Česká lékárnická komora

GDPR
v lékárenské praxi

duben 2018

Mgr. MUDr. Jaroslav Maršík

Obecná část

Česká lékárnická komora

GDPR

- zásady
- účely
- právní tituly
- přístup založený na riziku
- záměrná a standardní ochrana
- práva subjektu OÚ

Česká lékárnická komora

GDPR

- bezpečnostní incidenty
- pověřenec pro ochranu OÚ (DPO)
- posouzení vlivu na ochranu osobních údajů (DPIA)
- záznamy o činnostech
- kodexy
- šifrování a pseudonymizace
- sankce

Česká lékárnická komora

Zásady

- zákonnost – právní titul, ne rozpor se zákonem
- korektnost – rozumnost, očekávatelnost, bez negat. vlivu
- transparentnost – otevřenost, upřímnost, informovanost
- účelové omezení – určitý, výslovně vyjádřený a legitimní účel
- minimalizace údajů – jen nezbytný rozsah

Česká lékárnická komora

Zásady

- přesnost – opravy nebo výmaz nepřesných OÚ
- omezení uložení – jen na nezbytnou dobu
- integrita – ochrana celistvosti
- důvěrnost – zamezení neoprávněných přístupů
- odpovědnost – dodržovat zásady a doložit to

Česká lékárnická komora

Účely

- hlavní zásada zpracování OÚ
- bez účelu nelze zpracovávat
- účel rozhoduje o rozsahu, době, zákonnosti…
- stanoven určitě, výslovně vyjádřen, legitimní

Česká lékárnická komora

Právní tituly

- b) smlouva
- c) právní povinnost
- d) ochrana životně důležitých zájmů
- e) úkol ve veřejném zájmu nebo výkon veř. moci
- f) oprávněné zájmy (ne orgány veřejné moci)
- a) souhlas

Česká lékárnická komora

Přístup založený na riziku

- jeden ze dvou hlavních principů GDPR (spolu s odpovědností)
- správce volí technická a organizační opatření podle míry závažnosti rizika pro práva a svobody subjektů
- nutnost trvalého posuzování rizika

Česká lékárnická komora

Záměrná a standardní ochrana

- záměrná ochrana – volba vhodných opatření s přihlédnutím k rizikům od počátku do konce
- standardní ochrana – volba vhodných opatření ke zpracování OÚ jen v nezbytné míře

Česká lékárnická komora

Práva subjektu OÚ

- právo na informace
- právo na přístup
- právo na opravu
- právo na výmaz
- právo na omezení zpracování
- právo na přenositelnost
- právo na námitku
- právo nebýt předmětem automatiz. zpracování
- právo na oznámení porušení zabezpečení

Česká lékárnická komora

Právo na informace

- OÚ získány od subjektu
  - sada informací (čl.13)
  - v okamžiku získání
  - není nutné, má-li je

Česká lékárnická komora

Právo na informace

- OÚ získány z jiného zdroje
  - sada informací (čl. 14) – nepatrné rozdíly
  - v přim. lhůtě (do 1 M), při komunikaci, při zpřístupnění
  - není nutné
    - má-li je
    - nepřiměřené úsilí
    - výslovně stanoveno právem EU nebo čl. státu
    - OÚ musí zůstat důvěrné

Česká lékárnická komora

Právo na přístup

- právo na potvrzení o zpracování OÚ
- právo na přístup ke svým OÚ
- právo na další informace, obdobné právu na informace
- nejde o právo na informace o způsobu zabezpečení!

