Časopis zdravotnického práva a bioetiky
Journal of Medical Law and Bioethics
Vol 7, No 3 (2017), ISSN 1804-8137, http://www.ilaw.cas.cz/medlawjournal

Všeobecné nariadenie o ochrane údajov (GDPR) a jeho dopady na spracovanie osobných údajov v zdravotníctve

GDPR and data protection in healthcare services

Mgr. Zuzana Zoláková

Abstract: Data protection is an integral part of privacy protection in healthcare services as processing of personal data of patients is essential for providing health care services.
Currently, protection of personal data is regulated by Member State Law, transposing Directive 95/46/EC in individual Member States. From May 2018, Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) will apply. To what extent will the regulation affect the provision of health services? Will there be any major changes? What should health care services provider put his focus on when implementing GDPR?

Key words: Regulation (EU) 2016/679 – GDPR – data protection – privacy protection in health services

Abstrakt: Ochrana osobných údajov je komplementárnou súčasťou ochrany súkromia pri poskytovaní zdravotných služieb. Táto činnosť je totiž nevyhnutne spojená so zaznamenávaním (spracúvaním) osobných údajov, a to predovšetkým osobných údajov osôb, ktorým poskytujú zdravotné služby. Doteraz ochranu osobných údajov upravovali v jednotlivých členských štátoch vnútroštátne (národné) úpravy, ktorými sa transponovala smernica 95/46/ES. Od mája 2018 sa začne uplatňovať Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 (GDPR). V akom rozsahu sa nariadenie dotkne poskytovania zdravotných služieb? Dôjde k nejakým zásadným zmenám? Čomu by mal poskytovateľ venovať pozornosť?

Klíčová slova: Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 – GDPR – ochrana osobných údajov – ochrana súkromia v zdravotníctve

ÚVOD

Už o niekoľko mesiacov, presnejšie 25. mája 2018 sa v členských štátoch Európskej únie začne uplatňovať Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov). Ide o priamo aplikovateľný právny akt Európskej únie, ktorý má/mal za cieľ zjednotiť právnu úpravu ochrany osobných údajov v členských štátoch Európskej únie. Nariadenie sa teší živej pozornosti verejnosti. Mnohé webové portály venované téme aplikácie nariadenia pozorne odrátavajú čas do začiatku jeho uplatňovania, veľakrát ale redukujú podané informácie na zdôraznenie prevádzkových nákladov prevádzkovateľov (správcov) na zavedenie postupov v súlade s nariadením a možnej výšky[1] pokút uložených dozornými orgánmi za porušenie nariadenia.

Nemožno poprieť, že tento priamo aplikovateľný právny predpis s viac ako 150 úvodnými ustanoveniami (recitálmi) a 99 článkami núti adresáta normy zvyknúť si na neštandardnú štruktúru predpisu v porovnaní s doteraz platným predpismi ochrany osobných údajov. Pôsobí *„user unfriendly"* a diskomfort pri jeho štúdiu je pochopiteľný. Zároveň je ale nesporné, že v kontexte ochrany súkromia pri poskytovaní zdravotnej starostlivosti, nastupujúcej elektronizácie zdravotníctva, ale aj rozvoja personalizovanej medicíny využívajúcej zariadenia na princípe *Internet of Things* sa problematike ochrany osobných údajov ako imanentnej súčasti poskytovania zdravotnej starostlivosti nemožno vyhnúť.

Na mieste je teda otázka, do akej miery je nariadenie zásadným prelomom v ochrane osobných údajov v zdravotníctve?

1. OCHRANA SÚKROMIA PRI POSKYTOVANÍ ZDRAVOTNEJ STAROSTLIVOSTI

Vzťah medzi lekárom a pacientom je vzťah fiduciárny, a teda vzťah, v ktorom hrá dôvera kľúčovú úlohu. Podstatná je nielen dôvera v schopnosti lekára, ale aj v to, že informácie, ktoré mu pacient zverí, a ktoré ďalej spracúva, ostanú dôverné. Narušenie tejto dôvery môže mať za následok minimálne neochotu k spolupráci na strane pacienta, v horšom prípade sťaženie diagnostiky a terapie v dôsledku neúplných informácií, ktoré pacient nie je ochotný zdieľať, až po závažné incidenty vedúce k vypovedaniu zmluvy s poskytovateľom, prípadne využitie prostriedkov na vyvodenie administratívnej zodpovednosti (disciplinárne konanie, podnet/sťažnosť na *Úřad pro ochranu osobních údajů*) či občianskoprávnej zodpovednosti napr. v podobe návrhu na náhradu nemajetkovej ujmy.

Aj z vyššie uvedených dôvodov ochrana súkromia pacienta je zásadná etická[2] a dnes aj právna povinnosť poskytovateľa, prípadne zdravotníckeho pracovníka, ktorá nachádza svoje zakotvenie

[1] Nariadenie 2016/679 upravuje vysoké maximálne výšky pokút za porušenie povinností stanovených Nariadením, najzávažnejšie porušenia môžu byť sankcionované až do výšky 20 000 000 eur prípadne do 4 % celkového svetového ročného obratu podľa toho, ktorá suma je vyššia (článok 83 Nariadenia). Je potrebné zdôrazniť, že sa neočakáva, že by takto vysoké pokuty boli ukladané za bežné porušenia. Treba mať na pamäti, že Nariadenie má široko upravenú pôsobnosť (exteritoriálnu), a teda na jeho základe je možné ukladať sankcie globálne pôsobiacim firmám napr. na poli poskytovania informačných služieb.

[2] Zásadnú etickú povinnosť spojenú s vykonávaním lekárskeho povolania, a totiž chrániť súkromie pacienta a zachovávať mlčanlivosť o údajoch, ktoré sa lekár dozvedel obsahuje aj Hippokratova prísaha. *„Cokoli, co při léčbě i mimo svou praxi ve styku s lidmi uvidím a uslyším, co nesmí se sdělit, to zamlčím a uchovám v tajnosti*." Pozri bližšie k téme transformácie obsahu etických povinností do právnych predpisov DOLEŽAL, Tomáš. *Vztah lékaře a pacienta z pohledu soukromého práva*. Praha: Leges, 2012, s. 11–12, 101–104.

v teórii ľudských práv. Konkrétne vyplýva zo záväzku zmluvných štátov Dohovoru o ochrane základných práv a slobôd, ako aj Dohovoru o ľudských právach a biomedicíne[3] rešpektovať súkromný a rodinný život jednotlivcov (článok 8 Dohovoru o ochrane ľudských práv), ako aj záväzku rešpektovať súkromie jednotlivcov v súvislosti s informáciami o ich zdraví (článok 10 Dohovoru o biomedicíne). Tieto záväzky sú na úrovni vnútroštátneho práva reflektované v ústavách ako garantované ľudské práva na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života (článok 10 ods. 2 *Listiny základních práv a svobod* / článok 19 ods. 2 Ústavy SR), ako aj pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe (článok 10 ods. 3 *Listiny základních práv a svobod* / článok 19 ods. 3 Ústavy SR). Ďalej sú zakotvené v rade právnych inštitútov, ako je:

1) *informovaný súhlas s poskytovaním zdravotnej starostlivosti* zameraný na rešpektovanie ľudskej dôstojnosti, telesnej integrity a autonómie pacienta vrátane práva na informácie o zdravotnom stave a možnosti odmietnutia liečby;

2) *povinnosť poskytovateľa/zdravotníckeho pracovníka zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvedel v súvislosti s poskytovaním zdravotných služieb/výkonom svojho povolania* (§ 51 zákona č. 372/2011 *Sb., o zdravotních službách ve znění pozdějších předpisů* / § 82 ods. 5 zákona č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti v znení neskorších predpisov) až po

3) *dodržiavanie predpisov upravujúcich nakladanie so zdravotnou dokumentáciou*, najmä pokiaľ ide o jej poskytovanie či sprístupňovanie tretím stranám.

