

čj. UKKaM/106147/2019  
V Praze dne 10. 4. 2019

## **SMĚRNICE ŘEDITELE Č. 2/2019**

### **O OCHRANĚ A ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ VE STŘEDISCÍCH KOLEJÍ A MENZ**

Tato směrnice ředitele je určena pro jednotlivé zaměstnance Kolejí a menz, kteří přicházejí do styku s osobními údaji (dále jen „zaměstnanci“) a jsou povinni dodržovat zaměstnavatelem nastavené podmínky ochrany osobních údajů při zpracování evidencí obsahujících osobní údaje ve smyslu ust. § 13 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů a v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 ve všech střediscích Kolejí a menz v Praze, Brandýse n/Labem, Plzni a v Hradci Králové.

## Úvodní ustanovení

Správce osobních údajů je Univerzita Karlova, Ovocný trh 560/5, 116 36 Praha 1, IČO: 00216208, Koleje a menzy: <https://kam.cuni.cz/KAM-532.html>.

- (a) Koleje a menzy (dále také jen "KaM"), sídlící na adrese kolej Hvězda, blok A3, Zvoníčkova 1927/5, 162 08 Praha 6 – Břevnov, jsou součástí Univerzity Karlovy (IČO 00216208) jako její účelové zařízení. Univerzita Karlova je veřejná vysoká škola, zřízená zákonem č. 111/1998 Sb., zákon o vysokých školách, ve znění pozdějších předpisů, nemá zřizovací listinu a nezapisuje se do obchodního rejstříku.
- (b) V rámci činnosti Kolejí a menz dochází ke zpracovávání osobních údajů ubytovaných studentů, zaměstnanců a cizích klientů, dále vlastních zaměstnanců a strážníků (zaměstnanci, studenti, cizí klienti).
- (c) Koleje a menzy využívají zpracovatele, kteří na základě uzavřených smluv, včetně jejich příloh a dodatků, provádějí správu systémů, a to:
- pro oblast **ubytování** firma Mefisto Solutions s.r.o., U Továren 770/1b, 102 00 Praha 10, IČO 252 00 992 a firma YOUR SYSTEM, spol. s r.o., Türkova 2319/5b, 149 00 Praha 4 - Chodov, IČO 001 74 939 (rezervační portál);
  - pro oblast **stravování** firma ANETE spol. s r.o., Okružní 834/299, Brno – Lesná, IČO 469 70 126;
  - pro oblast **personální a mzdovou** firma DATACENTRUM systems & consulting, a.s., Písnická 30/13, 140 00 Praha 4, IČO 256 31 721; dále vnitrouniverzitní systém EGJE (Software Elanor Global Java Edition – EGJE představuje nástroj pro řízení lidských zdrojů informační systém komplexně řešící mzdovou, personální a docházkovou agendu pro firmy).
  - **pro oblast účetnictví** firma MÚZO Praha s.r.o., Politických vězňů 934/15, 110 00 Praha 1, IČO 496 22 897;
  - **pro oblast zabezpečení** majetku kamerovým systémem firma MC Systems & Services s.r.o., se sídlem Weilova 1450/2e, 102 00 Praha 10, IČO: 282 52 063
- (d) Pověřencem (DPO) za Univerzitu Karlovu je subjekt, který sám nebo společně s jinými monitoruje soulad zpracování osobních údajů s povinnostmi vyplývajícími z nařízení a celkově řídí agendy interní ochrany dat v souladu s GDPR. Pověřence lze kontaktovat na adrese [gdpr@cuni.cz](mailto:gdpr@cuni.cz). V KaM je možné kontaktovat koordinátora na adrese [gdpr@kam.cuni.cz](mailto:gdpr@kam.cuni.cz) nebo na adrese [office@kam.cuni.cz](mailto:office@kam.cuni.cz).
- (e) Směrnice pro ochranu osobních údajů upravuje technicko-organizační opatření k zajištění ochrany osobních údajů v souladu s platnou a účinnou legislativou v oblasti ochrany osobních údajů, zejména nikoliv však výlučně zákonem č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů a Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 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) (dále jen „Předpisy na ochranu osobních údajů“), s cílem zajištění zpracování osobních údajů v souladu s touto legislativou a principy, na kterých je vystavěná.
- (f) Směrnice je závazná pro jednotlivé zaměstnance Kolejí a menz, kteří přicházejí do styku s osobními údaji (dále jen „zaměstnanci“) a Oprávněné osoby (jak je tento pojem definován níže).

