VÝNOS REKTORA Č. 6/2018

ŘEŠENÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

zpracovatel a věcně odpovědná osoba:	PhDr. Evžen Mrázek, kvestor a PhDr. Jan Michl, pověřenec pro ochranu osobních údajů
schválil:	doc. MgA. Tomáš Vaněk, rektor
schváleno dne:	21. 5. 2018
nabývá účinnosti ode dne:	25. 5. 2018
kontrola aktuálnosti výnosu:	jednou ročně

Článek 1
Úvodní ustanovení

1. Tento interní předpis (dále také „výnos“) upravuje některá práva a povinnosti každého jednotlivého zaměstnance Akademie výtvarných umění v Praze (dále jen „AVU“) vyplývající z pracovněprávního vztahu k AVU nebo s tímto pracovněprávním vztahem související.
2. Tento výnos dále upravuje práva a povinnosti osoby, která má provozní odpovědnost za vyřizování případů porušení (dále také „odpovědná osoba“). Odpovědnou osobou je pověřenec pro ochranu osobních údajů.
3. Tento výnos navazuje na Výnos rektora č. 5/2018 – Ochrana a zpracování osobních údajů.
4. Zaměstnancem se pro účely tohoto výnosu rozumějí zaměstnanci pracující pro AVU v pracovním poměru, jakož i další osoby vykonávající pro AVU činnosti na základě jiných právních titulů, zejména na základě dohody o provedení práce či dohody o pracovní činnosti.
5. Výnos je pro zaměstnance závazný a každý zaměstnanec je povinen jej dodržovat.

Článek 2
Vymezení pojmů

1. Osobními údaji se pro účely tohoto výnosu rozumějí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále též 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. Porušením zabezpečení osobních údajů (dála také „porušení zabezpečení“) se pro účely tohoto výnosu rozumí porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.
3. Porušení zabezpečení je bezpečnostní incident, který má za následek, že AVU není schopna zajistit soulad se zásadami zpracování osobních údajů. Jedná se o případy:

a) porušení důvěrnosti – porušení zabezpečení osobních údajů v případě neoprávněného nebo náhodného poskytnutí nebo zpřístupnění osobních údajů;
b) porušení dostupnosti – porušení zabezpečení osobních údajů v případě náhodné nebo neoprávněné ztráty přístupu nebo zničení osobních údajů. Porušením dostupnosti je vždy incident, při kterém dojde k trvalé ztrátě nebo zničení osobních údajů, a to buď smazáním náhodným, nebo úmyslným, zašifrováním dat, ztrátou dešifrovacího klíče a podobně;
c) porušení integrity – porušení zabezpečení osobních údajů v případě neoprávněného nebo náhodného pozměnění osobních údajů.

4. Porušení zabezpečení může být zjištěno zejména:

- přímo odpovědnou osobou
- na základě upozornění zaměstnance
- na základě upozornění subjektů údajů
- na základě ohlášení zpracovatelů
- na základě upozornění jiných třetích stran
- na základě jiných informací (vč. informací publikovaných v médiích).

Článek 3
Povinnosti všech zaměstnanců

1. Tento výnos vymezuje povinnosti zaměstnanců při porušení zabezpečení osobních údajů, a to dle požadavků, které na AVU klade Nařízení (EU) č. 2016/679 (GDPR).
2. Každý zaměstnanec, který porušení zabezpečení způsobí nebo se o porušení zabezpečení dozví nebo má důvod se domnívat, že k porušení zabezpečení došlo, či hrozí, má povinnost toto nahlásit odpovědné osobě. Při ohlašování porušení zabezpečení se zaměstnanci řídí čl. 5. Pokud se zaměstnanci z jakéhokoli důvodu nepodaří kontaktovat odpovědnou osobu, je povinen nahlásit výše uvedené skutečnosti svému nadřízenému.
3. Každý zaměstnanec má povinnost poskytnout odpovědné osobě součinnost při vyšetřování porušení zabezpečení a při odstranění jeho následků.

