

ŠKOLENÍ

GDPR pro školy a školská zařízení

Školitelé:

Bc. Radek Kubíček, MBA

Bezpečností auditor

pověřenec pro ochranu osobních údajů



2K CONSULTING

AUTORSKÁ PRÁVA

Organizace nebo fyzická osoba, která tuto prezentaci získala, není oprávněna bez předchozího písemného souhlasu společnosti 2K Consulting s.r.o. půjčovat, kopírovat, upravovat, dále prodávat ani jiným způsobem šířit žádný z poskytnutých materiálů či jakýkoliv obsah semináře. Prezentace je určena pouze pro interní potřebu organizace nebo fyzické osoby.

Představení lektora

Bc. Radek Kubíček, MBA

Předseda komise pro školství a spolky v ČR, člen pracovní skupiny pro Evropský sbor pro ochranu osobních údajů...

Ocenění : Pověřenec roku 2020 za oblast veřejného sektoru.



PROFESIONÁLNÍ POMOC V OBLASTI BEZPEČNOSTI

ZAPOJTE SE DO PROJEKTU A ZÍSKEJTE
PRESTIŽNÍ OCENĚNÍ



Přidejte se mezi nás

<https://www.facebook.com/2Kconsultingsro>

Zahájení školení



LEGISLATIVA

CO JE TO GDPR?

- **GDPR (z angl. General Data Protection Regulation)**

= Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů

- jedná se o evropský předpis, jež vstoupil v platnost

- 25. května 2018**

- je **PŘÍMO ÚČINNÝ** – pro všechny členské státy EU

KDE NAJÍT INFORMACE KE GDPR?

GDPR V PLNÉM ZNĚNÍ K DISPOZICI ZDE
(klikněte)

Další informace o GDPR na stránkách ÚOOÚ
(klikněte zde)

JAK SE GDPR PROJEVUJE GDPR V ČESKÉ LEGISLATIVĚ?

- ***Zákon č. 110/2019 Sb. o zpracování osobních údajů***, který ruší zákon č. 101/2000 Sb. o ochraně osobních údajů
- ***Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů***



V nově podepisovaných dokumentech už nesmí být zák. č. 101/2000 Sb. uváděn!!!

ZÁKLADNÍ POJMY

ZÁKLADNÍ POJMY – OSOBNÍ ÚDAJ

- **osobní údaj chápeme jako veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“)**

➤ Jméno a příjmení	➤ IP adresa	➤ Výše příjmů
➤ Pohlaví	➤ Datum narození	➤ Fotografie
➤ Věk	➤ Rodinný stav	➤ Audiozáznam
➤ Telefonní číslo	➤ Údaje o manželovi/ manželce	➤ Videozáznam
➤ E-mailová adresa	➤ Podpis	➤ Koníčky
➤ Adresa bydliště	➤ Číslo občanského průkazu	➤ Občanství

Ve městě nebo větší škole křestní jméno jako Tereza nebo Jan nebudou bez dalšího chápány jako osobní údaj, protože dětí tohoto jména je obvykle více. V malé obci nebo malé škole může např. Viktorie být jediná a je tedy i křestní jméno chápáno jako osobní údaj (protože už podle křestního jména je jednoznačně identifikovatelná). Vždy je potřeba si uvědomit kontext nebo situaci. Čím více osobních údajů o jednom subjektu údajů máme k dispozici a uloženo na jednom místě, o to více je nutné ochraně těchto údajů věnovat pozornost.

ZÁKLADNÍ POJMY – „CITLIVÝ“ OSOBNÍ ÚDAJ

- Dle nařízení GDPR = **zvláštní kategorie osobních údajů**

➤ Rasový či etnický původ	➤ Zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby
➤ Politický názor	
➤ Náboženské vyznání	➤ Zdravotní stav
➤ Filozofické přesvědčení	➤ Sexuální orientace
➤ Členství v odborech	➤ Údaje o dětech (děti zasluhují zvláštní ochranu osobních údajů, protože si mohou být méně vědomy dotčených rizik, důsledků a záruk a svých práv v souvislosti se zpracováním osobních údajů)

ZÁKLADNÍ POJMY – SUBJEKT ÚDAJŮ

- je fyzická osoba, k níž se osobní údaje vztahují a která je na základě těchto údajů identifikovatelná

➤ Pedagogický pracovník školy (učitel, vychovatel, asistent pedagoga...)	➤ Provozní pracovník školy (kuchařka, vedoucí ŠJ, hospodářka, účetní...)
➤ Žák/ student	➤ Zákonný zástupce dítěte

