Časopis zdravotnického práva a bioetiky
Journal of Medical Law and Bioethics
Vol 8, No 3 (2018), ISSN 1804-8137, http://www.ilaw.cas.cz/medlawjournal

# Biometrické údaje ve zdravotních aplikacích

## Biometric data in health applications

*JUDr. Mgr. Eva Fialová, LL.M., Ph.D., Ústav státu a práva AV ČR, v. v. i.*

**Abstract:** This article deals with the processing of personal data by the use of applications that monitor and evaluate human health, both consumer-focused applications, and applications used by doctors to assess the patient's health. By means of algorithms, these applications evaluate biometric data collected from users. Because the health applications evaluate a large amount of personal data, the processing of such data involves a risk to the rights and freedoms of individuals. If a controller or processor violates the law on the processing of personal data, the data subject is entitled to compensation for damages resulting from the breach of the data protection regulation.

**Keywords:** algorithms – biometric data – special categories of personal data

**Abstrakt:** Tento článek se zabývá zpracovávání osobních údajů při používání aplikací, které monitorují a vyhodnocují zdravotní stav člověka, a to jak aplikací, které se zaměřují na spotřebitele, tak aplikací, které používají lékaři pro zhodnocení zdravotního stavu pacienta. Tyto aplikace vyhodnocují pomocí algoritmů biometrické údaje shromážděné při používání aplikace uživatelem. Jelikož zdravotní aplikace vyhodnocují velké množství osobních údajů, znamená toto zpracování riziko pro práva a svobody fyzických osob. Pokud správce nebo zpracovatel poruší právní předpisy upravující zpracovávání osobních údajů, má subjekt údajů nárok na náhradu škody, která mu porušením těchto předpisů vznikla.

**Klíčová slova:** algoritmy – biometrické údaje – zvláštní kategorie osobních údajů

## ÚVOD

Spotřebitelé i lékaři se v čím dál větší míře spoléhají na pomoc aplikací, které měří fyzickou kondici uživatele, jeho výkonnost a další aspekty týkající se jeho tělesného stavu a pochodů. V lékařské praxi se používají specializované programy za účelem diagnostiky nemocí a zdravotního stavu pacienta. Aplikace využívané spotřebiteli i lékaři využívají umělou inteligenci k vytvoření požadovaného výstupu.[1] Příkladem aplikace zaměřené na spotřebitele je *Fitbit* měřící tělesnou aktivitu, váhu nebo spánek svého uživatele.[2] Na spotřebitele se specifickými zdravotnickými problémy, jako je cukrovka, jsou zaměřeny specializované aplikace vyhodnocující určitá data vztahující se k takovému zdravotnímu problému. Další kategorií zdravotních aplikací jsou zdravotnické prostředky používané lékaři, kupříkladu digitální dermatoskop.[3] Poskytovatelé těchto aplikací zpracovávají biometrické údaje uživatele jako je srdeční tep, krevní tlak, hladina cukru v krvi apod., které nejsou určeny k identifikaci uživatele, nýbrž ke zhodnocení jeho zdravotní kondice nebo jeho chování. Z těchto biometrických údajů mohou být sestavovány biometrické profily a následně na základě těchto profilů může být hodnocen zdravotní stav. Zpracovávané biometrické údaje se v těchto aplikacích nepoužívají zpravidla k identifikaci subjektu údajů. Z biometrických údajů lze odvodit údaje o zdravotním stavu. Poskytovatelé zdravotních aplikací tedy zpracovávají citlivé údaje, neboli podle terminologie nařízení Evropského parlamentu a Rady (EU) 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. Zpracování těchto údajů může zasáhnout do základních práv a svobod subjektu údajů. Poskytovatelé zdravotních aplikací jsou povinni zpracovávat osobní údaje v souladu s nařízením. Ne všechny zdravotní aplikace právní předpisy na ochranu osobních údajů dodržují. Podle nedávného výzkumu porušovala většina zdravotních aplikací, které si uživatelé mohli stáhnout zdarma do mobilního telefonu (tzv. *mhealth*), předpisy na ochranu osobních údajů, čímž mohlo dojít k zásahu do práva na soukromí uživatelů, zejména předáním údajů o zdravotním stavu a zdravotních symptomech třetím osobám.[4] V tomto článku se zaměříme na analýzu povinností poskytovatele zdravotních aplikací podle nařízení a odpovědnost tohoto poskytovatele, pokud nezpracovává osobní údaje v souladu s nařízením a toto porušení povinností má za následek zásah do základního práva subjektu údajů.

[1] LINCOLN, Tsang – KRACOV, Daniel A. – MULRYNE, Jacqueline et al. The Impact of Artificial Intelligence on Medical Innovation in the European Union and United States. *Intellectual Property & Technology Law Journal*. 2017, Vol. 29, No. 8. Dostupné z: https://www.arnoldporter.com/~/media/files/perspectives/publications/2017/08/the-impact-of-artificial-inteelligence-on-medical-innovation.pdf.

[2] *Fitbit* [online]. [cit. 2018-08-11]. Dostupné z: https://www.fitbit.com/eu/home.

[3] KRAJSOVÁ, Ivana. Využití dermatoskopie a digitální dermatoskopie v diagnostice melanomu. *Dermatologie pro praxi*. 2011, roč. 5, č. 1., s. 23. Dostupné z: https://www.dermatologiepropraxi.cz/pdfs/der/2011/01/06.pdf.

[4] PAPAGEORGIOU, Achilleas – STRIGKOS, Michael – POLITOU, Eugenia – ALEPIS, Efthimios – SOLANAS, Agusti – PATSAKIS, Constantinos. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access* [online]. 2018, Vol. 6. [cit. 2018-11-04]. Dostupné z: https://ieeexplore.ieee.org/document/8272037.

