

Ochrana a zpracování osobních údajů

Anotace: Tato směrnice s celoškolskou působností stanoví zásady a pravidla při zpracování osobních údajů v rámci Vysoké školy ekonomické v Praze (dále jen „VŠE“), stanoví odpovědnost osob zajišťujících ochranu osobních údajů na VŠE, vymezuje práva a povinnosti zaměstnanců, studentů, případně dalších fyzických i právnických osob účastnících se činností souvisejících se zpracováním těchto údajů.

	Zpracovatel:	Schválil:
Jméno:	Ing. Milan Nidl, MBA	prof. Ing. Hana Machková, CSc.
Útvar / funkce	ředitel Centra informatiky	rektorka
Datum:	7.11.2018	7.11.2018
Podpis:	Ing. Milan Nidl, MBA v. r.	prof. Ing. Hana Machková, CSc. v. r.
Platnost od:	25. května 2018	odvolání
Účinnost		
1. změny od:	8. listopadu 2018	

Část první

Základní ustanovení

Článek 1

Předmět úpravy

- (1) Tato směrnice stanoví zásady a pravidla při zpracování osobních údajů v rámci Vysoké školy ekonomické v Praze (dále jen „VŠE“), stanoví odpovědnost osob zajišťujících ochranu osobních údajů na VŠE, vymezuje práva a povinnosti zaměstnanců, studentů, případně dalších fyzických i právnických osob účastnících se činností souvisejících se zpracováním těchto údajů.
- (2) Předmětem úpravy této směrnice jsou zpracování osobních údajů realizovaná zaměstnanci a studenty VŠE při plnění jejich pracovních či studijních povinností, případně dalšími fyzickými a právnickými osobami, které zpracovávají osobní údaje na základě smlouvy s VŠE.
- (3) Tato směrnice vychází z nařízení Evropského parlamentu a Rady (EU) č. 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) (dále jen „nařízení“) a ze zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“), s tím, že doplňuje a rozpracovává některá jejich ustanovení pro úpravu vztahů v rámci VŠE a stanoví organizační řešení v rámci VŠE zajišťující jejich realizaci.

Článek 2

Výklad vybraných souvisejících pojmů

- (1) „Osobními údaji“ se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „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.
- (2) „Zpracováním osobních údajů“ se rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn 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.
- (3) „Správcem“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.
- (4) „Zpracovatelem“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.
- (5) „Pseudonymizací“ se rozumí zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;
- (6) „Evidencí“ se rozumí jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;

- (7) „Příjemcem“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování.
- (8) „Třetí stranou“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů;
- (9) „Souhlasem“ subjektu údajů se rozumí jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;
- (10) „Porušením zabezpečení osobních údajů“ se rozumí porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;
- (11) „Genetickými údaji“ se rozumí osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby;
- (12) „Biometrickými údaji“ se rozumí osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;
- (13) „Údaji o zdravotním stavu“ se rozumí osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu;
- (14) Definice dalších pojmů užitých při zacházení a ochraně osobních údajů jsou uvedeny v čl. 4 nařízení, případně v textu či přílohách této směrnice tam, kde je to účelné.

Část druhá

Odpovědnost osob zajišťujících ochranu osobních údajů

Článek 3

Postavení VŠE

VŠE je subjektem odpovědným za zpracování osobních údajů uvedených v čl. 1 odst. 2. Dle konkrétních případů může VŠE vystupovat jak v roli správce, tak v roli zpracovatele. Za účelem naplňování ochrany osobních údajů tak, jak je požadováno nařízením a zákonem o ochraně osobních údajů, jsou v části druhé této směrnice stanoveny osoby participující na zajišťování výše uvedeného účelu.

Článek 4

Centrální úroveň

- (1) Postavení rektora je dáno zákonem, Statutem Vysoké školy ekonomické v Praze, vnitřními předpisy VŠE dle čl. 3 Statutu Vysoké školy ekonomické v Praze a ostatními vnitřními předpisy VŠE. Rektor jedná jako statutární orgán VŠE odpovědný za dodržování zásad, pravidel a postupů při zpracování osobních údajů vně i dovnitř VŠE, a to v případech realizovaných na centrální úrovni VŠE a tam, kde nedošlo k posunu pravomocí na další osoby uvedené v této části.

