

GDPR pro ředitele škol

Pavel Škarban

Pardubice, 06. 03. 2018



Harmonogram školení

- 10:00 – 10:15 Úvod
- 10:15 – 10:45 Obecné nařízení o ochraně osobních údajů jako legislativní norma
- 10:45 – 11:15 Zásadní změny GDPR ve vztahu k zákonu 101/2000 Sb., účinnost, základní pojmy – zpracování, osobní údaj
- 11:15 – 11:30 Povinnosti vyplývající školám po účinnosti GDPR, správce/zpracovatel
- 11:30 – 11:45 Přestávka**
- 11:45 – 12:00 Právní důvody zpracování, souhlas s poskytnutím údajů
- 12:00 – 12:30 Pověřenec pro ochranu osobních údajů
- 12:30 – 12:45 Práva subjektu údajů
- 12:45 – 13:00 Porušení zabezpečení, pokuty a sankce
- 13:00 – 13:30 Jak implementovat GDPR na školách, mapování, analýzy, ukázky
- 13:30 – 13:45 Organizační a technická opatření pro zajištění souladu vnitřních procesů školy s GDPR
- 13:45 – 14:00 Zodpovězení dotazů a závěr



Co to je GDPR?

General **D**ata **P**rotection **R**egulation

=

Obecné nařízení o ochraně osobních údajů

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



Co to je GDPR?

- GDPR není ČR zákon, je to sekundární právní předpis EU, jež je třeba implementovat do vnitrostátního práva
- Týká se práv běžných občanů na ochranu dat (veřejné a komerční služby – nikoliv soukromé a trestní věci)
- Současně vydána směrnice EP a Rady (EU) 2016/680 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů
- Platí pro všechny státy Unie stejně



Proč bylo zavedeno?

Cíl = hájit práva občanů EU proti neoprávněnému zacházení s jejich daty a osobními údaji

- Platí ve všech státech EU (28) + Island, Norsko, Lichtenštejnsko
- Platí pro správce a zpracovatele se sídlem v EU, i na firmy, které sídlí jinde, ale sbírají data EU občanů
- Ochrana osobních dat není „výmysl EU“, obdobnou legislativu zavedli v Rusku a Indii
- V USA nemají jednotnou legislativu na ochranu osobních údajů
- Safe Harbour, Privacy Shield – domluva USA vs EU



Proč bylo zavedeno?

- Stávající nařízení EU nevyhovovala po věcné stránce (komplexní zpracování, profilování, automatizace zpracování, obchod s OÚ)
- Stávající legislativa (směrnice 95/46/ES) nebyla v členských zemích implementována jednotně
- Hodnota osobních dat byla podceňována

Kdo chtěl být poctivý, neměl legislativu napříč EU. Kdo na to kašlal, na toho neměl stát téměř žádné páky.

GDPR toto mění !!!!!



Co je obecné nařízení a jak vypadá?

- Nařízení má stejnou váhu jako zákon ČR - přímo adresátům stanovuje povinnosti a práva
- Skládá se z Preambule a vlastního textu nařízení
- Preambule obsahuje recitály = výklad, důvodová zpráva k samotným paragrafům nařízení
- Preambule = 173 odstavců
- Nařízení = 11 kapitol a 99 článků
- Ke stažení zde: <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679>



Další legislativa související s ochranou OÚ

- Občanský zákoník 89/2012 (soulad, tělesná a duševní integrita)
- Směrnice Evropského parlamentu a Rady (EU) 2016/680 (vyšetřování trestných činů)
- Směrnice Evropského parlamentu a Rady (EU) 2016/680 (opatření k zajištění vysoké společenské úrovně bezpečnosti sítí a inf. systémů v Unii)
- Nařízení Evropského parlamentu a Rady (EU) 910/2016 o elektronické identifikaci a službách vytvářejících důvěru pro el. transakce na vnitřním trhu (EIDAS)
- Zákon 297/2016 o službách vytvářejících důvěru pro el. transakce
- Zákon 181/2016 o kybernetické bezpečnosti



Co se stane se zákonem 101/2000 Sb.?

- GDPR platí bez ohledu na národní legislativu
- zákon č. 101/2000 Sb., o ochraně osobních údajů bude zrušen
- Vznikne nový (výkladový) zákon o zpracování osobních údajů (ZZOÚ)
 - Ukončeno připomínkové řízení (15. 9. 2017)
 - Předchozí vláda nestihla projednat, bude o něm hlasovat příští parlament (PSP ČR)
 - 65§§
 - Účinnost od 25. 5. 2018 (tzn. stejně jako GDPR)



Metodika MŠMT

- 6. 11. 2017 vydalo MŠMT **Metodickou pomůcku k aplikaci obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství**
- <http://www.msmt.cz/dokumenty-3/metodicka-pomucka-k-aplikaci-obecneho-narizeni-o-ochrane?highlightWords=gdpr>
- 91 stran
 - Předmluva
 - Co se musí udělat do 25. 5. 2018
 - Novinky v ochraně OÚ od 25. 5. 2018
 - Základní zásady
 - Doporučení k aplikaci stěžejních článků
- MŠMT a NIDV realizují semináře *Novinky v právních předpisech škol a školských zařízení Legislativní novinky ve školním roce 2017/2018* ve všech krajích ČR