2. OCHRANA OSOBNÝCH ÚDAJOV V ZDRAVOTNÍCTVE

Komplementárnou súčasťou ochrany súkromia jednotlivcov (fyzických osôb) pri poskytovaní zdravotnej starostlivosti je právo na ochranu osobných údajov. Toto právo pritom vyplýva nielen z vyššie uvedených záväzkov štátov stanovenými medzinárodnými dohovormi, ale tiež z primárneho práva Európskej únie, konkrétne z článku 16 Zmluvy o fungovaní Európskej únie, ako aj z článkov 7 a 8 Charty základných práv Európskej únie, ktorá na rozdiel od Dohovorov Rady Európy upravuje v článku 8 samostatné právo na ochranu osobných údajov.[4]

[3] Implementácia, ako aj interpretácia záväzku rešpektovať súkromie jednotlivcov vyplývajúceho z Dohovorov, najmä pokiaľ ide o naplnenie podmienok primeranosti a nevyhnutnosti zásahov do súkromia upravenej v článku 8 ods. 2 Dohovoru o ochrane základných práv a slobôd a článku 26 Dohovoru o ľudských právach a biomedicíne je dynamická, nie je jednotná, pokiaľ ide o jednotlivé zmluvné strany Dohovoru. Okrem toho je práve porušenie tohto článku často predmetom sťažností z oblasti medicínskeho práva prejednávaných Európskym súdom pre ľudské práva. Okrem toho je dôležité uviesť, že Európsky súd pre ľudské je zdráhavý, pokiaľ ide o vyjadrenie sa k zásadným etickým/právnym otázkam týkajúcim sa ochrany súkromia v zdravotníctve (umelé prerušenie tehotenstva/ochrana života nenarodeného, domáce pôrody, asistovaná reprodukcia, náhradné materstvo), kde uplatňuje širokú mieru voľnej úvahy štátov (*margin of appreciation*). Pozri ŠIKUTA, Ján. Doktrína „miery voľnej úvahy“ (*The Margin of Appreciation Doctrine*) a judikatúra Európskeho súdu pre ľudské práva v Štrasburgu. *Justičná revue.* 2012, roč. 64, č. 8–9, s. 952–958. HUMENÍK, Ivan. – SZANISZLÓ, Vladimír M. – ZOLÁKOVÁ, Zuzana (eds). *Reprodukčné zdravie ženy v centre záujmu*. Bratislava: Wolters Kluwer, 2014, s. 112–121.

[4] Je nutné poznamenať, že práve tento ľudskoprávny presah ochrany osobných údajov zásadne odlišuje európsky systém ochrany osobných údajov a právnu reguláciu od amerického chápania a v posledných rokoch spôsobuje nie málo problémov v oblasti prenosov osobných údajov do Spojených štátov amerických. Pozri Rozsudok zo dňa

Ochranu osobných údajov upravujú aktuálne stále platné a účinné právne predpisy, zákon č. 101/2000 *Sb., o ochraně osobních údajů o změně některých zákonů, ve znění pozdějších předpisů*, a zákon č. 122/2013 Z. z. o ochrane osobných údajov v znení neskorších predpisov. Oba predpisy sú implementáciou smernice 95/46/ES o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov. Tento právny akt Európskej únie je bezprecedentný v tom, že pre členské štáty Európskeho spoločenstva stanovuje základný rámec respektíve minimálny štandard ochrany osobných údajov, a to konkrétne:

1) *úpravou legálnych definícií právnych pojmov súvisiacich so spracúvaním osobných údajov* (*správce*/prevádzkovateľ, *zpracovatel*/sprostredkovateľ, osobitná kategória osobných údajov, tretia strana, *přijímatel*/príjemca, *souhlas subjektu údajů* / dotknutej osoby) (článok 2 smernice);[5]

2) *stanovením základných zásad spracúvania osobných údajov* (článok 6 ods. 1 smernice):

a) *obmedzenie účelu*: spracúvanie je možné len na konkrétne, vyjadrené (výslovne uvedené) a legitímne účely,

b) *obmedzenie rozsahu respektíve minimalizácia údajov*: spracúvanie obmedzené na rozsah nevyhnutný vzhľadom na účely spracúvania,

c) *správnosť, aktuálnosť a úplnosť údajov*,

d) *anonymizácia/vymazanie údajov po naplnení účelu spracúvania* (článok 6 ods. 1 písm. e);

3) *úpravou všeobecných podmienok zákonnosti spracúvania osobných údajov* (tzv. právnych základov spracúvania) (článok 7 smernice):

a) *súhlas subjektu údajů / dotknutej osoby*,

b) *spracovanie je nevyhnutné pre splnenie zmluvy*, ktorej zmluvnou stranou je *subjekt údajů* / dotknutá osoba,

c) *spracúvanie je nevyhnutné pre plnenie právnej povinnosti prevádzkovateľa*,

d) *spracúvanie je nevyhnutné pre zachovanie životne dôležitého záujmu subjektu údajů* / dotknutej osoby,

e) *spracúvanie je nevyhnutné na vykonanie úlohy vo verejnom záujme* alebo pri výkone verejnej moci,

f) *spracúvanie je nevyhnutné pre uskutočnenie oprávneného záujmu správce* (prevádzkovateľa) alebo tretej osoby;

4) *úpravou výnimiek zo zákazu spracúvanie osobitnej kategórie osobných údajov*, vrátane výnimky pre spracúvanie na účely preventívneho lekárstva, určenia diagnózy, poskytovania zdravotnej starostlivosti alebo manažmentu poskytovania zdravotnej starostlivosti, a kde sú tieto údaje spracúvané zdravotníckym pracovníkom (odborne spôsobilou osobou), ktorá je viazaná

6. 10. 2015, *Maximillian Schrems v. Data Protection Commissioner*, C-362/14, tiež Vykonávacie rozhodnutie Komisie (EÚ) 2016/1250 z 12. júla 2016 podľa smernice Európskeho parlamentu a Rady 95/46/ES o primeranosti ochrany poskytovanej štítom na ochranu osobných údajov medzi EÚ a USA. Ochrana osobných údajov a jej vynucovanie v Spojených štátoch aj na základe *Privacy Shield* vykonávajú orgány verejnej moci (agentúry) zodpovedné primárne za kontrolu správania subjektov na trhu, dodržiavanie práv spotrebiteľov a ochranu hospodárskej súťaže (*Federal Trade Commission*, v podstate plniaci funkcie Protimonopolného úradu), nie dodržiavanie ľudských práv, tak ako je to v Európskej únii (Súdny dvor Európskej únie).

[5] Niektoré definície, napr. definíciu osobných údajov, upravoval už Dohovor Rady Európy č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (článok 2 Dohovoru).

vnútroštátnym právom alebo pravidlami kompetentných orgánov povinnou mlčanlivosťou, alebo inou osobou, ktorá je viazaná podobnou povinnosťou;

5) *úpravou práv subjektů údajů / dotknutých osôb*

a) *právo na informácie o spracúvaní* (článok 10 a 11),

b) *právo na prístup k údajom* (článok 12 smernice),

c) *právo na opravu a opravu v súvislosti so zásadou správnosti a aktuálnosti údajov*,

d) *právo namietať* (článok 14);

6) *úpravou minimálneho štandardu pre opatrenia na zabezpečenie ochrany osobných údajov* vyplývajúce zo spôsobu spracúvania a charakteru údajov (článok 17), ako napr. sprostredkovateľská zmluva, oznámenia úradu, osoba poverená ochranou údajov, predbežná kontrola;

7) *úpravou nástrojov pre prenosy osobných údajov do tretích krajín* (článok 25 smernice).