- (2) Kvestor odpovídá rektorovi VŠE za dodržování zásad, pravidel a postupů při zpracování osobních údajů realizovaných v oblastech své působnosti dané čl. 13 Statutu Vysoké školy ekonomické v Praze.
- (3) Proreктоři odpovídají rektorovi VŠE za dodržování zásad, pravidel a postupů při zpracování osobních údajů realizovaných v rámci oblasti jejich činnosti a působností daných čl. 8, odst. (2) Statutu Vysoké školy ekonomické v Praze.

Článek 5

Vedoucí jednotlivých součástí

- (1) Děkani jednotlivých fakult VŠE odpovídají rektorovi za dodržování zásad, pravidel a postupů při zpracování osobních údajů realizovaných zaměstnanci a studenty fakulty VŠE při plnění jejich pracovních či studijních povinností, případně dalšími fyzickými a právníckými osobami, které zpracovávají osobní údaje na základě smlouvy s fakultou VŠE ve věcech jim svěřených ustanovením § 24 zákona, čl. 15 Statutu Vysoké školy ekonomické v Praze, vnitřními předpisy VŠE dle čl. 3 Statutu Vysoké školy ekonomické v Praze a ostatními vnitřními předpisy VŠE.
- (2) Ředitelé dalších součástí VŠE odpovídají rektorovi VŠE za dodržování zásad, pravidel a postupů při zpracování osobních údajů realizovaných zaměstnanci další součástí VŠE při plnění jejich pracovních povinností, případně dalšími fyzickými a právníckými osobami, které zpracovávají osobní údaje na základě smlouvy s další součástí VŠE ve věcech jim svěřených Statutem Vysoké školy ekonomické v Praze, statutem dané další součástí VŠE, vnitřními předpisy VŠE dle čl. 3 Statutu Vysoké školy ekonomické v Praze a ostatními vnitřními předpisy VŠE.

Článek 6

Garant zpracování osobních údajů

- (1) Za účelem zajištění ochrany osobních údajů a jejich zpracování v souladu s nařízením a zákonem o ochraně osobních údajů jsou ustanoveni pro jednotlivé případy či oblasti zpracování garanti zpracování osobních údajů (dále jen „garant“).
- (2) Garant je osoba odpovědná za dodržování zásad, pravidel a postupů (uvedených v této směrnici, nařízení a dalších relevantních obecně závazných právních předpisech) při zpracování osobních údajů realizovaných v jemu svěřeném případě/oblasti/činnosti včetně zajištění vypořádání práv subjektů údajů. Garant odpovídá za uvedené činnosti od data svého ustanovení až po ukončení činnosti, a to včetně zajištění bezpečné archivace dat.
- (3) Garant provádí v jemu svěřeném případě/oblasti posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů podle čl. 35 nařízení. Za tímto účelem si vyžádá posudek pověřence pro ochranu osobních údajů.
- (4) Garanty pro jednotlivé případy/oblasti stanoví:
 - a) rektor pro případy zpracování osobních údajů, které zasahují celou VŠE;
 - b) vedoucí pracovníci součástí dle Organizační struktury VŠE ve smyslu čl. 14 Statutu Vysoké školy ekonomické v Praze v případě zpracování osobní údajů v působnosti dané součástí;
 - c) dohodou určený vedoucí součástí tam, kde se jedná o zpracování zasahující více konkrétních součástí. V případě, kdy by nedošlo ke stanovení garanta, stanoví garanta rektor.
- (5) V případech již existujících systémů zpracování osobních údajů bude garant ustanoven osobami uvedenými v čl. 4 a 5 nejpozději do deseti dnů po nabytí účinnosti této směrnice. U nových systémů bude garant určen před zahájením zpracování osobních údajů.
- (6) Osoby uvedené v odstavci 4 o ustanovení garanta neprodleně informují pověřence pro ochranu osobních údajů.
- (7) Není-li pro nějaký případ či oblast zpracování dat garant stanoven, odpovídají za plnění úkolů garanta věcně příslušné osoby uvedené v čl. 4 a 5.