Základní principy GDPR

■ Princip odpovědnosti

- legislativa apriori vyvozuje odpovědnost správce za dodržení zásad zpracování
- Správce musí být schopen soulad s GDPR doložit (kodex, osvědčení, certifikace, záznamy o činnostech zpracování)

■ Přístup založený na riziku

- již od počátku koncipování zpracování osobních údajů je třeba brát v potaz povahu, rozsah, kontext a účel zpracování a přihlédnout k pravděpodobným rizikům
- Riziku je třeba přizpůsobit zabezpečení osobních údajů.



Soulad s GDPR – kodexy, osvědčení, záznamy o činnostech

Základní princip GDPR vychází z principu odpovědnosti a správce/zpracovatel musí soulad svých činností s GDPR doložit.

Kodexy

- vydávají odborná sdružení, např. kodex OÚ v bankovníctví, zdravotnictví
- Kodex schvaluje ÚOOÚ

Osvědčení

- Vydává akreditovaný subjekt
- Český institut pro akreditaci, o.p.s.

Záznamy o činnostech

- náhrada za oznamovací povinnost zákona 101
- neplatí pro firmy zaměstnávající méně než 250 osob,



Pojmy – ZPRACOVÁNÍ

Zpracováním je jakákoli operace (soubor operací) s osobními údaji (soubory OÚ), který je prováděn pomocí či bez pomoci automatizovaných postupů.

- shromáždění
- zaznamenání
- uspořádání
- strukturování
- uložení
- přizpůsobení
- pozměnění
- vyhledání
- nahlédnutí
- použití
- zpřístupnění
- šíření
- seřazení či zkombinování
- omezení
- výmaz
- zničení



Co je a není zpracování?

PŘÍKLADY:

- Uveřejnění fotek na webu školy
- Poskytnutí čísel BÚ žáků/rodičů zřizovateli
- Osobní údaje na pracovní smlouvě
- Vyhlášení nejlepších žáků školy ve školním rozhlase, ocenění žáků za účast v soutěžích (nástěnka)
- Zveřejnění výsledků přijímacího řízení bez uvedení identifikátorů (pod kódem)
- Zapsání do knihy návštěv
- Pořadové číslo na poště



Co je osobní údaj?



- Fotografie
- IP adresa
- Podpis

Citlivé údaje:

- rasa
- etnický původ
- politický názor
- náboženské nebo filoz. vyznání
- členství v odborech
- zdravotní stavu
- sexuální orientace
- trestní delikty či prav. odsouzení
- genetické a biometrické údaje



Co je osobní údaj?

- osobní údaj = veškeré informace o identifikované nebo identifikovatelné fyzické osobě
- identifikovatelná fyzická osoba = fyzická osoba, kterou lze přímo či nepřímo identifikovat

ÚKOL: zadejte svoje jméno a příjmení do vyhledávání v google.com

I kombinace jména a příjmení vede k identifikaci osoby a je nutné je považovat za osobní údaj !!!!!



Jak poznat osobní údaj?

Pakliže údaj splní jednu z podmínek, jedná se o osobní údaj:

- 1) Jednoznačná identifikace – např. RČ
- 2) Účelem je identifikace – např. tel. číslo, IP adresa, MAC adresa, cookie, SPZ
- 3) Existuje „protikus“ – tzn. údaj je sám o sobě anonymní, ale existuje klíč k rozkódování - např. číslo žáka, číslo kreditní karty, otisk prstu



Co není osobní údaj?

Osobním údajem není:

- anonymizované údaje
- údaje zemřelých osob
- údaje získané v rámci činnosti čistě osobní povahy, které nemají obchodní či institucionální charakter

Příklad:

Výsledek přijímacího řízení na střední školu

ID žáka	Výsledky z ČJ	Výsledky z matematiky	Status
2017P001452	42	38	Přijat



Co je a není osobní údaj?

PŘÍKLADY:

Jméno, příjmení a e-mail zákonného zástupce žáka evidovaný ve školském informačním systému?

Služební telefon a služební e-mailová adresa třídních učitelů?

Zasílací adresa pro potvrzení odběru stravy ze školní jídelny?

Jméno a příjmení osoby, která vyzvedává dítě ze školní družiny?



Budou se muset školy GDPR zabývat?



Kdo nakládá s osobními údaji?

SPRÁVCE OSOBNÍCH ÚDAJŮ

- „určuje účely a prostředky zpracování osobních údajů“
tzn. říká co a jak se má evidovat a nese za to zodpovědnost

ZPRACOVATEL OSOBNÍCH ÚDAJŮ

- zpracovává osobní údaje pro správce

TŘETÍ STRANA

- není ani správcem ani zpracovatelem, ale má oprávněný zájem na zpracování osobních údajů



Kdo nakládá s osobními údaji?