## **Definice a výklad pojmů**

Pro účely této Směrnice se rozumí:

- (g) **automatizovaným zpracováním** zejména:
  - (i) ukládání informací na nosiče dat;
  - (ii) provádění logických nebo aritmetických operací s těmito daty, zejména jejich změna, výmaz, vyhledávání nebo rozšiřování uskutečňované zcela nebo zčásti pomocí automatizovaných postupů;
  - (iii) provádění archivace informací jejich uložením na archivační paměťová média a v případě potřeby obnovení informací z archivních médií;
- (h) **DPIA** posouzení vlivu na ochranu osobních údajů (anglicky *Data Protection Impact Assessment*) (jak je tento pojem definován v Předpisech na ochranu osobních údajů).
- (i) **DPO** pověřenec pro ochranu osobních údajů (anglicky *Data Protection Officer*) (jak je tento pojem definován v Předpisech na ochranu osobních údajů).
- (j) **ICT** informační a telekomunikační technologie.
- (k) **manuálním zpracováním** rozumíme jakékoliv zpracování s výjimkou zpracování automatizovaného (např. listinná podoba, kartotéky, právní agenda - spisy).
- (l) **oprávněnou osobou** rozumíme
  - (i) zaměstnanec, který v rámci plnění povinností plynoucích mu z pracovní náplně má přístup k osobním údajům a dále je zpracovává, a
  - (ii) právnická osoba, které na základě smluvního vztahu má Kolejemi a menzami povolený přístup k osobním údajům - viz čl. 1, písm. c).
- (m) **osobním údajem** rozumíme jakékoliv informace o identifikované nebo identifikovatelné fyzické osobě (**subjekt údajů**); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.
- (n) **osobním údajem zvláštní kategorie** rozumíme osobní údaj vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.
- (o) **profilováním** rozumíme jakoukoliv formu automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, chování, místa, kde se nachází, nebo pohybu.
- (p) **příjemcem** rozumíme každý subjekt, kterému jsou osobní údaje zpřístupněny. Za příjemce se nepovažuje subjekt, který zpracovává osobní údaje pro potřeby výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci; v případech veřejného pořádku a vnitřní bezpečnosti; předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů; významného hospodářského a finančního zájmu České republiky nebo Evropské unie.
- (q) **souhlasem** subjektu údajů rozumíme jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.
- (r) **správce** rozumíme právnickou osobu, orgán veřejné moci, který sám nebo společně s jinými určuje účely a prostředky zpracování.
- (s) **ÚOOÚ** znamená Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, PSČ 170 00, Praha 7, webové stránky [www.uoou.cz](http://www.uoou.cz).
- (t) **zpracováním** osobních údajů rozumíme jakoukoliv operaci nebo soubor operací s osobními údaji nebo soubory osobních údajů, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování,

uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

- (u) **zpracovatelem** rozumíme fyzickou nebo právnickou osobu, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

#### **Úkony před započítáním zpracování osobních údajů**

- (v) Před započítáním zpracování osobních údajů je správce povinen vypracovat záznamy o činnostech zpracování.
- (w) Účely (důvody) zpracování osobních údajů v jednotlivých agendách vychází ze zvláštních zákonů, nebo jsou osobní údaje zpracovávány na základě rozhodnutí správce.
- (x) Ke každému účelu zpracování musí být přiřazen právní titul, právními tituly pro zpracování jsou:
- (i) souhlas subjektu údajů;
  - (ii) plnění smlouvy, které stranou je subjekt údajů;
  - (iii) plnění právní povinnosti KaM;
  - (iv) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů;
  - (v) splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci; a
  - (vi) oprávněný zájem KaM.
- (y) Není-li zpracování osobních údajů nezbytné (i) pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů, (ii) pro splnění právní povinnosti, která se na KaM vztahuje, (iii) zpracování není nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, (iv) zpracování není nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým by KaM byla pověřena, (v) zpracování není nezbytné pro účely oprávněných zájmů KaM či třetí strany, zajistí KaM/zpracovatel před zpracováním osobních údajů souhlas subjektu údajů se zpracováním osobních údajů a tento souhlas (včetně podmínek, za kterých byl udělen) uchovává po celou dobu zpracování osobních údajů tohoto subjektu.
- (z) Za souhlas se zpracováním osobních údajů je považováno poskytnutí těchto údajů subjekty osobních údajů:
- (i) v listinné podobě s uvedením vlastnoručního podpisu včetně údaje o čase podpisu;
  - (ii) v elektronické podobě s např. připojením elektronického podpisu, se zaškrtnutím příslušného políčka se souhlasem v elektronickém formuláři, atd.
- (aa) Udělený souhlas musí být prokazatelný po celou dobu zpracování, včetně všech podmínek, ze kterých je zřetelné k čemu a v jakém znění byl souhlas udělen. V případě, že subjekt údajů souhlas neposkytne, nelze jeho osobní údaje zpracovávat. Souhlasy jsou archivovány v SW, lze vytisknout. V písemné podobě potom na daném středisku.