Článek 7

Další oprávněné osoby

- (1) S osobními údaji mohou přicházet do styku:
 - a) osoby, které jsou podle charakteristiky příslušného zpracování údajů dle čl. 13 pověřeny vkládáním a likvidací osobních údajů;
 - b) osoby, které jsou nadřizeny osobám uvedeným v písm. a) po organizační či metodické linii;
 - c) osoby, které zabezpečují organizační, funkční a technickou správu příslušného zpracování údajů (zpravidla analytici, programátoři, správci systémů, sítí, referenti na jednotlivých útvarech apod.);
 - d) další osoby, které jsou podle charakteristiky příslušného zpracování údajů dle čl. 13 pověřeny, aby tyto osobní údaje využívaly k plnění svých úkolů.
- (2) Další oprávněné osoby jsou ustanoveny garantem zpracování. Podmínkou přijetí či přeřazení osob na místa s pověřením dle odstavce 1 je jejich předchozí průkazné seznámení s touto směrnicí, nařízením a dalšími relevantními obecně závaznými právními předpisy.
- (3) Osoby uvedené v odstavci 1 a odstavci 2 jsou povinny zpracovávat osobní údaje vždy jen v rozsahu podmínek realizace/typového řešení příslušného zpracování údajů dle čl. 6.
- (4) Osoby uvedené v odstavci 1 a odstavci 2 jsou povinny zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po ukončení pracovního poměru, studia nebo výkonu příslušných prací.

Článek 8

Závěrečné a jiné práce

V případech, kdy by u závěrečných kvalifikačních prací (bakalářské, magisterské, disertační, habilitační nebo jiné) byly zpracovávány osobní údaje, je školitel povinen seznámit autora s povinnostmi dle nařízení a směrnice a zajistit případné další kroky v souladu se směrnicí. Obecně se tato povinnost týká i jiných případů, kdy student zpracovává v rámci svých povinností projekt či realizuje jinou činnost, v rámci níž jsou zpracovávány osobní údaje. Další podrobnosti může stanovit vnitřní předpis VŠE, případně fakulty.

Část třetí

Pověřenec pro ochranu osobních údajů

Článek 9

Jmenování pověřence pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů na VŠE (dále jen „pověřenec“) je jmenován rektorem na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany osobních údajů a schopnosti plnit úkoly uvedené v čl. 11. Rektor jej může také odvolat.

Článek 10

Postavení pověřence

- (1) Pověřenec je zaměstnancem VŠE a je přímo podřízen rektorovi.
- (2) Pověřenec je zapojen do veškerých procesů a záležitostí souvisejících s ochranou a zpracováním osobních údajů na VŠE.

- (3) Pověřenec je ze strany VŠE podporován v udržování svých odborných znalostí a je mu umožněn přístup k osobním údajům, operacím zpracování a k veškerým zdrojům potřebným pro plnění úkolů, uvedených čl. 11.
- (4) Pověřenci nejsou ze strany VŠE udělovány žádné konkrétní pokyny, týkající se naplňování jeho povinností pověřence. Může mu však být rektorem zadáno i plnění jiných úkolů a povinností. Žádný z těchto úkolů či povinností však nesmí vést ke střetu zájmů s výkonem funkce pověřence.
- (5) Pověřenec je v souvislosti s výkonem svých úkolů vázán mlčenlivostí. Povinnost mlčenlivosti trvá i po skončení pracovního poměru s VŠE.
- (6) Údaje o pověřenci včetně kontaktu na něj jsou uvedeny ve veřejné části internetových stránek VŠE.