Článek 4
Povinnosti odpovědné osoby při porušení zabezpečení

1. Odpovědná osoba má následující povinnosti:

a) povinnost zajistit, aby všichni zpracovatelé osobních údajů byli ve smlouvách s AVU zavázáni ohlásit AVU veškeré případy porušení zabezpečení,

b) povinnost přijímat upozornění od zaměstnanců, zpracovatelů a jiných subjektů o porušení zabezpečení,
c) povinnost jednat na základě prvního upozornění a vyšetřit porušení zabezpečení,
d) v případě, že jsou splněny podmínky dle čl. 7, ohlásit bezodkladné porušení zabezpečení dozorovému úřadu – Úřadu pro ochranu osobních údajů (dále také „ÚOOÚ“) a spolupracovat s ÚOOÚ úřadem při vyšetřování porušení zabezpečení,
e) v případě, že jsou splněny podmínky dle čl. 8, oznámit porušení zabezpečení subjektům údajů,
f) povinnost vést záznamy a dokumentovat veškeré případy porušení zabezpečení, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření.

2. Odpovědná osoba se při plnění povinností uvedených v odst. 1 tohoto článku řídí následujícími ustanoveními výnosu, jakož i postupy uvedenými v příloze č. 1 a příloze č. 2.

Článek 5
Povinnost odpovědné osoby přijímat upozornění o porušení zabezpečení

1. Odpovědná osoba má za účelem přijímání upozornění zřízený e-mail gdpr@avu.cz.
2. Všichni zaměstnanci mohou upozornit na porušení zabezpečení na e-mail uvedený v odst. 1, telefon odpovědné osoby a dále mohou odpovědnou osobu kontaktovat přímo ústně nebo prostřednictvím písemného podání do určené schránky. Zaměstnanci mají povinnost zvolit takový způsob upozornění odpovědné osoby, aby se odpovědná osoba o porušení zabezpečení dozvěděla bezodkladně.

Článek 6
Povinnosti odpovědné osoby při vyšetřování porušení zabezpečení

1. Odpovědná osoba má povinnost prošetřit každé upozornění obdržené dle čl. 5 nebo jiné obdržené upozornění o porušení zabezpečení.
2. Odpovědná osoba pravidelně kontroluje, zda neobdržela ohlášení porušení zabezpečení některým uvedeným způsobem dle čl. 5.
3. Odpovědná osoba může požádat při vyšetřování porušení zabezpečení příslušný útvar AVU, který poskytne odpovědné osobě součinnost.
4. Odpovědná osoba při prošetřování porušení zabezpečení postupuje následujícím způsobem:

a) odpovědná osoba na základě obdržených informací posoudí, zda k porušení zabezpečení skutečně došlo;
b) odpovědná osoba vyhodnotí, o který druh porušení zabezpečení se jedná (viz čl. 2.3);
c) odpovědná osoba vyhodnotí možné důsledky a rizika porušení zabezpečení pro subjekty údajů (např. materiální, či imateriální škoda, krádež identity, podvod apod.), spolu s množstvím údajů, u nichž došlo k porušení zabezpečení;
d) odpovědná osoba vyhodnotí, zda je nutné porušení zabezpečení dle čl. 7 ohlásit ÚOOÚ a dle čl. 8 oznámit subjektům údajů;

e) odpovědná osoba navrhne opatření k řešení daného porušení zabezpečení, včetně vhodných opatření ke zmírnění možných nepříznivých dopadů (např. zprovoznění záložní kopie v případě porušení dostupnosti údajů).
f) odpovědná osoba o porušení informuje rektora a kvestora AVU.

Článek 7

Povinnost ohlásit porušení zabezpečení ÚOOÚ a spolupracovat s ním

1. Na základě provedeného šetření dle čl. 6 odpovědná osoba vyhodnotí, zda je porušení zabezpečení nutno ohlásit ÚOOÚ.
2. Porušení zabezpečení odpovědná osoba ohlásí ÚOOÚ v každém případě, pokud k porušení zabezpečení skutečně došlo, mimo případy kdy:

a) došlo k porušení zabezpečení, které nemá a nemůže mít žádný vliv na subjekty údajů,
b) došlo ke ztrátě zařízení, které je však bezpečně zašifrované a není zde možnost, že by mohlo být zneužito třetí osobou,
c) došlo k porušení zabezpečení, ale osoba, která osobní údaje obdržela, je důvěryhodná, data zaslala zpět či je bezpečně zničila.

