masarykova veřejná knihovna vsetín

GDPR v knihovnách

Masarykova veřejná knihovna Vsetín
Březen 2018
Daniela Divínová

GDPR

General Data Protection Regulation

Obecné nařízení o ochraně údajů (GDPR) bylo parlamentem Evropské unie zavedeno do právního řádu v dubnu 2016 a jeho vstoupení v platnost bylo stanoveno na **25. května 2018.**

Toto Nařízení zavazuje osoby v ČR přímo, aniž by jej musel provádět zákon. Některé dílčí záležitosti umožňuje či přímo ukládá Nařízení členským státům upravit podrobněji – bude tedy ještě přijat prováděcí zákon, který pravděpodobně ponese název **zákon o zpracování osobních údajů**, aby se nepletl se současným zákonem **č. 101/2000 Sb., Zákon o ochraně osobních údajů a změně některých zákonů.**

Zdroje:

1. Úřad na ochranu osobních údajů

www.uoou.cz

https://www.uoou.cz/gdpr-obecne-nbsp-narizeni/ds-3938/p1=3938

2. Pracovní skupina podle článku 29 (WP29)

- skupina má poradní statut a jedná nezávisle

https://www.uoou.cz/pokyny-pracovni-skupiny-wp29/ds-4728/p1=4728

3. Národní knihovna Praha

http://ipk.nkp.cz/legislativa/01_LegPod/ochrana-osobnich-udaju/ochrana-osobnich-udaju-prirucka-pro-knihovny#_Toc504730187

GDPR = kontinuita

- Obecné nařízení o ochraně údajů **(GDPR) není ve věci ochrany osobních údajů zásadním předělem.**

- Nařízení navazuje ve sledovaných cílech a obsahových zásadách zpracování a ochrany osobních údajů na směrnici 95/46/ES (byla základem evropských zákonů o ochraně soukromí od roku 1995) a sleduje překonání stávající roztříštěnosti v provádění ochrany osobních údajů v Unii soudržným a jednotným uplatňováním pravidel ochrany osobních údajů.

- Nařízení přináší změny především v rovině procesní, snaží se o změnu kultury při nakládání s osobními údaji.

- **Jedinou skutečnou novinkou je právo na přenositelnost údajů podle čl. 20 obecného nařízení.**

Terminologie GDPR:

Osobní údaj

Osobním údajem je jakákoliv informace, která se týká konkrétního člověka.

Nejde jen o údaje, na základě kterých lze tohoto člověka přímo identifikovat jako je např. jméno, číslo občanského či čtenářského průkazu, adresa, telefonní číslo, webové údaje (IP adresy, informace z cookies, údaje z RFID tagů), ale i další údaje, které se ho týkají, jako je např. záznam historie výpůjček či výše dluhu.

Osobními údaji nejsou údaje o právnické osobě, ani údaje o člověku, který již zemřel.

Terminologie GDPR:

Subjekt údajů

Subjektem údajů je člověk, o jehož údaje se jedná, například uživatel, návštěvník, zaměstnanec knihovny apod.

Zpracování osobních údajů

Zpracování osobních údajů je jakákoliv operace s nimi, tj. shromáždění, zaznamenání, uspořádání, použití, zpřístupnění přenosem, včetně jejich zobrazení na monitoru počítače, uložení v papírové podobě, přepsání do databáze, oprava, vytvoření kopie, anonymizace apod.

Terminologie GDPR:

Správce osobních údajů

Správcem osobních údajů je ten, kdo určuje účel a prostředky konkrétního zpracování osobních údajů, v našem případě tedy provozovatel knihovny.

