

„ŠKOLENÍ PŘÍSPĚVKOVÝCH ORGANIZACÍ –
VSTUPNÍ A ROZDÍLOVÁ ANALÝZA DLE
POŽADAVKŮ GDPR“



Krajský úřad Libereckého kraje

GDPR

5. 2. 2018

prezentující: Miroslav Pavelka

„ŠKOLENÍ PŘÍSPĚVKOVÝCH ORGANIZACÍ – VSTUPNÍ A ROZDÍLOVÁ ANALÝZA DLE POŽADAVKŮ GDPR“



Tato prezentace byla vypracována výlučně pro potřeby osobní prezentace autora při současném slovním výkladu problematiky GDPR pro účel akce „ŠKOLENÍ PŘÍSPĚVKOVÝCH ORGANIZACÍ – VSTUPNÍ A ROZDÍLOVÁ ANALÝZA DLE POŽADAVKŮ GDPR“ konané 5.2.2018 v prostorách Krajského úřadu Libereckého kraje. Prezentace zohledňuje stav problematiky k 31.1.2018. Prezentaci je možno využít pouze pro potřeby KRAJSKÉHO ÚŘADU LIBERECKÉHO KRAJE a pro potřeby jeho příspěvkových organizací. Bez předchozího svolení autora není možné využívat prezentaci, ani její části, pro jiné účely.

Miroslav Pavelka

Program



- **9:00 – 10:00**
 - Úvodní slovo ředitele KÚ LK
 - Informace o GDPR týmu KÚ LK
 - Představení DPO - Pověřence pro ochranu osobních údajů
 - Strategie a rozsah pomoci Příspěvkovým organizacím
 - GDPR - vysvětlení základních pojmů
 - Anonymizace, pseudonymizace
- **10:00 – 10:15**
 - PŘESTÁVKA
- **10:15 – 11:15**
 - Účely zpracování z pohledu GDPR
 - Zajištění DPO
 - Harmonogram spolupráce
 - Kontaktní informace pro vzájemnou komunikaci
 - Další nařízení EU ve vazbě na GDPR (eIDAS, ePrivacy)
 - Školení a kontroly
- **11:15 – 11:45**
 - Praktické informace, diskuze, zpětná vazba

Pomoc příspěvkovým organizacím

- Příprava na vstupní analýzu
 - jak začít „zkoumat a sledovat“ procesy zpracování osobních dat
 - jak začít „uklízet“ ve své organizaci

- Sdílení informací
 - zasílání „přeložených“ výkladových stanovisek
 - pravidelné odpovědi na Vaše dotazy!
 - zpracování Vašich podnětů
 - metodická pomoc
 - doplňky do směrnic
 - dodatky ke smlouvám / návrhy vnitřních předpisů
 - instrukce

- Kam to všechno psát?
 - obdržíte od nás tabulku obsahující mnoho předvyplněných vzorů zpracování osobních dat

Pomoc příspěvkovým organizacím

- Zachování zdravého rozumu
 - Nepodléhejte panice a zejména ne dezinformaci o nesmyslných pokutách (až 20 mil. €), realita pro veřejné subjekty je jiná.
 - Platná česká právní úprava (ZOOÚ 101/2000 Sb.) již nyní definuje pokuty až 10 mil. Kč a nový návrh zákona (ZZOÚ) na této skutečnosti pro veřejné subjekty nic nemění.
 - K udělování vysokých pokut dochází zřídka, nicméně se musíte připravit na situaci, kdy může někdo cíleně využít možné slabiny v ochraně osobních údajů ve Vaší organizaci. (např. zaměstnanec, dodavatel, stěžovatel...)

Pomoc příspěvkovým organizacím

- Co se stane po 25. 5. 2018?
- Co se stalo 4. 4. 2000, kdy Zákon 101/2000 Sb. vstoupil v platnost?
- Co se stalo po mnoha novelách Zákona 101?

... školy dál učí

... nemocnice léčí

... knihovny a muzea mají otevřeno

Pomoc příspěvkovým organizacím

- Pozor na obhájení příliš nákladných změn a rozsáhlých investic při implementaci GDPR
 - Zákon 101/2000 Sb. již nyní řeší ochranu osobních údajů poměrně komplexně a pokud je dodržován ...
 - Nejsme tu od toho, abychom Vás šikanovali nesmyslnými požadavky, ale pomohli Vám.
 - Nebudeme Vás strašit hrozbou pravidelných přísných kontrol, dodržování nařízení GDPR a souvisejících zákonů je zodpovědností ředitele.
 - Případné první audity a kontroly v oblasti ochrany osobních dat budou interní a vedené spíše formou poradenství.

GDPR - základní informace a pojmy

■ **General Data Protection Regulation**

- Nařízení EP a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, nahrazuje směrnici 95/46/ES.
- Vztahuje se na všechny veřejné subjekty, právnické osoby a fyzické osoby podnikající, které poskytují služby nebo zboží občanům EHP (EU28 + Island, Norsko a Lichtenštejnsko)

GDPR - základní informace a pojmy



Nařízení je přímo účinné...

...tedy pokud „neuděláme“ nic, bude platit bez důležitých úprav.

Návrh zákona o zpracování osobních údajů...

... „musí“ být schválen před účinností nařízení GDPR, byl předán (22.1. 2018) k projednání Legislativní radě vlády

...nahradí zákon o ochraně osobních údajů, je adaptovaný na nařízení GDPR 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680

(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).

GDPR - základní informace a pojmy



Návrh zákona o zpracování osobních údajů...

...nahradí zákon o ochraně osobních údajů, je adaptovaný na nařízení GDPR 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680 (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).