#### **Informační povinnost**

- (bb) Při shromažďování osobních údajů přímo od subjektu údajů musí být subjekt osobních údajů, k němuž se osobní údaje vztahují, informován nejpozději v okamžiku získávání jeho osobních údajů o:
- (i) totožnosti a kontaktních údajích KaM a jejich zástupci;
  - (ii) kontaktních údajích DPO UK;
  - (iii) účelech zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;
  - (iv) oprávněných zájmech KaM nebo třetí strany v případě, že je zpracování založeno na tomto právním důvodu zpracování;
  - (v) případných příjemcích nebo kategoriích příjemců osobních údajů;
  - (vi) případném úmyslu KaM předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Evropské komise o odpovídající ochraně nebo, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny;
  - (vii) době, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby – stanoveno ve Spisovém a skartačním řádu;
  - (viii) existenci práva požadovat od KaM, přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;

- (ix) pokud je zpracování založeno na souhlasu subjektu údajů, existenci práva kdykoli odvolat tento souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;
  - (x) existenci práva podat stížnost u ÚOOÚ;
  - (xi) skutečnosti, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů; a
  - (xii) skutečnosti, že nedochází k automatizovanému rozhodování, včetně profilování a informacích týkajících se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.
- (cc) Při shromažďování osobních údajů jiným způsobem než od subjektu údajů, musí být subjekt osobních údajů, k němuž se osobní údaje vztahují, informován nejpozději v okamžiku získávání jeho osobních údajů o skutečnostech v odstavcích (i), (ii), (iii), (iv), (v), (vi), písmene (a) tohoto článku a kategoriích dotčených osobních údajů.

**Informační povinnost** dle tohoto článku plní oprávněné osoby shromažďující osobní údaje od subjektů údajů, a to formou tzv. Informační povinností správce v oblastech činností:

- a) ubytování, kdy je dokument zobrazen na obrazovce PC ihned po poskytnutí osobních údajů studentem do rezervačního systému REHOS;
- b) stravování, kdy je dokument zobrazen na obrazovce pracovníka provozu, který ho vytiskne 2x, jedno podepsané paré si ponechá a druhé obdrží cizí strážník, osobní údaje ostatních studentů čerpáme z centrální evidence rektorátu UK. Informace jsou uvedeny na úřední desce KaM.
- c) zaměstnanci KaM byli proškoleni, dále obdrželi publikaci Příručku pro zaměstnance v elektronické podobě. Noví zaměstnanci obdrží publikaci v tištěné podobě proti podpisu v personální agendě KaM. Publikace byla vydána v rámci CRP projektu MŠMT 2018 „Komplexní řešení ochrany osobních údajů v prostředí vysokých škol“, vydavatel Zdeněk Šustr.

Koleje a menzy připravily pro studenty, klienty, obchodní partnery a zaměstnance podrobné **Informační memorandum**, které je zveřejněno na webových stránkách KaM na úřední desce na adrese: <https://kam.cuni.cz/KAM-532.html>, spolu s odkazy na další informace vydané rektorátem UK.

#### **Vyřizování žádostí subjektů údajů**

- (dd) **Základní zásady vyřizování žádosti**

Žádosti subjektů údajů vyřizuje za všechny fakulty a součásti Univerzity Karlovy jen DPO na adrese: [gdpr@cuni.cz](mailto:gdpr@cuni.cz). KaM mají také na svých webových stránkách uvedenou adresu pro zasílání žádostí a to: [gdpr@kam.cuni.cz](mailto:gdpr@kam.cuni.cz). Žádosti na tuto adresu subjektem údajů poslané jsou automaticky přesměrovány na adresu DPO, kde jsou zaevidovány a v přímé posloupnosti jsou přeposlány zpět do KaM k vyřízení.

- (i) KaM přijímá žádosti subjektů údajů v elektronické podobě, zaslané e-mailem nebo v listinné podobě zaslané na adresu sídla KaM. V případě, že se subjekt údajů obrátí na KaM se žádostí ve věci výkonu svých práv v ústní formě telefonicky nebo osobně, příslušný zaměstnanec subjekt údajů informuje o možnosti zformulovat svoji žádost elektronicky; v případě, že subjekt trvá na vyřízení žádosti telefonicky nebo ústně, nelze žádosti tímto způsobem vyhovět, neboť nelze identifikovat žadatele, v tom případě bude požádán, aby se dostavil osobně k prokázání totožnosti. Následně bude jeho žádost vyřízena obvyklým způsobem popsáním výše.
- (ii) Žádosti mohou být KaM zaslané i jí určeným zpracovatelem, odpovědnost za vyřízení takových žádostí má však vždy KaM – správce.
- (iii) KaM bude nakládat se zaevidovanou žádostí dle postupu níže v případě, že:

- (A) se žádost týká osobních údajů a/nebo jejich zpracování; nebo

- (B) se v žádosti uvádí požadavek na výkon práv subjektu údajů dle Právních předpisů v oblasti ochrany osobních údajů; nebo
- (C) se v žádosti uvádí, že je spojena s Právními předpisy v oblasti ochrany osobních údajů.