„Správce poskytne kopii zpracovávaných osobních údajů.“

Česká lékárnická komora

Právo na opravu

- oprava nepřesných údajů na žádost bez zbyteč. odkladu
- doplnění neúplných údajů

Česká lékárnická komora

Právo na výmaz

- povinnost správce vymazat OÚ
  - není-li jich potřeba pro jiný účel
  - není-li jiný právní důvod pro zpracování, než souhlas
- neuplatní se
  - svoboda projevu a informací
  - splnění právní povinnosti
  - veřejný zájem
  - archivace, výzkum
  - právní nároky

Česká lékárnická komora

Právo na přenositelnost

- jen, je-li zpracování
  - založeno na souhlasu
  - prováděno automatizovaně
- strukturovaný, běžně používaný, strojově čitelný formát
- nový správce není povinen je přijmout

Česká lékárnická komora

Právo na námitku

- jen u
  - zpracování ve veřejném zájmu nebo při výkonu veřejné moci
  - nebo v případě oprávněného zájmu
  - nebo při účelu přímého marketingu
  - nebo při účelu věd. či hist. výzkumu či stat. zprac.
- správce nezpracovává, pokud neprokáže závažné oprávněné důvody, u marketingu nikdy

Česká lékárnická komora

Právo na ohlášení incidentu

- v případě porušení zabezpečení OÚ s následkem vysokého rizika pro práva a svobody fyzických osob

Česká lékárnická komora

Bezpečnostní incidenty

- jakékoliv porušení zabezpečení OÚ, ledaže je nepravděpodobné riziko pro práva a svobody FO
- ohlášení ÚOOÚ do 72 hodin
  - popis povahy
  - údaje o pověřenci
  - popis důsledků
  - popis opatření
- dokumentace
- u vysokého rizika i oznámení subjektu

Česká lékárnická komora

Pověřenec pro ochranu OÚ

- musí být
  - orgány veřejné moci
  - rozsáhlé pravidelné a systematické monitorování subjektů údajů
  - hlavní činnosti správce – rozsáhlé zpracování zvláštních kategorií údajů

Česká lékárnická komora

Pověřenec pro ochranu OÚ

- znalosti práva, IT, ochrany OÚ, GDPR
- zaměstnanec nebo outsorcing
- plnou podporu správce, přímý kontakt na vedení, zdroje
- nesmí být ve střetu zájmů
- nesmí být propuštěn ani sankcionován

Česká lékárnická komora

Pověřenec pro ochranu OÚ

- poskytuje poradenství a informace
- je kontaktním místem pro subjekty a ÚOOÚ
- monitoruje soulad s GDPR
- posuzuje a radí při DPIA

Česká lékárnická komora

Posouzení vlivu DPIA

Povinně při:

- systematickém a rozsáhlém vyhodnocování aspektu týkajících se FO, automatizované zpracování, rozhodnutí s právními účinky nebo jinými dopady vůči FO
- rozsáhlé zpracování zvláštních kategorií
- rozsáhlé systematické monitorování veřejně přístupných prostorů

Výjimka pro zpracování s právním základem při splnění právní povinnosti nebo výkonu veřejné moci.

Česká lékárnická komora

Záznamy o činnostech

- nemusí je vést
  - podnik do 250 zaměstnanců, ledaže
    - riziko pro práva a svobody subjektů údajů
    - není příležitostné
    - zahrnuje zvláštní kategorii údajů
- správce některé záznamy vést musí a jiné nemusí
- náležitosti záznamů viz čl. 30
- písemně vč. elektronicky
- předkládají se ÚOOÚ, základní způsob doložení souladu

Česká lékárnická komora

Kodexy

- sdružení zastupující různé kategorie správců mohou vydat kodexy chování a ty průběžně upravovat či rozšiřovat
- kodexy jsou schvalovány, registrovány a zveřejňovány ÚOOÚ
- na kodexy mohou odkazovat správci a zpracovatelé

Česká lékárnická komora

Šifrování a pseudonymizace

- způsoby zabezpečení
- nejsou povinné
- jsou výhodné zejména jako vhodná ochrana před narušením bezpečnosti zpracování OÚ a jako prvek snižující míru rizika při bezpečnostních incidentech na úroveň nevyžadující ohlášení nebo oznámení

Česká lékárnická komora

Sankce

- vysoké, ale…
- zásady pro ukládání pokut
- nutná snaha se s GDPR vypořádat
- pravděpodobnost postihu nízká, ale reálná
- právo stížnosti na ÚOOÚ
- právo na soudní ochranu vůči ÚOOÚ i vůči správci a zpracovateli
- právo na náhradu újmy

Zvláštní část

Česká lékárnická komora

Jak se vypořádat s GDPR v lékárně?