## 1. BIOMETRIE A BIOMETRICKÉ ÚDAJE

Biometrie se vztahuje k pojmu měřitelnosti, jelikož udává měřitelné fyzikální a biologické vlastnosti člověka.[5] Morandi a Tzovaras rozlišují silnou, jemnou a slabou biometrii. Silnou biometrií (*strong biometrics*) rozumí rysy, které můžeme považovat za jedinečné a trvalé, jako jsou otisky prstů, duhovky, struktura žil atd. Jemná biometrie (*soft biometrics*) je méně stabilní než silná biometrie. Jemná biometrie se musí vždy posuzovat podle kontextu, času nebo místa, kde se daná osoba nachází. Jemná biometrie zahrnuje prvky, jako jsou gesta, chůze, dynamika obličeje nebo srdeční činnost. Slabá biometrie (*weak biometrics*) představuje rysy, které nelze primárně přiřadit konkrétní osobě (barva očí, rasa nebo pohlaví).[6] Význam a použití biometrie se postupně mění. Od identifikace, která byla donedávna primárním účelem biometrie, ke screeningu, čili k měření a hodnocení fyziologických rysů.

Biometrika bývá rozlišována na biometriku první a druhé generace. Pro první generaci biometriky byla typická identifikace člověka, tedy odpověď na otázku, kdo jste. Druhá generace biometriky si klade důraz na screening a hodnocení, tudíž na otázku, jak jste. Druhá generace biometriky se již v takové míře nezabývá údaji, které se vztahují k identitě jednotlivce, ale zaměřuje se na člověka, na jeho úmysly a projevy těchto úmyslů.[7]

*„Druhá generace biometriky odkazuje na novou vlnu biometrických technologií, které mají za cíl přiblížit se k tomu, aby mohly napodobovat způsob, jakým se lidé identifikují a jak se sobě prokazují. To jest, prostřednictvím rozpoznání jednotlivých rysů a průběžné analýze jedinečné dynamiky těla, která může být zachycena v ‚reálném čase' a nenápadně ve smyslu, že nutně nevyžaduje, aby se jednotlivec zastavil u stroje, který umožňuje proces skenování. Tyto biometrie mají tendenci soustředit se na méně persistentní (slabší) rysy než standardní biometrie (jako jsou otisky prstů nebo skenování duhovky) a často mají sklony se měnit v průběhu času. Ačkoli se druhá generace biometrie zaměřuje na rysy, které jsou nestabilní a méně rozlišující, mohou být úspěšně využity k jakémukoli druhu rozpoznávání, od autentizace, identifikace až po screening, zvláště v případě, že několik biometrických prvků je spojeno do multimodálního systému, který zohledňuje najednou několik různých biometrických prvků*."[8]

Druhá generace biometrických prvků může být použita k získání informací o zdravotním stavu jednotlivce. Zdravotní stav lze odvodit z různých biometrických charakteristik nebo porovnáním změn jednoho biometrického znaku. Informace o zdraví mohou být shromažďovány zjevně nebo dokonce skrytě bez vědomí jednotlivce o možném získávání údajů o zdravotním stavu,[9] pokud aplikace shromažďuje taková biometrická data, jejichž kombinací lze zdravotní stav dovodit bez toho, aniž by uživatel o tomto druhu zpracování věděl.

[5] MORANDI, Emilio – TZOVARAS, Dimitros. *Second Generation Biometrics: The ethical, Legal and Social Context.* Dordrecht: Springer, 2011, s. 7.
[6] Ibidem, s. 8.
[7] Ibidem, s. 11.
[8] MORDINI, Emilio – ASHTONS, Holly. The Transparent Body: Medical Information, Physical Privacy and Respect for Body Integrity. In: MORANDI, Emilio – TZOVARAS, Dimitros. *Second Generation Biometrics: The ethical, Legal and Social Context*. Dordrecht: Springer, 2011, s. 262.
[9] Ibidem, s. 259.

Na základě konceptu biometriky první a druhé generace můžeme rozlišovat biometrické údaje na biometrické údaje v širším a užším smyslu. Biometrickými údaji v širším smyslu jsou údaje týkající se fyziologické nebo biologické charakteristiky člověka. Tyto údaje nemusí nutně identifikovat jednotlivce. Biometrické údaje v širším smyslu referují o chování, záměru, nebo fyzickém stavu. Biometrické údaje v užším smyslu jsou údaje, které umožňují identifikaci osoby. Tyto biometrické údaje jsou definovány v nařízení. Podle čl. 4 (14) GDPR jsou biometrické údaje osobní údaje vyplývající z konkrétního technického zpracování týkajícího se fyzických nebo fyziologických znaků nebo vlastností fyzické osobnosti, které umožňují nebo potvrzují jedinečnou identifikaci, například obraz obličeje nebo daktyloskopické údaje. Biometrické údaje za účelem jednoznačné identifikace fyzické osoby jsou citlivé údaje podle čl. 9 GDPR, nebo podle terminologie GDPR zvláštní kategorie údajů.

Pokud údaje neumožňují nebo nepotvrzují jednoznačnou identifikaci osoby, budou tyto údaje osobními údaji, nikoliv biometrickými údaji v užším smyslu – tedy biometrickými údaji ve smyslu GDPR. Přestože data, která neumožňují nebo nepotvrzují jedinečnou identifikaci, nejsou biometrickými údaji ve smyslu GDPR, jsou tyto údaje stále osobními údaji podle čl. 4 odst. 1 nařízení. Osobní údaje jsou informace o identifikované nebo identifikovatelné fyzické osobě. Za předpokladu, že biometrické údaje v širším smyslu odkazují na zdravotní stav jednotlivce, spadají do zvláštní kategorie údajů ve smyslu GDPR.

