Ministerstvo zdravotnictví ČR
Ústav zdravotnických informací a statistiky ČR

Jak implementovat 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

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

(vypracováno jako metodický materiál pro PŘO a ÚZIS ČR)

VERZE 1.1

V Praze dne 30. listopadu 2017

Autorský kolektiv: Mgr. JUDr. Vladimíra Těšitelová, zástupce ředitele ÚZIS ČR
JUDr. Radek Policar, náměstek ministra zdravotnictví
Ing. Milan Blaha, Ph.D., vedoucí odboru IT ÚZIS ČR
RNDr. Daniel Klimeš, Ph.D., vedoucí datového centra ÚZIS ČR
doc. RNDr. Ladislav Dušek, Ph.D., ředitel ÚZIS ČR

Recenze: doc. JUDr. Radim Polčák, Ph.D., Ústav práva a technologií, Masarykova univerzita Brno

Konzultováno: Úřad pro ochranu osobních údajů
MV ČR, odbor legislativy a koordinace předpisů

Obsah

Přílohy:

Použité zkratky:

Pro účely tohoto materiálu je používáno:

- již obecně zažité označení Obecného nařízení pro ochranu osobních údajů – GDPR (General Data Protection Regulation),
- pojem citlivé osobní údaje pro zvláštní kategorie osobních údajů definované čl. 9 GDPR

MZ ČR – Ministerstvo zdravotnictví ČR

PŘO – přímo řízené organizace MZ ČR

ÚZIS ČR – Ústav zdravotnických informací a statistiky ČR

NZIS – Národní zdravotnický informační systém

DPO – pověřenec pro ochranu osobních údajů

ÚOOÚ – Úřad pro ochranu osobních údajů

DPIA – posouzení vlivu na ochranu osobních údajů

EPDB – Evropský sbor pro ochranu osobních údajů

Autorský kolektiv děkuje zejména PhDr. M. Matoušové a JUDr. S. Matochové, Ph.D. a Mgr. J. Prokešovi, pracovníkům Úřadu pro ochranu osobních údajů, kteří svojí konzultační činností přispěli k vydání této publikace.

1. Úvod

Téměř každá publikace přicházející s něčím novým nese na svém samotném počátku větu „Dostáváte do rukou…“ a dále pokračuje. Zkusme ji zde v samotném úvodu vyslovit také a návazně na ni si položme pár otázek z ní vycházejících.

Dostáváte do rukou praktický návod, jak se připravit na novou evropskou legislativu v oblasti ochrany osobních údajů. Jde o 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 anglickém jazyce „General Data Protection Regulation“, ve zkratce „**GDPR**“) s účinností od 25. 5. 2018. Jelikož zkratka GDPR je již široce zavedena, budeme ji takto používat i v tomto dokumentu.

Jaké si tato publikace klade cíle? Pouze jeden jediný. Provést čtenáře ustanoveními GDPR krok za krokem a vysvětlit jednotlivá ustanovení, upozornit na úskalí a odstranit obavy ještě předtím, než nové nařízení nabude účinnosti. Další logickou otázkou čtenáře je: stihneme to? Odpověď je poměrně jednoduchá. Pokud v současné době dodržujete platné právní předpisy týkající se ochrany osobních údajů a začnete s přípravou právě nyní, potom lze s přiměřenou jistotou říci, že přípravu stihnete.

Pokud přijmete i tuto odpověď, jistě Vás napadne i otázka, jakou závaznost má tato publikace, proč se řídit právě jí? Zde si pomůžeme přímo ustanoveními samotného GDPR. Odpovědnost za ochranu osobních údajů leží pouze a jedině na správci či zpracovateli osobních údajů. Ani vydané osvědčení souladu s GDPR nezbavuje správce či zpracovatele jejich odpovědnosti. Vnímejte proto tuto publikaci jako prvotní metodický návod pro resort zdravotnictví, vydaný na základě detailního právního rozboru GDPR ze strany Ministerstva zdravotnictví ve spolupráci s Ústavem zdravotnických informací a statistiky ČR.

Ve své stručnosti publikace nemůže mít za cíl kompletně danou problematiku vyčerpat. Ochraně osobních údajů ve zdravotnictví by bylo možné věnovat stovky stran a dále toto téma rozpracovat ve vztahu ke kybernetické bezpečnosti, nastupující elektronizaci zdravotnictví nebo s ohledem na úskalí personalizované medicíny, která nevyhnutelně pracuje s velkým objemem citlivých údajů, včetně informací genetických. Vnímejme tato a další témata jako výzvy pro další publikace a autory, naším cílem zde bylo udržet materiál v přijatelném rozsahu jako pragmaticky orientovanou uživatelskou příručku.

Na závěr tohoto úvodu nezbývá, než dodat, že tato publikace Vám není předávána v definitivní verzi, mimo jiné z toho důvodu, že samotní tvůrci GDPR dosud nevydali jednoznačné a kompletní prováděcí předpisy či výkladová stanoviska. Pokud se tedy budou měnit výkladová hlediska, bude se průběžně doplňovat i tato publikace.

Věříme, že tato publikace bude pro Vás pomocníkem a zbaví Vás alespoň těch největších obav ještě před účinností GDPR!

2. Pro koho je publikace určena

Primárně byla publikace zpracována jako metodický materiál pro přímo řízené organizace MZ ČR a ÚZIS ČR. Jak bylo řečeno výše, materiál by měl sloužit pro seznámení se s GDPR a pro základní orientaci v nových právech subjektu údajů, v nových povinnostech správců a zpracovatelů a ukázat na jednu z možných cest konkrétních implementačních kroků GDPR.

Okruhem adresátů jsou zejména velké nemocnice či větší organizační celky. Pro menší organizační celky či ambulantní sféru lze jednotlivé kapitoly doporučení použít přiměřeně. V některých místech je v publikaci uveden odkaz či doporučení, konkrétně pro menší poskytovatele zdravotních služeb, resp. organizační celky či ambulantní sféru.

V současné době je finalizován materiál zohledňující odpovědi na základní otázky menších ordinací praktických lékařů či ambulantních specialistů. Bude zveřejněn v elektronické podobě na webových stránkách MZ ČR a ÚZIS ČR.

3. Co to je GDPR

3.1. 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.

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

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 jsou pak uplatňovány ve vztahu ke každému takovému subjektu.

3.2. 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 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 resort 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 a podmínkách jejich poskytování (zákon o specifických zdravotních službách) ve znění pozdějších předpisů
  Konkrétní právní úprava práv a povinnosti pacientů a poskytovatelů zdravotních služeb a práva a povinnosti 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, 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, 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 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.

3.3. V jakém stavu je GDPR

GDPR je spíše evolucí v ochraně osobních údajů, nikoli její revolucí, jak je často některými autory prezentována.

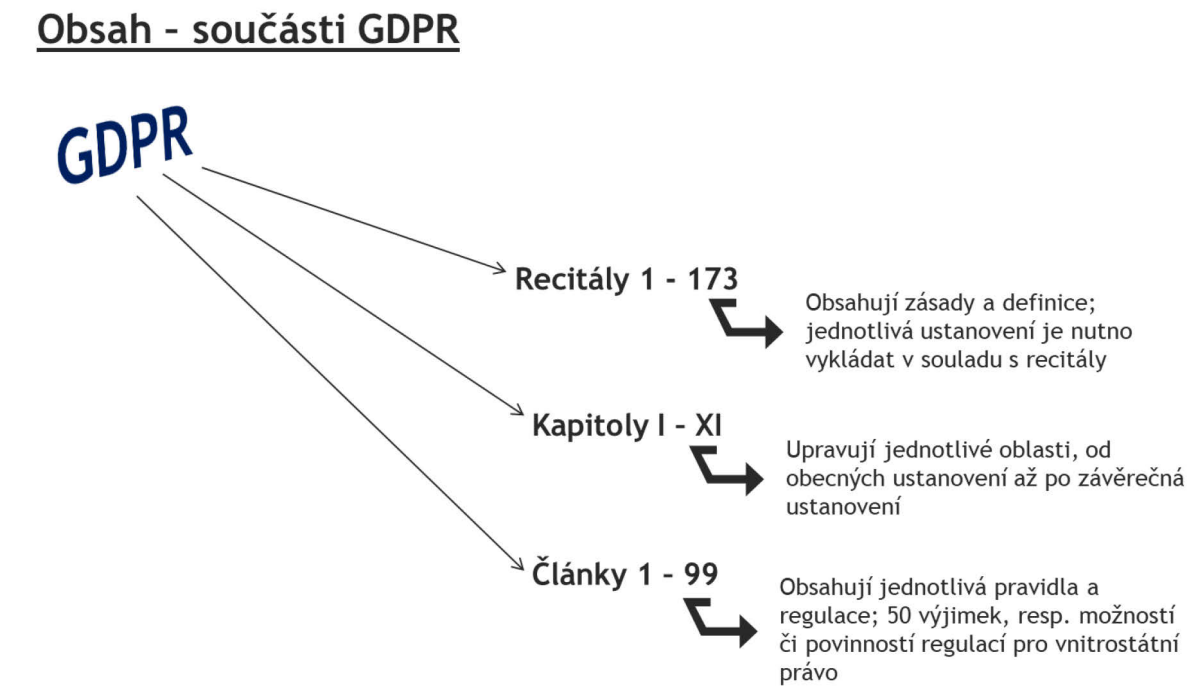
Jeho výhodou je explicitní stanovení práv subjektu údajů, nastavení povinností správců a zpracovatelů či dozorových úřadů, vymezení povinností ve vztahu k zahraničí a mezinárodním organizacím.

GDPR je normou velmi obecnou. Je postaveno na modelu performance-based regulace, který počítá s tím, že jsou právní úpravou jen velmi obecně stanoveny povinnosti a každý subjekt si sám určuje způsoby, jakým tyto povinnosti plní. Jedinou nevýhodou je menší předvídatelnost a menší počáteční jistota - naopak to má ale řadu výhod. Předně si regulované subjekty mohou samy vymyslet řešení na míru vlastním potřebám. Jak již bylo řečeno výše, i samotní tvůrci nevydali zcela jasná výkladová stanoviska pro některé články, a proto na úrovni EU pracovní skupina WP 29 vydala již několik výkladových stanovisek k jednotlivým článkům GDPR a vodítko pro posouzení vlivu na ochranu osobních údajů. Jedná se o pracovní skupinu, která byla vytvořena na základě článku 29. směrnice 95/46/EC. Je evropským poradním orgánem na ochranu údajů a soukromí. S účinností GDPR se z tohoto tělesa stane Evropský sbor pro ochranu osobních údajů (EPDB). Připomínky k nejasnostem některých ustanovení GDPR jsou extenzivně debatovány v řadě významných evropských projektů a platforem a z těchto důvodů můžeme v budoucnosti jistě očekávat další zpřesňování výkladu některých ustanovení.

3.4. Struktura GDPR

GDPR představuje ucelenou soustavu ustanovení, kterou je nutné vykládat ve vzájemných souvislostech. Je to ucelená soustava závazných pravidel. Kapitoly I–IX obsahují ve svých 99 článcích konkrétní výčet pravidel pro jednotlivé subjekty nakládající s osobními údaji a rozsah práv pro subjekt údajů samotný. Úvodní ustanovení – tzv. recitály, napomáhají porozumění textu a výkladu jednotlivých ustanovení obecného nařízení.

K těmto jednotlivým regulacím musíme přidat ještě výkladová stanoviska pracovní skupiny WP 29, která byla popsána v předchozím bodě a bude jim věnována i část následujících kapitol.



GDPR je ucelená soustava závazných pravidel, k nimž publikuje výkladové materiály pracovní skupina WP 29 (vytvořena na základě článku 29. směrnice 95/46/EC). WP 29 vydala v současné době již několik výkladových stanovisek k jednotlivým článkům GDPR a vodítko pro posouzení vlivu na ochranu osobních údajů.

4. Jaké změny s sebou GDPR přináší. Lze se vyhnout GDPR?

Odpověď je velmi jednoduchá. Vyhnout se GDPR nelze. Lze se na něj pouze připravit. Změny, které GDPR přináší, jsou shrnuty v následujících podkapitolách.

4.1. Rozšířená práva pro subjekt osobních údajů

Pro subjekt údajů jsou v GDPR kodifikována práva, která jsou již v současné době upravena v právních předpisech ČR, avšak některá jsou zcela nová. Konkrétně se jedná o následující práva subjektu osobních údajů:

Článek	Obsah	Dopad
čl. 12	**právo subjektu údajů na transparentní, srozumitelné a snadno přístupným způsobem dostupné informace o osobních údajích, které byly získány se souhlasem i bez souhlasu**	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.
čl. 13	**právo subjektu údajů na informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů**	Správce musí 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)
čl. 14	**právo subjektu údajů na informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů**	Správce je povinen tyto informace poskytnout. Neplatí v případě, že: ➢ subjekt údajů údaje má, ➢ poskytnutí údajů by vyžadovalo nepřiměřené úsilí (zejména pro archivaci ve veřejném zájmu, pro vědecký a historický výzkum a pro statistické účely), ➢ získávání je stanoveno právem členského státu nebo právem EU, ➢ osobní údaje musí s ohledem na povinnost zachovávat mlčenlivost zůstat důvěrnými.

Článek	Obsah	Dopad
čl. 15	**právo subjektu údajů na přístup k osobním údajům**	Správce vydá potvrzení o tom, zda osobní údaje, které se týkají daného subjektu údajů, jsou, či nejsou zpracovávány. Správce poskytne kopii zpracovávaných osobních údajů (za další kopie na žádost subjektu údajů může správce účtovat přiměřený poplatek na základě administrativních nákladů); jestliže subjekt údajů podává žádost v elektronické formě, informace jsou poskytovány v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.
čl. 16	**právo subjektu údajů na opravu** **právo subjektu údajů na doplnění neúplných osobních údajů**	Správce bez zbytečného odkladu opraví nepřesné osobní údaje, které se týkají subjektu údajů.
čl. 17 odst. 1	**právo na výmaz („právo být zapomenut“)**	Správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů: a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovávány; b) subjekt údajů odvolá souhlas, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) zpracovány, a neexistuje žádný další právní důvod pro zpracování; c) subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 1 a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 2; d) osobní údaje byly zpracovány protiprávně; e) osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na správce vztahuje; f) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1.