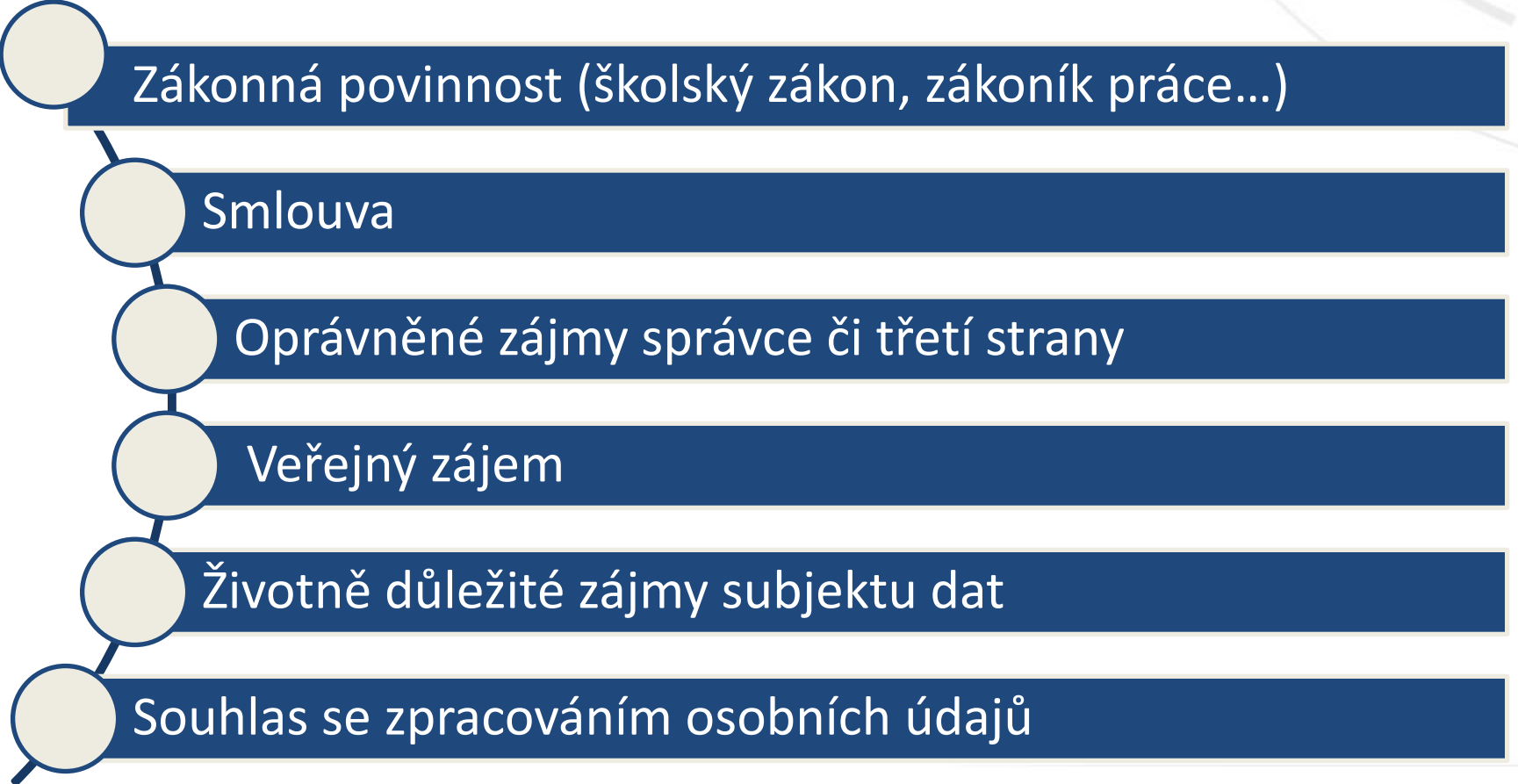
ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

- Zpracováním osobních údajů se chápe jakákoliv operace nebo soubor operací, které správce nebo zpracovatel **systematicky** provádějí s osobními údaji, a to pomocí či bez pomoc automatizovaných postupů.

<i>shromažďování</i>	<i>uspořádání</i>	<i>vyhledávání</i>	<i>nahlédnutí</i>	<i>používání</i>	<i>předávání</i>
<i>zveřejňování</i>	<i>strukturování</i>	<i>zaznamenání</i>	<i>ukládání na nosiče informací</i>	<i>šíření</i>	<i>třídění nebo kombinování</i>
<i>výměna</i>	<i>uchovávání</i>	<i>úprava nebo pozměňování</i>	<i>omezení</i>	<i>výmaz nebo likvidace</i>	<i>zpřístupňování</i>

PRÁVNÍ DŮVODY A ZÁSADY ZPRACOVÁNÍ

PRÁVNÍ ZÁKLAD ZPRACOVÁNÍ OS. ÚDAJŮ DLE ČL. 6 GDPR, Odst. 1



Zákonná povinnost (školský zákon, zákoník práce...)

Smlouva

Oprávněné zájmy správce či třetí strany

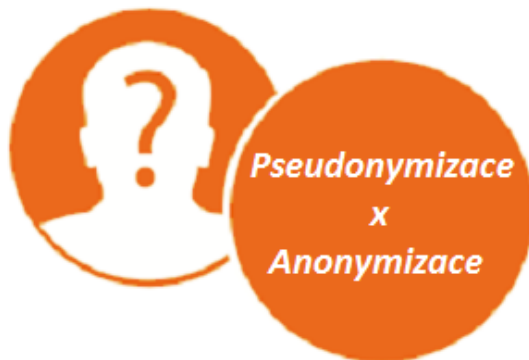
Veřejný zájem

Životně důležité zájmy subjektu dat

Souhlas se zpracováním osobních údajů

ANONYMIZACE x PSEUDONYMIZACE

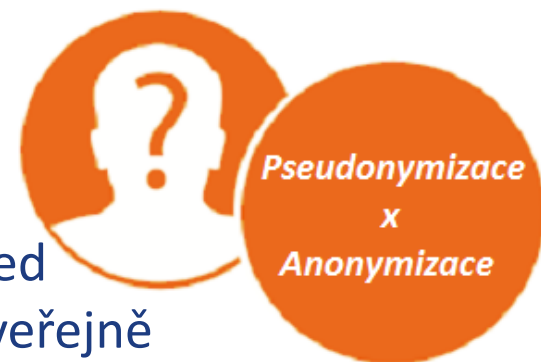
- PSEUDONYMNÍ ÚDAJ = OSOBNÍ ÚDAJ
 - Pseudonymizace spočívá v nahrazení některých identifikačních údajů jiným vhodným identifikátorem
 - „klíč“ držen odděleně od osobních údajů



