Univerzita Palackého v Olomouci

Právnická fakulta

Jana Andraščiková

Implementace evropského právního rámce ochrany osobních údajů v pojišťovnictví České republiky

Rigorózní práce

Olomouc 2022

Prohlášení

Prohlašuji, že jsem předkládanou rigorózní práci vypracovala samostatně a že všechny použité zdroje byly řádně uvedeny.

V Olomouci dne 04. 04. 2022

...……

Jana Andraščiková

Poděkování

Děkuji panu doc. JUDr. Michalu Petrovi, Ph.D., za užitečné připomínky a konstruktivní dialog během zpracování tohoto neustále se vyvíjejícího tématu.

Abstrakt

Tato práce pojednává o implementačním procesu evropského rámce ochrany OÚ v odvětví českého pojišťovnictví. Na konkrétním příkladu modelového dokumentu *Samoregulační standardy ČAP k uplatňování GDPR v pojišťovnictví*, vyjadřujícího dobrovolný závazek kompatibility a dodržování minimální míry ochrany OÚ, a to primárně z hlediska jejich důvěrnosti, bezpečnosti, ale i výkonu práv subjektů OÚ při zajištění plné informovanosti, sekundárně pak z hlediska rozvoje finančního trhu, analyzuje specifičnosti implementace s ohledem na obecnou povahu pojišťovnictví.

Při nalézání legislativních, praktických a interpretačních řešení se vychází z legislativních požadavků a zkušeností v českém i evropském kontextu. Proto je GDPR pojímáno nikoli jako izolovaný předpis, nýbrž jako součást komplexního ekosystému požadavků obecného i sektorově specifického charakteru, a to *de lege lata*, ale i *de lege ferenda*, např. u revize ePrivacy, hromadných žalob, budoucí úpravy KB, sdílení dat či UI.

Některé instituty jsou z důvodu vykreslení kontinuální fragmentace rámce ochrany OÚ, ale i jejich relevance pro pojistný sektor komparovány. Práce se zaměřuje na řešení implementačně náročných situací specifických pro pojišťovnictví, jako např. citlivé OÚ s orientací na gender či OÚ o zdravotním stavu, nejen v kontextu právních základů zpracování OÚ. Prioritně je pozornost věnována souhlasovému režimu. Také je analyzována praktická rovina informační povinnosti v kontextu informačního přetížení a následné eventuality učinit skutečně informované rozhodnutí. Vzhledem k aktuální judikatuře SDEU je pojednáváno i o SCCSs a režimu upravujícím vztahy ke třetím zemím. Z důvodu nabývajícího významu je detailně analyzována také problematika AR neboli profilování, a to v kontextu GDPR, hodnocení rizik i underwritingu.

Dále se tato práce věnuje hodnocení rámce GDPR, primárně evropskými institucemi a sekundárně pojistným sektorem. Tato oblast je vysvětlena především v souvislosti s výkladovou praxí EDPB. Kriticky jsou hodnoceny interpretační nedostatky a jejich dopady či vytvořené bariéry, což ilustruje potenciální změna obsahu a formy *Standardů* na kodex chování dle GDPR *stricto sensu*.

Z důvodu možného obsahového rozšíření *Standardů* a významného (*de facto* a zanedlouho i *de iure*) přesahu do oblasti regulované GDPR se tato práce orientuje také na nové technologie s významným optimalizačním či transformačním potenciálem pro pojistný sektor

– na insurtech. Hlavním hybatelem je zde UI, na kterou je pohlíženo z hlediska jak přínosů, tak možných rizik, především z důvodu ochrany práv subjektů OÚ. Obdobně jako u AR, akcentuje se právo na lidský zásah. Práce nepomíjí ani rostoucí evropské tendence ke sdílení dat, na což pohlíží optikou GDPR. V neposlední řadě prakticky dokazuje přímou souvislost ochrany dat, včetně OÚ, s odůvodněně rostoucími požadavky na KB – to se výrazně dotýká právě sektoru finančních služeb obecně. Přímý dopad je akcentován u pojišťovnictví, které vzhledem ke své tradičně datacentrické povaze potřebuje pro řádný a korektní výkon své činnosti, včetně minimalizace rizik, zpracovávat velké množství dat, OÚ nevyjímaje. *Pro futuro* tak doporučuje syntézu vzájemně logicky provázaných předpisů za účelem vytvoření evropského robustního, odolného rámce, který bude po vzoru GDPR globální inspirací.

Abstract

This thesis deals with the implementation process of the European data protection framework in the Czech insurance sector. Using the specific example of the model document *Self--regulatory Standards of the Czech Insurance Association on the application of GDPR in the insurance sector*, expressing a voluntary commitment to compatibility and compliance with a minimum level of protection of personal data primarily in terms of confidentiality, security, but also the exercise of the rights of data subjects while ensuring a full level of information access, and secondarily in terms of the development of the financial market, the paper analyses the specifics of implementation due to the nature of the insurance sector.

In finding legislative, practical and interpretative solutions, it is based on legislative requirements and experience in the Czech and European context. Therefore, the GDPR is conceived not as an isolated parameter, but as part of a complex ecosystem of requirements of a general and sector-specific nature, both *de lege lata* and *de lege ferenda*, e.g. the ePrivacy review, collective redress, future cybersecurity, data sharing or artificial intelligence regulation.

Several institutes are compared in order to portray the continuous fragmentation of the data protection framework, but also the relevance for the insurance sector. The thesis focuses on addressing implementationally challenging situations specific to the insurance sector, such as gender-sensitive personal data and personal health data, including but not limited to the context of the legal basis of personal data processing. Priority attention is given to the consent

regime. The practicalities of the information obligation are also analyzed in the context of information overload and the subsequent eventuality of making a truly informed decision. In view of the recent case law of the Court of Justice of the European Union, standard contractual clauses and the regime governing relations with third countries are also discussed. Due to its growing importance, the issue of automated decision-making or profiling is also examined in detail, both in the context of GDPR and risk assessment or underwriting.

Furthermore, the thesis is devoted to the evaluation of the GDPR framework by primarily European institutions, and secondarily by the insurance sector. This area is explained in the context of the interpretative practice of the EDPB in particular. The interpretative shortcomings and their impact or barriers created are critically assessed, illustrating the potential change of the content and form of the *Standards* into a GDPR code of conduct *stricto sensu*.

In view of the possible content extension of the *Standards* and the significant (*de facto* and soon *de iure*) overlap into the GDPR regulated area, the work is also oriented towards new technologies carrying significant optimization or transformation potential for the insurance sector – insurtech. The main momentum here is artificial intelligence, which is looked at both in terms of benefits and potential risks, mainly due to the protection of data subjects' rights. Similar to automated decision-making, the right to human intervention is emphasized. The work through the lens of GDPR does not neglect the growing European tendency towards data sharing, which is seen through the GDPR limits.

Last but not least, it practically demonstrates the direct relevance of data protection, including personal data, in light of the justifiably growing demands for cyber security, which significantly affects the financial services sector in general. The direct impact is accentuated in the insurance sector, which, due to its traditionally data-centric nature, needs to process large amounts of data, not excluding personal data, for the proper and correct performance of its activities, including risk minimization. For the future, it thus recommends a synthesis of logically interlinked regulations to create a European robust, resilient framework that, following the GDPR model, will be a global inspiration.