Ustanovenia smernice 95/46/ES boli transponované do vnútroštátnych poriadkov členských štátov rôzne, čo malo za následok rad podstatných odlišností, predovšetkým pokiaľ ide o zákonom uložené opatrenia na zabezpečenie ochrany osobných údajov prípadne ukladanie sankcií za porušenie či forma týchto sankcií.[6] Ako vhodný príklad poslúži už len komparácia českého a slovenského zákona o ochrane osobných údajov. Tie sa odlišujú tak terminológiou, čo reflektuje aj dvojaká verzia niektorých pojmov v tomto článku (*správce*/prevádzkovateľ, *zpracovatel*/sprostredkovateľ, *subjekt údajů* / dotknutá osoba), ale tiež aplikáciou notifikačných povinností (slovenských zákon o ochrane osobných údajov rozlišuje evidenčnú povinnosť, oznámenie a osobitnú registráciu), ako aj konkrétnymi technickými, organizačnými a personálnymi opatreniami. Napríklad, zákon č. 122/2013 Z. z. na rozdiel od českého zákona upravoval podmienky vymenovania tzv. zodpovednej osoby / *pověřence pro ochranu údajů* (§ 23 a nasl. zákona č. 122/2013 Z. z.) a tiež povinnosť vypracovať bezpečnostný projekt pre prípady spracúvania osobitnej kategórie osobných údajov v systéme prepojenom s verejne prístupnou počítačovou sieťou (§ 19 ods. 2 zákona č. 122/2013 Z. z.).

Pokiaľ ide o vzťah predpisov o ochrane osobných údajov a spracúvania údajov pri poskytovaní zdravotnej starostlivosti možno konštatovať, že k prepojeniu pôsobnosti týchto predpisov dochádza pri regulácii vedenia zdravotnej dokumentácie. Túto oblasť tradične upravujú špeciálne právne predpisy, preto sa v zmysle zásady *lex specialis derogat lex generali* právne predpisy vzťahujúce na ochranu osobných údajov aplikujú na vedenie zdravotnej dokumentácie (iba) subsidiárne. V českom právnom poriadku ide o ustanovenia § 52 a nasl. *zákona č. 372/2011 Sb., o zdravotních službách ve znění pozdějších předpisů*, ako aj ustanovenia § 2647 až 2650 a § 109 a § 2828 (pre získanie tzv. druhého stanoviska – *second opinion*) *zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů*. Napriek niektorým problémom súvisiacich s kolidujúcimi ustanoveniami zákona o zdravotných službách a *Občanského zákoníka*, pokiaľ ide o sprístupňovanie údajov o tretích osobách v zdravotnej

[6] Niektoré členské štáty neukladali pokuty za porušenie predpisov ochrany osobných údajov (napr. Estónsko). V iných krajinách fungoval dvojaký systém vynucovania dodržiavania pravidiel ochrany osobných údajov – ombudsmanský a dozorný/kontrolný vo forme začatia správneho konania v prípade závažného/neodstráneného porušenia (Maďarsko).

dokumentácii,[7] je potrebné vysoko vyzdvihnúť precíznu úpravu postupu nakladania so zdravotnou dokumentáciou v prípadoch zániku oprávnenia poskytovateľa zdravotných služieb (§ 57 až 64 *zákona o zdravotních službách*), ktorá zaručuje ochranu údajov pacienta po zániku poskytovateľa prípadne jeho oprávnenia, rešpektuje právo pacienta na slobodnú voľbu poskytovateľa okrem prípadov poskytovateľa pracovnolekárskych služieb, právo zdravotníckych pracovníkov / poskytovateľa / jeho zamestnanca nahliadnuť do dokumentácie v prípade sporu, ako aj dodržiavanie povinnej mlčanlivosti o údajoch takto sprístupnených (§ 64 ods. 2 *zákona o zdravotních službách*).[8]

Na rozdiel od českej úpravy je slovenská právna úprava menej precízna, čo ale možno pripísať aj tomu, že ide o starší právny predpis, hoci často novelizovaný, a to zákon č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o zdravotnej starostlivosti“). Spracúvanie, sprístupňovanie a poskytovanie údajov zo zdravotnej dokumentácie upravené § 18 a nasl. tohto zákona a tiež zákonom č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o NCZI“). Je pomerne nešťastné, a to nielen z hľadiska aplikácie ale aj z hľadiska normotvorby, že oba predpisy sú len minimálne konzistentné a navzájom spolu „nekomunikujú“. V prípade zákona o NCZI ide o technickú normu, ktorá nereflektuje na ustanovenia zákona o zdravotnej starostlivosti.

Do spracúvania osobných údajov v zdravotníctve musíme zaradiť aj tzv. transplantačné zákony, 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. 317/2016 Z. z. o požiadavkách a postupoch pri odbere a transplantácii ľudského orgánu, ľudského tkaniva a ľudských buniek a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, vzhľadom na to, že do kategórie osobných údajov, dokonca údaje osobitnej kategórie osobných údajov (inak aj *„citlivé údaje“*) sú zaradené tiež genetické údaje, preto sa právna úprava ochrany osobných údajov dotýka subsidiárne aj nakladania s bunkami, tkanivami ap.

V praxi zdravotníckych zariadení sa mnohokrát stretávame s minimálnou respektíve absentujúcou reflexiou na subsidiárne aplikovanie predpisov ochrany osobných údajov, a to aj tam, kde sú na spracúvanie údajov / vedenie dokumentácie (alebo jej časti) využívané moderné technológie, a teda ide o automatizované spracovanie osobných údajov.[9] Je ale nutné dodať, že využitie takýchto prostriedkov nie je predpokladom aplikácie predpisov ochrany osobných údajov; keďže v súlade s ustanoveniami § 3 ods. 2 a § 4 písm. e) *zákona o ochraně osobních údajů* a § 2 ods. 3 zákona o ochrane

[7] Pozri ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ ČESKÉ REPUBLIKY. *Stanovisko č. 3/2015 – Zpracování osobních údajů v souvislosti s vedením zdravotnické dokumentace* [online]. 2015, jún, s. 2 Dostupné na: <https://www.uoou.cz/stanovisko%2Dc%2D3%2D2015%2Dzpracovani%2Dosobnich%2Dudaju%2Dv%2Dsouvislosti%2Ds%2Dvedenim%2Dzdravotnicke%2Ddokumentace/d-15127/p1=1099> [cit. 13. 11. 2017].

[8] Zaujímavou otázkou ostáva napr. riešenie dlhodobej práceneschopnosti ošetrujúceho (ambulantného) lekára a prístupu k údajom uloženým v priestoroch zdravotníckeho zariadenia, riešenie odovzdania dokumentácie medzi poskytovateľmi ako aj hlbšia otázka „vlastníctva“ respektíve kontroly nad údajmi spracúvanými v zdravotnej dokumentácii.