Článek 11

Úkoly pověřence

- (1) Pověřenec vykonává zejména tyto úkoly:
 - a) poskytuje informace a poradenství studentům a zaměstnancům VŠE, kteří provádějí zpracování osobních údajů, o jejich povinnostech podle této směrnice, nařízení a dalších obecně závazných právních předpisů v oblasti ochrany osobních údajů;
 - b) monitoruje soulad s touto směrnicí, nařízením, dalšími obecně závaznými právními předpisy v oblasti ochrany osobních údajů a s koncepcemi VŠE v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;
 - c) dohlíží nad realizací ochrany a zpracování osobních údajů,
 - d) poskytuje poradenství a odbornou pomoc na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitoruje jeho uplatňování podle čl. 35 nařízení;
 - e) po předchozí konzultaci s osobami uvedenými v čl. 4 a 5 ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu (čl. 33 nařízení) a oznamování případů porušení ochrany osobních údajů subjektu údajů (čl. 34 nařízení).
 - f) spolupracuje a komunikuje s dozorovým úřadem;
 - g) působí jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování osobních údajů, včetně předchozí konzultace podle článku 36 nařízení, a případně vede konzultace v jakékoli jiné věci;
 - h) přijímá od garantů dle čl. 6, odst. 1, a osob dle 6, odst. 4, návrhy na zahájení nového, resp. změnu dosavadního zpracování osobních údajů a zaujímá k takovýmto návrhům stanoviska;
 - i) komunikuje se subjekty údajů, kteří se na něj mohou obracet ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv dle této směrnice a nařízení;
 - j) plní další úkoly vyplývající pro jeho pozici z nařízení, zákona či jiných obecně závazných právních předpisů, či vyplývajících z této směrnice a ostatních předpisů VŠE.
- (2) Pověřenec dohlíží na fungování registrů zpracování osobních údajů VŠE uvedené v čl. 13.
- (3) Pověřenec bere při plnění svých úkolů patřičný ohled na riziko spojené s činnostmi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování.

Článek 12

Působnost pověřence na VŠE

- (1) Dozví-li se pověřenec, že hrozí porušení pravidel na ochranu osobních údajů vyplývajících z nařízení, zákona či této směrnice nebo je-li porušení zjištěno, je povinen na to upozornit garanta a písemně doporučit odstranění závadného či rizikového stavu. Garant je povinen v přiměřené lhůtě projednat s pověřencem stav, a pokud se se zjištěním pověřence ztotožnil, zdržet se dalšího závadného či rizikového chování. Garant je rovněž povinen přijmout veškerá opatření k tomu, aby se situace neopakovala. Nesouhlasí-li garant s doporučením pověřence, tak pověřenci písemně zdůvodní vytýkané chování a uvede důvody, proč se domnívá, že nedošlo, či nehrozí, že by mohlo dojít k porušení pravidel uvedených v první větě. V takovém případě pověřenec oznámí tuto skutečnost věcně příslušným osobám uvedeným v čl. 4 a 5 a postoupí jim celou dokumentaci.
- (2) Hrozí-li porušení pravidel na ochranu osobních údajů vyplývajících z nařízení, zákona či této směrnice, nebo je-li porušení zjištěno a pro daný případ/oblast /činnost zpracování nebyl stanoven garant, je pověřenec povinen na to písemně upozornit věcně příslušné osoby uvedené v čl. 4 a 5.
- (3) Pověřenec je povinen dát podnět k přijetí obecných či individuálních opatření v oblasti ochrany osobních údajů osobám uvedeným v čl. 4 a 5 vždy, když:
 - a) na základě svých zjištění dle odstavce 1 zjistí hrozbu porušení či porušení pravidel;
 - b) to bude vhodné v návaznosti na zobecňování praxe v oblasti ochrany osobních údajů.
- (4) Ustanoveními odstavců 1 až 3 není dotčena povinnost pověřence po předchozí konzultaci s osobami uvedenými v čl. 4 a 5 ohlásit porušení zabezpečení osobních údajů dozorovému úřadu a subjektu údajů dle čl. 11 odst. 1 písm. e).

