Ministerstvo zdravotnictví ČR
Ústav zdravotnických informací a statistiky ČR

Jak implementovat v ambulantní sféře

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY 2016/679

o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES do resortu zdravotnictví

2018

EVROPSKÁ UNIE
Evropský sociální fond
Operační program Zaměstnanost

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

ÚZIS

Jak implementovat v ambulantní sféře

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 (obecné nařízení o ochraně osobních údajů)

do resortu zdravotnictví

(na co si dát pozor v ambulantní sféře)

V Praze dne 26. ledna 2018

(Poznámka: **verze určená k plošnému připomínkování**; doplněno po konzultaci s MV ČR a ÚOOÚ v lednu 2018 a dále doplněno na základě konzultace s ambulantními specialisty)

Autorský kolektiv: Mgr. JUDr. Vladimíra Těšitelová, zástupce ředitele ÚZIS ČR
JUDr. Radek Policar, náměstek ministra zdravotnictví
doc. RNDr. Ladislav Dušek, Ph.D., ředitel ÚZIS ČR

Obsah

Přílohy:

1. Úvod

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 (obecné nařízení o ochraně osobních údajů), jako nový právní předpis týkající se ochrany osobních údajů, nabude účinnosti od 25. května 2018. V anglickém jazyce jde o „General Data Protection Regulation“, ve zkratce „**GDPR**“. Jelikož tato zkratka je již široce zavedena a používána, budeme ji používat i v tomto dokumentu.

V současné době na úrovni EU působí pracovní skupina WP 29, která již vydala několik výkladových stanovisek k jednotlivým článkům GDPR a vodítka pro posouzení vlivu na ochranu osobních údajů. Skupina WP 29 byla vytvořena na základě článku 29 směrnice 95/46/EC a je evropským poradním orgánem na ochranu údajů a soukromí. S účinností GDPR se z tohoto tělesa stane Evropský sbor pro ochranu osobních údajů (EPDB).

Hlavní motivací autorů tohoto textu je přispět k lepší orientaci poskytovatelů ambulantní zdravotní péče v dané problematice. Velkým problémem GDPR je totiž jeho obecnost a nejednoznačnost, a to zejména z toho důvodu, že se vztahuje obecně na všechny oblasti, kde se s ochranou osobních údajů fyzických osob běžně potkáváme. Situaci bohužel nezlepšují ani samotní tvůrci GDPR, kteří dosud nevydali jednoznačné a kompletní prováděcí předpisy a pravidla k uvedenému právnímu předpisu. Vzhledem k tomu, že GDPR je novou normou, neexistuje v současné době aplikační praxe, resp. příslušná judikatura, která by obsahovala kodifikaci výkladových pravidel.

Připomínky k nejasnostem některých ustanovení GDPR jsou tak extenzivně debatovány v řadě významných evropských projektů a platforem a z těchto důvodů lze v budoucnosti jistě očekávat další zpřesňování výkladu některých ustanovení.

V následujícím dokumentu čtenáři naleznou vybrané praktické rady a také návrhy konkrétních kroků k implementaci GDPR zpracované formou odpovědí na některé často kladené otázky. Nejedná se o závazné pokyny či komplexní popis problematiky ochrany osobních údajů v ambulantní praxi. Dokument vzhledem ke své stručnosti nemá ambici podat vyčerpávající přehled všech aspektů týkajících se GDPR, jde o základní přehled problémů, se kterými se může setkat ambulantní segment zdravotní péče při implementaci GDPR v praxi.

Věříme, že text usnadní praktickým lékařům a ambulantním specialistům orientaci v problematice a usnadní jim vlastní zavedení těchto zásad do praxe.

2. Co to je GDPR

2.1. Charakteristika právní úpravy

Oficiální název je 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 (Obecné nařízení o ochraně osobních údajů). Jeho účinnost je stanovena od 25. května 2018.

GDPR je právní předpis, který sebou nese přímou aplikovatelnost na všechny fyzické a právnické osoby, aniž by byla nutná jeho implementace do národních právních řádů. Jedná se o obecné nařízení, jehož účinnost nastává automaticky v plném rozsahu s výjimkou ustanovení, které členským státům umožňují/ukládají upravit si danou věc na vnitrostátní úrovni zákony, resp. legislativními akty. Těchto „výjimek" je relativně mnoho, zejména pro resort zdravotnictví.

GDPR je právním předpisem, který má celosvětový dopad, neboť se vztahuje na všechny subjekty, které nakládají s osobními údaji občanů EU nebo mají sídlo na území EU.

Vztahuje se nejen na správce, ale i na zpracovatele osobních údajů. Ukládá povinnosti všem subjektům, které se na nakládání s osobními údaji podílí; sankce za porušení pak mohou být rovněž ukládány každému takovému subjektu.

2.2. Možnosti úpravy národními právními předpisy

GDPR umožňuje či dokonce ukládá úpravu národními právními předpisy v některých případech (cca 50 ustanovení), které umožňují odchylnou či zpřesňující úpravu oproti GDPR. Resortu zdravotnictví se dotýká celá řada z nich a je možné konstatovat, že Česká republika v celé řadě ustanovení nové právní regulaci GDPR vyhovuje.

Právní úprava týkající se zpracování osobních údajů v resortu zdravotnictví je již nyní obsažena v zákonech regulujících oblast resortu zdravotnictví. Připomeňme si některé z nich:

- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdější pozdějších předpisů, který bude zrušen a bude nahrazen novým zákonem, jenž však nepřevezme z dosavadního zákona ustanovení, která jsou již součástí přímo použitelného obecného nařízení;
- zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů – explicitně pro rezort zdravotnictví, zejména ustanovení týkající se zdravotnické dokumentace či NZIS;
  Konkrétní příklad:
  Pro vedení zdravotnické dokumentace jsou to ustanovení § 53 – 69 o zdravotnické dokumentaci a navazující prováděcí vyhláška MZ č. 98/2012 Sb., o zdravotnické dokumentaci.
  Pro správu NZIS a povinnosti ÚZIS ČR jako správce jsou to ustanovení § 70 – 78 a navazující prováděcí vyhlášky MZ č. 373/2016 Sb., o předávání údajů do Národního zdravotnického informačního systému.

- zákon č. 373/2011 Sb., o specifických zdravotních službách, ve znění pozdějších předpisů;
  Konkrétní právní úprava práv a povinností pacientů a poskytovatelů zdravotních služeb a práv a povinností dalších právnických a fyzických osob v souvislosti s poskytováním specifických zdravotních služeb, zahrnující i zpracování osobních údajů, vč. jejich předávání dalším příjemcům.
- zákon č. 374/2011 Sb., o zdravotnické záchranné službě, ve znění pozdějších předpisů;
  Konkrétní právní úprava práv a povinností poskytovatelů zdravotnické záchranné služby, řešení krizových a mimořádných událostí, zahrnující i zpracování osobních údajů.
- zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů;
  Konkrétní příklad:
  Povinnosti poskytovatelů při vykazování hrazených zdravotních služeb zdravotním pojišťovnám, vč. údajů o pojištěncích
- zákon č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech), ve znění pozdějších předpisů;
  Konkrétní příklad:
  Pravomoci správních orgánů v oblasti humánních léčiv či veterinárních léčiv, vč. sběru a zpracování osobních údajů, centrální úložiště receptů
- zákon č. 268/2014 Sb., o zdravotnických prostředcích a o změně zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů;
- zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů;
  Konkrétní příklad:
  Dle ustanovení §79 jsou orgány ochrany veřejného zdraví oprávněny ke sběru osobních údajů a jsou zde stanoveny konkrétní podmínky jejich zpracování.
- zákon č. 285/2002 Sb., o darování, odběrech a transplantacích tkání a orgánů a o změně některých zákonů (transplantační zákon), ve znění pozdějších předpisů;
- zákon č. 296/2008 Sb., o zajištění jakosti a bezpečnosti lidských tkání a buněk určených k použití u člověka a o změně souvisejících zákonů (zákon o lidských tkáních a buňkách), ve znění pozdějších předpisů;
- atd.

Výčet uvedl pouze některé z platných zákonů a nesmíme zapomenout také na jejich prováděcí právní předpisy.

Obecně můžeme konstatovat následující: správce či zpracovatel, který v současnosti dodržuje zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdější pozdějších předpisů a dále zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů, má dobrý základ pro implementaci GDPR již hotov.

3. GDPR v praxi poskytovatelů ambulantních zdravotních služeb

Každý poskytovatel zdravotních služeb si jistě klade základní otázku: jakými kroky a kde začít a co konkrétně dělat? Jak promítnout do běžné praxe implementaci GDPR? Následující shrnutí přináší stručný nástin základních kroků a odpovědí na vybrané otázky. Nejde přitom o nijak složitou sadu opatření – nejprve je nutné vypracovat vlastní přehled typů osobních údajů, se kterými ambulance pracuje, specifikovat důvody, proč tak činí, a dále popsat procesy a nástroje, kterými tak činí. Vstupem do GDPR je tedy jakýsi audit práce s osobními údaji a z něho vyplývající další případná opatření.

3.1. Vztahuje se GDPR na ambulantní sféru?

Odpověď zní zcela jednoznačně ano. Pro resort zdravotnictví platí v dosud vydaných ustanoveních výše zmíněné pracovní skupiny WP29 jedna výjimka pro ambulantní sféru. Poskytovatelé primární ambulantní péči nemusí nutné zpracovávat tzv. posouzení vlivu na ochranu osobních údajů. Tato výjimka však nijak nemění povinnosti vyplývající z ostatních ustanovení GDPR a ambulantní praxe se tak implementaci pravidel GDPR nemohou vyhnout.

Široké spektrum typů ambulantní péče pak ovšem určuje i rozsah potřebných opatření. Jiný přístup budou vyžadovat ordinace o síle jednoho lékaře s jednou zdravotní sestrou, jiný poskytovatelé zdravotních služeb čítající velké množství zdravotnických pracovníků.

3.2. Kdo se bude v ambulanci věnovat ochraně osobních údajů?

První odpovědí je, že odpovědnost za ochranu osobních údajů leží na správci. Zlaté pravidlo GDPR, nehledě na jakýkoliv metodický návod, zní: Odpovědnost za ochranu osobních údajů leží pouze a jedině na správci či zpracovateli osobních údajů. Dokonce ani vydané osvědčení souladu s GDPR nezbavuje správce či zpracovatele jejich trvalé odpovědnosti.

Konkrétní implementaci GDPR by se měl věnovat v ideálním případě interní zaměstnanec, však není vyloučena ani externí spolupráce.

Potřebné personální zajištění implementace GDPR se samozřejmě odvíjí od velikosti ambulance či zdravotnického zařízení. S přihlédnutím k rozsahu zpracovávaných úkolů se tak může jednat o jednotlivce či o spolupracující tým více pracovníků. V případě ambulancí s jedním lékařem či zdravotní sestrou to může být lékař sám či je možné zvolit spolupráci s jinými poskytovateli zdravotních služeb a společně zvolit externí zajištění. Vše je na rozhodnutí samotného správce.

3.3. Je nutné jmenovat pověřence pro ochranu osobních údajů, a kdo jím může být?

Jmenování pověřence pro ochranu osobních údajů v případě jednotlivé ambulance není vyžadováno. V konečném důsledku to znamená, že ustavení pověřence pro ochranu osobních údajů je pouze doporučením např. ve velkých poliklinikách.

Jedním z prvních kroků při implementaci GDPR by mělo být jmenování (určení) pozice tzv. pověřence na ochranu osobních údajů (DPO z anglického „Data Protection Officer"). Pověřenec pro ochranu osobních údajů avšak není nutně tím, kdo bude zpracovávat všechny implementační kroky. Tato pozice by měla být zřízena pouze pro dohled nad implementací GDPR a jako konzultační podpora.

Vlastní pracovní postavení pověřence pro ochranu osobních údajů není nijak striktně vymezeno. Tuto funkci může zastávat zaměstnanec zodpovídající za bezpečnost informací, pracovník zodpovídající za IT systémy, zaměstnanec zodpovědný za nastavení ISO norem anebo zaměstnanec právního oddělení. Tento zaměstnanec bude spolupracovat:

- se všemi zaměstnanci zpracovávajícími osobní údaje,
- s odbornými pracovišti v případě, kdy vyvstanou konkrétní otázky (např. právního charakteru – právní oddělení či externí právník, technologie IT – interní zaměstnanec s odpovědností za IT či externí dodavatel).

Ve vztahu k ambulantním poskytovatelům zdravotních služeb se nutně nabízí otázka, zda vůbec jmenovat pověřence pro ochranu osobních údajů a kdo může být pověřencem pro ochranu osobních údajů zejména v malých v ambulantních zdravotnických zařízeních. Ustanovení GDPR obecně uvádí, že správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy:

a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;
b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli povaze, rozsahu nebo účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů;
c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Z uvedeného vyplývá, že poskytovatel lůžkové péče jmenuje pověřence pro ochranu osobních údajů ve většině případů. U ambulantních poskytovatelů je jmenování pověřence pro ochranu osobních údajů zcela dobrovolné. S přihlédnutím k jejich organizační struktuře a velikosti, může být jmenován pověřenec pro ochranu osobních údajů, a pokud jmenován bude, může být jmenován jediný pověřenec pro ochranu osobních údajů pro několik správců/zpracovatelů. Rovněž je možné obsadit tuto pozici pomocí externího dodavatele. Vždy je však nutné splnit podmínku jeho snadné dosažitelnosti.

Jmenovaný pověřenec pro ochranu osobních údajů musí dále splňovat tyto podmínky:

- musí mít neomezený přístup k tomu, kdo určuje zpracování osobních údajů (správci – tedy lékaři),
- musí mít přístup k veškerým informacím týkajícím se zpracování osobních údajů,
- nesmí být ve střetu zájmů (zjednodušeně řečeno: sám jediný lékař v ordinaci nemůže býti sám sobě pověřencem pro ochranu osobních údajů).

Pověřenec tedy může být interním zaměstnancem s tím, že v organizační struktuře je jeho zařazení přímo pod statutárním orgánem organizace či v obdobném postavení, které splňuje základní požadavky uvedené výše. Pověřenec může být i externím dodavatelem.

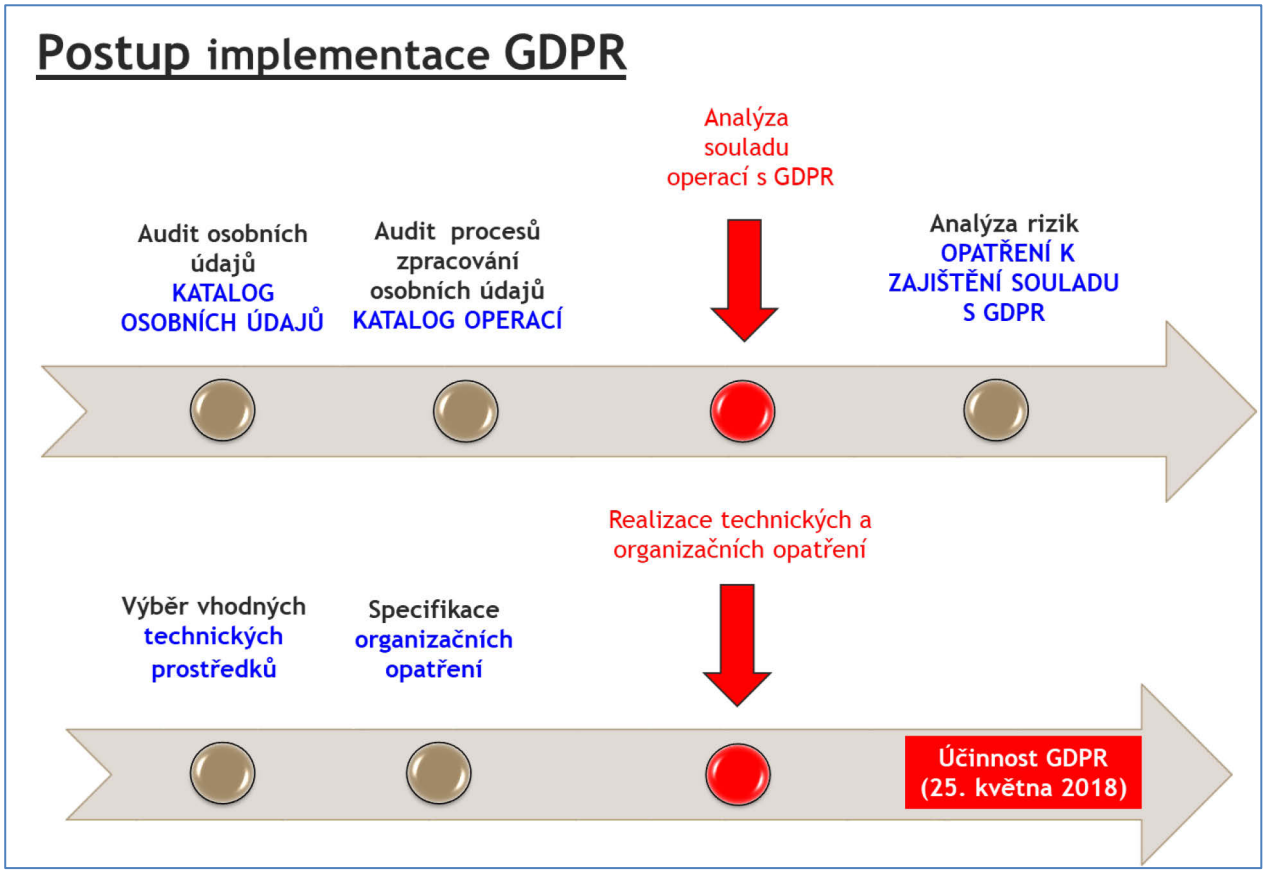
Každá jednotlivá ambulance o síle jednoho lékaře a jedné zdravotní sestry nemusí mít jmenovaného pověřence pro ochranu osobních údajů, na straně druhé není vyloučené, aby měla společného pověřence pro ochranu osobních údajů s jinými poskytovateli zdravotních služeb.