Aplikace o zdravotním stavu můžeme rozlišit na tři základní kategorie. První z nich se zaměřuje na osobní motivaci a vlastní sledování, druhá kategorie je určena lékařům a třetí kategorii využívají pacienti se specifickými zdravotními problémy a potřebami. Do první kategorie aplikací náleží již zmiňovaný *Fitbit* nebo *Nokia Health*.[10] Příkladem druhé kategorie aplikací je výše uvedený digitální dermatoskop. Jako příklad třetí kategorie aplikací mohou sloužit aplikace pro pacienty s diabetem, jako je *hedia* nebo *MecicScan*. Poskytovatelé aplikací vesměs uvádějí, že zpracovávají osobní údaje týkající se určité fyziologické hodnoty. Pomocí aplikace jsou proto zpracovávány biometrické údaje v širším smyslu. Z těchto hodnot lze odvodit informace o zdravotním stavu uživatele nebo pacienta. Aplikace *Fitbit* sleduje osobní zvyky a cvičení uživatele. Aplikace shromažďuje údaje o jídle, hmotnosti, spánku, tekutinách a ženském zdraví za účelem odhadu různých ukazatelů.[11] „*Vaše zařízení shromažďuje data, aby odhadlo různé metriky, jako je počet kroků, které jste podnikli, překonanou vzdálenost, spálené kalorie, hmotnost, srdeční frekvence, stupně spánku, aktivní minuty a polohu.*"[12] Stejně tak *Nokia Health* shromažďuje prostřednictvím svých zdravotních produktů údaje jako hmotnost, objem svalů, tělesný tuk, srdeční frekvenci, rychlost dýchání, krevní tlak a tělesnou teplotu uživatele.[13] Třetí

[10] *Nokia Health* [online]. [cit. 2018-08-11]. Dostupné z: https://health.nokia.com/cz/en/.
[11] Fitbit Privacy Policy. *Fitbit* [online]. [cit. 2018-08-11]. Dostupné z: https://www.fitbit.com/eu/legal/privacy-policy#info-we-collect.
[12] Ibidem.
[13] Your Privacy when Using Nokia Health Products and Services. *Nokia Health* [online]. [cit. 2018-08-11]. Dostupné z: https://health.nokia.com/cz/en/legal/privacy-policy-supplement.

kategorie aplikací zpracovává údaje související s konkrétním onemocněním. V kontextu pacientů s diabetem se zpracované údaje týkají hodnoty glukózy v krvi.[14]

Na základě biometrických údajů lze sestavovat biometrické profily za účelem určení zdravotního stavu osoby nebo lékařské diagnózy.[15] Vstupní informace používané pro sestavování profilů mohou pocházet z lékařských studií nebo/a z kombinování, analýzy a porovnání údajů získaných od uživatelů aplikace. Údaje jsou předávány partnerům, kteří poskytují *Fitbit, Inc.* mimo jiné analýzu dat, výzkum a nejrůznější průzkumy.[16] Ke stejným účelům jsou biometrické údaje sdílené s třetími stranami společností Nokia.[17]

## 2. ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ VE ZDRAVOTNICKÝCH APLIKACÍCH

Poskytovatel, který službu zaměřuje přímo na spotřebitele a zpracovává osobní údaje těchto spotřebitelů, je správcem podle čl. 4 bod 7) GDPR. Pokud je aplikace nabízena a používána lékařem, je poskytovatel v pozici zpracovatele, neboť správcem osobních údajů svých pacientů je lékař, který tyto údaje zpracovává pro účely poskytování lékařské péče. Lékař používá zdravotní aplikaci nejčastěji v podobě zdravotnického prostředku pro účely diagnostiky nebo léčby svých pacientů. Poskytovatel zdravotní aplikace tak poskytuje lékaři nástroj k výše uvedeným účelům a zároveň zpracovává pro lékaře osobní údaje jeho pacientů. Je to lékař, kdo určuje účel a prostředky zpracování. Určení účelu a prostředků zpracování je definičním znakem správce. Správce a zpracovatel spolu musí mít uzavřenu zpracovatelskou smlouvu podle čl. 28 GDPR. Tato smlouva by měla zavazovat zpracovatele, aby při zpracování zohlednil povahu osobních údajů, zvláště aby přijal technická a organizační opatření odpovídající míře rizika porušení zabezpečení u zvláštní kategorie údajů.

Jestliže bude mít poskytovatel vlastní účel zpracování osobních údajů, bude samostatným správcem či bude spolu s lékařem v pozici společného správce podle čl. 26 GDPR. O samostatné správce se bude jednat, pokud každý správce určuje *„jiný účel a jiné prostředky a samostatně má kontrolu nad tím, jaké údaje, za jakým účelem a jakým způsobem budou zpracovávané […] pouhý fakt, že se na zpracování podílí více subjektů, neznamená, že se jedná o společné správce“.*[18] Společné správcovství znamená, že oba správci *„rozhodují o zásadních aspektech, jako jsou cíl zpracování, rozsah zpracovávaných údajů, jak dlouho budou údaje zpracovávané či kdo k nim bude mít přístup*“.[19] O samostatné správce by se jednalo, pokud by účelem zpracování osobních údajů bylo kupříkladu zlepšování funkcí aplikace, respektive výstupů generovaných algoritmem na bázi strojového učení,

[14] Terms and conditions of web use. *Medicsen* [online]. [cit. 2018-08-12]. Dostupné z: https://www.medicsen.com/en/privacy_policy, nebo Terms and Conditions for your use of the Hedia Application. *Hedia* [online]. [cit. 2018-08-12]. Dostupné z: http://hedia.dk/terms-and-conditions/.