- něco vědět o ochraně OÚ a GDPR
- mít přehled o OÚ v provozu lékárny
- nastavit správně zacházení s OÚ
- doložit správné nastavení

Česká lékárnická komora

Je možné svěřit zcela ochranu OÚ jinému subjektu?

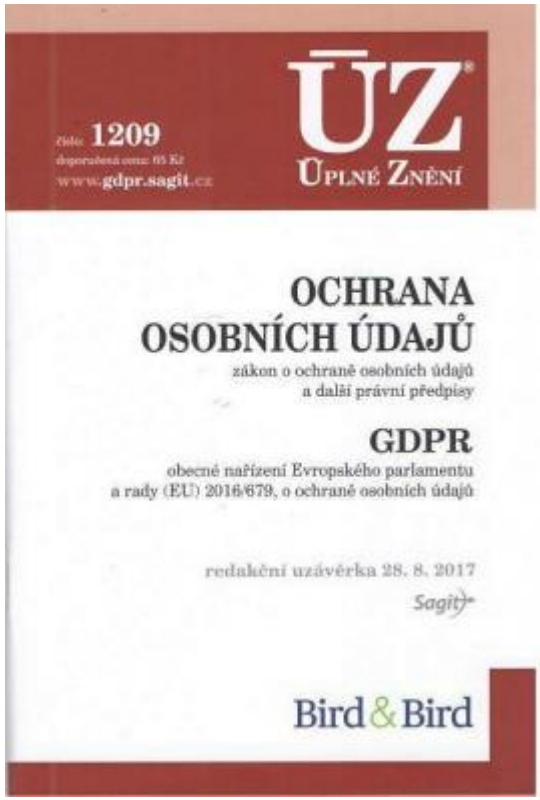
- není
- zacházení samotné za vás nikdo dělat nemůže
- třetí strany mohou pomoci, poskytnout servis, nastavení, vzory, připravit analýzu, záznamy…