ANONYMIZACE x PSEUDONYMIZACE

- ANONYMIZOVANÝ ÚDAJ ≠ OSOBNÍ ÚDAJ

- proces anonymizace je procesem nevratné ztráty vazby mezi informacemi a subjektem údajů
- anonymizovaná data mohou mít velkou přidanou hodnotu pro statistické účely
- formou anonymizace je také „začernění“ textu před zveřejněním na webových stránkách nebo jiném veřejně dostupném místě
- pro anonymizaci dokumentů vytvořilo MV ČR na portálu veřejné správy **Nástroj pro anonymizaci dokumentů**. Přístup do něj má bezplatně každý orgán veřejné moci prostřednictvím přihlašovacích údajů do CzechPointu nebo datové schránky. Více informací najdete [zde](#).



ANONYMIZACE x PSEUDONYMIZACE

- **pseudonymizace** – v tuto chvíli školy využívají při zveřejňování výsledků zápisů do MŠ a ZŠ na webových stránkách (přidělení registračních čísel žákům)
- **anonymizace** – využití pro statistické účely – přehledy počtů žáků, poměrů děvčat/ chlapců apod. do ročenky nebo výroční zprávy školy

NESPRÁVNÁ ANONYMIZACE

Původní podoba



Obec Horní Lideč

Horní Lideč 292, 756 12 Horní Lideč, IČO: 00303780, DIČ: CZ00303780
tel.: 571447428, e-mail: obec.hornilidec@tiscali.cz

Vyřizuje: [REDACTED]
Telefon: 571 447 469
E-mail: [REDACTED]
Naše č.j./sp. zn.: [REDACTED]
Horní Lideč, 8.11.2016

[REDACTED]
182 00 Praha 8 – Kobylisy

zůstalo čitelné i přes začernění

VĚC: Žádost o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím

Vážený pane [REDACTED],

Na základě Vaší žádosti ze dne 4.11.2016 Vám poskytují požadované informace:

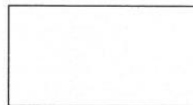
Po úpravě



Obec Horní Lideč

Horní Lideč 292, 756 12 Horní Lideč, IČO: 00303780, DIČ: CZ00303780
tel.: 571447428, e-mail: obec.hornilidec@tiscali.cz

Vyřizuje: [REDACTED]
Telefon: 571 447 469
E-mail: [REDACTED]
Naše č.j./sp. zn.: [REDACTED]
Horní Lideč, 8.11.2016



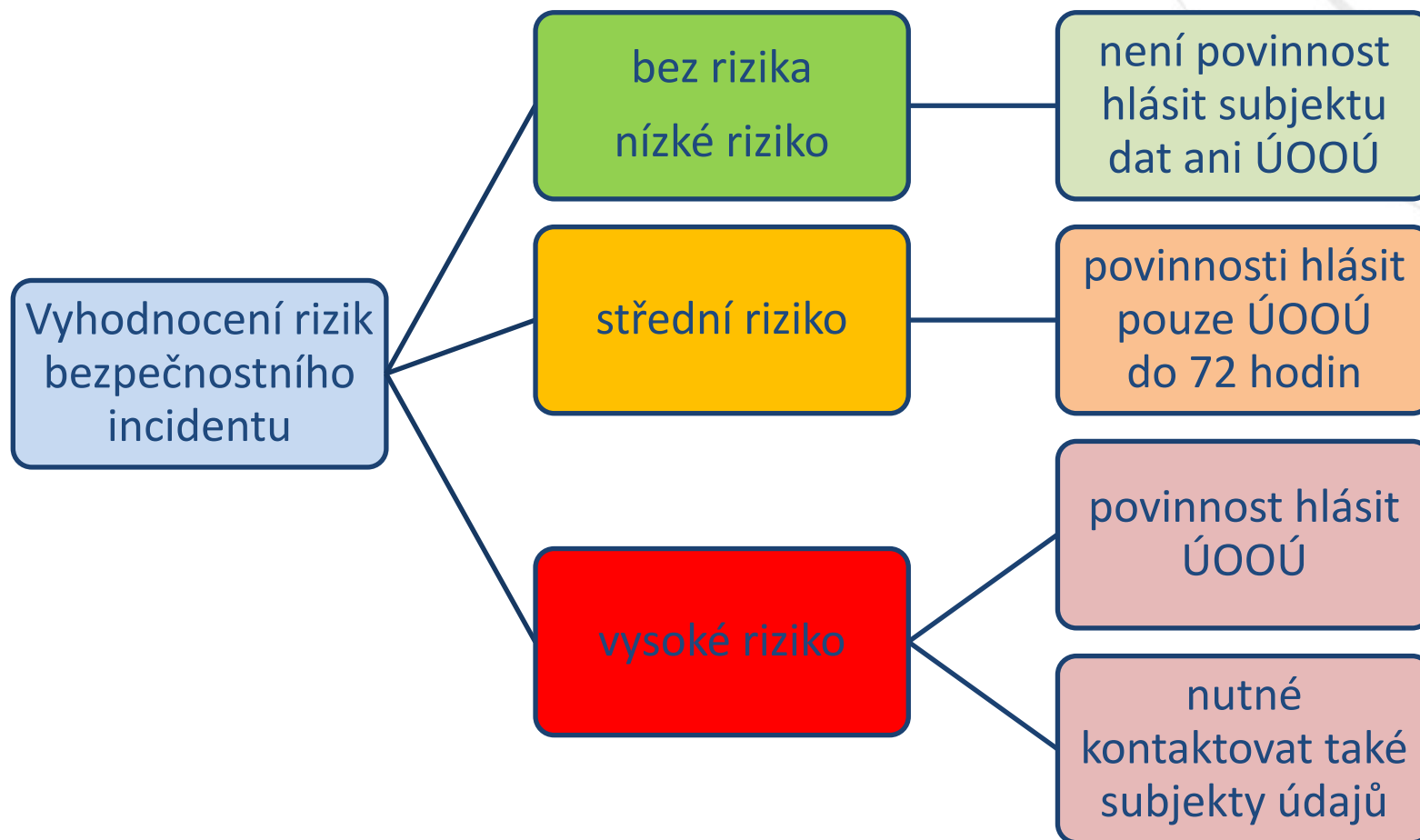
VĚC: Žádost o informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím

Vážený pane,

Na základě Vaší žádosti ze dne 4.11.2016 Vám poskytují požadované informace:

OHLAŠOVACÍ POVINNOST SPRÁVCE A BEZPEČNOSTNÍ INCIDENTY

OHLAŠOVACÍ POVINNOST



OHLAŠOVACÍ POVINNOST

- V ohlášení správce uveďte, pokud jsou mu tyto údaje známy, alespoň
 - **a)** popis povahy porušení zabezpečení osobních údajů,
 - **b)** kategorie a přibližný počet subjektů údajů a záznamů osobních údajů, kterých se porušení zabezpečení týká,
 - **c)** jméno a kontaktní údaje pověřence nebo jiného pracoviště, které poskytne bližší informace k porušení zabezpečení osobních údajů,
 - **d)** popis pravděpodobných důsledků porušení zabezpečení osobních údajů a
 - **e)** popis opatření přijatých nebo navržených spravujícím orgánem k nápravě nebo zmírnění újmy způsobené porušením zabezpečení osobních údajů.

BEZPEČNOSTNÍ INCIDENTY

Vždy je nutné vyhodnotit, k jak rozsáhlému úniku osobních údajů došlo a nakolik mohla být poškozena práva dotčených subjektů údajů.

Ne každý bezpečnostní incident je nutné hlásit Úřadu pro ochranu osobních údajů, správce by si však měl vést evidenci všech – i méně závažných – bezpečnostních incidentů! Od toho slouží kniha bezpečnostních incidentů, která je uložena u ředitele.

PŘÍKLADY BEZPEČNOSTNÍCH INCIDENTŮ

1. Správce uložil zálohu archivu na zašifrované CD/ DVD.
Toto paměťové médium bylo odcizeno během vloupání.
2. Ztráta CD nebo DVD s nezašifrovanými daty.
3. Ztráta bezpečně zašifrovaného mobilního zařízení
využívaného správcem a jeho zaměstnanci.
4. Ztráta nezašifrovaného mobilního zařízení využívaného
správcem a jeho zaměstnanci.

PŘÍKLADY BEZPEČNOSTNÍCH INCIDENTŮ

5. Během kybernetického útoku byly z webové stránky provozované správcem získány osobní údaje jednotlivců.
6. Správce utrpí útok ransomwarem (vyděračským softwarem), při němž dojde k zašifrování dat. Jiný škodlivý software nebyl zjištěn. Zálohy nejsou k dispozici a data nelze obnovit.
7. Osobní údaje žáků byly omylem rozeslány na nesprávný adresář obsahující adresy různých příjemců.
8. E-mail v rámci přímého marketingu byl odeslán v kolonce Komu nebo Kopie, čímž každý z příjemců mohl zjistit elektronickou adresu ostatních příjemců.

PRÁVA SUBJEKTŮ ÚDAJŮ

PRÁVA SUBJEKTU ÚDAJŮ

Právo na informace (přístup ke svým os. údajům) – žádost musí být zpracována do **30 dnů**

Právo na opravu

Právo vznést námitku

Právo na omezení zpracování

Právo na přenositelnost – pouze elektronická forma údajů, které organizaci subjekt údajů předal na základě smlouvy nebo souhlasu (netýká se CzechPointu a IS)

Právo být zapomenut

Právo podat stížnost k Úřadu pro ochranu osobních údajů

ORGANIZAČNÍ OPATŘENÍ

- **Spisový a skartační řád** – pravidelná aktualizace a jeho důsledné dodržování
- **Organizační řád** – vytvořit funkci a jmenovat DPO, který provádí nezávislou kontrolní funkci ochrany os. údajů
- **Směrnice o ochraně osobních údajů a kybernetické bezpečnosti**
- **Směrnice o práci uživatelů v počítačové síti a v informačních agendových systémech**
- **Zásady zpracování osobních údajů** – povinnost zveřejnění na webových stránkách obce nebo na jiném oficiálním místě (úřední deska, kancelář vedení...)
- **Pravidelná školení zaměstnanců v oblasti GDPR a informační bezpečnosti**
- **Vedení provozně bezpečnostní dokumentace včetně evidence bezpečnostních incidentů**