- *Je-li knihovna právním subjektem, pak sama je provozovatelem knihovny,*
- *nemá-li knihovna právní subjektivitu (pokud např. je součástí organizace nebo je organizační složkou ÚSC nebo státu), pak provozovatelem je příslušný právní subjekt.*

Terminologie GDPR:

Zpracovatel

Zpracovatelem osobních údajů je **ten, kdo pro knihovnu s osobními údaji jakkoli nakládá, nikoli však její vlastní zaměstnanec.**

Typicky půjde o poskytovatele automatizovaného knihovního systému či toho, kdo pro knihovnu vymáhá pohledávky. Může jím ale být například i poskytovatel webhostingu, společnost Google, pokud knihovna využívá její formuláře či cloudové služby. Dle okolností i provozovatel kamerových systémů v knihovně, ekonomických systémů či systémů správy zaměstnaneckých dat.

Zásady zpracování OÚ:

Osobní údaje musí být zpracovány podle následujících zásad:

- zpracovávány pouze na základě konkrétních právních důvodů
- zpracovávány korektně a transparentně
- shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely
- přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány
- přesné a v případě potřeby aktualizované
- uloženy pouze po dobu nezbytnou pro účely, pro které jsou zpracovávány
- zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů

Právní důvody:

Zpracování musí vždy probíhat na základě alespoň jednoho z právních důvodů vyjmenovaných v čl. 6 odst. 1 Nařízení, kterými jsou:

- **plnění smlouvy**

  Provozovatel knihovny může na základě tohoto právního důvodu zpracovávat osobní údaje, které jsou nezbytné pro plnění smlouvy, např. smlouvy o poskytování služeb (přihlášky do knihovny).

  K těmto osobním údajům tedy nemusí získávat další právní důvod, např. souhlas.

- **plnění právní povinnosti**

  Lze aplikovat v případě, pokud nějaký právní předpis provozovateli knihovny přímo ukládá, aby osobní údaje zpracovával (užití pro většinu osobních údajů zaměstnanců)

- **plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci**

  Takovým zájmem může být například naplňování práva veřejnosti na informace.

Právní důvody:

- **oprávněný zájem**
  Oprávněný zájem musí být aktuální a reálný, není možné shromažďovat osobní údaje, protože by se někdy mohly hodit.

- **ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby**
  Jde o právní důvod, který pravděpodobně v činnosti knihovny své uplatnění nenalezne.

- **souhlas se zpracováním osobních údajů**

  Souhlas je třeba žádat pro konkrétní účel.
  Nebude tedy již například možná formulace: „Uživatel souhlasí, aby knihovna zpracovávala jeho osobní údaje v rozsahu a v souladu s účelem uvedeným v knihovním řádu.“

Právní důvody:

Souhlas musí být poskytnut **jednoznačně,** např. podepsáním souhlasu na listině, zaškrtnutím nepředvyplněného políčka v listinné či elektronické podobě nebo zasláním e-mailu. Jeho poskytnutí musí být knihovna schopna doložit po celou dobu, po kterou na jeho základě s údaji nakládá.

Souhlas nesmí být **podmíněný** a musí být **odvolatelný**.

Není tedy možné poskytnutím souhlasu podmiňovat poskytnutí služby, např. v této podobě: „Pokud uživatel nebude souhlasit s poskytnutím rodného čísla, nemůže využívat služeb knihovny.“

Souhlas lze **kdykoli odvolat**, není proto vhodné jej vyžadovat v situaci, kdy nelze po odvolání souhlasu údaje přestat zpracovávat, protože je knihovna potřebuje a užívá je na základě jiného právního důvodu - typicky při výpůjčkách dokumentů.

Korektnost a transparentnost:

Knihovna musí najít vhodný způsob, jak subjekty údajů informovat, aby se k nim to podstatné opravdu dostalo.

Pro **uživatele** může kapitolu o ochraně osobních údajů zařadit do knihovního řádu a vytvořit vnitřní směrnici, která celý proces zmapuje a popíše.

Zaměstnance knihoven by měl provozovatel knihovny informovat přímo a kromě stávajících zaměstnanců nesmí zapomenout ani na ty, kteří nastoupí později.