Budeme neustále sledovat vývoj legislativy a informovat Vás o všech důležitých změnách!

Informace budeme pravidelně zveřejňovat na portálu EDULK.cz !

GDPR - základní informace a pojmy

- Celé nařízení je napsané velmi obecně a dává prostor pro různé výklady ustanovení.
- Pomoci mají vodítka vydávaná pracovní skupinou „WP29“ - Working Party
(pracovní skupina podle čl. 29 směrnice 95/46/ES)
- Do dnešního dne však stále nevyšla, nebo nebyla přeložena, všechna přislíbená výkladová stanoviska a související metodické pokyny ministerstev.
- Proto se proces implementace GDPR neustále vyvíjí a dochází při něm k mnoha nejasnostem.

GDPR - základní informace a pojmy



- **Osobní údaj...**

...je každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů), jestliže lze subjekt údajů přímo či nepřímo pomocí tohoto údaje identifikovat

- **Subjekt údajů...**

je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

- **Citlivé osobní údaje...**

... mohou subjekt údajů samy o sobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci.

Národnostní, rasový nebo etnický původ, politické postoje, členství v politických stranách či hnutích nebo odborových či zaměstnaneckých organizacích, náboženství a filozofické přesvědčení, údaje o trestné činnosti, zdravotní stav a sexuální život.

(tzv. zvláštní kategorie osobních údajů)...

Zpracování zvláště citlivých osobních údajů



- Citlivé osobní údaje lze zpracovávat v případech, kdy ...

... je zpracování nezbytné pro plnění povinností v oblasti pracovního práva, práva sociálního zabezpečení a sociální ochrany

... byl udělen výslovný souhlas subjektu údajů

... je to nezbytné pro ochranu životně důležitých zájmů subjektu (např. v situaci, kdy subjekt není schopen udělit souhlas)

... údaje prokazatelně zveřejnil sám subjekt údajů

... je to ve veřejném zájmu (na základě EU nebo národního práva) nebo v oblasti veřejného zdraví

... je zpracování nutné pro obhájení právních nároků (např. trestní řízení)

... je to nutné pro posouzení pracovní schopnosti zaměstnanců, účely preventivního nebo pracovního lékařství, lékařské diagnostiky, poskytování zdravotní nebo sociální péče

... je to nezbytné pro účely vědeckého či historického výzkumu nebo statistické účely ve veřejném zájmu

GDPR - základní informace a pojmy



- **Správce osobních údajů**
 - sám nebo společně určuje účely (na základě čeho) a prostředky zpracování (formu)
 - za zpracování primárně zodpovídá
- **Zpracovatel osobních údajů**
 - pro správce zpracovává osobní údaje, buď na základě zákona nebo pověření Správce
- **Zpracování osobních údajů**
 - jakákoli operace (soubor operací) s osobními údaji
shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení
- **Vztah Správce x Zpracovatel**
 - vždy písemná smlouva (i elektronicky uzavřená)
 - pokud je určen zákonem, možno bez smlouvy
 - Správce určuje pravidla, má auditní právo
 - Správce rozhoduje i o případném „Sub-zpracovateli“

Povinnosti Správce osobních údajů



1. **Minimalizace** - zpracovávat pouze osobní údaje nezbytné pro daný účel, v nezbytně nutném rozsahu, přiměřeně a pouze pro nutnou dobu
2. **Přesnost** - zajistit maximální přesnost a aktuálnost zpracovávaných osobních údajů
3. **Bezpečnost** - zajistit údaje před neoprávněným či nezákonným zpracováním a náhodnou ztrátou, zničením nebo poškozením
4. **Dokumentace** - vést záznamy o zpracování a doložit svůj soulad s nařízením a zákony ČR
5. **Data protection by design** - počítat s ochranou osobních údajů již od počátku návrhu praktického řešení jejich zpracování
(může se jednat o technická řešení typu anonymizace, pseudonymizace a rozdělení oblastí s uloženými daty, nebo personální a organizační opatření)
6. **Transparentnost** - plnit informační povinnost vůči subjektu údajů (např. oznamovat úniky osobních dat aj.)
7. **Umožnit subjektu údajů realizovat svá práva** (např. vytvoření kopie zpracovaných osobních údajů, zajistit přenositelnost údajů, omezit zpracování osobních údajů aj.)
8. **Oznámit všem příjemcům osobních údajů informace** - ohledně opravy, výmazu osobních údajů nebo omezení zpracování
9. **Kontrolovat Zpracovatele**

Povinnosti Zpracovatele osobních údajů



1. **Dodržovat pokyny Správce** - zpracovávat a uchovávat osobní údaje pouze dle doložených pokynů Správce
2. **Postupovat dle smlouvy** - jednat v zásadě pouze v rozsahu písemné smlouvy se Správce
3. **Spolupracovat se správcem** - být Správci nápomocen při dodržování povinností vyplývajících z práv subjektů údajů, provádění posouzení vlivu na ochranu osobních údajů, vést záznamy o všech kategoriích činností zpracování prováděných pro Správce
4. **Součinnost s ÚOOÚ** - poskytnout záznamy na požádání dozorového úřadu
5. **Zajistit mlčenlivost** - zavázat osoby zpracovatele oprávněné zpracovávat osobní údaje Správce k mlčenlivosti
6. **Vzdělávání** – zajistit dostatečné proškolení osob, které zpracovávají osobní údaje
7. **Bezpečnost** – zajistit údaje před neoprávněným či nezákonným zpracováním a náhodnou ztrátou, zničením nebo poškozením

