GDPR PRAKTICKY

Koho se GDPR týká

* Výhradně živých fyzických osob;
* Nevztahuje se na osoby zesnulé;
* NETÝKÁ SE ZPRACOVÁNÍ OÚ PRO OSOBNÍ POTŘEBU;

Zvláštní ochranu požívají nezletilí a dále pak zpracování osobních údajů tzv. zvláštní kategorie (zdravotní stav, národnost, náboženské vyznání apod.)

Mlčenlivost

Je základní zákonná povinnost všech zaměstnanců, kteří při výkonu svého povolání přichází do kontaktu s osobními údaji dalších osob, případně je přímo zpracovávají.

Mlčenlivost v praxi

* neřešit záležitosti subjektů osobních údajů na veřejnosti (parky, hromadná doprava, ...);
* neřešit děti/žáky/zaměstnance jinak, než na profesionální úrovni;
* neposkytovat informace neoprávněným osobám, neposkytovat informace po telefonu;
* mlčenlivost se týká samozřejmě také interních záležitostí zaměstnavatele (zabezpečení objektu, budoucí záměry apod.);

Mlčenlivost v praxi

Nelze např. šířit osobní údaje a informace kolegů a o kolezích (nemoc, rodinná situace, finanční situace, výše platu/mzdy, odměn, datum narození apod.), pokud k těmto údajům má zaměstnance z titulu své role přístup před dalšími kolegy, žáky a jejich zákonnými zástupci ;

POZOR, ZA PORUŠENÍ MLČENLIVOSTI HROZÍ TREST I DLE TRESTNÍHO ZÁKONÍKU (§ 180 – zákaz výkonu činnosti, až 3 roky odnětí svobody) – samozřejmě za velmi významné a rozsáhlé porušení mlčenlivosti.

Typické znaky osobních údajů

* Za osobní údaj lze považovat každou informaci, která se vztahuje k určité fyzické osobě (bez ohledu např. na její věrohodnost či kvalitu).
* Tato informace musí být schopna fyzickou osobu identifikovat, odlišit od ostatních fyzických osob. Zde mohou nastat dvě situace:
  - Je možné nalézt přímý vztah mezi údajem a fyzickou osobou, v tomto případě jde o tzv. přímou identifikaci (určenost);
  - Nelze nalézt a tedy vytvořit přímou vazbu mezi údajem a konkrétní fyzickou osobou, nicméně lze získat další údaje, spojit je s předešlými získanými údaji a následně díky kombinaci více údajů fyzickou osobu identifikovat – jde o tzv. nepřímou identifikaci (určitelnost).

ZVLÁŠTNÍ KATEGORIE OSOBNÍCH ÚDAJŮ

Zvláštní kategorie osobních údajů jsou osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu, sexuálním životě nebo sexuální orientaci fyzické osoby.

TYTO ÚDAJE LZE ZPRACOVÁT JEN NA ZÁKLADĚ PLNĚNÍ PRÁVNÍ POVINNOSTI NEBO SE SOUHLASEM SUBJETU OÚ

Zaměstnavatel by např. neměl být vůbec informován o tom, který zaměstnanec je členem odborové organizace v organizaci).

Údaje zvláštní kategorie zpracovávané školami/školskými zařízeními

* údaje o zdravotním stavu dětí, žáků, studentů i zaměstnanců (včetně informací o absolvování očkování či prodělání nemoci);

  POZOR, informace o výsledku povinné periodické prohlídky nebo, že např. je zaměstnanec dočasně pracovně nezpůsobilý (neschopenka) není údaj o zdravotním stavu, tím je např. konkrétní diagnóza;
* údaje o specifických vzdělávacích potřebách žáků (doporučení z PPP/SPC, IVP);
* údaje o potravinových alergiích, speciálních dietách (školní jídelna);

Tyto údaje musí být vždy velmi dobře zabezpečeny, jsou považovány za důvěrné (dobře chráněný přístup, uzamykatelné skříně/šuplíky).