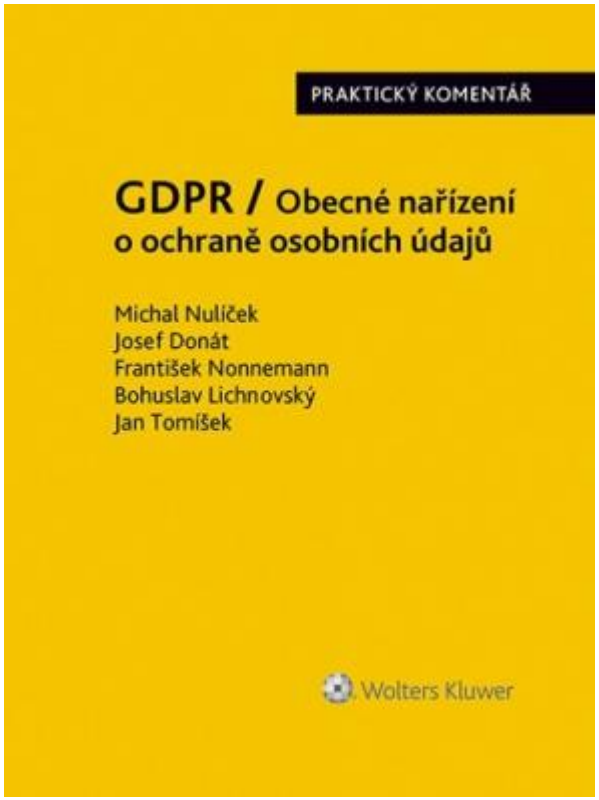
Česká lékárnická komora

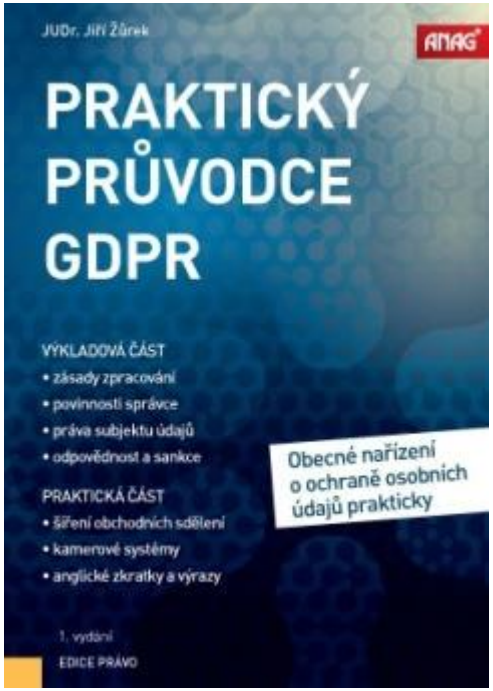
Jak se vzdělat?

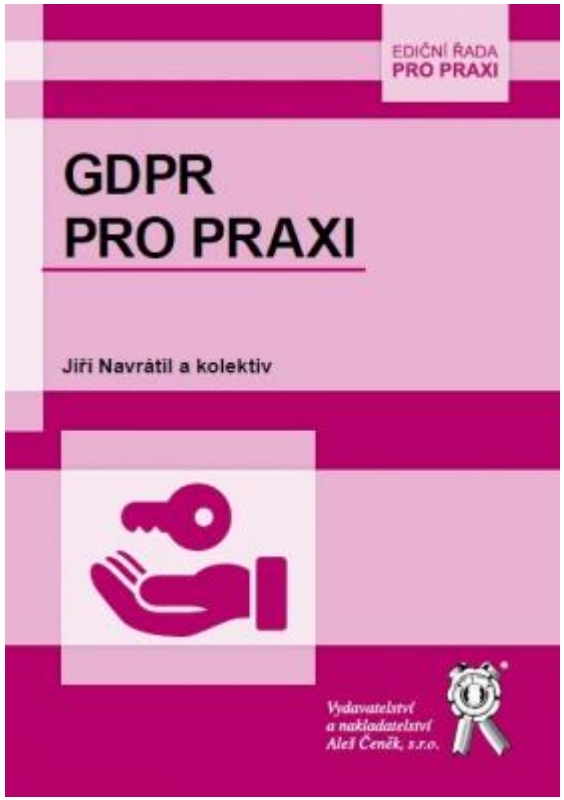
- trvalý proces, nutno se s tím smířit
- zdroje
  - GDPR samotné
  - literatura
  - internet, zejména stránky ÚOOÚ, MV, MZd
  - semináře

Česká lékárnická komora








EDIČNÍ ŘADA
PRO PRAXI
GDPR
PRO PRAXI
Jiří Navrátil a kolektiv
Vydavatelství
a nakladatelství
Aleš Čeněk, s.r.o.


Luděk Nezmar
GDPR
PRAKTICKÝ PRŮVODCE
IMPLEMENTACÍ
bezpečnost informací
hodnota dat
ISO 27001 a použití v GDPR
postupy, procesy, příklady
úkoly a povinnosti pověřence
identifikace zpracování
GRADA

Česká lékárnická komora

- http://www.mzcr.cz/Legislativa/dokumenty/metodika-implementace-gdpr-v-ambulantni-sfere_14867_3805_11.html

- http://www.mvcr.cz/gdpr/Default.aspx

úřad pro ochranu osobních údajů
the office for personal data protection

Česky | English

hledaný výraz

Témata

Základní odkazy | ÚŘAD · NÁZORY ÚŘADU · TISKOVÉ ZPRÁVY · ZAZNAMENALI JSME V MÉDIÍCH · KONTAKT

- Povinně zveřejňované informace
- **GDPR (obecné nařízení)**
  - Základní příručka
  - GDPR stručně (nové!)
  - Desatero zpracování pro správce
  - Desatero omylů
  - Dokumenty k GDPR
  - Otázky a odpovědi
  - Pokyny Pracovní skupiny WP29
  - GDPR nově
  - Role ÚOOÚ
  - Důležité odkazy