Klíčová slova

Ochrana osobních údajů, osobní údaj, GDPR, osobní údaje o zdravotním stavu, pojišťovnictví, Česká asociace pojišťoven, Insurance Europe, gender, právní základy zpracování osobních údajů, souhlas, samoregulace, underwriting, Schrems II, standardní smluvní doložky, automatizované rozhodování, profilování, informační přetížení, Evropská komise, Evropský sbor pro ochranu osobních údajů, kodex chování, ePrivacy, IDD, kybernetická bezpečnost, umělá inteligence, big data, inovace, insurtech.

Key words

Data protection, personal data, GDPR, personal health data, insurance, Czech insurance association, Insurance Europe, gender, legal basis for data processing, consent, self-regulation, underwriting, Schrems II, standard contractual clauses, automated decision making, profiling, information overload, European Commission, European Data Protection Board, code of conduct, ePrivacy, IDD, cybersecurity, artificial intelligence, big data, innovation, insurtech.

Obsah

1 Úvod

Tato práce se věnuje problematice ochrany OÚ v pojistném sektoru, jež je v ČS EU výrazně ovlivněna a unifikována evropským právním rámcem – přelomovým GDPR.

Důraz na tuto oblast, stupňující se nejen v pojišťovnictví, je rozebírán v širším kontextu *de lege lata* i očekávaných legislativních a regulatorních požadavků na národní a evropské úrovni. Smyslem je ukázat, že se nejedná o izolovanou oblast, nýbrž o vzájemně provázanou soustavu, která ovlivňuje výkon pojišťovnictví.

Pojišťovnictví je odvětvím finančních služeb, jež se věnuje přesunům rizik finanční či jiné ztráty v důsledku specifikované, ale nepředvídatelné události z jednotlivce na pojistitele formou úhrady pojistného. Pokud dojde ke v pojistné smlouvě vymezené události, pojistník je oprávněn požadovat kompenzaci od pojistitele. Smyslem pojištění je tak v obecné rovině prevence a snížení negativních dopadů nepředvídatelných událostí.

V této práci vycházím z teze, že vzhledem k povaze pojistného odvětví je pro jeho řádný a korektní výkon, včetně minimalizace rizik, potřeba zpracovávání četného množství dat, OÚ nevyjímaje. To uznává i de Azevedo Cunha[1]. Jedná se např. o OÚ potřebné pro uzavírání pojistné smlouvy, trvání pojištění, kalkulaci pojistného ve vztahu k oceňování rizik (underwriting) apod. Na základě těchto OÚ lze pak nastavit nejvíce vyhovující individuální podmínky pro klienta a poskytovat optimální služby. Platí to především u ŽP nebo pojištění nemoci, které jsou sjednávány obvykle na poměrně dlouhou dobu, a např. znalost zdravotního stavu zájemce o pojištění je v těchto případech při rozhodování pojistitele o přijetí návrhu podstatná[2].

Z pozice právničky pro evropské záležitosti ČAP, působící v IE, evropské federaci asociací pojistného trhu, a gestora PS GDPR ČAP a PS Kybernetická bezpečnost ČAP se v této práci zaobírám implementací relevantní obecné i sektorově specifické legislativy související s oblastí ochrany OÚ v širším kontextu regulace pojistného odvětví a vyplývajícími praktickými požadavky současnými i *pro futuro*. Představím a podložím myšlenku, že pojistný sektor navzdory své spíše tradiční, až rigidní povaze nemůže zachovat svůj *status*

[1] DE AZEVEDO CUNHA, Mario V. *Market integration through data protection: an analysis of the insurance and financial industries in the EU*. Dordrecht: Springer, 2013, s. 45. Law, Governance and Technology Series, Vol. 9. ISBN 978-94-007-6084-4.
[2] MESRŠMÍD, Jaroslav. *Regulace pojišťovnictví v EU*. První vydání. Praha: Professional Publishing, 2015, s. 130. ISBN 978-80-7431-146-8.

quo paralelně s konkurenceschopností. Je nezbytná jeho adaptace na nové *de iure*, *de facto* i tržní nároky. To zde nahlížím optikou GDPR, ve světle stávajících požadavků, ale i nových faktorů, jako generační obměny, stupňující se tendence spotřebitelské ochrany, digitalizace, virtualizace, rozvoje ICT a navazující nepostradatelnosti KB.

V této práci jsem vycházela ze své praxe, poznatků, komparací a analýz, veřejně dostupných informací, platných a účinných obecně závazných právních předpisů, odborné literatury, soudní judikatury a v neposlední řadě z dokumentu *Samoregulační standardy ČAP k uplatňování GDPR v pojišťovnictví*[3].

Tato práce je orientována na implementaci GDPR, z povahy vlastní přímo použitelnému evropskému předpisu, do sektoru pojišťovnictví v ČR prostřednictvím tohoto páteřního dokumentů. Během jeho formulace nebyl ještě přijat adaptační zákon č. 110/2019 Sb., o zpracování OÚ, doplněný doprovodným zákonem č. 111/2019 Sb., jenž se stal platným a účinným až dne 24. 4. 2019. Jelikož tento zákon nepřináší významné odchylky od GDPR a obsah *Standardů* neovlivnil, nebude o něm pojednáváno ani v této práci.

Stěžejní hodnotu OÚ vykresluji na konkrétním příkladu tohoto dokumentu *soft law* povahy, jejž členské pojišťovny ČAP přijaly s úmyslem explicitně zdůraznit význam připisovaný ochraně soukromí a OÚ. Na přípravě *Standardů* jsem se aktivně podílela a jejich aktuálnost a kompatibilitu s požadavky dále garantuji. Proto si uvědomuji složitost diskuzí v mnohých faktických a také interpretačních otázkách, a to jak před samotnou účinností GDPR, tak po ní. Jedná se např. o správné nastavení zpracování OÚ na GDPR vymezeném právním základu, především ve věci souhlasu, o souhlas samotný, přístup k citlivým neboli zvláštním kategoriím OÚ, zajištění plné informovanosti subjektu OÚ nebo o vhodnou úpravu AR či profilování.

Na úvod bych ráda uvedla, že *Standardy* jsou dokumentem vyjadřujícím dobrovolný závazek členských pojišťoven dodržovat zakotvenou minimální míru ochrany OÚ. Přistoupení ke *Standardům* je vyjádřením závazku kompatibility s jejich obsahem a zároveň dobré vůle pojišťoven, jež veřejně proklamují respekt k ochraně osobnosti, důvěrnosti a bezpečnosti OÚ, plné míře informovanosti klienta či ke zvýšení jeho ochrany a sekundárně slouží k rozvoji finančního trhu. *Standardy* byly tedy přijaty za účelem přispění k řádnému uplatňování GDPR

[3] ČAP. *Samoregulační standardy ČAP k uplatňování GDPR v pojišťovnictví* [online]. Druhé, revidované vydání. Praha: ČAP, 1. 8. 2020 [cit. 12. 2. 2022]. Dostupné z: https://www.cap.cz/images/o-nas/CAP_GDPR_standardy.PDF.

a zároveň reflektují specifickou povahu pojišťovnictví a konkrétní potřeby členů ČAP při zpracovávání OÚ. Pro přistoupivší členy jsou koncipovány jednotně, s cílem upřesnit uplatňování GDPR.