Doporučení z PPP/SPC (a jiné dokumenty obsahující OÚ zvláštní kategorie)

* musí být stanoven a dodržován režim práce s těmito dokumenty:
* tedy kdo je oprávněn s nimi pracovat a jakým způsobem jsou v rámci pedagogického sboru předávány příslušné informace;
* způsoby předávání OÚ zvláštní kategorie (škola x PPP, SPC, OSPOD, Policie ČR apod.).

Kdy mohu OÚ zpracovávat?

* pokud existuje právní důvod;
* určím účel zpracování a rozsah údajů;
* určím dobu zpracování ;
* zajistím bezpečnost OÚ;
* znám práva subjektů OÚ a respektuji je;

ÚDAJE PRO KTERÉ NEEXISTUJE PRÁVNÍ DŮVOD/ÚČEL ZPRACOVÁNÍ LZE DEFINOVAT JAKO NADBYTEČNÉ ÚDAJE A NELZE JE ZPRACOVÁVAT!!

Právní tituly pro zpracování OÚ

* plnění zákonné povinnosti;
* jednání za účelem uzavření smlouvy;
* souhlas – neměl by být nadužíván;
* oprávněný zájem organizace;
* veřejný zájem (epidemie, katastrofy);
* ochrana životně důležitých zájmů (záchrana života);

Škola, školské zařízení

Jsou zde zpracovávány zpravidla osobní údaje:

* dětí, žáků, studentů;
* zákonných zástupců;
* zaměstnanců, popř. studentů VŠ či VOŠ na praxi;
* smluvních stran (např. v rámci doplňkové činnosti) ;

Většina údajů je zpracovávána ze zákona, v oprávněném či veřejném zájmu.

Některé osobní údaje pak na základě uděleného Souhlasu subjektu údajů (například fotografie).

Děti, žáci studenti z Ukrajiny

* Ve vztahu ke zpracování OÚ je **postup školy u osob z Ukrajiny zcela stejný**, jako u ostatních cizinců, dětí, žáků, studentů, viz školský zákon, který stanoví, jaké OÚ lze zpracovávat.
* Ověřuje a eviduje se úroveň znalosti českého jazyka (pro potřeby výuky).

Zásady zpracování OÚ

* **zákonnost, korektnost, transparentnost** – správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně a korektně;
* **omezení účelu** – osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely;
* **minimalizace údajů** – osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány;

Zásady zpracování OÚ

* přesnost – osobní údaje musí být přesné;
* omezení uložení – osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány;
* integrita a důvěrnost – technické a organizační zabezpečení osobních údajů;

Základní pravidla pro práci s osobními údaji

* **neshromažďovat nadbytečné údaje** (národnost, členové rodiny a jejich OÚ apod., pokud to není nezbytné);
* **zamýšlet se nad tím, jaké OÚ jsou na nástěnkách v kancelářích nebo položeny na stolech přístupné návštěvám:**
  * seznamy zaměstnanců s daty narození či jinými osobními údaji;
  * prohlášení poplatníka k dani;
  * přihlášky žáků ke studiu apod.;

Práva subjektu OÚ (zaměstnanec, žák, klient..)

* na informace o zpracování - v okamžiku získání osobních údajů má správce povinnost informovat subjekt údajů o svém úmyslu tyto osobní údaje zpracovávat;
* na přístup k osobním údajům;
* na opravu a doplnění;
* vznést námitku proti zpracování;
* na omezené zpracování;
* na výmaz;
* na možnost stížnosti u dozorového úřadu ÚOOÚ;

Pověřenec pro ochranu OÚ

* Vyjma monitorování, zda je zpracování OÚ v souladu s platnou legislativou a navrhování možných postupů pro jejich ochranu jde o **osobu, které by měly být adresovány připomínky, popř. stížnosti ke zpracování OÚ organizací**
* Nikdo vyjma pověřence a není-li stěžovatel spokojen, následně ÚOOÚ /vyjma moci soudní/ není oprávněn se závazně vyjadřovat k případným stížnostem.