GDPR a práva subjektů údajů



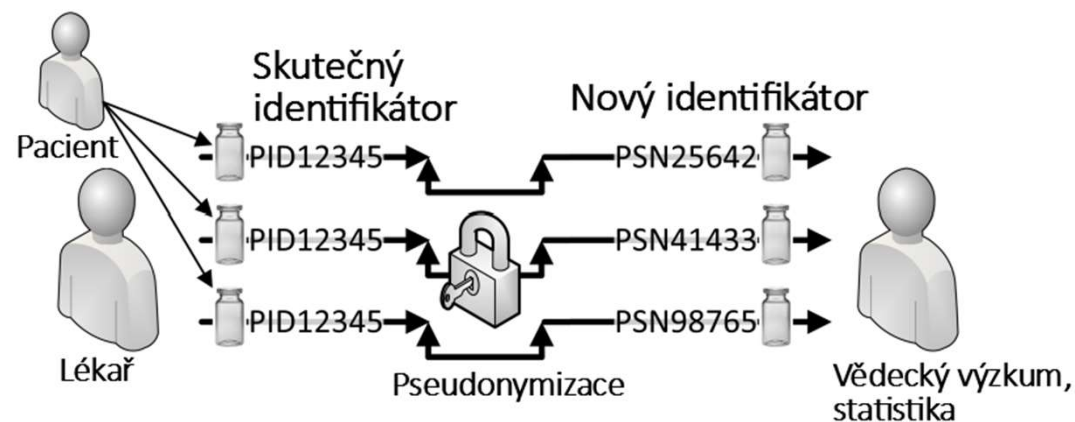
Subjekt údajů je často ve slabším postavení než správce a práva definovaná nařízením GDPR tak vybalancovávají vztah mezi ním a správcem údajů. Pozor na dodržování lhůty pro reakci na podněty subjektů údajů (30 dnů)!

Subjekt údajů má právo:

1. být informován o zpracování jeho osobních údajů
např. zda jsou či nejsou údaje zpracovávány
2. na přístup k osobním údajům
např. informace o účelu zpracování, totožnosti správce, o jeho oprávněných zájmech, o příjemcích osobních údajů, plánované době uložení a zpracování, o příjemcích s přístupem k údajům
3. na opravu (doplnění)
4. na výmaz (být zapomenut)
5. na omezení zpracování (např. pro potřeby vyšetřování)
6. přenositelnost údajů (přenos k jinému správci)
7. vznést námitku
8. nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování

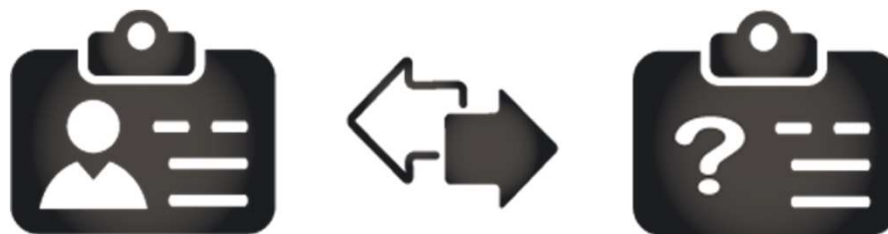
Pseudonymizace

- Zpracování osobních údajů způsobem, že nemohou být bez dodatečných informací přiřazeny konkrétnímu subjektu.



- Dodatečné informace je třeba uchovávat odděleně!
- Je třeba přijmout taková opatření, aby přidělení ke konkrétnímu subjektu může provést jen pověřená osoba!
- I šifrování je určitou formou pseudonymizace !
- Výrazné snížení dopadu na ochranu osobních dat a omezení práv subjektů údajů! Jejich práva jsou podmíněna schopností subjektu identifikovat! (např. oznamovací povinnost v případě bezpečnostního incidentu)

Anonymizace



- Zpracování osobních údajů způsobem, že nemohou být již nikdy přiřazeny konkrétnímu subjektu a jeho identifikaci ani nenapomáhají.
- Vhodné pro statistické účely, výzkum...
- **NUTNÉ** např. pro REGISTR SMLUV nebo zveřejňování informací podle zákona 106/1999 Sb.
(Zákon o svobodném přístupu k informacím)

■ Jeden z postupů anonymizace

Anonymizované údaje se zcela překryjí (začerní) nebo odstraní, aby je nebylo možné přečíst. Není-li z textu jednoznačně poznatelný obsah anonymizovaného údaje, připojí se k anonymizovanému údaji charakter anonymizovaného údaje (např. „datum narození“, „rodné číslo“, „adresa“, „číslo účtu“ apod.), a to například formou poznámky vložené do dokumentu. U elektronické verze je nutné dbát na sloučení vrstev a odstranění metadat.

DAROVACÍ SMLOUVA

Bytem: [redacted]
Rodné číslo: [redacted]
Číslo účtu: [redacted]
(dále jen „dárce“)

a

Divadlo Na nebi, příspěvková organizace
Sídlo: Virtuální 1, 110 01 Praha 1
IČ: 00319741
Zastoupená: Ing. Josef Novotný, ředitel email: [redacted]
číslo účtu: [redacted]
(dále jen „obdarovaný“)

uzavřeli níže uvedeného dne, měsíce a roku tuto
darovací smlouvu
podle §2055 a násl. zákona č. 89/12 Sb., občanského zákoníku

1. Dárce daruje obdarovanému finanční částku ve výši 50 000 Kč a to převodem z účtu dárce na účet obdarovaného.
2. Dárce osobně předá dar obdarovanému nejpozději do 30 dnů od podpisu této smlouvy.
3. Obdarovaný předmět darovací smlouvy přijímá a současně souhlasí se způsobem a lhůtou předání daru.
4. Obdarovaný bere na vědomí možnost odvolání daru z důvodů stanovených platným právním předpisem.
5. Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami. Smlouva je uzavřena ve dvou vyhotoveních, po jednom pro každou ze smluvních stran.
6. Smluvní strany prohlašují, že si tuto smlouvu před podpisem přečetly, že s jejím obsahem souhlasí a na důkaz toho připojují své podpisy.