Článek	Obsah	Dopad
čl. 18	**právo na omezení zpracování**	Správce omezí zpracování, v kterémkoli z těchto případů: a) subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit; b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití; c) správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků; d) subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.
čl. 19	**oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování**	Správce oznamuje jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování provedené v souladu s čl. 16, čl. 17 odst. 1 a čl. 18, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Správce informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje.
čl. 20	**právo na přenositelnost údajů**	Správce má povinnost předat osobní údaje druhému správci (za předpokladu technické proveditelnosti) a pouze za kumulativního splnění 2 podmínek: ➢ zpracování založeno na souhlasu nebo smlouvě a ➢ jedná se o automatizované zpracování.
čl. 21	**právo vznést námitku** proti zpracování osobních údajů, které se subjektu údajů týkají, na základě čl. 6 odst. 1 písm. e) nebo písm. f), včetně profilování založeného na těchto ustanoveních	Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

Článek	Obsah	Dopad
čl. 22	**právo na to, aby subjekt údajů nebyl předmětem automatizovaného rozhodování, vč. profilování**	Správce nesmí provádět výhradně automatizované individuální rozhodování, vč. profilování, s následujícími výjimkami: ➢ je zákonem stanoveno, ➢ je založeno na souhlasu subjektu, ➢ je nezbytné pro uzavření smlouvy nebo jejího plnění se subjektem.
čl. 77	**právo podat stížnost u dozorového úřadu**	Správce se stává součástí, resp. předmětem šetření.
čl. 78	**právo na účinnou soudní ochranu vůči dozorovému úřadu**	
čl. 79	**právo na účinnou soudní ochranu vůči správci nebo zpracovateli**	Správce se stává stranou soudního sporu.
čl. 80	**právo na to být zastoupen neziskovým subjektem, organizací nebo sdružením**	Povinnost správce jednat s takovýmto subjektem, který zastupuje subjekt údajů, např. v případě podání stížnosti.
čl. 82	**právo na náhradu újmy**	Vznikne-li subjektu údajů újma, ať již hmotná, či nehmotná, má správce povinnost tuto újmu nahradit.

V příloze č. 1 naleznete tabulku názorně zobrazující vazbu práv subjektu údajů na právní titul jejich zpracování.

4.2. Nové povinnosti správců

4.2.1. Soulad se zásadami GDPR

Správce je povinen zpracovávat osobní údaje **v souladu se zásadami GDPR**, kterými jsou:

- **Zákonnost, korektnost a transparentnost**
  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.

- **Účelové omezení** – zpracování je možné pouze za určitým účelem: osobní údaje smějí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely.
- **Minimalizace údajů** – ve vazbě na účel jejich zpracování, přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.
- **Přesnost a v případě potřeby aktualizace** – přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny.
- **Omezení uložení** – pouze po dobu do naplnění účelu, pro který byly osobní údaje shromažďovány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, a to za předpokladu provedení příslušných technických a organizačních opatření.
- **Integrita a důvěrnost** – je nutné přijmout technická a organizační opatření odpovídající předpokládanému riziku; osobní údaje tedy musí být zpracovávány způsobem, který zajistí jejich náležité zabezpečení, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.
- **Odpovědnost správce** – správce musí být schopen dodržení souladu doložit.

4.2.2. Zpracování na základě souhlasu subjektu údajů

V případě **zpracování na základě souhlasu subjektu údajů** GDPR stanoví minimální požadavky na informovaný souhlas:

- totožnost správce,
- všechny účely zpracování,
- možnost odmítnout nebo odvolat souhlas.

Definice souhlasu je uvedena v čl. 4 bod 11) „… ‚souhlasem' subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;…".

Pokud se týká rovněž jiných skutečností, musí být souhlas jasně odlišitelný. Jakákoli část tohoto prohlášení, která představuje porušení GDPR, není závazná. Souhlas musí být výslovným. Mlčení, předem zaškrtnutá políčka nebo nečinnost nejsou považovány za souhlas.

4.2.3. Odpovědnost správce

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.

4.2.4. Záměrná a standardní ochrana

Jednou z možností, jak je možné doložit plnění výše uvedených povinností, je dodržování schválených kodexů chování či mechanismů pro vydání osvědčení. Správce je povinen **provádět záměrnou a standardní ochranu osobních údajů**. Je povinen zavést vhodná technická a organizační opatření. Tato opatření zavádí v době:

- určení prostředků pro zpracování,
- zpracování samotného.

Jako příklad takových opatření je uvedena pseudonymizace osobních údajů. Dalším prostředkem minimalizace údajů je zavedení vhodných technických a organizačních opatření k zajištění stavu, kdy jsou zpracovávány pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká:

- množství shromážděných osobních údajů,
- rozsahu jejich zpracování,
- doby jejich uložení a jejich dostupnosti.

Tato opatření zejména zajistí, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob.

4.2.5. Zástupce správce

Správce či zpracovatel neusazený v EU si může jmenovat svého zástupce v EU usazeného. GDPR definuje „zástupcem" jakoukoliv fyzickou nebo právnickou osobu usazenou v EU, která je správcem nebo zpracovatelem určena písemně podle článku 27 k tomu, aby správce nebo zpracovatele zastupovala, pokud jde o příslušné povinnosti správce nebo zpracovatele ve smyslu GDPR.

Tím, že správce nebo zpracovatel jmenuje svého zástupce, však nejsou dotčeny právní kroky, které by mohly být zahájeny proti správci nebo zpracovateli samotnému.

4.2.6. Společní správci

Pokud účely a prostředky zpracování stanoví společně dva nebo více správců, jsou **společnými správci**. Společní správci mezi sebou transparentním ujednáním 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.

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. Bez ohledu na podmínky ujednání může subjekt údajů vykonávat svá práva podle tohoto nařízení u každého ze správců; i vůči každému z nich je nutné zavést legislativní nebo smluvní transparentní ujednání. Transparentním ujednáním je myšleno smluvní ujednání.

4.2.7. Řetězení zpracování

GDPR připouští **řetězení zpracování.** Správce využije pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů.

Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího **konkrétního** nebo **obecného** písemného povolení správce. 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.

4.2.8. Smlouva o zpracování

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. 2 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.

4.2.9. Záznamy o činnostech zpracování

Správce i zpracovatel mají **povinnost vést záznamy o činnostech zpracování**. Záznamy o činnostech zpracování mohou sloužit k prokázání souladu s GDPR.

Každý správce a jeho případný zástupce je povinen vést záznamy o činnostech zpracování. Tyto záznamy obsahují všechny tyto informace:

- jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;
- účely zpracování;
- popis kategorií subjektů údajů a kategorií osobních údajů;
- kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk;
- je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;
- je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.

Každý zpracovatel a jeho případný zástupce vede záznamy o činnostech zpracování v následujícím rozsahu:

- 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;
- kategorie zpracování prováděného pro každého ze správců;
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk;
- je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.

4.2.10. Posouzení vlivu na ochranu osobních údajů

Správce je dále povinen provést **posouzení vlivu na ochranu osobních údajů,** pokud:

- je zaváděna nová technologie,
- dochází k výrazným změnám,
- jsou zcela nového druhu a správce neprovedl posouzení vlivu na ochranu osobních údajů.

Pracovní skupina WP 29 vydala k této problematice vodítka obsahující celkem 10 charakteristik zpracování osobních údajů; při splnění 2 z nich je posouzení vlivu nezbytné. Pro resort zdravotnictví platí v tomto ustanovení výjimka pro ambulantní sféru, resp. v případech poskytovatelů poskytujících primární ambulantní péči není nutné zpracovávat posouzení vlivu na ochranu osobních údajů.

Posouzení vlivu na ochranu osobních údajů je nutné zejména v těchto případech:

a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;
b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 (zvláštní kategorie osobních údajů) nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; nebo
c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

Dozorový úřad sestaví seznam zpracování, kde je posouzení vlivu na ochranu osobních údajů povinné a může sestavit seznam zpracování, kde posouzení vlivu není povinné.

Minimální struktura posouzení vlivu na ochranu osobních údajů:

- systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce;
- posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;
- posouzení rizik pro práva a svobody subjektů údajů a
- plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

Výjimka z povinnosti zpracovat posouzení vlivu – čl. 35 odst. 10 za předpokladu, pokud je zpracování nezbytné:

- pro plnění právní povinnosti,
- pro plnění úkolu prováděného ve veřejném zájmu,
- a má právní základ v právu Unie nebo členského státu, které se na správce vztahuje,
- právo upravuje konkrétní operaci nebo soubor operací zpracování,
- posouzení vlivu na ochranu osobních údajů bylo již provedeno jakožto součást obecného posouzení dopadů v souvislosti s přijetím uvedeného právního základu.

4.2.11. Spolupráce s dozorovým úřadem a předchozí konzultace

Správce a zpracovatel na požádání spolupracují s dozorovým úřadem.

Správce je povinen si vyžádat předchozí konzultaci u dozorového úřadu za předpokladu, že riziko vlivu na ochranu osobních údajů zůstává vysoké v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika, resp. pokud uvedené skutečnosti vyplývají z posouzení vlivu na ochranu osobních údajů.

4.2.12. Zabezpečení osobních údajů

Správce je povinen zabezpečit zpracování osobních údajů a ohlašovat případy porušení osobních údajů ať již dozorovému úřadu, tak i subjektu údajů.

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;

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.

4.2.13. Ohlašování porušení zabezpečení

Ohlašování porušení zabezpečení dozorovému úřadu se provádí pouze v případě, pokud takové porušení znamená riziko pro práva a svobody fyzických osob. Lhůta pro ohlášení porušení zabezpečení osobních údajů je bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm správce dozvěděl. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění. Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu správci.

Oznamování případů porušení zabezpečení subjektu údajů se provádí pouze, pokud je pravděpodobné, že určitý případ bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Lhůta pro toto oznamování je bez zbytečného odkladu. Oznámení se nevyžaduje, je-li splněna kterákoli z těchto podmínek:

a) správce zavedl náležitá opatření, která byla použita u osobních údajů dotčených porušením, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;
b) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví;
c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Jestliže správce dotčenému subjektu údajů porušení ještě neoznámil, může dozorový úřad po posouzení požadovat,

a) aby tak učinil,
b) nebo může rozhodnout, že je splněna některá z podmínek uvedených v odstavci předcházejícím.

4.2.14. Pověřenec pro ochranu osobních údajů

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.

Jak vyplývá z výše uvedeného, v případě zpracování zvláštní kategorie osobních údajů (citlivé osobní údaje) je nutno jmenovat pověřence pro ochranu osobních údajů.

Je-li správce nebo zpracovatel orgánem veřejné moci či veřejným subjektem, může být s přihlédnutím k jejich organizační struktuře a velikosti jmenován jediný pověřenec pro ochranu osobních údajů pro několik takových orgánů nebo subjektů.

Skupina podniků může jmenovat jediného pověřence pro ochranu osobních údajů, pokud je snadno dosažitelný z každého podniku.

Pověřenec pro ochranu osobních údajů:

- musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly jemu stanovené na základě GDPR,
- může být pracovníkem správce či zpracovatele, nebo může úkoly plnit na základě smlouvy o poskytování služeb.

Správce nebo zpracovatel zveřejní kontaktní údaje pověřence pro ochranu osobních údajů a sdělí je dozorovému úřadu. Postavení pověřence pro ochranu osobních údajů:

- Je náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů.
- Jsou mu poskytovány zdroje nezbytné k plnění těchto úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí.
- Nedostává žádné pokyny týkající se výkonu těchto úkolů. V souvislosti s plněním svých úkolů není správcem nebo zpracovatelem propuštěn ani sankcionován.
- Je přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele.
- Subjekty údajů se na něj mohou obracet ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle GDPR.
- Je v souvislosti s výkonem svých úkolů vázán tajemstvím nebo důvěrností, v souladu s právem Unie nebo členského státu.
- Může plnit i jiné úkoly a povinnosti. Správce nebo zpracovatel zajistí, aby žádné z těchto úkolů a povinností nevedly ke střetu zájmů.

Úkoly pověřence pro ochranu osobních údajů:

- poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech v oblasti ochrany údajů;
- monitorování souladu s tímto nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;
- poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování;
- spolupráce s dozorovým úřadem;
- působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace, a případně vedení konzultací v jakékoli jiné věci.

Závěrem je možné shrnout, že pověřenec může být zaměstnancem, stejně tak může být zajištěn externím dodavatelem. Je potřeba dále zajistit, aby byl ošetřen střet zájmů. Není možné, aby funkci pověřence pro ochranu údajů zajišťoval zaměstnanec či pracovník, který provádí nebo se podílí na provádění technickoorganizačních opatření k zajištění ochrany osobních údajů nebo ze své pozice rozhoduje o účelu a prostředcích zpracování osobních údajů, jak vyplývá, mimo jiné, z Metodického doporučení k organizačně technickému zabezpečení funkce pověřence pro ochranu osobních údajů v podmínkách obcí vydaného MV ČR ze dne 10. 8. 2017. Dále je důležité, aby DPO měl přímý přístup jak k vrcholovému managementu správce, tak i k relevantním informacím.

4.2.15. Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím

V GDPR je stanovena následující obecná zásada pro předávání osobních údajů do třetích zemí nebo mezinárodním organizacím:

K jakémukoli předání osobních údajů může dojít pouze tehdy, splní-li správce a zpracovatel podmínky explicitně stanovené v kapitole GDPR, a to včetně podmínek pro další předávání osobních údajů z dané třetí země nebo mezinárodní organizace do jiné třetí země nebo jiné mezinárodní organizaci.

Veškerá ustanovení se použijí s cílem zajistit, aby úroveň ochrany fyzických osob zaručená GDPR nebyla znehodnocena.

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.

Předání založené na rozhodnutí Komise o odpovídající ochraně

Předávání se může uskutečnit, jestliže Komise rozhodla, že tato třetí země, určité území nebo jedno či více konkrétních odvětví v této třetí zemi, nebo tato mezinárodní organizace zajišťují odpovídající úroveň ochrany.

Takovéto předání nevyžaduje žádné zvláštní povolení.

Komise zveřejní v Úředním věstníku Evropské unie a na svých internetových stránkách seznam třetích zemí, území a konkrétních odvětví ve třetích zemích a mezinárodních organizací, v nichž podle jejího rozhodnutí odpovídající úroveň ochrany je, nebo naopak již není zajištěna.

Předávání založené na vhodných zárukách

Neexistuje rozhodnutí Komise podle předchozího odstavce.

Správce nebo zpracovatel mohou předat osobní údaje do třetí země nebo mezinárodní organizaci, pouze pokud správce nebo zpracovatel:

a) poskytl vhodné záruky,
b) za podmínky, že jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana subjektů údajů.

Vhodné záruky mohou být stanoveny bez zvláštního povolení dozorového úřadu, pomocí:

a) právně závazného a vymahatelného nástroje mezi orgány veřejné moci nebo veřejnými subjekty;
b) závazných podnikových pravidel;
c) standardních doložek o ochraně osobních údajů přijatých Komisí;
d) standardních doložek o ochraně údajů přijatých dozorovým úřadem a schválených Komisí;
e) schváleného kodexu chování spolu se závaznými a vymahatelnými závazky správce nebo zpracovatele ve třetí zemi uplatňovat vhodné záruky, a to i ohledně práv subjektů údajů;

f) schváleného mechanismu pro vydání osvědčení spolu se závaznými a vymahatelnými závazky správce nebo zpracovatele ve třetí zemi uplatňovat vhodné záruky, a to i ohledně práv subjektů údajů.
g) s výhradou povolení dozorového úřadu, pomocí:
h) smluvních doložek mezi správcem nebo zpracovatelem a správcem, zpracovatelem nebo příjemcem osobních údajů ve třetí zemi nebo v mezinárodní organizaci;
i) ustanovení určených k vložení do správních ujednání mezi orgány veřejné moci nebo veřejnými subjekty, která zahrnují vymahatelná a účinná práva subjektu údajů.