### **Postup při vyřízení žádosti subjektu údajů**

- (iv) Ověření identity subjektu údajů – aby bylo zajištěno jednání s konkrétní dotčenou osobou, a to nejen v případě, že je žádost podaná zmocněncem subjektu údajů;
- (v) Vyjasnění žádosti a jejího předmětu – v případě, že ze žádosti není zřejmé, čeho se subjekt údajů dožaduje, nebo jsou v žádosti obsažené chybné informace, jejichž správné znění je však nevyhnutné pro její vyřízení, subjekt údajů bude vyzván k jejímu upřesnění;
- (vi) Posouzení žádosti – zda má subjekt údajů právo na výkon daného práva a zda neexistuje výjimka, která by tento výkon znemožňovala;
- (vii) Vyřízení žádosti:
  - (A) Zamítnutí žádosti – subjekt údajů není oprávněn vykonat požadované právo nebo existuje výjimka, kvůli které tento výkon není možný. V odůvodnění zamítavé odpovědi na žádost musí být uvedeny důvody zamítnutí a informace o možnosti podat stížnost u ÚOOÚ a vyřízení záležitosti soudní cestou; nebo
  - (B) Vyhovění žádosti – subjekt údajů je oprávněn vykonávat svoje právo a neexistuje výjimka, která by mu v tom bránila.
- (ee) Subjekt údajů musí být informován o krocích, které byly podniknuty v souvislosti s vyřizováním jeho žádosti do 1 měsíce od jejího podání. V případě větší složitosti záležitosti nebo většího počtu žádosti či námitek podaných subjektem údajů během 1 měsíce, může být lhůta pro vyřízení prodloužena o 2 měsíce, o čem bude subjekt údajů informován, včetně důvodů pro tento odklad. Odpověď bude subjektu údajů podána ve stejné formě, v jaké byla podána jeho žádost, pokud nebude dohodnuto jinak.
- (ff) Vyřizování žádosti se činí bezplatně. Jsou-li však žádosti subjektem údajů podané zjevně nedůvodně nebo nepřiměřeně, zejména pokud se opakují, může Společnost účtovat za vyřízení žádosti přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím požadovaných informací nebo s učiněním požadovaných úkonů, případně může odmítnout žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost žádosti musí být KaM schopny doložit.

### **Specifické postupy ohledně jednotlivých práv subjektů údajů**

#### **Právo na přístup**

V obdržené žádosti o uplatnění práva na přístup se identifikuje jeden z následujících předmětů žádosti:

- ✓ potvrzení, jestli jsou nebo nejsou v KaM zpracovávány osobní údaje daného subjektu údajů;
- ✓ informace o tom, jak jsou osobní údaje subjektu údajů zpracovávány; nebo
- ✓ přehled veškerých nebo určitých osobních údajů, které jsou o subjektu údajů zpracovávány.

Toto právo je nepodmíněné a nejsou zde žádné výjimky, takže se žádosti musí vyhovět, přičemž se musí brát ohled na práva a svobody třetích osob, které by mohly být dotčeny poskytnutím vyžádaného přehledu. V případě dotazů či nejasností prosím kontaktujte koordinátora KaM.

#### **Právo na opravu**

Osobní údaje zpracovávané KaM musí být úplné, správné a aktuální. Na základě žádosti subjektu údajů se do všech systémů KaM a jí pověřených zpracovatelů či příjemců vloží opravené nebo doplněné údaje a ty budou použity při všech dalších zpracováních.

Pokud je v žádosti subjektů údajů obsažen také požadavek na omezení zpracování po dobu, než bude korekce údajů předložena a takové opatření je nezbytné pro ochranu práv a svobod subjektu údajů, dojde k přerušení zpracování osobních údajů po dobu, kdy probíhá jejich korekce.

### **Právo na výmaz (právo být zapomenut)**

Subjekt údajů je oprávněn požadovat výmaz jen za určitých podmínek, a to když:

- ✓ osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovávány;
- ✓ subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování;
- ✓ subjekt údajů vznesl námitku proti zpracování a neexistují žádné převažující oprávněné důvody KaM pro zpracování;
- ✓ osobní údaje byly zpracovány protiprávně;
- ✓ osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Evropské unie nebo České republiky.

Každá žádost musí být individuálně posouzena, zda jsou podmínky splněny a zda se neuplatní žádné výjimky, na základě, kterých musí být určité osobní údaje i přes žádost o výmaz zpracovávány (např. k plnění zákonné povinnosti).

V případě, že KaM vyhodnotí, že požadované údaje lze vymazat, uvědomí o této skutečnosti i všechny ostatní zpracovatele a zajistí, aby ani tito již předmětné osobní údaje nezpracovávali.

### **Právo na omezení zpracování**

Omezení zpracování je dočasné opatření, o které může být subjektem údajů žádáno v případě:

- ✓ že zpracování je protiprávní, subjekt dat odmítá výmaz a žádá místo něho omezení;
- ✓ aby se aplikovalo během vyřizování žádosti o opravu nebo námitky subjektu údajů proti zpracování (subjekt dat popírá přesnost údajů); a
- ✓ jako ochrana proti vymazání osobních údajů, ke kterému by jinak došlo (např. subjekt vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody KaM převažují nad důvody subjektů dat).

Za některých podmínek mohou být osobní údaje, u kterých je zpracování omezeno, zpracovány pro určité účely, např. ochrana právních zájmů nebo zpracování se souhlasem subjektu.