TECHNICKÁ OPATŘENÍ

- **nastavení oprávněného přístupu** k serveru, do informačního agendového systému, do účetního softwaru, do spisové služby, na cloudové úložiště, do e-mailových schránek...
- **pravidelná aktualizace systémů**, antivirového programu, firewallu...
- **autentizace a autorizace** uživatelů do informačních systémů i do PC (nastavení práv administrátora vs. uživatelské účty)
- data uložená na bezpečných místech (**šifrované úložiště**)
- **kontrola USB portů, využívání šifrovaných USB disků**
- **evidence kódů k alarmu, vydávání klíčů oproti podpisu**
- **zabezpečení webových stránek SSL certifikátem** (https)
- **monitoring přístupů do systémů** (kdy se kdo a kam přihlásil, doba přihlášení, kdy se odhlásil)
- **pseudonymizace osobních údajů** (osobní čísla zaměstnanců...)
- **anonymizace osobních údajů**

VYUŽITÍ SOCIÁLNÍCH SÍTÍ ŠKOLAMI A ŠKOLSKÝMI ZAŘÍZENÍMI



Fotografie, kterou je možné zveřejnit na sociální síti bez souhlasu se zpracováním osobních údajů.

Fotografie, u které před zveřejněním na sociální síti potřebujeme získat souhlas se zpracováním osobních údajů.



VYUŽITÍ SOCIÁLNÍCH SÍTÍ ŠKOLAMI A ŠKOLSKÝMI ZAŘÍZENÍMI

Mohou novináři volně stáhnout fotografie z facebookového profilu školy nebo školského zařízení a použít je do reportáže za účelem toho, že vlastní zpravodajskou licenci?

V takových situacích je třeba se vždy zabývat hlediskem přiměřenosti zveřejnění. Podle Nejvyššího soudu by v případě použití fotografií z profilů na sociálních sítí novinářem zveřejněná fotka svým obsahem měla věcně souviset s reportáží a její zveřejnění nesmí nepřiměřeně zasahovat do důstojnosti, vážnosti, cti a soukromí dotčených osob. Ani zveřejnění povedené profilové fotky neznamená souhlas uživatele, že je možné ji šířit kýmukoli a k jakémukoli účelu.

Před Nejvyšší soud se nedávno dostal spor uživatelky Facebooku a internetového zpravodajského portálu bulvárního zaměření. Internetový portál použil veřejně dostupnou profilovou fotku uživatelky pořízenou v ateliéru a v pokročilé fázi těhotenství, a to u dvou článků, jež se týkaly vyšetřování smrti její kamarádky. Takové jednání podle Nejvyššího soudu není možné – podrobnosti o případu a více informací najdete na stránkách České advokátní komory.

INFORMAČNÍ POVINNOST PŘI ORGANIZACI AKCÍ ŠKOL, SPOLKŮ A PO

- informace o pořizování fotodokumentace a videozáznamu a účelech použití AV záznamů již na pozvánce na akce
- v den konání akce plakát/ banner/ roll-up znovu s upozorněním o pořizování fotodokumentace a videozáznamu a účelech použití AV záznamů, včetně uvedení kontaktních údajů správce a právech subjektů údajů s odvoláním na Zásady zpracování osobních údajů

INFORMAČNÍ POVINNOST – PŘEDPRACOVNÍ VZTAHY

- Agenda předpracovních vztahů – zák. č. 262/2006 Sb., zákoník práce
- Pro samotné výběrové řízení není nutný souhlas, stačí splnit informační povinnost
- Souhlas pouze pokud chceme CV a motivační dotaz neúspěšného kandidáta uchovat
- Nezapomínat odpovídat i zájemcům mimo výběrová řízení
- Vrácení/ potvrzení o likvidaci osobních údajů

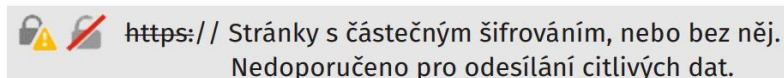
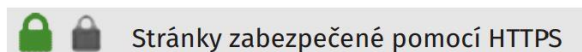
KYBERNETICKÁ BEZPEČNOST

JAK SI ZABEZPEČIT PRACOVNÍ NEBO SOUKROMÝ POČÍTAČ?

1. **Omezte přístup dalších osob** k soukromým i pracovním zařízením.
2. **Využívejte silné heslo**, číselný kód, gesto nebo jiný způsob zabezpečení. Chráníte tím svá data pro případ odcizení či ztráty zařízení.
3. Nikdy si **neukládejte přihlašovací údaje** k zařízením a účtům **v blízkosti svého počítače**.
4. Ujistěte se, že **při zadávání přihlašovacích údajů je nikdo cizí nevidí**, například pohledem přes rameno.
5. **Po dokončení práce se** z informačního agendového systému (či jiného software) i ze svého účtu **odhlaste** – před odchodem na poradu, na poštu, před odchodem domů apod. (pro rychlé odhlášení můžete použít klávesovou zkratku WINDOWS+L).

JAK SI ZABEZPEČIT PRACOVNÍ NEBO SOUKROMÝ POČÍTAČ?