V Praze, dne 26.4.2013
[redacted]
dárce

V Praze, dne 26.4.2013
[redacted]
Ing. Josef Novotný
ředitel

GDPR – bezpečnostní incident

- Porušení zabezpečení - náhodné nebo protiprávní zničení, ztráta, změna nebo neoprávněné poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních dat.
- Správce osobních údajů má povinnost ohlašovat dozorovému úřadu či oznamovat subjektu údajů tzv. případy porušení zabezpečení osobních údajů!
- Správce musí oznámení učinit (pokud možno) do 72 hodin. Pokud není možné ohlášení učinit ve této lhůtě, musí to správce zdůvodnit!



Proces oznamování řídí DPO, pokud je stanoven.



GDPR – právní důvody zpracování dat



- Základním předpokladem pro LEGÁLNÍ zpracování osobních dat je PRÁVNÍ DŮVOD!
- Data se zpracovávají pro různé účely a pro každý tento účel musí být zřejmý právní základ.

Účely zpracování:

1. SOUHLAS
2. PLNĚNÍ SMLOUVY
3. PRÁVNÍ POVINNOST
4. OPRÁVNĚNÝ ZÁJEM
5. VEŘEJNÝ ZÁJEM
6. ŽIVOTNĚ DŮLEŽITÝ ZÁJEM
7. ZVLÁŠTNÍ PRÁVNÍ DŮVOD PRO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ VEŘEJNOU SPRÁVOU

Aplikace GDPR pro mobilní telefony



Explore GDPR

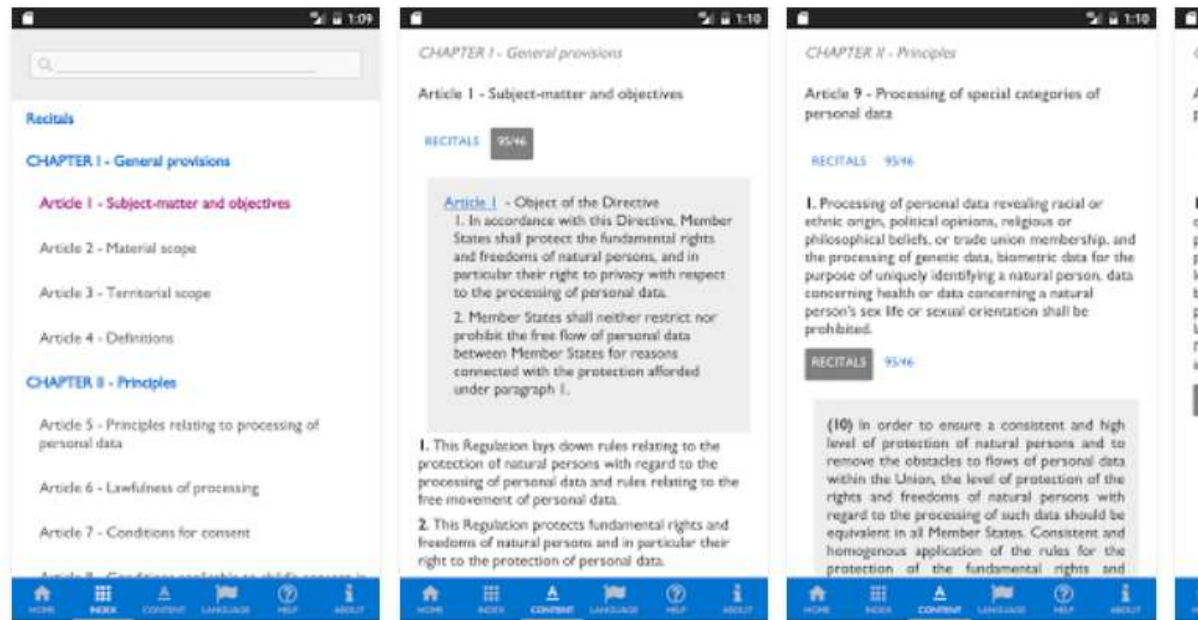
DLA Piper UK LLP Byznys

★★★★★ 25

PEGI 3

Přidat do seznamu přání

Nainstalovat



GDPR – právní důvody zpracování dat



- Základním předpokladem pro LEGÁLNÍ zpracování osobních dat je PRÁVNÍ DŮVOD!
- Data se zpracovávají pro různé účely a pro každý tento účel musí být zřejmý právní základ.

Účely zpracování:

1. SOUHLAS
2. PLNĚNÍ SMLOUVY
3. PRÁVNÍ POVINNOST
4. OPRÁVNĚNÝ ZÁJEM
5. VEŘEJNÝ ZÁJEM
6. ŽIVOTNĚ DŮLEŽITÝ ZÁJEM
7. ZVLÁŠTNÍ PRÁVNÍ DŮVOD PRO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ VEŘEJNOU SPRÁVOU

GDPR – právní důvody zpracování dat



▪ SOUHLAS

Dle nařízení GDPR může souhlas udělit subjekt údajů starší 16 let.