■ SPRÁVCE



■ ZPRACOVATEL



■ TŘETÍ STRANA



Povinnosti správců a zpracovatelů

- Princip zodpovědnosti – nutno postupovat v souladu s GDPR (neznalost neomlouvá)
- Povinnost vést záznamy o zpracování OÚ (organizace s více jak 250 zaměstnanci nebo zpracovávající citlivé údaje)
- Povinnost nahlásit únik či ohrožení zabezpečení osobních dat Úřadu pro ochranu osobních údajů nejpozději do 72 hodin od okamžiku, kdy se o incidentu dozvěděli



Vztah správce a zpracovatele

- Správce musí vybrat důvěryhodného zpracovatele poskytujícího dostatečné záruky
- Zpracovatel může zpracovávat OÚ jen na základě pokynů správce
- Zpracovatel nesmí údaje dále zpracovávat pro vlastní účely (např. marketing)
- Je zakázáno řetězení zpracovatelů bez vědomí správce
- Zpracovatelská smlouva v písemné podobě



Náležitosti zpracovatelské smlouvy

- Závazek zpracování OÚ pouze na základě zdokumentovaných pokynů od zákazníka;
- Osoby, které mají oprávnění zpracovávat osobní údaje, se zavázaly dodržovat jejich důvěrnost nebo se na ně vztahuje zákonná povinnost mlčenlivosti;
- Přijetí všech opatření požadovaných článkem 32 GDPR (zabezpečení osobních údajů);
- Dodrží podmínky pro zapojení dalšího zpracovatele dle odstavců 2 a 4 článku 28 GDPR;
- Pomoc zákazníkovi prostřednictvím příslušných technických a organizačních opatření při plnění povinnosti správce reagovat na žádosti o uplatňování práv subjektu údajů stanovených v kapitole III GDPR;
- Pomoc zákazníkovi při zajištění shody s povinnostmi stanovenými články 32 až 36 GDPR s ohledem na povahu zpracování (zabezpečení OÚ a předchozí konzultace);
- Závazek odstranění nebo vrácení veškerých OÚ na konci poskytování služeb souvisejících se zpracováním a vymazání kopií;
- Poskytnutí informací nezbytných k prokázání shody s povinnostmi stanovenými v článku 28 GDPR (audity, inspekci prováděné zákazníkem nebo jím pověřeným auditorem);
- Informace správci v případě, pokud zjistí, že některý z pokynů správce porušuje obecné nařízení o zpracování osobních údajů nebo jiné právní předpisy.
- Oznamovací povinnost při bezpečnostních incidentech



Zabezpečení dat

- Organizační opatření – co nemáme, to nám nemohou ukrást
- Technická opatření – fyzické zabezpečení prostor, antivirová ochrana
- SW opatření
 - ANONYMIZACE = subjekt údajů nelze nijak identifikovat
 - PSEUDONYMIZACE = osobní údaje a další data existují odděleně, samy o sobě nedokáží subjekt údajů identifikovat

Výhoda – pseudonymizovaná data lze zpracovávat i nad rámec původně definovaného účelu.



Role školy v oblasti GDPR

- Správce osobních údajů žáků
- Správce osobních údajů zákonných zástupců
- Správce a zpracovatel osobních údajů zaměstnanců
- Jako veřejný subjekt musí ustanovit Pověřence pro ochranu osobních údajů
- Provést Posouzení vlivu na ochranu osobních údajů pokud provádí rozsáhlé zpracování zvláštních kategorií údajů
- Vést záznamy o činnostech, pokud zaměstnává více jak 250 osob nebo zpracovává zvláštní kategorie údajů





Právní důvody zpracování

- Nezbytné pro zákonnost zpracování
- Existují tyto důvody:
 1. Plnění smlouvy (např. obědy ve školní jídelně)
 2. Plnění právní povinnosti (např. školní matrika)
 3. Splnění úkolu prováděného ve veřejném zájmu (např. kontaktní údaje rodičů)
 4. Oprávněný zájem správce či třetí strany (např. kamerový systém)
 5. Ochrana životně důležitých zájmů (vážný úraz dítěte)
 6. Souhlas subjektu údajů pro jeden či více konkrétních účelů



Souhlas se zpracováním osobních údajů

- svobodný, konkrétní, informovaný a jednoznačný projev vůle
- poskytuje se k určitému **účelu** zpracování, který musí subjekt údajů znát
- musí být odlišen od jiných skutečností, ke kterým se subjekt údajů vyjadřuje.
- uzavření smlouvy nesmí být podmiňováno poskytnutím souhlasu
- subjekt údajů má právo svůj souhlas kdykoli odvolat

Veřejnost údajů nikdy a priori neznamená možnost jejich dalšího bezmezného zpracovávání.



Vzor souhlasu

Vyplněním a podpisem tohoto formuláře poskytnu ZŠ 123, se sídlem Ulice 12, Město, PSČ, IČO: 123 45 67 („ZŠ 123“), aby správci osobních údajů, souhlas se zpracováním níže uvedených osobních údajů, a to pro níže stanovené účely a dobu trvání.

