. Studijní agenda

a) Primárním kanálem pro komunikaci se studenty je IS STAG.
b) Přijímací zkoušky – nezveřejňovat seznamy volně na internetu, pouze v den konání zkoušky a v místě konání může být vyvěšen jmenný seznam studentů – ne u vchodu do budovy či areálu, ne celý den.
c) Výsledky testů a zkoušek – zadávat do STAGu, nezasílat e-mailem, nevyvěšovat volně, pokud volné zveřejnění – ne pod jménem, ale pod osobním číslem studenta ano.
d) Průběžné výsledky ročníkových zkoušek (dílčí výsledky) – lze zadávat body (nově řeší CI).
e) Státnicové zkoušky a obhajoby závěrečných prací – výsledky lze vyhlašovat po skupinkách, citlivě (popř. individuálně) vyhlašovat neúspěšný výsledek, na web lze umístit obecné informace o čase a místu konání (protože SZZ je veřejná zkouška), seznamy studentů – jen v den konání a ne u vchodu do budovy, lze uveřejnit jméno a obor.
f) Odborné praxe – není třeba souhlas se zpracováním osobních údajů od studenta, nutno podchytit zpracování těchto údajů smluvně s partnerem.
g) Doručení rozhodnutí veřejnou vyhláškou – není nutný souhlas s uveřejněním osobních údajů od studenta (jde o alternativu doručení) – uveřejňované údaje mají být nezbytné.
h) Minimalizace sběru osobních dat na formulářích
i) Promoce – zpracovatelská smlouva s fotografem, lze pořizovat dokumentační (novinářské) fotografie bez souhlasu – nesouhlas je třeba ale respektovat, absolventi by měli být poučení o fotografování (individuální souhlas není třeba), ostatní účastníci by měli být jen poučeni o focení a natáčení, nesouhlas musí být vždy respektován.

K. Žádost a o sdělení osobních údajů:

a) Řeší děkanát PF – u žádostí postoupených PF, jinak rektorát UJEP.
b) Je nutné ověření totožnosti žadatele o sdělení.
c) Mohou poskytovat jen pověřené osoby na UJEP.
d) Vyřízení do 30 dnů – popř. výjimky prodloužení o 60 dnů.

L. Mlčenlivost

a) Mlčenlivost musí být zajištěna (poučením podepsaným formulářem – viz příloha) u všech, kteří osobní údaje zpracovávají – týká se osobních údajů studentů a účastníků kurzů CŽV (tzn. pracovníků studijních odd. a pracovníků CCV), zaměstnanců a externích spolupracovníků fakulty (tzn. sekretářky a ti, kdo zpracovávají mzdovou agendu a agendu dohod o provedení práce a dohod o pracovní činnosti).

b) Stejný postup musí být užit i u závěrečných prací a u spoluřešitelů projektů. Zde je odpovědnost na vedoucích těchto prací a na hlavních řešitelích projektů.

c) Pokud je vybrán externí partner pro zpracování dat (např. výzkumných) – musí být odpovědně vybrán s ohledem na zásady GDPR a musí být v tomto smyslu prověřen.

M. Ohrožení osobních dat

a) Nejen vlastní ohrožení, ale i podezření tohoto typu musí být hlášeno děkanovi fakulty či kontaktní osobě pro politiku GDPR na fakultě.

V Ústí nad Labem dne 24. 7. 2018

Doc. PaedDr. Pavel Doulík, Ph.D.
děkan PF

Zpracoval:
dr. Bertl, kontaktní pracovník pro oblast GDPR na PF UJEP

Příloha:
formulář poučení o práci s osobními údaji (mlčenlivost)