3. Při posuzování nutnosti ohlásit porušení zabezpečení ÚOOÚ se odpovědná osoba přiměřeně řídí příklady uvedenými v příloze č. 2.
4. Odpovědná osoba má povinnost ohlásit porušení zabezpečení ÚOOÚ bez zbytečného odkladu po tom, co je potvrzeno, že k porušení zabezpečení došlo a bylo zjištěno, že toto porušení vyžaduje ohlášení ÚOOÚ. Odpovědná osoba porušení zabezpečení ohlásí ÚOOÚ nejpozději do 72 hodin od okamžiku jeho zjištění.
5. V případě, že odpovědná osoba neohlásí porušení zabezpečení ve stanovené lhůtě, bude ÚOOÚ informovat bezodkladně a kromě informací uvedených v následujícím odstavci uvede odpovědná osoba v ohlášení také důvody zpoždění při ohlášení a tyto důvody doplní dokumentací prokazující důvody zpoždění.
6. Při ohlašování porušení zabezpečení ÚOOÚ odpovědná osoba uvede:

a) popis povahy daného případu porušení zabezpečení včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
b) své jméno a kontaktní údaje;
c) popis pravděpodobných důsledků porušení zabezpečení;
d) popis opatření, která AVU přijala nebo navrhla s cílem vyřešit dané porušení zabezpečení, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

7. Nemůže-li odpovědná osoba poskytnout všechny údaje uvedené v odst. 6 tohoto článku současně, poskytne je ÚOOÚ následně bez dalšího zbytečného odkladu.

Článek 8

Povinnost oznámit porušení zabezpečení subjektům údajů

1. Pokud je pravděpodobné, že určitý případ porušení zabezpečení bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí odpovědná osoba toto porušení zabezpečení bez zbytečného odkladu subjektu údajů.

2. V oznámení subjektu údajů podle odst. 1 tohoto článku použije odpovědná osoba jasných a jednoduchých jazykových prostředků, popíše povahu porušení zabezpečení a uvede v něm přinejmenším informace a opatření uvedená v čl. 6 odst. 5 písm. b), c) a d) a je-li to možné, také kroky, které mohou subjekty údajů učinit pro vlastní ochranu.
3. Oznámení subjektu údajů uvedené v odst. 1 se nevyžaduje, je-li splněna kterákoli z těchto podmínek:

a) AVU zavedla náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení. Jde zejména o taková opatření, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup (např. šifrování);
b) AVU přijala následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů podle odst. 1 tohoto článku se již pravděpodobně neprojeví;
c) oznámení by vyžadovalo nepřiměřené úsilí, v takovém případě odpovědná osoba zajistí, že subjekty údajů budou informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Článek 9

Povinnost vést záznamy a dokumentovat případy porušení zabezpečení

1. Odpovědná osoba dokumentuje všechny případy porušení zabezpečení, které byly ohlášeny.
2. Odpovědná osoba dokumentaci vede v takové podobě, aby z ní byl zřejmý přinejmenším:

- popis porušení zabezpečení (popis toho, co se stalo),
- datum, kdy bylo porušení zabezpečení zjištěno,
- zdroj zjištění porušení zabezpečení,
- osobní údaje dotčené porušením zabezpečení,
- zjištěné příčiny porušení zabezpečení,
- důsledky porušení zabezpečení,
- nápravná opatření přijatá AVU,
- pokud bylo porušení zabezpečení ohlášeno ÚOOÚ, či oznámeno subjektům údajů, také informace o tomto ohlášení a oznámení.