6. **Aktualizujte pravidelně software** a nevypínejte automatické aktualizace systému. Díky tomu zajistíte opravu známých zranitelností, které by mohly ohrozit používané zařízení.
7. **Šifrujte citlivá data** na externích discích a dalších přenosných zařízeních a **pravidelně svá data zálohujte**. Využít můžete například flashky nebo externí disk. Důležité je, aby záloha byla na jiném místě než v mém zařízení, byla šifrována a připojena pouze v okamžiku zálohování.
8. Do svých zařízení **nepřipojujte neznámé USB disky**, externí disky a jiná paměťová zařízení.
9. Při procházení webu **preferujte webové stránky zabezpečené pomocí protokolu https**.



10. **Dávejte pozor, na jaké odkazy klikáte** – je-li to technicky možné, zkontrolujte, že odkaz nevede na pozdeřelou URL adresu (Na odkaz klikněte pravým tlačítkem myši, zvolíte možnost “Kopírovat adresu odkazu” a ten zkopírujete např. do poznámkového bloku.)

DOPORUČENÁ PRAVIDLA PRO BEZPEČNÁ HESLA

1. Pro přístup do počítače, internetového bankovníctví, e-mailu a jednotlivých programů používejte **RŮZNÁ hesla**.
2. Pokud si svá hesla nepamatujete, používejte **správce hesel** – aplikace, která si za vás pamatuje přihlašovací jména a hesla.
3. Při vymýšlení hesla **bud'te originální** – nepoužívejte běžná slova a slovní spojení. Nepožívejte však ani diakritiku – můžete se dostat do situace, kdy na klávesnici nebude české rozložení klávesnice a pak byste heslo nebyli schopni napsat.
4. Bezpečné heslo musí obsahovat **minimálně 12 znaků**. Čím delší heslo používáte, tím obtížnější je pro hackery ho uhodnout.

DOPORUČENÁ PRAVIDLA PRO BEZPEČNÁ HESLA

4. Bezpečné heslo by mělo obsahovat **kombinaci malých písmen** (26 znaků), **velkých písmen** (26 znaků), **číslic** (10 znaků) a **speciálních znaků** (32 znaků). Pro heslo, které má 7 znaků a obsahuje malá a velká písmena, číslice i speciální znak, existuje 65 bilionů kombinací.
5. Pokud nemáte dost fantazie na vymýšlení bezpečných hesel, máte možnost použít **generátor hesel**. U generátoru hesel si můžete zvolit délku hesla i znaky, které má heslo obsahovat. Online generátor hesel najdete třeba zde.
6. **Nesdílejte přihlašovací údaje a hesla** s třetími osobami. V případě pracovního i soukromého e-mailu, pracovního intranetu, docházkového systému nebo hesla do počítače může mít takové jednání závažné následky.
7. Dávejte přednost **dvoufázovému ověření přístupu**. Dvoufázové ověření přístupu, kdy po zadání přihlašovacího jména a hesla musí uživatel ještě zadat kód z smsky nebo e-mailu, garantuje silnější zabezpečení přístupu.

NEJČASTĚJŠÍ CHYBY PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

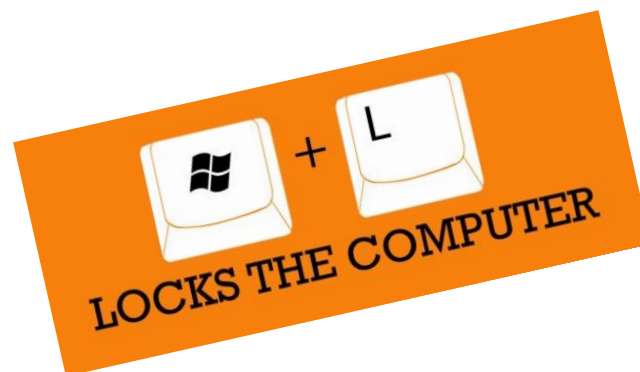
NEJČASTĚJŠÍ CHYBY PŘI PRÁCI S OSOBNÍMI ÚDAJI – ANEB NA CO SI DÁT POZOR

- podcenění nestrukturovaných dat a dat v listinné podobě
– *nestrukturovaná data jsou různé tabulky v excelu, seznamy kontaktů na rodiče ve wordu, v listinné podobě pak třídní výkazy, i třeba složky s písemkami žáků, podklady z PPP, SPC apod.*



NEJČASTĚJŠÍ CHYBY PŘI PRÁCI S OSOBNÍMI ÚDAJI – ANEB NA CO SI DÁT POZOR

- odemčené počítače v nepřítomnosti na pracovišti
– *jednotlivé PC by měly mít nastaveny zaheslované uživatelské účty, každý pedagog by se měl po dokončení práce ze svého účtu odhlásit – před odchodem do hodiny, před odchodem domů apod.*



NEJČASTĚJŠÍ CHYBY PŘI PRÁCI S OSOBNÍMI ÚDAJI – ANEB NA CO SI DÁT POZOR

- ponechání dokumentů s os. údaji bez dozoru
 - *v kabinetech by bez dozoru a dostatečného zabezpečení neměly ležet složky dětí, třídní výkazy, záznamy z PPP a SPC apod.*

DODRŽOVAT PRAVIDLO ČISTÉHO STOLU !!!