Aktualizace informací – září 2018

- **Písemný souhlas se zpracováním osobních údajů musí být využíván minimálně** – Úřad pro ochranu osobních údajů může postihnout i nadbytečné užívání tohoto nástroje.
- **Osobní údaje nesmí být shromažďovány „pro jistotu" apod.**
- Poučení o zpracování osobních údajů se týká i externích spolupracovníků PF (externích vyučující, externích vedoucích závěrečných prací apod.).
- **Osobní fotografie (tzn. portrétové) uveřejněné na webu:**
    - Souhlas nemusí být u vedení univerzity a u vedení fakulty.
    - Souhlas se zveřejněním osobní fotografie musí být u vedení katedry, členů katedry apod.
    - Souhlas se zveřejněním osobní fotografie nemusí být u běžných dokumentačních (nikoliv portrétních) fotografií z akcí (konferencí, závodů apod.); pokud ale jednotlivec nesouhlasí s fotografováním a uveřejněním, fotografování ani uveřejnění neproběhne.
    - Pokud se dokumentační fotografie na akci týká nezletilého a jeho zákonný zástupce s fotografováním nesouhlasí, musí být nesouhlas respektována a fotografování ani uveřejnění neproběhne.
    - Ustanovení o uveřejnění fotografií se týká identicky i životopisů.
- **Jména v článku** (kolegů, participantů) uváděna být mohou (bez bližších osobních údajů).
- **Zabezpečení osobních údajů**: vždy uzamčením prostoru (fyzické údaje) nebo šifrováním (elektronické údaje).
- **Prezenční a docházkové listiny** – týká se jich podobný režim jako jiných osobních údajů:
    - nesmí být veřejně přístupné,
    - docházková listina na pracoviště nesmí ležet volně na chodbě,
    - musí obsahovat jen nezbytné údaje – ne datum narození,
    - pokud se tam uvádí datum narození (aby mohlo být snadněji např. vyhotoveno osvědčení), nelze tyto údaje shromažďovat na prezenční listině (protože je k nahlédnutí ostatním účastníkům).
- **Hlášení napadení osobních údajů** musí proběhnout do 72 hod. od zjištění.
- **Seznamy studentů – přijímací zkoušky**:
    - nelze zveřejňovat jmenné seznamy předem na internetu,
    - lze zveřejnit v den konání zkoušky jmenné seznamy – ale ne vně budovy a u hlavního vchodu, lze jen po dobu konání přijímací zkoušky,
    - výsledky zkoušky lze uveřejňovat jen v systému STAG – tzn. pod osobním přístupem – nikoliv veřejně.
- **Seznamy studentů – státní závěrečné zkoušky a obhajoby:**
    - nelze zveřejňovat jmenné seznamy předem na internetu,

  - lze uveřejnit obecnou informaci o konání státní zkoušky na internetu předem,
  - lze zveřejnit v den konání zkoušky jmenné seznamy – ale ne vně budovy a u hlavního vchodu, lze jen po dobu konání zkoušky,
  - výsledky zkoušky a obhajoby lze vyhlásit v okruhu zkoušených (nikoliv veřejně) – vyžadování souhlasu od těchto účastníků jen pro tento účel je nezákonné, resp. nadbytečné.
- **Praxe**: není nutné vyžadovat po studentech souhlas se zpracováním osobních údajů jen v této souvislosti.
- **Doručování veřejnou vyhláškou**:
  - je přípustné jen s uveřejněním základních identifikačních údajů příjemce, resp. adresáta,
  - nelze řešit formou vyvěšením nedoručené obálky.
- **Promoce (aktualizace 06/2019)**:
  - ~~je nutný písemný vztah s externím fotografem (PF má),~~
  - ~~je nutné poučení studentů – v rozsahu běžného souhlasu studenta, resp. pro promoci není nutný další souhlas (PF má),~~
  - prostor konání promocí musí být označen jako prostor, kde se bude fotografovat a natáčet – textem nebo piktogramem (PF používá),
  - fotografie a videa z promocí nesmí být volně přístupná.
- **Fotografie pro marketing, newslettery:**
  - lze rozesílat bez předchozího speciálního souhlasu,
  - nesouhlas musí být ale lehce proveditelný a účinný,
  - tento typ informací (pozvánky na další ročník konference, na další typ studia na další závody atd.) musí souviset s předmětem dosavadního kontaktu, resp. nelze takto distribuovat odlišné či obecné komerční informace.

<u>*Zpracoval:*</u>
dr. Bertl, kontaktní pracovník pro oblast GDPR na PF UJEP

POUČENÍ O PRÁCI S OSOBNÍMI ÚDAJI

Jméno a příjmení .....

Datum narození .....

Potvrzuji, že jsem byl/a poučen/a o svých povinnostech plynoucích z přístupu k osobním údajům zaměstnanců a studentů Univerzity Jana Evangelisty Purkyně v Ústí nad Labem (dále jen „univerzita“), stanovených v nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) v platném znění a o podmínkách a rozsahu zpracování těchto osobních údajů.

Zavazuji se zachovávat mlčenlivost ohledně zpracovávaných osobních údajů. Zejména se zavazuji tyto údaje žádným způsobem **nezaznamenávat, nekopírovat, nepřenášet a nesdělovat ani neposkytovat** neoprávněným osobám či za jiným účelem než bylo určeno, a to ani jako celek ani jakoukoli jejich část, ani jim toto neumožním jiným způsobem, např. svou nečinností. Jsem si vědom toho, že pokud tak učiním, mohu být trestně stíhán. Zavazuji se univerzitě nahradit škodu způsobenou porušením výše uvedených povinností.

Povinnost mlčenlivosti se zavazuji dodržovat i po skončení mého právního vztahu k univerzitě.

Datum …….....

Podpis .....