[15] ANDRONIKOU, Vassiliki – YANNOPOULOS, Angelos – VARVARIGOU, Theodora. Biometric Profiling: Opportunities and Risks. In: HILDEBRANDT, Mireille – SERGE, Gutwirth. *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer, 2008, s. 132.

[16] *Fitbit Privacy Policy*.

[17] Privacy Policy. *Nokia Health* [online]. [cit. 2018-08-11]. Dostupné z: https://www.nokia.com/en_int/privacy.

[18] PATTYNOVÁ, Jana – SUCHÁNKOVÁ, Lenka – ČERNÝ, Jiří a kol. *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. Praha: Leges, 2018, s. 232.

[19] Ibidem.

pokud by k tomuto účelu poskytovatel aplikace zpracovával osobní údaje. Jestliže jsou tyto údaje anonymizované, tedy podle bodu odůvodnění 26 GDPR, pokud subjekt údajů není nebo již přestal být identifikovatelným, nařízení se na zpracování těchto údajů vztahovat nebude. Anonymizace musí být účinná tak, aby poskytovatel nemohl ze souboru údajů identifikovat konkrétní osobu.[20]

Některé povinnosti podle GDPR jsou směrovány pouze na správce, zatímco jiné se vztahují na zpracovatele, stejně jako na správce osobních údajů. Poskytovatel aplikace, ať již v pozici správce nebo zpracovatele, musí dodržovat evropskou legislativu v oblasti ochrany osobních údajů, a to i v případě, že není usazen v členském státě EU, pokud zpracovává osobní údaje subjektů údajů, kteří se nacházejí v Unii, a pokud činnosti zpracování souvisejí s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, nebo tyto činnosti spočívají v monitorování jejich chování, pokud jde o jejich chování v EU (čl. 3 GDPR). V případě poskytovatele zdravotní aplikace bude přítomna jak nabídka služeb, tak monitorování chování. Pokud poskytovatel není usazen v EU, musí jmenovat zástupce jako kontakt pro subjekty údajů a místní orgány pro ochranu údajů (čl. 27 GDPR). Určený zástupce by měl být v souladu s bodem odůvodnění 80 podroben vymáhacímu řízení v případě nedodržení předpisů.

Vedle určení zástupce v případě správce, který není usazen v EU, stanoví GDPR správci řadu dalších povinností. Přestože data zpracovávaná prostřednictvím zdravotní aplikace nejsou zpravidla biometrickými údaji ve smyslu GDPR, spadají tyto údaje stále do kategorie zvláštní kategorie údajů týkajících se zdraví. Podle SDEU je pojem údaje o zdraví třeba vykládat široce. Údaje o zdraví zahrnují informace týkající se všech stránek zdraví člověka, ať fyzických či duševních.[21] Pracovní skupina zřízená podle čl. 29 směrnice 46/95/ES (dále jen „Pracovní skupina 29“) platné a účinné do 24. 5. 2018 považuje údaje o zdraví za širší kategorie údajů než pouhé zdravotní údaje (*medical data*). Mezi údaje o zdraví řadí Pracovní skupina 29 údaje o návycích a zvycích subjektu údajů, údaje získané měřením tělesných pochodů, či údaje, ze kterých se dá odvodit riziko vzniku onemocnění, přestože vstupní údaje nemusí mít samy o sobě povahu údajů o zdraví.[22] Bod 35 odůvodnění GDPR zahrnuje mezi údaje o zdraví mimo jiné i údaje o fyziologickém stavu subjektu údajů.

Správce, který nabízí aplikaci spotřebiteli, zpracovává údaje o zdraví na základě výslovného souhlasu (čl. 9 odst. 2 písm. a) GDPR). Výslovný souhlas znamená výslovné vyjádření vůle subjektu. Pokud je aplikace zaměřena na lékaře, údaje jsou zpracovány podle čl. 9 odst. 2 písm. h) GDPR tedy, že zpracování je nezbytné pro účely lékařské diagnostiky, poskytování zdravotní nebo sociální péče nebo léčení na základě právních předpisů EU nebo členských států nebo na základě smlouvy se zdravotnickým pracovníkem a podléhající povinnosti profesního tajemství. Zákonným důvodem zpracování je v tomto případě plnění právní povinnosti správce dle čl. 6 odst. 1 písm. c) GDPR. Právní

[20] PRACOVNÍ SKUPINA 29. Stanovisko č. 5/2014 k technikám anonymizace (WP216) [online]. [cit. 2018-11-01], s. 9. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf.

[21] Rozsudek Soudního dvora Evropské unie ze dne 6. listopadu 2003, věc č. C-101/01 (*Lindqvist*).

[22] Příloha k dopisu Pracovní skupiny 29 ze dne 5. 2. 2015. *Europa* [online]. 2015 [cit. 2018-08-20]. Dostupné z: http://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

povinnost je v tomto případě stanovena zákonem č. 372/2011 Sb., o zdravotních službách a o podmínkách jejich poskytování (zákon o zdravotních službách).