[9] Pozri ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ ČESKÉ REPUBLIKY. *Stanovisko č. 3/2015 – Zpracování osobních údajů v souvislosti s vedením zdravotnické dokumentace* [online]. 2015, jún, s. 5 Dostupné na: <https://www.uoou.cz/stanovisko%2Dc%2D3%2D2015%2Dzpracovani%2Dosobnich%2Dudaju%2Dv%2Dsouvislosti%2Ds%2Dvedenim%2Dzdravotnicke%2Ddokumentace/d-15127/p1=1099>.

osobných údajov[10] sa tieto predpisy vzťahujú aj na vedenie zdravotnej dokumentácie v písomnej forme. Zásadným a častým nedostatkom spracúvania osobných údajov je v konkrétnych prípadoch absencia primeraných technických, organizačných a personálnych opatrení na zabezpečenie údajov, ako je zabezpečenie dokumentácie pred prístupom tretích osôb, logovanie prístupov oprávnených osôb, vytváranie rôznych prístupov pre rôznych zamestnancov ap. Zabezpečenie dokumentácie pred stratou alebo zneužitím je podstatné aj tam, kde predpisy osobitne upravujúce vedenie zdravotnej dokumentácie (odovzdanie novému poskytovateľovi) boli dodržané.[11] V slovenských podmienkach je vhodným príkladom nedodržiavania povinností vyplývajúcich zo zákona o ochrane osobných údajov absencia bezpečnostných projektov a bezpečnostných opatrení (!) v prípadoch, kedy sa údaje osobitnej kategórie spracúvajú poskytovateľom zdravotnej starostlivosti v systéme prepojenom s verejne prístupnou počítačovou sieťou, a teda sú splnené podmienky § 19 ods. 2 písm. a) zákona o ochrane osobných údajov či nezabezpečením údajov pred sprístupnením tretím osobám, ktoré nato nie sú oprávnené.[12] Ďalej možno spomenúť nerešpektovanie zásady integrity údajov tam, kde dochádza k spracúvaniu neúplnej zdravotnej dokumentácie, čo môže nastať vedením elektronickej dokumentácie bez zaručeného elektronického podpisu bez „duplikátu“ v papierovej verzii, neodovzdaním zdravotnej dokumentácie novému poskytovateľovi, absenciou záznamov špecialistov v dokumentácii vedenej všeobecným lekárom. Za zmienku stojí aj nedodržiavanie doby uschovávania údajov či porušovanie predpisov o ochrane osobných údajov spôsobené využívaním údajov o pacientoch na zasielanie marketingových informácií o poskytovateľom ponúkaných zdravotníckych prostriedkoch.[13] Príčiny niektorých problémov možno hľadať aj v nedôslednosti zákonodarcu, keďže možno len súhlasiť s konštatovaním R. Policara,[14] že zdravotnícke predpisy[15] redukovali úlohu počítača pri spracúvaní na inteligentný písací stroj a vyhľadávaciu pomôcku, keďže samotná právna úprava

[10] Je zaujímavé poukázať na odlišnú úpravu vecnej pôsobnosti v českom a slovenskom zákone o ochrane osobných údajov. Zatiaľ čo, český zákon stanovuje, že *„tento zákon sa vztahuje na veškeré zpracování osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky“*, slovenský zákon č. 122/2013 Z. z. takmer totožne s článkom 3 ods. 1 smernicou 95/46/ES (*„This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system“*) vymedzuje vecnú pôsobnosť zákona nasledovne: *„Tento zákon sa vzťahuje na osobné údaje systematicky spracúvané úplne alebo čiastočne automatizovanými prostriedkami spracúvania alebo inými ako automatizovanými prostriedkami spracúvania, ktoré sú súčasťou informačného systému alebo sú určené na spracúvanie v informačnom systéme*.“ Dôsledkom slovenského prekladu je nejednoznačnosť výkladu pri aplikácii ustanovenia § 2 ods. 2 zákona o ochrane osobných údajov.

[11] Tu možno upozorniť na kontrolu *Úřadu pro ochranu osobních údajů* na základe sťažnosti na konanie lekárky, ktorá nedostatočne zabezpečila zdravotnú dokumentáciu pacienta pri jej odovzdaní inému (novému) poskytovateľovi a odovzdala ju na prepravu spolu s laboratórnymi vzorkami. Príklad dokladá práve subsidiárne aplikovanie predpisov ochrany osobných údajov. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Předávaní zdravotnické dokumentace* [online]. 13. 12. 2013. Dostupné na: <https://www.uoou.cz/nakladani%2Dse%2Dzdravotnickou%2Ddokumentaci/d-1747/p1=1099> [cit. 13. 11. 2017].

[12] Napr. nezabezpečenie papierovej zdravotnej dokumentácie počas stavebných prác v zdravotníckom zariadení.

[13] Pozri ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Předávaní zdravotnické dokumentace* [online]. 13. 12. 2013. Dostupné na: <https://www.uoou.cz/nakladani%2Dse%2Dzdravotnickou%2Ddokumentaci/d-1747/p1=1099> [cit. 13. 11. 2017].

[14] POLICAR, Radek. *Zdravotnická dokumentace v praxi*. Praha: Grada, 2009, s. 95–99.

[15] V Českej republike tomu tak bolo od prijatia *zákona o zdravotních službách* v roku 2011.

vedenia zdravotnej dokumentácie nereflektovala na nové spôsoby a možnosti spracúvania údajov (elektronické spracúvanie osobných údajov, možnosť ukladania údajov s využitím poskytovateľa cloudových služieb). Je paradoxné, že právna úprava poskytuje viac usmernení poskytovateľovi (*správci*/prevádzkovateľovi), ktorý vedie dokumentáciu s pomocou písacieho stroja než tomu, ktorý používa počítač. Na druhej strane je potrebné vyzdvihnúť definíciu elektronickej formy vedenia zdravotnej dokumentácie upravenú v ustanovení § 54 ods. 1 *zákona o zdravotních službách*.[16]

Pokiaľ ide o výkon dozoru na vedením zdravotnej (zdravotníckej) dokumentácie zo strany úradov na ochranu osobných údajov, ten nie je taký priamočiary vzhľadom na existenciu množstva osobitných právnych predpisov (*lex specialis*) a ďalšiu rezortnú reguláciu a usmernenia. Úrady sú ale často krát prostriedkom ochrany práv pacientov *ultima ratio* vo veciach týkajúcich sa zdravotnej dokumentácie práve tam, kde sa im so sťažnosťou nepodarilo uspieť u poskytovateľa ani v konaní pred správnym orgánom udeľujúcim oprávnenie na poskytovanie zdravotných služieb / povolenie na prevádzkovanie zdravotníckeho zariadenia (SR).

3. NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 (GDPR)

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/67 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „Nariadenie“ alebo „Nariadenie 2016/679“) je výsledkom viac ako päť rokov trvajúcich prác a rokovaní, ktoré boli ukončené schválením textu v apríli 2016. Nariadenie 2016/679 je účinné od 24. mája 2016 a začne sa uplatňovať 25. mája 2018.

Ako bolo spomenuté už vyššie, nejde práve o stručný právny predpis. Nariadenie pozostáva zo 173 úvodných ustanovení (recitálov), ktoré nie sú právne záväzné a majú charakter podobný dôvodovej správe, a 99 článkov. Pokiaľ ide o systematiku Nariadenia, základné členenie predpisu kopíruje členenie smernice 95/46/ES (pôsobnosť, zásady, právne základy, práva subjektov údajov, bezpečnosť údajov, prenosy údajov), ktoré sú rozšírené o detailné vymedzenie úloh, právomocí a kompetencií dozorných orgánov vrátane nových spôsobov a schém spolupráce pri výkone dozoru dozornými orgánmi tzv. mechanizmus *one-stop-shop* (články 60 a nasledujúce),[17] splnomocnenia pre členské štáty, pokiaľ ide o prijatie vnútroštátnych výnimiek, obmedzení, špecifikáciu a úpravu osobitných situácií (vyvážanie práva na informácie a ochrany osobných údajov, spracúvanie na účely vedeckého výskumu a ďalšie).