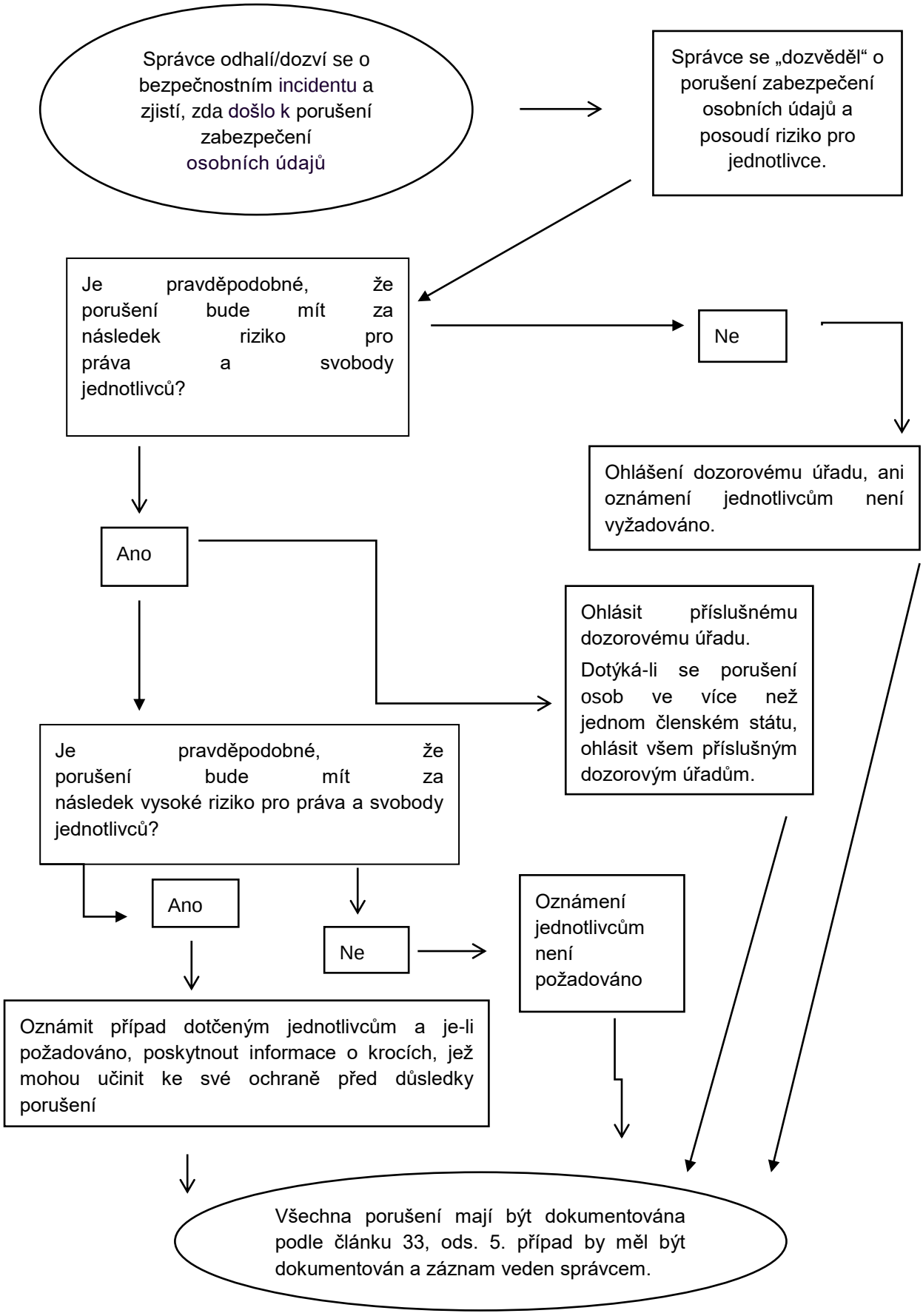
3. Pro vedení dokumentace odpovědná osoba využívá přílohy č. 3.

V Praze dne 21. května 2018

doc. MgA. Tomáš Vaněk
rektor AVU

Příloha č. 1

Diagram znázorňující požadavky na ohlášení Porušení zabezpečení



Příloha č. 2

Příklady Porušení zabezpečení a postupů

Odpovědná osoba se při ohlašování Porušení zabezpečení přiměřeně řídí postupy uvedenými v této příloze.