3.4. Čím začít?

Pracovníci zodpovědní za zajištění implementace GDPR, či lékař samotný, by si v úvodu měli zodpovědět některé základní otázky, které s implementací souvisí a po vyhodnocení odpovědí na ně zpracovat velmi jednoduchý dokument, vč. harmonogramu jednotlivých kroků. Zjednodušeně jde o inventuru zpracovávaných osobních údajů a operací, které jsou s nimi prováděny.

Kontrolní seznam základních parametrů implementace GDPR je uveden v příloze č. 1 tohoto dokumentu.

Konkrétní postup implementace u každého správce je plně v jeho moci, resp. záleží na jeho rozhodnutí. Jednou z možností je následující postup, který je postupem doporučeným. Může zahrnovat následující postupy, které by měly být promítnuty do časové osy harmonogramu:



3.5. Inventura osobních údajů

Základním doporučujícím implementačním krokem je inventura osobních údajů, a tedy konkrétně **zpracování katalogu osobních údajů a katalogu operací** s nimi realizovaných v organizaci.

3.5.1. Katalog osobních údajů

Na samotném počátku postupu je vhodné zpracovat katalog osobních údajů, vč. jejich kategorizace. Jedná se o užitečný nástroj a vhodný první krok. Jedná se o revizi všech osobních údajů, se kterými správce, resp. zpracovatel nakládá.

V případě resortu zdravotnictví by se mělo jednat zejména o členění osobních údajů na:

- standardní osobní údaje,
- zvláštní kategorie osobních údajů (citlivé osobní údaje).

Katalog osobních údajů by měl zároveň obsahovat specifikaci účelu, resp. právního titulu, jejich zpracování a rozsah oprávněných zájmů. Ke všem osobním údajům by měly být zároveň přiřazeny jednotlivé informační systémy či jiné datové zdroje, ve kterých jsou tyto údaje shromážděny a uchovávány.

Přesná struktura, resp. forma katalogu osobních údajů není stanovena. Přístupy k tvorbě katalogu osobních údajů mohou být různé, v **příloze č. 2** jsou zpracovány ukázky možného přístupu ke zpracování. Ke kategorizaci osobních údajů lze přistupovat z pohledu datového zdroje, informačního systému, organizační složky poskytovatele zdravotních služeb apod.

3.5.2. Katalog operací zpracování osobních údajů

Zpracování přehledu všech procesů zpracování ve vazbě na jednotlivé kategorie osobních údajů je dalším doporučujícím krokem implementace GDPR. Katalog operací by měl obsahovat zejména:

- příjemce, resp. kategorie příjemců,
- typy zpracování (např. validace dat, nahlížení apod.).

Katalog operací by měl zohledňovat zejména standardní životní cyklus zpracování osobních údajů, tedy konkrétně:

- sběr,
- uchovávání,
- validaci, analýzu či jinou formu konkrétního zpracování či využití,
- předávání,
- likvidaci
- atd.

Ke všem operacím by měly být přiřazeny jednotlivé informační systémy, jichž bude při operacích využito, pokud tomu tak je.

Přesná struktura, resp. forma katalogu operací s osobními údaji není stanovena. V **příloze č. 2** je vypracována velmi jednoduchá osnova pro zpracování katalogu operací s osobními údaji.

Zpracováním katalogu osobních údajů a katalogu operací s nimi prováděnými, stejně jako přehledu o tom, kde jsou uvedené operace dokumentovány a kdo je za ně odpovědný, získává ambulance základní dokumenty, kterými bude dokládat připravenost na implementaci GDPR. Vznik a pravidelnou aktualizaci těchto dokumentů lze označit za základní krok. V podstatě jde o základní inventarizaci zpracovávaných údajů. Zároveň jde o vstup do analýzy souladu s GPDR neboli vytvoření záznamů o činnostech zpracování, kterými se soulad prokazuje.

Vypracování výše uvedených dokumentů nepřináší nutně žádnou novou administrativní zátěž, jde skutečně o inventarizaci stávajícího stavu. Poskytovatel ambulantních zdravotních služeb může

katalog osobních údajů a katalog operací zpracování osobních údajů vypracovat jako přehledové tabulky při využití již nastavených číselníků v jeho informačních systémech nebo se domluvit s dodavatelem IT technologií na zpracování speciálního SW, který dané seznamy vygeneruje.

3.6. Analýza souladu

Po inventuře osobních údajů (kapitola 3.5) by poskytovatel ambulantních služeb měl zpracovat analýzu souladu s GDPR. Jejím hlavním cílem je vyhodnocení, jak jsou plněny zásady GDPR a jednotlivé povinnosti stanovené správci či zpracovateli osobních údajů.

Obecné informace k analýze souladu jsou uvedeny níže a příloha č. 3 dále přináší praktický návod na její zpracování.

Jedním ze dvou základních principů, na kterých je založeno GDPR, je princip odpovědnosti správce. Správce musí dodržet zásady obsažené v čl. 5 odst. 1 GDPR a zároveň musí být schopen tento soulad doložit. Právě k tomu slouží zmíněná analýza souladu. Analýzu souladu by následně měl posoudit pověřenec pro ochranu osobních údajů, je-li jmenován. Ke zpracovanému katalogu operací zpracování osobních údajů je nezbytně nutné přiřadit adekvátní povinnosti dle GDPR. Výsledkem je stav připravenosti na GDPR.

K prokázání, resp. doložení souladu mohou sloužit též kodexy chování zaměstnanců, získání osvědčení či certifikace a zejména záznamy o činnostech zpracování.

Ke zpracování záznamů o činnostech zpracování lze přistoupit různým způsobem, je však nezbytně nutné dodržet základní parametry stanovené GDPR, a to bez výjimky. Záznamy o činnostech zpracování se liší dle typu subjektu, který má povinnost tyto záznamy o činnostech zpracování vést. Jsou tedy odlišné pro správce a zpracovatele.

V **příloze č. 3** je v obecných bodech naznačena struktura prokázání souladu založená na záznamech o činnostech zpracování, která by měla tvořit ucelenou dokumentaci. Záznamy o činnostech zpracování představují souhrn veškeré dokumentace, která je vedena ke zpracování osobních údajů, ať již správcem, tak i zpracovatelem. Jeho obsahem mohou být jak konkrétní právní předpisy, resp. právní analýza či rozbor, pokud se jedná o zákonem stanovené povinnosti či dokumentace jednotlivých informačních systémů dodávaná dodavatelem informačních technologií. Nezbytnou součástí je i souhrn vnitřních normativních aktů organizace (ambulance) týkajících se ochrany osobních údajů i bezpečnosti informací.

Záznamy o činnostech zpracování obsahují v ideálním případě nejen informace explicitně stanovené v GDPR v členění dle správce a zpracovatele, ale i komplex ucelené dokumentace jednotlivých IT systémů (např. obsah systémů, dokumentace k jejich bezpečnosti apod.), ale také ucelený systém vnitřních právních předpisů organizace, který kodifikuje ochranu osobních údajů, např. i včetně bezpečnostní dokumentace či dokumentace norem ISO.

U menších subjektů je nutné tyto záznamy o činnostech zpracování přizpůsobit velikosti ambulance. Základním cílem je mít zmapovány všechny činnosti zpracování alespoň v rozsahu, který je jmenovitě, resp. taxativně dán GDPR.

3.7. Analýza a hodnocení rizik

Dalším krokem či krokem souběžným by měla být analýza rizik. Dle konzultace s MV ČR dne 10. ledna 2018 není nezbytné v případě zpracování na základě zákona, což u poskytovatelů zdravotních služeb je v případě vedení zdravotnické dokumentace beze sporu zákon o zdravotních službách a jeho prováděcí předpisy, analýzu rizik, resp. posouzení vlivu na ochranu osobních údajů provádět. Hlavní význam této činnosti odpoví na otázku, zda v organizaci existují či neexistují rizika pro práva a svobody subjektů údajů. V případě existence rizika je nutné vytvořit systém jejich hodnocení a rozčlenit je na kategorie. Tento proces je zcela nezbytný pro následné kroky, na které GDPR pamatuje (např. konzultace s dozorovým úřadem v případě detekovaného vysokého rizika pro práva a svobody subjektu údajů).

Analýzu a hodnocení rizik obecně popisuje tato kapitola a praktický návod na její zpracování je připraven v příloze č. 4.

Analýza a hodnocení rizik je hlavním principem implementace GDPR. Přístup založený na riziku znamená, že správce či zpracovatel jsou si vědomi existujících rizik, tato umí vyhodnotit a kategorizovat dle závažnosti a následně rozhodnout o přijetí opatření ke snížení a eliminaci rizika. Pro riziko existuje celá řada definic, které v tomto krátkém textu nelze rozebírat. Obecně můžeme riziko definovat jako součin velikosti následků nežádoucí události a pravděpodobnosti, že k uvedené nežádoucí události dojde.

Analýza rizik by měla obsahovat stanovení **pravděpodobnosti** a **míry rizika**, a to vzhledem k **povaze**, **rozsahu**, **kontextu** a **účelu** zpracování osobních údajů.

Z pohledu analýzy rizik by mělo být stanoveno, zda zpracování osobních údajů představuje **riziko** nebo **vysoké riziko** pro práva a svobody subjektu údajů.

Na základě analýzy rizik by měl být zpracován návrh konkrétních opatření ke snížení pravděpodobnosti a závažnosti rizik identifikovaných analýzou.

Proces analýzy, hodnocení a řízení rizik je základem implementace úspěšného systému řízení ochrany osobních údajů, resp. ochrany práv a svobod subjektů osobních údajů. Souvisí s bezpečnosti informací (ISMS) a tvoří významnou součást standardu ISO/IEC 27001. Pouze tím, že se plně porozumí rizikům, se zajistí, že zavedené kontroly jsou dostatečné k tomu, aby poskytly odpovídající úroveň ochrany před ohrožením práv a svobod subjektů osobních údajů.

Pravidelné vyhodnocování rizik a uplatňování komplexních kontrol je zásadní pro trvalou důvěru klientů a pro plnění povinností při ochraně osobních a jinak citlivých informací před příliš častými hrozbami.

Tímto postupem je zajištěno, že rizika jsou účinně řízena a kontrolována.

3.8. Technická a organizační opatření

Z již zpracované analýzy rizik i analýzy souladu pak může vyplynout:

- skutečnost, že technická a organizační opatření přijatá v ambulanci jsou dostatečná; v takovém případě se pouze připojí či stanou součástí komplexní dokumentace zpracování a ochrany osobních údajů v organizaci

nebo

- fakt, že je nutné přijetí nových technických a organizačních opatření.

Nově přijímaná opatření by měla odpovídat stupni nebezpečnosti zjištěných rizik.

Technická opatření spočívají ve výběru vhodných technických prostředků ochrany osobních údajů. Stejně jako v případě ostatních konkrétních implementačních kroků je možné vycházet z bezpečnostních norem ISO 27002 a je vhodné zavést systém řízení bezpečnostních opatření podle normy ISO 27001. Je tedy možné přiměřeně použít dokumentaci pro certifikaci, resp. aplikovat normy kvality ISO.

V případě organizačních opatření je důležité nezapomenout následně odpovídajícím způsobem upravit vnitřní normativní akty nastavující pravidla chování zaměstnanců, pravidla přístupů k osobním údajům a zejména pak i veškeré smlouvy o zpracování osobních údajů.

Parametry smlouvy o zpracování osobních údajů ve vazbě na jednotlivé články GDPR a povinnosti tam stanovené shrnuje příloha č. 5 tohoto dokumentu.

3.9. Jednání s dodavatelem IT technologií či jiným dodavatelem

V momentě, kdy z uceleného procesu vyplyne nutnost realizace technických opatření, je nutno zvážit, zda je možné realizovat opatření vlastními silami, eventuálně vlastním vývojem či úpravou IT nástrojů anebo zahájit jednání s dodavatelem IT technologií o změnách.

V případě zapojení dodavatelů je nutné zajistit nové smlouvy o zpracování osobních údajů tak, jak byly popsány v předcházejícím bodě 3.8. (viz též **příloha č. 5**).

3.10. Zpracování informací o zpracování osobních údajů pro pacienty

V momentě, kdy jsou zpracovány a k realizaci připravena technická i organizační opatření, je možné, resp. nutné zpracovat informaci pro pacienty či potenciální pacienty. Lze doporučit zpracovat základní informace o zpracování osobních údajů a jejich ochraně na webové stránky (zde je nutné sledovat legislativní proces nového zákona o zpracování osobních údajů nahrazujícího zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, který navrhuje možnost informovanosti subjektu údajů na webových stránkách v případech, kdy je právním titulem k jejich zpracování plnění právní povinnosti správcem či zpracovatelem) a dále připojit i právní rozbor, zejména co se týče právního titulu, tedy plnění právní povinnosti stanovené správci osobních údajů.

Na zvážení může být písemná informace předávaná v listinné podobě. **Obecné informace jsou uvedeny v příloze č. 6 tohoto dokumentu.**

3.11. Školení zaměstnanců

Jsou-li splněny všechny výše uvedené kroky, je nutné proškolit zaměstnance. Forma jejich proškolení, ať již osobní formou či elektronicky, je plně v kompetenci poskytovatele zdravotních služeb. O podstatě realizovaných opatření by měli býti proškoleni nejen zaměstnanci správce a

zpracovatele, ale i zaměstnanci či pracovníci dodavatelů či dalších zpracovatelů v případech řetězení zpracování.

O provedených školeních by měly být prováděny záznamy, explicitně prokazující pravidelná proškolení u všech zaměstnanců.

U organizačně menších jednotek stačí zjednodušená forma.

3.12. Audit a aktualizace

Je nutné nastavit frekvenci auditů provedených opatření a pravidla aktualizace.

Výše uvedený postup je nutné pravidelně a průběžně hodnotit a aktualizovat. Časová frekvence průběžného hodnocení by měla být stanovena vnitřními normativními akty správce či zpracovatele.

Časový harmonogram by měl zahrnovat:

a) pravidelnou lhůtu pro audit a aktualizaci,
b) ad hoc audity či aktualizace např. v případech porušení ochrany osobních údajů. Nezbytně však v případě zavádění nových operací zpracování osobních údajů.

Závěrem k této kapitole je nutné konstatovat, že každý správce by měl jednak ustanovit zaměstnance zodpovědného za ochranu osobních údajů či tým zaměstnanců, který bude řádnou ochranu osobních údajů zajišťovat. Kontrolní a konzultační role pak přísluší pověřenci pro ochranu osobních údajů. To nic nemění na skutečnosti, že s ochranou osobních údajů by měli býti seznámeni všichni zaměstnanci správce i jeho dodavatelé a měli by dodržovat nastavená pravidla vnitřními normativními akty správce.

Harmonogram nastavených kroků by měl být v ideálním případě připraven k 25. 5. 2018.

4. Závěr

Pro jednoduché propojení právních titulů zpracování dle GDPR na rozšířená práva subjektu údajů odkazujeme na **přílohu č. 7**.

Příloha č. 8 dále přináší odpovědi na nejčastěji kladené otázky k GDPR od různých typů ambulantních poskytovatelů zdravotních služeb.

A slova závěrem? Jen přání, aby se všem poskytovatelům zdravotních služeb implementace GDPR v rámci možností podařila!

Zdroje:

- Jak implementovat 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 (obecné nařízení o ochraně osobních údajů) do resortu zdravotnictví VERZE 1.1 - DOKUMENT URČENÝ K RECENZI A DALŠÍMU DOPRACOVÁNÍ INTERNÍ MATERIÁL, Autorský kolektiv: Mgr. JUDr. Vladimíra Těšitelová, zástupce ředitele ÚZIS ČR, JUDr. Radek Policar, náměstek ministra zdravotnictví, doc. RNDr. Ladislav Dušek, Ph.D., ředitel ÚZIS ČR, kolektiv zaměstnanců ÚZIS ČR
- 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 (obecné nařízení o ochraně osobních údajů)
- webové stránky Úřadu pro ochranu osobních údajů https://www.uoou.cz/obecne%2Dnarizeni%2Deu%2Dgdpr/ds-3938/p1=3938
- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdější pozdějších předpisů
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů
- zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů – explicitně pro rezort zdravotnictví, zejména ustanovení týkající se zdravotnické dokumentace či NZIS
- zákon č. 373/2011 Sb., o specifických zdravotních službách a podmínkách jejich poskytování (zákon o specifických zdravotních službách), ve znění pozdějších předpisů
- zákon č. 374/2011 Sb., o zdravotnické záchranné službě, ve znění pozdějších předpisů
- zákon č. 89/1995 Sb., o státní statistické službě, ve znění pozdějších předpisů
- zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
- zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů
- zákon č. 378/2007 Sb., o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech), ve znění pozdějších předpisů
- zákon č. 123/2000 Sb., o zdravotnických prostředcích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů
- zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů
- zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
- zákon č. 285/2002 Sb., o darování, odběrech a transplantacích tkání a orgánů a o změně některých zákonů (transplantační zákon), ve znění pozdějších předpisů
- zákon č. 296/2008 Sb., o zajištění jakosti a bezpečnosti lidských tkání a buněk určených k použití u člověka a o změně souvisejících zákonů (zákon o lidských tkáních a buňkách), ve znění pozdějších předpisů
- dokument pracovní skupiny WP29 obsahující vodítka k posouzení vlivu na ochranu osobních údajů a návod pro hodnocení úrovně rizika zpracování dostupné z https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=28330
- návrh adaptačního zákona k zákonu č. 101/2000 Sb., o ochraně osobních údajů
- dokument pracovní skupiny WP29 obsahující vodítka k přenositelnosti údajů dostupné z https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=28333
- dokument pracovní skupiny WP 29 obsahující vodítka k pověřencům pro ochranu osobních údajů dostupné z https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=28337
- Zákon o ochraně osobních údajů. Komentář, ISBN: 978-80-7179-226-0, JUDr. Alena Kučerová a kolektiv

- doporučení Komise 2003/361/ES
- zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

Příloha č. 1

Seznam nových povinností podle GDPR

Checklist – nové povinnosti

dle

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 (obecné nařízení o ochraně osobních údajů)

V následujícím přehledu je uveden demonstrativní výčet činností, na které se váží nové povinnosti dle GDPR a jedná se o demonstrativní výčet okruhů, nad kterými je nutné se zamyslet a zajistit následně jejich realizaci. V publikaci je pak jako výsledek těchto činností navržena jedna z možných cest pro realizaci konkrétních implementačních kroků.