Nariadenie takto reaguje na potrebu jednotnej celoeurópskej úpravy spracúvania osobných údajov, ktorá má vyhovieť potrebám jednotného digitálneho trhu a celkovo trendom, ktoré vedú ku globalizácii podnikania, zvýšeniu prenosov údajov medzi členskými štátmi a do tretích krajín, ako aj novým spôsobom spracúvania (najmä využívanie cloudových služieb). Týmto požiadavkám už nevyhovovala roztrieštenosť spôsobená odlišnými implementáciami smernice vo vnútroštátnych

[16] § 54 ods. 1 *zákona o zdravotních službách* definuje elektronickú podobu/podobu nasledovne: *„V elektronické podobě je zdravotnická dokumentace pořizována, zpracovávána, ukládána a zprostředkovávána v digitální formě s využitím informačních technologií.*“ V porovnaní so slovenskou právnou úpravou ide o výrazný posun pri odstraňovaní konfúzií ohľadom toho, čo považovať a čo nepovažovať za elektronickú podobu zdravotnej dokumentácie.

[17] Sem patrí aj zriadenie nového orgánu, *Evropského sboru pro ochranu osobních údajů* / Európskeho úradu pre ochranu údajov (článok 68 an. Nariadenia).

zákonoch členských štátov, ako sme demonštrovali aj na príklade slovenského a českého zákona o ochrane osobných údajov.

V súvislosti s nariadením sa najviac pozornosti dostáva informáciám o „nových" povinnostiach *správců*/prevádzkovateľov a *zpracovatelů*/sprostredkovateľov, ako aj podstatnému navýšeniu možných sankcií za porušenie nariadenia. Nemožno však inak než súhlasiť s názorom autorov len nedávno vydaného komentára k nariadeniu v tom, že zmeny, ktoré nariadenie prináša, nie sú až tak prelomové.[18] Zásady spracúvania vymedzené smernicou vrátane právnych základov ostávajú zachované, dochádza skôr k precizovaniu jednotlivých práv a povinností (napr. práva na výmaz) a odstráneniu šedej zóny, najmä v oblasti bezpečnostných opatrení jasným zakotvením určitých inštitútov (*pověřenec pro ochranu údajů* / zodpovedná osoba, posudzovanie vplyvu na ochranu údajov, notifikačná povinnosť oznamovať porušenia). Implementácia nariadenia (odhliadnuc od práce s týmto právnym predpisom) sa môže zdať náročnejšia (a nákladnejšia) tým, ktorí tejto sfére svojich povinností doteraz (aj kvôli relatívne nízkym pokutám) venovali malú respektíve žiadnu pozornosť.

Samozrejme, nariadenie nie je dokonalým právnym predpisom. Možno na ňom nájsť celý rad nedokonalostí. Od zmieňovanej systematiky, ktorá je síce štandardná, ale neznáma oku bežného adresáta normy, cez ďalšie ešte zásadnejšie výhrady.[19]

Tie smerujú, po prvé k tomu, že mnohé ustanovenia nariadenia sú metaforické, nedostatočne špecifické, pripomínajúc potom smernicu, ktorá ale na rozdiel od nariadenia pripúšťa/ukladá povinnosť implementácie vnútroštátnym predpisom. To je v prípade nariadenia, priamo aplikovateľného právneho aktu Európskej únie, vylúčené zákazom duplicity medzi nariadením a vnútroštátnym právom. Dôvody možno hľadať v chýbajúcom politickom konsenze (napr. otázka stanovenia veku maloletého, ktorý môže udeliť súhlas so spracúvaním osobných údajov informačnou spoločnosťou). Druhou možnosťou je aj aplikácia inej regulačnej metódy, ktorá vychádza z predpokladu, že zámer regulátora a regulovaného nie je v konflikte, vychádzajúca z predpokladu, že regulovaný má záujem na spolupráci a dodržiavaní pravidiel vo svojom vlastnom záujme.[20] Výsledný stav je taký, že právna úprava čiastkových otázok spojených s určitými inštitútmi (napr. odborná príprava zodpovednej osoby) úplne absentuje alebo nariadenie explicitne pripúšťa špecifikáciu podmienok v práve členského štátu. To ale môže mať nežiaduce dopady na aplikáciu nariadenia v reálnych podmienkach a tiež v istom zmysle koliduje so základnými cieľmi nariadenia, medzi ktoré patrí voľný tok údajov a harmonizované/jednotné uplatňovanie pravidiel vo všetkých členských štátoch. Flagrantným príkladom je ponechanie určenia veku dieťaťa (maloletého) spôsobilého na vyjadrenie súhlasu s používaním služieb informačnej spoločnosti podľa článku 8 Nariadenia na právnu úpravu jednotlivých členských štátov. Odhliadnuc od problému s overovaním veku, vytvára pre správcov/prevádzkovateľov problém so zisťovaním uplatňovaného práva v každom jednotlivom prípade.

Absencia konkrétnych podmienok spracúvania sa dotkla aj spracúvania genetických údajov, biometrických údajov a údajov týkajúcich sa zdravia (článok 9 ods. 4 Nariadenia). V tomto prípade ale

[18] NULÍČEK, Michal a kol. *GDPR / Obecné nařízení o ochraně osobních údajů (2016/679/EU) – Praktický komentář*. Praha: Wolters Kluwer, 2017, s. XIII–XVIII.

[19] Jednou z výhrad je aj preklad Nariadenia do jazykov členských štátov, ktorý sa líši svojou precíznosťou a dokonca významom (!) aj medzi blízkymi jazykmi, akými je český a slovenský jazyk. Porovnaj napr. znenie článku 10 Nariadenia.

[20] Za tento komentár a postreh vďačím doc. JUDr. Radimovi Polčákovi.

nejde o bezprecedentný prípad chýbajúceho konsenzu o celoeurópskej právnej úprave z dôvodu existencie citlivých etických otázok, ktoré sú aj v závislosti od kultúrnych a historických faktorov upravené v jednotlivých členských štátoch odlišne prípadne ich regulácia (zámerne) absentuje.[21]

Ďalšiu výhradu možno formulovať voči nedostatku technologickej neutrality Nariadenia, ktoré vychádza z reakcie na existenciu informačných spoločností a *big data* a zabúda na to, že svet technológií sa vyznačuje extrémnou dynamickosťou, ktorá sa môže spätne prejaviť v rýchlom „zastaraní" až obsoletnosti niektorých inštitútov upravených nariadením. Ďalším následkom je aj to, že týmto zameraním na „globálne" cezhraničné spracúvanie Nariadenia len minimálne reaguje na potreby miliónov mikro, malých a stredných podnikov, ktoré osobné údaje spracúvajú v menšom či väčšom rozsahu. Zákonodarcovia vidia možné riešenie v širšom uplatnení mäkkej regulácie (*soft law*),[22] tá ale nemusí predstavovať zázračný liek na všetko a pre všetky členské štáty. Najmä nie tam, kde sú žiaduce jasné, právne záväzne a jednotne vynucované pravidlá.