Závazná podniková pravidla

Příslušný dozorový úřad schvaluje v souladu s mechanismem jednotnosti závazná podniková pravidla za předpokladu, že:

a) jsou právně závazná a platná pro všechny a prosazovaná všemi dotčenými členy skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost, včetně jejich zaměstnanců;
b) subjektům údajů výslovně přiznávají vymahatelná práva v souvislosti se zpracováním jejich osobních údajů;
c) splňují minimální obsah.

Podniková pravidla zahrnují následující minimální obsah podnikových pravidel

a) strukturu a kontaktní údaje skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a každého z jejích členů;
b) předání údajů nebo soubor předání, včetně kategorií osobních údajů, typu zpracování a jeho účelů, typu dotčených subjektů údajů a určení dané třetí země nebo daných třetích zemí;
c) svoji právně závaznou povahu, a to interně i externě;
d) použití obecných zásad pro ochranu údajů, zejména účelové omezení, minimalizaci údajů, omezenou dobu uložení, kvalitu údajů, záměrnou a standardní ochranu osobních údajů, právní základ pro zpracování, zpracování zvláštních kategorií osobních údajů; opatření k zajištění zabezpečení údajů a požadavky ohledně dalšího předávání subjektům, které podnikovými pravidly nejsou vázány;
e) práva subjektů údajů v souvislosti se zpracováním jejich osobních údajů a prostředky jejich výkonu, včetně práva nebýt předmětem rozhodnutí založených výhradně na automatizovaném zpracování, včetně profilování v souladu s článkem 22, práva podat stížnost u příslušného dozorového úřadu a příslušných soudů členských států v souladu s článkem 79, právní ochrany a případně i práva na odškodnění v případě porušení závazných podnikových pravidel;
f) přijetí odpovědnosti správcem nebo zpracovatelem usazeným na území některého členského státu za jakékoli porušení závazných podnikových pravidel kterýmkoli dotčeným členem neusazeným v Unii; správce nebo zpracovatel se může této odpovědnosti zcela nebo zčásti zprostit, pouze pokud prokáže, že za okolnost, jež vedla ke vzniku škody, není daný člen odpovědný;

g) způsob poskytování informací o závazných podnikových pravidlech, zejména o ustanoveních uvedených v písmenech d), e) a f) tohoto odstavce, subjektům údajů, vedle informací uvedených v článcích 13 a 14;
h) úkoly všech pověřenců pro ochranu osobních údajů jmenovaných v souladu s článkem 37, nebo jakékoli jiné osoby či subjektu pověřeného monitorováním souladu se závaznými podnikovými pravidly v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a sledování školení a vyřizování stížností;
i) postupy pro vyřizování stížností;
j) mechanismy, které mají v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost zajistit ověřování souladu se závaznými podnikovými pravidly. Tyto mechanismy zahrnují audity ochrany údajů a metody zajištění opravných opatření pro ochranu práv subjektu údajů. Výsledky takového ověření by měly být oznámeny osobě nebo subjektu uvedenému v písmenu h) a radě řídicího podniku skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a na požádání by měly být zpřístupněny příslušnému dozorovému úřadu;
k) mechanismy pro podávání zpráv a pro zaznamenávání změn pravidel a hlášení těchto změn dozorovému úřadu;
l) mechanismus spolupráce s dozorovým úřadem, který zajistí dodržování pravidel každým členem skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost, zejména zpřístupňování výsledků ověřování opatření uvedených v písmenu j) dozorovému úřadu;
m) mechanismy pro podávání zpráv příslušnému dozorovému úřadu o právních požadavcích, kterým je člen skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost podřízen ve třetí zemi a které mohou mít podstatný negativní účinek na záruky poskytované závaznými podnikovými pravidly; a
n) vhodnou odbornou přípravu v oblasti ochrany údajů pro pracovníky, kteří mají k osobním údajům trvalý nebo pravidelný přístup.

Může existovat i situace, kdy není možné předání osobních údajů do třetích zemí nebo mezinárodním organizacím, založená na rozhodnutí Komise či na vhodných zárukách. V tom případě správce informuje subjekt údajů o předání a předání je možné při splnění jedné z následujících podmínek:

a) daný subjekt údajů byl informován o možných rizicích, která pro něj v důsledku absence rozhodnutí o odpovídající ochraně a vhodných záruk vyplývají, a následně k navrhovanému předání vydal svůj výslovný souhlas;
b) předání je nezbytné pro splnění smlouvy mezi subjektem údajů a správcem nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost subjektu údajů;
c) předání je nezbytné pro uzavření nebo splnění smlouvy, která byla uzavřena v zájmu subjektu údajů mezi správcem a jinou fyzickou nebo právnickou osobou;
d) předání je nezbytné z důležitých důvodů veřejného zájmu;
e) předání je nezbytné pro určení, výkon nebo obhajobu právních nároků;
f) předání je nezbytné k ochraně životně důležitých zájmů subjektu údajů nebo jiných osob v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit svůj souhlas;

g) k předání dochází z rejstříku, který je na základě práva Unie nebo členského státu určen pro informování veřejnosti a je přístupný k nahlížení veřejnosti obecně nebo jakékoli osobě, která může prokázat oprávněný zájem, avšak pouze, pokud jsou v daném případě splněny podmínky pro nahlížení stanovené právem Unie nebo členského státu.

Netýká se činnosti prováděné orgány veřejné moci při výkonu jejich úředních pravomocí.

Závěrem je možné říci, že předání do třetích zemí či mezinárodním organizacím je možné pouze v případech, kdy jsou splněna explicitně nastavená pravidla GDPR. V této souvislosti uvádíme ještě definici přeshraničního zpracování (nejedná se o předání do třetích zemí).

„Přeshraničním zpracováním" je buď:

a) zpracování osobních údajů, které probíhá v souvislosti s činnostmi provozoven ve více než jednom členském státě správce či zpracovatele v Unii, je-li tento správce či zpracovatel usazen ve více než jednom členském státě;

nebo

b) zpracování osobních údajů, které probíhá v souvislosti s činnostmi jediné provozovny správce či zpracovatele v Unii, ale kterým jsou nebo pravděpodobně budou podstatně dotčeny subjekty údajů ve více než jednom členském státě.

4.2.16. Povinnost úhrady správních pokut, resp. sankcí

V případě porušení povinností je možné uložit správci sankce, resp. správní pokuty.

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, pouze však orgánům veřejné moci a veřejným subjektům.

4.2.17. Další povinnosti

Další povinnosti správce korespondují s novými právy subjektu údajů – viz předcházející oddíl.

5. Kdo bude dodržování GDPR kontrolovat?

Dodržování GDPR a plnění všech povinností v něm kodifikovaných je oprávněn kontrolovat dozorový úřad. Dozorové úřady se člení na dozorový úřad členského státu, resp. členských států – vnitrostátní dozorový úřad a dále Evropský sbor pro ochranu osobních údajů.

5.1. Vnitrostátní dozorový úřad v ČR

Kontrola dodržování GDPR je v případě ČR v rukou Úřadu pro ochranu osobních údajů (ÚOOÚ).

Základní charakteristikou dozorového úřadu je jeho nezávislost a spolupráce s ostatními dozorovými úřady v EU.

Jeden z nových úkolů, které ÚOOÚ dostává, s dopadem i do resortu zdravotnictví, je následující: „Dozorový úřad **sestaví** seznam zpracování, kde je posouzení vlivu na ochranu osobních údajů povinné a **může** sestavit seznam zpracování, kde posouzení vlivu není povinné.“

Úkoly dozorového úřadu jsou následující:

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 GDPR;
e) na požádání poskytuje všem subjektům údajů informace ohledně výkonu jejich práv podle GDPR 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, 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;
k) připravuje a udržuje seznam v souvislosti s požadavkem provádět posouzení vlivu na ochranu osobních údajů;
l) poskytuje poradenství o operacích zpracování;

m) podporuje vypracování kodexů chování, vydává stanoviska a schvaluje takové kodexy chování, které poskytují dostatečné záruky;
n) vybízí k zavedení mechanismů pro vydávání osvědčení o ochraně údajů a pečetí a známek dokládajících ochranu údajů a schvaluje kritéria pro vydávání osvědčení;
o) případně provádí pravidelný přezkum vydaných osvědčení;
p) navrhuje a zveřejňuje kritéria pro schvalování subjektu pro monitorování kodexů chování a subjektu pro vydávání osvědčení;
q) provádí schvalování subjektu pro monitorování kodexů chování a subjektu pro vydávání osvědčení;
r) schvaluje smluvní doložky a ustanovení;
s) schvaluje závazná podniková pravidla;
t) přispívá k činnostem sboru;
u) vede interní záznamy o porušeních tohoto nařízení a o opatřeních přijatých; a
v) plní veškeré další úkoly související s ochranou osobních údajů.

Každý dozorový úřad má následující pravomoci vyšetřovací, nápravné a povolovací a nápravné.

1. Každý dozorový úřad má všechny tyto vyšetřovací pravomoci:

a) nařídit správci a zpracovateli, případně zástupci správce nebo zpracovatele, aby mu poskytli veškeré informace, které potřebuje k plnění svých úkolů;
b) provádět vyšetřování formou auditů ochrany údajů;
c) provádět přezkum vydaných osvědčení;
d) ohlásit správci nebo zpracovateli údajné porušení tohoto nařízení;
e) získat od správce a zpracovatele přístup ke všem osobním údajům a ke všem informacím, které potřebuje k výkonu svých úkolů;
f) získat přístup do všech prostor, v nichž správce a zpracovatel působí, včetně přístupu k veškerému zařízení a prostředkům určeným ke zpracování údajů, v souladu s procesním právem Unie nebo členského státu.

2. Každý dozorový úřad má všechny tyto nápravné pravomoci:

a) upozornit správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují toto nařízení;
b) udělit napomenutí správci či zpracovateli, jehož operace zpracování porušily toto nařízení;
c) nařídit správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv podle tohoto nařízení;
d) nařídit správci či zpracovateli, aby uvedl operace zpracování do souladu s tímto nařízením, a to případně předepsaným způsobem a ve stanovené lhůtě;
e) nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů;
f) uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu;
g) nařídit opravu či výmaz osobních údajů nebo omezení zpracování podle článků 16, 17 a 18 a ohlašování takových opatření příjemcům, jimž byly osobní údaje zpřístupněny podle čl. 17 odst. 2 a článku 19;
h) odebrat osvědčení nebo nařídit, aby subjekt pro vydávání osvědčení odebral osvědčení vydané podle článků 42 a 43, nebo aby osvědčení nevydal, pokud požadavky na osvědčení plněny nejsou nebo již přestaly být plněny;

i) uložit správní pokutu podle článku 83 vedle či namísto opatření uvedených v tomto odstavci, podle okolností každého jednotlivého případu;
j) nařídit přerušení toků údajů příjemci ve třetí zemi nebo toků údajů mezinárodní organizaci.

3. Každý dozorový úřad má všechny tyto povolovací a poradní pravomoci:

a) poskytovat poradenství správci v souladu s postupem předchozí konzultace;
b) z vlastního podnětu nebo na požádání vydávat stanoviska určená vnitrostátnímu parlamentu, vládě členského státu nebo v souladu s právem členského státu dalším institucím a subjektům, jakož i veřejnosti, ohledně veškerých otázek souvisejících s ochranou osobních údajů;
c) povolovat zpracování, pokud právo členského státu takové předchozí povolení vyžaduje;
d) vydávat stanoviska a schvalovat návrhy kodexů chování;
e) akreditovat subjekty pro vydávání osvědčení;
f) vydávat osvědčení a schvalovat kritéria pro vydávání osvědčení;
g) přijímat standardní doložky o ochraně údajů;
h) povolovat smluvní doložky;
i) povolovat správní ujednání;
j) schvalovat závazná podniková pravidla.

Závěrem je nutné doporučit sledování webových stránek ÚOOÚ (www.uoou.cz), kde naleznete nejen cenné rady, ale i výkladová stanoviska skupiny WP 29. Tato jsou nejprve publikována aktuálně v jazyce anglickém a s menším časovým odstupem jsou přeložena do češtiny.

5.2. Evropský sbor pro ochranu osobních údajů

Zřizuje se dále Evropský sbor pro ochranu osobních údajů. Sbor tvoří vedoucí jednoho dozorového úřadu z každého členského státu a evropský inspektor ochrany údajů nebo jejich zástupci. Jedná se o evropský orgán, který bude zajišťovat jednotnou aplikaci GDPR v rámci EU. S účinností GDPR vznikne ze stávající pracovní skupiny WP 29.

Sbor tvoří vedoucí jednoho dozorového úřadu z každého členského státu a evropský inspektor ochrany údajů nebo jejich zástupci.