Uvedený dokument proto v této práci používám jako základ pro analýzu implementace GDPR, se zohledněním pojistných specifik, a zároveň pro vykreslení interpretačních nedostatků s praktickým přesahem, jež byly ve fázi prvního hodnocení GDPR rámce komunikovány s EK, ale i EDPB.

Je nutno zdůraznit, že smyslem *Standardů* není nahradit právní úpravu GDPR ani doporučené postupy a výkladová stanoviska na národní či evropské úrovni. Na národní úrovni mluvím o DPA dle čl. 51 a násl. GDPR, kterým je v ČR ÚOOÚ, s pravomocemi dle čl. 58 a 83 GDPR. Na evropské úrovni odkazuji na činnost WP29 a následně EDPB. Tento nezávislý orgán je upraven čl. 68 a násl. GDPR. Jeho členy jsou vedoucí DPA a EDPS.

Standardy mají tedy sloužit jako doplněk interpretačních pokynů ÚOOÚ, EDPB a EDPS či jako obecné výkladové vodítko při aplikaci zásad a jednotlivých povinností upravených GDPR v prostředí pojišťovnictví. V této práci vycházím z předpokladu, že uvedený dokument vhodně ilustruje specifika implementace GDPR v pojistném sektoru, a pro účely této práce zároveň slouží k vykreslení dalších případných směrů, které mohou v blízké budoucnosti ovlivnit případnou změnu jeho formy neboli rozšiřování jeho obsahu, a to i vzhledem k publikaci *Zprávy*[4] v červnu 2020. Proto zohledňuji iniciativy EK či jiných evropských orgánů, především EIOPA, ale i rapidní faktický vývoj v oblasti ICT a dalších okruzích.

Relevanci pro pojistný sektor vykresluji na příkladech big dat a blockchainu; kriticky pak analyzuji především UI, včetně IoT. Důvodem je dle mého názoru nejsilnější souvislost s ochranou OÚ. Zde rozebírám jak pozitivní transformační kapacitu pro subjekty OÚ i pojišťovny, tak potenciální zvýšené riziko ohrožení OÚ. Proto je do této práce absorbován také podstatný aspekt relace OÚ, insurtechu a digitalizačních procesů či zde analyzovaný přesah do KB.

[4] EK. *Sdělení Komise Evropskému parlamentu a Radě. Ochrana osobních údajů jakožto pilíř posílení postavení občanů a přístup EU k digitální transformaci – dva roky uplatňování obecného nařízení o ochraně údajů* [online]. V Lucemburku: 24. 6. 2020 [cit. 17. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?from=EN&uri=CELEX%3A52020DC0264.

Z perspektivy pojistného sektoru se důkladně věnuji komplikovanému vztahu GDPR s dlouhodobě revidovanou ePrivacy[5].

V oblasti KB hodnotím jako relevantní aktuálně revidovanou směrnici NIS[6] a především DORA[7]. Provázanost agendy KB s ochranou OÚ analyzuji na základě svých vědomostí, zkušeností s evropským legislativním procesem a poznatků z činnosti gestora PS GDPR a PS Kybernetická bezpečnost ČAP.

Vzhledem k povaze pojišťovnictví, vyvíjející se nejen dle legislativních a regulatorních požadavků, ale i spotřebitelských potřeb, není v této práci opomenut ani rozměr spotřebitele jakožto subjektu OÚ. Ten spočívá jak v samotné zvyšující se ochraně spotřebitelů napříč EU, tak v optice budoucího vývoje poskytování služeb. Proto zde zmiňuji též informační přetížení, na evropské úrovni nově upravený institut hromadných žalob či inovace. *Pro futuro* lze důvodně předpokládat jejich rostoucí význam. Ve srovnání s praktickým charakterem zbytku této práce si zde dovolím zakomponovat teoretické hypotézy a dedukci.

Cílem této práce je důkladně vykreslit implementační proces evropského rámce ochrany OÚ (samozřejmě se zaměřením na GDPR), ale v nezbytném kontextu i dalších legislativních a regulatorních požadavků v pojišťovnictví ČR. Pro bližší pochopení významu především GDPR v pojišťovnictví je třeba stanovit jeho implementaci ve vztahu k dalším zásadním legislativním předpisům evropské i lokální povahy, jelikož se jedná o důkladně regulované odvětví, ve kterém jsou jednotlivé požadavky vzájemně provázané, a to nejen na úrovni level 1, ale též level 2 a level 3 předpisů.

Vzhledem k limitaci rozsahu této práce se zaměřím pouze na nejvýznamnější evropskou legislativu, okrajově pak na její transpozici do národního právního řádu. Považuji za nezbytné tento rámec specifikovat, jelikož na jeho základě vzniká prostor a podmínky určující způsob implementace a výkonu ochrany OÚ v dotčeném odvětví.

Z povahy mého působení v ČAP a IE vidím, že během implementace legislativního rámce ochrany OÚ i dalších relevantních předpisů je značně nápomocné i sdílení zkušeností napříč

[5] EPrivacy. In: *Úřední věstník* [online], L 201, 31. 7. 2002, s. 37–47 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32002L0058.
[6] NIS. In: *Úřední věstník* [online], L 194, 19. 7. 2016, s. 1–30 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX%3A32016L1148.
[7] EK. *Návrh nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014* [online]. V Bruselu: 24. 9. 2020 [cit. 17. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0595.

EU. To má nezpochybnitelnou hodnotu pro jednotné vnímání taxonomie a následnou praktickou aplikaci výkladu, popř. pro vymezení diskutabilních oblastí, kde může vznikat nežádoucí stav právní nejistoty. V této práci proto detailně řeším pojistně specifické okruhy z pohledu GDPR, např. gender nebo informační povinnost, a dále srovnávám některé instituty s praxí jiných ČS, např. v případě OÚ o zdravotním stavu, i v kontextu právních základů se zaměřením na souhlas nebo přístupy ke kodexu chování dle čl. 40 GDPR.

Pro úplnost uvádím, že obsahem této práce není detailní specifikace úpravy údajů neosobní povahy, tj. dat, jež nejsou OÚ, a to od počátku nebo po provedení anonymizace dle nařízení o rámci pro volný tok neosobních údajů[8]. Vycházejíce z čl. 8 odst. 3 tohoto nařízení byly v roce 2019 EK publikovány pokyny[9] s příklady z oblastí OÚ, neosobních údajů a smíšených souborů údajů (např. daňové záznamy, platební údaje, IoT). Pro případy neoddělitelně propojených údajů se doporučuje aplikovat GDPR jako standardní volbu, což pro účely této práce reflektuji v předposlední kapitole u IoT.

Tato práce se nevěnuje ani datům veřejného sektoru, ani úpravě zaměstnaneckých vztahů, jelikož dle *Standardů* náleží do interního rámce pojišťoven. Specifika zajišťovací činnosti ve vztahu k pojišťovnictví rovněž nejsou předmětem této práce.

Obsahem *Standardů*, a tedy ani této práce, nejsou některé instituty upravené v GDPR. I když se jedná o zajímavé oblasti, v této práci je zmiňuji pouze okrajově nebo vůbec. Konkrétně jde o: věk, záznamy o činnostech zpracování náležející do interních procesů pojišťoven, mezinárodní spolupráci, DPA, odpovědnost, správní pokuty a sankce, ustanovení týkající se zvláštních situací, při nichž dochází ke zpracování OÚ, akty v přenesené pravomoci a prováděcí akty.