Příklad	Ohlásit dozorovému úřadu?	Oznámit subjektu údajů?	Poznámky/doporučení
I. Správce uložil záložní kopii archivu osobních údajů v zašifrované podobě na CD. Toto CD bylo odcizeno během vloupání.	Ne.	Ne.	Pokud jsou data zašifrovaná pomocí algoritmu na úrovni doby, data jsou zálohovaná a jedinečný klíč nebyl prozrazen, pak nemusí jít o hlásitelný případ. Je-li však později prolomen, ohlášení je nutné.
II. Osobní údaje jednotlivců jsou vyfiltrovány z bezpečné webové stránky provozované správcem během kybernetického útoku. Správce má zákazníky jen v jednom členském státě.	Ano, ohlásit případ příslušnému dozorovému úřadu je třeba, pokud hrozí možné důsledky pro jednotlivce.	Ano, oznámení jednotlivcům je nutné v závislosti na povaze dotčených osobních údajů a v případě vysoké závažnosti případných dopadů na jednotlivce.	Není-li riziko vysoké, doporučujeme, aby správce informoval subjekt údajů podle okolností případu. Oznámení například nemusí být vyžadováno, pokud jde o porušení důvěrnosti při zasílání novinek týkajících se televizní estrády, avšak může být nutné, pokud newsletter (zpravodaj) může vést k rozpoznání politických názorů subjektu údajů.
III. Krátký, jen několikaminutový výpadek proudu ve správcově call centru způsobí, že se s ním zákazníci nemohou spojit a získat přístup ke svým záznamům.	Ne.	Ne.	Nejedná se o porušení zabezpečení osobních údajů, které by bylo nutno ohlašovat, ale pořád je to incident, který je potřeba dokumentovat podle článku 33, odst. 5. Správce by měl vést náležité záznamy.
Příklad	**Ohlásit dozorovému úřadu?**	**Oznámit subjektu údajů?**	**Poznámky/doporučení**
IV. Správce utrpí útok ransomwarem (vyděračským softwarem), čímž dojde k zašifrování všech jeho dat. K dispozici nejsou žádné zálohy a data nelze obnovit. Během šetření se přijde na to, že jedinou schopností ransomwaru bylo zašifrování údajů, a že systém neobsahoval žádný	Ano, ohlásit případ příslušnému dozorovému úřadu je nutné, pokud hrozí možné důsledky pro jednotlivce, neboť se jedná o ztrátu dostupnosti.	Ano, nutnost oznámit případ jednotlivcům bude záviset na povaze dotčených osobních údajů a na možných dopadech ztráty dostupnosti, jakož i na dalších pravděpodobných důsledcích.	Pokud by existovala záložní kopie a data by bylo možno v přijatelném čase obnovit, pak nebude třeba ohlašovat dozorovému úřadu ani oznamovat jednotlivci, protože by se nejednalo o trvalou ztrátu dostupnosti nebo důvěrnosti. Dozorový úřad však může zvážit provedení šetření k posouzení souladu s obecnějšími