Sbor z vlastního podnětu nebo případně na žádost Komise zejména:

a) monitoruje a zajišťuje řádné uplatňování tohoto nařízení v případech uvedených v článcích 64 a 65, aniž jsou dotčeny úkoly vnitrostátních dozorových úřadů;
b) poskytuje poradenství Komisi ve veškerých záležitostech souvisejících s ochranou osobních údajů v Unii včetně jakýchkoli navrhovaných změn tohoto nařízení;
c) poskytuje poradenství Komisi ohledně formy a postupů výměny informací mezi správci, zpracovateli a dozorovými úřady pro závazná podniková pravidla;
d) vydává pokyny, doporučení a osvědčené postupy týkající se postupů pro výmaz odkazů, kopií nebo replikací osobních údajů z veřejně dostupných komunikačních služeb, jak je uvedeno v čl. 17 odst. 2;
e) prošetřuje z vlastního podnětu, na žádost některého ze svých členů nebo na žádost Komise veškeré otázky týkající se uplatňování tohoto nařízení a vydává pokyny, doporučení a osvědčené postupy, aby podporoval soudržné uplatňování tohoto nařízení;

f) vydává pokyny, doporučení a osvědčené postupy v souladu s písmenem e) tohoto odstavce za účelem dalšího vymezení kritérií a podmínek, které mají platit pro rozhodnutí založená na profilování podle čl. 22 odst. 2;

g) vydává pokyny, doporučení a osvědčené postupy v souladu s písmenem e) tohoto odstavce, jak zjistit případy porušení zabezpečení osobních údajů a jak určit zbytečný odklad podle čl. 33 odst. 1 a 2 a konkrétní okolnosti, za nichž jsou správce a zpracovatel povinni porušení ohlásit;

h) vydává pokyny, doporučení a osvědčené postupy v souladu s písmenem b) tohoto odstavce, pokud jde o okolnosti, za jakých je pravděpodobné, že porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, jak je uvedeno v čl. 34 odst. 1;

i) vydává pokyny, doporučení a osvědčené postupy v souladu s písmenem e) tohoto odstavce za účelem dalšího vymezení kritérií a požadavků pro předávání osobních údajů na základě závazných podnikových pravidel, kterými se řídí správci, a závazných podnikových pravidel, kterými se řídí zpracovatelé, a dalších požadavků potřebných k zajištění ochrany osobních údajů dotčených subjektů údajů uvedených v článku 47;

j) vydává pokyny, doporučení a osvědčené postupy v souladu s písmenem e) tohoto odstavce za účelem dalšího vymezení kritérií a požadavků pro předávání osobních údajů na základě čl. 49 odst. 1;

k) vypracovává pokyny pro dozorové úřady o uplatňování opatření uvedených v čl. 58 odst. 1, 2 a 3 a stanoví správní pokuty podle článku 83;

l) přezkoumává praktické uplatňování pokynů, doporučení a osvědčených postupů uvedených v písmenech e) a f);

m) vydává pokyny, doporučení a osvědčené postupy v souladu s písmenem e) tohoto odstavce pro zavedení společných postupů pro podávání zpráv fyzickými osobami v případě porušení tohoto nařízení podle čl. 54 odst. 2;

n) podporuje vypracování kodexů chování a zavedení mechanismů pro vydávání osvědčení o ochraně údajů a zavedení pečetí a známek dokládajících ochranu údajů podle článků 40 a 42;

o) provádí akreditaci subjektů pro vydávání osvědčení a její pravidelný přezkum podle článku 43 a provozuje veřejný registr akreditovaných subjektů podle čl. 43 odst. 6 a akreditovaných správců či zpracovatelů usazených ve třetích zemích podle čl. 42 odst. 7;

p) stanoví požadavky uvedené v čl. 43 odst. 3 pro účely akreditace subjektů pro vydávání osvědčení podle článku 42;

q) poskytuje Komisi stanovisko k požadavkům na vydání osvědčení uvedeným v čl. 43 odst. 8;

r) poskytuje Komisi stanovisko k ikonám uvedeným v čl. 12 odst. 7;

s) poskytuje Komisi stanovisko pro posouzení odpovídající úrovně ochrany ve třetí zemi nebo v mezinárodní organizaci, i pro posouzení, zda určitá třetí země, určité území nebo jedno či více konkrétních odvětví v určité třetí zemi nebo určitá mezinárodní organizace již nezajišťuje odpovídající úroveň ochrany. Za tímto účelem poskytne Komise sboru veškerou potřebnou dokumentaci, včetně korespondence s vládou dané třetí země s ohledem na tuto třetí zemi, území či konkrétní odvětví nebo s mezinárodní organizací;

t) vydává stanoviska k návrhům rozhodnutí dozorových úřadů podle mechanismu jednotnosti uvedeného v čl. 64 odst. 1, k záležitostem předloženým podle čl. 64 odst. 2 a vydává závazná rozhodnutí podle článku 65, včetně v případech uvedených v článku 66;

u) podporuje spolupráci a účinnou dvoustrannou a vícestrannou výměnu informací a osvědčených postupů mezi dozorovými úřady;

v) podporuje společné školicí programy a usnadňuje výměny pracovníků mezi dozorovými úřady a případně i s dozorovými úřady třetích zemí nebo s mezinárodními organizacemi;

w) podporuje výměnu znalostí a dokumentů o právních předpisech v oblasti ochrany údajů a zavedených postupech s dozorovými úřady pro ochranu údajů po celém světě;

x) vydává stanoviska ke kodexům chování vypracovaným na úrovni Unie podle čl. 40 odst. 9); a

y) provozuje veřejně přístupný elektronický registr rozhodnutí přijatých dozorovými úřady a soudy k otázkám řešeným v rámci mechanismu jednotnosti.

V případě, kdy bude aktuální rozhodovací pravomoc dozorových úřadů a soudů ve věcech ochrany osobních údajů dle GDPR (tj. po účinnosti GDPR 25. 5. 2018), je vhodné sledovat elektronický registr rozhodnutí přijatých těmito orgány.

6. Výjimky pro resort zdravotnictví

6.1. Výjimky zpracování osobních údajů pro procesy související s poskytováním zdravotních služeb

Obecně dle GDPR platí, že zpracování zvláštních kategorií osobních údajů (citlivé údaje) je možné pouze v případech, které jsou v GDPR upraveny, což bezesporu platí pro resort zdravotnictví, jak je vysvětleno dále. Dle ustanovení čl. 9 odst. 2 písm. a) až j) však GDPR stanoví podmínky, kdy při splnění alespoň jedné z nich tyto údaje povoluje zpracovávat. Konkrétně ve dvou bodech uvedeného ustanovení existuje výjimka pro resort zdravotnictví:

a) *zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem a při splnění podmínek a záruk uvedených v odstavci 4;*
b) *zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako jsou ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství.*

6.1.1. Omezení právem členského státu

Dle článku 23 odst. 1 existuje možnost **omezit** právem členského státu nebo právem EU práva subjektu údajů, a to ve veřejném zájmu k plnění „jiných cílů“ obecného veřejného zájmu (veřejné zdraví tam je uvedeno) (viz níže tabulka).

Pozn. definice „veřejného zdraví“ ve smyslu širším – dle R 45 GDPR je tento pojem vykládán ve smyslu definice v nařízení Evropského parlamentu a Rady (ES) č. 1338/2008 11, totiž jako *veškeré prvky týkající se zdraví, zejména zdravotní stav včetně nemocnosti a zdravotního postižení, determinanty ovlivňující tento zdravotní stav, potřeby zdravotní péče, prostředky přidělené na zdravotní péči, poskytování zdravotní péče a její všeobecná dostupnost, výdaje na zdravotní péči a její financování a příčiny úmrtnosti.*

Na straně druhé odst. 2 téhož článku 23 stanoví, že každý takovýto legislativní akt mimo jiné stanoví rozsah zavedených omezení (písm. c). Z uvedeného lze dovozovat, že není-li konkrétní rozsah zavedených omezení uveden, má se za to, že omezení neexistuje.

V následující tabulce jsou uvedeny články, ve kterých je možné omezení právem členského státu či právem EU upravit:

Článek	Obsah
čl. 12	**právo subjektu údajů na transparentní, srozumitelné a snadno přístupným způsobem dostupné informace o osobních údajích, které byly získány se souhlasem i bez souhlasu**
čl. 13	**právo subjektu údajů na informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů**
čl. 14	**právo subjektu údajů na informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů**
čl. 15	**právo subjektu údajů na přístup k osobním údajům**
čl. 16	**právo subjektu údajů na opravu** **právo subjektu údajů na doplnění neúplných osobních údajů**
čl. 17	**právo na výmaz**
čl. 18	**právo na omezení zpracování**
čl. 19	**oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování**
čl. 20	**právo na přenositelnost údajů**
čl. 21	**právo vznést námitku**

Již nyní v zákonech v gesci MZ ČR existují konkrétní omezení některých práv subjektu údajů. Typickým příkladem je omezení práva na výmaz stanovením lhůt pro vedení zdravotnické dokumentace či pro anonymizaci osobních údajů v případě NZIS dle zákona č. 372/2011 Sb., o poskytování zdravotních služeb a podmínkách jejich poskytování (zákon o zdravotních službách) a navazující prováděcí vyhlášky.

6.1.2. Generální oprávnění pro resort zdravotnictví

Jak již bylo řečeno výše, platí obecný zákaz zpracování zvláštních kategorií osobních údajů, resp. citlivých osobních údajů, do kterých spadají, mimo jiné, i osobní údaje o zdravotním stavu. Stejně tak bylo výše uvedeno, že struktura GDPR je členěna nikoliv a pouze na jednotlivé kapitoly a ustanovení konkrétních článků, ale je nutné pracovat i s recitály uvedenými v úvodu samotného GDPR a jsou jakousi důvodovou zprávou GDPR a i těchto 173 ustanovení obsahují výkladová pravidla k jednotlivým článkům či přímo regulace samotné.

Generální oprávnění pro resort zdravotnictví je stanovena v níže uvedeném recitálu 52.

Recitál 52	**zákaz zpracování zvláštních kategorií osobních údajů GENERÁLNÍ VÝJIMKA/ODCHYLKA PRO ZDRAVOTNICTVÍ**	Je třeba povolit odchylky od zákazu zpracování zvláštních kategorií osobních údajů, jsou-li stanoveny v právu Unie nebo členského státu a chráněny vhodnými zárukami na ochranu osobních údajů a jiných základních práv, je-li toto zpracování ve veřejném zájmu, zejména zpracování osobních údajů v oblasti pracovního práva a práva v oblasti sociální ochrany, včetně důchodů, a pro účely zdravotní bezpečnosti, monitorování a varování, předcházení přenosným chorobám a jiným závažným hrozbám pro zdraví nebo jejich kontroly. Tato odchylka může být učiněna z důvodů zdraví, včetně veřejného zdraví a řízení zdravotnických služeb, zejména v zájmu zajištění kvality a hospodárnosti v postupech používaných pro vyřizování nároků na plnění a služby v systému zdravotního pojištění, nebo pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely. Odchylka by rovněž měla umožnit zpracování těchto osobních údajů v případech, kdy je to nezbytné pro stanovení, výkon nebo ochranu právních nároků, ať již v soudním řízení, nebo ve správním či mimosoudním řízení.

Dále pro resort zdravotnictví platí i další ustanovení GDPR týkající se výjimek pro zpracování osobních údajů ve veřejném zájmu, pro splnění právní povinnosti či pro účely archivace ve veřejném zájmu či pro statistické účely.

Závěrem je tedy možné konstatovat, že v resortu zdravotnictví je možné zpracovávat zvláštní kategorie osobních údajů (citlivé osobní údaje), avšak pouze pro vymezený účel. Nesmíme však zapomenout na tu skutečnost, že tato výjimka platí pouze v případě, že existují vhodné záruky pro ochranu těchto zpracovávaných osobních údajů, resp. této zvláštní kategorie osobních údajů. V některých případech dochází i k omezení práv subjektu údajů oproti obecné úpravě GDPR.

6.2. Výjimky pro účely archivace ve veřejném zájmu, pro vědecký a historický výzkum a pro statistické účely

6.2.1. Obecně o výjimkách dle čl. 89

Generální výjimka z GDPR existuje v ustanovení čl. 89 o zpracování osobních údajů pro účely archivace ve veřejném zájmu, pro vědecký a historický výzkum a pro statistické účely.

V případě výzkumu dochází ke kolizi dvou obecných zájmů, tedy zájmu na pokroku v oblasti ochrany zdraví s obecným zájmem na zajištění přiměřené nedotknutelnosti osob. Z praxe víme, že se jedná o oblast vysoce konfliktní a je možné, že dojde k žádostem o test proporcionality – mimo jiné i z pohledu etického.

Jedna ze základních zásad zakotvených v GDPR je účelovost zpracování dle čl. 5 odst. 1 písm. b) – neplatí účelové zpracování. Znamená to, že archivace pro výzkum a statistické účely se považuje za účely slučitelné s původním účelem zpracování. Další zásadou není omezení uložení ve smyslu čl. 5 odst. 1 písm. e).

Jedno ze základních práv a tomu odpovídající povinností správce a zpracovatele je povinnost informovat subjekt údajů v případě, že údaje nejsou získány od subjektu údajů v rozsahu č. 14 o všech údajích, způsobu zpracování, předávání dalším subjektům a o dalších bodech v tomto článku uvedeným. Výjimky jsou tři:

1) pokud by poskytnutí vyžadovalo nepřiměřené úsilí nebo znemožnilo účel – v případě archivace ve veřejném zájmu, pro účely vědeckého nebo historického výzkumu (dle čl. 89);
2) stanoveno zákonem, který se na správce vztahuje – tedy rozsah všech údajů**; zde je v ČR nezbytně nutno vyjasnit vazbu zákona č. 101/2000 Sb., resp. této výjimky, na poskytování konkrétních údajů, které jsou o subjektu údajů vedeny a zpracovávány; dále je nutné ověřit, zda je zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) dostatečnou právní úpravou.**
3) zákonem stanovená povinnost mlčenlivosti.

I další nové právo subjektu údajů – právo být zapomenut, právo na výmaz (čl. 17) – neplatí v případech:

1) pro výkon práva na svobodu projevu a informace;
2) pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje;
3) pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;
4) z důvodů veřejného zájmu v oblasti veřejného zdraví;
5) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1.

Podle čl. 21 právo vznést námitku – pro účely vědeckého a historického výzkumu a pro statistické účely dle čl. 89 má subjekt právo vznést námitku proti zpracování, avšak ne v případě, že zpracování je nezbytné pro splnění úkolu prováděného z důvodu veřejného zájmu.

Dle článku 89 odst. 2 a 3 plus ustanovení uvedená výše existuje možnost stanovit odchylky právem členského státu nebo EU, které uvádíme v následujících 3 bodech **(zde je v ČR nezbytně nutno vyjasnit vazbu zákona, zda je zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) a ostatní právní předpisy ve zdravotnictví dostatečnou právní úpravou, pro následující).**

6.2.2. Výjimky pro účely vědeckého a historického výzkumu a pro statistické účely

Pro účely vědeckého a historického výzkumu a pro statistické účely se jedná o možnosti úprav povinností správců či práv subjektů údajů, a to v následujících článcích:

Článek	Obsah
čl. 14	**právo subjektu údajů na informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů**
čl. 15	**právo subjektu údajů na přístup k osobním údajům**
čl. 16	**právo subjektu údajů na opravu** **právo subjektu údajů na doplnění neúplných osobních údajů**
čl. 17	**právo na výmaz**
čl. 18	**právo na omezení zpracování**
čl. 21	**právo vznést námitku**

6.2.3. Výjimky pro účely archivace ve veřejném zájmu

Pro účely archivace ve veřejném zájmu se jedná o možnosti úprav povinností správců či práv subjektů údajů, a to v následujících článcích:

Článek	Obsah
čl. 14	**právo subjektu údajů na informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů**
čl. 15	**právo subjektu údajů na přístup k osobním údajům**
čl. 16	**právo subjektu údajů na opravu** **právo subjektu údajů na doplnění neúplných osobních údajů**
čl. 17	**právo na výmaz**
čl. 18	**právo na omezení zpracování**
čl. 19	**oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování**
čl. 20	**právo na přenositelnost údajů**
čl. 21	**právo vznést námitku**

6.2.4. Primární a sekundární zpracování klinických dat bez zákonného zmocnění

Pokud se jedná o primární nebo sekundární zpracování klinických dat bez zákonného zmocnění, může být takovéto zpracování osobních údajů považováno za zákonné za předpokladu, že byl subjektem údajů udělen k takovémuto zpracování souhlas.