Do této práce však byla zahrnuta problematika postavení správců a zpracovatelů OÚ, jelikož se dle mého názoru jedná o zajímavý interpretační oříšek.

Z povahy mé pozice v ČAP i postavení ČAP jako takové mám pochopitelně omezený přístup k informacím o interních postupech a procesech členských pojišťoven. ČAP představuje sdružení k organizaci a podpoře vzájemné pomoci, spolupráce a zabezpečení zájmů jejích

[8] Nařízení EP a Rady (EU) 2018/1807 ze dne 14. 11. 2018, o rámci pro volný tok neosobních údajů v EU. In: *Úřední věstník* [online]. L 303, 28. 11. 2018, s. 59–68 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32018R1807.

[9] EK. *Sdělení Komise Evropskému parlamentu a Radě. Pokyny k nařízení o rámci pro volný tok neosobních údajů v Evropské unii* [online]. V Bruselu: 29. 5. 2019 [cit. 19. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A250%3AFIN.

členů. Posláním ČAP je koordinovat, zastupovat, hájit a prosazovat společné zájmy pojišťoven. Proto, z důvodu respektu k jejich zájmům a k pravidlům hospodářské soutěže, bude tato práce, obdobně jako *Standardy*, koncipována obecným způsobem. Pro důkladnější analýzu jednotlivých institutů ale uvádím praktické příklady nebo komparaci.

Na základě výše uvedeného jsem se rozhodla zvolit kombinaci sběru informací, teoretické výzkumné metody a právní výkladové metody. Je aplikován analytický přístup, a to za využití kritické analýzy, komparace a dedukce. U výkladu je využívána metoda gramatická, systematická, logická, teleologická a analogická.

Dle praktických zkušeností na lokální i evropské úrovni je teoretický aspekt průběžně obohacen o empirické zkušenosti získané v průběhu mé profesní praxe. To se odráží u komparace výkladové a praktické roviny některých institutů, což deklaruje přetrvávající fragmentace úprav GDPR v ČS, a bylo to z mé strany komunikováno i s EK před publikací *Zprávy*.

Co se týče struktury této práce, byl zvolen přístup od obecného ke konkrétnímu. Po specifikaci obecných faktorů determinujících ochranu OÚ, s důrazem na legislativní základ pojišťovnictví v ČR, se tak věnuji konkrétním ustanovením GDPR, na jejichž příkladu uvádím specifika pojistného odvětví. Následně rozebírám otázky, u kterých považuji za vhodné, aby byly v blízkém časovém horizontu vyřešeny a do úpravy *Standardů* potenciálně zakomponovány. Jedná se jak o výkladové nejasnosti plynoucí z interpretace EDPB, a to v návaznosti na *Zprávu* a vlastní zkušenosti, tak o oblast hromadných žalob, digitalizace, KB a nových technologií, které nelze dle mého názoru od GDPR oddělit.

Tato práce je strukturována do osmi kapitol, za účelem přehledného vymezení dílčích aspektů a zároveň systematického celku, který poskytne odpovědi a návrhy řešení nastolených otázek.

Stanovuje si několik cílů. Zaprvé, analyzovat implementaci GDPR do sektoru pojišťovnictví v ČR na příkladu *Standardů* v souvislostech s představenými tradičními regulatorními a legislativními požadavky a vysvětlit řešení implementačně náročných situací specifických pro pojišťovnictví, jako např. explicitního souhlasu, informačního přetížení v kontextu informačních povinností, OÚ o zdravotním stavu či AR, rovněž v kontextu UI, včetně IoT.

Zadruhé, upozornit na nedostatky současné úpravy především ve vztahu k GDPR a interpretačním pokynům EDPB a navrhnout vhodná řešení pro *de lege ferenda* obecně

i doplnění obsahu *Standardů* za kritického objasnění limitací pro možnou vyšší formu evoluce v kodex chování dle čl. 40 GDPR.

Zatřetí, představit budoucí výzvy úzce provázané s GDPR a specifické pro dané odvětví a nabídnout vhodný přístup, konkrétně např. u hromadných žalob, ePrivacy, DORA a insurtechu, s důrazem na UI z pohledu její úpravy v rámci AIA i z pohledu odpovědnostního režimu.

Následně tyto faktory vyhodnotit nikoli odděleně, nýbrž jako provázaný organizmus a závěry aplikovat vymezením eventuálního rozšíření *Standardů* do budoucna. Smyslem této práce je tedy nejen popsat současný stav, ale také dle mých zkušeností a představených podkladů predikovat budoucí vývoj a jeho dopad na požadavky minimální ochrany OÚ v pojišťovnictví ČR. Cílem je tak prokázat, že GDPR rámec skutečně není jenom o GDPR, ale že se jedná o komplexní syntézu.

Náležitosti a členění této práce odpovídají pravidlům pro rigorózní řízení dle předpisů Právnické fakulty Univerzity Palackého v Olomouci[10]. Postup zvolený u poznámek pod čarou je v souladu s ČSN ISO 690. Přehledné uvádění legislativních předpisů, literatury, článků a internetových zdrojů umožňuje snadné dohledání citovaného zdroje a ověření informací. Dotčené právní předpisy a jiné pojmy označuji etablovanými zkratkami.

[10] Právnická fakulta Univerzity Palackého v Olomouci. Rigorózní řízení. In: *Pf.upol.cz* [online]. V Olomouci: Univerzita Palackého v Olomouci [cit. 16. 2. 2022]. Dostupné z: https://www.pf.upol.cz/studenti/studium/rigorozni-rizeni/.

2 Evropský legislativní rámec pojišťovnictví

V této kapitole představím výchozí legislativní úpravu relevantní pro výkon pojišťovnictví v EU a transpozici do právního řádu ČR. I když je předmětem této práce ochrana OÚ, je třeba stručně vykreslit stávající legislativní požadavky, do kterých byla ochrana OÚ zakomponována. Považuji to za nezbytné pro porozumění toho, že sektor pojišťovnictví při implementaci GDPR disponoval silnou legislativní základnou. To se týká jak sektorově specifické roviny, tak podstatných předpisů obecnějšího charakteru.

Proto zde vysvětlím v této práci opakovaně zmiňovanou tezi o vysoké míře regulace tohoto odvětví. Důvodem je nikoli pouze rozsáhlá právní, administrativní, organizační a finanční náročnost *compliance* z hlediska subjektů pojistného trhu, ale především přímý dopad na spotřebitele, který se odráží v extenzivním navýšení informační povinnosti. To úzce souvisí i s faktickým přístupem spotřebitelů k výkonu a ochraně jejich práv plynoucích z GDPR.