Osobní údaj	Účel zpracování	Doba poskytnutí souhlasu	SOUHLAS*	
			ANO	NE
Fotografie žáka	Webové stránky školy, školní publikace, nástěnky, školní Facebook	10 let	ANO	NE
Audio či videozáznam žáka	Webové stránky školy, školní Facebook.	10 let	ANO	NE
Jméno, příjmení, třída žáka, dosažené výsledky	Informování o školních či mimoškolních akcích (soutěže, olympiády, sportovní, kulturní a umělecké akce) na webu, Facebooku školy, školních publikacích, nástěnkách a jiných veřejně dostupných prostorách ve škole.	10 let	ANO	NE
Jméno, příjmení, e-mailová adresa zákonného zástupce	Zasílání informací o doplňkových aktivitách školy (workshopy, nepovinné školní akce)	10 let	ANO	NE

Souhlas je udělen dle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, a Obecného nařízení o ochraně osobních údajů (2016/679) a to na výše uvedenou dobu od udělení souhlasu, příp. do odvolání tohoto souhlasu.

ZŠ a MŠ 123 je oprávněna zpracovávat osobní údaje manuálně i automatizovaně rovněž prostřednictvím určených zpracovatelů, jejichž aktuální seznam poskytne na vyžádání. Osobní údaje budou zpřístupněny pouze oprávněným zaměstnancům školy či zaměstnancům zpracovatele, a to pouze v míře nezbytné pro účely zpracování. Tento souhlas se zpracováním osobních údajů lze kdykoli písemně odvolat.

Svým podpisem tohoto formuláře prohlašuji, že jsem byl ZŠ a MŠ 123 informován o svých právech a povinnostech. Dále prohlašuji, že jsem byl poučen o tom, že poskytnutí osobních údajů prostřednictvím tohoto formuláře je zcela dobrovolné.



Souhlas s poskytnutím údajů

- Souhlas musí mít jasně definovaného správce (hlavičkový papír školy)
- Odvolání souhlasu musí být stejně pracné jako jeho udělení (písemné = písemné)

Souhlas není potřeba:

- Při plnění právní povinnosti
- Při oprávněném zájmu správce
- Při plnění či uzavření smlouvy (iniciované subjektem údajů)



Pověřenec pro ochranu osobních údajů

Povinně ustanoven pokud:

- zpracování provádí **orgán veřejné moci či veřejný subjekt** (bez ohledu na to, jaká data jsou zpracovávána)
- hlavní činnosti spočívají v operacích zpracování, které vyžadují **rozsáhlé pravidelné a systematické monitorování subjektů údajů**
- hlavní činnosti spočívají v rozsáhlém **zpracování zvláštních kategorií údajů** a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.



Pověřenec pro ochranu osobních údajů

- Poskytuje informace a poradenství správci či zpracovateli, včetně zaměstnancům, kteří se na zpracování podílejí
- Monitoruje soulad zpracování s GDPR
- Spolupracuje na tvorbě Posouzení vlivu na ochranu OÚ
- Spolupracuje s dozorovým úřadem (ÚOOÚ)
- Působí jako kontaktní místo pro dozorový úřad (škola uveřejní jméno a kontakt)
- Obrací se na něj subjekty údajů
- Vázán tajemstvím a důvěrností



Pověřenec pro ochranu osobních údajů

- Musí být jmenován na základě profesních kvalit
- Požadována je znalost práva a praxe v oblasti OÚ
- Legislativa taxativně nestanovuje potřebné vzdělání či certifikaci
- V ČR neexistuje certifikační orgán pro pověřence (ani se s ním do budoucna nepočítá)
- Aktuálně lze získat certifikaci European e-Competence Framework (e-CF) pro kompetenci definovanou Evropským Nařízením a Radou EU: General Data Protection Regulation

<http://www.tcox.cz/gdpr/kurz/poverenec-pro-ochranu-osobnich-udaju/>



Pověřenec pro ochranu osobních údajů

- Více škol či subjektů veřejné správy může jmenovat jediného pověřence, avšak ten musí být pro každý podnik snadno dosažitelný
- Musí být přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele
- Nedostává žádné pokyny týkající se výkonu jeho úkolů
- Nelze ho propustit ani sankcionovat za plnění jeho úkolů
- Lze nakoupit i jako externí službu



Práva subjektu údajů

1. Právo na informace o zpracování (proč někdo sbírá moje data)
2. Právo na opravu a doplnění (oprava neplatných dat)
3. Právo vznést námitku proti zpracování (správce musí prokázat zákonný důvod zpracování)
4. Právo na přenositelnost osobních údajů (strukturovaný, strojově čitelný formát)
5. Právo na výmaz /být zapomenut(zrušení souhlasu se zpracováním, smazání všech osobních dat)
6. Právo nebýt předmětem automatizovaného rozhodování (úvěr v bance, dopravní data)