Napokon stojí za zmienku v súvislosti s nariadením, že dochádza k posunu regulácie ochrany osobných údajov k hlbšiemu zakotveniu v teórii ľudských práv a rozšíreniu pôsobnosti o niekdajší tretí pilier. Smernica 95/46/ES mala prioritne za cieľ odstránenie prekážok pre voľný trh, výmenu tovaru a služieb. Hoci sa odkazovala na dodržiavanie základných práv, akcent na ľudskoprávny presah nie je až taký dôrazný. Nariadenie sa oproti tomu už v Recitáli 1 a neskôr v článku 1 ods. 2 Nariadenia odkazuje na základné právo na ochranu osobných údajov upravené v článku 8 ods. 1 Charty základných práv Európskej únie a dopad na základné práva a slobody je reflektovaný vo viacerých inštitútoch (oznámenie porušenia ochrany osobných údajov, posúdenie vplyvu na ochranu údajov). Tento posun k hlbšiemu zasadeniu ochrany osobných údajov do teórie ľudských práv sa prejavuje tiež rastúcim významom a počtom súdnych rozhodnutí Súdneho dvora Európskej únie v otázkach ochrany osobných údajov,[23] ako aj zväčšovaním rozdielu medzi reguláciou ochrany osobných údajov v Spojených štátoch amerických a Európe.

3.1 Dopady nariadenia 2016/679 na spracúvanie osobných údajov pri poskytovaní zdravotnej starostlivosti

3.1.1 Zásady a podmienky spracúvania

Ako už bolo niekoľkokrát spomenuté, základné zásady a podmienky spracúvania osobných údajov ostávajú v nariadení zachované (článok 5 a článok 6 Nariadenia). Pre oblasť poskytovania zdravotnej starostlivosti to znamená, že väčšina spracúvaní sa môže (a bude) naďalej realizovať bez súhlasu subjektu údajov (pacienta), vzhľadom na to, že pôjde o spracúvanie upravené osobitným (špeciálnym) zákonom. Pôjde teda buď o spracúvanie:

[21] Ako ďalšie príklady možno uviesť právny status embrya *in vitro* a jeho právna ochrana, surogátne (náhradné materstvo), darcovstvo pohlavných buniek, povolenie výskumu na embryonálnych kmeňových bunkách, prístup k asistovanej reprodukcii partnermi rovnakého pohlavia. Pozri napr. rozhodnutie Veľkej komory.

[22] Panel venovaný téme spolupráce úrad na ochranu osobných údajov. *Svetová konferencia komisárov pre ochranu osobných údajov*. Marrakesh, Maroko. 18. 10. 2016.

[23] Pozri napr. Rozsudok Súdneho dvora (druhá komora) z 27. septembra 2017. *Peter Puškár proti Finančnému riaditeľstvu Slovenskej republiky a Kriminálnemu úradu finančnej správy*. C-73/16, Rozsudok Súdneho dvora (druhá komora) z 19. októbra 2016. *Patrick Breyer proti Spolkovej republike Nemecko* (Bundesrepublik Deutschland). C-582/14.

a) nevyhnutné na splnenie právnej povinnosti [článok 6 ods. 1 písm. c) nariadenia], alebo
b) nevyhnutné na splnenie úlohy vo verejnom záujme alebo výkon verejnej moci zverenej prevádzkovateľovi/správcovi [článok 6 ods. 1 písm. e) nariadenia].

V podstate výnimočne, z dôvodu potreby preukázať nevyhnutnosť takéhoto spracúvania, je možné uplatniť právny základ spracúvania nevyhnutného na účely ochrany životne dôležitého záujmu subjektu údajov [článok 6 ods. 1 písm. d) nariadenia]. Rovnako v menšom počte prípadov prichádza do úvahy spracúvanie osobných údajov na účely zmluvy alebo spracúvanie nevyhnutné na účely oprávneného záujmu, ktorý sleduje *správce* alebo tretia strana, pričom tento záujem nesmie prevážiť nad základnými právami a slobodami subjektov údajov [článok 6 ods. 1 písm. f) nariadenia].

K zmenám nedochádza ani v definícii *správce*/prevádzkovateľa a *zpracovatele*/sprostredkovateľa (článok 4 bod 7 a 8), a teda za *správce* sa považuje naďalej ten (fyzická alebo právnická osoba, orgán verejnej moci), ktorý sám alebo spoločne s inými určí účel a prostriedky spracúvania; prípadne jeho určenie ako *správce* vyplýva z práva členského štátu alebo práva Únie. V kontexte zdravotnej starostlivosti ním bude poskytovateľ zdravotných služieb / poskytovateľ zdravotnej starostlivosti, nie samotný zdravotnícky pracovník. Za *zpracovatele* je naďalej považovaný ten (fyzická alebo právnická osoba, orgán verejnej moci), kto spracúva osobné údaje v mene *správce*/sprostredkovateľa. Sem môžu patriť napríklad laboratóriá alebo aj účtovníci, pokiaľ poskytovateľ tieto služby zabezpečuje prostredníctvom inej ako pracovnej zmluvy.

Pokiaľ ide o zásady spracúvania, ani tu nemožno pozorovať zásadnú zmenu, hoci je potrebné zdôrazniť, že k princípom upraveným smernicou pribudol princíp zodpovednosti (ktorý subsumuje zásadu transparentnosti) (článok 5 ods. 2 nariadenia), podľa ktorého je *správce*/prevádzkovateľ zodpovedný za súlad (dodržiavanie) zásad stanovených nariadením a musí vedieť tento súlad preukázať. Z pohľadu výkonu dozoru ide o podstatnú zmenu, ktorá uľahčuje vynucovanie dodržiavania zásad spracúvania vymedzených nariadením. Z pohľadu *správce*/prevádzkovateľa respektíve poskytovateľa zdravotných služieb to znamená predovšetkým zvýšenie nárokov na reálnu implementáciu zásad (článok 5 ods. 1 nariadenia), bezpečnostných opatrení (článok 32 nariadenia) a vedenie dokumentácie preukazujúcej tieto skutočnosti (minimálny rozsah predstavujú záznamy o spracovateľských činnostiach/*záznamy o činnostech zpracování* podľa článku 30 nariadenia). V zmysle dodržiavania zásad je preto pozitívne hodnotiť právnu úpravu vedenia zdravotnej dokumentácie v zákone o *zdravotních službách*, ktorá reflektuje:

- *zásadu správnosti údajov* [článok 5 ods. 1 písm. d) nariadenia] napr. v ustanovení § 55 písm. g) zákona, ktorý vyžaduje prevedenie dokumentov z listinnej podoby do digitálnej podoby,
- *zásadu bezpečnosti*: vymedzením rozsahu oprávnení oprávnených osôb (jednotlivých zdravotníckych pracovníkov prípadne osôb, ktorý majú dokumentáciu k dispozícii) či uložením povinnosti zabezpečiť údaje proti zmene a logovaním [§ 55 písm. a) *zákona o zdravotních službách*],
- *právo na prenosnosť údajov* (článok 20 nariadenia) reflektovaný v povinnosti viesť systém tým spôsobom, že umožňuje vytvorenie špeciálnej kópie vo formáte čitateľnom a spracovateľnom aj v inom informačnom systéme [§ 55 písm. i) *zákona o zdravotních službách*].

Z hľadiska podmienok spracúvania údajov týkajúcich sa zdravia, biometrických a genetických údajov je potom potrebné venovať osobitnú pozornosť podmienkam určeným domácou vnútroštátnou úpravou (napr. *občanský zákoník*, transplantačné zákony, *zákon o zdravotních službách*).