Stížnosti adresované ČŠI či zřizovateli apod. se vždy vrací/mají vracet k pověřenci či ÚOOÚ (ten si stanovisko pověřence dané organizace při prošetřování podnětů a stížností vyžádá).

Ochrana OU v kyberprostoru

* používání aktualizovaného antivirového programu;
* zachovávat obezřetnost – neotevírat podezřelé e-maily a jejich přílohy, lze tak ohrozit celou školní síť;
* důsledně se odhlašujte a opakovaně přihlašujte při opouštění pracoviště, využívejte spořič obrazovky;
* používejte silná hesla, kombinace různých typů znaků;
* nevyužívejte stejné heslo pro různé e-maily (soukromý, pracovní), hesla pravidelně měňte, nikomu je nesdělujte;
* neukládat hesla lokálně (pro další přihlášení), pozor na odpozorování.

Jak ochránit data „na cestě“

opatrnost

* nenechávat notebook, mobil bez dozoru (v autě, veřejné prostory...);
* šifrovat data (na disku, flash disky..);

čtěte licenční podmínky

* většina mobilních aplikací vyžaduje internetové připojení, čte ID a stav telefonu, zjišťuje GPS polohu, některé mohou samy odesílat prémiové SMS;

správa mobilních zařízení

* vyhledání ztraceného zařízení, vzdálené smazání dat;

pozor na nezabezpečené veřejné sítě

* internetové kavárny, veřejně přístupné a tedy špatně zabezpečené wi-fi sítě;

Komunikace se žáky, zákonnými zástupci, zaměstnanci

Pokud obsahuje osobní údaje, musí být použit pouze zabezpečený komunikační kanál, tedy:

* datová schránka;
* zpráva v listinné podobě (ideálně doporučený dopis);
* osobní předání.

Nelze využívat nezabezpečený e-mail, nelze poskytovat informace po telefonu, byť jsou např. Policií ČR nebo OSPODem v této formě někdy vyžadovány.

Kabinety, sborovna, hovorny

* vždy je třeba zohlednit, jaký provozní režim je u těchto prostor využíván – nakolik je umožněn vstup žáků, zákonných zástupců a dalších osob;
* pokud je přístup dalších osob možný, je třeba důsledněji uschovávat dokumenty obsahující OÚ (testy, písemné práce, studijní průkazy, omluvné listy, seznamy žáků, případně další dokumentaci);

Školní chodby

* lze zveřejnit výsledky v soutěžích, jejich fotografie i práce (nutno ošetřit souhlasem, vyjma prací žáků, které jsou vystaveny a zůstávají pouze ve škole);
* **nelze zveřejňovat práce opatřené hodnocením, tedy zejména známkou** – rysy, výkresy, slohové práce apod. ;

Nejčastější chyby při používání e-mailů

* Hromadně rozesílané e-maily bez použití f**unkce „skryté kopie“**, všichni příjemci pak „vidí“ e-mailové adresy všech ostatních příjemců, platí zejména při komunikaci prostřednictvím soukromých e-mailů (již řešena stížnost zákonných zástupců adresovaná ÚOOÚ).
* Předávání osobních údajů prostřednictvím nezabezpečených e-mailů.
* Přeposílání e-mailů z pracovního na soukromý, případně také následné odpovídání ze soukromého e-mailu zaměstnance.

Příklad z praxe

Vyučující TV zaslal rodiči s typickým českým příjmením na jeho soukromý e-mail s doménou seznam.cz kompletní přehled žáků účastnících se LVVZ včetně rozpisu nočních dozorů pedagogů apod. (tento rodič s učitelem na téma LVVZ komunikoval, dotazoval se na některé detaily). Na dotaz rodiče, proč dokumenty obdržel se tento rodič dozvěděl, že má stejné příjmení jako účetní školy.