Ochrana osobních údajů by měla být součástí vstupního školení, a to jak z hlediska nakládání s osobními údaji zaměstnanců, tak z hlediska jejich povinností vzhledem k osobním údajům uživatelů.

Korektnost a transparentnost:

Každému, jehož osobní údaje uchovává, by měl provozovatel knihovny sdělit:

- Kontakt, kam se může ohledně svých osobních údajů obrátit.
- K čemu které osobní údaje knihovna potřebuje.
- Které údaje jsou nezbytné pro uzavření smlouvy (tato informace může být případně pouze na přihlášce).
- Bližší vysvětlení, proč knihovna uchovává osobní údaje, dělá-li to na základě oprávněného zájmu, např. proč uchovává historii výpůjček.
- Proti kterému zpracování osobních údajů konkrétně může vznést námitku. Jde o ty, které knihovna zpracovává na základě oprávněného nebo veřejného zájmu.

Korektnost a transparentnost:

- Kdo další má k osobním údajům přístup. Informaci o tom, že knihovna předává údaje společnosti vymáhající pohledávky, lze uživateli sdělit s předstihem až ve chvíli, kdy je to relevantní.
- Jak dlouho které údaje knihovna uchovává.
- Že má právo zjistit, jaké osobní údaje uchovává knihovna o něm konkrétně; kde je najde, jsou-li přístupné online, např. po přihlášení do čtenářského konta.
- Že tyto údaje může získat i ve strojově čitelné podobě.
- Jak může požádat o opravu osobních údajů, které o něm knihovna zpracovává.
- Jak může požádat o výmaz osobních údajů a za jakých podmínek bude žádosti vyhověno.
- Že může podat stížnost u Úřadu pro ochranu osobních údajů.

Účelové omezení:

Knihovna smí v souladu se zásadou účelového omezení zpracovávat osobní údaje pouze pro **výslovně stanovené účely**, které navíc musí být subjektům osobních údajů sděleny.

Osobní údaje lze zpracovávat i pro více účelů.

Zpracování osobních údajů registrovaných uživatelů může knihovna činit například za těmito účely:

- vedení evidence uživatelů dle knihovního zákona
- poskytování knihovnických, informačních a dalších služeb dle knihovního zákona
- ochrana knihovního fondu
- informování uživatelů o službách a akcích knihovny
- hodnocení spokojenosti uživatelů
- statistika

Osobní údaje zpracovávané knihovnou:

Aby knihovna byla schopna naplnit povinnosti, které jí nařízení ukládá, je nezbytné, aby **měla přehled o všech zpracováních, která provádí.**

Přehled typických případů, kdy knihovny zpracovávají osobní údaje (každá knihovna si musí vytvořit vlastní kompletní přehled):

1. Registrovaní uživatelé
2. Další uživatelé
3. Zaměstnanci
4. Smluvní partneři
5. Autoři a jiné autority

Ad 1 – Registrovaní uživatelé:

Podpisem čtenářské přihlášky uzavře uživatel s knihovnou smlouvu o poskytování služeb, na základě které mu knihovna umožňuje využívat výpůjční a jiné knihovnické a informační služby, a stává se tak uživatelem registrovaným.

Ilustrativní výčet osobních údajů zpracovávaných k registrovanému uživateli:

- **identifikační údaje** (jméno a příjmení, datum narození, rodné číslo, druh a číslo osobního dokladu, číslo čtenářského průkazu, pohlaví, titul, občanství)
- **kontaktní údaje** (adresa trvalého pobytu, korespondenční adresa, email, telefon)
- fotografie, číslo bankovního účtu, údaj, zda je držitelem průkazu ZTP či ZTP/P, údaj o vzdělání
- heslo ke čtenářskému kontu, historie výpůjček, historie zobrazení konta
- údaje o provedených peněžitých transakcích
- IP adresa a cookie
- údaje o zákonném zástupci
- údaje o vymáhání dluhu a další

Ad 1 – Registrovaní uživatelé - děti:

Nařízení zdůrazňuje potřebu zvýšené ochrany dětí.