1. jmenování **pověřence pro ochranu osobních údajů** (článek 37–39)
2. rozlišení **zpracování**, vč. informačního systému a databáze
3. pokud se jedná o společné zpracování a tím **existence společných správců**, je nutné uzavřít smlouvu podle čl. 26 a upravit si vzájemné vztahy
4. pokud má správce **zpracovatele** (článek 28), upravit vztahy (musí se upravit všechny i platné smlouvy podle § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů)
5. **posoudit rizikovost zpracování** (recitály 75 a 76) a promítnout do dalších povinností správce (čl. 25, 32–36)
6. jde-li o **připravované zpracování** – zpracovat záměrnou a standardní ochranu údajů (čl. 25)
7. rozhodnout, zda je nutno **provést hodnocení dopadu**, zejména u nových zpracování (článek 35)
8. existující zpracování – **dodatečná technická a organizační opatření** ve vazbě na GDPR
9. zaměřit se na to, zda je plněn **účel** zpracování a **kompatibilita dalších účelů** zpracování
10. **předmět** zpracování – jak osobní údaje, tak i subjekty (např. děti, pacienti, zaměstnanci atd.)
11. **zdroj** údajů – důležité pro zajištění informační povinnosti – rozlišit, zda-li jsou údaje získány od subjektu údajů či nikoliv (čl. 13 a 14)
12. **informační povinnost** subjektu údajů (čl. 13 a 14) – ideálně zpracovat písemně potvrdit, resp. připravit informace na webové stránky
13. zpracování procesu **vyřizování žádostí** dle GDPR
14. **prostředky zpracování** – zohlednit záměrnou a standardní ochranu dat (čl. 25)
15. **technická a organizační opatření** – jejich revize, resp. zpracování a aktualizace
16. **předávání** údajů – jaké, jak a komu se osobní údaje předávají + předávání do zahraničí
17. **zabezpečení** osobních údajů (čl. 32) podle rizikovosti zpracování rozšířenější oproti § 13 zákona 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů – obnovitelnost systému a pravidelné testování a audit
18. proces **ohlášení narušení** zabezpečení ÚOOÚ (čl. 33) a subjektům údajů (čl. 34)
19. **práva subjekt údajů**, které ano, které ne – resp. které jsou omezeny zákonem (čl. 12 až 22)
20. **řetězení** zpracování osobních údajů – zapojení do zpracování pouze takového dodavatele, který poskytuje dostatečné záruky
21. **likvidace** osobních údajů (čl. 17) – likvidační nebo skartační lhůty nebo prověřování potřebnosti dalšího vedení osobních údajů
22. **záznamy o činnostech zpracování** (čl. 30)
23. **vnitřní kontrola** - novelizace
24. **nezávislá kontrola** – osvědčení

atd.

Příloha č. 2

Katalog osobních údajů a katalog operací

KATALOG OSOBNÍCH ÚDAJŮ A KATALOG OPERACÍ

dle

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 (obecné nařízení o ochraně osobních údajů)

Obsah

1. Úvod

Ke zpracování katalogu osobních údajů lze přistoupit různými způsoby. Jednou z možností je přistoupit k rozčlenění katalogu osobních údajů na samotném počátku dle kategorií osobních údajů a právního důvodu jejich zpracování. Další možností, která se nabízí, je zpracování katalogu osobních údajů podle jednotlivých datových zdrojů a k tomu posléze přiřazení jejich kategorie, účelu i právního důvodu jejich zpracování. Další možnosti jsou nasnadě.

Jak již bylo řečeno několikrát, není dána oficiální forma či šablona uvedených katalogů, níže uvedené vzory jsou návodem k jejich vlastnímu zpracování správcem či zpracovatelem.

Tato šablona je zpracována tak, že obsahuje základní rozčlenění v celkové tabulce a následně pak popis jednotlivých jejích součástí ve sloupcích s možností jejich kategorizace a číselníkového vyjádření. Pro praktické užití je možné tabulku zpracovat ve formátu MS Excel s přednastavenými možnostmi vyplnění jednotlivých polí či domluvit se s dodavateli IT technologií na zpracování speciálního SW, který by uvedené parametry zautomatizoval.

V níže uvedené tabulce máte sloučen jak katalog osobních údajů, tak katalog operací v jeden dokument. Důvodem je praktické využití a vyloučení duplicitního zpracování, oddělení je bezesporu možné.

2. Základní rozčlenění

Hlavním cílem zpracování Katalogu osobních údajů je na počátku provedení inventury existujících zpracovávaných osobních údajů.

Základní parametry rozčlenění jsou:

a) datový zdroj
b) osobní údaj
c) subjekt osobních údajů
d) kategorie osobního údaje
e) právní titul zpracování
f) účel zpracování
g) informační systém
h) operace
i) kategorie příjemců
j) zdokumentovaný postup
k) odpovědnost
l) atd.

Toto členění však nemusí býti konečným. Může se nadále větvit do dalších atributů. Například je možné už v tomto případě přidat sloupec např. kategorie příjemců.

Jak již bylo uvedeno výše, v následujícím textu naleznete tabulku, která obsahuje navržené základní rozčlenění, které může býti dle vůle i potřeb správce libovolně doplňováno. V případech, kdy je to možné, je uvedeno i navrhované standardizované naplnění jednotlivých polí a jejich popis či číselník.

Dále je možné členit dle jednotlivých organizačních složek správce.

Datový zdroj	Osobní údaj	Subjekt osobních údajů	Kategorie osobních údajů	Právní titul	Získáno od subjektu údajů či nikoliv	Účel	Operace	Proces zdokumentován	Odpovědnost

2.1. Datový zdroj

Datovým zdrojem může být cokoliv, může se jednat o informační systém, datový sklad, databázi, datové centrum, ale může se jednat i o jednotlivý počítač.

Zároveň je nutné nezapomenout na listinné datové zdroje. Typickým příkladem je kartotéka či osobní spisy zaměstnanců, ale třeba také vizitky zaměstnanců.

Příklad:

Číselník

1. databáze
2. SW
3. disk
4. externí úložiště
5. databáze
6. listina
7. osobní spis
8. vizitka
9. atd.

2.2. Osobní údaje

Osobní údaje je vhodné uvádět vždy jeden údaj na jeden řádek. Pravda je, že tím získáváme poměrně rozsáhlou databázi, nicméně dle stanoviska ÚOOÚ je nutno osobní údaje takto strukturovat.

Příklad:

1. jméno
2. příjmení
3. pohlaví
4. datum narození
5. trvalé bydliště
6. okres
7. věk
8. diagnoza

2.3. Subjekt osobních údajů

Opět si můžeme pomoci číselníkem a mezi nejčastější subjekty osobních údajů mohou patřit např:

1. pacient
2. zaměstnanec
3. osoba blízká

2.4. Kategorie osobních údajů

Je zde uveden zvláštní sloupec na Kategorii osobních údajů, kdy je nutné rozlišit, zda se jedná o:

Číselník

1. standardní osobní údaj
2. zvláštní kategorii osobního údaje (citlivé osobní údaje)

2.5. Právní titul

Právní titul bezesporu představuje významný atribut, jehož určení následně určuje rozsah práv subjektu údajů a na to navazujících povinností správce.

Číselník

1. plnění právní povinnosti
2. životně důležitý zájem
3. souhlas subjektu údajů
4. plnění smlouvy
5. veřejný zájem, výkon pravomoci
6. oprávněný zájem správce

2.6. Osobní údaj získán od subjektu údajů či nikoliv

Rozlišení na to, od koho je osobní údaj získán, je nezbytné pro plnění některých povinností správce, např. v případě zajištění informovanosti subjektu údajů či řetězení zpracování, jak jest popsáno v dokumentu.

Číselník

1. osobní údaje získané od subjektu údajů
2. osobní údaje nejsou získány od subjektu údajů

2.7. Účel

Zjištění účelu je nezbytným jednak pro stanovení rozsahu zpracovávaných údajů za účelem splnění jedné ze základních povinností dle GDPR, a to zásady minimalizace zpracovávaných osobních údajů.

V případě, že políčko o příslušného účelu zůstane prázdné, jedná se o signál pro zúžení rozsahu zpracovávaných osobních údajů.

Příklad:

Osobní údaje jsou zpracovávány pro vlastní potřeby (managerské rozhodování, analýza dat, klinický výzkum) či pro potřeby třetích osob.

2.8. Operace a jejich katalog

Vzhledem k tomu, že existuje celá řada operací, které jsou používány standardně u jednotlivých kategorií osobních údajů. Jeví se velmi vhodným zavedení jednotného číselníku operací, které jsou s osobními údaji prováděny. Níže jsou uvedeny možné operace, které vycházejí jednak ze samotného GDPR a dále mohou odrážet i všechny další, resp. návazné operace, které jsou realizovány přímo v prostředí poskytovatele zdravotních služeb.

Číselník

Číslo operace	Název operace	Obsah operace
1	SHROMÁŽDĚNÍ	SBĚR OSOBNÍCH ÚDAJŮ
2	ZAZNAMENÁNÍ	UMÍSTĚNÍ OSOBNÍCH ÚDAJŮ V INFORMAČNÍCH ČI JINÝCH SYSTÉMECH
3	KONTROLA	POROVNÁNÍ JIŽ SHROMÁŽDĚNÝCH NEBO ZAZNAMENANÝCH ÚDAJŮ S ÚČELEM
4	STRUKTUROVÁNÍ	TRANSFORMACE OSOBNÍCH ÚDAJŮ
5	ULOŽENÍ	UKLÁDÁNÍ OSOBNÍCH ÚDAJŮ DO DATABÁZÍ
6	VALIDACE	KOREKCE SYSTÉMOVÝCH CHYB A ZKRESLENÍ
7	VYHLEDÁNÍ	APLIKAČNÍ A ANALYTICKÁ PRÁCE S OSOBNÍMI ÚDAJI
8	NAHLÉDNUTÍ	APLIKAČNÍ A ANALYTICKÁ PRÁCE S OSOBNÍMI ÚDAJI
9	POUŽITÍ	APLIKAČNÍ A ANALYTICKÁ PRÁCE S OSOBNÍMI ÚDAJI
10	ZPŘÍSTUPNĚNÍ PŘENOSEM	PŘEDÁNÍ OSOBNÍCH ÚDAJŮ
11	ŠÍŘENÍ NEBO JAKÉKOLIV JINÉ ZPŘÍSTUPNĚNÍ	ZPŘÍSTUPNĚNÍ ČI PUBLIKACE OSOBNÍCH ÚDAJŮ (ZPRAVIDLA AGREGACE)
12	SEŘAZENÍ ČI ZKOMBINOVÁNÍ	ANALYTICKÁ PRÁCE S OSOBNÍMI ÚDAJI
13	OMEZENÍ	OZNAČENÍ ULOŽENÝCH OSOBNÍCH ÚDAJŮ ZA ÚČELEM OMEZENÍ JEJICH ZPRACOVÁNÍ V BUDOUCNU
14	VÝMAZ NEBO ZNIČENÍ	
15	ZPŘÍSTUPNĚNÍ DALŠÍMU ZPRACOVATELI	ZPŘÍSTUPNĚNÍ NA ZÁKLADĚ SMLOUVY O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ
16	ANONYMIZACE	TAKOVÁ ZMĚNA OSOBNÍCH ÚDAJŮ, V JEJÍMŽ DŮSLEDKU JE PŘIŘAZENÍ OSOBNÍCH ÚDAJŮ URČITÉ FYZICKÉ OSOBĚ NEMOŽNÉ NEBO MOŽNÉ POUZE ZA NEPŘIMĚŘENÉHO VYNALOŽENÍ ČASU, NÁKLADŮ A PRACOVNÍHO ÚSILÍ.
17	PSEUDONYMIZACE	ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ TAK, ŽE JIŽ NEMOHOU BÝT PŘIŘAZENY KONKRÉTNÍMU SUBJEKTU ÚDAJŮ BEZ POUŽITÍ DODATEČNÝCH INFORMACÍ, POKUD JSOU TYTO DODATEČNÉ INFORMACE UCHOVÁVÁNY ODDĚLENĚ A VZTAHUJÍ SE NA NĚ TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, ABY BYLO ZAJIŠTĚNO, ŽE NEBUDOU PŘIŘAZENY IDENTIFIKOVANÉ ČI IDENTIFIKOVATELNÉ FYZICKÉ OSOBĚ

Vzor pro samostatný katalog operací

Osobní údaj	Popis operace	Dokumentovaný postup	Odpovědnost

3. Další možnosti členění

Jak již bylo uvedeno výše, je možné strukturu členění od samotného počátku či následně postavit dle jiných kritérii. Jednou z možností je členění dle kategorií osobních údajů, dalším pak členění dle právního titulu apod. Výhodou tohoto členění může být kumulace některých povinností, které pro tyto atributy ze strany správce vyplývají a tím je zajištěna i větší transparentnost i podklad pro analýzu souladu.

Pro potřeby tohoto dalšího členění je možné přiměřeně použít i přiloženou tabulku s tím, že datový zdroj je nahrazen vždy názvem.

V případě databázového zpracování je bezesporu možné níže uvedené členění zajistit formou PC sestav či datových dávek.

Další možností je členění na katalog osobních údajů a katalog operací.

Příklady dalšího členění:

3.1. Členění dle kategorie osobních údajů

a) standardní osobní údaje

Jedná se o osobní údaje zaměstnanců, dodavatelů správce osobních údajů a dále údaje vznikající při provozu správce. Zde je nutné zajistit standardní ochranu

- osobní údaje zaměstnanců,
- osobní údaje jiných osob - v tomto případě se jedná o osobní údaje osob blízkých, dodavatelů apod.
- provozní údaje - jedná se o údaje vedené na prezenčních listinách, zápisech či záznamech z jednání, tabulkách kontaktních osob, údaje smluvních partnerů apod.

b) zvláštní kategorie osobních údajů

Jedná se o citlivé osobní údaje pacientů a zaměstnanců, event. dalších osob. Mimo jiné se jedná i o údaje o zdravotním stavu či o politické příslušnosti nebo členství v odborové organizaci.

- citlivé osobní údaje pacientů – zejména zdravotnická dokumentace,
- citlivé osobní údaje zaměstnanců – jedná se o údaje o zdravotním stavu zaměstnanců, o jejich účasti v odborech apod.

3.2. Členění dle právního titulu

a) osobní údaje zpracovávané pro plnění právní povinnosti

Jedná se o osobní údaje, kdy je správci uložena povinnost právním předpisem, ať již zákonem či jiným právním předpisem.

b) osobní údaje zpracovávané na základě souhlasu subjektu údajů
c) osobní údaje zpracovávané pro ochranu životně důležitých zájmů subjektu údajů
d) osobní údaje zpracovávané pro plnění smlouvy

e) osobní údaje zpracovávané ve veřejném zájmu či k výkonu pravomoci
f) osobní údaje zpracovávané pro oprávněné zájmy správce

3.3. Členění osobních údajů dle toho, od koho byly získány

a) osobní údaje získané od subjektu údajů
b) osobní údaje získané nikoliv od subjektu údajů - jedná se o všechny osobní údaje, které byly získány jinak než od subjektu údajů, např. laboratorní výsledky, výsledky extramurální péče, získané na základě smlouvy apod.

4. Závěr

Zpracování katalogu osobních údajů je zcela jednoznačně nezbytností a prvním krokem v implementaci GDPR. Jedná se o inventarizaci všech osobních údajů zpracovávaných správcem osobních údajů. Porovnáním s právním titulem či účelem zpracování povede evidentně k tomu, že správce či zpracovatel zjistí ucelený okruh vedených osobních údajů a povede to k redukci některých údajů či vyjasnění právních titulů jejich vedení či spíše omezení rozsahu zpracovávaných osobních údajů, což vše je nezbytným předpokladem pro analýzu souladu zpracování osobních údajů s GDPR.

Příloha č. 3

Prokázání souladu s GDPR

Prokázání souladu

(metodický návod)

s

NAŘÍZENÍM

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 (obecné nařízení o ochraně osobních údajů)

Obsah

1. Úvod

Jedním ze dvou základních principů, na kterých je založeno GDPR je princip odpovědnosti správce. Správce musí dodržet zásady obsažené v čl. 5 odst. 1 GDPR a zároveň musí být schopen tento soulad doložit.