Dopady GDPR jsou v plné šíři všech ustanovení, která se vztahují na zpracování osobních údajů se souhlasem subjektu údajů bez jakéhokoliv omezení pro účely archivace, pro vědecký či historický výzkum nebo pro statistické účely.

7. Co je nutné při zpracování osobních údajů respektovat?

Při zpracování osobních údajů je nutné respektovat zásady zpracování osobních údajů nastavené GDPR a z pozice správce či zpracovatele si plnit povinnosti GDPR nastavené, stejně jako plně respektovat rozšířená práva subjektu údajů. S odchylkami stanovenými právními předpisy ČR.

V následujícím uvádíme některá z nich.

7.1. Poskytnutí informací subjektům údajů

Není možné pominout zejména **poskytnutí informací subjektům údajů**, a to vždy ze strany správce. GDPR jasně stanoví i definici, jakým způsobem mají být tyto informace poskytnuty – tedy stručným, transparentním, srozumitelným a snadno přístupným způsobem, za použití jasných a jednoduchých jazykových prostředků.

Jaký je rozsah informací, které je správce povinen poskytnout? Rozsah je členěn na informace, které jsou získány od subjektu údajů či bez jeho souhlasu. **V případě, že *jsou získávány údaje od subjektu údajů,* neexistuje v GDPR výjimka pro možnou odchylku právem členského státu.**

Z výše uvedeného důvodu platí tedy i pro resort zdravotnictví povinnost poskytnout subjektu údajů veškeré informace uvedené v článku 13. S jedinou výjimkou, a to v případě, že se bude jednat o záchranu života.

Jaké konkrétní údaje jsou subjektu údajů poskytovány?

V okamžiku získání osobních údajů subjektu údajů tyto informace:

a) totožnost a kontaktní údaje správce a jeho případného zástupce;
b) případně kontaktní údaje případného pověřence pro ochranu osobních údajů;
c) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;
d) oprávněné zájmy správce nebo třetí strany v případě, že 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;
e) případné příjemce nebo kategorie příjemců osobních údajů;
f) případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně nebo, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny.

V okamžiku získání osobních údajů i další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování.

V této souvislosti je třeba upozornit, že důkazní břemeno na prokázání toho, že tyto údaje **nejsou** nutné pro zajištění spravedlivého a transparentního zpracování, leží na správci.

Konkrétně se jedná o následující údaje:

a) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;

b) existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;
c) pokud je zpracování založeno na souhlasu, existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;
d) existence práva podat stížnost u dozorového úřadu;
e) skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a možné důsledky neposkytnutí těchto údajů;
f) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

Správce poskytne subjektu informace:

a) v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce, s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovávány;
b) nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace; nebo
c) nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému příjemci.

Pozornost je nutno věnovat případům, kdy jsou informace získávány jinak než od subjektu údajů. To se týká např. ÚZIS ČR, ale i dalších zpracovatelů osobních údajů ze zákona. Zde existuje výjimka, kdy pokud 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, není nutno údaje uvedené v čl. 14 poskytnout subjektu údajů.

Údaje dle čl. 13 a 14 mohou být doplněny standardizovanými ikonami.

Další informační povinnosti ve vztahu k subjektu údajů je sdělit subjektu údajů informace o právech ve smyslu článku č. 15 až 22 – tedy práva subjektu údajů na přístup k osobním údajům, práva na opravu a výmaz, práva na omezení zpracování, práva na přenositelnost údajů (pouze v případě smluvního základu nebo udělení souhlasu), práva vznést námitku a automatizovaného individuálního rozhodování, včetně profilování.

V případě těchto dalších informačních povinností jedinou nejasnou zůstává otázka automatizovaného individuálního rozhodování, vč. profilování. Jedná se např. o případy, kdy poskytovatelé zdravotních služeb poskytují jiné než standardní služby související s léčebnou péčí. Tento bod explicitně upravený není.

Informační povinnost není nutné plnit za předpokladu, že:

a) subjekt údajů již uvedené informace má;
b) 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, 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.

Závěrem upozorňujeme na tu skutečnost, že ke dni zpracování tohoto materiálu je v legislativním procesu nový zákon v gesci MV ČR (tzv. adaptační zákon), který modifikuje stávající právní úpravu ČR pro ochranu osobních údajů. V rámci navrhované právní úpravy je zde navrhováno omezení této informační povinnosti, aby bylo možné zajistit informovanost subjektu údajů na webových stránkách správce v případech, kdy je zpracování osobních údajů prováděno na základě zákona nebo ve veřejném zájmu. Doporučujeme sledovat legislativní proces týkající se navrhovaného zákona.

7.2. Poskytování informací na žádost

V případě sdělení dle čl. 15-22 a výše uvedených informací je další povinností, kterou není možné pominout, poskytnutí informací o přijatých opatřeních na žádost. V tomto případě je nutné zapracovat proces vyřizování žádostí do vnitřních normativních aktů. Lhůta na vyřízení žádosti je bez zbytečného odkladu nejdéle do 1 měsíce. Lhůtu lze při řádném zdůvodnění prodloužit maximálně o 2 měsíce. Forma této žádosti i jejího vyřízení je elektronická, pokud žadatel nepožádá o vyřízení jinou formou. Vyřízení žádosti je bezplatné. Pouze za předpokladu, že žádost je nedůvodná či nepřiměřená, je možné uložit poplatek za vyřízení žádosti nebo žádost odmítnout. Důkazní břemeno pak leží na správci.

7.3. Oznamování porušení zabezpečení osobních údajů

Dále je třeba učinit veškerá sdělení podle článků 33 a 34 o zpracování. Jedná se konkrétně o oznamování případů porušení zabezpečení osobních údajů. Správce v případě porušení zabezpečení osobních údajů oznamuje tuto skutečnost

- **dozorovému úřadu**
  Jedná se o případy, kdy správce má povinnost ohlásit jakékoli porušení, a to bez zbytečného odkladu, nejdéle však do 72 hodin – ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.
- **subjektu údajů**
  Jedná se o případy, kdy by se jednalo o vysoké riziko pro práva a svobody subjektu údajů. Tato sdělení není nutné činit, za předpokladu, že:
  a) správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;
  b) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví;

c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

7.4. Smlouvy o zpracování osobních údajů

Dalším nevyhnutelným krokem je úprava smluv o zpracování osobních údajů. V této souvislosti uvádíme definici zpracování dle čl. 4 bod 2), kdy **„zpracováním“** se rozumí jakákoli operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako jsou shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení. Ke konkrétním úpravám smluv o zpracování osobních údajů může sloužit jako metodický návod tabulka uvedená v příloze č. 2.

7.5. Posouzení vlivu na ochranu osobních údajů

Dalším nevyhnutelným momentem je posouzení vlivu na ochranu osobních údajů. Ve smyslu ustanovení článku 35 a recitálů 89 a 90 je nutné provádět toto posouzení pouze za předpokladu, že se jedná o zavádění nového zpracování či při jeho podstatné změně či zavádění nových technologií. Dle výkladového stanoviska pracovní skupiny WP 29 je však toto posouzení doporučeno i tam, kde započalo zpracování před účinností GDPR, a to zejména v případě, kdy je zpracování vysoce rizikovým; v tomto stanovisku jsou i výslovně jako příklad uvedeny nemocnice a jejich informační systémy.

Na straně druhé je v současné době v legislativním procesu nový zákon na ochranu osobních údajů (tzv. adaptační zákon) v gesci MV, kdy je navrhováno, že posouzení vlivu na ochranu osobních údajů není potřeba dělat, pokud je zpracování stanoveno právním předpisem, což ve většině případů v resortu zdravotnictví je.

7.6. Vnitřní normativní předpisy správce a školení zaměstnanců

Nezanedbatelnou činností, které se nelze vyhnout, je novelizace vnitřních předpisů zohledňující všechny povinnosti správce. Dalším aspektem je také pravidelné školení zaměstnanců o ochraně osobních údajů.

7.7. Jmenování pověřence pro ochranu osobních údajů

Jak již bylo naznačeno výše v kapitole o nových povinnostech správce, jeví se i pro oblast poskytování zdravotních služeb, zejména v segmentu nemocnic, jmenovat pověřence pro ochranu osobních údajů.

Další neopomenutelné skutečnosti jsou uvedeny výše pod bodem nové povinnosti správce.

8. Specifika GDPR pro resort zdravotnictví

8.1. Pacient

Dochází k rozšíření práv pacientů jako subjektu údajů. Tato rozšířená práva subjektu údajů jsou však v některých případech pro oblast zdravotnictví modifikována. V následující tabulce naleznete rozšířená práva subjektu údajů se zopakováním dopadu pro správce, event. v některých případech s příklady modifikací pro resort zdravotnictví:

Článek	Obsah	Dopad a event. konkrétní omezení
čl. 12	**právo subjektu údajů na transparentní, srozumitelné a snadno přístupným způsobem dostupné informace o osobních údajích, které byly získány se souhlasem, i bez souhlasu**	Povinnost správce informovat subjekt údajů transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace dle čl. 13, 14, 15–22 a 34. Informace písemná, elektronická a na žádost ústní. Zavést mechanismus vyřizování žádostí. *Dle návrhu zákona o zpracování osobních údajů (adaptační zákon) je možné informovat na webových stránkách, resp. způsobem umožňujícím dálkový přístup – viz níže čl. 13 a 14.*
čl. 13	**právo subjektu údajů na informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů**	*Správce musí tyto informace poskytnout v okamžiku získání osobních údajů s výjimkou případů, že je již subjekt údajů má. Jedná se o novou povinnost, kterou je nutné zohlednit. Je nutno zavést systém zajištění informovanosti pacientů.* *Výjimkou je například situace, kdy se jedná o záchranu života.* *Dále dle návrhu zákona o zpracování osobních údajů (adaptační zákon) je možné informovat na webových stránkách, resp. způsobem umožňujícím dálkový přístup, ve vazbě zejména na zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) § 53–69 o zdravotnické dokumentaci a prováděcí vyhláška MZ č. 98/2012 Sb., o zdravotnické dokumentaci.* *§ 7* ***Informační povinnost pro zpracování upravená zákonem*** *Pokud provádí správce zpracování nezbytné pro splnění své právní povinnosti nebo svého úkolu*

Článek	Obsah	Dopad a event. konkrétní omezení
		prováděného ve veřejném zájmu nebo při výkonu své pravomoci, může poskytnout informace subjektu údajů podle článku 13 odst. 1 a 2 nebo článku 14 odst. 1 a 2 nařízení Evropského parlamentu a Rady (EU) 2016/679 také zveřejněním informací způsobem umožňujícím dálkový přístup.
čl. 14	**právo subjektu údajů na informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů**	*Pokud se jedná o údaje, které jsou získány od jiného subjektu údajů na základě zákona, je toto právo omezeno.* *Jedním z příkladů jsou např. údaje zcela nezbytné k zajištění návaznosti dalších zdravotních a sociálních služeb poskytovaných pacientovi ve smyslu ustanovení § 45 odst. 2 písm. g) zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách).* *Dále dle návrhu zákona o zpracování osobních údajů (adaptačního zákona) je možné informovat na webových stránkách ve vazbě zejména na zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) § 53–69 o zdravotnické dokumentaci a prováděcí vyhláška MZ. 98/2012 Sb., o zdravotnické dokumentaci.* *§ 7* ***Informační povinnost pro zpracování upravená zákonem*** *Pokud provádí správce zpracování nezbytné pro splnění své právní povinnosti nebo svého úkolu prováděného ve veřejném zájmu nebo při výkonu své pravomoci, může poskytnout informace subjektu údajů podle článku 13 odst. 1 a 2 nebo článku 14 odst. 1 a 2 nařízení Evropského parlamentu a Rady (EU) 2016/679 také zveřejněním informací způsobem umožňujícím dálkový přístup.*
čl. 15	**právo subjektu údajů na přístup k osobním údajům**	Povinnost uložená správci vyhovět žádosti subjektu údajů a sdělit, resp. předat zpracovávané osobní údaje v jejich plném rozsahu.

Článek	Obsah	Dopad a event. konkrétní omezení
čl. 16	**právo subjektu údajů na opravu** **právo subjektu údajů na doplnění neúplných osobních údajů**	Správce bez zbytečného odkladu opraví nepřesné osobní údaje, které se týkají subjektu údajů.
čl. 17 odst. 1	**právo na výmaz („právo být zapomenut“)**	Vzhledem k tomu, že zpracování osobních údajů je ve zdravotnictví ve většině stanoveno právními předpisy, je toto právo omezeno v tomto případě. Jako příklad lze uvést: zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) § 53–69 o zdravotnické dokumentaci a prováděcí vyhláška MZ. 98/2012 Sb., o zdravotnické dokumentaci či § 70-78 týkající se NZIS a lhůt uchovávání osobních údajů.
čl. 18	**právo na omezení zpracování**	Správce omezí zpracování, v kterémkoli z těchto případů: 1) subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit; 2) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití; 3) správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků; 4) subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.
čl. 19	**oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování**	Správce oznamuje jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování provedené v souladu s čl. 16, čl. 17 odst. 1 a čl. 18, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí, správce informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje.