NEJČASTĚJŠÍ CHYBY PŘI PRÁCI S OSOBNÍMI ÚDAJI – ANEB NA CO SI DÁT POZOR

- práce na nezabezpečených lokálních úložištích
- neprověřené datové nosiče (flashky), otevřené porty
- využívání nezabezpečených komunikačních kanálů



NEJČASTĚJŠÍ CHYBY PŘI PRÁCI S OSOBNÍMI ÚDAJI – ANEB NA CO SI DÁT POZOR

- nesprávná archivace a likvidace dokumentů



NEJČASTĚJŠÍ CHYBY PŘI PRÁCI S OSOBNÍMI ÚDAJI – ANEB NA CO SI DÁT POZOR

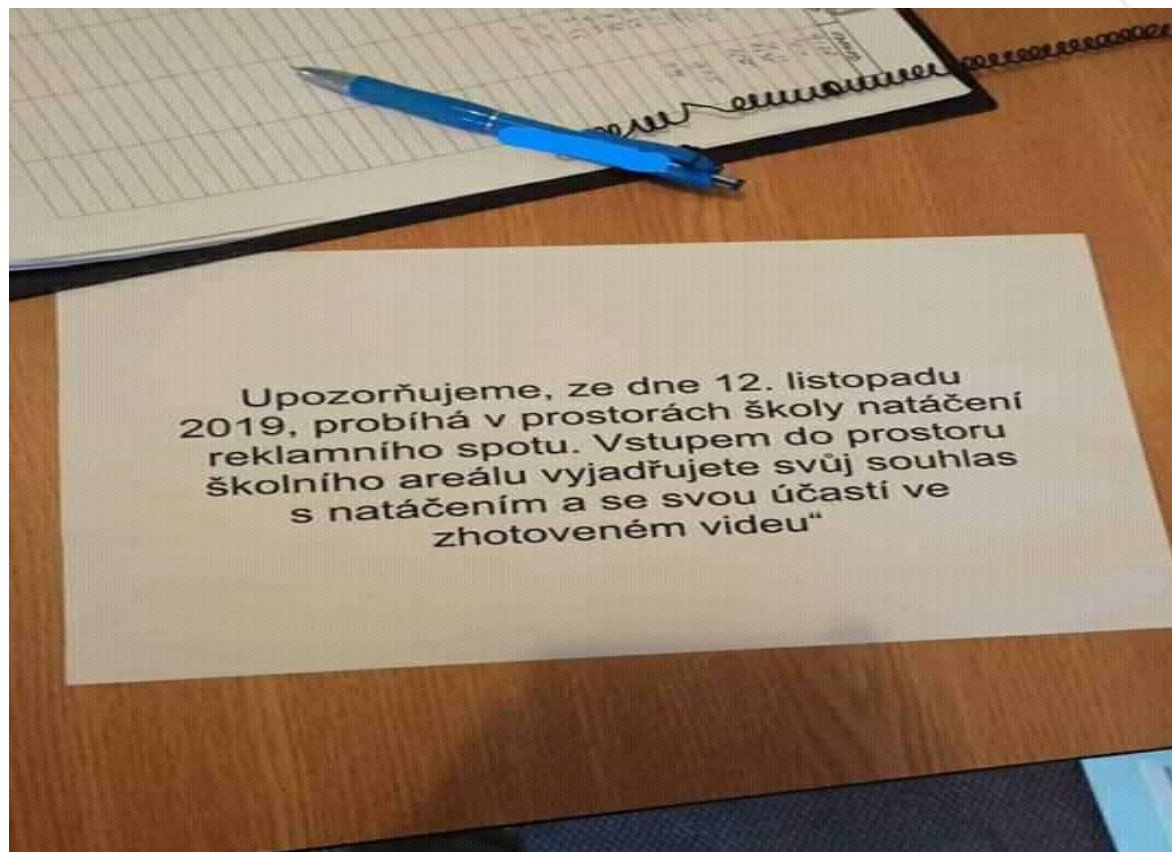
- sdělování osobních údajů po telefonu



NEJČASTĚJŠÍ CHYBY PŘI PRÁCI S OSOBNÍMI ÚDAJI – ANEB NA CO SI DÁT POZOR

- pracovníci školy při projednávání informací citlivé povahy týkající se žáků (kázeňské přestupky, týrání dětí v rodině, poruchy učení či chování...) nedodržují princip diskrétnosti a právo na soukromí – se žáky hovoří na chodbách, ve společných kabinetech, před ostatními žáky či jinými nepovolanými osobami apod.

Kontrolní otázka č.1 / Je to v pořádku?



Kontrolní otázka č.2 /Odeslání vysvědčení přes aplikace MS TEAMS, GOOGLE/ Je to v pořádku?

ČESKÁ REPUBLIKA
STÁTNÍ ZKŮŠEBNÍ KOMISE PŘI VVOŠ - STÁTNÍM TĚSNOPISNÉM ÚSTAVU V PRAZE
Císlo 1369
Rok 2000

VYSVĚDČENÍ

o státní zkoušce z kancelářského psaní na stroji

Markéta Šebánová

den, měsíc a rok narození 21. září 1982 rodíště Brandýs nad Labem okres Praha-východ

vykonala(a) podle směrnic Státního těsnopisného ústavu v Praze pověřeného ministerstvem školství, mládeže a tělovýchovy ze dne 8. dubna 1992 o státních zkouškách z těsnopisu, z psaní na stroji, ze stenotypistiky, z obchodní korespondence a ze sekretářských prací

státní zkoušku z kancelářského psaní na stroji

s tímto prospěchem:

1. Desetiminutový opis textu, v němž dosáhl(a) rychlosti 244,1 čistých úhozů za minutu (při přesnosti 99,88 %), byl výborný

2. Písemnosti se zřetelem k normalizované úpravě podle daných dispozic vypracoval(a) dobře

V Praze dne 25. května 2000

Ing. L. Kovář
předseda zkušební komise

M. An. Kubínka
za členy zkušební komise

Stupnice známek:	1	2	3	4
	výborný	velmi dobrý	dobry	neprospěl

Patisk zakázán

SEVT - 92 561 0

Kontrolní otázka č.3 /Je to v pořádku?