2.1 Primární právo

Primární právo EU, tj. zakládající smlouvy: SEU[11] a SFEU[12], doplněné o novelizace a protokoly, či LZPEU[13], jež jsou nadány nejvyšší právní silou a přímým účinkem[14], se pojišťovnictví věnují spíše marginálně. Obecná zmínka se nachází v čl. 58 odst. 2 SFEU: *Liberalizace bankovních a pojišťovacích služeb, které jsou spojeny s pohybem kapitálu, se uskuteční v souladu s liberalizací pohybu kapitálu.* To znamená, že i pro pojišťovací služby má stěžejní význam čl. 63 SFEU a navazující ustanovení s tím, že jsou zakázána všechna omezení kapitálu mezi ČS i třetími zeměmi, čímž ale není dotčeno právo ČS EU uplatňovat mj. příslušná ustanovení jejich daňových předpisů, která rozlišují mezi daňovými poplatníky podle místa bydliště nebo podle místa, kde je kapitál investován[15]. Důvodem je klíčový

[11] SEU (konsolidované znění). In: *Úřední věstník* [online], C 326, 26. 10. 2012, s. 13–390 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=celex%3A12012M%2FTXT.
[12] SFEU (konsolidované znění). In: *Úřední věstník* [online], C 326, 26. 10. 2012, s. 47–390 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX%3A12012E%2FTXT.
[13] LZPEU. In: *Úřední věstník* [online], C 326(2), 26. 10. 2012, s. 391–407 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex%3A12012P%2FTXT.
[14] SDEU. *Rozsudek Soudního dvora ze dne 5. února 1963*, C26/62 [online]. V Lucemburku: 5. 2. 1963 [cit. 16. 2. 2022]. Dostupné z: https://curia.europa.eu/arrets/TRA-DOC-CS-ARRET-C-0026-1962-200406974-05_01.html.
[15] MESRŠMÍD, 2015, op. cit., s. 19.

význam pojišťovnictví pro efektivní fungování vnitřního trhu.[16] Výlučné kompetence EU aplikované v rámci zásad subsidiarity a proporcionality jsou vymezeny čl. 3 SFEU. Patří mezi ně i stanovení pravidel hospodářské soutěže a vnitřního trhu dle čl. 101 a 102 SFEU, což samozřejmě dopadá i na odvětví pojišťovnictví. V oblasti sdílených pravomocí zakotvených čl. 4 SFEU je relevantní ochrana spotřebitele detailněji upravena čl. 169 SFEU.

2.2 Sekundární právo

2.2.1 Úvod

Detailnější regulace se nachází na úrovni sekundárních aktů EU legislativního a nelegislativního charakteru, které jsou přijímány na základě zmocnění uvedeného v aktu legislativním.

V případě legislativních aktů se jedná o přímo, bezprostředně účinná a použitelná, plně závazná nařízení a směrnice závazné z hlediska zamýšleného výsledku. ČS tak samy disponují implementačními formami a prostředky k jejich dosažení. Nelegislativní akty, především delegované a prováděcí akty, jejichž počet v pojišťovnictví skutečně není nízký, mají významný dopad na jeho konkrétní výkon.

V rámci režimu minimální harmonizace směrnic, přístupu regulátorů a výkladu národních orgánů pochopitelně existují odchylky. Níže uvedené legislativní předpisy a jejich národní protějšky však v současnosti formují pojistné odvětví a tvoří podklad pro aplikaci rámce k ochraně OÚ. Pochopitelně se však nejedná o výčet kompletní, spíše exemplifikativní. Rozlišují se předpisy specializované na oblast pojišťovnictví, ale velký dopad nesou také obecně laděné předpisy, které pojistný sektor nepřímo ovlivňují, např. GDPR.

Na vymezení těchto stěžejních předpisů lze vidět detailní regulaci pojišťovnictví na unijní a národní úrovni. Pozitivním následkem je tak důkladné vymezení jeho výkonu. Negativní následek je ale spatřován v existenci duplicitních nebo i kontradiktorních požadavků, u spotřebitelů pak v jejich extrémním informačním zatížení, což může značně komplikovat reálné učinění informovaného rozhodnutí. To je blíže rozebráno v kapitole 5.8 této práce.

[16] SYLLOVÁ, Jindřiška et al. *Lisabonská smlouva: komentář*. První vydání. Praha: C. H. Beck, 2010, s. 333. Beckova edice Komentované zákony. ISBN 978-80-7400-339-4.

2.2.2 Sektorově specifická legislativa

V této kategorii se jedná především o klíčovou, aktuálně revidovanou SII[17], jež byla do národního právního systému transponována ZPOJ. Na procesu implementace se podílela ČAP[18]. Robustní předpis, účinný od roku 2016, vymezuje pravidla a požadavky na výkon pojišťovací a zajišťovací činnosti. Obsáhl solventností požadavky *stricto sensu*. Správná identifikace a klasifikace jednotlivých rizik, kterým je pojišťovna vystavena, je nedílnou součástí projektu SII[19]. Kromě toho upravil i ŽP a neživotní pojištění.

Navenek je však více viditelnou oblastí distribuce pojistných produktů, upravená směrnicí IDD[20], transponovanou ZDPZ. IDD sice není prvním evropským aktem pro oblast distribuce pojištění, je však výsledkem dlouhodobé snahy o regulaci zprostředkování, jež se v ČS znatelně odlišovalo. Vymezuje detailní podmínky pro dohled nad pojišťovacími zprostředkovateli např. u informačních požadavků a předsmluvní i smluvní fáze vztahu, což následně přímo ovlivnilo GDPR z hlediska práv subjektů OÚ i právních základů zpracování OÚ.

To rozebírám u *Standardů* níže, neboť IDD – ale např. také PRIIPs[21], jež zavádí klíčový informační dokument pro distribuci strukturovaných retailových investičních produktů a pojistných produktů s investiční složkou – má v každodenním výkonu pojistné činnosti největší dopad. Optikou ochrany OÚ tak nese významnější roli než interně orientovaná SII. Za *de lege ferenda* relevantní považuji její revizi v kontextu digitalizace, online prodeje i nových technologií.

Pochopitelně má na charakter pojišťovnictví dopad i nařízení o zřízení evropského orgánu dohledu[22] (EIOPA), který ovlivňuje výklad a praxi v dotčeném odvětví. Na národní úrovni je správním dohledovým orgánem ČNB, a to podle zákona č. 219/2021 Sb.

---

[17] SII. In: *Úřední věstník* [online], L 335, 17. 12. 2009, s. 1–155 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX%3A32009L0138.
[18] MESRŠMÍD, 2015, op. cit., s. 20.
[19] BOKŠOVÁ, Jiřina. Solventnost I a II v pojišťovnictví. *Český finanční a účetní časopis* [online]. 2006, 1(3), 127–132 [cit. 15. 2. 2022]. ISSN 18022200. Dostupné z: https://cfuc.vse.cz/pdfs/cfu/2006/03/12.pdf.
[20] IDD. In: *Úřední věstník* [online], L 352, 9. 12. 2014 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32016L0097.
[21] PRIIPs. In: *Úřední věstník* [online], L 352, 9. 12. 2014 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?from=EN&uri=CELEX%3A32014R1286.
[22] Nařízení EP a Rady (EU) č. 1094/2010 ze dne 24. 11. 2010, o zřízení evropského orgánu dohledu (Evropského orgánu pro pojišťovnictví a zaměstnanecké penzijní pojištění), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí EK 2009/79/ES. In: *Úřední věstník* [online], L 331, 15. 12. 2010, s. 48–83 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:32010R1094.

2.2.3 Obecná legislativa

Do druhé kategorie se řadí např. legislativní rámec ochrany spotřebitelů a hospodářské soutěže nebo také ochrana soukromí elektronických komunikací a informačních sítí, tj. na evropském poli čím dál tím více prioritizovaná digitalizace a KB. Dopad na pojišťovnictví je zřetelný např. také u směrnice AML/CFT[23].