Dle návrhu české legislativy je to **13 let!** (může ještě dojít ke změně)

Souhlasem se rozumí **svobodný, konkrétní, informovaný a jednoznačný** projev vůle.

Může být učiněn písemně, elektronicky i ústně.

POZOR!

Souhlas se snažte využívat jen v nouzi. Poskytnutí služby veřejným subjektem nesmí být podmíněno udělením souhlasu.

„Vyžadujte ho pouze pro údaje, které chcete, ale nepotřebujete!“

Souhlas lze kdykoliv odvolat, proto je nutné vést záznamy o činnosti a být připravený na případný výmaz.

Za osoby mladší 13 let je nutné vyžadovat souhlasy zákonných zástupců.



Neudělení souhlasu nesmí mít pro subjekt žádný dopad (neposkytnutí služby, znevýhodnění aj.)

GDPR – právní důvody zpracování dat

- **PLNĚNÍ SMLOUVY**

Je možné zpracovávat osobní data nezbytná pro plnění smlouvy nebo pro přípravu smlouvy, pokud je to na žádost klienta (subjektu údajů).

Např.: dodávky zásilek, služeb, fakturace, komunikace s klientem.

Nevztahuje se na marketing a vyhledávání potenciálních klientů!
Právní titul **zaniká s ukončením smlouvy!**

Neznamená to nutně, že musí být smazána všechna data. Pro některá může být použitelný jiný právní titul, další zpracování může být i oprávněným zájmem.



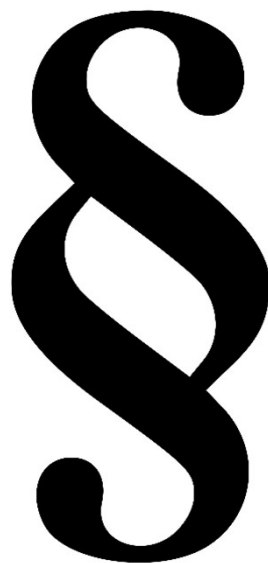
GDPR – právní důvody zpracování dat



▪ PRÁVNÍ POVINNOST

Tento účel použijeme, pokud je zpracování nezbytné pro splnění právní povinnosti, která se na správce vztahuje. Velmi častý účel zpracování pro veřejné subjekty a orgány veřejné moci!

*Např.: Školský zákon č. 561/2004 Sb.
Zákon o účetnictví č. 563/1991 Sb.
Zákoník práce č. 262/2006 Sb.*



GDPR – právní důvody zpracování dat

▪ OPRÁVNĚNÝ ZÁJEM

Oprávněné zájmy správce, včetně správce, jemuž mohou být osobní údaje poskytnuty, se mohou stát právním základem zpracování za předpokladu, že nepřevažují zájmy subjektu údajů.

Např.: zpracování osobních údajů nezbytně nutné pro účely zamezení podvodům, krádežím, vyzrazení tajemství, ochrany majetku (kamerové systémy), logování přístupů

Široký právní základ s jistou mírou rizika

POZOR!

Proti zpracování lze vznést námitku na základě osobní situace subjektu údajů. Při námitce je třeba omezit zpracování a při vyhovění námitce (negativní výsledek testu přiměřenosti) údaje smazat.



GDPR – právní důvody zpracování dat



■ VEŘEJNÝ ZÁJEM

Zpracování nezbytné ke splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci.

Tento účel zpracování by měl mít základ v právu členského státu nebo EU.

Aplikovatelný zejména ve veřejné a státní správě.

(např. vláda, ministerstva, samospráva – obce a kraje, složky integrovaného záchranného systému aj.)

Informační povinnost vůči subjektům osobních údajů zpracovávaných při povinnosti správce nebo jeho úkolu ve veřejném zájmu, nebo o zpracování při výkonu jeho pravomoci, je splněna i uveřejněním informací na webových stránkách.

■ ŽIVOTNĚ DŮLEŽITÝ ZÁJEM

Zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.

Definice

OVM / veřejný subjekt



▪ VEŘEJNÝ SUBJEKT

GDPR přímo nedefinuje, co znamená „orgán veřejné moci nebo veřejný subjekt“, toto má být dle stanoviska WP29 určeno vnitrostátními právními předpisy. Návrh ZZOÚ uvádí, že veřejné úkoly mohou vykonávat a veřejnou moc uplatňovat nejen orgány veřejné moci a veřejné subjekty, ale také fyzické nebo právnické osoby veřejného nebo soukromého práva, a to v závislosti na vnitrostátní právní úpravě v každém členském státu, v odvětvích jako služby veřejné dopravy, dodávky vody a energie, silniční infrastruktura, veřejnoprávní vysílání a obecní bydlení, nebo disciplinárními orgány pro regulovaná povolání.

Subjekt, který je založen nebo zřízen za zvláštním účelem uspokojování potřeb obecného zájmu, který nemá průmyslovou nebo obchodní povahu, má právní subjektivitu, a zároveň je financován převážně (tj. z více než 50 %) státem, regionálními nebo místními orgány nebo jinými veřejnoprávními subjekty, nebo je těmito orgány řízen, nebo je v jeho správním, řídicím nebo dozorčím orgánu více než polovina členů jmenovaná státem, regionálními nebo místními orgány nebo jinými veřejnoprávními subjekty. Jde zejména o Českou republiku, státní příspěvkovou organizaci, územní samosprávný celek nebo příspěvkovou organizaci, u níž funkci zřizovatele vykonává územní samosprávný celek, nebo jinou právnickou osobu, pokud byla založena či zřízena za účelem uspokojování potřeb veřejného zájmu, které nemají průmyslovou nebo obchodní povahu, a je financována převážně některým z výše uvedených subjektů nebo těmito subjekty ovládána nebo tento subjekt jmenuje či volí více než polovinu členů v jejím statutárním, správním, dozorčím či kontrolním orgánu.