### **Právo vznést námitku**

Prvním krokem ke zpracování námitky je zjištění, zda je podávána proti zpracování osobních údajů týkající se KaM, resp. zda pro marketingové účely, oprávněné zájmy KaM nebo zda jde o zpracování ve veřejném zájmu nebo pro vědecké či statistické účely týkající se jedinečné situace subjektu údajů.

- ✓ Právo vznést námitku proti zpracování pro účely přímého marketingu je nepodmíněné a námitce musí vždy vyhovět, přičemž není podstatné, na jakém právním důvodu se toto zpracování zakládá.
- ✓ Každá žádost musí být individuálně posouzena, zda jsou podmínky splněny a zda se neuplatní žádné výjimky.



- ✓ Po vyhovění žádosti nesmí být osobní údaje používány pro dané účely (marketing, oprávněný zájem, statistika, výzkum) a budou v souladu s principem minimalizace vymazány. Pokud jsou dané osobní údaje zpracovávány pro jiné účely, toto zpracování může probíhat i nadále.

### **Právo na přenositelnost**

- ✓ Právo na přenositelnost může subjekt údajů uplatnit v případě, že je zpracování založeno na právním důvodu uděleného souhlasu a pro účely uzavření a plnění smlouvy a zároveň když je zpracování prováděno automatizovaně. Výjimkou je zpracování nezbytné ve veřejném zájmu nebo při výkonu veřejné moci.
- ✓ Osobní údaje, které byly poskytnuty KaM subjektem údajů nebo které byly vytvořeny na základě požadavků subjektu údajů, budou předány ve strojově čitelném formátu (např. XML).
- ✓ Přenos osobních údajů se uskuteční v takové formě, která minimalizuje bezpečnostní rizika (např. za využití šifrování).

Pokud byly vyžádané osobní údaje předány subjektu údajů, oznámení subjektu údajů se podá jen v případě, že došlo k omezením v důsledku např. dopadu na práva třetích subjektů.

### **Oznámení subjektům ohledně výmazu, opravy nebo omezení zpracování**

V případě vyhovění výkonu výše uvedených práv, musí být zpracovatelé a jiní příjemci osobních údajů informováni o jakémkoliv výmazu, opravě nebo omezení zpracování. Zároveň musí být jasně instruováni k podniknutí kroků k danému výmazu, opravě nebo omezení zpracování.

V případě dotazů či nejasností prosím kontaktujte koordinátora KaM.

Žádosti subjektu údajů týkající se ubytování vyřizuje vedoucí Útvaru ubytovacích služeb.

Žádosti subjektu údajů týkající se stravování vyřizuje vedoucí Útvaru stravovacích služeb.

Žádosti subjektu údajů týkající se personalistiky vyřizuje vedoucí Organizačně správního útvaru.

Vyřízená žádost je přeposlána zpět přes podatelnu KaM na adresu DPO: [gdpr@cuni.cz](mailto:gdpr@cuni.cz). V tomto okamžiku je žádost ze strany KaM považována za vyřízenou. Odeslání vyřízené žádosti subjektů údajů zajistí DPO. V případě dotazů či nejasností prosím kontaktujte DPO.

### **Hlavní bezpečnostní rizika**

Mezi hlavní bezpečnostní rizika, která hrozí při zpracování osobních údajů v rámci provozování personálních, ubytovacích a stravovacích činností, vč. kamerového systému patří zejména:

- ✓ zničení nebo zneužití technických prostředků;
- ✓ přístup neoprávněných osob k osobním údajům;
- ✓ zneužití záznamů ohledně osobních údajů oprávněnými osobami;
- ✓ živelní událost.

### **Pravidla řízení přístupu k osobním údajům**

(a) Řízení přístupu k prostředkům ICT je prováděno za uplatnění následujících principů, které se uplatňují jak pro zaměstnance, tak pro externí subjekty jako obchodní partnery a dodavatele, např. zajišťující služby pro KaM na základě smluvního vztahu:

- (i) princip minimálního oprávnění, tzn. přidělení pouze takových oprávnění, která jsou nezbytná k plnění jeho/jejích pracovních/smluvních povinností;
- (ii) princip periodického přezkoumávání přístupových oprávnění;
- (iii) princip revize a změny přístupových oprávnění při změně pracovní pozice či pracovní náplně zaměstnance či změně smluvního vztahu s jinými subjekty; a



- (iv) princip odebrání všech přístupových oprávnění při ukončení pracovního/smluvního vztahu.
- (b) Pravidla řízení přístupu se uplatňují pro uživatele, administrátory, privilegované účty s rozšířenými přístupovými oprávněními, externí subjekty, kterým má být umožněn přístup do informačního systému KaM.
- (c) Uživatel (vedoucí pracovník KaM) podá svoji žádost o přidělení přístupových práv stanoveným a formálním způsobem, a to na ÚVT RUK na adresu: [podpora@ruk.cuni.cz](mailto:podpora@ruk.cuni.cz), dále v KaM k rukám hlavní účetní (zajistí či zablokuje přístup do účetního systému), k rukám vedoucího ÚSS (zajistí či zablokuje přístup do stravovacího systému), k rukám vedoucího ÚUS (zajistí či zablokuje přístup do ubytovacího systému).
- (d) Okamžité zablokování přístupových oprávnění při zjištění porušení pravidel autorizace.