Část čtvrtá

Registr zpracování osobních údajů VŠE

Článek 13

Registrace a evidence zpracování osobních údajů

- (1) Za účelem dosažení přehledu o zpracování osobních údajů na VŠE se zřizuje registr činností zpracování osobních údajů na VŠE (dále jen „registr“). Provozem tohoto registru je pověřeno Centrum informatiky Vysoké školy ekonomické v Praze (dále jen „CI“). Odpovědným za provoz registru je ředitel CI. Pracoviště a funkční místa osob zabezpečujících provoz systému stanoví ředitel CI.
- (2) Součástí VŠE, které zpracovávají, chtějí zpracovávat osobní údaje chráněné touto směrnicí, resp. chtějí změnit dosavadní způsob zpracování osobních údajů, oznámí tuto skutečnost pověřenci prostřednictvím registru.
- (3) Oznámení dle odstavce 2 musí obsahovat úplnou charakteristiku příslušného zpracování osobních údajů ve formátu stanoveném provozovatelem registru.
- (4) Garant si vždy vyžádá od pověřence předchozí stanovisko k postupu realizace a nastavení typového řešení ochrany osobních údajů zde zpracovávaných.
- (5) Garant dle čl. 6, odst. 1, nebo osoba dle 6, odst. 4, má právo zahájit nové, resp. změnit, dosavadní zpracování osobních údajů, až poté, kdy od pověřence obdrží oficiální stanovisko na základě výsledku oznámení. Je-li stanovisko záporné je celá věc konzultována s osobami uvedenými v čl. 4 a 5.

Část pátá

Zásady zpracování osobních údajů

Článek 14

Zásady zpracování osobních údajů

- (1) Zásady zpracování osobních údajů jsou uvedeny v kapitole 2 nařízení. V souladu s ním musí být osobní údaje:
 - a) ve vztahu k subjektu údajů zpracovány zákonným, korektním a transparentním způsobem;
 - b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný;
 - c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovány;
 - d) přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny;
 - e) uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány;
 - f) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí technických a organizačních opatření, které VŠE přijala, před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.
- (2) Za dodržování zásad dle odstavce 1 odpovídají osoby uvedené v části druhé této směrnice a musí být rovněž schopny toto dodržení souladu doložit.

Článek 15

Zákonnost zpracování

- (1) V souladu s čl. 6 nařízení je zpracování zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:
 - a) Zpracování je v souladu s platnými obecně závaznými právními předpisy nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
 - b) zpracování je v souladu s platnými obecně závaznými právními předpisy nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
 - c) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
 - d) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě;
 - e) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
 - f) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů (Podmínky vyjádření souhlasu jsou podrobně uvedeny v čl. 7 a 8 nařízení).
- (2) Odstavec 1 písm. f) se netýká zpracování osobních údajů prováděného VŠE v případech, kdy VŠE vystupuje jako orgán veřejné moci ve věcech jí svěřených zákonem.
- (3) Pokud zpracování pro jiný účel, než pro který byly osobní údaje shromážděny, není založeno na souhlasu subjektu údajů nebo na platných obecně závazných právních předpisech, zohlední garant v zájmu zjištění toho, zda je zpracování pro jiný účel slučitelné s účely, pro něž byly osobní údaje původně shromážděny, mimo jiné:

- a) jakoukoli vazbu mezi účely, kvůli nimž byly osobní údaje shromážděny, a účely zamýšleného dalšího zpracování;
- b) okolnosti, za nichž byly osobní údaje shromážděny, zejména pokud jde o vztah mezi subjekty údajů a VŠE;
- c) povahu osobních údajů, zejména zda jsou zpracovávány zvláštní kategorie osobních údajů podle čl. 9 nařízení nebo osobní údaje týkající se rozsudků v trestních věcech a trestných činů podle čl. 10 nařízení;
- d) možné důsledky zamýšleného dalšího zpracování pro subjekty údajů;
- e) existenci vhodných záruk, mezi něž může patřit šifrování nebo pseudonymizace.