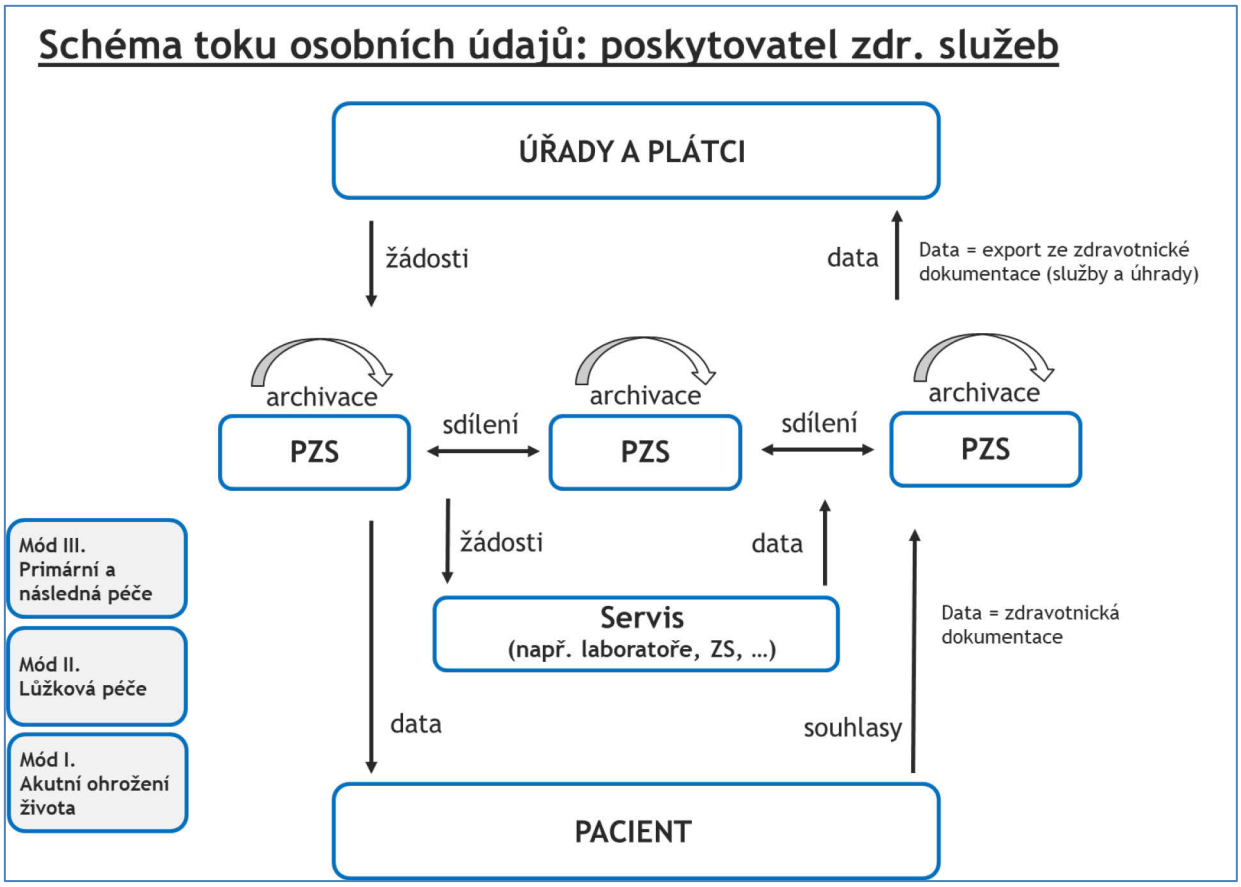
Článek	Obsah	Dopad a event. konkrétní omezení
čl. 20	**právo na přenositelnost údajů**	Předávání osobních údajů jedním správcem správci druhému (za předpokladu technické proveditelnosti) lze realizovat pouze za kumulativního splnění 2 podmínek: ➢ zpracování založeno na souhlasu nebo smlouvě a ➢ jedná se o automatizované zpracování. *V případě poskytování zdravotních služeb a zpracování zdravotnické dokumentace v mezích platných právních předpisů, se toto právo neuplatní*
čl. 21	**právo vznést námitku**	Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.
čl. 22	**právo na to, aby subjekt údajů nebyl předmětem automatizovaného rozhodování, vč. profilování**	Správce nesmí provádět výhradně automatizované individuální rozhodování, vč. profilování, s následujícími výjimkami: ➢ je zákonem stanoveno, ➢ je založeno na souhlasu subjektu, ➢ je nezbytné pro uzavření smlouvy nebo jejího plnění se subjektem.
čl. 77	**právo podat stížnost u dozorového úřadu**	Správce se stává součástí, resp. předmětem šetření.
čl. 78	**právo na účinnou soudní ochranu vůči dozorovému úřadu**	
čl. 79	**právo na účinnou soudní ochranu vůči správci nebo zpracovateli**	Správce se stává stranou soudního sporu.
čl. 80	**právo na to být zastoupen neziskovým subjektem, organizací nebo sdružením**	Povinnost správce jednat s takovýmto subjektem, který zastupuje subjekt údajů, např. v případě podání stížnosti.
čl. 82	**právo na náhradu újmy**	Vznikne-li subjektu údajů újma, ať již hmotná či nehmotná, má správce povinnost tuto újmu nahradit.

8.2. Poskytovatel

U poskytovatelů zdravotních služeb dochází k rozšíření povinností, které musí respektovat v takovém rozsahu, jak byly popsány výše.

Obdobné povinnosti s přiměřenými úpravami se vztahují i na ostatní subjekty v resortu zdravotnictví (plátci, zřizovatelé, správní úřady).

Zjednodušené schéma toku osobních údajů v resortu zdravotnictví z hlediska poskytovatelů je následující:



Rozsah osobních údajů, se kterými poskytovatelé zdravotních služeb nakládají, je možné rozčlenit do následujících kategorií osobních údajů:

- údaje pacientů, kdy základním zdrojem dat je zdravotnická dokumentace,
- údaje zaměstnanců, kdy základním zdrojem jsou osobní spisy,
- údaje dodavatelů, návazně na smlouvy o zpracování osobních údajů apod.

Poskytovatelé zdravotních služeb zpracovávají osobní údaje, resp. jejich nakládání s osobními údaji plně vyhovuje definici zpracování ve smyslu ustanovení čl. 2 bod 2) GDPR, kdy „zpracováním“ se rozumí jakákoli operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako jsou shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Toky zpracování osobních údajů jsou:

a) ve vztahu k pacientům – poskytování informací o zpracování osobních údajů i v případě, kdy je zpracování prováděno na základě zákona bez jeho souhlasu či pro splnění právní povinnosti, dále potom v případě poskytování „nadstandardních služeb“ či z pohledu marketingového oslovení s nabídkou služeb – s jeho souhlasem;
b) ve vztahu k zaměstnancům – zejména v souvislosti s plněním právních povinností, zde je nutné rozlišit, kdy je a není nutný souhlas se zpracováním osobních údajů,
c) ve vztahu k dodavatelům – obousměrné nakládání s osobními údaji, musí být zakotvena ochrana osobních údajů.

Dalším důležitým aspektem je časové hledisko. Situace je rozdílná, pokud:

a) je pacient v přímém ohrožení života,
b) je pacientovi poskytována akutní či plánovaná zdravotní péče.

V prvním případě dochází k omezení některých práv subjektu údajů. Jako příklad je možné uvést zdravotnickou záchrannou službu zasahující u pacienta v bezvědomí či při zástavě základních životních funkcí.

Konkrétní kroky, které vyplývají pro poskytovatele zdravotních služeb v případě implementace GDPR, mimo jiné zahrnují:

Článek	Obsah	Kroky
čl. 24	**zpracovávat osobní údaje v souladu s GDPR**	Musí zavést technická organizační opatření a doložitelná, že jsou údaje zpracovávány v souladu s GDPR, evidence a aktualizace, zpracování koncepce ochrany osobních údajů.
čl. 25	**záměrná a standardní ochrana osobních údajů**	S přihlédnutím ke stavu techniky, nákladům apod. zavedení pseudonymizace, implementace do vnitřních normativních aktů.
čl. 28	**smlouvy o zpracování**	Zpracování nových smluvních ujednání s každým zpracovatelem zahrnující všechny požadavky GDPR, vč. odkazů na certifikace či zajištění auditů.
čl. 29	**zpracování z pověření správce nebo zpracovatele**	Uvést do všech smluv o zpracování osobních údajů.
čl. 30	**záznamy o činnostech zpracování**	Aktualizace systému vnitřních normativních aktů týkajících se činností zpracování.
čl. 31	**spolupráce s dozorovým úřadem**	Event. zavedení spolupráce s ÚOOÚ
čl. 32	**zabezpečení zpracování**	Aktualizace systému vnitřních normativních aktů týkajících se zabezpečení zpracování.
čl. 33	**ohlášení porušení zabezpečení osobních údajů dozorovému úřadu**	Uvést do vnitřních normativních aktů.

Článek	Obsah	Kroky
čl. 34	**ohlášení případů porušení zabezpečení osobních údajů subjektu údajů**	Uvést do vnitřních normativních aktů.
čl. 35	**posouzení vlivu na ochranu osobních údajů a předchozí konzultace**	Návazně na doporučující stanovisko pracovní skupiny WP 29 je nutno provést.
čl. 37–39	**jmenování pověřence na ochranu osobních údajů**	Jmenovat.
čl. 42	**vydání osvědčení**	Event. požádat o vydání osvědčení certifikační autoritu.
čl. 44 a násl.	**předávání osobních údajů do třetích zemí a mezinárodním organizacím**	Upravit do vnitřních normativních aktů pro předávání údajů.

Závěrem lze konstatovat, že povinnosti poskytovatele zdravotních služeb je možno rozčlenit do dvou kategorií:

1) **obecné povinnosti**
2) **povinnosti korespondující s právy pacientů.**

Jak obecné povinnosti správců, tak i povinnosti korespondující s rozšířenými právy pacientů jsou popsány ve výše uvedených obecných kapitolách s omezeními, resp. specifiky popsanými pro resort zdravotnictví v této kapitole.

8.3. Správní a veřejný subjekt

Na správní orgány a ostatní veřejné subjekty jednající ve veřejném zájmu (MZ, krajské úřady, orgány ochrany veřejného zdraví, zdravotní pojišťovny) se vztahují všechny výše uvedené povinnosti/dopady uvedené u poskytovatelů zdravotních služeb. V některých případech se dále uplatní i zvláštní ustanovení týkající se výkonu veřejné moci.

Jmenování pověřence pro ochranu osobních údajů je pro tyto subjekty povinné.

Při výkonu veřejné moci je, mimo jiné, omezeno právo subjektu na výmaz osobních údajů, právo být zapomenut, stejně jako se neuplatní právo na přenositelnost údajů. Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.

8.4. Primární a sekundární zpracování klinických dat pro výzkum na základě zákona

Na správce a zpracovatele v případě primárního a sekundárního zpracování klinických dat stanovených v zákoně se vztahují výše uvedené povinnosti/dopady uvedené u poskytovatelů zdravotních služeb popsané výše, avšak s omezeními uvedenými níže.

V případě sekundárního zpracování se jedná zejména o zpracování osobních údajů pro přesně specifikované oblasti stanovené zákonem. Relevantní zákony v této oblasti jsou např. zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) ve znění pozdějších předpisů v paragrafech 70 až 78 nebo zákon č. 378/2007 Sb., o léčivech ve znění pozdějších předpisů či zákon č. 258/2000 Sb., o ochraně veřejného zdraví ve znění pozdějších předpisů.

Životní cyklus zpracování osobních údajů je stanoven zákonem, stejně jako rozsah či účel jejich zpracování a dále i další podmínky či omezení. Standardní životní cyklus zpracování osobních údajů, tedy konkrétně zahrnuje:

- sběr,
- uchovávání,
- analýza či jiné formy konkrétního zpracování či využití,
- předávání,
- likvidaci.

Obecně lze konstatovat, že na primární a sekundární zpracování dat za účelem archivace ve veřejném zájmu, pro účely vědeckého a historického výzkumu a pro statistické účely se GDPR vztahuje s výjimkami, resp. omezeními, které GDPR připouští. Tedy, jak již bylo popsáno výše, jedná se o následující okruh jednotlivých práv subjektu údajů, který je možné zákonem omezit:

Dle článku 89 odst. 2 a 3 plus ustanovení uvedená výše existuje možnost stanovit odchylky právem členského státu nebo EU: **zde je v ČR nezbytně nutno vyjasnit, zda je zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) a ostatní právní předpisy ve zdravotnictví dostatečnou právní úpravou.**

8.4.1. Výjimky pro účely vědeckého a historického výzkumu a pro statistické účely

Pro účely vědeckého a historického výzkumu a pro statistické účely se jedná o možnosti úprav povinností správců či práv subjektů údajů, a to v následujících článcích:

Článek	Obsah
čl. 14	**právo subjektu údajů na informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů**
čl. 15	**právo subjektu údajů na přístup k osobním údajům**
čl. 16	**právo subjektu údajů na opravu** **právo subjektu údajů na doplnění neúplných osobních údajů**
čl. 17	**právo na výmaz**

Článek	Obsah
čl. 18	**právo na omezení zpracování**
čl. 21	**právo vznést námitku**

Je nutné na tomto místě konstatovat, že tyto výjimky musí být uvedeny explicitně zákonem. Jedním z příkladů je Národní zdravotnický informační systém a jeho právní úprava stanovená zákonem č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) § 70–78.

8.4.2. Výjimky pro účely archivace ve veřejném zájmu

Pro účely archivace ve veřejném zájmu se jedná o možnosti úprav povinností správců či práv subjektů údajů, a to v následujících článcích:

Článek	Obsah
čl. 14	**právo subjektu údajů na informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů**
čl. 15	**právo subjektu údajů na přístup k osobním údajům**
čl. 16	**právo subjektu údajů na opravu** **právo subjektu údajů na doplnění neúplných osobních údajů**
čl. 17	**právo na výmaz**
čl. 18	**právo na omezení zpracování**
čl. 19	**oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování**
čl. 20	**právo na přenositelnost údajů**
čl. 21	**právo vznést námitku**

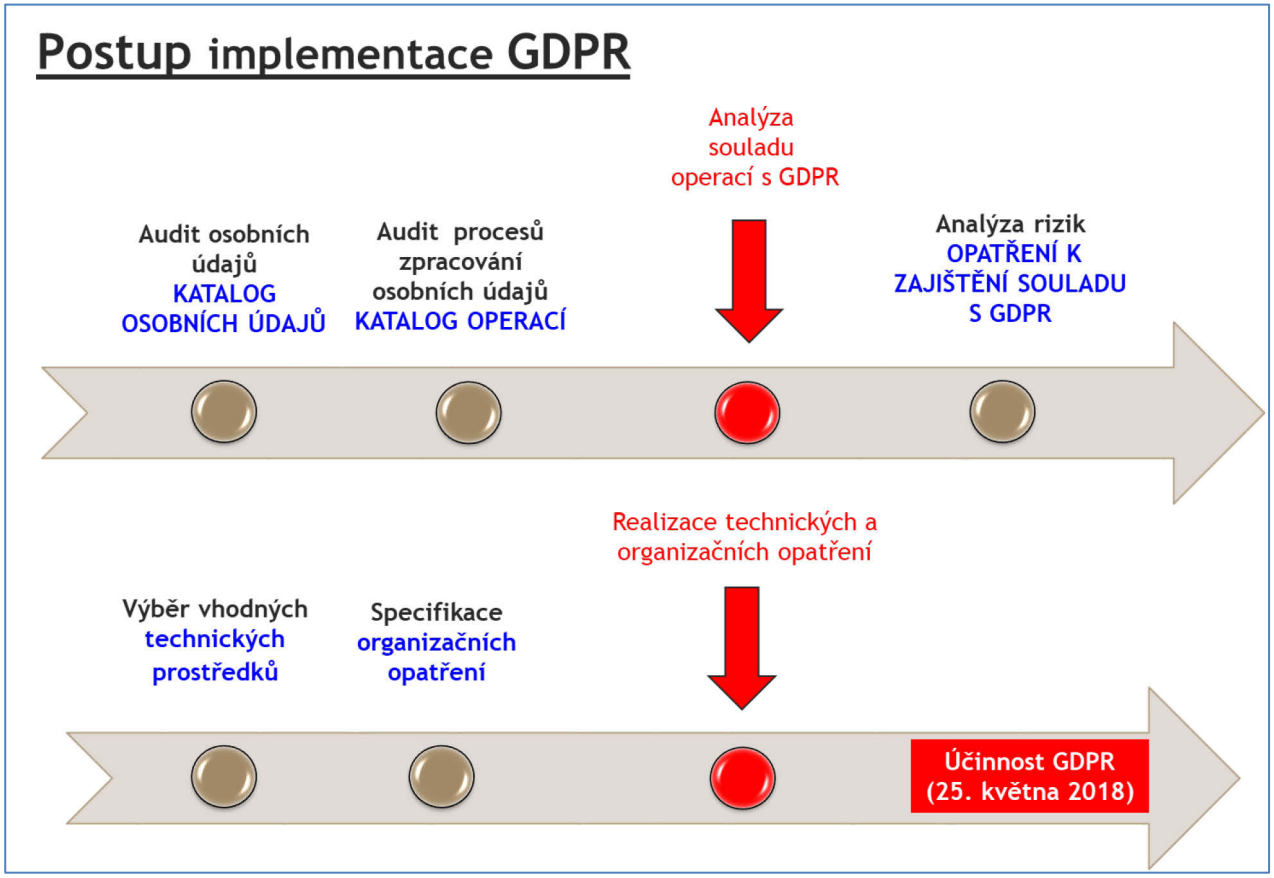
I zde je nutné konstatovat, že omezení je platné pouze v případě, že je omezení explicitně stanoveno právními předpisy.