K prokázání, resp. doložení souladu mohou sloužit kodexy chování, získání osvědčení či certifikace, případně záznamy o činnostech zpracování.

V následujícím textu jsou uvedena některá metodická východiska pro zpracování prokázání souladu s GDPR formou záznamů o činnostech zpracování.

2. Rozsah záznamů o činnostech zpracování

Článek 30 GDPR stanoví rozsah záznamů o činnostech zpracování, které jsou členěny na záznamy, které vede správce osobních údajů a dále zpracovatel osobních údajů.

2.1. Záznamy o činnostech vedené správcem

Dle čl. 30 odst. 1 GDPR vede správce záznamy o činnostech zpracování, jejichž výčet je taxativní:

a) jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;
b) účely zpracování;
c) popis kategorií subjektů údajů a kategorií osobních údajů;
d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
e) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a tehdy, pokud tento převod není opakovaný, týká se pouze omezeného počtu subjektů údajů, je nezbytný pro účely závažných oprávněných zájmů správce, které nejsou převáženy zájmy nebo právy a svobodami subjektu údajů, a pokud správce posoudil všechny okolnosti daného předání údajů a na základě tohoto posouzení poskytl vhodné záruky pro ochranu osobních údajů doložení vhodných záruk;
f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;
g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených tj.:
   - pseudonymizace a šifrování osobních údajů;
   - schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
   - schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
   - procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Následující odstavce obsahují metodický návod k jednotlivým částem záznamů o činnostech zpracování:

2.1.1. Kontaktní údaje správce a pověřence pro ochranu osobních údajů

Kontaktní údaje správce jsou standardními. Pro pověřence doporučujeme zřízené samostatného kontaktu, resp. samostatné telefonní linky a emailové adresy.

2.1.2. Účely zpracování

Zde by mělo být definováno, jaký je účel zpracování a z jakého právního titulu vychází.

2.1.3. Popis kategorií subjektů údajů a kategorií osobních údajů

Pro popis kategorií subjektů či kategorií osobních údajů je možné využít jednak již zpracovaný katalog osobních údajů a dále i právní rozbor v případě zpracování osobních údajů na základě plnění právní povinnosti.

2.1.4. Kategorie příjemců

Vhodným prostředkem se jeví zpracování rozčlenění podle právního titulu, resp. opět je možné využít i zpracovaný právní rozbor.

2.1.5. Předání do zahraničí a mezinárodním organizacím

Nezapomenout na přeshraniční spolupráci a dále zpracovat rozčlenění zahraničí na jednotlivé kategorie států (EU a třetí země) a v případě třetích států na kategorie, kdy předání osobních údajů do třetích zemí nebo mezinárodním organizacím může být:

1) založeno na rozhodnutí Komise o odpovídající ochraně nebo
2) založeno na vhodných zárukách, kdy neexistuje rozhodnutí Komise o odpovídající ochraně.

2.1.6. Lhůty pro výmaz

Opět možné použít právní rozbor zahrnující přísl. právní předpisy:

např.

- zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů – explicitně pro rezort zdravotnictví, zejména ustanovení týkající se zdravotnické dokumentace či NZIS,
- zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů,

plus prováděcí předpisy.

2.1.7. Technická a organizační bezpečnostní opatření

Je možné využít dokumentaci dle norem ISO.

Záznamy o činnostech zpracování jsou dále doplněny všemi vnitřními normativními akty, které upravují ochranu osobních údajů, resp. bezpečnost informací.

2.2. Záznamy o činnostech vedené zpracovatelem

Dle čl. 30 odst. 2 vede zpracovatel záznamy o činnostech zpracování, jejichž výčet je taxativní:

a) jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná, a případného zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů;
b) kategorie zpracování prováděného pro každého ze správců;

c) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a tehdy, pokud tento převod není opakovaný, týká se pouze omezeného počtu subjektů údajů, je nezbytný pro účely závažných oprávněných zájmů správce, které nejsou převáženy zájmy nebo právy a svobodami subjektu údajů, a pokud správce posoudil všechny okolnosti daného předání údajů a na základě tohoto posouzení poskytl vhodné záruky pro ochranu osobních údajů doložení vhodných záruk;

d) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření, tj.:
   - pseudonymizace a šifrování osobních údajů;
   - schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
   - schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
   - procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Následující odstavce obsahují metodický návod k jednotlivým částem záznamů o činnostech zpracování (platí všechny paramenty výše uvedené u záznamů o činnostech zpracování, které jsou platné pro správce a níže pouze rozdílové požadavky, resp. metodická doporučení):

2.2.1. Kontaktní údaje zpracovatele, správce a pověřence pro ochranu osobních údajů

Nezapomenout na specifikaci každého správce, pro kterého je zpracování prováděno.

2.2.2. Informace o každém zpracování pro každého správce

Zde je nutné specifikovat všechny zpracování pro každého správce ve struktuře uvedené výše pro správce (myšleno kategorie subjektu údajů, kategorie osobních údajů, kategorie příjemců apod.).

2.2.3. Předání do zahraničí a mezinárodním organizacím

Viz výše u kapitoly pro správce.

2.2.4. Technická a organizační bezpečnostní opatření

Viz výše u kapitoly pro správce.

Záznamy o činnostech zpracování jsou dále doplněny všemi vnitřními normativními akty, které upravují ochranu osobních údajů, resp. bezpečnost informací.

3. Závěr

Proces analýzy souladu, jehož výsledkem je doložení souladu, by měl být popsán ve vnitřních směrnicích správce a zpracovatele, který napomáhá implementaci úspěšného systému řízení ochrany osobních údajů, resp. ochrany práv a svobod subjektů osobních údajů.

Pravidelné vyhodnocování, resp. testování, je zásadní pro trvalou důvěru klientů a pro plnění povinností při ochraně osobních a jinak citlivých informací před příliš častými hrozbami a současně je základní dokumentací pro předložení dozorovému úřadu.

Příloha č. 4

Analýza rizik na ochranu osobních údajů

Analýza a hodnocení rizik

pro práva a svobody subjektů údajů

dle

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 (obecné nařízení o ochraně osobních údajů)

(STRUKTUROVANÉ BODY)

Obsah

Použité zkratky:

Pro účely tohoto materiálu je dále používáno již obecně zažité označení Obecného nařízení pro ochranu osobních údajů – GDPR (General Data Protection Regulation).

1. Úvod

1.1. Základní definice

Hlavním principem implementace GDPR je *přístup založený na riziku (jak z pohledu subjektu údajů, tak z pohledu správce/event. zpracovatele údajů).* Znamená to, že v prvé řadě je nezbytností vyhodnotit rizika, následně pak rizika posoudit a rozhodnout o přijetí opatření ke snížení a eliminaci rizika nebo riziko přijmout.

Pro riziko existuje celá řada definic. Riziko je nejčastěji definováno jako součin velikosti následků nežádoucí události a pravděpodobnosti, že k uvedené nežádoucí události dojde.

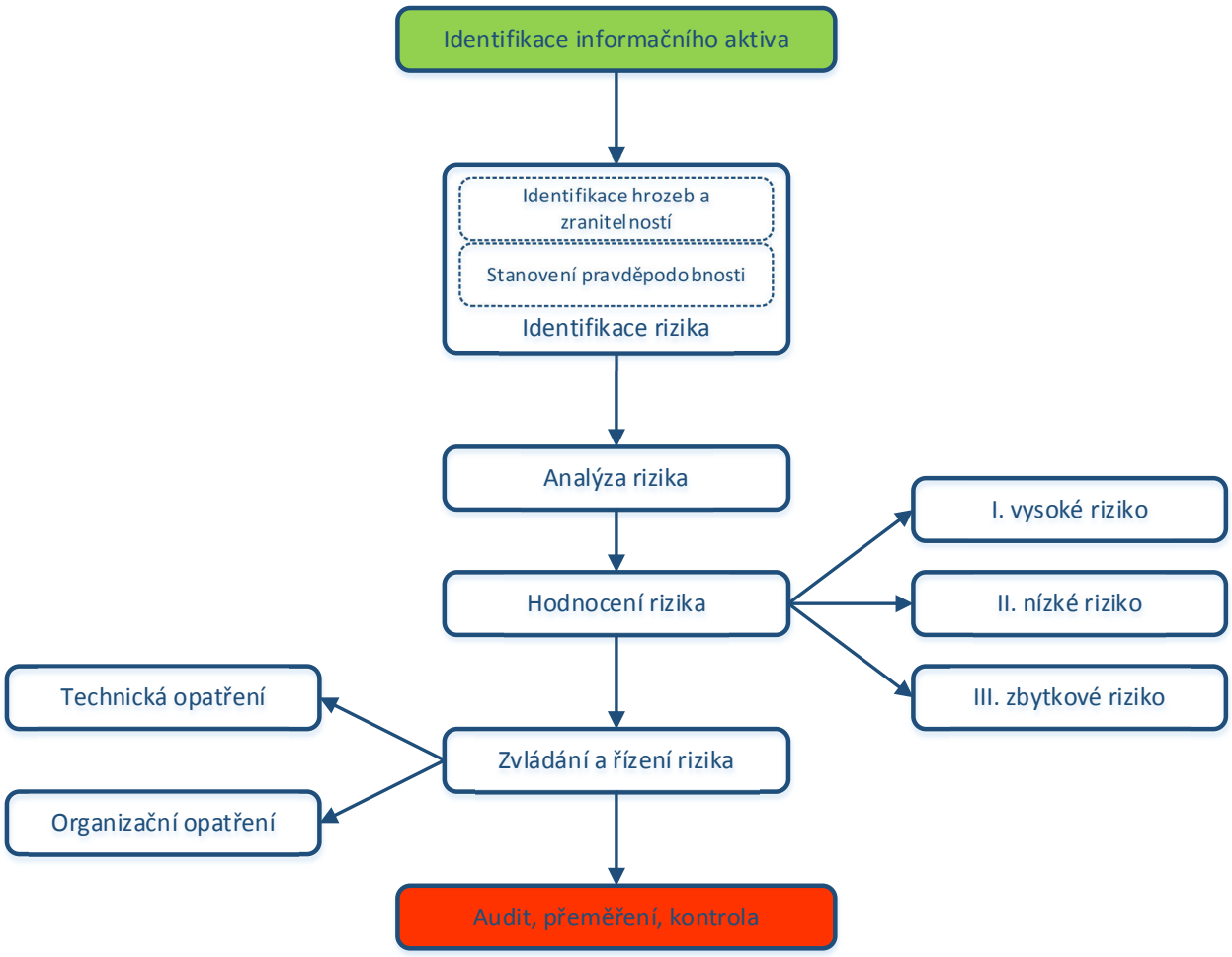
Analýzu rizik je možné zpracovat ve vztahu k základním právům a svobodám subjektu údajů, kterými jsou např.:

- ochrana identity,
- právo na informace,
- právo na ochranu osobních údajů,
- právo na duševní a tělesnou integritu,
- právo na soukromí,
- atd.

Jedná-li se o zpracování na základě právního předpisu, což bezesporu v případě poskytovatele zdravotních služeb je zákon o zdravotních službách a jeho prováděcí předpisy v případě zdravotnické dokumentace, není nutné analýzu rizik zpracovat – doplněno na základě konzultace s MV ČR dne 10. ledna 2018.

2. Obecný proces hodnocení a řízení rizika

2.1. Schéma procesu



2.2. Identifikace informačního aktiva

Rizika jsou vždy vztažena ke konkrétním aktivům – v případě procesu řízení rizik GDPR tedy osobním údajům, respektive konkrétním datasetům, jejichž subjekty mohou být v rámci případné aktivace rizika poškozeny.

Prvním krokem procesu hodnocení a řízení rizika je tak vždy identifikace informačních aktiv, pro která budou následně rizika identifikována a řízena.

2.3. Identifikace rizika

Riziko má dvě základní komponenty – zranitelnost a hrozbu. V případě zpracování osobních údajů se jedná konkrétně o náhodné zničení, ztrátu, pozměňování, neoprávněné zpřístupnění atd.

2.3.1. Zranitelnost

Zranitelnost je pojem používaný pro označení slabiny či nedostatku aktiva. Zranitelnost umožňuje uplatnění hrozby. Při analýze rizik je zranitelnost vlastností aktiva. Mezi hlavní zranitelnosti v případě osobních údajů patří:

- náhodné zničení,
- ztráta,
- pozměnění,
- neoprávněné zpřístupnění.

2.3.2. Hrozba

Hrozba je pojem používaný pro označení zdroje nějaké negativní události, síly, osoby či aktivity, která chce nebo může poškodit aktivum. Hrozba má nežádoucí vliv na bezpečnost nebo může způsobit škodu, ztrátu, nežádoucí změnu, či jiný nežádoucí jev.

Hrozby lze členit podle různých způsobů. Pro účely tohoto metodického návodu je uvedeno následující členění:

2.3.2.1. Lidský faktor

Je nezbytné dbát pravidla přiměřenosti přístupů zaměstnanců dané organizace ke spravovaným osobním údajům a snažit se omezit nutnost těchto přístupů na minimum. Rovněž je nezbytné pečlivě zvážit rozdělení rolí mezi zaměstnance a dbát na jejich striktní odebírání v případě oprávnění danou roli vykonávat.

2.3.2.2. Pracovní prostředí

Nedostatečně zabezpečené pracovní prostředí (nízká fyzická bezpečnost pracoviště) zvyšuje riziko kompromitace osobních údajů tam, kde se s nimi nakládá. Může jít o nezabezpečené prostory, kde je nakládáno s papírovými dokumenty či kde jsou ukládány, stejně jako o nízkou úroveň zabezpečení elektronických nosičů.

2.3.2.3. Finanční prostředky

Nedostatek finančních prostředků může vést k nedostatečnému technickému zabezpečení osobních údajů, případně může mít i negativní vliv na kvalifikaci a možnosti proškolení zaměstnanců.

2.3.2.4. Technické prostředky

Technické prostředky pro zabezpečení osobních údajů jsou základním opatřením jejich ochrany. Mimo fyzického zabezpečení papírových dokumentů se jedná zejména o IT infrastrukturu pro ukládání elektronických dat, ve kterých se nacházejí osobní údaje.

2.3.2.5. Externí dodavatelé

Využívání externích dodavatelů je jedním ze zásadních zdrojů možných porušení pravidel bezpečnosti nakládání s osobními údaji a jako takové musí být podrobeno dostatečné formalizaci a kontrole. Existenci smluv, které v písemné podobě detailně specifikují roli, úkoly, kompetence a odpovědnosti externího dodavatele zapojeného do správy a zpracování osobních údajů ve většině případů přímo vyžaduje i obecné nařízení o ochraně osobních údajů.

2.4. Analýza rizik

V rámci procesu analýzy rizik se stanoví číselné hodnoty pravděpodobnosti a dopadu rizika. Tyto hodnoty se pak násobí, aby se dosáhlo hodnoty vysokého rizika, nízké úrovně nebo zbytkové klasifikace rizika.

2.4.1. Posouzení pravděpodobnosti

Pravděpodobnost každého rizika je rozdělena na číselné stupnici od 1 (nízké) do 5 (vysoké). Obecné pokyny pro význam každého stupně jsou uvedeny v tabulce níže. Při posuzování pravděpodobnosti rizika jsou zohledněny stávající kontroly, což může vyžadovat posouzení efektivity stávajících kontrol.

Podrobné pokyny mohou být určeny pro každou pravděpodobnost stupně v závislosti na předmětu posuzování rizik.

Úroveň		Popis
1	Vyloučené	Nikdy se to nestalo a není důvod si myslet, že se někdy stane.
2	Nepravděpodobné	Je možné, že by se to mohlo stát, ale pravděpodobně se to nestane.
3	Pravděpodobné	Je pravděpodobné, že se riziko stane.
4	Téměř jisté	Je vysoce pravděpodobné, že za současných okolností k riziku dojde.
5	Jisté	Stává se pravidelně nebo existuje důvod domnívat se, že je prakticky bezprostřední.

Tabulka 1: Pravděpodobnost výskytu rizika

Důvod pro přidělení daného stupně by měl být zaznamenán, aby pomohl pochopení a umožnil opakovatelnost v budoucích hodnoceních

2.4.2. Hodnocení dopadu

Ovlivnění dostupnosti, důvěrnosti či integrity aktiva bude hodnoceno v souladu s postupem pro hodnocení dopadů, pro každý výskyt spojení **aktivum + hrozba + zranitelnost** samostatně. Jako velmi obecné vodítko pro určení úrovně dopadu lze využít tabulku vycházející z vyhlášky o kybernetické bezpečnosti.

Úroveň		Popis dopadu
1	Nízký	Dopad je v omezeném časovém období a malého rozsahu a nesmí být katastrofický. Představuje dopad na subjekty údajů se závažným zásahem do jejich práv a svobod postihujícího nejvýše …… osob.
2	Střední	Dopad je omezeného rozsahu a v omezeném časovém období. Představuje dopad na subjekty údajů se závažným zásahem do jejich práv a svobod postihujícího od …… osob do …… osob.
3	Vysoký	Dopad je omezeného rozsahu, ale trvalý. Představuje dopad na subjekty údajů se závažným zásahem do jejich práv a svobod postihujícího od …… osob do …… osob.
4	Kritický	Dopad je plošný rozsahem, trvalý. Představuje dopad na subjekty údajů se závažným zásahem do jejich práv a svobod postihujícího od …… osob do …… osob.

Tabulka 2: Hodnocení dopadu

Je možné, resp. vhodné také hodnotit jiné subjektivní dopady, které se těžko vyčíslují (ztráta dobrého jména apod.).