Vyššie uvedené by pre poskytovateľa malo znamenať, že *zodpovedne* pristúpi najprv:

1) k identifikácii jednotlivých spracúvaní, ktoré sa ho týkajú (okrem vedenia zdravotnej dokumentácie, najmä mzdová a personálna agenda, spracúvanie osobných údajov prostredníctvom diagnostických zariadení, vyhotovovanie kamerových záznamov na zabezpečenie bezpečnosti budovy či spracúvanie biologického materiálu pre diagnostické účely),
2) identifikovaniu účelov a právnych základov spracúvania,
3) zadefinovaniu rozsahu údajov vo vzťahu k účelom spracúvania, najmä tam, kde rozsah nie je jasne vymedzený zákonom, a to z dôvodu dodržania zásady minimalizácie údajov,
4) k určeniu svojho postavenia v spracúvaní, a teda či je *správcem*/prevádzkovateľom alebo *zpracovatelem*/sprostredkovateľom.

Až následne je možné identifikovať dopady nariadenia a prípadné nedostatky (*gaps*) a stanoviť konkrétne kroky na ich riešenie. Posledným krokom by mala byť implementácia týchto krokov spolu so zavedením nových postupov a procesov vyžiadaných nariadením reflektujúcich „realitu spracúvania" konkrétneho poskytovateľa zdravotných služieb.

3.1.2 Bezpečnosť spracúvania

Pokiaľ ide o bezpečnosť spracúvania, v tejto oblasti došlo k precizovaniu radu inštitútov respektíve k ich plošnému/jednotnému zavedeniu do všetkých spracúvaní realizovaných v rámci pôsobnosti nariadenia (článok 2 nariadenia). Zároveň ide o jeden z významne diskutovaných aspektov nariadenia reálne dopadajúcich takmer na všetkých *správcov a zpracovateľov* osobných údajov. Nižšie sa budeme venovať dvom povinnostiam/inštitútom:

a) *ohlašování případů porušení zabezpečení osobních údajů* / oznámenie o porušení ochrany osobných údajov (*data breach notification*),
b) *pověřenec pro ochranu údajů* / zodpovedná osoba.

Ad a) *Ohlašování případů porušení zabezpečení osobních údajů* / oznámenie o porušení ochrany osobných údajov (*data breach notification*)

Ohlášování případů porušení zabezpečení osobních údajů alebo *data breach notification* je povinnosť stanovená *správcům* a *zpracovatelům* článkom 33 a 34 Nariadenia. Ide o jednu zo zásadných zmien pre ich prax, realitu spracúvania spojenú s nariadením, pretože notifikácie nie sú momentálne povinné vo väčšine členských štátov.[24] V menšom rozsahu boli notifikácie realizované na základe ustanovení smernice o súkromí v elektronických komunikáciách, ktoré stanovovali poskytovateľom služieb elektronických komunikácií povinnosť ohlasovať príslušným orgánom bezpečnostné incidenty týkajúce sa osobných údajov.

Nová úprava stanovuje povinnosť v článku 33 ods. 1 Nariadenia ohlásiť/oznámiť: *„Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, (ohlásí) dozorovému úřadu příslušnému podle článku 55, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob."*

[24] Výnimkou je Holandsko, kde sa notifikačná povinnosť vzťahuje na incidenty týkajúce sa osobných údajov.

Povinnosť ohlásiť incident (porušenie údajov) sa dotkne aj poskytovateľov zdravotných služieb/zdravotnej starostlivosti. Mnohí riešili takéto incidenty aj doteraz, bohužiaľ až v rovine dopadov na práva konkrétnych pacientov (výmaz z dokumentácie, modifikácie, strata dokumentácie), ktoré sa zároveň tešili patričnej publicite. Výhoda novej povinnosti pre poskytovateľov preto môže spočívať v poskytnutí vodítok,[25] ako identifikovať bezpečnostný incident, ktorý sa dotýka osobných údajov a ako takéto porušenie riešiť tak, aby bol dopad na práva subjektov údajov minimálny.

Samotné porušenie *zabezpečení osobních údajů* možno definovať vychádzajúc z definície článku 4 ods. 12 Nariadenia ako *„porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů“.*

V prvom kroku by mal ale *správce* identifikovať, či ide o také porušení zabezpečení, ktoré sa týka osobných údajov (*detection*). Až následne môže bližšie určiť povahu (typ) porušenia a jeho následky (predpokladané následky). Ako už naznačuje samotná definícia porušenie sa môže týkať troch základných atribútov (informačnej) bezpečnosti:

1) *dôvernosti údajov* (*confidentiality*) – pri strate, neoprávnenom poskytnutí alebo sprístupnení údajov,
2) *integrity údajov* (*integrity*) – pri neoprávnenej zmene údajov,
3) *dostupnosti údajov* (*availability*) – pri protiprávnom zničení, strate údajov.

V praxi zdravotníckeho zariadenia pôjde predovšetkým o prípady:

1) neoprávneného sprístupnenia zdravotnej dokumentácie (napr. sprístupnenie osobe blízkej, ktorá nato nebola určená pacientom), krádež alebo stratu dokumentácie, kde môže ísť potenciálne o narušenie dôvernosti,
2) *ramsoware* útok, duplicity v dokumentácii, nedopĺňanie papierovej verzie do elektronicky vedenej dokumentácie, poškodenie časti dokumentácie vodou/ohňom,
3) *ramsoware* útok – zablokovanie prístupu k údajom prípadne ich zašifrovanie hackermi, neoprávnené zničenie dokumentácie, krádež dokumentácie.

Správce je následne povinný posúdiť, aké dopady toto porušenie má na práva a slobody subjektov údajov. V prípade rizika, je povinný spraviť ohlásenie dozornému orgánu najneskôr 72 hodín, odkedy sa o incidente dozvedel. *Zpracovatel* je incident povinný oznámiť bezodkladne. V prípade vysokého rizika je potrebné porušenie oznámiť aj subjektu údajov.

Je evidentné, že tieto požiadavky sú náročné na nastavenie procesov:

1) identifikovania incidentov a určenie, či ide o porušenie zabezpečenia ochrany údajov,
2) určenie typu incidentu a jeho dopadu na práva a slobody subjektov údajov,
3) urobiť oznámenie – dozornému orgánu v krátkej lehote, v niektorých prípadoch aj subjektom údajov s niekoľkými výnimkami upravenými v článku 34 ods. 3 Nariadenia.

   V každom prípade, všetky porušenia je *správce*/prevádzkovateľ povinný evidovať (článok 32 ods. 4 Nariadenia).

[25] Pozri PRACOVNÁ SKUPINA ZRIADENÁ PODĽA ČLÁNKU 29. *Guidelines on Personal data breach notification under Regulation 2016/679* [online]. 03. 10. 2017. Dostupné na: <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083> [cit. 23. 11. 2017].

Ad b) *Pověřenec pro ochranu údajů* / zodpovedná osoba

Pověřenec pro ochranu údajů / zodpovedná osoba je ďalším inštitútom zabezpečenia ochrany osobných údajov, ktorý nebol predmetom regulácie a požiadavkou na zabezpečenie v mnohých členských štátoch, vrátane Českej republiky. Náznakom s týmto konceptom pracovala už smernica 95/46/ES, ktorá v článku 18 ods. 2 upravujúcom oznamovaciu povinnosť správcov, pričom *pověřenec* vystupuje ako prostredník medzi dozorným orgánom a *správcem*, znižuje administratívnu záťaž *správce*/prevádzkovateľa a je zodpovedný za výkon povinností *správce* vyplývajúcich z regulácie v oblasti ochrany osobných údajov.