8.5. Primární a sekundární zpracování klinických dat bez zákonného zmocnění

Pokud se jedná o primární nebo sekundární zpracování klinických dat bez zákonného zmocnění, může být takovéto zpracování osobních údajů považováno za zákonné za předpokladu, že byl subjektem údajů udělen k takovémuto zpracování souhlas.

9. Konkrétní kroky implementace

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:



9.1. 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, 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. 4 naleznete možnosti přístupu pro zpracování takového katalogu osobních údajů. Jedním z možných přístupů je přístup z pohledu datového

zdroje, informačního systému, organizační složky poskytovatele zdravotních služeb apod. Bližší informace přináší přímo uvedená příloha č. 4.

9.2. Katalog operací zpracování osobních údajů

Zpracování přehledu všech procesů zpracování ve vazbě na jednotlivé kategorie osobních údajů. Katalog operací by měl obsahovat zejména:

- příjemce, resp. kategorie příjemců,
- typy zpracování (např. validace dat, nahlížení apod.),
- osoby oprávněné přístupem k osobním údajům,
- dobu jejich uchovávání,
- způsob likvidace.

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

- sběr,
- uchovávání,
- validace, analýza či jiné formy konkrétního zpracování či využití,
- předávání,
- likvidace.

Ke všem operacím by měly být zároveň 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. 4 naleznete velmi jednoduchou osnovu pro zpracování takového katalogu operací s osobními údaji.

Závěrem k bodům 8.1 a 8.2 je možné uvést tu skutečnost, že zpracováním katalogu osobních údajů a katalogu operací s nimi prováděnými, stejně jako informací o tom, kde jsou uvedené operace dokumentovány a kdo je za ně odpovědný, docházíme k základní inventarizaci zpracovávaných údajů a zároveň se tyto dokumenty stávají základním kamenem pro zpracování analýzy souladu s GDPR.

9.3. Analýza souladu s GDPR

Ke zpracovanému katalogu procesu zpracování je nezbytně nutné přiřadit adekvátní povinnosti dle GDPR. Výsledkem je stav připravenosti na GDPR.

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.

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 v subjektu, který má povinnost tyto záznamy o činnostech zpracování vést. Jsou tedy odlišné pro správce a zpracovatele.

V příloze č. 6 je pouze 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 týkající se ochrany osobních údajů i bezpečnosti informací.

9.4. Analýza rizik

Dalším krokem by měla být identifikace rizik, která při stávajícím stavu zpracování osobních údajů hrozí právům a svobodám subjektů osobních údajů.

Hlavním principem implementace GDPR je přístup založený na riziku. 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.

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

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, 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 jsou 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.

V příloze č. 6 tohoto dokumentu jsou nastíněny strukturované body analýzy rizik.

9.5. Technická opatření

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.

9.6. Organizační opatření

Jedním ze základních organizačních opatření je jmenování pověřence pro ochranu osobních údajů, dalším opatřením je pak úprava systému vnitřních normativních aktů, vč. základních dokumentů.

Konkrétní organizační opatření by měla vycházet z konkrétních podmínek každého poskytovatele zdravotních služeb, resp. správce či poskytovatele.

9.7. Školení zaměstnanců

O všech realizovaných opatřeních 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.

9.8. Pravidelná aktualizace a audit

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 stanovit 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.

10. Souhrn – executive summary - pro poskytovatele zdravotních služeb

Po přečtení tohoto materiálu si jistě položíte mnoho otázek a bezesporu jedna z nich či velmi podobná bude znít - jakými kroky a kde začít a co konkrétně dělat? Jak promítnout do běžné praxe tento materiál?

V následujícím shrnutí naleznete velmi zjednodušený nástin základních kroků či postupů a jejich vazbu na jednotlivé části tohoto materiálu a odpovědi na některé otázky.

Poznámka:

Vztahuje se GDPR na ambulantní sféru?

Odpověď zní zcela jednoznačně ano. Na straně druhé existuje jedna z výjimek pro ambulantní sféru, kdy výše zmíněná Pracovní skupina WP29 vydala k této problematice vodítka pro posouzení vlivu obsahující celkem 10 charakteristik zpracování osobních údajů; při splnění 2 z nich je posouzení vlivu nezbytné. Pro resort zdravotnictví platí v tomto ustanovení výjimka pro ambulantní sféru, resp. v případech poskytovatelů poskytujících primární ambulantní péči není nutné zpracovávat posouzení vlivu na ochranu osobních údajů.

10.1. Kdo se bude v organizaci věnovat ochraně osobních údajů

První odpovědí je, že odpovědnost za ochranu osobních údajů leží na správci. Jinými slovy zamyslet se nad základními kroky by měl jistě samotný správce osobních údajů. Jiné zamyšlení bude pro ordinace o síle jednoho lékaře s jednou zdravotní sestrou, jiné pro poskytovatele zdravotních služeb čítající velké množství zdravotnických pracovníků.

Zlaté pravidlo dle GDPR, nehledě na jakýkoliv metodický návod obdržený odkudkoliv, zní: Odpovědnost za ochranu osobních údajů leží pouze a jedině na správci či zpracovateli osobních údajů. Ani vydané osvědčení souladu s GDPR nezbavuje správce či zpracovatele jejich odpovědnosti.

Úplně prvním krokem by mělo být zvážení, kdo se bude v organizaci věnovat samotnému zpracování implementace GDPR. Zároveň je nutno zvážit jmenování pověřence na ochranu osobních údajů.

Již v případě této prvotní úvahy je nutno připomenout, že pověřenec pro ochranu osobních údajů (DPO) není tím, kdo bude zpracovávat všechny implementační kroky. Naopak on by měl pouze dohlížet na jejich zpracování a poskytovat konzultace.

Pročtěte si opětovně pozorně základní náplň činnosti pověřence pro ochranu osobních údajů, která začíná na str. 21 tohoto dokumentu.

Jak vyplývá z výše uvedeného, konkrétnímu zpracování implementačních kroků GDPR by se měl věnovat v ideálním případě interní zaměstnanec (ALE externí spolupráce není vyloučena), který by nastavil základní implementační kroky.

Příklad:

Může to být zaměstnanec zodpovídající za bezpečnost informací, může to být pracovník zodpovídající za IT systémy, může to být zaměstnanec zodpovědný za nastavení ISO norem, může to být zaměstnanec právního oddělení.

Tento zvolený 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).

Návazně na velikost organizace či s přihlédnutím k rozsahu zpracovávaných úkolů se 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 či zvolit externí zajištění. Vše jest to o rozhodnutí samotného správce.

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

Pokud již máte nastaveno, kdo bude zajišťovat implementaci GDPR po realizační stránce, vyvstane Vám otázka, zda vůbec jmenovat pověřence pro ochranu osobních údajů a kdo může být pověřencem pro ochranu osobních údajů.

Pročtěte si opětovně pozorně, který subjekt má za povinnost jmenovat pověřence pro ochranu osobních údajů – opět na str. 21 tohoto dokumentu.

Poskytovatel lůžkové péče jmenuje pověřence pro ochranu osobních údajů vždy.

Základními parametry, kromě informací uvedených výše, jsou tyto:

- musí mít přístup k top managementu neomezený,
- musí mít přístup k veškerým informacím týkajícím se zpracování osobních údajů,
- nesmí být ve střetu zájmů.

S přihlédnutím k jejich organizační struktuře a velikosti je jmenován jediný pověřenec pro ochranu osobních údajů pro několik správců/zpracovatelů. Je nutné splnit několik podmínek a jednou z nich je např. jeho snadná dosažitelnost.

Příklad:

Pověřenec 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. S pověřencem je uzavírána pracovní smlouva, která může poskytnout potřebné záruky nezávislosti pověřence.

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.

10.3. Čím začít

Pracovníci zodpovědní za zajištění implementace GDPR by si v úvodu měli zodpovědět některé základní otázky, které s implementací souvisejí a po vyhodnocení odpovědí na ně zpracovat ucelenou zprávu top managementu organizace, vč. harmonogramu ke schválení.

Checklist základních parametrů implementace GDPR naleznete v příloze č. 3 tohoto dokumentu.

Již na tomto místě musíme upozornit na nutnost spolupráce s DPO, pokud je jmenován.

10.4. Inventura osobních údajů

Základním implementačním krokem je inventura osobních údajů a tedy konkrétně zpracování katalogu osobních údajů a katalogu operací s nimi realizované v organizaci.

Popis katalogu osobních údajů a operací s nimi naleznete rámcově v popisu základních implementačních kroků na stranách 51 a 52 tohoto dokumentu a konkrétní možnou podobu, resp. možnosti přístupu k tvorbě katalogu osobních údajů a ke katalogu operací naleznete v příloze č. 4 tohoto materiálu.

Příklad:

V této fázi si můžete vypracovat vlastní tabulky při využití nastavených číselníků či domluvit se s dodavatelem IT technologií na zpracování speciálního SW. Stejně tak je možné zaúkolovat všechny organizační jednotky poskytovatele (např. jednotlivé kliniky či oddělení) nebo začít předvyplněním některých kategorií přímo pracovníky zodpovědnými za implementaci GDPR nebo jinými odbornými útvary (např. personální odbor atd.) či si vzít tabulky a pokusit si je vyplnit sám vlastními silami.

Závěrem k tomuto bodu je možné uvést tu skutečnost, že zpracováním katalogu osobních údajů a katalogu operací s nimi prováděnými, stejně jako informací o tom, kde jsou uvedené operace dokumentovány a kdo je za ně odpovědný, docházíme k základní inventarizaci zpracovávaných údajů a zároveň se tyto dokumenty stávají základním kamenem pro zpracování analýzy souladu s GPDR či záznamům o činnostech zpracování, kterými se soulad prokazuje.

10.5. Analýza souladu

Po inventuře osobních údajů si zpracujete analýzu souladu s GDPR. Jejím hlavním cílem je vyhodnocení, jak jsou plněny zásady GDPR a plněny jednotlivé povinnosti GDPR správci, event. zpracovateli stanovené.

Obecné informace ke zpracování analýzy souladu naleznete na str. 52 materiálu a praktický návod na její zpracování naleznete v příloze č. 5 tohoto materiálu.

Analýzu souladu by následně měl posoudit pověřenec pro ochranu osobních údajů, je-li jmenován.

V příloze č. 5 je pouze 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 týkající se ochrany osobních údajů i bezpečnosti informací.

Příklad:

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

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 v subjektu, který má povinnost tyto záznamy o činnostech zpracování vést. Jsou tedy odlišné pro správce a zpracovatele. U organizačně menších subjektů je nutné tyto záznamy o činnostech zpracování přizpůsobit velikosti ambulance. Jedná se konkrétně o to mít zmapovány všechny činnosti zpracování alespoň v rozsahu, který je jmenovitě, resp. taxativně dán GDPR.

10.6. Analýza a hodnocení rizik

Dalším krokem či krokem souběžným by měla být analýza rizik. Hlavní význam této činnosti odpoví na otázku, zda v organizaci existují či neexistují rizika pro práva a svobody subjektů údajů, zároveň v případě existence rizika vytvoří systém jejich hodnocení a rozčlení 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).

Obecné informace k analýze a hodnocení rizik naleznete na str. 53 materiálu a praktický návod na její zpracování naleznete v příloze č. 6 tohoto materiálu.

10.7. Technická a organizační opatření

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

- jednak ta skutečnost, že technická a organizační opatření jsou v pořádku a v tomto případě se pouze připojí či stanou součástí komplexní dokumentace zpracování a ochrany osobních údajů v organizaci nebo
- nutné přijetí nových technických a organizačních opatření.

Jeví se vhodným rozčlenit tato opatření ve vazbě na kategorizaci rizik na vysoké riziko, nízké riziko a riziko zbytkové spolu se specifikací osobních údajů, kterých se tato opatření týkají.

Obecné informace k analýze a hodnocení rizik naleznete na str. 53 materiálu a karty opatření naleznete v příloze č. 7 tohoto materiálu.

Příklad:

Možné přiměřeně použít dokumentaci pro certifikaci, resp. normy kvality ISO.

V případě organizačních opatření nezapomenout na úpravu vnitřních normativních aktů a zejména pak i veškerých smluv o zpracování osobních údajů.

Parametry smlouvy o zpracování osobních údajů ve vazbě na jednotlivé články GDPR a povinnosti tam stanovené naleznete v příloze č. 2 tohoto dokumentu. Obecný popis pak na straně 17 tohoto dokumentu.

10.8. Jednání s dodavatelem IT technologií (NIS)

V momentě, kdy z uceleného procesu vyplyne nutnost realizace technických opatření, je nutno zvážit, zda je možné realizovat opatření vlastními silami, event. in-house vývojem anebo začít v této fázi jednat s dodavatelem IT technologií o změnách.

Dále potom v případě spolupráce s ostatními dodavateli je nutné zrealizovat nové smlouvy o zpracování osobních údajů tak, jak byly popsány v předcházejícím bodě 9.7.

10.9. Zpracování informací pro pacienty o zpracování osobních údajů

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

Na zvážení je písemná informace předávaná v listinné podobě.

Obecné informace naleznete v příloze č. 8 tohoto dokumentu a v dokumentu samotném u jednotlivých dopadů pro správce.

10.10. Školení zaměstnanců

Máte-li splněny všechny výše uvedené kroky, nezbývá, než proškolit zaměstnance. Forma jejich proškolení, ať již osobní či elektronická, je plně v kompetenci poskytovatele zdravotních služeb. Nezapomeňte na prokazatelné proškolení zaměstnanců.