Úroveň	Popis	Dopad na klienty	Finanční dopad	Zdraví a bezpečnost	Dopad na reputaci	Právní dopad
1	Zanedba-telný	Bez dopadu	Velmi malý nebo žádný	Velmi malý	Zanedbatelný	Žádné důsledky
2	Mírný	Místní omezení	Malý	V přijatelných mezích	Mírný	Malé riziko porušení povinností dle GDPR
3	Střední	Stále lze poskytovat služby s určitými obtížemi	Nežádoucí	Zvýšené riziko vyžadující okamžitou pozornost	Střední	Nebezpečí porušení povinností dle GDPR
4	Vysoký	Nelze poskytovat služby v klíčových oblastech	Silný vliv na příjem nebo zisk	Významné nebezpečí pro život	Vysoký	Porušení povinností dle GDPR
5	Kritický	Nelze poskytovat žádné služby	Likvidace	Skutečné nebo silné potenciální ztráty na životě	Kritický	Velké sankce

Tabulka 3: Hodnocení dopadu subjektivní

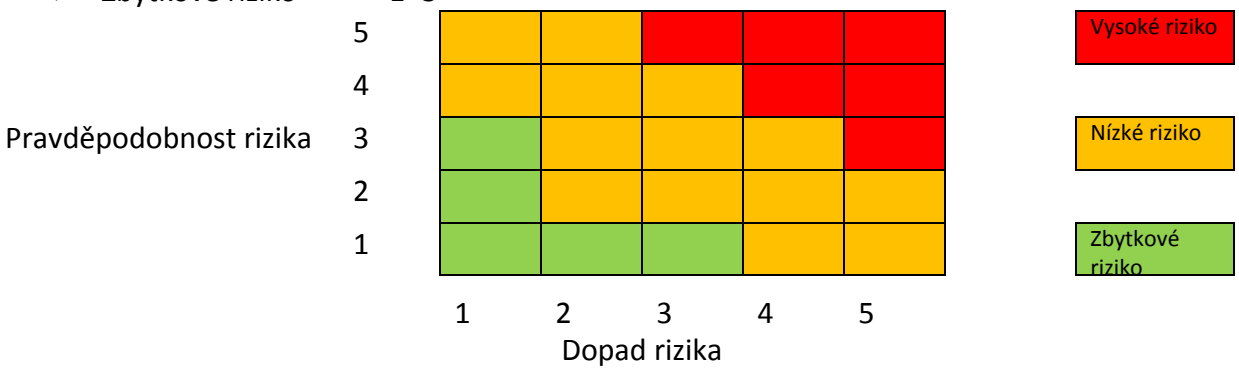
2.5. Hodnocení rizik

2.5.1. Klasifikace rizik

Na základě posouzení stupně pravděpodobnosti a dopadu se pro každé riziko vypočítá skóre vynásobením hodnoty pravděpodobnosti a dopadu. Toto výsledné skóre se pak použije při rozhodování o klasifikaci rizika na základě matice znázorněné na obrázku níže.

Každému riziku bude přidělena klasifikace na základě jeho skóre takto:

- Vysoké riziko 12–25
- Nízké riziko 4–12
- Zbytkové riziko 1–3



Obrázek 1: Klasifikace rizik

Klasifikace každého rizika bude zaznamenána jako vstup do fáze hodnocení rizika.

2.5.2. Organizace hodnocení rizik

Hodnocení rizik probíhá v rámci úvodní analýzy informačních aktiv, zpravidla jako součást úvodní analýzy připravenosti na implementaci GDPR.

2.5.3. Odpovědné osoby za hodnocení rizik

Osobou odpovědnou za hodnocení rizik jsou garanti jednotlivých aktiv, a to zejména s ohledem na skutečnost, že jsou s aktivem nejlépe obeznámeni a mohou tak nejpřesněji stanovit jednotlivé atributy a provést objektivní hodnocení rizik.

V případě, kdy není garant aktiva stanoven nebo není z objektivních příčin schopen provést hodnocení rizik samostatně, je možné realizovat průzkum se zapojením uživatelů aktiva, a to formou řízeného pohovoru, případně dotazníkového šetření.

2.6. Prostředky pro hodnocení rizika

2.6.1. Seznamy zdrojů rizik

V rámci provádění analýzy rizik je možné se v určitých oborech opřít o existující seznamy zdrojů rizik, které vycházejí ze statistických šetření, odborných znalostních bází a dalších zdrojů. Seznamy zdrojů rizik mohou být neocenitelným zdrojem zejména při sestavení úvodní analýzy rizik.

2.6.2. Checklisty – kontrolní seznamy

Check-listy, nebo-li kontrolní seznamy, jsou dobrou metodickou pomůckou při provádění hodnocení rizika, zejména pokud je prováděno nezávisle na sobě větší skupinou respondentů, nebo je realizováno s větším časovým odstupem (např. v rámci jednotlivých revizí systému řízení rizik). Využití kontrolního seznamu především přispívá k porovnatelnosti výsledků jednotlivých hodnocení.

2.7. Zvládání a řízení rizika

Zvládání a řízení identifikovaných rizik souvisí s přijímáním opatření, která mají za úkol snížit buď pravděpodobnost aktivace rizika, anebo snížit negativní dopady související s aktivací rizika. V obou případech se jedná o opatření, směřující k převedení rizika ze zóny vysokého rizika do zóny nízkého nebo zbytkového rizika, případně převedení nízkého rizika na riziko zbytkové.

V rámci volby opatření a cílové úrovně rizika po jeho aplikaci je vždy nutné poměřovat náklady na opatření a případné náklady na sanaci škod souvisejících s případnou aktivací rizika.

2.7.1. Technická opatření

Jednou z dvou hlavních skupin opatření, která je možné přijmout při snižování rizika v oblasti ochrany osobních údajů, jsou opatření technická. Tento typ opatření představuje především zavádění takových technologií, které budou garantovat vyšší míru fyzické bezpečnosti osobních údajů, vyšší míru zabezpečení ICT systémů proti neoprávněnému přístupu, poškození či ztrátě údajů, apod.

2.7.2. Organizační opatření

Druhou významnou skupinou opatření jsou opatření organizační. Tato skupina opatření se věnuje především vytváření takových procesů a nastavení kompetencí a odpovědností, které vedou k minimalizaci spravovaných údajů, minimalizaci oprávnění konkrétních osob pro nakládání s údaji, nastavení maximální auditovatelnosti všech operací a přístupů, atd.

2.8. Kontrola, přeměření a audit

Každý proces, který je v organizaci vykonáván dlouhodobě a měl by být rutinní součástí jejího fungování, musí být zahrnut do systému kontroly a auditu, a to jednak proto, aby byl zajištěn jeho správný výkon, a pak také aby bylo možné jej podrobit kontinuálnímu zlepšování na základě analýzy jeho průběhu a změn v čase.

Organizace by měla pro jednotlivé procesy stanovit klíčové výkonností ukazatele (KPI), které budou zaměřeny na podstatné atributy procesu – v případě osobních údajů např. jako klíčová metrika může sloužit množství incidentů, celkový objem zpracovávaných údajů, četnost provádění konkrétních operací, atp. Jejich pravidelné vyhodnocování pak může sloužit jednak jako základní kontrolní mechanismus, ale díky sledování trendů a odchylek také jako podklad pro kontinuální zlepšování.

3. Závěr

Proces analýzy, hodnocení a řízení rizik je základem implementace úspěšného systému řízení ochrany osobních údajů, resp. ochrany práv a svobod subjektů osobních údajů, jejichž je daná instituce správcem, event. zpracovatelem. Souvisí s bezpečností informací (ISMS) a tvoří významnou součást standardu ISO/IEC 27001. Pouze tím, že se plně porozumí rizikům, se zajistí, že zavedené kontroly jsou dostatečné k tomu, aby poskytly odpovídající úroveň ochrany před ohrožením práv a svobod subjektů osobních údajů.

Pravidelné vyhodnocování rizik a uplatňování komplexních kontrol je zásadní pro trvalou důvěru klientů a pro plnění povinností při ochraně osobních a jinak citlivých informací před příliš častými hrozbami.

Tímto postupem je zajištěno, že rizika jsou účinně řízena a kontrolována.

Příloha č. 5

Parametry smlouvy o zpracování osobních údajů

PARAMETRY SMLOUVY O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

dle čl. 28

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 (obecné nařízení o ochraně osobních údajů)

V následující tabulce je ke každé povinnosti stanovené GDPR uveden metodický návod, resp. dopad pro správce osobních údajů, které je nutné promítnout do smlouvy o zpracování osobních údajů.

Článek GDPR	Povinnost správce/zpracovatele	Dopad do smlouvy
čl. 28 odst. 9	Požadavek na písemnou formu, vč. elektronické formy.	Smlouva musí mít písemnou formu. Zásadně a bezvýjimečně.
čl. 28 odst. 1	Správce může jako zpracovatele zapojit pouze takového zpracovatele, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů.	Je nutné explicitní prohlášení zpracovatele, že zaručí zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů.
čl. 28 odst. 2, věta první	Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce.	V případě, že je předpoklad „řetězení zpracovatelů“, je nutné explicitně uvést do ustanovení smlouvy ve variantě konkrétního nebo obecného písemného povolení ze strany správce.
čl. 28 odst. 2, věta druhá	V případě obecného písemného povolení zpracovatel správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak správci příležitost vyslovit vůči těmto změnám námitky.	Je-li ve smlouvě uvedeno obecné povolení ze strany správce, že je umožněno „řetězení zpracovatelů“ je nutné zakotvit ve smlouvě proceduru pro přijetí nových zpracovatelů nebo jejich nahrazení a pro reakci správce.
čl. 28 odst. 3, věta první	Zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce.	V současnosti dle § 6 ZOOÚ. Smlouva musí obsahovat taxativně uvedené náležitosti: ➢ závazky zpracovatele vůči správci, ➢ předmět a doba trvání zpracování, ➢ povaha a účel zpracování, ➢ typ osobních údajů, ➢ kategorie subjektu údajů, ➢ povinnosti a práva správce.

Článek GDPR	Povinnost správce/zpracovatele	Dopad do smlouvy
čl. 28 odst. 3, věta druhá	povinnosti zpracovatele	Je nutné ve smlouvě uvést všechny dále uvedené povinnosti zpracovatele.
čl. 28 odst. 3, písm. a)	zpracovatel je oprávněn zpracovávat osobní údaje na základě doložených pokynů správce, vč. předání do třetích zemí a mezinárodním organizacím	Všechny pokyny musí být výslovně uvedeny ve smlouvě s výjimkou případů, kdy je mi to uloženo právem EU nebo členského státu, které se na správce vztahuje. V tomto případě jde pouze o informování správce ze strany zpracovatele (pokud to není zakázáno v důležitém veřejném zájmu).
čl. 28 odst. 3, písm. b)	osoby oprávněné zpracovávat musí být zavázány k mlčenlivosti nebo musí být zavázány k mlčenlivosti zákonnou povinností	Ve smlouvě specifikovat jednu z možností, tedy buď, že se zpracovatel zavazuje zajistit, aby všechny osoby, které zpracovávají osobní údaje, byly vázány mlčenlivostí nebo uvést konkrétně právní předpis, na základě kterého už tyto osoby vázány k mlčenlivosti jsou.
čl. 28 odst. 3, písm. c)	zpracovatel se zaváže, že přijme všechna opatření k zabezpečení zpracování	Ve smlouvě musí být specifikován závazek zpracovatele přijmout všechna opatření dle GDPR (čl. 32) a dále uvedena ona opatření.
čl. 32		S přihlédnutím k ➢ stavu techniky, ➢ nákladům na provedení, ➢ povaze zpracování, ➢ rozsahu zpracování, ➢ kontextu zpracování a ➢ účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, tj. tato opatření musí kopírovat analýzu rizik v případě uzavíraných smluvních vztahů.

Článek GDPR	Povinnost správce/zpracovatele	Dopad do smlouvy
		Konkrétně – GDPR zná DEMONSTRATIVNÍ VÝČET, což znamená, že se jedná pouze o příklady, opatření mohou být i jiná, ALE správce/zpracovatel musí prokazovat, proč použil zrovna tato opatření. a) pseudonymizace a šifrování osobních údajů; b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování; c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů; d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.
čl. 28 odst., 3 písm. d) čl. 28 odst. 4 čl. 28 odst. 2	zpracovatel dodržuje pravidla „řetězení“ zpracovatelů	Ve smlouvě je uveden závazek zpracovatele, že v případě, že zapojí do zpracování dalšího zpracovatele, zaváže ho smlouvou ke stejným povinnostem, které má ve vztahu ke správci, zejména k poskytnutí dostatečných záruk k zavedení vhodných technických a organizačních opatření k zajištění souladu podmínek zpracování osobních údajů s GDPR. Zároveň by měla ve smlouvě být uvedena ta skutečnost (s odkazem na čl. 28 odst. 4), že v případě, pokud tuto povinnost dále zapojený zpracovatel nesplní – odpovídá pak za všechny povinnosti ve vztahu ke správci on.
čl. 28 odst. 3, písm. e)	zpracovatel zohledňuje povahu zpracování a je nápomocen správci i při vyřizování žádostí subjektu údajů	Ve smlouvě stanoven závazek zpracovatele být nápomocen zejména tím, že přijme vhodná technická a organizační opatření

Článek GDPR	Povinnost správce/zpracovatele	Dopad do smlouvy
čl. 28 odst. 3, písm. f) čl. 32 až 36	zpracovatel je nápomocen správci v plnění povinností dle čl. 32 až 36	Ve smlouvě jsou konkrétně vyjmenované povinnosti správce, při kterých je zpracovatel nápomocen: ➢ zabezpečení zpracování (čl. 32), ➢ ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu (čl. 33), ➢ oznamování případů porušení zabezpečení osobních údajů subjektu údajů (čl. 34), ➢ posouzení vlivu na ochranu osobních údajů (čl. 35), ➢ předchozí konzultace (čl. 36).
čl. 28 odst. 3, písm. g)	Na pokyn správce zpracovatel osobní údaje vymaže nebo po ukončení zpracování vrátí správci a všechny osobní údaje vymaže (s výjimkou případů, kdy je stanoveno právem EU nebo členského státu)	Ve smlouvě musí být upraven celý životní cyklus osobních údajů.
čl. 28 odst. 3 písm. h)	Povinnost zpracovatele doložit správci to, že jsou splněny všechny povinnosti dle čl. 28 a umožnit audity, vč. inspekcí prováděných správcem či jím pověřenou osobou a poskytne součinnost u těchto auditů.	Explicitně tuto novou povinnost uvést ve smlouvě. Zároveň s povinností zpracovatele informovat neprodleně správce v případě, že jeho pokyn porušuje GDPR nebo jiný právní předpis.
čl. 26	Povinnosti společných správců	V případě společných správců mezi sebou transparentním ujednáním tito vymezí: ➢ své podíly na odpovědnosti za plnění povinností podle GDPR, zejména pokud jde o výkon práv subjektu údajů, ➢ své povinnosti poskytovat informace uvedené v článcích 13 a 14, pokud tuto odpovědnost správců nestanoví právo Unie nebo členského státu, které se na správce vztahuje.

Článek GDPR	Povinnost správce/zpracovatele	Dopad do smlouvy
		V ujednání může být určeno kontaktní místo pro subjekty údajů. Dále ujednání zohlední úlohy společných správců a jejich vztahy vůči subjektům údajů. Subjekt údajů musí být o podstatných prvcích ujednání informován. POZOR: Bez ohledu na podmínky ujednání může subjekt údajů vykonávat svá práva podle tohoto nařízení u každého ze správců.

Poznámka: Pokud zpracovatel poruší GDPR tím, že stanoví účel a prostředky zpracování, považuje se ve vztahu k takovému zpracování za správce.

Příloha č. 6

Informace poskytované subjektu údajů o zpracování osobních údajů

Informace je možné připojit k obecným informacím pro pacienty, které jsou uvedeny na webových stránkách ordinace nebo na jiných obecných informačních materiálech určených pro pacienta ze strany lékaře (např. nástěnka v čekárně).

INFORMACE O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ
dle čl. 13
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 (obecné nařízení o ochraně osobních údajů)

Vaše osobní údaje jsou zpracovávány ve zdravotnické dokumentaci v plném souladu s platnými právními předpisy zejména v souladu se zákonem č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) a jeho prováděcími předpisy.
Jejich zabezpečení a ochrana je zajištěna v souladu s těmito předpisy i v souladu s Obecným nařízením pro ochranu osobních údajů 2016/679.

Kromě možnosti přístupu k Vašim osobním údajům námi vedených, máte právo požadovat jejich opravu či omezení zpracovánípokud zjistíte, že jsou tyto údaje nesprávné. ……..*možno doplnit dle specifických situací např. při pořizování kamerového záznamu.*

V případě, když se domníváte, že zpracováním osobních údajů dochází k porušení Obecného nařízení na ochranu osobních údajů Vašich práv, máte právo podat stížnost u Úřadu pro ochranu osobních údajů, v místě svého obvyklého bydliště, v místě výkonu zaměstnání nebo místě, kde došlo k údajnému porušení.

Poskytování Vašich osobních údajů je zákonným požadavkem a máte jako pacient povinnost je poskytnout, stejně jako zdravotnický pracovník má právo jej po Vás požadovat. Neposkytnutí Vašich osobních údajů bude znamenat, že správce Vám nebude moci poskytnout zdravotní služby, a tím může dojít k poškození Vašeho zdraví či přímému ohrožení života.

Možno doplnit právním rozkladem jednotlivých práv a povinností dle GDPR a platné zdravotnické legislativy.