Uživatelé jsou odpovědní za autentizační informace (hesla) a jsou povinni zajistit jim řádnou ochranu.

### **Řízení rozšířených oprávnění**

- (a) V rámci přidělování rozšířených přístupových oprávnění je uplatňován princip minimální potřeby pro danou provozní roli. Rozšířená oprávnění jsou řízena a přidělována dle stanoveného formálního procesu autorizace.
- (b) Rozšířená práva, by měla být přiřazena k identifikátoru uživatele odlišného od identifikátoru, používaného pro běžné činnosti v KaM. Přehled o identifikátorech (účtech), kterým byla udělena rozšířená přístupová oprávnění, není veden, neboť tato práva mají pouze vedoucí útvarů ředitelství a ředitel organizace.

### **Zabezpečení přístupu heslem**

Systém správy hesel v KaM, má za cíl zajištění kvality hesla a způsobů jeho implementace při autentizaci uživatele dle potřeb KaM pro zajištění zabezpečení přístupu do informačního systému KaM. Systém správy hesel zabezpečí mimo jiné požadavky vynucení pravidelné změny hesla uživateli a stanovení parametrů hesel (např. doba platnosti nebo existence stanovených znaků). Zajišťuje UVT RUK.

### **Pravidla používání prostředků ICT (informační a komunikační technologie): zařízení (notebook, tablet, mobilní telefon, stolní počítač - PC) datový nosič (externí disk, SD karta, USB flash disk apod.)**

- (a) Zaměstnanci pracující ICT prostředky, které mu byly svěřené KaM, je mohou využívat pouze k výkonu svých pracovních povinností.
- (b) Zaměstnanci mají povinnost chránit svěřené ICT prostředky před ztrátou, poškozením, zničením či zcizením. Zejména jsou povinni uzamykat místnosti s ICT technologií při nepřítomnosti a přiměřeným způsobem chránit přidělené mobilní ICT prostředky.
- (c) V případě, že zaměstnanec ICT prostředek nemá pod přímou kontrolou (např. při opuštění kanceláře), musí používat základní ochranné prostředky, tj. např. software „uzamykání“ ICT prostředku, nebo jeho vypínání.
- (d) Pro bezpečný vzdálený přístup do ICT prostředí KaM je administrátorem ICT prostředků technologicky zajištěna bezpečná cesta.

### **BEZPEČNOSTNÍ UDÁLOSTI A INCIDENTY**

- (a) **Základní pravidla řízení bezpečnostních incidentů**

Řízení bezpečnostních incidentů a událostí zahrnuje v KaM, následující pravidla:

- (A) Pro oznamování událostí a incidentů, je v KaM, určen koordinátor GDPR, který přijímá oznámení o bezpečnostních událostech a incidentech na adrese: [gdpr@kam.cuni.cz](mailto:gdpr@kam.cuni.cz). Tato adresa je

propojená s adresou přímo na DPO, který přijaté oznámení o bezpečnostní události zaeviduje a dále zpracuje.

- (B) Všechny bezpečnostní incidenty jsou následně ve spolupráci s DPO vyhodnoceny s cílem určit příčinu výskytu incidentu a přijmout nápravné opatření.
- (C) Postup a opatření ke zvládnutí bezpečnostního incidentu jsou průběžně dokumentovány, veškeré dokumentované informace k bezpečnostnímu incidentu, jsou v KaM uchovávány v administraci koordinátora GDPR.

(b) **Postup zvládnutí bezpečnostních incidentů**

Postup při řešení bezpečnostního incidentu zahrnuje následující činnosti:

- (A) oznámení incidentu např. e-mailem prostřednictvím zaměstnance, který incident zjistil pověřenému koordinátorovi, který přijme oznámení na uvedené adrese: [gdpr@kam.cuni.cz](mailto:gdpr@kam.cuni.cz). Tímto úkonem se splněna podmínka ihned informovat DPO. Oznámení lze podat také telefonicky nebo ústně. Koordinátor KaM bude obratem informovat DPO, v případě jeho nepřítomnosti zajistí informování DPO jeho písemně jmenovaný zástupce.
- (B) DPO provede prvotní posouzení a prověření incidentu, jeho kategorizaci, posouzení incidentu a jeho dopadů, stanoví míru závažnosti incidentu.
- (C) DPO dále navrhne KaM konkrétní opatření ke zmírnění či eliminaci dopadů incidentu dle odhadnuté závažnosti incidentu a dle aktuálních možností. KaM (ředitel) rozhodne o přijetí okamžitých protiopatření k eliminaci incidentu a tím zabránění šíření jeho dopadů.
- (D) DPO provede analýzu a vyhodnocení příčin vzniku incidentu, posouzení slabého místa zabezpečení osobních údajů v KaM a podá návrh opatření ke zlepšení.
- (E) Projednání události proběhne na celopodnikové úrovni na poradách vedoucích útvarů a provozů KaM, kde budou přítomni seznámeni s navrženými protiopatřeními a opatřeními ke zlepšení ochrany dat. Koordinátor monitoruje realizaci protiopatření, vyhodnotí jejich účinnost a informuje DPO.