Právo na informace o zpracování

Každý může zpracovatele požádat o informace o:

- účelu zpracování
- kategorii dotčených osobních údajů
- příjemci nebo kategorii příjemců, kterým osobní údaje byly nebo budou zpřístupněny
- plánované době, po kterou budou osobní údaje uloženy
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů
- informace, zda dochází k automatizovanému rozhodování, včetně profilování



Právo na opravu a doplnění

- Subjekt údajů má právo aby správce OÚ bez zbytečného odkladu opravil nepřesné osobní údaje či doplnil relevantní osobní údaje
- Povinnost aktivního vyhledávání nepřesných údajů však není správci legislativou určena

Obecně k výkonu práv subjektů:

- výkon práv je bezplatný (s výjimkou šikanózních žádostí)
- Výkon práva musí být uskutečněn bez zbytečného odkladu (30 dní max.)



Právo na výmaz / být zapomenut

Povinnost správce zlikvidovat osobní údaje, pokud je splněna alespoň jedna podmínka:

- údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány
- subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování
- subjekt údajů vznesl námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování
- osobní údaje byly zpracovány protiprávně
- osobní údaje musí být vymazány ke splnění právní povinnosti



ŠKOLA
ONLINE



SOFTWARE



Právo na přenositelnost

- Pokud je zpracování OÚ prováděno automatizovaně a je založené na souhlasu či smlouvě
- Netýká se zpracování na základě jiných právních důvodů tzn. netýká se orgánů veřejné moci
- Data by měla být poskytnuta ve strukturované formě a v běžně používaném a strojově čitelném formátu (např. CSV, XML)
- Subjekt údajů může žádat o předání dat i jinému správci a původní správce se tomu musí podřídít

Předání musí být bezplatné a ve lhůtě 1 měsíc



Porušení zabezpečení osobních údajů

Porušení zabezpečení je akt, který vede k náhodnému nebo protiprávnímu:

- zničení,
- ztrátě,
- změně,
- neoprávněnému poskytnutí,
- zpřístupnění,

přenášených, uložených nebo jinak zpracovávaných osobních údajů.

Pokud dojde k porušení zabezpečení osobních údajů, musí správce zvážit, zdali nejde o okolnost, kterou je nutné ohlásit dozorovému úřadu, resp. oznámit subjektu údajů.



Sankce a pokuty

- Každé porušení GDPR neznamená automatické uložení správní pokuty
- Budou zde instituty upozornění, napomenutí, nařízení ÚOOÚ
- Pokuty rozděleny do dvou skupin:

10 mil. EUR (nebo až do 2% ročního celosvětového obrátu) –
např. chyby v záznamech o činnostech

20 mil. EUR (nebo až do 4% ročního celosvětového obrátu) –
např. nezákonnost zpracování, chyby ve zpracování zvláštních kategorií údajů



Podmínky pro ukládání pokut

- Pokuty se ukládají podle okolností každého případu
- Sankce mají mít **preventivní** a nikoliv **likvidační účinek**
- Při stanovení výše se bere v potaz:
 - Povaha, závažnost a délka porušení povinnosti
 - Kategorie OÚ
 - Úmysl vs nedbalost
 - Kroky podniknuté ke zmírnění škod
 - Předchozí pochybení
 - Míra spolupráce s ÚOOÚ
 - Dodržování (existence) kodexu, osvědčení
 - **Přiznání je polehčující okolnost**



Jak implementovat GDPR na školách?

1. Mapování osobních údajů a procesů shromáždění a zpracování
2. Analýza souladu s GDPR – důvody zpracování
3. Zavedení nových metodik, směrnic, pravidel, postupů...
4. Jmenování Pověřence pro ochranu osobních údajů
5. Proškolení pedagogů v oblasti ochrany osobních údajů a řešení GDPR na škole



Vzorový harmonogram implementace

Harmonogram implementace GDPR na škole

Činnost	2/2018	3/2018	4/2018	5/2018	6/2018
Mapování osobních dat	X				
Stanovení právního důvodu zpracování	X	X			
Identifikace procesů s osobními daty	X	X			
Revize interních směrnic a metodik		X	X		
Zpracování vzorových souhlasů s poskytnutím osobních údajů		X	X		
Metodiky / opatření pro naplnění práv subjektu údajů			X	X	
Stanovení kontrolních mechanismů GDPR			X	X	
Jmenování pověřence pro ochranu osobních údajů			X	X	
Analýza fyzického zabezpečení, popis přístupu k datům	X	X	X		
Revize smluv se zpracovateli OÚ	X	X			
Proškolení pedagogů				X	X



Jak provést mapování?