Často zmiňovaná **hranice 16 let**, která může být zákonem o zpracování osobních údajů snížena až na 13 let, **se vztahuje pouze ke službám informační společnosti, tedy takovým, které jsou poskytovány elektronicky na dálku.**

Ohledně uzavření právního vztahu s knihovnou platí nadále občanský zákoník, tedy že děti jsou způsobilé k právním jednáním co do povahy přiměřeným rozumové a volní vyspělosti nezletilých jejich věku.

Hranici 15 let, kterou většina knihoven pro samostatný zápis do knihovny vyžaduje, tak není třeba upravovat.

Smlouvu o poskytování služeb uzavírají jménem dětí jejich zákonní zástupci, knihovna tedy zpracovává i jejich osobní údaje.

Pro nakládání s nimi platí víceméně totéž, jako pro nakládání s údaji registrovaných čtenářů.

Ad 2 – Další uživatelé:

Uživatelem je každý, kdo využívá jakékoliv služby poskytované knihovnou, tedy i ty které nejsou vyhrazeny pouze uživateli registrovanému, např. účastní se akce knihovnou pořádané, využívá internet či knihy ve volném výběru apod.

Uživatelem je rovněž každý, kdo se zdržuje v prostorách knihovny.

Údaje o těchto uživatelích knihovna zpracovává, pokud provozuje kamerový systém se záznamem a také, pokud pro nabízené služby poskytnutí osobních údajů požaduje (např. registrace na akci pomocí formuláře).

Zpracováním osobních údajů může být za určitých okolností i fotodokumentace akce.

Ad 3 – Zaměstnanci:

Provozovatel knihovny zpracovává i osobní údaje svých zaměstnanců, a to i těch, jejichž pracovněprávní vztah je založen dohodou o práci konané mimo pracovní poměr.

Při vytváření přehledu o zpracovávaných osobních údajích je důležité nezapomenout na údaje o uchazečích o zaměstnání a též o bývalých zaměstnancích.

Ad 4 – Smluvní partneři:

Jde o fyzické osoby, se kterými knihovna spolupracuje na základě jiných smluv než zaměstnaneckých (příkazní, smlouvy o dílo), například dobrovolníci, lektoři, stážisté apod.

Ad 5 – Autoři a jiné autority:

V katalozích knihoven je možné dohledat nejen jména a příjmení autorů, ale i další osobní údaje včetně data narození.

Knihovny také často vytvářejí databáze dalších regionálních osobností.

Osobní údaje se nacházejí i v článkových databázích.

Knihovna - správce osobních údajů:

Nařízení klade na odpovědnost správce vyšší důraz, než činila předchozí úprava.

S rozšířením odpovědnosti správců také souvisí zrušení oznamovací povinnosti. Knihovny tedy již nebudou muset ohlašovat nová zpracování osobních údajů Úřadu pro ochranu osobních údajů.

Knihovna jako správce osobních údajů odpovídá nejen za dodržování všech povinností, které z výše uvedených zásad vyplývají, ale také musí být schopna dodržování povinností v kterémkoli okamžiku doložit.

Pokud je knihovna organizační složkou obce či jiné právnické osoby, je vhodné řešit problematiku ochrany osobních údajů v rámci celé obce či organizace.

Doporučený průběh vnitřního procesu:

- prvním krokem by mělo být **určení osoby, která bude v rámci knihovny odpovědná za správné nastavení procesů v oblasti ochrany osobních údajů**

*Někteří provozovatelé knihoven budou navíc povinni jmenovat **pověřence pro ochranu osobních údajů**. Které veřejné subjekty to nakonec budou, bude upravovat prováděcí zákon o zpracování osobních údajů, který však ještě nebyl přijat.*
Je pravděpodobné, že povinnost jmenovat pověřence budou mít obce a školy, ale nikoli knihovny, které jsou příspěvkovými organizacemi.