Příloha č. 7: Vazba práv subjektu údajů na právní titul jejich zpracování

Právní důvod	Informování, jsou-li údaje získány od subjektu údajů	Informování, jsou-li údaje získány z jiného zdroje	Právo na přístup	Právo na opravu (řetězení)	Právo na výmaz (řetězení)	Právo na omezení zpracování (řetězení)	Právo na přenositelnost (smlouva, souhlas a automatizované zpracování)	Právo vznést námitku	Právo nebýt podroben automatizovanému rozhodování
článek GDPR	13	14	15	16	17	18	20	21	22
Právní povinnost uložená správci vedení zdr. dokumentace	Ano	Ne, je-li výslovně stanoveno předpisem spolu se zárukami	Ano	Ano	Ne (do skartační lhůty)	Ano	Ne	Ne	Ne, pokud není povoleno právním předpisem stanovícím záruky
Životně důležitý zájem subjektu údajů	Ne	Ne, je-li výslovně stanoveno předpisem spolu se zárukami	Ano	Ano	Ne (ne do skartační lhůty)	Ano	Ne	Ne	Ne, pokud není povoleno právním předpisem stanovícím záruky
Souhlas udělený subjektem údajů kl. studie	Ano, upozornit na možnost odvolání souhlasu	Ano	Ano	Ano	Ano	Ano	Ano	Ne (ale může odvolat souhlas)	Ne, pokud je souhlas výslovný
Plnění smlouvy, smluvní stranou je subjekt údajů zaměstnanec	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ne	Ano
Úkol ve veřejném zájmu nebo výkon pravomoci inf.choroby	Ano	Jako právní povinnost. Ne, pokud by popřelo smysl zpracování	Ano	Ano	Ne (do skartační lhůty, pokud je)	Ano	Ne	Ano	Ne, pokud není povoleno právním předpisem stanovícím záruky
Oprávněný zájem mimo oblast úkolů správce kamer. system	Ano	Ano. Ne, pokud by popřelo smysl zpracování	Ano	Ano	Ano. Ne, pokud jde o ochranu právních nároků	Ano	Ne	Ano	Ano

Příloha č. 8
Problematika GDPR z pohledu poskytovatelů ambulantních zdravotních služeb v otázkách a odpovědích

Otázka č. 1: Týká se vůbec GDPR primární a specializované ambulantní péče?

Odpověď:
Ano, týká, protože zpracovávají osobní údaje, včetně zvláštní kategorie osobních údajů podle platných právních předpisů resortu zdravotnictví.. Nicméně je třeba přistupovat k implementaci přiměřeně a zejména u malých ambulancí by implementace GDPR neměla znamenat významnou organizační či administrativní zátěž.

Otázka č. 2: Dokument popisující GDPR je tak rozsáhlý, že jej lékaři nemají prostor nastudovat. V mnoha ohledech je obecný a vyžaduje zpřesňující výklad. Kde lze takový souhrn získat?

Odpověď:
Závazný a zcela jednoznačný výklad, podpořený např. jasným prováděcím předpisem, v současné době bohužel neexistuje. Jediným závazným výkladem je rozhodovací praxe ve sporech. V současné době existují pouze doporučující stanoviska či metodiky, a to buď dozorových úřadů (v případě ČR jde o Úřad pro ochranu osobních údajů - ÚOOÚ), komerčních subjektů (advokátních či konzultačních kanceláří) nebo metodický materiál zpracovaný MZ ČR ve spolupráci s ÚZIS ČR, jehož je tento text přílohou.

Právní stanovisko:
Regulace je nastavena jednotlivými ustanoveními samotného GDPR v 99 článcích, které je nutno vykládat v souvislostech se 173 recitály. Vzhledem k neexistenci aplikační rozhodovací praxe závazný výklad dosud neexistuje. Odpovědnost za ochranu osobních údajů leží pouze a jedině na správci či zpracovateli osobních údajů.

Otázka č. 3: Mají praktičtí lékaři a ambulantní specialisté očekávat nějaké kontroly a audity ohledně GDPR? A kdo bude oprávněn je provádět a jak (budou např. předem ohlášeny)?

Odpověď:
Kontrolovat GDPR je oprávněn dozorový úřad, kterým je v případě ČR Úřad pro ochranu osobních údajů. Jeho kontroly budou prováděny podle stejné praxe jako doposud. Kontroly jsou vždy předem ohlášeny.

Právní stanovisko:
Kontroly budou prováděny příslušným dozorovým úřadem. Právní regulace je uvedena v kapitole VI. GDPR Nezávislé dozorové úřady v čl. 51 a násl. kontroly budou prováděny v souladu se zákonem č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů.

Kontroly budou prováděny jako:

- *kontroly na základě kontrolního plánu, který je vypracováván ve spolupráci s předsedou Úřadu a schvalován na každý rok,*
- *kontroly incidenční, které jsou prováděny na základě podnětů a stížností subjektů údajů nebo na základě jiných podnětů (předání od soudů, policie, upozornění ve sdělovacích prostředcích apod.),*
- *kontroly na základě podnětu předsedy Úřadu.*

Otázka č. 4: Co musí mít praktický lékař či ambulantní specialista připraveno, aby doložil, že je na GDPR připraven, resp. že normu implementoval a postupuje v souladu s ní? – myšleno jaké dokumenty mají být nachystány a jaká opatření doložena a jak?

Odpověď:
Poskytovatel ambulantních zdravotních služeb by měl mít zdokumentováno, jaké osobní údaje zpracovává, na základě čeho je zpracovává, kde je shromažďuje, kdo je oprávněn k nim a jakým způsobem přistupovat, jak je zajištěna jejich ochrana a jak je s nimi nakládáno a za jakým účelem a jak jsou případně likvidovány. Jde tedy o soubor dokumentů či jejich přehled s odkazem na platné právní předpisy v resortu zdravotnictví, které představují v podstatě inventarizaci práce s osobními údaji klientů, pacientů. V tomto smyslu nejde zásadně o nové povinnosti, obdobnou přípravu očekává od ambulantní sféry již stávající legislativa o ochraně osobních údajů. Hlavním momentem je doložit všechna bezpečnostní opatření, jak jsou osobní údaje zabezpečeny. Nezapomenout při tom na zcela jednoduchá bezpečnostní opatření (např. zámek na dveřích či logování přístupů)

Právní stanovisko:

Jedním ze dvou základních principů, na kterých je založeno GDPR je princip odpovědnosti správce. Správce musí dodržet zásady obsažené v čl. 5 odst. 1 GDPR a zároveň musí být schopen tento soulad doložit.

K prokázání, resp. doložení souladu mohou sloužit kodexy chování, získání osvědčení či certifikace, případně záznamy o činnostech zpracování.
Záznamy o činnostech vedené správcem. Dle čl. 33 odst. 1 vede správce záznamy o činnostech zpracování, jejichž výčet je taxativní:

a) jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;
b) účely zpracování;
c) popis kategorií subjektů údajů a kategorií osobních údajů;
d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
e) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a tehdy, pokud tento převod není opakovaný, týká se pouze omezeného počtu subjektů údajů, je nezbytný pro účely závažných oprávněných zájmů správce, které nejsou převáženy zájmy nebo právy a svobodami subjektu údajů, a pokud správce posoudil všechny okolnosti daného předání údajů a na základě tohoto posouzení poskytl vhodné záruky pro ochranu osobních údajů doložením vhodných záruk;
f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;
g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených tj.:
    - *pseudonymizace a šifrování osobních údajů;*

- *schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;*
- *schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;*
- *procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.*

Otázka č. 5: Jaké nejčastější chyby nebo jaká nejčastější rizika lze při práci s osobními údaji očekávat v ambulancích a v primární praxi? Je možné získat takový výčet hlavních rizikových oblastí, procesů, na které je třeba se primárně připravit?

Odpověď:
Na zajištění ochrany osobních údajů a jejich zpracování je nutné pohlížet optikou možnosti ohrožení práv a svobod subjektu údajů. Jinými slovy, smyslem inventarizace a následně přijatých opatření je zabránit rizikům, které ze zpracování osobních údajů mohou vyplynout. Je logické, že hlavní pozornost by měla být upřena na bezpečnost používaných IT systémů, zajištění kontroly nad přístupy k osobním datům pacientů a nad procesy, kterými jsou tyto údaje zpracovávány a případně předávány dalším subjektům. Tedy hlavní a nejzávažnější chyby zcela jistě zahrnují nekontrolovanou práci s dokumentací pacientů (nechráněné a nekontrolované přístupy), nezabezpečenou komunikaci obsahující osobní a citlivé údaje pacientů či rizika vyplývající z používaných IT systémů (nelegální software, chybějící elementární zabezpečení, apod.). Je třeba kontrolovat, zda-li jsou přijatá opatření dostatečná. Odborně řečeno je to analýza rizik – posouzení jaké jak velké je či není riziko pro pacienta při nakládání s jeho osobními údaji v ordinaci.

Právní stanovisko:

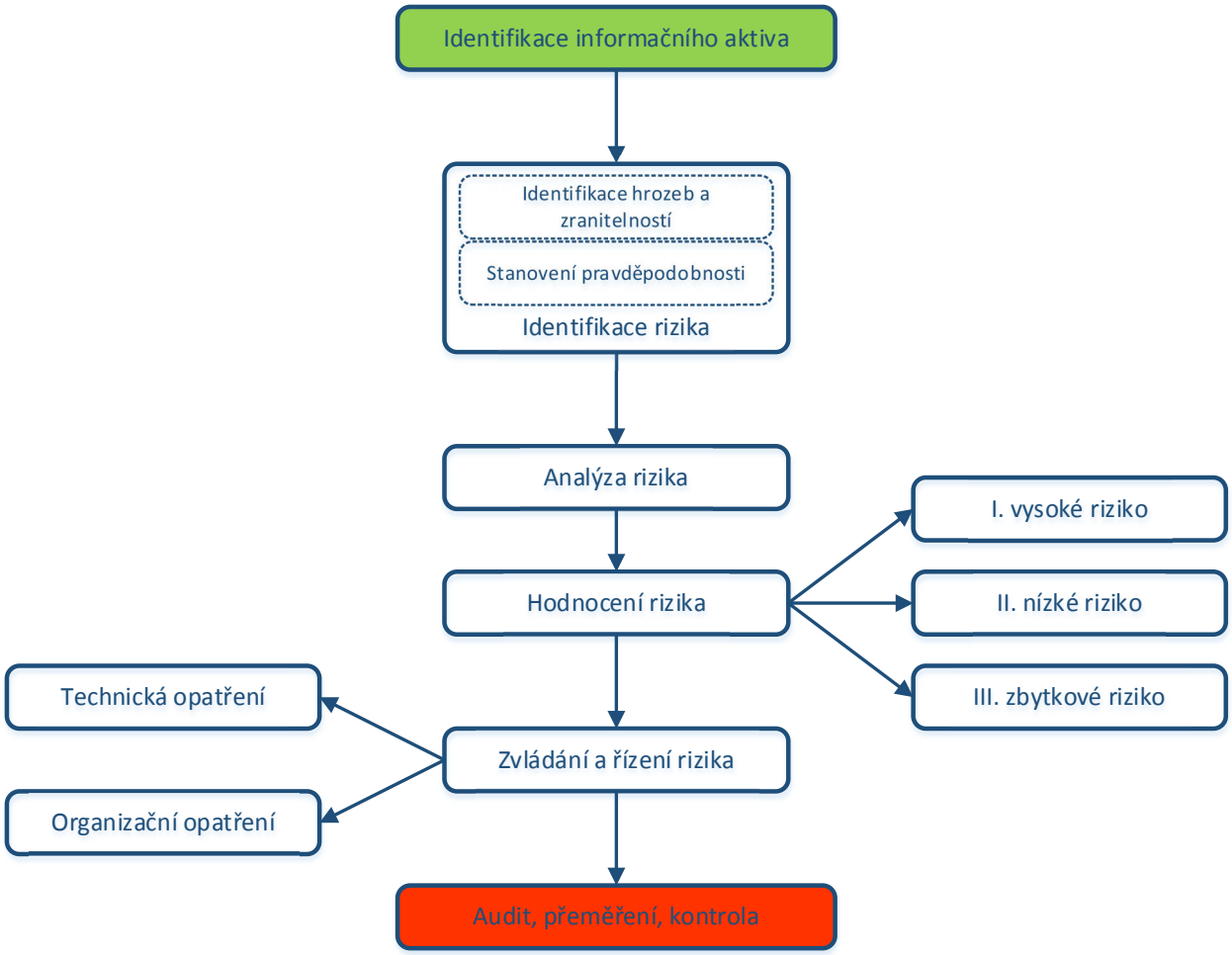
Hlavním principem implementace GDPR je přístup založený na riziku (jak z pohledu subjektu údajů, tak z pohledu správce/event. zpracovatele údajů). Znamená to, že v prvé řadě je nezbytností vyhodnotit rizika, následně pak rizika posoudit a rozhodnout o přijetí opatření ke snížení a eliminaci rizika nebo riziko přijmout.

Pro riziko existuje celá řada definic. Riziko je nejčastěji definováno jako součin velikosti následků nežádoucí události a pravděpodobnosti, že k uvedené nežádoucí události dojde.

Analýzu rizik je možné zpracovat ve vztahu k základním právům a svobodám subjektu údajů, kterými jsou např.:

- *ochrana identity,*
- *právo na informace,*
- *právo na ochranu osobních údajů,*
- *právo na duševní a tělesnou integritu,*
- *právo na soukromí,*
- *atd.*

Obecný proces hodnocení a řízení rizika - schéma procesu



Otázka č. 6: Co hrozí v případě nedodržení GDPR, jaké postihy? A kdo je může a bude udělovat? Jaká „provinění" patří z hlediska GDPR mezi nejvážnější?

Odpověď:
Sankce za porušení jsou „dvourychlostní". Za méně závažné porušení je pokuta maximálně 10 000 000 EUR, či 2 % ročního obratu. Za „závažnější" porušení jako například za porušení základních zásad je sazba dvojnásobná. Kromě pokut/sankcí může úřad uložit omezení nebo pozastavení zpracování. Data bridges – oznamování o zpracování dat

Právní stanovisko:
V případě porušení povinností je možné uložit správci sankce, resp. správní pokuty. Právní úprava je stanovena v čl. 83 GDPR.

Správní pokuty jsou dvourychlostní. Za porušení některých ustanovení lze uložit správní pokuty až do výše 10 000 000 EUR, resp. 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 2 %, resp. 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší.

Vyšší sankce jsou ukládány za porušení základních zásad zpracování, práv subjektu údajů, předání osobních údajů do třetích zemí a mezinárodním organizacím, nesplnění příkazu dozorového úřadu dočasného omezení zpracování a porušení jakékoli povinnosti vyplývající z právních předpisů členského státu dle kapitoly IX (zpracování a svoboda projevu informací, přístup veřejnosti k úředním dokumentům, zpracování národních identifikačních čísel, zpracování v souvislosti se zaměstnáním, pro účely archivace ve veřejném zájmu, pro vědecký a historický výzkum a pro statistické účely).

Členské státy mohou stanovit i jiné sankce.

Otázka č. 7: Může se praktický lékař či ambulantní specialista na GDPR vůbec připravit svépomocí? Nebo musí použít externí služby, a jaké (právní, IT, …)?

Odpověď:
Může. Záleží zcela jednoznačně na ambulantním specialistovi a jeho svobodné volbě. I na výši finančních prostředků, které na tuto „novou" agendu může či plánuje vydat. Implementace GDPR de facto znamená zpracování základní inventarizace práce s osobními údaji, vyhodnocení možných rizik a přijetí adekvátních opatření. A kvalitní zdokumentování těchto úkonů. Implementace GDPR musí rozumně korespondovat s velikostí ambulance. Lze tedy konstatovat, že poskytovatel, který má v pořádku používané IT systémy a dodržuje stávající legislativu ochrany osobních údajů, je již na GDPR velmi dobře připraven a v podstatě „pouze" doplní odpovídající dokumentaci. To lze jistě zvládnout svépomocí, zvláště pak u menších ambulancí.

Právní stanovisko:
Odpovědnost za ochranu osobních údajů leží pouze a jedině na správci či zpracovateli osobních údajů.

Otázka č. 8: Kde si může praktický lékař či ambulantní specialista ověřit, že je na GDPR dobře připraven, případně kde lze konzultovat problémy? Existuje nějaký úřad, odpovědná instituce v tomto směru?

Odpověď:
Konzultovat je možné u Úřadu pro ochranu osobních údajů.