Dále jsou samostatně upraveny některé typy pojištění, a to např. směrnicí o souborných cestovních službách[24] nebo nedávno revidovanou směrnicí o pojištění občanskoprávní odpovědnosti z provozu motorových vozidel[25]. Tento pro pojišťovnictví páteřní předpis je s GDPR silně propojen, přičemž lze předpokládat další zintenzivnění z důvodu rychlého vývoje nových technologií s přesahem do výkonu pojišťovací činnosti, např. IoT či autonomizace vozidel. Z důvodu limitace rozsahu této práce níže zmiňuji pouze vybrané oblasti přesahující do GDPR.

2.2.3.1 Ochrana spotřebitele

Ochrana spotřebitele, označovaná za tzv. „průřezovou disciplínu“[26], nese v pojišťovnictví významnou roli. Z hlediska této agendy je relevantní jak směrnice o právech spotřebitelů[27], tak zákon č. 634/1992 Sb., o ochraně spotřebitele. Dle čl. 3 odst. 3 písm. d) se tato směrnice nevztahuje na finanční služby. Nicméně v § 1840 OZ nebyly finanční služby, pokud jde o obecná ustanovení k uzavírání smluv distančním způsobem a závazky ze smluv uzavřených mimo obchodní prostory, vyňaty jako výjimka.[28]

---

[23] Směrnice EP a Rady (EU) 2015/849 ze dne 20. 5. 2015, o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení EP a Rady (EU) č. 648/2012 a o zrušení směrnice EP a Rady 2005/60/ES a směrnice EK 2006/70/ES. In: *Úřední věstník* [online], L 141(73), 5. 6. 2015 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?from=EN&uri=CELEX%3A32015L0849.

[24] Směrnice EP a Rady 2015/2302 ze dne 25. 11. 2015, o souborných cestovních službách a spojených cestovních službách, o změně nařízení EP a Rady (ES) č. 2006/2004 a směrnice EP a Rady 2011/83/EU a o zrušení směrnice Rady 90/314/EHS. In: *Úřední věstník* [online], L 326, 11. 12. 2015 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?from=EN&uri=CELEX%3A32015L2302.

[25] Směrnice EP a Rady (EU) 2021/2118 ze dne 24. 11. 2021, kterou se mění směrnice 2009/103/ES, o pojištění občanskoprávní odpovědnosti z provozu motorových vozidel a kontrole povinnosti uzavřít pro případ takové odpovědnosti pojištění. In: *Úřední věstník* [online], L 430(64), 2. 12. 2021, s. 1–23 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:L:2021:430:FULL&from=EN.

[26] ŠVENDOVÁ, Dagmar. *Legislativní proces EU z pohledu Evropského parlamentu: (na příkladu tzv. „Balíčku energetické účinnosti“)*. Ostrava: Key Publishing, 2011, s. 59. ISBN 978-80-7418-112-2.

[27] Směrnice EP a Rady 2011/83/EU ze dne 25. 10. 2011, o právech spotřebitelů, kterou se mění směrnice Rady 93/13/EHS a směrnice EP a Rady 1999/44/ES a ruší se směrnice Rady 85/577/EHS a směrnice EP a Rady 97/7/ES. In: *Úřední věstník* [online], L 304, 22. 11. 2011, s. 64–88 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:32011L0083.

[28] MESRŠMÍD, 2015, op. cit., s. 55.

Z hlediska distribuce pojistných produktů má význam také např. směrnice o uvádění finančních služeb pro spotřebitele na trh na dálku[29]. Do výrazné míry je tato úprava duplicitní k IDD. EK praktičtější prosazování a modernizaci spotřebitelského práva, zejména ve světle digitalizace, zohlednila např. ve své *Nové politice pro spotřebitele*[30]. To je nepochybně relevantní, jak uvádí Zuboff; proces digitalizace již krátce po roce 2000 zasáhl 98 % informací na světě[31].

Nová politika se odrazila také v roce 2020 ukončeném evropském legislativním procesu ke směrnici o zástupných žalobách na ochranu kolektivních zájmů spotřebitelů[32], kterou lze i v rámci pojišťovnictví aplikovat kromě tradičního spotřebitelského pojímání také v případech kolektivního porušení GDPR práv. Právě zde vidím přesah na čl. 80 GDPR, upravující zastupování subjektů OÚ neziskovým subjektem ve věcech podání stížností nebo uplatnění práv dle čl. 77–79, 82, bodu 142 preambule GDPR. Platí, že kdo v důsledku porušení GDPR utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu. Připouští se liberace, a to za okolnosti, že tito prokážou, že nenesou odpovědnost za událost, která ke vzniku újmy vedla. V případě většího počtu správců či zpracovatelů platí solidární, společná a nerozdílná odpovědnost.

Reálný dopad zákonem zatím netransponované směrnice upravující institut v českém prostředí dosud neznámý ukáže až čas a praxe. Z příkladu přístupu ÚOOÚ u sankcionování společnosti Mall v ČR[33] za rozsáhlý únik dat, který sice zvrátil NSS[34] (ale trvalo to tři roky), nebo z aktivit rakouské neziskové organizace *None of Your Business* (NOYB, založené Maxem Schremsem, lze dovodit, že tuto rovinu není vhodné ani z hlediska GDPR podceňovat. Dle mého názoru porušení GDPR nemusí vést pouze k sankcím *stricto sensu*. Nebezpečí, častokrát i více likvidačního charakteru, může spočívat v reputačním riziku a ztrátě důvěry subjektů OÚ či obchodních partnerů. Např. NOYB vyvinula systém, který

[29] Směrnice EP a Rady 2002/65/ES ze dne 23. 9. 2002, o uvádění finančních služeb pro spotřebitele na trh na dálku a o změně směrnice Rady 90/619/EHS a směrnic 97/7/ES a 98/27/ES. In: *Úřední věstník* [online], L 271, 9. 10. 2002, s. 16–24 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:32002L0065.
[30] EK. *Nová politika pro spotřebitele* [online]. V Bruselu: 2. 4. 2019 [cit. 16. 2. 2022]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/cs/IP_19_1755.
[31] ZUBOFF, Shoshana. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. London: Profile Books, 2019, s. 186–187. ISBN 978-1-78125-685-5.
[32] Směrnice EP a Rady (EU) 2020/1828 ze dne 25. 11. 2020, o zástupných žalobách na ochranu kolektivních zájmů spotřebitelů a o zrušení směrnice 2009/22/ES. In: *Úřední věstník* [online], L 409, 4. 12. 2020, s. 1–27 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32020L1828.
[33] ÚOOÚ. *Výroční zpráva 2018* [online]. ÚOOÚ, 2018 [cit. 19. 2. 2022]. ISBN 978-80-210-9225-9. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=33526.
[34] ČR. *Rozsudek NSS 1 As 238/2021–33* [online]. V Brně: 11. 11. 2021 [cit. 19. 2. 2022]. Dostupné z: http://www.nssoud.cz/files/SOUDNI_VYKON/2021/0238_1As__2100033S_20211111111159.pdf.

automaticky analyzuje toky souhlasů s cookies za účelem identifikace problémů s dodržováním předpisů. Pokud systém vyhodnotí cookie banner jako chybný, automaticky vygeneruje koncept zprávy, společně s návrhem případné stížnosti, která je při nečinnosti správce po 30 dnech zaslána DPA.

Zmíním také PLD[35], kterou analyzuji v předposlední kapitole této práce.