(a) **Při kategorizaci bezpečnostních incidentů se zohlední:**

- (A) důležitost dotčených osobních údajů,
- (B) dopady na poskytované služby KaM,
- (C) předpokládané škody a jiné dopady na práva a povinnosti subjektů údajů.

(b) **Pro potřeby zvládnutí bezpečnostních incidentů se incidenty dělí do následujících kategorií:**

Kategorie	Bezpečnostní incident
Kategorie 1 <b>(Méně závažný bezpečnostní incident)</b>	Dochází k méně významnému narušení bezpečnosti osobních údajů. Musí být zamezeno další šíření bezpečnostního incidentu.
Kategorie 2 <b>(Závažný bezpečnostní incident)</b>	Je narušena bezpečnost osobních údajů. Jeho řešení vyžaduje neprodlený zásah k zamezení dalšímu šíření bezpečnostního incidentu.
Kategorie 3 <b>(Velmi závažný bezpečnostní incident)</b>	Je významně narušena bezpečnost osobních údajů. Řešení vyžaduje neprodlený zásah obsluhy, všemi dostupnými prostředky musí být zabráněno dalšímu šíření bezpečnostního incidentu.

(c) **Oznamování případů porušení zabezpečení osobních údajů**

- (i) Druh, způsob a lhůty podávání oznámení závisí na tom, do které kategorie bezpečnostní incident/událost spadá:
  - (A) Kategorie 1: žádné oznámení není nutné;
  - (B) Kategorie 2: v případě porušení zabezpečení osobních údajů jsou KaM povinny oznámit toto bez zbytečného odkladu DPO, DPO oznámí pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl toto porušení ÚOOÚ, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob; nebo
  - (C) Kategorie 3: KaM musí oznámit porušení zabezpečení osobních údajů bez zbytečného odkladu subjektu údajů.
- (ii) Oznámení o porušení zabezpečení osobních údajů musí být vyhotoveno v souladu se vzorem Oznámení o porušení zabezpečení osobních údajů – zajistí DPO.
- (iii) Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu správci.
- (iv) Oznámení subjektu údajů dle tohoto článku se nevyžaduje, je-li splněna kterákoli z těchto podmínek:
  - (A) KaM zavedla náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;
  - (B) KaM přijala následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví;
  - (C) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

**Likvidace osobních údajů**

(a) **Zpracování osobních údajů je ukončeno:**

- (i) jakmile pomine účel, pro který byly osobní údaje zpracovávány,
- (ii) na základě žádosti subjektu údajů v případě, že
  - (A) již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
  - (B) pokud subjekt údajů odvolal svůj souhlas se zpracováním;
  - (C) pokud subjekt údajů vznesl námitku proti zpracování osobních údajů, které se jej týkají;
  - (D) zpracování jeho osobních údajů je v rozporu s Právními předpisy na ochranu osobních údajů z jiných důvodů.

**Osobní údaje budou neprodleně zlikvidovány:**

- (i) po uplynutí doby, po kterou byly osobní údaje uchovávány dle pravidel uvedených v příslušných právních předpisech podle Spisového řádu. Dokumenty jsou uloženy v zabezpečených spisovných na provozech a je vedena archivační kniha, po skončení doby uchování jsou archivační soupisy předány hlavní účetní, která je odpovědná za archiv KaM. Po kontrole obsahu a náležitostí jsou soupisy zaevidovány do ESS a odeslány do archivu RUK k rozhodnutí, které konkrétní dokumenty budou převezeny do centrálního

archivu RUK a které budou zničeny. Dokumenty jsou obvykle odvezeny do firmy, která zajistí jejich ekologickou likvidaci a doloží o tom protokol.

### **Předání osobních údajů do jiných zemí**

KaM nepředávají osobní údaje do jiných zemí.

### **Smluvně zajištěný zpracovatel**

Zpracovatelé jsou právnické osoby pověřené zpracováváním osobních údajů v souladu s podmínkami zakotvenými v uzavřené smlouvě o zpracování s KaM nebo s uzavřeným dodatkem k již existující smlouvě. Smlouva i dodatek mají písemnou formu - viz úvodní ustanovení, bod d).