GDPR vs. veřejné subjekty



- výrazně nižší pokuty
- minimální dopad nařízení GDPR při zpracovávání dat v souvislosti s plněním právní povinnosti nebo výkonu pravomoci
 - dálkový přístup pro zveřejňování informací subjektům údajů
 - není nutné posouzení vlivu
 - jednodušší analýza zpracování (ne na jednotlivé procesy, ale na celé agendy)



- povinnost stanovit DPO
- důsledné dodržování nařízení GDPR při plnění povinnosti:
 - zveřejňování údajů na základě zákona 106/1999 Sb.
 - zveřejňování smluv dle zákona 340/2015 Sb. v registru smluv.
 - Důsledné dodržování zákona 499/2004 Sb. (Zákon o archivnictví a spisové službě)

GDPR – školy, školská zařízení

- Přímý dopad na školy
- V souvislosti s registrací agendy A3082 Školský zákon, jsou školy a školská zařízení ve smyslu § 50 zákona č. 111/2009 Sb., o základních registrech, vedeny v základním registru práv a povinností jako orgány veřejné moci.
- Je nutné ověřovat totožnosti subjektů údajů pro některé úkony v základních registrech – zajistí se tak správnost zpracovávaných dat zejména při uveřejňování v registru smluv, odpovídání na žádosti na základě z.106 nebo elektronických komunikacích (např. DS).

Přenesená zodpovědnost při dodržování ochrany osobních údajů



Je vhodné vyvážit zodpovědnost statutárního zástupce za dodržování nařízení GDPR a odpovídajícím způsobem zodpovědnost zaměstnanců a spolupracovníků podílejících se na zpracování osobních údajů.

1. Uvést povinnost mlčenlivosti a dodržování nařízení GDPR a ZZOÚ
 - a) jako dodatek pracovní smlouvy
nebo
 - b) do pracovní náplně do obecných povinností

2. Do oblastí povinností zaměstnanců uvést povinnost zachování zvláštní mlčenlivosti o zpracovávaných osobních údajích podle nařízení GDPR a ZZOÚ
 - a) v organizačním řádu
nebo
 - b) v pracovní řádu

Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů (DPO) je pozice v rámci organizace, v níž působí zaměstnanec nebo externí pracovník jako ochránce osobních údajů klientů, zákazníků, pacientů, zaměstnanců apod. Funguje mj. jako prostředník pro komunikaci mezi subjektem údajů, správcem a dozorovým úřadem.

Problematika pověřence je podrobně popsána v samotném nařízení, nicméně nový návrh ZZOU přesněji definuje požadavky na pověřence včetně mlčenlivosti.

Pověřenci nenesou v případě nedodržování souladu s obecným nařízením o ochraně osobních údajů osobní odpovědnost.

Mlčenlivost pověřence a jemu podřízených osob

Návrh zákona v ustanovení § 12 stanovuje zákonnou povinnost mlčenlivosti pověřence pro ochranu osobních údajů, která by se netýkala pouze pověřence, ale i jemu podřízených osob, podílejících se na plnění jeho úkolů. Povinnost mlčenlivosti by trvala i po skončení výkonu činnosti. Zprostit pověřence a jemu podřízené osoby mlčenlivosti by byl oprávněn správce, popř. zpracovatel osobních údajů.

Pověřenec pro ochranu osobních údajů

Nařízení vlády č. 399/2017 Sb. doplnilo od 1. 1. 2018 katalog prací o činnosti referenta správy osobních údajů. Sem jsou zařazeny též činnosti pověřence, a to od 10. do 13. platové třídy.

(dle náročnosti zpracování osobních údajů správcem).

Všechny veřejné subjekty (včetně veřejných škol) mají povinnost pověřence jmenovat.

Je přímo podřízený řídicím pracovníkům organizace. Nesmí být ve střetu zájmu, tedy podílet se např. na zpracování osobních dat.

V případě, že PO nebudou mít k datu účinnosti nařízení GDPR svého Pověřence z důvodu, že ho nemohou najít z řad svých zaměstnanců nebo jako externí spolupráci např. sdílením pověřence s jinou PO, mohou si požádat KÚ LK o dočasné přidělení Pověřence z KÚ LK pro výkon této funkce i na jejich PO. Na konci roku 2018 bude vyhodnocena zátěž takto sdíleného pověřence z KÚ LK a vytvořen metodický pokyn k dalšímu postupu pro zajištění Pověřenců na příspěvkových organizacích.

Začátek spolupráce



POTŘEBUJEME VĚDĚT...

...JAK NA TOM JSTE S OOÚ!

...ZDA PROBLEMATICE ROZUMÍTE

POTŘEBUJEME ZNÁT...

...VAŠE NÁZORY

...NEJZÁVAŽNĚJŠÍ NEDOSTATKY VČAS!