Článek 16

Zpracování zvláštních kategorií osobních údajů

- (1) Je zakázáno zpracování osobních údajů, které vypovídají 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 v případech, na které se nevztahuje odstavec 2 a 3.
- (2) Výjimky ze zákazu zpracování osobních údajů dle odstavce 1 jsou dány čl. 9 nařízení.
- (3) Výjimkami ze zákazu v odstavci 1 jsou také údaje o:
 - a) zdravotním stavu v osobních evidencích zaměstnanců a studentů za předpokladu, že tyto údaje byly subjektem údajů do zmíněné evidence dobrovolně předány a jsou vedeny v jeho prospěch (např. mají vliv na přijetí ke studiu, poskytování služeb osobám se specifickými nároky, ubytování v kolejích nebo jeho daňové povinnosti či jiných zákonných dávek);
 - b) členství v odborových organizacích působící na VŠE uvedené v osobních a mzdových evidencích zaměstnanců za předpokladu, že byly subjektem údajů do zmíněné evidence dobrovolně předány a slouží pro placení členských příspěvků či jiných dávek, včetně účtování o těchto platbách,
 - c) biometrické údaje, které umožňují přímou identifikaci nebo autentizaci subjektu údajů,
 - d) zvláštní kategorie osobních údajů zpracovávané pro účely projektů/výzkumu a publikační činnosti.
- (4) Zpracování údajů definovaných v odstavci 1 může probíhat pouze na základě výslovného souhlasu subjektu údajů. Tento souhlas musí být dán písemně, podepsán subjektem údajů a musí z něho být zřejmé, jakých údajů se týká, k jakému účelu, na jaké období a kdo jej poskytuje. Subjekt údajů svým podpisem také potvrzuje, že byl předem poučen o svých právech. Oprávněné osoby, které jsou podle charakteristiky příslušného zpracování dat dle čl. 6 určeny ke vkládání a likvidaci uvedených údajů, jsou povinny být schopny existenci tohoto souhlasu doložit po celou dobu jejich zpracování.
- (5) V případě dalšího zpracování pro účely vědeckého, či historického výzkumu, nebo statistické účely se nevyžaduje souhlas subjektů údajů dle bodu (4). V takovém případě zpracování podléhá vhodným zárukám práv a svobod subjektu údajů zavedením technických a organizačních opatření, které přijala VŠE. Současně musí být zajištěna zásada minimalizace údajů.
- (6) Zpracování údajů podle odstavce 3 písm. c) může být používáno pouze tehdy, pokud paralelně existuje možnost dosáhnout daného účelu užitím jiných identifikačních nebo autentizačních prostředků, které nebudou na biometrických údajích závislé, a subjekt údajů bude mít možnost volby mezi nimi.
- (7) Zpracování osobních údajů, které nevyžaduje identifikaci subjektu údajů, upravuje čl. 11 nařízení.

Část šestá Subjekt údajů

Článek 17

Informace poskytované subjektu údajů

- (1) VŠE v roli správce poskytuje subjektu údajů v souladu s čl. 12 nařízení stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v čl. 13 a 14 nařízení a učiní veškerá sdělení podle čl. 15 až 22 a 34 nařízení o zpracování. Informace je poskytována v elektronické formě na webových stránkách VŠE a v informačních systémech VŠE.
- (2) Subjekty údajů se mohou obracet ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv dle této směrnice a nařízení na pověřence.

Článek 18

Práva subjektu údajů

Právo subjektu údajů na:

- a) přístup k osobním údajům upravuje čl. 15 nařízení;
- b) opravu upravuje čl. 16 a 19 nařízení;
- c) výmaz upravuje čl. 17 a 19 nařízení;
- d) omezení zpracování upravuje čl. 18 a 19 nařízení;
- e) přenositelnost údajů upravuje čl. 20 nařízení;
- f) vznesení námítky a automatizované individuální rozhodování upravuje čl. 21 a 22 nařízení.

Část sedmá

Zveřejňování a zabezpečení osobních údajů a jejich poskytování třetím stranám

Článek 19

Zveřejňování osobních údajů

- (1) Zveřejněním osobních údajů se rozumí jejich zpřístupnění konkrétně neurčeným osobám či skupinám osob, zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu (např. ve veřejné části internetových stránek VŠE).
- (2) Osobní údaje chráněné podle této směrnice lze zveřejňovat nejvýše v rozsahu:
 - a) jméno;
 - b) příjmení;
 - c) tituly;
 - d) fotografie;
 - e) pracovní zařazení na VŠE;
 - f) zařazení v organizační struktuře VŠE;
 - g) zastávané funkce na VŠE;
 - h) kontaktní údaje v souvislosti s VŠE (adresy pracovišť, telefonní a faxová čísla, e-mailové adresy);