Cesta: Titulní stránka > Hlavní menu > GDPR (obecné nařízení)

GDPR (obecné nařízení)

Základní informace

Nařízení (EU) 2016/679 (GDPR) představuje právní rámec ochrany osobních údajů platný na celém území EU, který hájí práva jejích občanů proti neoprávněnému zacházení s jejich daty a osobními údaji. GDPR přebírá všechny dosavadní zásady ochrany a zpracování údajů, na nichž unijní systém ochrany osobních údajů stojí a potvrzuje, že ochrana cestuje přes hranice současně s osobními údaji.

V souladu s tím dále obecné nařízení rozvíjí a posiluje práva lidí dotčených zpracováním, a to v obou složkách: mít (získávat) informace o tom, které jejich údaje jsou zpracovávány a proč, a domáhat se dodržování pravidel, včetně nápravy stavu. GDPR klade systematicky důraz na vymahatelnost práv lidí a povinností správců (odpovědných za zpracování). Obsahuje proto propracovanější a náročnější pravidla pro zvláštní kategorie údajů a zpracování a současně vymáhá od správců a zpracovatelů výrazně aktivnější přístup, zejména se jedná o to, že před zahájením nového zpracování je třeba posoudit vliv jednotlivých zpracování na ochranu osobních údajů (DPIA) a zvolit vhodné nástroje ochrany údajů, za určitých podmínek si vyžádat předběžnou konzultaci u dozorového úřadu. Klíčem k nastavování povinností pro správce je rizikovost, která je dovozována z rozsahu zpracování, zpracovávaných osobních údajů a

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

Česká lékárnická komora

Hrozí mi kontrola ze strany ÚOOÚ? Nebudu pro smích kolegům, kteří neudělají nic?

- možná ano, ale kdo se směje naposled…
- kontrola krajně nepravděpodobná
- ÚOOÚ má malou kapacitu
- hrozí udání – konkurence, bývalí zaměstnanci, nespokojení pacienti, naschválisti
- práva subjektů nelze bez adaptace splnit
- a hlavně – mít pořádek se vyplatí

Česká lékárnická komora

Doporučení ČAK advokátům

informace o aktivitách některých … kolegů, kteří interpretují … GDPR …, přičemž jejich interpretace je podle všeho ne zcela přesná a přiměřená tomu, že jde o předpis, který ještě není účinný a jehož výklad se zcela jistě bude ještě ustalovat.

… vyzývá advokáty, aby – pokud poskytují právní poradenství v oblasti GDPR – tak činili s patřičnou odbornou péčí a profesionální zdrženlivostí a s vědomím odpovědnosti za škodu způsobenou nesprávnou informací nebo radou

Česká lékárnická komora

Všeobecné vyčkávání vs. 25. květen 2018

Není nač čekat, ale je iluze, že příprava může být dokonalá.

Půjde o trvalý proces podle vývoje interpretace GPDR po účinnosti.

I v lékárenské praxi velké množství sporných otázek.

Česká lékárnická komora

Konflikt mezi

- krajní obecností GDPR a
- nutností zavést zcela konkrétní opatření

Z nevýhody výhodu

- nejsem formálně svázán
- mohu GDPR uchopit jakkoliv, budu-li s ním v souladu a obhájím si to

Co dělat v lékárně?

- další výklad bude zaměřen na prostý lékárenský provoz
- zásilkový výdej (lékárenský eShop), věrnostní programy, předávání v rámci virtuálních řetězců, kamerové systémy, sledování pohybu nebo mailingu zaměstnanců, přenos OÚ do zahraničí a další je třeba vnímat jako další moduly, které je nutné přiřadit k běžnému provozu

Česká lékárnická komora

- zcela zásadní postavení v lékárenském provozu mají lékárenské informační systémy (LIT)
- drtivá většina zpracování v elektronické formě probíhá v nich
- poskytovatelé LIT jsou zpracovateli
- různé úrovně služeb
  - základní – jen zpracování, jako dosud
  - rozšířené – různé služby v oblasti GDPR

Česká lékárnická komora

Co dělat v lékárně?