2.2.3.2 EPrivacy

Komplikovaný vztah se nachází mezi GDPR a ePrivacy, u které momentálně probíhá zdlouhavý proces revize zahrnující modernizaci obsahu a změnu její formy na nařízení, z důvodu překonání fragmentace národních úprav a sjednocení postavení uživatelů, což povede k jejich komfortnějšímu využívání služeb a zakotvení komplexnější úpravy elektronických komunikací s důrazem na aktuální vývoj v technologické a digitální oblasti v souladu s čl. 7, 8 LZPEU a na technologickou neutralitu.

Návrh revize ePrivacy je společně s GDPR součástí legislativního balíčku zaměřeného na ochranu a posílení jednotného digitálního trhu EU. Problematiku vymezila EK jako prioritní ve svém programu prací pro rok 2019, avšak až v roce 2021 dochází k započetí trialogů mezi EK, EP a Radou.

K datu vyhotovení této práce není možné odhadnout jejich konec, navzdory tomu, že k přijetí předpisu existuje silná politická vůle, jelikož v dnešní digitálně orientované společnosti probíhá čím dál tím větší množství komunikace elektronickou formou, zahrnující údaje osobní i neosobní povahy, jež se mohou nacházet v primární nebo strukturované podobě – metadata (odvozené údaje, např. čas, lokace, doba a délka volání, volaná čísla či navštívené weby) použitá k vyhodnocování chování, zvyků, preferencí apod. uživatele. To skýtá nepřeberné možnosti jejich využití ve prospěch samotného uživatele, v kontextu pojištění pak např. při tvorbě personalizovaných produktů a telematiky, ale i pro jejich zneužití.

I když návrh ePrivacy nevzbuzuje u veřejnosti ani poskytovatelů služeb šílenství srovnatelné s GDPR, ovlivní tato staronová regulace širokou škálu subjektů napříč trhem, a to včetně pojišťoven. Vysoká úroveň ochrany OÚ a jejich proporcionální zpracování jsou klíčovým faktorem i pro pojistný sektor z hlediska výkonu vlastní činnosti i důvěry veřejnosti.

[35] Směrnice Rady ze dne 25. 7. 1985, o sbližování právních a správních předpisů ČS týkajících se odpovědnosti za vadné výrobky. In: *Úřední věstník* [online], L 210, 7. 8. 1985, s. 29–33 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:31985L0374.

Vztah GDPR a v současnosti ještě účinné směrnice ePrivacy je výslovně vymezen čl. 95 a bodem 173 preambule GDPR, podle kterých GDPR neukládá žádné další povinnosti FO ani PO, pokud jde o zpracování ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích v EU, co se týče záležitostí, u nichž se na ně vztahují konkrétní povinnosti s týmž cílem stanovené v ePrivacy. U ePrivacy totiž došlo na základě názoru WP29 4/2007[36] k rozšíření některých ustanovení na PO. V tomto smyslu rozhodl i SDEU ve věci Société Colas Est vs. France.[37]

Pro futuro bude vůči GDPR nové nařízení ePrivacy patrně *lex specialis* – zvláštním, přednostním předpisem detailně upravujícím konkrétní část obecné úpravy GDPR, a tedy data elektronické komunikace, která lze považovat za OÚ. Z důvodu silného propojení obou předpisů bylo nezbytné důkladné vymezení jejich obsahu tak, aby nebyly duplicitní, či dokonce kontradiktorní. Zároveň bylo potřeba zohlednit přiměřenost mezi ochranou OÚ a vývojem nových digitálních byznysových modelů. Propojení těchto předpisů se věnoval i EDPB[38].

Návrh nařízení se věnuje všem typům elektronické komunikace bez ohledu na použité technické zařízení a zavádí také ochranu koncových zařízení technologicky neutrální formou, a to zaručením integrity informací uložených v koncovém zařízení a ochranou informací vysílaných z koncového zařízení, jelikož by mohly umožnit identifikaci koncového uživatele.

Proč je však natolik zásadní pro pojistný trh? Z tohoto hlediska je nejvíce relevantní úprava právních základů pro zpracování, která by měla být kompatibilní s čl. 6 GDPR. Navzdory tomu, že toto stanovisko bylo komunikováno i během konzultace předcházející hodnocení dle čl. 97 GDPR, EK dané problematice ve *Zprávě* nevěnovala přílišnou pozornost. Zmínka se nachází pouze v pracovním dokumentu[39], kde je tento postoj potvrzen, ale naneštěstí se

[36] Article 29 Data Protection Working Party. *Opinion 4/2007 on the concept of personal data* [online]. Brussels: Article 29 Data Protection Working Party, 20. 6. 2007 [cit. 19. 2. 2022]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.
[37] SDEU. *Rozsudek Soudního dvora ze dne 4. října 2018, Société Colas Est vs. France*, C416/17 [online]. 4. 10. 2018 [cit. 19. 2. 2022]. Dostupné z: https://curia.europa.eu/juris/document/document.jsf?text=&docid=206426&pageIndex=0&doclang=EN&.
[38] EDPB. *Stanovisko č. 5/2019 ke vzájemnému působení mezi směrnicí o soukromí a elektronických komunikacích a obecným nařízením o ochraně osobních údajů (GDPR), zejména pokud jde o příslušnost, úkoly a pravomoci úřadů pro ochranu údajů* [online]. EDPB, 12. 3. 2019 [cit. 19. 2. 2022]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_cs.pdf.
[39] European Commission. *Commission staff working document Accompanying the document Communication from the commission to the European parliament and the council Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data*

neodráží v návrzích nařízení ePrivacy. Dle dostupných podkladů je v čl. 8 návrhu nařízení zvažován jako dominantní právní základ souhlas, který přebírá požadavky GDPR. To je v kontextu efektivního poskytování pojistných služeb nevhodným přístupem, především v kontextu kontinuity poskytování služeb a odvolatelnosti souhlasu. To je relevantní především u inovativních služeb typu telematika (např. blackbox) u pojištění vozidel nebo u aplikací či přístrojů, které jsou součástí oděvu, tzv. *wearables* u ŽP, a které díky personalizaci umožní výhodnější podmínky pro klienty a zároveň mohou pozitivně ovlivnit jejich způsob řízení v oblastech jako rychlost, akcelerace nebo životní styl. Navzdory tomu, že rozvoj inovativních produktů je na českém trhu na počátku cesty, je vhodné předcházet možné budoucí překážce v konkurenceschopnosti.

V rámci trialogu je proto za vyhovující považována pouze formulace ve verzi Rady, která pojistitelům umožní poskytovat inovativní produkty typu telematika bez potřeby souhlasu. Zde je základním argumentačním bodem, že aby byl souhlas platný, musí být udělen svobodně. Pokud je však souhlas *condicio sine qua non* k uzavření pojistné smlouvy, může být vykládán jako nesvobodně udělený. To zmiňuje i EDPB, který ve svých pokynech 5/2020[40] explicitně uvedl, že souhlas není vhodným právním základem, je-li zpracování OÚ nezbytné pro plnění smlouvy. V praktické rovině je komplikací také právo souhlas kdykoliv odvolat a tím přerušit zpracování OÚ, které je nezbytné pro plnění smlouvy. Dle výkladu čl. 7 odst. 4 GDPR vyplývá, že situace „svazování“ souhlasu s přijetím podmínek nebo „vázání“ poskytnutí smlouvy nebo služby na žádost o souhlas se zpracováním OÚ, jež nejsou nezbytné pro plnění smlouvy ani poskytnutí služby, je považována za vysoce nežádoucí. Je-li souhlas za takovéto situace poskytnut, podle bodu 43 odůvodnění se nepovažuje za svobodný. Ustanovení čl. 7 odst. 4 GDPR se snaží zajistit, aby účel zpracování OÚ nebyl skrytý ani svázaný s poskytnutím smlouvy nebo služby, pro kterou nejsou tyto OÚ nezbytné. GDPR tím zabezpečuje, aby se zpracování OÚ, pro které se žádá o souhlas, nemohlo stát přímo ani nepřímo protiplněním smlouvy. Oba tyto zákonné základy pro zpracování OÚ, tj. souhlas a smlouva, nemohou být sloučeny a jejich hranice rozostřeny. Co se týká řešení, tato praktická potíž by se dle mého názoru dala odstranit doplněním právních základů plnění smlouvy a oprávněného zájmu k danému účelu do návrhu ePrivacy.