...VAŠE NÁVRHY

Harmonogram – fáze 1



| TERMÍN | ÚKOL | KDO |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| do 6. 2. 2018 | předání podkladů pro vstupní analýzu GDPR pilotním organizacím (tabulka + návod na vyplnění) | GDPR tým KÚ LK |
| do 12. 2. 2018 | zašlete prosím Pověřenci KÚ LK kontakt na osobu zodpovědnou za implementaci GDPR ve Vaší organizaci (e-mailem na adresu: dpo@kraj-lbc.cz) | PO |
| do 13. 2. 2018 | dokončení analýzy a zpracování výstupů z pilotních organizací | pilotní PO, GDPR tým KÚ LK |
| do 14. 2. 2018 | rozeslání tabulek pro vstupní analýzu (spolu s návodem na vyplnění) všem kontaktním osobám příspěvkových organizací | DPO KÚ LK |
| 14. 2. 2018 (8:00 – 17:00) | konzultační dny pro PO (telefonické, po dohodě osobní) | GDPR tým KÚ LK |
| 22. 2. 2018 (8:00 – 15:00) | | |
| 5. 3. 2018 (8:00 – 17:00) | | |
| 7. 3. 2018 (8:00 – 17:00) | | |

Harmonogram – fáze 2



| TERMÍN | ÚKOL | KDO |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| do 9. 3. 2018 | odevzdání vyplněných tabulek spolupracujícími PO (ve formátu .xlsx) Pověřenci KÚLK e-mailem na adresu dpo@kraj-lbc.cz | PO |
| 12. 3. – 16. 3. 2018 | kontrola vstupní analýzy, vyhodnocení nedostatků | GDPR tým KÚ LK, PO |
| | návrhy řešení | |
| | vyžádání / kontrola smluv s externími subjekty | PO |
| do 29. 3. 2018 | vytvoření změn ve vnitřních předpisech nebo zapracování dodatků do zaměstnaneckých smluv | PO |
| | úprava směrnic | |
| | definice „NE“ problémů (nedostatků/nevyřešitelného/neodstranitelného/neaplikovatelného) | |
| do konce března 2018 | kontaktním osobám na PO budou zaslány školící materiály pro školení zaměstnanců | GDPR tým KÚ LK |
| | provést základní analýzu stavu archivů, dalších prostor pro ukládání listinné podoby dokumentů, provést analýzu IT prostředí vč. fyzického zabezpečení místností se servery, zálohami aj. | PO |

Harmonogram – fáze 3



| TERMÍN | ÚKOL | KDO |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-------------------|
| 3. 4. – 6. 4. 2018 (8:00 - 15:00) | konzultační dny pro PO (telefonické, po dohodě osobní) | GDPR tým KÚ LK |
| | pokusy o vyřešení „NE“ problémů | |
| | finální konzultace s vedoucími pracovníky PO | |
| do konce dubna 2018 | PO zajistí proškolení vlastních zaměstnanců (dodržování ochrany OÚ při práci s listinou i elektronickou podobou osobních dat) | PO |
| | stanovení DPO a nahlášení na ÚOOÚ | |
| | odkazy / instrukce pro žádosti subjektů údajů na web organizace | |
| do 24. 5. 2018 | zajištění platných souhlasů od subjektů údajů (pokud jsou zpracovávána nějaká data na základě souhlasu) | PO |
| | uzavření revidovaných smluv s externími dodavateli | |
| | zajištění platných zpracovatelských smluv | |
| | otestování postupů při žádostech subjektů údajů | |

Harmonogram – fáze 4



| TERMÍN | ÚKOL | KDO |
|----------------------------------|---------------------------------------------------------------------|-------------------|
| 25. 5. – 31. 12. 2018 | zvýšená podpora GDPR týmu | GDPR tým KÚ LK |
| | analýza dopadu GDPR na provoz organizace | |
| | průběžné odstraňování nedostatků | PO |
| | „ladění“ směrnic, smluv, souhlasů | |
| | analýza reálného využití DPO a vytíženosti případných sdílených DPO | GDPR tým KÚ LK |
| | průběžná školení zaměstnanců PO | PO |
| ? 2018 | Úprava WWW stránek PO pro soulad s nařízením ePrivacy | PO |
| do 29. 9. 2018 | finální opatření pro soulad s nařízením eIDAS | PO |
| | výměna úložišť certifikátů aj... | |

ePRIVACY a vazba na GDPR

- ePrivacy - Nařízení o soukromí a elektronických komunikacích
- Zavádí právo subjektu údajů na odsouhlasení, zda o něm mohou poskytovatelé shromažďovat data – vztahuje se i na právnické osoby!

Plánovaná účinnost ePrivacy byla ke dni účinnosti GDPR, nebude však dodržena. Účinnost nařízení bude pravděpodobně ke konci roku 2018.

V oblasti elektronických komunikací rozšiřuje plošně ochranu a zpracovávání údajů i na právnické osoby. V kombinaci s GDPR ukládá povinnosti přísného dodržování pravidel zejména při provozu webových služeb, IoT (internet věcí).

Dotkne se telekomunikací, datových sítí, online služeb a zpracování cookies. Ovlivní i bezpečnost komunikace přes aplikace Skype, Facebook, Viber, WhatsApp aj.

eIDAS a vazba na GDPR

eIDAS - Nařízení o soukromí a elektronických komunikacích

Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014

Adaptační zákon - č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce

Zavádí přísnější pravidla pro veřejné subjekty vč. škol.

Nutné ovládat autorizovanou konverzi listinné a elektronické verze dokumentů.

od 29. 9. 2018 – povinnost vzájemného uznávání eID

Při poskytování online služeb je nutné zajistit autentizaci webu! (<https> / platný certifikát)



Spisová služba



- **Důrazně doporučujeme vedení elektronické spisové služby!** (zejména v souvislosti s eIDAS)

Dbát na dodržování Zákona č. 499/2004 Sb., o archivnictví a spisové službě a respektovat nová pravidla GDPR.

Povinnost ověřovat subjekt (ztotožňovat) při elektronické komunikaci přes základní registry.

Povinnost využít datovou schránku, pokud ji má subjekt zřízenou.