- i) nezbytné identifikace a specifikace v modulech informačního systému (osobní číslo, číslo pracovního vztahu, druh pracovního vztahu, uživatelské jméno do sítě VŠE, příznak hlavního pracovního vztahu, příznak mimo evidenčního stavu, kmenová zakázka);
- j) informace o publikační a výzkumné činnosti;
- k) průběh akademické kvalifikace;
- l) podíl na jednotlivých formách tvůrčí činnosti VŠE;
- m) informace o vydaných publikacích;
- n) výuka uskutečňovaná na VŠE;
- o) akademické osobní www-stránky (tj. WWW-stránky zaměstnanců a studentů VŠE související s jejich akademickým anebo studijním působením na VŠE),
- p) případně další údaje, které si zde subjekt o sobě zveřejnil sám.

Subjekt údajů má právo zvolit si konkrétní rozsah zveřejňovaných údajů uvedených pod písm. d), i), a n), případně tyto údaje nezveřejnit vůbec.

- (3) Údaje uvedené v odstavci 2 lze zveřejňovat pouze o subjektech údajů, jež:
 - a) jsou zaměstnanci VŠE nebo byli zaměstnanci VŠE v době vzniku údaje, který má přetrvávající relevanci;
 - b) jsou zaměstnanci či studenti VŠE a aktuálně působí v samosprávných akademických či poradních orgánech VŠE;
- (4) V případě akademických funkcionářů a vedoucích součástí VŠE bude zveřejňování osobních údajů upravováno individuálně.
- (5) V případě akademických funkcionářů a osob aktuálně působících v samosprávných akademických či poradních orgánech VŠE, které nejsou v pracovním poměru k VŠE, bude zveřejňování osobních údajů upravováno individuálně.

Článek 20

Poskytování osobních údajů třetím stranám

- (1) Poskytování osobních údajů třetím stranám mimo VŠE se řídí touto směrnicí, nařízením a platnými obecně závaznými právními předpisy.
- (2) O každém poskytnutí osobních údajů třetí straně mimo VŠE musí být garantem dle čl. 6, odst. 1, nebo osobou dle 6, odst. 4, předem písemně listinnou nebo elektronickou formou informován pověřenec se sdělením rozsahu poskytnutých údajů, účelu poskytnutí a identifikací třetí strany.
- (3) Za dodržování správného postupu při poskytování osobních údajů třetím osobám mimo VŠE v souladu s touto směrnicí, nařízením a platnými obecně závaznými právními předpisy je odpovědný garant ustanovený pro daný případ/oblast zpracování. Není-li pro daný případ/oblast zpracování ustanoven garant, odpovídají za dodržování správného postupu při poskytování osobních údajů třetím osobám mimo VŠE věcně příslušné osoby uvedené v čl. 4 a 5.

Článek 21

Zabezpečení osobních údajů

- (1) Písemnosti a mobilní/externí/přenosné technické nosiče informací, jimiž disponuje VŠE a které obsahují osobní údaje chráněné podle této směrnice, musí být uchovávány pouze v uzamkatelných skříních na pracovištích VŠE, případně na jiných bezpečných místech určených charakteristikou příslušného zpracování údajů dle čl. 11, nebo zabezpečeny šifrováním.
- (2) Pokud jsou zpracovávány osobní údaje, které se bezprostředně vztahují k činnostem vykonávaným na VŠE (např. docházkové archy, odpovědní listy, testy, poznámkové bloky, prezenční listiny), postupuje se při jejich zabezpečení obvyklým způsobem tak,

aby se předcházelo riziku zneužití osobních údajů. Další povinnosti stanovené v tomto článku se na zpracování takových osobních údajů použijí pouze v takovém rozsahu, v jakém to odpovídá jejich povaze a okolnostem jejich obvyklého zpracovávání.