Další povinnosti správce jsou uvedeny v čl. 5 GDPR. Správce musí zpracovávat osobní údaje pro určité, výslovně vyjádřené a legitimní účely. Osobní údaje nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný. Typickým účelem zpracování v případě použití zdravotní aplikace je poskytnutí služby spotřebiteli spočívající v monitorování a vyhodnocování jeho biometrických údajů společně s marketingovými účely. V případě využívání aplikace lékařem, je účelem lékařská diagnostika. Dalším účelem těchto aplikací, které spotřebitelé nebo lékaři používají, je vědecký výzkum. Tento účel není neslučitelný s původními účely za předpokladu, že jsou přijata vhodná opatření k zajištění práv a svobod subjektu údajů a zásady minimalizace údajů. Osobní údaje musí dále být přesné a nesmí být uchovávány po delší časové období, než je nezbytné pro tyto účely s výjimkou výzkumných účelů.

Nařízení dává subjektu údajů řadu práv, jimž musí správce vyhovět. Jedná se zejména o informační povinnost vůči subjektům údajů podle čl. 13 GDPR, která je v případě zdravotních aplikací zaměřených přímo na spotřebitele splněna zpravidla zveřejněním tzv. podmínek ochrany osobních údajů na webových stránkách poskytovatele. Dalšími právy subjektu údajů jsou práva na přístup k osobním údajům podle čl. 15 GDPR, právo na opravu podle čl. 16 GDPR a právo na výmaz dle čl. 17 GDPR. Právo na výmaz má mimo jiné subjekt údajů, který odvolal svůj souhlas se zpracováním. Právo na výmaz naopak nesvědčí subjektu údajů, jehož osobní údaje v podobě výstupů vygenerovaných pomocí zdravotní aplikace, jsou zpracovány ve zdravotnické dokumentaci lékaře, neboť lékař zpracovává tyto osobní údaje z titulu plnění právní povinnosti správce. V případě tohoto právního titulu pro zpracování subjekt údajů právo na výmaz nemá. Subjekt údajů, jehož údaje o zdraví nejsou zpracovávány lékařem za účelem poskytnutí zdravotních služeb má právo na přenositelnost údajů, čili právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, podle čl. 20 GDPR. Subjekt údajů může právo na přenositelnost vůči poskytovateli zdravotní aplikace uplatnit ohledně dat, která buďto aktivně a vědomě poskytl, nebo která poskytl na základě využívání služby nebo zařízení. Právo na přenositelnost nemůže subjekt naproti tomu uplatnit u údajů, které jsou správcem z výše uvedených údajů dovozena nebo odvozena.[23] Pokud poskytovatel zdravotní aplikace bude na základě údajů poskytnutých uživatelem při využívání služby, vytvářet profily uživatelů a na základě těchto profilů dovozovat údaje o uživatelích, nebude mít subjekt ve vztahu k těmto údajům právo na přenositelnost vůči správci.

Správce i zpracovatel je povinen zajistit integritu a důvěrnost zpracování. Podle čl. 32 GDPR musí správce a zpracovatel přijmout vhodná technická a organizační opatření, aby byla zajištěna úroveň bezpečnosti odpovídající riziku pro práva a svobody subjektu údajů. GDPR nestanoví žádná povinná opatření k zajištění bezpečnosti zpracování. GDPR uvádí některé příklady možných bezpečnostních opatření, mimo jiné pseudonymizaci a šifrování, schopnost zajistit trvalou důvěrnost, integritu,

[23] PRACOVNÍ SKUPINA 29. Pokyny k právu na přenositelnost. *Úřad pro ochranu osobních údajů* [online]. 2018, s. 7 [cit. 2018-10-11]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31882.

dostupnost a odolnost zpracovatelských systémů a služeb nebo schopnost obnovit dostupnost a přístup k osobním údajům v případě fyzické nebo technické události. Porušení důvěrnosti a integrity zvláštních kategorií údajů týkajících se zdraví může způsobit zejména porušení práva na soukromí a práva na to, aby subjekt údajů nebyl diskriminován na základě svého zdravotního stavu. To je důvod, proč poskytovatel aplikace musí věnovat pozornost vysoké míře rizika a přizpůsobit technická a organizační opatření tomuto riziku. Návrh *Kodexu chování* pro tzv. *mhealth* doporučuje poskytovatelům aplikací zabezpečení ve formě vhodné autorizace uživatele, šifrování a pravidelných bezpečnostních auditů.[24]

V případě porušení zabezpečení osobních údajů musí správce podle čl. 33 GDPR bez zbytečného odkladu oznámit porušení zabezpečení orgánu dozoru, kterým je v České republice Úřad pro ochranu osobních údajů, a to nejpozději do 72 hodin poté, co se dozvěděl o tomto porušení, ledaže je nepravděpodobné, že by porušení zabezpečení mohlo vést k ohrožení práv a svobod fyzických osob. Pokud porušení zabezpečení osobních údajů pravděpodobně povede k vysokému riziku pro práva a svobody fyzických osob, musí správce informovat o porušení zabezpečení také přímo tyto subjekty. Je pravděpodobné, že v případě porušení zabezpečení osobních údajů o zdraví, zejména pokud se toto porušení dotkne většího počtu subjektů údajů, dojede k porušení práva na soukromí a tím i k povinnosti informovat tyto subjekty, a nejen dozorový orgán. Porušení zabezpečení osobních údajů může vyústit i v diskriminaci subjektů údajů, pokud se s údaji o zdraví seznámí osoba, která může se subjektem údajů zacházet méně příznivě z důvodu nepříznivého zdravotního stavu. Takovou osobou může být pojišťovna nebo zaměstnavatel. Podle Pokynů k ohlašování případů porušení zabezpečení osobních údajů podle Nařízení 2016/679 by měl být výskyt škody v případě porušení zabezpečení údajů týkající se zdraví považován za pravděpodobný.[25] Z tohoto vyplývá, že správci zpracovávající údaje o zdraví by měli porušení zabezpečení osobních údajů vždy hlásit Úřadu pro ochranu osobních údajů, ledaže se v konkrétním případě lze důvodně domnívat, že není pravděpodobné, že škoda subjektu údajů vznikne.