- koupit

- většinu lze vést i elektronicky

Česká lékárnická komora

Co dělat?

- rozmyslet se, zda potřebuji **pověřence**
- uvažujeme lékárnu, která DPO nepotřebuje
- pozor na rozsáhlé zpracování zvláštní kategorie údajů
- o rozsáhlé by nemělo jít u provozovatele jedné nebo několika lékáren, který nepředává údaje třetím osobám vyjma zpracovatele nebo ZP či SÚKL
- velké řetězce určitě ano
- otázka u věrnostních programů, virtuálních řetězců, velkého eShopu

pokud pověřence nepotřebuji

připravit **materiál s rozborem důvodů**

I bez pověřence je vhodné mít ustanovenu osobu odpovědnou za ochranu OÚ.

Česká lékárnická komora

Co dělat?

- rozmyslet se, zda potřebuji **DPIA**
- uvažujeme lékárnu, která DPIA dělat nemusí
- neprovádí systematické a rozsáhlé automatizované zpracování zakládající rozhodnutí…
- neprovádí rozsáhlé zpracování zvláštních kategorií OÚ
- neprovádí rozsáhlé systematické monitorování veřejně přístupných prostorů

pokud DPIA nepotřebuji

připravit **materiál s rozborem důvodů**

- i bez DPIA je třeba
  - mít přehled o rozsahu zpracování OÚ
  - rizicích
  - zabezpečení
- k tomu ideálně záznamy o činnostech zpracování

Česká lékárnická komora

Co dělat?

Záznamy o činnostech

- musí každý provozovatel lékárny
- i když nemá 250 zaměstnanců, není jeho zpracování příležitostné a zpracovává zvláštní kategorie OÚ

Česká lékárnická komora

Co dělat?

Záznamy o činnostech

- neexistuje žádný závazný formulář
- každý si může připravit dle svého nebo využít služeb třetích osob
- možný vzor záznamů viz příloha

Česká lékárnická komora

Vzor záznamů o činnostech

- základní členění podle kategorie subjektu OÚ
- dále členění podle účelu
  - zvolit rozumné členění účelů
- ke každému účelu uvést všechny právní tituly a všechny způsoby zpracování
- následují samostatné řádky s jednotlivými údaji
- další kolonky vyjma poslední (Zabezpečení) se vyplňují na řádku ke každému údaji

Česká lékárnická komora

Vzor záznamů o činnostech

- jde o
  - kategorie OÚ
  - potřeba souhlasu subjektu OÚ
  - zdroj OÚ
  - forma OÚ
  - místo uložení
  - geografické umístění
  - přístup k OÚ podle pracovních pozic

Česká lékárnická komora

Vzor záznamů o činnostech

- kategorie příjemce
- geografické určení příjemce
- doba zpracování (lhůta pro výmaz)
- existence práva na výmaz
- existence práva na přenositelnost
- existence práva námitky
- automatizované zpracování s rozhodováním s právními účinky pro subjekt

- zabezpečení – souhrnně pro celý účel

Česká lékárnická komora

Vzor záznamů o činnostech

- vzor obsahuje
  - příklady pro vyplnění polí
  - vzor vyplnění pro účel Výdej léků na eRecept
- kompletně vyplněný vzor by měl obsahovat veškeré zacházení se všemi osobními údaji všech kategorií subjektů pro všechny účely
- příprava záznamů by současně měla vést k nápravě zjištěných nesouladů s GDPR

Česká lékárnická komora

Přehled rizik

- kromě záznamů o činnostech by měl být pořízen přehled alespoň nejzřejmějších rizik zpracování s určením míry rizika (zanedbatelné, nízké, střední, vysoké) a opatření rizika omezující
- opatření budou spočívat zejména ve způsobech zabezpečení