- (3) Počítače a další technické prostředky, na nichž jsou uložena data obsahující osobní údaje chráněné podle této směrnice, musí být zabezpečeny před volným přístupem neoprávněných osob, zpravidla přístupovými hesly, šifrováním či uzamčením.
- (4) Kopie osobních údajů chráněných podle této směrnice musí být pořizovány na technické nosiče informací podle provozních pravidel stanovených pro jednotlivá zpracování údajů a uchovávány v uzamykatelných skříních na pracovištích VŠE, případně na jiných bezpečných místech určených charakteristikou příslušného zpracování údajů dle čl. 11, nebo zabezpečeny šifrováním.
- (5) V případě, kdy garant či oprávněná osoba zjistí nebo nabude podezření, že by mohlo dojít nebo že došlo k porušení zabezpečení osobních údajů (incident), je povinen to neprodleně oznámit na Helpdesk Centra informatiky. Na Helpdesk mohou hlásit incidenty i další osoby, pokud zjistí či mají podezření na incident týkající zpracování osobních údajů uvedených v čl. 1 odst. 2. Helpdesk zaeviduje a ve spolupráci s oznamujícím popíše incident a předá neprodleně Oddělení bezpečnost a ochrana dat Centra informatiky.

Oznámení incident na Helpdesk dle tohoto předpisu nenahrazuje povinnost oznamování událostí dle jiných předpisů, např. povinnost hlásit bezpečnostní incidenty správci části informačního systému VŠE dle PR 07/2018.

- (6) Oddělení bezpečnost a ochrana dat Centra informatiky doplní v co nejkratší době popis a kategorizaci incidentu s návrhem opatření, která zajistí vyřešení daného incidentu, včetně opatření ke zmírnění možných nepříznivých dopadů. Kategorizaci provede dle následující stupnice:

Incident s nízkým rizikem (I.), který nemá vliv na práva a svobodu subjektu údajů, incident se středním rizikem (II.) s vlivem na omezení práv, nebo svobod subjektu údajů a incident s velmi vysokým rizikem (III.) se zásadním dopadem na svobody a práva subjektu údajů.

Rozdělování do kategorií monitoruje pověřenec. Pověřenec může připravit metodiky pro kategorizaci jednotlivých typů incidentů.

Veškeré incidenty jsou oddělením trvale dokumentovány a archivovány.

Oddělení postoupí neprodleně po doplnění informací incidenty II. a III. kategorie Správci (vedení VŠE).

- (7) V případě incidentu II. kategorie správce (vedení VŠE) po projednání incident ohlašuje pokud možno do 72 hodin ÚOOÚ. V případě incidentu III. kategorie správce ohlašuje incident ÚOOÚ a dotčeným subjektům údajů. Ohlášení provede pověřenec, nebo jiná vedením VŠE zmocněná osoba. Ohlášení musí obsahovat minimálně údaje, které vymezuje čl. 33 odst. 3 nařízení.

Část osmá Závěrečná ustanovení

Článek 22

Přechodná a závěrečná ustanovení

- (1) Součásti VŠE, které zpracovávají osobní údaje chráněné touto směrnicí, oznámí bez zbytečného odkladu tuto skutečnost písemně, v to počítaje i elektronickou formu, pověřenci prostřednictvím registru dle čl. 13 s uvedením pro každou činnost zpracování minimálně následujících údajů:

- a) název činnosti, název jejích složek;
 - b) údaj o pracovišti, jméno a kontaktní údaje garanta;
 - c) popis kategorií subjektů údajů;
 - d) popis kategorií osobních údajů;
 - e) účely zpracování;
 - f) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
 - g) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce nařízení doložení vhodných záruk;
 - h) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;
 - i) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1 nařízení;
 - j) je-li zpracování realizováno externí osobou (zpracovatelem), identifikaci zpracovatele a též smlouvy, na jejímž základě zpracování probíhá;
 - k) právní titul, na jehož základě zpracování probíhá;
 - l) zdroj osobních údajů;
 - m) doporučení garanta, zda je nutno provádět posouzení vlivu operací zpracování na ochranu osobních údajů podle čl. 35 nařízení.
- (2) Tato směrnice ruší příkaz rektorky č. 4/2001 - Aplikace zákona č. 101/200 Sb., v platném znění "o ochraně osobních údajů a o změně některých zákonů" (PR 04/2001).
- (3) Kontrolu dodržování této směrnice vykonává pověřenec.