- **mít všechny postupy v oblasti ochrany osobních údajů dobře zdokumentované**

Je vhodné shromáždit veškeré obecné dokumenty, které se týkají ochrany osobních údajů, na jednom místě, ať již v šanonu či na zabezpečené intranetové stránce (přehled zpracovávaných údajů, vnitřní směrnice, informace poskytované subjektům údajů, formuláře, smlouvy s dodavateli systémů, doklad o proškolení zaměstnanců, kteří nakládají s osobními údaji, apod.).

Doporučený průběh vnitřního procesu:

- **uzavřít zpracovatelské smlouvy**

Jak již bylo řečeno výše, **zpracovatelem je každý, kdo pro knihovnu jakkoli zpracovává osobní údaje, ne však její vlastní zaměstnanec.**

Smlouva mezi provozovatelem knihovny a zpracovatelem musí být uzavřena písemně, což zahrnuje i prostou elektronickou formu.

Téměř určitě tedy bude potřebné uzavřít nové smlouvy nebo dodatky s provozovateli automatizovaných knihovních systémů, poskytují-li software jako službu nebo servis systému, a jsou tedy v postavení zpracovatelů. Dle okolností i provozovatelů kamerových systémů, systémů správy zaměstnaneckých dat, ekonomických systémů, systémů spisové služby či osob zabývajících se vymáháním pohledávek pro knihovnu.

Vzor smluvní doložky:
http://ipk.nkp.cz/docs/gdpr/GDPR_Vzor_smluvni_dolozky.docx

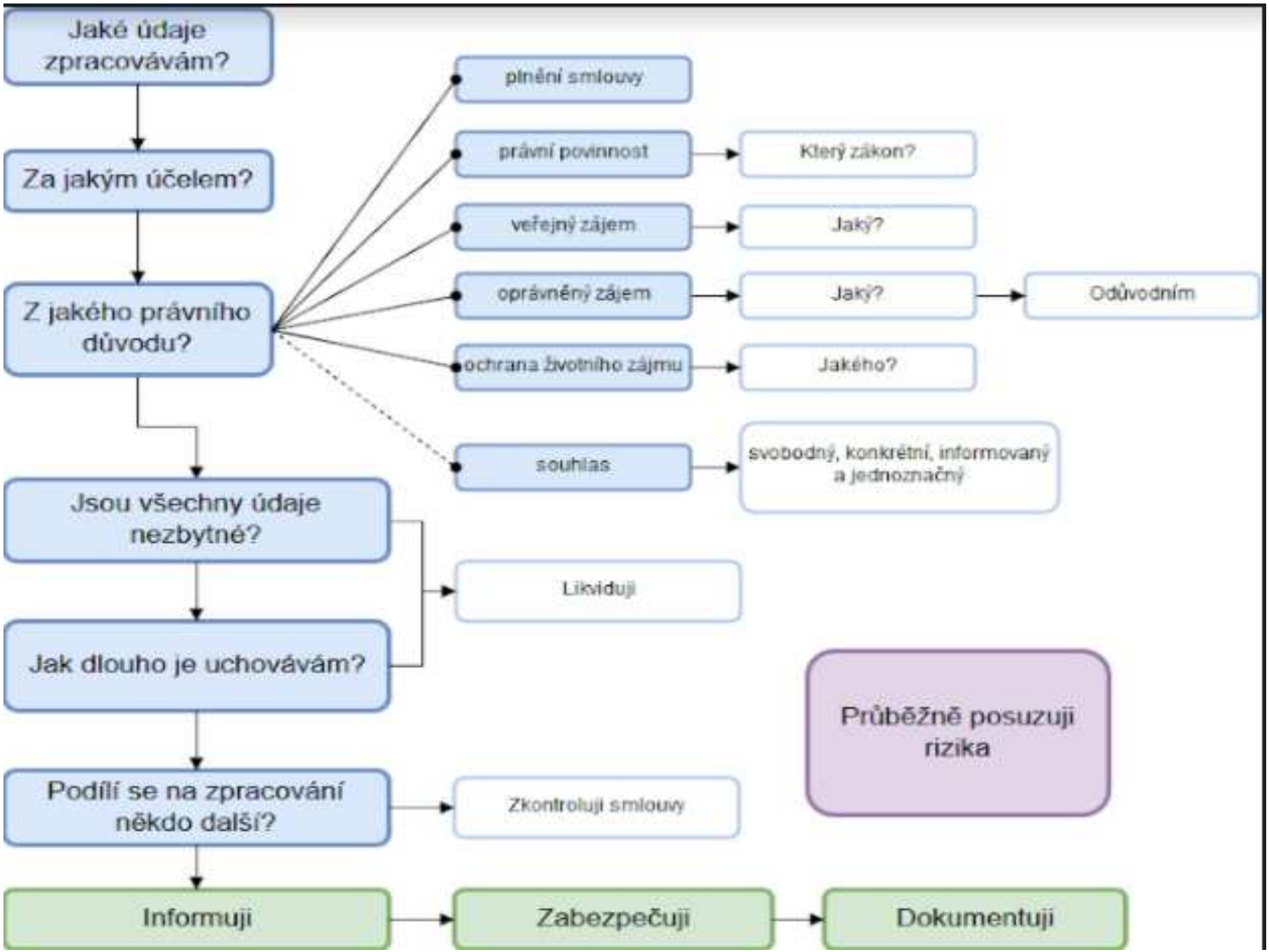
Doporučený průběh vnitřního procesu:

- **hlásit porušení zabezpečení osobních údajů**

Dojde-li k porušení zabezpečení osobních údajů, **je to provozovatel knihovny povinen ohlásit Úřadu pro ochranu osobních údajů**, a to **do 72 hodin od okamžiku, kdy se o něm dozvěděl**.

Není podstatné, zda k porušení zabezpečení došlo v důsledku kybernetického útoku nebo porušením povinností zaměstnance, zda se to stalo záměrně nebo omylem, a zda důsledkem je ztráta osobních údajů nebo jejich neoprávněné vyzrazení, nebo dokonce jen jejich dočasná nedostupnost, např. v případě výpadku proudu. Této povinnosti se zprostí pouze v případě, že je nepravděpodobné, že by toto porušení zabezpečení znamenalo nějakou újmu pro dotčené osoby.

V případě, kdy by riziko pro subjekty údajů bylo velké, je třeba incident oznámit nejen Úřadu, ale vhodným způsobem i dotčeným lidem, aby mohli podniknout kroky pro svou ochranu.


Jaké údaje zpracovávám?
Za jakým účelem?
Z jakého právního důvodu?
Jsou všechny údaje nezbytné?
Jak dlouho je uchovávám?
Podílí se na zpracování někdo další?
Informuji
Zabezpečuji
Dokumentuji
plnění smlouvy
právní povinnost
Který zákon?
veřejný zájem
Jaký?
oprávněný zájem
Jaký?
Odůvodním
ochrana životního zájmu
Jakého?
souhlas
svobodný, konkrétní, informovaný a jednoznačný
Likviduji
Zkontroluji smlouvy
Průběžně posuzuji rizika

Shrnutí

Splnění nových nařízení o ochraně dat, která vejdou v platnost v květnu 2018, je náročným a komplikovaným úkolem. Nicméně pro organizace, které sbírají, kontrolují a zpracovávají osobní údaje občanů EU je splnění těchto nařízení povinností.

Čas na vytvoření plánu k identifikaci, klasifikaci, řízení, zabezpečení a dokumentaci ochrany těchto údajů a na implementaci řešení, která splní všechny požadavky GDPR, rychle utíká.

Vzor směrnice o ochraně osobních údajů:

http://ipk.nkp.cz/docs/gdpr/GDPR_vnitrni_predpis.docx

masarykova veřejná knihovna vsetín

Děkuji vám za pozornost

Daniela Divínová