Tento koncept chápajúci *poveřence*/zodpovednú osobu ako prostredníka medzi dozorným orgánom – správcom a verejnosťou/subjektmi údajov ostáva zachovaný, vrátane predpokladov pre výkon tejto činnosti a podmienok pre výkon činnosti (nezávislosť *pověřence* na *správci*/prevádzkovateľovi, nemožnosť vyvodiť osobnú zodpovednosť voči *pověřenci* za porušenie ochrany osobných údajov[26]).

Zmenou je povinnosť obligatórne určiť (*designate*) *poveřence* v každom prípade, kedy:

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 své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo*
c) *hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.*

Z vyššie uvedeného môžeme dovodiť, že táto povinnosť sa bude vzťahovať na „veľké“ zdravotnícke zariadenia, ktorých spracúvania spadajú pod podmienku článku 37 ods. 1 písm. c) Nariadenia.[27] Interpretácii a zrejme už len precizovaniu na základe konkrétnych prípadov ostáva určenie, ako definovať *„rozsáhlé zpracování“*. Usmernenie upresňuje, že môže ísť o spracúvanie rozsiahle lokálne (vo viacerých krajinách), dotýkajúce sa veľkého počtu subjektov alebo typu údajov, hranica nie je dané exaktne. V každom prípade, vždy keď sa správce rozhodne *pověřence* nemenovať/neurčiť, mal by svoje dôvody uviesť v dokumentácii prístupnej dozornému orgánu.

Opäť ako v prípade ohlasovania porušení zabezpečenia ochrany údajov ide o zákonnú požiadavku, ktorá má dopad na náklady a vytvorenie procesov na strane *správce*/prevádzkovateľa. Podľa môjho názoru možno tento vplyv vnímať aj pozitívne v tom zmysle, že ponúka *správci*/prevádzkovateľovi pomoc, ako sa vysporiadať s rastúcimi nárokmi na zabezpečenie ochrany osobných údajov. Pripúšťa sa dokonca menovanie kolektívu osôb alebo právnickej osoby ako *pověřence*/zodpovednej osoby. Ďalším pozitívom, a to pre poskytovateľa zdravotných služieb obzvlášť, je vytvorenie mechanizmu vybavovania sťažností subjektov údajov/dotknutých osôb, ktorý môže

[26] Táto požiadavka je vecou posúdenia konkrétnych prípadov a nedá sa uplatniť absolútne.
[27] PRACOVNÁ SKUPINA ZRIADENÁ PODĽA ČLÁNKU 29. *Určenie zodpovednej osoby* [online]. [cit. 13. 12. 2016]. Dostupné na: <https://www.uoou.cz/nakladani%2Dse%2Dzdravotnickou%2Ddokumentaci/d-1747/p1=1099>.

nadväzovať na povinnosti/požiadavky riešiť sťažnosti spojené s poskytovaním zdravotných služieb / starostlivosti podľa § 93 zákona o zdravotných službách.

3.2 Osobitné situácie spracúvania a otvorené otázky

V krátkosti stoja ešte za zmienku ďalšie oblasti ochrany osobných údajov, ktorých sa dotkne nová regulácia, Nariadenie. Medzi tieto oblasti patrí:

a) posudzovanie vplyvu na ochranu údajov (DPIA),
b) regulácia vedeckého výskumu, ktorý spadá pod tzv. privilegované účely,
c) odlišná právna úprava špecifík spracovania genetických údajov, údajov týkajúcich sa zdravia a biometrických údajov v súlade s článkom 9 ods. 4 Nariadenia,
d) v súvislosti s vyššie uvedeným dopad na prenos osobných údajov, najmä na účely výskumu,
e) využívanie poskytovateľov cloudových služieb pre uschovávanie údajov týkajúcich sa zdravia umiestnených mimo krajinu, kde má pobyt subjekt údajov.

ZÁVER

Ochrana osobných údajov je komplementárnou a rovnocennou súčasťou ochrany súkromia pacienta/fyzických osôb pri poskytovaní zdravotných služieb/zdravotnej starostlivosti, ktorú je potrebné odlíšiť od iných inštitútov ochrany súkromia. Túto oblasť bude od mája 2018 regulovať nový právny predpis, všeobecné nariadenie ochrany údajov (GDPR). Regulácia predstavuje niekoľko zmien, ktoré sa dotknú poskytovateľov zdravotných služieb, zmeny sa však primárne nedotknú zásad a podmienok spracúvania (právnych) základov, ale najmä implementácie zabezpečovacích inštitútov spracúvania. V článku sme sa dotkli dvoch z nich – porušenia zabezpečenia osobních údajov a *pověřence pro ochranu údajů*. Pozornosť by si určite zaslúžilo aj posudzovanie vplyvu na ochranu údajov (DPIA), regulácia vedeckého výskumu podľa nových pravidiel a využívanie poskytovateľov cloudových služieb pre uschovávanie údajov týkajúcich sa zdravia, ktorým sa snáď budeme venovať v niektorom z ďalších článkov.

Z vyššie uvedeného ale vieme vyvodiť, že nariadenie nepredstavuje zásadný prelom v ochrane osobných údajov, skôr precizuje a rozširuje niektoré inštitúty. Jeho dopad na náklady *správců*, ale nie je možné vylúčiť. Náklady na implementáciu sú však predovšetkým časové. Implementácia u konkrétneho *správce* závisí predovšetkým od existujúcich spracúvaní, kategórie spracúvaných údajov, rozsahu spracúvania, ktoré je potrebné v prvom kroku zmapovať a zrevidovať. Právnym základom dominujúcim pri spracúvaní osobných údajov pri poskytovaní *zdravotních služeb* naďalej ostáva zákon, a teda spracúvanie vychádza z toho, že je nevyhnutné pre plnenie právnej povinnosti *správce* prípadne jeho úloh vykonávaných vo verejnom záujme uložených najmä zákonom o *zdravotních službách*. Jeho platné a účinné znenie už teraz reflektuje na mnohé zo zásad spracúvania osobných údajov stanovených Nariadením. Bolo by optimálne, ak by zavádzanie moderných spôsobov spracúvania (*eHealthu*) viedlo k ešte dôslednejšiemu prepájaniu a konzistentnosti právnej úpravy vedenia zdravotnej dokumentácie a nastaveniu integrovaného systému.

Napokon možno konštatovať, že najviac želaným výstupom nariadenia by bolo, ak by sa jeho implementácia nestala len ďalším formalistickým produkovaním súhlasov, informácií a evidencií, ale

viedla k reálnej aplikácii jednotlivých inštitútov do procesov spracúvania poskytovateľov *zdravotnických služeb* a viedla k lepšiemu zabezpečeniu a k ochrane súkromia dotknutých osôb.

REFERENČNÍ SEZNAM:

DOLEŽAL, Tomáš. *Vztah lékaře a pacienta z pohledu soukromého práva*. Praha: Leges, 2012

HUMENÍK, Ivan. – SZANISZLÓ, Vladimír M. – ZOLÁKOVÁ, Zuzana (eds). *Reprodukčné zdravie ženy v centre záujmu*. Bratislava: Wolters Kluwer, 2014

NULÍČEK, Michal a kol. *GDPR / Obecné nařízení o ochraně osobních údajů (2016/679/EU) – Praktický komentář*. Praha: Wolters Kluwer, 2017

ŠIKUTA, Ján. Doktrína „miery voľnej úvahy“ (*The Margin of Appreciation Doctrine*) a judikatúra Európskeho súdu pre ľudské práva v Štrasburgu. *Justičná revue.* 2012, roč. 64, č. 8–9, s. 952–958.