Poskytovatel zdravotní aplikace, ať již v roli správce nebo zpracovatele musí vyhovět požadavku na záměrnou a standardní ochranu osobních údajů. Podle čl. 25 GDPR 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, jež s sebou zpracování nese, zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jejichž účelem je provádět zásady ochrany údajů a začlenit do zpracování nezbytné záruky, tak aby splnil požadavky tohoto nařízení a ochránil práva subjektů údajů (záměrná ochrana údajů) a zároveň zavede vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich

[24] *Draft Code of Conduct on privacy for mobile health applications* [online]. 2016, s. 12 [cit. 2018-11-05]. Dostupné z: https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised.
[25] PRACOVNÍ SKUPINA 29. Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle Nařízení 2016/679. *Úřad pro ochranu osobních údajů* [online]. 2018, s. 16 [cit. 2018-10-11]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31894.

zpracování, doby jejich uložení a jejich dostupnosti. Tato opatření zejména zajistí, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob (standardní ochrana údajů). Poskytovatel zdravotní aplikace by měl vývojáře softwaru, který používá, informovat o povaze zpracování a v souladu s bodem 78 odůvodnění GDPR jej vybídnout, aby při vývoji a designování, výběru služeb a produktů, zohlednil právo na ochranu osobních údajů a bral ohled na stav techniky s cílem zajistit, aby poskytovatel mohl splnit své povinnosti v oblasti ochrany osobních údajů, zejména zajistit dostatečné zabezpečení aplikace.

Jelikož poskytovatel zdravotní aplikace rozsáhle zpracovává zvláštní kategorie údajů, nadto za využití nových technologií a při vysokém riziku pro práva a svobody fyzických osob, má tento poskytovatel, který je správcem osobních údajů, podle čl. 35 GDPR povinnost vypracovat posouzení vlivu na ochranu osobních údajů. Vysoké riziko pro práva a svobody fyzických osob není přítomno pouze při zpracovávání zdravotnické dokumentace, ale dle vodítek Pracovní skupiny 29 hrozí takové riziko i při použití aplikací zaznamenávajících denní aktivity subjektu údajů (*lifelog*).[26] Při hodnocení rozsáhlosti zpracování bude podle Pracovní skupiny 29 nutné posoudit počet dotčených subjektů údajů, objem údajů nebo rozsah jednotlivých zpracovávaných údajů, délku nebo trvání zpracování údajů a zeměpisný rozsah zpracování.[27] Pokud je správcem osobních údajů poskytovatel zdravotních služeb, byť tyto údaje budou generovány pomocí zdravotní aplikace, posouzení vlivu na ochranu osobních údajů vypracovat nemusí, neboť toto zpracování správce provádí z důvodu splnění své právní povinnosti vést zdravotnickou dokumentaci pacienta stanovené v zákoně č. 371/2011 Sb. V takovém případě se uplatní výjimka uvedená v čl. 35 odst. 10 GDPR, a sice pokud má zpracování podle čl. 6 odst. 1 písm. c) GDPR, tj. zpracování z důvodu plnění právní povinnosti, právní základ v právu Unie nebo členského státu, které se na správce vztahuje, a toto právo upravuje konkrétní operaci nebo soubor operací zpracování a pokud bylo posouzení vlivu na ochranu osobních údajů již provedeno jakožto součást obecného posouzení dopadů v souvislosti s přijetím uvedeného právního základu, povinnost vypracovat posouzení vlivu se na takové zpracování nepoužije, pokud členské státy nestanoví ve svém právním řádu jinak. Obecné zásahy pro hodnocení dopadů regulace (RIA) vydané Vládou České republiky stanoví jako jedno z hodnocení při přípravě návrhů právních předpisů dopad na ochranu osobních údajů.[28] Posouzení vlivu na ochranu osobních údajů nemusí vypracovávat poskytovatelé zdravotních služeb, kteří údaje o zdravotním stavu zpracovávají v rámci zdravotnické dokumentace v režimu zákona č. 371/2011 Sb.

## 3. ODPOVĚDNOST ZA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Uživateli zdravotní aplikace nebo osobě, jejíž biometrické údaje jsou prostřednictvím zdravotní aplikace hodnoceny, může být použitím zdravotní aplikace vzniknout nejen újma na zdraví, ale i škoda

[26] PRACOVNÍ SKUPINA 29. Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/67. *Úřad pro ochranu osobních údajů* [online]. 2017, s. 11 [cit. 2018-08-11]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30196.

[27] Ibidem, s. 12.

[28] VLÁDA ČR. Obecné zásahy pro hodnocení dopadů regulace (RIA) účinné od 3. 2. 2016. *Vláda* [online]. 2016, s. 11 [cit. 2018-08-25]. Dostupné z: https://www.vlada.cz/assets/ppov/lrv/ria/Obecne-zasady-pro-RIA-2016_1.pdf.

spočívající v porušení jiných práv, typicky práva na soukromí a práva nebýt diskriminován. Tento druh škody může vzniknout, pokud poskytovatel zdravotní aplikace zpracovává výše uvedené údaje způsobem, který vznik takové škody zapříčiní.