O všech realizovaných opatřeních 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.

Obecné informace naleznete v dokumentu na str. 41 a 54.

10.11. Audit a aktualizace

Opakování je matka moudrosti, pravil klasik. Nezapomeňte, prosím, nastavit frekvenci auditu 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.

Obecné informace naleznete v dokumentu na str. 54.

Harmonogram nastavených kroků by měl být v ideálním případě kompletně dokončen k 25. květnu 2018.

11. Závěr

Slova závěrem? Jen přání, aby se Vám implementace GDPR v rámci možností podařila!

Základní pravidla pro implementaci GDPR budou pravidelně aktualizována návazně na výkladová stanoviska pracovní skupiny WP 29 a Úřadu pro ochranu osobních údajů.

Zdroje/literatura:

- 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 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 resort 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)
- zákon č. 374/2011 Sb., o zdravotnické záchranné službě
- zákon č. 89/1995 Sb., o státní statistické službě
- zákon č. 262/2006 Sb., zákoník práce
- zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů
- zákon č. 378/2007 Sb., o léčivech
- zákon č. 123/2000 Sb., o zdravotnických prostředcích
- zákon č. 258/2000 Sb., o ochraně veřejného zdraví
- zákon č. 40/2009 Sb., trestní zákoník
- zákon č. 285/2002 Sb., o darování, odběrech a transplantacích tkání a orgánů a o změně některých zákonů (transplantační zákon)
- 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) atd.
- 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/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=23837
- adaptační zákon (návrh) 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/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=23461
- dokument pracovní skupiny WP 29 obsahující vodítka k pověřencům pro ochranu osobních údajů dostupné z https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=23463
- 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
- Metodické doporučení k organizačně technickému zabezpečení funkce pověřence pro ochranu osobních údajů v podmínkách obcí vydaného MV ČR ze dne 10. 8. 2017.

Příloha č. 1: 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 automatizo-vanému rozhodování
	13	14	15	16	17	18	20	21	22
Právní povinnost uložená správci	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	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	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ne	Ano
Úkol ve veřejném zájmu nebo výkon pravomoci	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	Ano	Ano. Ne, pokud by popřelo smysl zpracování	Ano	Ano	Ano. Ne, pokud jde o ochranu právních nároků	Ano	Ne	Ano	Ano

Příloha č. 2

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.

Článek GDPR	Povinnost správce/zpracovatele	Dopad do smlouvy
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
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 správce 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.

Článek GDPR	Povinnost správce/zpracovatele	Dopad do smlouvy
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. 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 k takovému zpracování za správce.

Příloha č. 3

Checklist 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, které váží na 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 **existenci společných správců**, je nutné podle čl. 26 uzavřít smlouvu a upravit si vzájemné vztahy
4. pokud má správce **zpracovatele** (článek 28), upravit vztahy (musí se upravit všechny i platné smlouvy podle § 6 a § 8 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů)
5. **posoudit rizikovost zpracování** (recitály 75 a 76 a WP 248/17) 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 (čl. 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 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 č. 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. 4

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.

PŘÍLOHA č. 4 KATALOG OSOBNÍCH ÚDAJŮ A KATALOG OPERACÍ

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

U osobních údajů 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. diagnóza

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 u příslušného účelu zůstane prázdné, jedná se o signál pro zúžení rozsahu zpracovávaných osobních údajů.

Příklad:

Osobní údaje jsou zpracovávány pro vlastní potřeby (manažerské 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	ZPŘÍSTUPNĚN 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 kritérií. 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 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. 5

Prokázání souladu s GDPR

Prokázání souladu

(metodický návod)

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

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 33 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. 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 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 resort zdravotnictví, zejména ustanovení týkající se zdravotnické dokumentace či NZIS,
- zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů

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. 33 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 záznamech 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 všechna 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, jejichž je správcem, event. zpracovatelem.

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. 6

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.

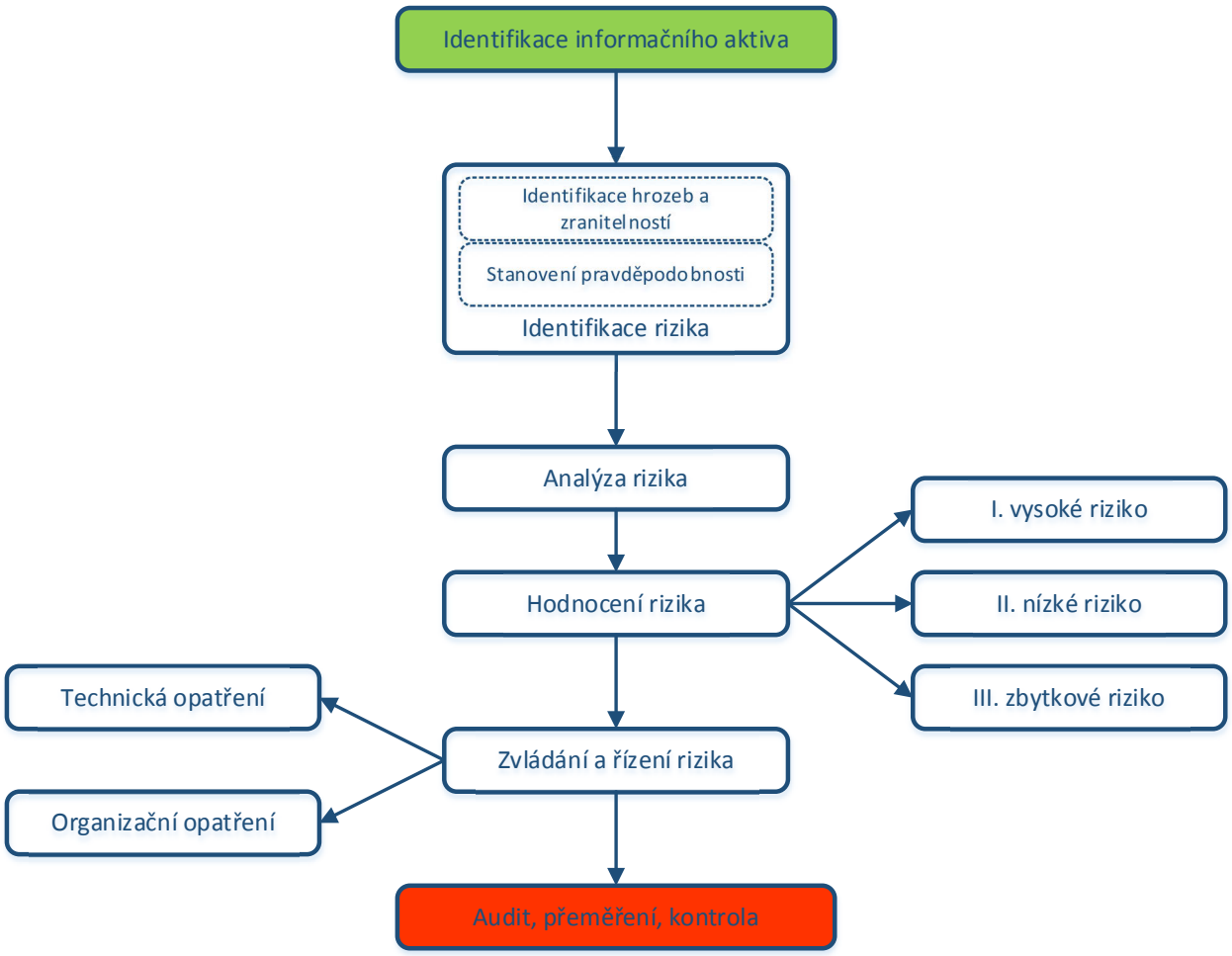
Pro riziko existuje celá řada definic. Riziko je nejčastěji definováno jako součin velikosti následků nežádoucí události a pravděpodobnosti, že k uvedené nežádoucí události dojde.

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.

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. Jedná se o vlastnost aktiva nebo slabina na úrovni fyzické, logické nebo administrativní bezpečnosti, která může být zneužita hrozbou.

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	Zanedba-telný	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

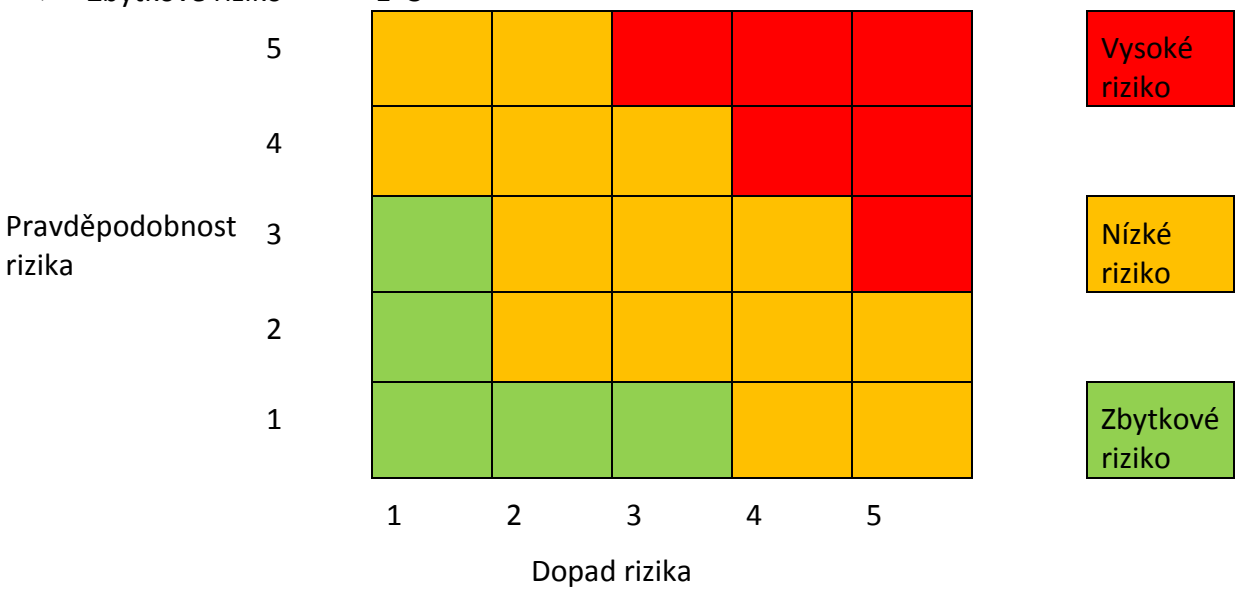
2.5. Hodnocení rizik

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, neboli 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 aplikace 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 výkonnostní 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. 7

Karta opatření

KARTA OPATŘENÍ

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

Analýza rizik, event. analýza souladu, je základem pro zpracování opatření, ať již technických či organizačních pro zajištění souladu s GDPR a bylo-li detekováno riziko (vysoké, nízké či zbytkové), tak pro jeho snižování na akceptovatelnou úroveň.

V následujícím naleznete jednu z možných šablon pro zpracování výše uvedených opatření. Opět se jeví vhodným nástrojem zpracování vhodného standardizovaného číselníku a možnost doplnit i finančním vyjádřením jeho realizace.

2. Vysoké riziko

Nezapomenout, je-li toto riziko detekováno na konzultaci s dozorovým úřadem pouze v případě, když i po zavedení všech možných opatření zůstává riziko vysoké (pro subjekt údajů, nikoliv pro organizaci).

Osobní údaj	Technická opatření	Realizace	Organizační opatření	Realizace

3. Standardní riziko

Osobní údaj	Technická opatření	Realizace	Organizační opatření	Realizace

4. Zbytkové riziko

Osobní údaj	Technická opatření	Realizace	Organizační opatření	Realizace

5. Závěr

Ucelená soustava opatření s vyplněním realizační části může sloužit i ke zpracování rozpočtu implementace GDPR.

Příloha č. 8

Vzor Informací poskytovaných subjektu údajů o zpracování osobních údajů

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)

Význam tohoto dokumentu:

Tato informace Vám slouží k zajištění plné a transparentní informovanosti o zpracování osobních údajů pacientů/klientů, vč. zvláštních kategorií osobních údajů (zejména údaje o zdravotním stavu), správcem těchto údajů.

1. Kontaktní údaje správce:

2. Kontaktní údaje případného pověřence pro ochranu osobních údajů:

3. Účely zpracování a právní základ pro zpracování:

4. Oprávněné zájmy správce nebo třetí strany v případě, že zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany:

5. Příjemci nebo kategorie příjemců osobních údajů:

6. Předávání osobních údajů do zahraničí:

7. Doba uložení osobních údajů:

8. Máte dále následující práva týkající se ochrany Vašich osobních údajů.

   - Máte právo požadovat od Správce **přístup k osobním údajům** týkajícím se Vás jako subjektu údajů, máte právo na jejich opravu.
   - Máte popřípadě **právo na omezení zpracování**, a to v následujících případech:

     a) jestliže popíráte přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;
     b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
     c) správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
     d) jestliže jste již vznesl námitku proti zpracování v případě zpracování v oprávněném zájmu správce či třetích osob, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

   - Máte právo vznést námitku proti zpracování v případě, že:

     a) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu či při výkonu státní moci nebo
     b) v případě, že zpracování je prováděno v oprávněném zájmu správce nebo třetí strany, jakož i práva na přenositelnost údajů.

   - Máte právo podat stížnost u dozorového úřadu, a to v případě, že se domníváte, že zpracováním osobních údajů dochází k porušení GDPR. Stížnost můžete podat u dozorového úřadu:

     a) v místě svého obvyklého bydliště,
     b) místě výkonu zaměstnání nebo
     c) místě, kde došlo k údajnému porušení.

9. Následující práva týkající se ochrany Vašich osobních údajů jsou omezena zákonem:

   - **právo na výmaz osobních údajů** [1][i].

10. Následující práva týkající se ochrany Vašich osobních údajů se na Vás nevztahují:

    - **právo na přenositelnost údajů**, a to vzhledem k tomu, že poskytování Vašich osobních údajů není založeno na souhlasu či smlouvě a neprobíhá pouze automatizovaně.

11. Poskytování Vašich osobních údajů je zákonným požadavkem[1]a máte jako pacient povinnost je poskytnout, stejně jako Správce 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.

[i] Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)

Jak implementovat
Nařízení evropského parlamentu a rady (EU) 2016/679

Mgr. JUDr. Vladimíra Těšitelová, JUDr. Radek Policar,
Ing. Milan Blaha, Ph.D., RNDr. Daniel Klimeš, Ph.D.,
doc. RNDr. Ladislav Dušek, Ph.D.

Vydalo Ministerstvo zdravotnictví ČR
(Palackého náměstí 4, 128 01 Praha 2)
v roce 2018 nákladem 500 výtisků
vydání první

Grafický návrh, sazbu a redakční úpravy provedl
Ústav zdravotnických informací a statistiky ČR

ISBN knižního vydání: 978-80-85047-55-4
ISBN online vydání: 978-80-85047-54-7