MANUÁL PRO VYPLNĚNÍ OMLUVY DĚTÍ

Vážení rodiče,

z důvodů zavedeného GDPR, prosíme, **VYPLŇUJTE POUZE ZNAČKU**
VAŠEHO DÍTĚTE. Nikoliv jeho jméno.

Příklad vyplněného řádku v omluvném listu:

23.9.2018 PRASÁTKO

(Tímto vyjádřením na omluvný list jasně pochopíme, že Vaše dítě 23.9.2018 nepřijde do MŠ a počítáme s tím.)

Děkujeme za pochopení.

Odpovědi na kontrolní test

Otázka č. 1

V případě takového spotu se jedná o marketingový účel a je nutné mít zpracovaný souhlas se zpracováním osobních údajů zaměstnanců, žáků, popřípadě i jiných osob. Pokud se však jedná o realizaci projektového dne, který dokládáte jako výstup v rámci školních aktivit, pak se jedná o veřejný zájem., můžete tak zveřejňovat na webových stránkách. Pozor jakékoliv fotografie umístěné nebo sdílené na sociálních sítích je možné pouze ze souhlasem fyzické osoby!!! Tento souhlas je kdykoliv odvolatelný = smazání fotografie.

Odpovědi na kontrolní test

Otázka č. 2

V takovém případě se jedná o bezpečnostní incident způsobený z nedbalosti. Není možné ověřit identifikaci dotyčného žáka nebo zákonného zástupce na základě přidělené emailové adresy. V řešení jsou nyní události, kdy došlo dokonce k hromadnému odeslání do skupiny třídy 20 žáků. Jedinou možnou volbou je tak osobní předání nebo cesta formou datové schránky nebo doporučené pošty.

Odpovědi na kontrolní test

Otázka č. 3

V takovém případě se jedná o nastavení ze strany správce, tedy vedení organizace, která nepochopila nutnost anonymizace osobních údajů. Je zakázáno zveřejňovat seznamy žáků na webových stránkách školy. Pokud se však jedná o vyzvedávání dětí ze školy nebo školského zařízení je v pořádku, aby bylo jasně definované jméno a příjmení dotyčného, pokud je tento údaj zapsaný v sešitu nebo na nástěnce ve vnitřních prostorách organizace.

NEJČASTĚJŠÍ CHYBY PŘI PRÁCI S OSOBNÍMI ÚDAJI – ANEB NA CO SI DÁT POZOR

- neznalost/ neuvědomění si rizik



DĚKUJEME ZA POZORNOST

Více o programech pro školy a školská zařízení zde:

<https://www.bezpecnaorganizace.eu/>

POUŽITÁ LITERATURA - LEGISLATIVNÍ DOKUMENTY

- *Nařízení 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)*
- *Zákon č. 262/2006 Sb., Zákoník práce*
- *Zákon č. 561/2004 Sb., Zákon o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon)*
- *Zákon č.181/ 2014 Sb. o kybernetické bezpečnosti*
- *Vyhláška č.82/ 2018 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidace dat*
- *ČSN ISO/ IEC 27005 - Informační technologie, Bezpečnostní techniky, Řízení rizik bezpečnosti informací*
- *ČSN ISO/ IEC 27 001 - Informační technologie, Bezpečnostní techniky, Systémy řízení bezpečnosti informací*
- *ČSN ISO 31000 - Management rizik - principy a směrnice*

POUŽITÁ LITERATURA - LEGISLATIVNÍ DOKUMENTY

- Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství: (dokument PDF). *MŠMT ČR* [online]. Publikováno: 2017-11-07 [cit. 2018-07-27]. Dostupné z: <http://www.msmt.cz/file/44569/>
- Schválené pokyny Evropského sboru pro ochranu osobních údajů (dříve Pracovní skupina WP29). [cit. 2018-07-27]. Dostupné z: <https://www.uoou.cz/schvalene-pokyny/d-28603>

POUŽITÁ LITERATURA

- NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.
- NONNEMANN, František. *Praktická příručka pro Pověřence pro ochranu osobních údajů*. Tayllorcox - ensure your certification. Praha, 2018.
- ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9.
- BARTÍK, Václav a Eva JANEČKOVÁ. *Zpracování osobních údajů školami: včetně úplného znění GDPR*. 2. aktualizované vydání. Praha: Wolters Kluwer Česká republika, 2013. Řízení školy (Wolters Kluwer). ISBN 978-80-7478-359-3.
- JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. Řízení školy (Wolters Kluwer). ISBN 978-80--7251-436-6.
- VALENTA, Jiří, Luděk NOVÁK a Josef POŽÁR. *Školské zákony a prováděcí předpisy s komentářem: Cyber security glossary*. Třetí aktualizované vydání. Olomouc: ANAG, 2005-. Práce, mzdy, pojištění. ISBN 978-80-7554-102-4.