- Důsledná analýza všech procesů školy a identifikace, jaké osobní údaje se kde vyskytují
- Pokud se účel zpracování liší, je třeba do analýzy zadat údaj vícekrát

Např. kontakt na rodiče

- a) informace zák. zástupcům o prospěchu,
- b) zasílání školního newsletteru

- Nezapomenout na všechny vedlejší činnosti školy
- Již ve fázi mapování identifikovat zvláštní kategorie údajů (citlivé údaje)



Kategorie osobních údajů na školách

- Údaje o žácích
- Údaje o zákonných zástupcích
- Údaje o zaměstnancích
- Údaje o uživatelích přidružených služeb (pronájem tělocvičny, cizí strážníci ve Šj apod.)
- Běžné osobní údaje
- Zvláštní kategorie údajů (citlivé údaje)
 - Školní poradenské pracoviště (IVP, psycholog, prevence šikany)
 - Školní jídelna (speciální dieta)



Jak provést mapování:

- Celý proces implementace GDPR vést jako projekt (termíny, úkoly, pravidelné porady)
- Oslovit klíčové nositele informací (ředitel, zástupce, vedoucí ŠJ, vedoucí ŠD, sekretářka, účetní, výchovný poradce)
- Postupovat po částech – výčet OÚ, navázání na proces, přiřazení účelu, oponentura, doplnění výčtu ...
- Mapování začít od informačních systémů (ukládáme do nich většinu dat)



Mapování právních důvodů

- u každého údaje definujeme právní důvod proč jej potřebujeme

Osobní údaj	Zvláštní kategorie údajů	Právní důvod zpracování					
		Plnění právní povinnosti	Veřejný zájem	Plnění smlouvy	Oprávněný zájem	Udělení souhlasu	Ochrana životně důležitých zájmů
Příjmení	NE	561/2004					
Jméno	NE	561/2004					
Rodné číslo	NE	364/2005					
Pohlaví	NE	364/2005					
Část školy	NE				ANO		
Číslo v třídním výkazu	NE				ANO		
Třída	NE	364/2005					
Datum narození	NE	Jen pokud nemá RČ.	ANO				
Místo narození	NE	561/2004					
Okres narození	NE	561/2004					
Stát narození	NE	561/2004					
Číslo OP	NE					ANO	
Kvalifikátor st. občanství (ČR x cizinec)	NE	364/2005					
Státní občanství	NE	364/2005					
Číslo pasu	NE					ANO	
Školní e-mail	NE				ANO		
Datová schránka	NE					ANO	
Ulice trvalého bydliště	NE	364/2005					
Číslo popisné / orientační TB	NE	364/2005					
Obec TB	NE	364/2005					



Právní důvody sběru OÚ na školách

- bude převažovat **plnění právní povinnosti správce** nebo **plnění úkolu ve veřejném zájmu**
- pro kamerové záznamy, zabezpečení vstupu do objektů **oprávněné zájmy správce**
- data o cizích strávnících, nájemcích školních prostor **plnění smlouvy**
- zveřejnění fotografií **souhlas subjektů údajů**



Analýza procesů

- Kdo a jak získává osobní data?
- Kdo k nim má přístup?
- Jak jsou data zabezpečena proti ztrátě, pozměnění, kompromitaci?
- Jak jsou vyřešeny souhlasy?
- Jak jsou informováni a proškoleni zaměstnanci?
- Existuje metodika ochrany OÚ?
- Jak je proces ochrany kontrolován?



Ukázka analýzy procesů – data žáků

Identifikace procesu	Popis procesu	Obs. citlivé údaje	Práv. důvod	Forma	Odpov. zprac.	Přístup pro editaci	Přístup pro čtení	Uložení	Skartace
Katalogové složky žáků	Evidence žáků, zákonných zástupců, informace o prospěchu, docházce, kontaktní údaje, údaje o zdravotním znevýhodnění, zapsané předměty	ANO	PPP	E	SOL	TU, A	TU, A, U	Cloud	A45
Třídní výkaz	Evidence žáků třídy, obsahuje jméno a příjmení žáka + anonymizovaný přehled o prospěchu a chování	NE	PPP	E	SOL	TU, A	TU, A	Cloud	A45
Třídní kniha	Obsahuje označení třídy, seznam žáků, seznam pedagogů, docházku	NE	PPP	E	SOL	TU, A, U	TU, A, U	Cloud	S10
Výstupy z IS - tisk vysvědčení	Osobní údaje žáka a informace o prospěchu, chování a zameškaných hodinách	NE	PPP	P	TU	TU	TU, Ř, R, Ž	AŘ	S3
Příhláška na ZŠ + rozhodnutí o přijetí	Osobní údaje žáka a jeho zákonných zástupců	může	PPP	P	Ř	Ř, PU	Ř, PU	AŘ	S20
Evidence docházky do ŠD, ŠK	Třídní kniha ŠD / docházkový sešit	NE	PPP	P	V	V	V	AA	S3
Seznam osob pro vyzvednutí z družiny	Obsahuje jméno a příjmení	NE	VZ	P	V	V	V	AA	S3
Evidence strážníků - vlastních	Seznamy dětí a učitelů stravující se ve ŠJ	NE	PPP	E	VŠJ	VŠJ	VŠJ, K	AA	S3