Česká lékárnická komora

Příklady nebezpečí

- kybernetická bezpečnost
  - nedostatečná ochrana hesly
  - pohyb uživatelů na jednom přístroji
  - vkládání vlastních nosičů
  - sdílení hesel

Česká lékárnická komora

Příklady nebezpečí

- pracovní zvyklosti a uspořádání pracoviště
  - volně přístupné šanony, stoly, kanceláře
  - přílišná důvěra mezi zaměstnanci
  - zaskakování
  - volné prostory
  - monitor viditelný pacientem

Česká lékárnická komora

Příklady nebezpečí

- používání elektřiny
- mechanické poškození
- povětrnostní vlivy
- lidský faktor
- pracovní pokyny
- organizace práce
- firemní kultura

Česká lékárnická komora

Směrnice pro zaměstnance

- ze záznamů o činnosti a přehledu o rizicích lze připravit směrnici pro zaměstnance obsahující zejména soubor pravidel a pokynů
  - užívání hesel
  - pravidla přístupů k OÚ
  - pravidla pro telefonní kontakt a mailový styk
  - uzamykání skříní, stolů, místností
  - neponechávání listin volně
  - skartace průvodek
  - atd.

Česká lékárnická komora

Co dělat?

- zvážit, zda pro některý účel potřebuji souhlas subjektu
- pokud ano, pak
  - zrevidovat staré souhlasy
  - připravit nové
  - zajistit jejich získání od subjektů
  - zavést jejich evidenci

Česká lékárnická komora

Co dělat?

- promyslet způsoby, jimiž budu schopen naplnit <u>práva subjektů</u>
  - připravit si vzorovou informaci o zpracování, je-li to nutné
  - připravit si postup pro vyřízení žádosti o
    - přístup vč. kopie OÚ
    - přenositelnost
    - omezení zpracování
    - výmaz
  - evidence žádostí a jejich vyřízení

Česká lékárnická komora

Co dělat?

- uzavřít smlouvy o zpracování se všemi zpracovateli

Česká lékárnická komora

Co dělat?

- proškolit zaměstnance
- vést o školeních záznamy
- opakovat školení alespoň 1x ročně

Česká lékárnická komora

Co dělat?

- průběžně vyhodnocovat zacházení s OÚ v lékárně
- rozpoznávat nové způsoby zpracování
- sledovat vývoj v interpretaci GDPR
- přizpůsobovat se novinkám

Česká lékárnická komora

Co do šanonu - opakování?

- záznamy o činnosti
- přehled rizik
- směrnice pro zaměstnance
- vzor souhlasu subjektu OÚ
- evidence souhlasů
- vzor informace o zpracování
- postup pro vyřízení žádostí subjektů

Česká lékárnická komora

Co do šanonu - opakování?

- evidence žádostí subjektů
- smlouvy se zpracovateli
- záznamy o školeních zaměstnanců
- rozbor, proč nepotřebuji pověřence
- rozbor, proč nemusím provést DPIA

Česká lékárnická komora

ČLnK

- komora nemůže zavádět GDPR v jednotlivých lékárnách, příliš individuální
- ambice připravit vzorové záznamy o činnostech pro základní provoz lékárny – nutná součinnost s lékárnami
- plus některé další materiály
- výhledově ve spolupráci s ÚOOÚ kodex pro provozovatele lékáren

Česká lékárnická komora

Lékové záznamy

- zde míněny záznamy vedené lékárnou
- typický příklad sporného zacházení
- jde o plnění smlouvy nebo zacházení na základě souhlasu?
- jde o zákonnou povinnost?
- jak se vypořádat s právem na výmaz?
- je jejich vyhodnocování povinné?

Česká lékárnická komora

eRecept

- je identifikátor eReceptu osobním údajem?
- je telefon uvedený na receptu od lékaře údajem podléhajícím souhlasu?
- které údaje podléhají výmazu?
- jak nakládat s průvodkou?

Česká lékárnická komora

Databáze pacientů

- databáze pacientů jen se jménem, telefonním číslem – účel?, právní důvod?, výmaz?

Česká lékárnická komora

Děkuji za pozornost