### **Zpracování zvláštních kategorií osobních údajů**

- (a) Před zpracováním zvláštních kategorií osobních údajů musí být subjekt údajů informován a poučen v rozsahu informační povinnosti dle této Směrnice. Zvláštní kategorie osobních údajů mohou být zpracovány pouze s výslovným souhlasem subjektu údajů, kterého se týkají. Za výslovný souhlas lze považovat pouze takové právní jednání, kterým dotčená fyzická osoba výslovně svoluje ke zpracování svých osobních údajů zvláštních kategorií. Nedá-li tato fyzická osoba výslovný souhlas jejich zpracováním, nelze její osobní údaje zvláštních kategorií zpracovávat.
- (b) Poskytnuté osobní údaje zvláštních kategorií jsou pokládány za důvěrné informace a v rámci jejich dalšího zpracování se s nimi mohou seznamovat pouze oprávněné osoby, které tyto údaje potřebují pro plnění svých pracovních povinností.
- (c) KaM běžně nezpracovávají zvláštní osobní údaje ani citlivé osobní údaje.

### **Povinnosti zaměstnanců odpovědných za agendu ochrany osobních údajů**

Nejedná se o DPO, ale o zaměstnance KaM, kteří s osobními údaji přímo pracují.

- (a) Zaměstnanci odpovědní v rámci své odpovědnosti za ochranu osobních údajů zajišťují informovanost oprávněných osob (nadřízených) o problematice ochrany osobních údajů se zaměřením na:
  - (A) nové skutečnosti promítající se do systému ochrany osobních údajů (např. organizační, personální změny, update software),
  - (B) zahrnutí problematiky ochrany osobních údajů do plánu vzdělávání zaměstnanců KaM,
  - (C) provedení aktualizace této Směrnice při výrazných změnách Právních předpisů v oblasti ochrany osobních údajů,
  - (D) realizaci neodkladných opatření v oblasti zabezpečení ochrany osobních údajů.

V KaM se jedná o pracovníky personální a mzdové agendy a agendy PAM.

- (b) Koordinátor KaM informuje o:
  - (A) změnách v Předpisech o ochraně osobních údajů, příp. dalších právních předpisů s dopadem do problematiky zpracování osobních údajů;
  - (B) zevšeobecnění poznatků z kontrolní činnosti ÚOOÚ;
  - (C) o pokynech vydaných DPO RUK.

### **Kamerové systémy**

- (a) Ve vnějších a vnitřních prostorách budov (kolejí) ve správě KaM jsou instalovány kamerové systémy se záznamovým zařízením. Účelem instalace těchto kamerových systémů je ochrana majetku, bezpečnosti a dalších chráněných zájmů KaM, jejich zaměstnanců i dalších osob, nacházejících se v kolejích KaM. Subjekty údajů jsou o kamerovém systému informováni formou piktogramu, kde je uveden i kontakt na správce s odkazem na webové stránky správce <https://kam.cuni.cz/KAM-532.html>, kde jsou uvedeny podrobnější informace o právech, které mohou subjekty údajů uplatňovat.
- (b) Jednotliví zaměstnanci (ostraha koleje) s přístupem ke kamerovým záznamům či LIVE obrazu vidí na obrazovce snímané záběry nepřetržitě. Snímané záběry jsou uchovávány v záznamových zařízeních po dobu nejvýše 10 dnů. Po této době jsou zaznamenaná data automaticky přemazána novým zápisem. Zaměstnanci byli proškoleni a poučeni o dodržování nejen zákona o ochraně osobních údajů, ale také o ustanoveních zákoníku práce, který zakazuje skryté i otevřené sledování pracovníků na pracovišti a Nařízení Evropského parlamentu - GDPR. Stejně tak jsou zaměstnanci povinni dbát i jiných právních norem, které zaručují jednotlivci právo na soukromí.
- (c) Kamerové systémy nejsou napojeny na žádnou databázi operující s osobními údaji. Záznamy z kamerových systémů budou využity v souladu s účelem jejich instalace, a to v případě vnitřního šetření identifikovaného incidentu, nebo budou předány na vyžádání orgánů činných v trestním řízení jako důkazní materiál vyšetřování.
- (d) Snímané záběry jsou zaznamenány na serverech v Jinonicích – úložiště dat. Nahlížení má firma MC systém, která v KaM kamerový systém instalovala a rovněž provádí jeho údržbu. Správu systému provádí Ústav výpočetní techniky UK.
- (e) O kamerovém systému v KaM je vyhotovena Směrnice o provozování kamerového systému. Pro každou kolej je vyhotoven situační plánec s vyznačením, kde je kamera umístěna a popis kamer.

### **Porušení pracovních povinností**

Porušení povinností stanovených touto směrnicí může být považováno za hrubé porušení pracovních povinností a může být postihnuto dle zákoníku práce. Podle míry úniku dat je věc dále řešena jako správní delikt dle zákona na ochranu osobních údajů, případně jako trestný čin.

Záležitosti, které nejsou upraveny touto směrnicí, se řídí ustanovením příslušných zákonů. V případě nesouladu této směrnice s ostatními interními předpisy KaM mají ustanovení této směrnice přednost.

Tato směrnice je platná a účinná dnem vydání.

V Praze dne 10. 4. 2019

Ing. Jiří M a c o u n, v.r.  
ředitel

Zpracovala na základě podkladů z Internetu:  
M. Halámková, vedoucí KÚ KaM UK, v. r.

Rozdělovník: vedoucí odborných útvarů ředitelství, vedoucí organizačních jednotek KaM