Právní stanovisko:
Dle ustanovení čl. 57 GDPR má národní dozorový úřad následující úkoly:

1. Aniž jsou dotčeny další úkoly stanovené tímto nařízením, každý dozorový úřad na svém území:
a) monitoruje a vymáhá uplatňování tohoto nařízení;
b) zvyšuje povědomí veřejnosti o rizicích, pravidlech, zárukách a právech v souvislosti se zpracováním a podporuje porozumění těmto otázkám. Zvláštní pozornost se přitom věnuje akcím, které jsou určeny speciálně pro děti;
c) v souladu s právem členského státu poskytuje poradenství vnitrostátnímu parlamentu, vládě a dalším orgánům a institucím ohledně legislativních a správních opatření týkajících se ochrany práv a svobod fyzických osob v souvislosti se zpracováním;
d) podporuje povědomí správců a zpracovatelů o jejich povinnostech podle tohoto nařízení;

e) na požádání poskytuje všem subjektům údajů informace ohledně výkonu jejich práv podle tohoto nařízení a, je-li to vhodné, spolupracuje za tímto účelem s dozorovými úřady v jiných členských státech;

f) zabývá se stížnostmi, které mu podá subjekt údajů nebo subjekt, organizace či sdružení v souladu s článkem 80, a ve vhodné míře prošetřuje předmět stížnosti a v přiměřené lhůtě informuje stěžovatele o vývoji a výsledku šetření, zejména v případech, kdy je zapotřebí další šetření nebo koordinace s jiným dozorovým úřadem;

g) s cílem zajistit jednotné uplatňování a prosazování tohoto nařízení spolupracuje s dalšími dozorovými úřady, mimo jiné formou sdílení informací, a s těmito úřady si vzájemně poskytuje pomoc;

h) provádí šetření o uplatňování tohoto nařízení, mimo jiné na základě informací obdržených od jiného dozorového úřadu či jiného orgánu veřejné moci;

i) monitoruje vývoj v relevantních oblastech, pokud má vliv na ochranu osobních údajů, zejména vývoj informačních a komunikačních technologií a obchodních praktik;

j) přijímá standardní smluvní doložky uvedené v čl. 28 odst. 8 a čl. 46 odst. 2 písm. d);

k) připravuje a udržuje seznam v souvislosti s požadavkem provádět posouzení vlivu na ochranu osobních údajů podle čl. 35 odst. 4;

l) poskytuje poradenství o operacích zpracování uvedených v čl. 36 odst. 2;

m) podporuje vypracování kodexů chování podle čl. 40 odst. 1, vydává stanoviska a schvaluje takové kodexy chování, které poskytují dostatečné záruky podle čl. 40 odst. 5;

n) vybízí k zavedení mechanismů pro vydávání osvědčení o ochraně údajů a pečetí a známek dokládajících ochranu údajů podle čl. 42 odst. 1 a schvaluje kritéria pro vydávání osvědčení podle čl. 42 odst. 5;

o) případně provádí pravidelný přezkum osvědčení vydaných v souladu s čl. 42 odst. 7;

p) navrhuje a zveřejňuje kritéria pro schvalování subjektu pro monitorování kodexů chování podle článku 41 a subjektu pro vydávání osvědčení podle článku 43;

q) provádí schvalování subjektu pro monitorování kodexů chování podle článku 41 a subjektu pro vydávání osvědčení podle článku 43;

r) schvaluje smluvní doložky a ustanovení uvedené v čl. 46 odst. 3;

s) schvaluje závazná podniková pravidla podle článku 47;

t) přispívá k činnostem sboru;

u) vede interní záznamy o porušeních tohoto nařízení a o opatřeních přijatých podle čl. 58 odst. 2; a

v) plní veškeré další úkoly související s ochranou osobních údajů.

Otázka č. 9: Primární a specializovaná ambulantní péče většinou pracuje s informačním systémem dodaným dodavateli – na co je třeba při nástupu GDPR v tomto ohledu dávat pozor? Mění se nějak postavení dodavatele? Bude třeba měnit smlouvy? - a pokud, tak jak?

Odpověď:
V případě, že bude mít dodavatel přístup k osobním údajům, pak ano, je třeba uzavřít nové smlouvy o zpracování osobních údajů nebo je třeba stávající smlouvy o zpracování osobních údajů doplnit formou dodatku. Jde o vysoce doporučený krok, neboť přesné vymezení povinností dodavatele IT, dle ustanovení GDPR, chrání poskytovatele zdravotních služeb proti externímu zavinění, které by neměl šanci při provozu ambulance ovlivnit nebo odhalit. V příloze 5 tohoto materiálu je uveden metodický návod pro zpracování smlouvy na ochranu osobních údajů.

Právní stanovisko:

*Zpracování zpracovatelem se řídí **smlouvou nebo jiným právním aktem** podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci. Smlouva má povinně písemnou formu, vč. elektronické formy. Náležitosti smlouvy o zpracování:*

- *předmět a doba trvání zpracování,*
- *povaha a účel zpracování,*
- *typ osobních údajů a kategorie subjektů údajů,*
- *povinnosti a práva správce.*

Podle článku 28 smlouva nebo jiný právní akt zejména stanoví, že zpracovatel:

- *zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládá právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;*
- *zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;*
- *přijme všechna opatření požadovaná podle článku 32;*
- *dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4 čl. 28;*
- *zohledňuje povahu zpracování, zpracovatel je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III;*
- *je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;*
- *v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;*
- *poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.*

V příloze č. 5 jsou uvedeny konkrétní parametry smlouvy o zpracování osobních údajů, které je nutné do smlouvy promítnout.

Zpracovatel a jakákoli osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, může tyto osobní údaje zpracovávat pouze na pokyn správce, ledaže jí jejich zpracování ukládá právo Unie nebo členského státu. Pokud zpracovatel poruší toto nařízení tím, že určí účely a prostředky zpracování, považuje se ve vztahu k takovému zpracování za správce.

Otázka č. 10: Jak má být dle GDPR správně zabezpečena zdravotnická dokumentace v používaném informačním systému? A je to odpovědnost dodavatele a provozovatele, nebo jde o primární odpovědnost poskytovatele zdravotních služeb? Problémem je, že lékaři nejsou IT odborníky – mělo by tedy jít o službu, kterou garantuje přímo její dodavatel – možnosti lékaře v kontrole jsou minimální.

Odpověď:

Odpovědnost leží zcela na správci osobních údajů, tedy na lékaři. Garance a odpovědnost dodavatele je potřeba zohlednit ve smlouvě o zpracování osobních údajů (viz otázka 9). V případě pochybností je nezbytné IT systém, či jeho komponenty, podrobit nezávislému auditu. A

nezapomenout na „zcela obyčejná“ opatření, kterými jsou např. zamykání dveří či logování přístupů.

Právní stanovisko:
Zabezpečení zpracování spočívá v provedení vhodných technických a organizačních opatření. Tato opatření provedou správce a zpracovatel, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:
a) pseudonymizace a šifrování osobních údajů;
b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:
a) náhodné nebo protiprávní zničení,
b) ztráta,
c) pozměňování,
d) neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která
a) jedná z pověření správce nebo zpracovatele
b) má přístup k osobním údajům,
zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování.

Otázka č. 11: Jaká ustanovení zejména je třeba vložit do smlouvy s dodavatelem – provozovatelem informačního systému, aby byla ambulance „kryta“ proti selhání na straně IT?

Odpověď:
Kvalitní smlouva o zpracování osobních údajů je základním předpokladem pro ochranu lékaře – poskytovatele zdravotních služeb. Vybrané parametry smlouvy o zpracování osobních údajů ve vazbě na jednotlivé články GDPR a povinnosti tam stanovené shrnuje příloha č. 5 tohoto dokumentu. Nutno mít nastavena jasná pravidla.

Právní stanovisko:

*Zpracování zpracovatelem se řídí **smlouvou nebo jiným právním aktem** podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci. Smlouva má povinně písemnou formu, vč. elektronické formy. Náležitosti smlouvy o zpracování:*

- *předmět a doba trvání zpracování,*
- *povaha a účel zpracování,*
- *typ osobních údajů a kategorie subjektů údajů,*
- *povinnosti a práva správce.*

Podle článku 28 smlouva nebo jiný právní akt zejména stanoví, že zpracovatel:

- *zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládá právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;*
- *zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;*
- *přijme všechna opatření požadovaná podle článku 32;*
- *dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4 čl. 28;*
- *zohledňuje povahu zpracování, zpracovatel je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III;*
- *je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;*
- *v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;*
- *poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.*

V příloze naleznete konkrétní parametry smlouvy o zpracování osobních údajů, které je nutné do smlouvy promítnout.

Zpracovatel a jakákoli osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, může tyto osobní údaje zpracovávat pouze na pokyn správce, ledaže jí jejich zpracování ukládá právo Unie nebo členského státu. Pokud zpracovatel poruší toto nařízení tím, že určí účely a prostředky zpracování, považuje se ve vztahu k takovému zpracování za správce.

Otázka č. 12: Co dělat v případě, kdy má ambulance data o pacientech vedeny v cloudu? (tedy využívá nějakou formu úložiště dat nebo vzdálený přístup k datům při potřebě pracovat na různých místech)

Odpověď:
Je nutné mít uzavřenu kvalitní smlouvu o zpracování osobních údajů, kdy vlastník a také provozovatel cloudu jsou v pozici zpracovatele osobních údajů a jsou pro něj specifikovány odpovídající povinnosti. V případě pochybností je nezbytné daný IT systém, či jeho komponenty, podrobit nezávislému auditu.

Právní stanovisko:

*Zpracování zpracovatelem se řídí **smlouvou nebo jiným právním aktem** podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci. Smlouva má povinně písemnou formu, vč. elektronické formy. Náležitosti smlouvy o zpracování:*

- *předmět a doba trvání zpracování,*
- *povaha a účel zpracování,*
- *typ osobních údajů a kategorie subjektů údajů,*
- *povinnosti a práva správce.*

Podle článku 28 smlouva nebo jiný právní akt zejména stanoví, že zpracovatel:

- *zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládá právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;*
- *zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;*
- *přijme všechna opatření požadovaná podle článku 32;*
- *dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4 čl. 28;*
- *zohledňuje povahu zpracování, zpracovatel je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III;*
- *je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;*
- *v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;*
- *poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.*

V příloze naleznete konkrétní parametry smlouvy o zpracování osobních údajů, které je nutné do smlouvy promítnout.

Zpracovatel a jakákoli osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, může tyto osobní údaje zpracovávat pouze na pokyn správce, ledaže jí jejich zpracování ukládá právo Unie nebo členského státu. Pokud zpracovatel poruší toto nařízení tím, že určí účely a prostředky zpracování, považuje se ve vztahu k takovému zpracování za správce.

Otázka č. 13: Praktický lékař sdílí dokumentaci a výsledky s jinými lékaři, nemocnicemi – je tato komunikace a předávání informací o jím vedených pacientech nadále možná bez zvláštních smluv? Nebo bude nutné uzavírat nějaké smlouvy se všemi poskytovateli, se kterými informace sdílí?

Odpověď:
Smlouva není potřeba za předpokladu, že se jedná o zajištění návaznosti dalších zdravotních nebo sociálních služeb. To platí za předpokladu, že budou dodrženy ostatní povinnosti dle GDPR – např. zabezpečená forma předání, kontrola přístupu k citlivým a osobním údajům, apod. V jiném případě

smlouva zapotřebí je, například pokud se jedná o klinickou studii, zpracování dat nesouvisejících se zajištěním zdravotních nebo sociálních služeb, apod.

Právní stanovisko:
Ve smyslu ustanovení § 45 odst. 2 písmeno g) je poskytovatel zdravotních služeb povinen předat jiným poskytovatelům zdravotních služeb nebo poskytovatelům sociálních služeb potřebné informace o zdravotním stavu pacienta nezbytné k zajištění návaznosti dalších zdravotních a sociálních služeb poskytovaných pacientovi. V tomto případě je předání osobních údajů zákonné za předpokladu, že budou dodrženy ostatní parametry, resp. povinností stanovené GDPR (záruky).

Otázka č. 14: Musí se pro vedení primární zdravotnické dokumentace vést informovaný souhlas pacienta?

Odpověď:
Ne, jedná se o plnění právní povinnosti pro lékaře, která vyplývá z právních předpisů.

Právní stanovisko:
***Zákonnost, korektnost a transparentnost** jsou základní zásady GDPR. Dle čl. 6 GDPR je zpracování zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a jsou zpracovávány osobní údaje pouze v odpovídajícím rozsahu:*

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

Vzhledem k tomu, že vedení zdravotnické dokumentace je upraveno právními předpisy ČR zejména:

- ***zákonem č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů:***
  - *§ 53 a 69 - Zdravotnická dokumentace*
- ***prováděcí vyhláškou k zákonu o zdravotních službách:***
  Vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci, ve znění pozdějších předpisů
  - *Příloha č. 1 - Minimální rozsah zdravotnické dokumentace*
  - *Příloha č. 2 - Zásady pro uchování zdravotnické dokumentace a postup při jejím vyřazování a zničení po uplynutí doby uchování*
  - *Příloha č. 3 - Doby uchování zdravotnické dokumentace nebo jejích částí*

Otázka č. 15: Může pacient dle GDPR odmítnout vedení primární zdravotnické dokumentace?

Odpověď:
Ne, jedná se o plnění právní povinnosti pro lékaře, která vyplývá z právních předpisů.

Právní stanovisko:
Ve smyslu ustanovení § 53 odst. 1 zákona o zdravotních službách je poskytovatel povinen vést a uchovávat zdravotnickou dokumentaci a nakládat s ní podle tohoto zákona a jiných právních předpisů. Podle odstavce 2 téhož ustanovení je zdravotnická dokumentace souborem informací vztahujících se k pacientovi, o němž je vedena.

Otázka č. 16: Jsou kontaktní údaje pacienta – tedy pouze jméno a telefon nebo jméno a e-mail – osobními údaji, které vyžadují zvláštní režim a ochranu?

Odpověď:
Osobními údaji je vše, podle čeho může být pacient identifikován. Telefonní číslo i emailová adresa k nim bezesporu patří.

Právní stanovisko:
Ve smyslu ustanovení čl. 4 odst. 1 GDPR jsou „osobními údaji" veškeré informace o identifikované nebo identifikovatelné fyzické osobě („subjektu údajů"), přičemž identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Otázka č. 17: Pokud ambulance vede u záznamů pacienta i záznamy (kontakty) na jeho příbuzné, kterým dal oprávnění k podávání informací apod. – lze tyto záznamy nadále vést? A je nutný informovaný souhlas těchto příbuzných?

Odpověď:
Tyto údaje lze nadále vést, protože na to pamatuje zákon jako na právo pacienta, ovšem při zachování všech pravidel GDPR pro jejich zpracování. Souhlas příbuzných není nutný.

Právní stanovisko:
Podle § 33 odst. 1 zákona o zdravotních službách může pacient při přijetí do péče určit osoby, které mohou být informovány o jeho zdravotním stavu, a současně může určit, zda tyto osoby mohou nahlížet do zdravotnické dokumentace o něm vedené nebo do jiných zápisů vztahujících se k jeho zdravotnímu stavu, pořizovat si výpisy nebo kopie těchto dokumentů a zda mohou v případech podle § 34 odst. 7 téhož zákona vyslovit souhlas nebo nesouhlas s poskytnutím zdravotních služeb. Pacient může určit osoby nebo vyslovit zákaz poskytovat informace o zdravotním stavu kterékoliv osobě kdykoliv po přijetí do péče, rovněž může určení osoby nebo vyslovení zákazu poskytovat informace o zdravotním stavu kdykoliv odvolat. Záznam o vyjádření pacienta je součástí zdravotnické dokumentace o něm vedené; záznam podepíše pacient a zdravotnický pracovník. Součástí záznamu je rovněž sdělení pacienta, jakým způsobem mohou být informace o jeho zdravotním stavu sdělovány.

Ve smyslu ustanovení čl. 14 odst. 5 GDPR není nutné informovat subjekt údajů, a to pokud a do té míry, v níž:
a) subjekt údajů již uvedené informace má;
b) se ukáže, že poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí; to platí zejména v případě zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého

či historického výzkumu nebo pro statistické účely s výhradou podmínek a záruk uvedených v čl. 89 odst. 1 GDPR, nebo pokud je pravděpodobné, že uplatnění povinnosti uvedené v odstavci 1 tohoto článku by znemožnilo nebo výrazně ztížilo dosažení cílů uvedeného zpracování. V takových případech přijme správce vhodná opatření na ochranu práv, svobod a oprávněných zájmů subjektu údajů, včetně zpřístupnění daných informací veřejnosti;

c) je získávání nebo zpřístupnění výslovně stanoveno právem Unie nebo členského státu, které se na správce vztahuje a v němž jsou stanovena vhodná opatření na ochranu oprávněných zájmů subjektu údajů; nebo

d) osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovávat služební tajemství upravenou právem Unie nebo členského státu, včetně zákonné povinnosti mlčenlivosti.

Otázka č. 18: Může pacient požadovat, aby mu lékař doložil, že postupuje dle GDPR? A co v takovém případě považovat za adekvátní doložení?

Odpověď:
Pacient jako subjekt údajů má právo a měl by být (musí) být informován o tom, jak jsou jeho osobní údaje zpracovávány. GDPR má přesné parametry této informace (tuto lze připravit předem písemně, aby vlastní informování nezdržovalo provoz ambulance a nepřipravovalo odborný personál o cenný čas); jedna z možných variant je uvedena i v přílohách materiálu (příloha č. 6).

Právní stanovisko:
Dle čl. 12 a 13 GDPR musí správce tyto informace poskytnout v okamžiku získání osobních údajů s výjimkou případů, že je již subjekt údajů má či v jiných případech, na které GDPR pamatuje (např. v případech, kdy jde o ochranu života subjektu údajů). Povinnost správce informovat subjekt údajů transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků informace dle čl. 13, 14, 15–22 a 34. Informace o opatřeních přijatých dle čl. 15–22 jsou předávány na základě žádosti. Lhůta pro vyřízení žádosti je 1 měsíc, maximálně je ji možné dvakrát prodloužit.

Otázka č. 19: Může pacient dle GDPR odmítnout předání své zdravotnické dokumentace jinému lékaři, nemocnici, pokud to jeho zdravotní stav, či navazující péče, vyžadují? A mění se nějak dle GDPR pravidla sdílení dokumentace mezi lékaři?