Ukázka analýzy procesů – škola jako zaměstnavatel

Kategorie	Popis	Osobní údaje	Zákonnost zpracování	Kategorie typu zpracování	Místo uložení dat	Dostupnost dat	Skartační doba
Osobní spisy zaměstnanců	Spis v papírové podobě. Osobní dotazník vyplněný zaměstnancem při nástupu.	Jméno Příjmení (i rodné) Místo narození Trvalé bydliště Datum narození Rodné číslo Informace o rodinných příslušnících Vzdělání a dovednosti Státní příslušnost Rodinný stav Pracovní historie	Plnění právní povinnosti	Systematické shromáždění údajů pro dlouhodobý účel	Písemný dokument - kancelář mzdové účetní.	Ředitel Personalista/ka Mzdová účetní	3 roky po ukončení pracovního poměru
Hodnocení zaměstnanců	ŘÚ a VP zpracovávají na předepsaných formulářích čtvrtletní a roční hodnocení zaměstnanců. Zde se uvádí minimálně jméno a příjmení. Může obsahovat citlivé informace jako např. výše platu atd.	Jméno Příjmení Plat (výše odměny)	Plnění právní povinnosti	Systematické shromáždění údajů pro dlouhodobý účel	Aktuální hodnocení má k dispozici ŘÚ, VP. Starší data jsou předávána do osobního spisu do kanceláře mzdové účetní.	Ředitel Zástupce ředitele Personalista/ka Mzdová účetní	3 roky po ukončení pracovního poměru
Životopis při přijímacím řízení	V písemné podobě založen v personálním spisu	Může obsahovat i fotografii a citlivé údaje, pokud je pracovník dobrovolně uvede	Oprávněný zájem správce údajů	Systematické shromáždění údajů pro dlouhodobý účel	Písemný dokument v personálním spise - kancelář mzdové účetní.	Personalista/ka Mzdová účetní	3 roky po ukončení pracovního poměru



Škola jako zaměstnavatel

- Zaměstnavatel smí shromažďovat pouze takové osobní údaje, které jsou nezbytné pro plnění povinnosti zaměstnavatele (výpočet mzdy, odvody pojistného atd.)
 - Jméno a příjmení (vč. dřívějších)
 - Datum a místo narození
 - Rodné číslo
 - Číslo občanského průkazu
 - Místo trvalého pobytu
 - Zdravotní pojišťovna
 - Jméno a příjmení manžela/ky, název a adresa zaměstnavatele
 - Jméno, příjmení a rodné číslo dítěte
 - Vzdělání a předchozí praxe
 - Zdravotní znevýhodnění a pobíraný důchod
 - Počet dětí
 - Státní občanství



Škola jako zaměstnavatel

- Zaměstnavatel smí s údaji pracovat jen pro účely, ke kterým je získal (nemůže tedy např. prodat adresy/telefony svých zaměstnanců MKT firmě)
- Musí učinit taková opatření, aby nemohlo dojít k neoprávněnému přístupu k osobním údajům
 - Definovat oprávněné osoby
 - Definovat přístupy
 - Fyzické zabezpečení dat
 - Logování přístupů k datům



Organizační opatření při zavedení GDPR

- Revize interních procesů
 - Organizační řád
 - Směrnice pro nakládání s osobními údaji
 - Bezpečnostní směrnice
 - Vzorový souhlas s poskytnutím OÚ
- Revize smluv s dodavateli
 - Informační systémy
 - Dodavatelé IT služeb (správa sítě, databází, webu)



Organizační opatření při zavedení GDPR

- Revize zaměstnaneckých vztahů
 - U vybraných profesí zakotvit povinnost mlčenlivosti a důvěrnosti do samostatného dokumentu
 - Získat souhlasy zaměstnanců se zpracováním OÚ (např. foto, soukromý telefon)
- Fyzické zabezpečení
 - Počítače, servery
 - Místa pro ukládání dokumentů, archiv



Cloud vs server

CLOUD

Výhody

- Vždy nejnovější HW a operační / db. SW
- Antivirová ochrana na nejvyšší úrovni
- Dokonalé fyzické zabezpečení
- Zdroj el. energie 24/7
- Řízené zálohování
- Geograficky redundantní zálohy
- Disaster recovery management

Nevýhody

- Data nemáte pod kontrolou, je třeba spoléhat na serióznost poskytovatele
- Závislost na internetovém připojení

SERVER

Výhody

- Data pod přímou kontrolou
- Data vždy lokálně dostupná

Nevýhody

- Udržení vysokého technického standardu je časově i finančně nákladné
- Fyzické zabezpečení jen pasivní
- Záložní zdroj energie jen dočasný
- Zálohování složité a náročné na čas
- V případě problému delší čas na obnovu dat