Pozor na povinnost ukládání dokumentů ve strojově čitelném formátu.

Možnost **bezplatného** využití spisové služby GINIS po dohodě s KÚ LK.

Bližší informace poskytnete:

Ing. Foktová Petra

petra.foktova@kraj-lbc.cz

garant hostované spisové služby



- **Pozor na způsob zveřejňování dokumentů**

Nelze uveřejňovat faktury, e-mailové adresy, telefonní čísla a podpisy !!!

Pozor na uveřejňování dalších osobních údajů !!!

Pozor na formu ukládání dokumentů – musí být ve strojově čitelném formátu.

Objednávka + potvrzení objednávky = povaha smlouvy

Tyto dokumenty však obsahují údaje, jejichž zveřejnění je ve střetu s nařízením GDPR.

Platí pro všechny dokumenty související s veřejnou zakázkou (objednávka, dodací list, faktura, smlouva apod.)

Vhodné prostudovat **Metodický návod k aplikaci zákona o registru smluv - 1.6i**
ze dne 27. listopadu 2017 (stránky MVČR)

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím



- Nutno identifikovat prokazatelně tazatele - ztotožnit subjekt
- Důkladně prověřit oprávněnost žádosti subjektu
- Pozor na poskytování informací v neanonymizované podobě
- Dodržovat oznamovací povinnost
- Dbát na transparentní jednání se subjektem a zveřejňovat jen nezbytné údaje – opět ve vazbě na GDPR

AML a povinné osoby (Anti-Money-Laundering)



- Povinné osoby mohou předávat osobní údaje pro splnění jejich povinností dané zákonem AML – předávání těchto dat je upraveno adaptačním zákonem a je z ochrany osobních údajů dané nařízením GDPR vyňato!

Připravte se na své...

... žáky a jejich rodiče

... zaměstnance

... spoluobčany

... úředníky ☺

Poučte své kolegy, spolupracovníky, podřízené, že je důležité vyhodnocovat potenciální problémy či hrozby a včas je konzultovat!

Jak se bránit proti sledování dnes?



GHOSTERY®

www.ghostery.com

The screenshot displays the Ghostery browser extension interface. At the top, there is a blue header with the Ghostery logo and a 'Sign In' button. The main content area is divided into two columns. The left column shows a circular progress indicator with the number '7' and the word 'Trackers' below it, indicating the total number of trackers found on the current page. Below this, it shows 'Blocked: 7' and 'Page Load: -'. There are three icons representing different protection levels: a shield, a shield with a slash, and a lightbulb. At the bottom of this column, there are three buttons: 'Trust Site', 'Restrict Site', and 'Pause'. The right column is titled 'TRACKERS' and shows a list of trackers. The first category is 'Advertising', which has 5 trackers and 5 blocked. The trackers listed under 'Advertising' are Gemius, Adform, AdOcean, BBelements, and Imedia. The second category is 'Essential', which has 1 tracker and 1 blocked. The tracker listed under 'Essential' is Google Tag Manager. At the bottom of the right column, there are several icons representing different protection features: a list view icon, a clock, a shield, a gift, and a diamond.

Praktické informace



- Zrušení registrační povinnosti správců osobních údajů
 - Například zřízení kamerového systému

- Délka platnosti souhlasu
 - Pro účely, pro které je souhlas aplikovatelný, jde o svobodný a odvolatelný projev vůle, může tak být udělen i na dobu neurčitou.

- Účty uživatelů v systémech
 - Nikdy nemazat, ale blokovat!

- Dotaz na ÚOOÚ ohledně fotografování dětí
 - Fotografování dětí, pokud rodiče výslovně nesouhlasí s jakýmkoliv zveřejňováním fotografií svého dítěte - musíme dbát o to, aby se toto dítě na žádné fotografii neobjevilo, nebo lze pro novinářské účely (článek na WWW stránkách či v periodiku) fotit toto dítě bez omezení?

Odpoověď ÚOOÚ ohledně fotografování dětí

V případě zveřejňování fotografií z různých akcí nejde o souhlas se zpracováním osobních údajů podle zákona o ochraně osobních údajů, ale o svolení k zachycení a šíření podoby člověka podle § 84 – § 90 zákona č. 89/2012 Sb., občanský zákoník. Podle § 89 se podobizna nebo zvukový či obrazový záznam mohou bez svolení člověka také poříditi nebo použít přiměřeným způsobem též k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství. K posouzení přiměřenosti by byl příslušný soud na základě občanskoprávní žaloby. Jestliže není zřejmé, zda jde o zpravodajství ve smyslu občanského zákoníku, lze v případě dětí, jejichž rodiče s jakýmkoliv zveřejňováním svého dítěte nesouhlasí, doporučit vyvarovat se zejména pořizování a zveřejňování detailních záběrů takového dítěte. Podle názoru poradního orgánu Komise (EU) pro ochranu osobních údajů by měla škola při organizaci akcí, na nichž se fotografie dětí určené ke zveřejnění pořizují, dbát na postoj rodičů, ale současně vytvářet pro děti nediskriminující podmínky, včetně vhodného okamžiku pořízení fotografií podpořeného odpovídajícím organizačním uspořádáním jako je rozsazení dětí, nebo záběr na část prostor, v nichž se soustředí děti, jejichž rodiče si fotografování přejí. Upozorňuji v této souvislosti na skutečnost, že použití zpravodajské licence ve školách není bez problémů, a proto Vám Úřad pro ochranu osobních údajů doporučuje záležitost konzultovat s Ministerstvem školství, mládeže a tělovýchovy.