V případě, že správce nebo zpracovatel zpracovávají osobní údaje v rozporu s nařízením, hrozí mu sankce ze strany Úřadu pro ochranu osobních údajů i bez toho, aby subjektu údajů vznikla v důsledku takového zpracování škoda. Pokud správce nebo zpracovatel poruší své povinnosti stanovené GDPR a v důsledku tohoto porušení dojde k zásahu do práv subjektu údajů má tento subjekt podle čl. 79 GDPR právo na účinnou soudní ochranu. Podání žaloby proti správci nebo zpracovateli nevylučuje možnost podání stížnosti u dozorového úřadu. Nařízení řeší v tomto ustanovení i soudní příslušnost. Řízení proti správci nebo zpracovateli se zahajuje u soudů toho členského státu, v němž má daný správce nebo zpracovatel provozovnu. Řízení se může popřípadě zahájit i u soudů členského státu, kde má subjekt údajů své obvyklé bydliště, s výjimkou případů, kdy je správce nebo zpracovatel orgánem veřejné moci některého členského státu, který jedná v rámci výkonu veřejné moci.

Článek 82 GDPR upravuje nároky subjektu údajů nebo i jiných osob, neboť GDPR toto právo neomezuje pouze na subjekt údajů, vůči správci nebo zpracovateli. Kdokoli, kdo v důsledku porušení nařízení utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy. Podle bodu 146 odůvodnění GDPR se nárok na náhradu újmy neomezuje pouze na porušení samotného nařízení. Nárok na náhradu újmy náleží i v případě, že došlo k porušení právního předpisu, které GDPR provádí. V České republice by měl být tímto prováděcím předpisem zákon o zpracování osobních údajů.

Odpovědnost za újmu nese primárně správce. Za určitých okolností nastupuje odpovědnost zpracovatele. Zpracovatel je za újmu způsobenou zpracováním odpovědný ve dvou případech. Prvním případem je nesplnění povinnosti stanovené nařízením pro zpracovatele. Takovou povinností je kupříkladu jmenování pověřence pro ochranu osobních údajů. Druhým případem je pak jednání nad rámec zákonných pokynů správce nebo v rozporu s nimi, např. nesplnění povinnosti předat osobní údaje správci po skončení zpracování a vymazat jejich kopie.

Odpovědnost správce a zpracovatele je odpovědností objektivní s možností liberace. Správce nebo zpracovatel se mohou odpovědnosti zprostit, pokud prokáží, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

Společní správci, zpracovatelé nebo správce a zpracovatel odpovídají za škodu společně a nerozdílně. Poškozený se tak může domáhat náhrady u kteréhokoliv správce nebo zpracovatele. Jestliže některý správce nebo zpracovatel zaplatil poškozenému úplnou náhradu způsobené újmy, má právo žádat od ostatních správců nebo zpracovatelů zapojených do téhož zpracování vrácení části náhrady, která odpovídá jejich podílu na odpovědnosti.

Aby byla žaloba poškozeného úspěšná, musí poškozený prokázat protiprávní jednání, tzn. porušení nařízení, existenci škody a příčinnou souvislost mezi protiprávním jednáním a vznikem škody. Podle čl. 5 odst. 2 GDPR správce odpovídá za dodržení zásad zpracování osobních údajů a musí být schopen toto dodržení souladu doložit. Podle Van Alsenoye nese sice zákonné důkazní břemeno

poškozený, nicméně *de facto* je toto důkazní břemeno přeneseno na správce, jakmile poškozený doloží dostatečné důkazy o skutečnosti, že správce zpracovával osobní údaje v rozporu s nařízením.[29]

Poruší-li poskytovatel zdravotní aplikace povinnosti stanovené nařízením a subjektu údajů vznikne materiální nebo imateriální újma, má subjekt právo na její náhradu. Typickým příkladem protiprávního jednání, které vede ke vzniku škody, je nedostatečné zabezpečení osobních údajů a jejich únik. Jelikož se v případě zdravotních aplikací bude jednat o osobní údaje týkající se zdraví, může subjektu údajů vzniknout značná nehmotná újma spočívající v tom, že se nepovolané osoby dozví o jeho zdravotním stavu a popřípadě budou se subjektem údajů podle jeho zdravotního stavu jednat, což pro subjekt údajů může mít nepříznivé následky.[30] Následky nemusí vzniknout pro poškozeného pouze v rovině nehmotné, typicky porušením práva na soukromí a práva na ochranu osobních údajů. Se subjektem údajů, s jehož údaji o zdraví se seznámil zaměstnavatel, nebo pojišťovací společnost, může být zacházeno méně příznivě. Zaměstnanci může být odepřeno povýšení či s ním dokonce může být ukončen pracovní poměr. Pojišťovna může přistoupit k úpravě pojistné smlouvy, nebo nemusí souhlasit s jejím prodloužením. V takových případech utrpí poškozený i hmotnou újmu.

GPDR hovoří v ustanovení čl. 82 o náhradě, nikoliv o nápravě újmy. V úvahu tedy připadá náhrada majetkové i nemajetkové újmy v penězích. Poškozený ji může vymáhat proti správci údajů i proti zpracovateli, pokud zpracovatel odpovídá za porušení nařízení. Pokud je poskytovatel zdravotní aplikace zpracovatelem osobních údajů, bude poškozený vymáhat náhradu škody pravděpodobně na správci, např. na poskytovateli zdravotních služeb, neboť si poškozený nemusí být vědom, zda povinnosti stanovené nařízením porušil správce nebo zpracovatel. Poškozený nemusí být ani o zapojení konkrétního zpracovatele informován, neboť čl. 13 a čl. 14 GDPR stanoví správcům povinnost informovat pouze o kategoriích třetích osob, kterým jsou osobní údaje předávány. Správce a zpracovatel by si proto měli ve smlouvě o zpracování upravit proces upozornění správce na porušení zabezpečení osobních údajů ze strany zpracovatele a na právo na regres správce, pokud zpracovatel smluvní ustanovení poruší.[31]