Došlo ke zcela neomluvitelnému zpřístupnění OÚ žáků neoprávněné osobě, tedy **porušení mlčenlivosti,** což představuje porušení pracovní kázně a dále využití e-mailu k předání OÚ, což není dovolené, právě s ohledem na možnost vzniku podobných situací (překliknutí se u osoby příjemce)

Správný postup: NEPOUŽÍVAT PRO ODESÍLÁNÍ OÚ E-MAILY!!!!
KONTROLOVAT ADRESY PŘÍJEMCŮ ZPRÁV!!!

Příklad z praxe

Zaměstnanec podal výpověď prostřednictvím datové schránky organizace, zdůraznil v ní, že podléhá GDPR, další den po příchodu do zaměstnání se jej na potkání různí zaměstnanci ptali, proč končí apod.

* Došlo k porušení mlčenlivosti ze strany příjemce zprávy v Datové Schránky.
* Jediný, kdo měl být informován: ředitel, přímý nadřízeny a zaměstnanec zajišťující personální a mzdovou agendu, NIKDO JINÝ A TITO MĚLI MLČET

Příklad z praxe

Učitel TV před odjezdem na lyžařský výcvik zřídil skupinu na WhatsAppu (využil kontaktní telefonní čísla na mobil zákonných zástupců) a tímto způsobem chtěl od zákonných zástupců získat souhlas s posunem odjezdu na LVVZ.

* Došlo tak k několika nepovoleným postupům:

  A) zpřístupnil telefonní čísla a později, když začali členové skupiny reagovat, tak také jména příjmení, jak zákonných zástupců, tak žáků mnoha neoprávněným osobám, **porušení mlčenlivosti**, což představuje porušení pracovní kázně;

  B) využil neoficiální komunikační prostředek bez povinnosti reakce ze strany zákonných zástupců;

  C) vedení školy nebylo informováno nemohlo tedy zasáhnout.

Nejvhodnější správný postup: použití Komens v Bakalářích, popř. srovnatelné možnosti pro rozeslání hromadných zpráv vybrané skupině (třída, několik tříd, škola) v rámci Škola OnLine, Edookit.

Časté chyby při zveřejňování OÚ na webu školy:

* v přehledu zaměstnanců je uvedeno, která zaměstnankyně čerpá mateřskou/rodičovskou dovolenou;
* fotografie zaměstnanců jsou zveřejňovány bez jejich souhlasu včetně dalších údajů, které nemají být přístupny veřejnosti, např. informace o dosaženém vzdělání, soukromé e-maily nebo telefonní čísla.

Kam vede sdílnost

Sdělení	Následek
Sdělení přílišného množství osobních údajů (pohromadě nebo i na různých zdrojích)	Vydávání se za dotyčného někým jiným. Ten pak snáze získá další údaje (vydává se např. za příbuzného), pod cizí identitou si půjčuje peníze atp.
Zveřejnění intimní fotografie	Znevažující nebo urážlivé komentáře, nejrůznější sexuální nabídky, útok kybergroomera, nekontrolovatelné šíření
Pochlubení se kvalitním vybavením bytu, „hlášení" své momentální polohy na sociální síti	Pozvánka pro bytového zloděje
Sdělení tel. čísla, mailové adresy vlastní nebo členů rodiny	Obtěžování prostřednictvím nevhodných telefonátů, sms, mms, mailů, komentářů na sociálních sítích, pozvánka ke kyberšikaně
Sdělení adresy	Nezvaná a neohlášená návštěva, první krok ke stalkingu, zvýšené riziko nátlaku, vyhrožování či vydírání a jejich horší dopad
Sdělování intimních myšlenek a pocitů nebo třeba nedobrých školních výsledků	Nevyžádané, nevhodné, posměšné nebo urážlivé komentáře
Podrobný popis postavy, vlastní nespokojenosti s ní	Posměšné, znevažující nebo urážlivé komentáře
Zveřejňování nebo poskytování osobních údajů a údajů o preferencích zboží atp.	Cílená reklama, spam

Děkuji za pozornost.