Odpověď:
Ne v případech, kdy je to nezbytné *k zajištění návaznosti dalších zdravotních a sociálních služeb poskytovaných pacientovi či pro ochranu práv jiných osob. Jedná se o plnění právní povinnosti pro lékaře, která vyplývá z právních předpisů. V tomto smyslu se nastavená pravidla nijak nemění.*

Právní stanovisko:
Ve smyslu ustanovení § 45 odst. 2 písmeno g) zákona o zdravotních službách je poskytovatel zdravotních služeb povinen předat jiným poskytovatelům zdravotních služeb nebo poskytovatelům sociálních služeb potřebné informace o zdravotním stavu pacienta nezbytné k zajištění návaznosti dalších zdravotních a sociálních služeb poskytovaných pacientovi. V tomto případě je předání osobních údajů zákonné za předpokladu, že budou dodrženy ostatní parametry, resp. povinností stanovené GDPR (záruky).

Totéž platí v případech, kdy jest tak stanoveno zákonem č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů.

Otázka č. 20: Lze e-mailovou komunikaci mezi lékaři, nebo mezi ambulancí a nemocničním lékařem – např. při předání pacienta, při konzultaci o jeho stavu – považovat za bezpečnou? Nebo má být nějak speciálně zabezpečena a jak?

Odpověď:
Obecně předání běžnou emailovou cestou není bezpečnou cestou. Předávání by mělo být řešeno zabezpečenými komunikačními prvky, kterými jsou v současné době datové schránky či sdílená datová uložiště zabezpečená např. šifrováním. Rovněž je možné i předávání osobní proti prokázání totožnosti. V případě telefonického předávání informací na základě hesla by toto mělo být podchyceno ve smlouvě o zpracování osobních údajů.

Právní stanovisko:

Správce musí ve smyslu ustanovení čl. 24 a násl. GDPR provádět zpracování v souladu s GDPR, a to s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování a k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob.

- *Za tím účelem zavede vhodná technická a organizační opatření,*
- *tato opatření musí být schopen doložit,*
- *tato opatření musí podle potřeby revidovat a aktualizovat,*
- *vhodné je i zpracování koncepce.*

Zabezpečení zpracování spočívá v provedení vhodných technických a organizačních opatření. Tato opatření provedou správce a zpracovatel, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:
a) pseudonymizace a šifrování osobních údajů;
b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:
a) náhodné nebo protiprávní zničení,
b) ztráta,
c) pozměňování,
d) neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která
a) jedná z pověření správce nebo zpracovatele
b) má přístup k osobním údajům,
zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování.

Otázka č. 21: Mění se v GDPR nějak práva a povinnosti nelékařského zdravotnického personálu, zejména zdravotních sester? V běžné praxi sestra v ambulanci pracuje s osobními údaji i se zdravotnickou dokumentací a komunikuje s pacienty. Bude toto nadále možné?

Odpověď:
Praxe zůstává zachována s tím, že je potřeba dodržet zásady zpracování a zajistit všechnu potřebnou dokumentaci, vč. přehledů o nahlížení do zdravotnické dokumentace jak v listinné, tak i elektronické podobě. Zdravotnický personál musí být také proškolen a znát vnitřní předpisy správné práce s osobními údaji. O proškolení by měl v ambulanci existovat záznam.

Právní stanovisko:
Zabezpečení zpracování spočívá v provedení vhodných technických a organizačních opatření. Tato opatření provedou správce a zpracovatel, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:
a) pseudonymizace a šifrování osobních údajů;
b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:
a) náhodné nebo protiprávní zničení,
b) ztráta,
c) pozměňování,
d) neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která
a) jedná z pověření správce nebo zpracovatele
b) má přístup k osobním údajům,
zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování.

Otázka č. 22: Jak postupovat při žádosti o nahlédnutí do zdravotní dokumentace oprávněnou osobou včetně pořízení kopie dokumentace (výpis z dokumentace)? Bude zde vyžadován zvláštní informovaný souhlas, a jaký?

Odpověď:
Nahlížení do zdravotnické dokumentace je upraveno zákonem o zdravotních službách. Stávající postupy se nemění.

Právní stanovisko:
Souhlas se zpracováním osobních údajů je pouze jedním z právních titulů jejich zpracování. V tomto případě se jedná o jiný právní titul zpracování – plnění právní povinnosti. Vzhledem k tomu, že dle ustanovení § 41 odst. 3 zákona o zdravotních službách pacient, zákonný zástupce nebo opatrovník pacienta, osoba určená pacientem, osoba blízká pacientovi nebo osoba ze společné domácnosti jsou povinni prokázat svou totožnost občanským průkazem, jestliže o to poskytovatel nebo zdravotnický pracovník, jehož prostřednictvím poskytovatel poskytuje pacientovi zdravotní služby, požádá. Povinnost prokázat se občanským průkazem má rovněž osoba, která uplatňuje podle tohoto zákona nebo jiného právního předpisu právo na informace o zdravotním stavu pacienta, a osoba, která hodlá hospitalizovaného pacienta navštívit a není osobou podle věty první. Jde-li o cizince, totožnost se prokazuje cestovním dokladem nebo jiným průkazem totožnosti. Má-li zdravotnický pracovník pochybnost, zda jde o osobu blízkou, osvědčí osoba blízká tuto skutečnost čestným prohlášením, ve kterém uvede své kontaktní údaje a číslo průkazu totožnosti; čestné prohlášení je součástí zdravotnické dokumentace vedené o pacientovi.

V tomto případě je nutné oprávněnou osobu jako subjekt údajů pouze informovat o všech parametrech zpracování jeho osobních údajů, nikoliv jej žádat o souhlas se zpracováním osobních údajů.

Otázka č. 23: Následující soupis shrnuje hlavní aktivity/činnosti praktického lékaře. Bylo by možné každou okomentovat, jaký na ni má dopad GDPR a co se pro ni má upravit/nastavit, aby byla vedena správně?

Soupis činností Praktického lékaře pro děti a dorost s použitím záznamů s osobními údaji			
	Činnost	**Práce s osobními údaji**	**Poznámka k právnímu titulu**
1	Registrace do obvodu	Založení dokumentace	plnění právní povinnosti
2	Prohlídka novorozence doma	Zápis do dokumentace	plnění právní povinnosti
3	1. návštěva v poradně	Zápis do dokumentace	plnění právní povinnosti
4	Návštěva nemocného	Zápis do dokumentace	plnění právní povinnosti
5	Prohlídka v poradně	Zápis do dokumentace	plnění právní povinnosti
6	Prohlídka v kurativě	Zápis do dokumentace	plnění právní povinnosti

7	Vystavení receptu/žádanky	Vystavení dokumentu a zápis	plnění právní povinnosti
8	Vystavení OČR	Vystavení dokumentu a zápis	plnění právní povinnosti
9	Vystavení neschopenky	Vystavení dokumentu a zápis	plnění právní povinnosti
10	Doporučení - laboratoř	Vystavení dokumentu a zápis	plnění právní povinnosti
11	Doporučení vyšetření specialistou	Vystavení dokumentu a zápis	plnění právní povinnosti
12	Doporučení k hospitalizaci	Vystavení dokumentu a zápis	plnění právní povinnosti
13	Potvrzení na žádost bezplatné	Vystavení dokumentu a zápis	plnění smlouvy
14	Potvrzení na žádost placené	Vystavení dokumentu a zápis	plnění smlouvy
15	Komunikace s OSPOT	Vystavení zprávy a zápis	plnění právní povinnosti
16	Vystavení žádosti o lázně	Vystavení poukazu a zápis	plnění právní povinnosti
17	Vystavení pojistky	Vyplnění pojistky a zápis	plnění smlouvy
18	Komunikace telefonem	Zápis do dokumentace	plnění smlouvy
19	Komunikace mailem	Zápis do dokumentace	plnění smlouvy
20	Dopis registrovanému pacientovi	Odeslání pozvánky	plnění právní povinnosti
21	Nepravidelná péče	Vystavení zprávy	plnění právní povinnosti
22	Administrace registrace	Zápis do dokumentace	plnění právní povinnosti
23	Vyřazení z péče	Zápis do dokumentace	plnění právní povinnosti
24	Záznam o zákroku v klinické studii	Zápis do dokumentace	nutný souhlas subjektu údajů
25	Zpráva o zákroku v klinické studii	Zápis do studiové dokumentace	nutný souhlas subjektu údajů
26	Kontrola a zápis pracovníka klinické studie	Nahlédnutí do dokumentace, zápis ve studiové dokumentaci	nutný souhlas subjektu údajů
26	Kontrola dokumentace pracovníkem hygienické služby	Nahlédnutí do dokumentace, hygienická služba vydává zprávu o kontrole	plnění právní povinnosti
27	Kontrola dokumentace revizním lékařem	Nahlédnutí do dokumentace, revizní lékař vydává zprávu o kontrole	plnění právní povinnosti
28	Vyžádání dokumentace policií	Předání dokumentace na základě řádné žádosti a zápis	plnění právní povinnosti
29	Vyžádání dokumentace soudem	Předání dokumentace na základě řádné žádosti a zápis	plnění právní povinnosti

30	Nahlédnutí do dokumentace oprávněnou osobou	Zápis do dokumentace	plnění právní povinnosti
31	Hlášení infekčního onemocnění	Zaslání hlášení	plnění právní povinnosti
32	Hlášení reakce po očkování	Zaslání hlášení a zápis	plnění právní povinnosti
33	Vyplnění povinného dotazníku	Zápis a založení do dokumentace	plnění právní povinnosti
34	Epikríza	Zápis a založení do dokumentace	plnění právní povinnosti
35	Hlášení ÚZIS	Odeslání souhrnného hlášení	plnění právní povinnosti

Odpověď:
Základní odpovědnost lékaře, resp. poskytovatele zdravotních služeb, je zpracovávat osobní údaje dle zásad GDPR a mít vše řádně zdokumentováno. Základní zásadou je zpracovávat osobní údaje zákonně. Ve výše uvedené tabulce jsou uvedeny předpokládané tituly zpracování osobních údajů, které jsou z pohledu GDPR zákonnými důvody jejich zpracování.

Právní stanovisko:

Správce musí ve smyslu ustanovení čl. 24 a násl. GDPR provádět zpracování v souladu s GDPR, a to s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování a k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob.

- *Za tím účelem zavede vhodná technická a organizační opatření,*
- *tato opatření musí být schopen doložit,*
- *tato opatření musí podle potřeby revidovat a aktualizovat,*
- *vhodné je i zpracování koncepce.*

Zabezpečení zpracování spočívá v provedení vhodných technických a organizačních opatření. Tato opatření provedou správce a zpracovatel, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) pseudonymizace a šifrování osobních údajů;
b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:

a) náhodné nebo protiprávní zničení,
b) ztráta,
c) pozměňování,

d) neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která
a) jedná z pověření správce nebo zpracovatele
b) má přístup k osobním údajům,
zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování.

Následující otázky se týkají praxe laboratoří obsluhujících praktické lékaře a ambulance

Otázka č. 24: V rámci laboratorní dokumentace jsou vedeny karty pracovníků (např. v MS Word), kde jsou údaje osobní, o vzdělání, školení, prohlídkách, platovém zařazení atd. Lze je vést i nadále a za jakých podmínek? Je pro vedení takové dokumentace v laboratoři nově potřebný informovaný souhlas pracovníků?

Odpověď:
Je možné vést tyto údaje, vzhledem k tomu, že jde o povinnost stanovenou zákonem pro správce (dle zákoníku práce), ovšem opět je nutné zohlednit technická a organizační opatření k jejich zabezpečení.

Právní stanovisko:
Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a jsou zpracovávány osobní údaje pouze v odpovídajícím rozsahu:
a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

Otázka č. 25: Změní nástup GDPR předávání dokumentace a výsledků mezi praxí lékařem a laboratoří?

Odpověď:
Povinnosti se nemění,je potřeba zajistit bezpečnost jejich předávání vhodnými zárukami. Nejen smluvními – předání musí být prováděno zabezpečenými cestami a nástroji a k těmto procesům by se měla vázat adekvátní analýza rizik a přijatá opatření k jejich minimalizaci. Otevřená komunikace elektronickou poštou (e-mailem) není bezpečnou cestou předávání citlivých údajů.

Právní stanovisko:
Zabezpečení zpracování spočívá v provedení vhodných technických a organizačních opatření. Tato opatření provedou správce a zpracovatel, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:
a) pseudonymizace a šifrování osobních údajů;
b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:
a) náhodné nebo protiprávní zničení,
b) ztráta,
c) pozměňování,
d) neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která
a) jedná z pověření správce nebo zpracovatele
b) má přístup k osobním údajům,
zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování.

Otázka č. 26: V laboratoři bývá na počítači adresář dodavatelů, servisů, jiných laboratoří, praktických lékařů z dané oblasti aj. Co je třeba učinit pro jeho zachování?

Odpověď:
Je možné vést tyto údaje, vzhledem k tomu, že jde o běžné dodavatelské kontakty a kontakty spolupracujících subjektů. Ovšem opět je nutné zohlednit technická a organizační opatření k jejich zabezpečení.

Právní stanovisko:
Viz výše otázky 25 – 26.

Otázka č. 27: V laboratoři je k dispozici „kniha výsledků" (identifikace pacienta a jeho výsledky k odběru), může být v el. podobě i papírová. Bude možné ji nadále mít? A za jakých podmínek?

Odpověď:
Laboratoř je poskytovatelem zdravotních služeb a na vedení těchto záznamů se vztahují stejná pravidla jako na primární zdravotnickou dokumentaci.

Právní stanovisko:
Ve smyslu ustanovení § 53 odst. 1zákona o zdravotních službách je poskytovatel povinen vést a uchovávat zdravotnickou dokumentaci a nakládat s ní podle tohoto zákona a jiných právních předpisů. Podle odstavce 2 téhož ustanovení je zdravotnická dokumentace je souborem informací vztahujících se k pacientovi, o němž je vedena.

Otázka č. 28: V informačním systému, v němž se řídí laboratorní dokumentace, jsou seznamy všech pracovníků, kteří mají k datům přístup se základní informací o nich. Je to nezbytné pro stanovení přístupových práv a sledování jejich práce s dokumenty. Nelze o ni kvůli GDPR přijít! – jak mají být tyto věci ošetřeny, aby laboratoř mohla pokračovat v činnosti?

Odpověď:
Je nutné zavést taková opatření (organizační i technická), aby byly zmapovány všechny přístupy do informačního systému a uložené informace byly zabezpečeny. Smyslem GDPR není zakazovat vedení takové dokumentace, ale minimalizovat riziko zneužití a poškození práv subjektů údajů. Odpovědný správce dat pak musí být schopen doložit, že má zmapované, jaké osobní údaje vede, kde je vede, jak je zabezpečuje a jak kontroluje přístupy k nim.

Právní stanovisko:
Zabezpečení zpracování spočívá v provedení vhodných technických a organizačních opatření. Tato opatření provedou správce a zpracovatel, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:
a) pseudonymizace a šifrování osobních údajů;
b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:
a) náhodné nebo protiprávní zničení,
b) ztráta,

c) pozměňování,
d) neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která
a) jedná z pověření správce nebo zpracovatele
b) má přístup k osobním údajům,
zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování.

Otázka č. 29: Je běžné a vstřícné ze strany laboratoře kolegům (lékařům) sdělit výsledky či další podrobnosti i telefonicky - někdy se ptají na předběžné (kultivační) výsledky, někdy nemohou papír najít, někdy je (ty zaslané) potřebují konzultovat. Co učinit, aby toto bylo nadále možné?

Odpověď:
Pokud se znají není problém. Telefonické předání, vč. hesla pro tuto komunikaci je vhodné upravit do smlouvy uzavíranou mezi lékařem a laboratoří, jako i další formy používané komunikace. Komunikace musí být bezpečná a musí minimalizovat riziko zneužití a poškození práv subjektů údajů.

Právní stanovisko:
Zabezpečení zpracování spočívá v provedení vhodných technických a organizačních opatření. Tato opatření provedou správce a zpracovatel, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:
a) pseudonymizace a šifrování osobních údajů;
b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:
a) náhodné nebo protiprávní zničení,
b) ztráta,
c) pozměňování,
d) neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která
a) jedná z pověření správce nebo zpracovatele
b) má přístup k osobním údajům,
zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování.

Otázka č. 30: V horské ordinaci je paní doktorka, která nemá a nebude mít počítač. Výsledky jí vozí kurýr, když jede pro odběry, nebo nosí pošta, když nelze jinak. Běžně jí laboratoř výsledky sděluje telefonicky. Jak to lze dělat i po květnu 2018?

Odpověď:
Osobní i citlivé údaje je nutné předávat zabezpečenou formou. Telefonické předání, vč. hesla pro tuto komunikaci je vhodné upravit do smlouvy uzavíranou mezi lékařem a laboratoří. Obdobně takto může být ošetřena i jiná forma komunikace. Poštovní předání musí být adekvátně zabezpečeno, předávání osobní (kurýrem) proti prokázání totožnosti je rovněž možné.

Právní stanovisko:
Zabezpečení zpracování spočívá v provedení vhodných technických a organizačních opatření. Tato opatření provedou správce a zpracovatel, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:
a) pseudonymizace a šifrování osobních údajů;
b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména:
a) náhodné nebo protiprávní zničení,
b) ztráta,
c) pozměňování,
d) neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

Správce a zpracovatel přijmou opatření pro zajištění, aby jakákoli fyzická osoba, která
a) jedná z pověření správce nebo zpracovatele
b) má přístup k osobním údajům,
zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Jedním z prvků, kterými lze prokázat soulad, je dodržování schváleného kodexu chování nebo uplatňování schváleného mechanismu pro vydávání osvědčení. V minimální podobě lze prokázat soulad záznamy o činnostech zpracování.