jiný škodlivý software (malware).			požadavky stanovenými v článku 32.
V. Jednotlivec zavolá call centrum banky, aby ohlásil případ porušení zabezpečení. Volající totiž obdržel měsíční výpis z účtu někoho jiného. Správce zahájí krátké šetření (tj. ukončené např. během 24 hodin) a s dostatečnou jistotou zjistí, že došlo k porušení zabezpečení osobních údajů a zda se jedná o systémovou chybu, takže i další jednotlivci byli nebo by mohli být postiženi.	Ano.	Potřeba je oznámit to pouze dotčeným jednotlivcům za předpokladu, že existuje vysoké riziko a je jasné, že nikdo další nebyl zasažen.	Pokud bude dalším šetřením zjištěno, že bylo postiženo více osob, ohlášení dozorovému úřadu musí být učiněno a správce také musí záležitost dodatečně oznámit příslušným dalším jednotlivcům, existuje-li vysoké riziko.
Příklad	**Ohlásit dozorovému úřadu?**	**Oznámit subjektu údajů?**	**Poznámky/doporučení**
VI. Nadnárodní online tržiště se stane obětí kybernetického útoku, přičemž útočník na internetu zveřejnění uživatelská jména, hesla a nákupní historii.	Ano, ohlášení dozorovému úřadu je nutné, týká-li se případ přeshraničního zpracování.	Ano, protože by mohlo mít za následek vysoké riziko.	Správce by měl podniknout kroky, např. vynutit resetování hesel u dotčených účtů a učinit i další kroky ke snížení rizika.
VII. Webhostingová firma (zpracovatel) zjistí chybu v kódu, který sleduje uživatelská oprávnění. Následkem této chyby může jakýkoliv uživatel vstoupit do účtu kteréhokoliv jiného uživatele.	Webhostingová firma, jsouce v postavení zpracovatele, musí věc bezodkladně ohlásit dotčeným klientům (správcům). Za předpokladu, že webhostingová firma provedla vlastní šetření, měli by mít dotčení správci důvodnou jistotu, zda každý z nich byl zasažen porušením a tedy se o případu „dozvěděl“ ve chvíli, kdy byl informován webhostingovou firmou (zpracovatelem). Správce pak musí případ ohlásit dozorovému úřadu.	Pokud není pravděpodobné, že by se mohlo objevit vysoké riziko pro jednotlivce, není potřeba jim případ oznámit.	Webhostingová firma (zpracovatel) musí vzít v úvahu veškeré další oznamovací povinnosti (např. podle Směrnice NIS). Neexistuje-li důkaz, že u konkrétního správce nebylo daného zranitelného místa zneužito, pak nemuselo dojít k porušení, které by bylo třeba ohlásit, ale mělo by být dokumentováno nebo být bráno jako záležitost, která je v nesouladu s článkem 32.
VIII. Zdravotní záznamy v nemocnici nejsou dostupné po dobu 30 hodin v důsledku kybernetického útoku.	Ano, nemocnice je povinna to ohlásit, vzhledem k vysokému riziku pro pacientovo zdraví a soukromí.	Ano, je třeba provést oznámení dotčeným jednotlivcům.	
Příklad	**Ohlásit dozorovému úřadu?**	**Oznámit subjektu údajů?**	**Poznámky/doporučení**
IX. Osobní údaje 5000 studentů byly omylem	Ano, ohlásit případ dozorovému úřadu je	Ano, nutnost oznámení jednotlivcům bude záviset	

zaslány na nesprávný adresář čítající 1000 a více příjemců.	nutné.	na rozsahu a druhu dotčených osobních údajů a na závažnosti možných důsledků.	
X. E-mail v rámci přímého marketingu byl odeslán příjemcům v kolonce „komu“ nebo „kopie“, čímž každý z příjemců mohl zjistit elektronickou adresu ostatních příjemců.	Ano, ohlášení dozorovému úřadu může být povinné, jestliže byl postižen velký počet jednotlivců, došlo k odhalení citlivých údajů (např. adresář psychoterapeuta) nebo pokud existují jiné faktory představující vysoké riziko (např. zpráva obsahuje iniciační hesla).	Ano, nutnost oznámení jednotlivcům bude záviset na rozsahu a druhu dotčených osobních údajů a na závažnosti možných důsledků.	Ohlášení nemusí být nutné, pokud nedošlo k odhalení citlivých údajů a pokud došlo k odkrytí jen menšího počtu e-mailových adres.

Zdroj: Vodítka k ohlašování případů porušení zabezpečení osobních údajů podle Nařízení 2016/679 vytvořená Pracovní skupinou WP 29, schválená 3. října 2017

Příloha č. 3

Vzor Dokumentace záznamů všech ohlášených případů Porušení zabezpečení

A) Popis Porušení zabezpečení:

B) Datum zjištění Porušení zabezpečení:

C) Zdroj zjištění Porušení zabezpečení:

D) Zjištění Odpovědné osoby.

Bylo zjištěno, že k Porušení zabezpečení skutečně došlo?

Ano ☐ Ne ☐

E) Osobní údaje dotčené Porušením zabezpečení:

F) Zjištěné příčiny Porušení zabezpečení:

G) Důsledky Porušení zabezpečení:

H) Přijatá **nápravná opatření**:

CH) Ohlášení Porušení zabezpečení ÚOOÚ (datum a obsah)

I) Oznámení Porušení zabezpečení subjektům údajů (datum a obsah)

J) Informace vedení