## ZÁVĚR

Zdravotní aplikace vyhodnocují údaje o fyzické kondici nebo dokonce o zdravotním stavu jednotlivce. Tyto údaje mají povahu biometrických údajů, jelikož se vztahují k fyziologickým a biologickým procesům. Výše uvedené biometrické údaje nejsou biometrickými údaji podle GDPR. Nicméně se jedná o údaje o zdraví spadající do zvláštní kategorie údajů. Správcem osobních údajů nemusí být pouze poskytovatel zdravotní aplikace. Správce může být i lékař, který zpravidla aplikaci využívá k diagnostice a k léčbě svých pacientů. Poskytovatel zdravotní aplikace je v tomto případě

[29] VAN ALSENOY, Brendan. Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and E-Commerce Law*. 2016, Vol. 7, No. 3, s. 283. Dostupné z: https://www.jipitec.eu/issues/jipitec-7-3-2016/4506/van_alsenoy_liability_under_eu_data_protection_law_jiptec_7_3_2016_271.pdf.

[30] Srov. rozsudek Evropského soudu pro lidská práva ze dne 17. července 2008, č. 20511/03 (*I. proti Finsku*).

[31] VAN DE BUNT, Tineke – STRIJBOS, Anke. De bewerkersovereenkomst onder de AVG. Een redelijke verdeling van risico's (Zpracovatelská smlouva podle GDPR. Přiměřené rozdělení rizik). *Nederlands juristenblad*. 2018, č. 7, s. 485. Dostupné z: http://www.njb.nl/Uploads/2018/2/De-bewerkersovereenkomst-onder-de-AVG.pdf.

v postavení zpracovatele. Správce a zpracovatel musí dodržovat povinnosti stanovené nařízením, přičemž musí zohlednit citlivou povahu údajů o zdraví. Z porušení povinností podle GDPR může subjektu údajů vzniknout újma. Újma při zpracování tohoto typu osobních údajů může spočívat zejména v právu na soukromí a v právu nebýt diskriminován může být uživateli způsobena zpracováním osobních údajů v rozporu s nařízením. Správce a zpracovatel by si proto ve smlouvě o zpracování měli přesně vymezit své povinnosti a odpovědnost za porušení nařízení, v jehož důsledku vznikla subjektu údajů újma.

*Příspěvek vznikl za podpory projektu Grantové agentury České republiky č. 16-26910S s názvem Biometrické údaje a jejich zvláštní právní ochrana (Biometric Data and Their Specific Legal Protection).*

**REFERENČNÍ SEZNAM**

ANDRONIKOU, Vassiliki – YANNOPOULOS, Angelos – VARVARIGOU, Theodora. Biometric Profiling: Opportunities and Risks. In: HILDEBRANDT, Mireille – SERGE, Gutwirth. *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer, 2008, 374 s. ISBN 978-1-4020-6913-0.

KRAJSOVÁ, Ivana. Využití dermatoskopie a digitální dermatoskopie v diagnostice melanomu. *Dermatologie pro praxi*. 2011, roč. 5, č. 1, s. 23–25. Dostupné z: https://www.dermatologiepropraxi.cz/pdfs/der/2011/01/06.pdf.

LINCOLN, Tsang – KRACOV, Daniel A. – MULRYNE, Jacqueline et al. The Impact of Artificial Intelligence on Medical Innovation in the European Union and United States. *Intellectual Property & Technology Law Journal*. 2017, Vol. 29, No. 8, s. 1–8. Dostupné z: https://www.arnoldporter.com/~/media/files/perspectives/publications/2017/08/the-impact-of-artificial-inteelligence-on-medical-innovation.pdf.

MORANDI, Emilio – TZOVARAS, Dimitros. *Second Generation Biometrics: The ethical, Legal and Social Context.* Dordrecht: Springer, 2011, 354 s. ISBN 978-94-007-3891-1.

MORDINI, Emilio – ASHTONS, Holly. The Transparent Body: Medical Information, Physical Privacy and Respect for Body Integrity. In: MORANDI, Emilio – TZOVARAS, Dimitros. *Second Generation Biometrics: The ethical, Legal and Social Context*. Dordrecht: Springer, 2011, 354 s. ISBN 978-94-007-3891-1.

PAPAGEORGIOU, Achilleas – STRIGKOS, Michael – POLITOU, Eugenia – ALEPIS, Efthimios – SOLANAS, Agusti – PATSAKIS, Constantinos. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access* [online]. 2018, Vol. 6 [cit. 2018-11-04]. Dostupné z: https://ieeexplore.ieee.org/document/8272037.

PATTYNOVÁ, Jana – SUCHÁNKOVÁ, Lenka – ČERNÝ, Jiří a kol. *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. Praha: Leges, 2018, 488 s. ISBN 978-80-7502-288-2.

VAN ALSENOY, Brendan. Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and E-Commerce Law*. 2016, Vol. 7, No. 3, s. 271–288. Dostupné z: https://www.jipitec.eu/issues/jipitec-7-3-2016/4506/van_alsenoy_liability_under_eu_data_protection_law_jiptec_7_3_2016_271.pdf.

VAN DE BUNT, Tineke – STRIJBOS, Anke. De bewerkersovereenkomst onder de AVG. Een redelijke verdeling van risico's (Zpracovatelská smlouva podle GDPR. Přiměřené rozdělení rizik). *Nederlands juristenblad*. 2018, č. 7, s. 357–485. Dostupné z: http://www.njb.nl/Uploads/2018/2/De-bewerkersovereenkomst-onder-de-AVG.pdf.