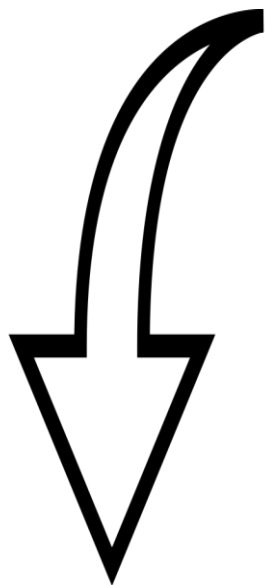
Organizační opatření při zavedení GDPR

- Udělat si pořádek a postupovat dle platných metodik
 - Archivace a skartace
 - Dodržovat přístupy k datům, metoda „prázdného stolu“
- Proškolení zaměstnanců
 - Pověřenec pro ochranu osobních údajů
 - Osoby pracující s citlivými údaji
 - Řadoví učitelé, vychovatelé



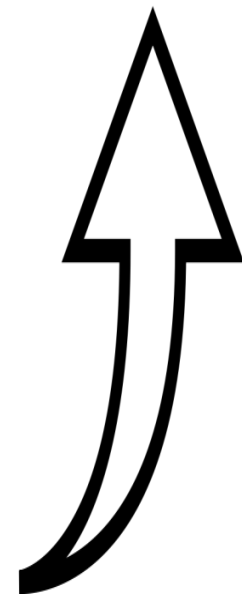
Možnosti implementace GDPR compliance

CENA



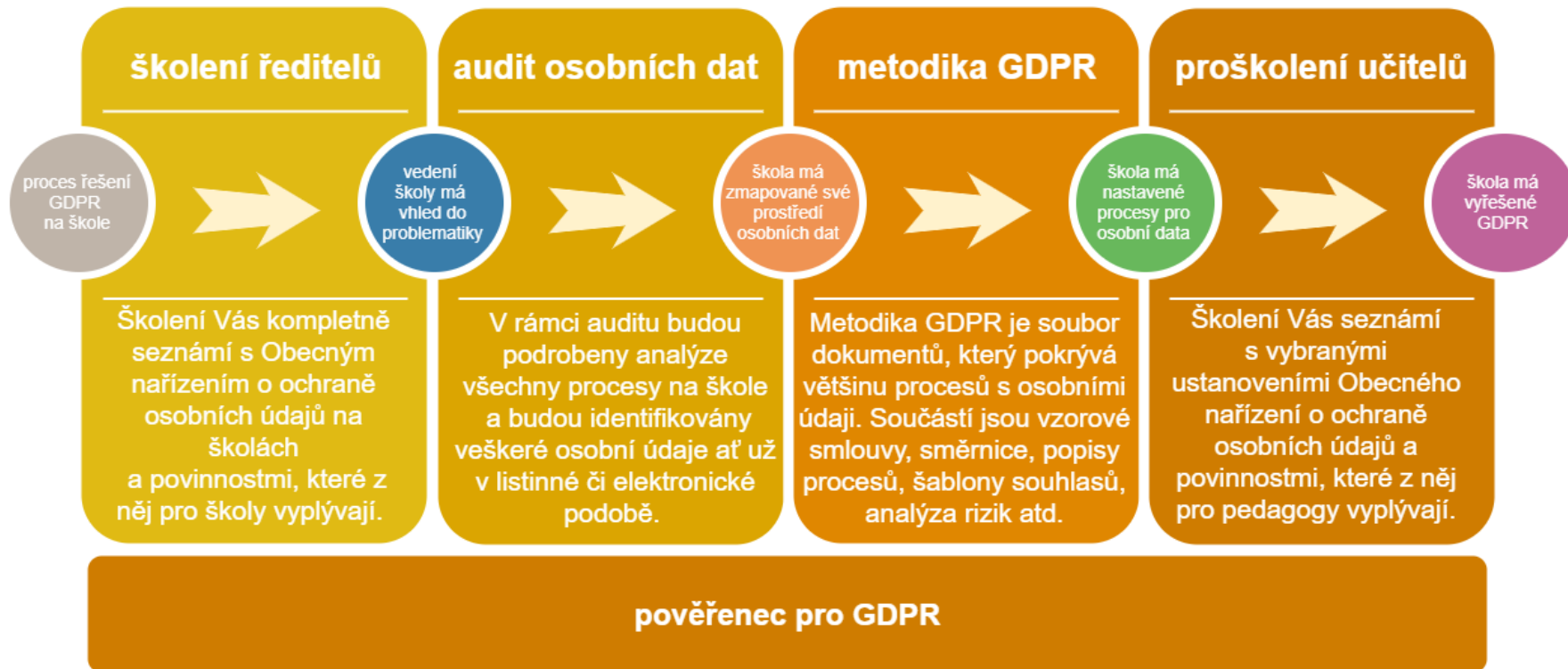
- Vše vymyslet a zrealizovat sám
- Inspirovat se jinými školami
- Postupovat dle metodiky MŠMT + vzorový audit
- Koupit komerční produkt a přizpůsobit jej potřebám školy
- Najmout si specialistu
- Najmout si právníka

ÚSILÍ



Služby ŠKOLA ONLINE a.s.

konzultační služby k GDPR



pověřenec pro GDPR

<http://www.skolaonline.cz/GDPR/>



Diskuse a dotazy