Protection Regulation [online]. Brussels: 24. 6. 2020 [cit. 19. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0115.

[40] European Data Protection Board. *Guidelines 05/2020 on consent under Regulation 2016/679*. Version 1.1 [online]. Brussels: EDPB, 4. 5. 2020 [19. 2. 2022]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

Diskuze k aktuální revizi jsou ale zdlouhavé. Fakt, že se jedná o rozvleklý projekt, se dá dedukovat i z vyjádření Smejkala[41] v publikaci z roku 2018, kde již v té době uvedl, že situace kolem tohoto předpisu není ani jednoduchá, ani přehledná. Debaty připomínají z celkového hlediska spíše točení v bludném kruhu a je složité odhadovat, zda, kdy a s jakým obsahem bude legislativní proces uzavřen. Lze jen doufat, že bude spíše objektivním mantinelem jako GDPR, nikoli legislativní brzdou faktického pokroku.

2.2.3.3 KB

Úvodem je vhodné vyjasnit, že technické hledisko a hledisko KB jsou čím dál tím víc podstatným aspektem plnohodnotného provozu, zajišťovaní služeb a kontinuity ve vztahu k samotným pojišťovnám i ve vztahu ke klientům, a to i v postavení subjektů OÚ. Dynamický rozvoj ICT, jejich význam pro fungování společnosti a vzrůstající riziko sofistikovanějších kybernetických útoků[42] totiž vedou ke zvýšené potřebě zabezpečení systémů a dat, především OÚ[43].

Ochranu OÚ je proto třeba vnímat v širším kontextu KB a prevence nežádoucích kybernetických incidentů, které mohou vést ke zničení, ztrátě, pozměňování, neoprávněnému zpřístupnění zpracovávaných OÚ[44] nebo neoprávněnému přístupu k nim. I při dosažení nejvyšší míry souladu s legislativními požadavky je však faktický vývoj v oblasti kybernetických hrozeb natolik pružný, že ne vždy lze předvídat všechny možné varianty narušení KB. Úkol prevence je tak ze dne na den ztížen extrémně dynamickým vývojem, ale i vynalézavostí hackerů či častým selháním lidského faktoru. Navzdory tomu, že v této oblasti panuje nejednotnost taxonomie, už třeba i u základního pojmu, jako je „kybernetické riziko“, stávají se kybernetická rizika nejen ve vztahu k pojišťovnictví fenoménem.[45]

---

[41] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Druhé, rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, s. 252. ISBN 978-80-7380-720-7.
[42] V roce 2019 bylo v oblasti kybernetické kriminality evidováno 8417 trestných činů, což je ve srovnání s rokem 2018 nárůst o více než 1600 skutků. Tradičně nejpočetnější skupinou jsou různé formy podvodného jednání, vedle kterých jsou nemalou měrou zastoupeny i pojistné podvody. Téměř o jednu třetinu vzrostl počet případů tzv. „hackingu“ (na 930), zejména případy neoprávněného přístupu k počítačovému systému a nosiči informací. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx.
[43] Ve finančním a pojistném sektoru bylo v roce 2021 83 % případů porušení zabezpečení dat orientováno právě na OÚ. Dostupné z: https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report.
[44] POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 541. Právní monografie. ISBN 978-80-7598-045-8.
[45] SMEJKAL, Vladimír. Formy kybernetické kriminality a jejich možný vliv na pojišťovací praxi. *Pojistný obzor: časopis českého pojišťovnictví* [online]. 2020, (2), s. 44–51 [cit. 15. 2. 2022]. ISSN 2464-7381. Dostupné z: https://www.pojistnyobzor.cz/archiv/92-2020-2.

Tento vývoj je vnímán ve dvou rovinách. Zaprvé z hlediska kybernetické ochrany samotných pojišťoven, což je rozebráno v DORA. To reflektuje i EIOPA[46], která se zabývá rostoucí hrozbou kybernetických útoků pro odvětví, jakož i důsledky pro podnikání v oblasti kybernetického upisování. EIOPA kromě jiného uvádí, že pojistný sektor je přirozeným cílem kybernetických útoků, protože disponuje značným množstvím důvěrných údajů o pojistnících. Produkty, pojistné smlouvy a ceny jsou založeny na datech. Právě proto jsou tak hodnotné. Díky datům je pojišťovna schopna nabídnout spotřebiteli vhodný produkt za proporcionální cenu. Větší výběr a nižší náklady jsou důvodem, proč jsou spotřebitelé ochotni sdílet své údaje. Na rozdíl od jiných odvětví finančních služeb, která uchovávají především citlivé finanční údaje, pojišťovny obvykle shromažďují také velké množství citlivých OÚ. I proto EIOPA vyjádřila pozitivní názor na DORA.

Zadruhé je relevantní hledisko nabídky pojistných produktů s kybernetickým přesahem, kterému se zde však z důvodu limitace rozsahu nemám prostor věnovat, je ovšem v hledáčku EIOPA, jež např. publikovala zprávu *Cyber risk for insurers – challenges and opportunities*[47], věnovanou zlepšení porozumění kybernetických rizik, nebo *Cyber underwriting strategy*[48].

Co se týká současné úpravy, v českém právním řádu je základní obecnou povinností prevence dle § 2900 a násl. OZ. Její nerespektování může vést ke vzniku odpovědnosti za škodu. Konkrétním výchozím předpisem v oblasti KB je pak ZoKB, doplněný o podzákonné předpisy. Zákon byl novelizován zákonem č. 205/2017 Sb., čímž byla provedena transpozice NIS a ustanoven NÚKIB. NIS zavedla *ex ante* připravenost na KB. Věcná působnost těchto norem je užší než u GDPR. Je limitována pouze na některé typy subjektů v rámci kritické informační infrastruktury a významných IS. NIS má za cíl harmonizovat právní úpravu v oblasti bezpečnosti sítí a IS a zavést jednotný standard úrovně KB[49]. Až na nepočetné výjimky nespadá většina pojišťoven na českém trhu pod regulaci NIS, popř. ZoKB. To však neznamená, že tyto předpisy nejsou faktickou inspirací pro zajištění vysoké míry kompatibility z důvodu vlastního zájmu na KB.

[46] EIOPA. *Cyber risks: what is the impact on the insurance industry?* [online]. © EIOPA, 15. 10. 2021 [cit. 16. 2. 2022]. Dostupné z: https://www.eiopa.europa.eu/media/feature-article/cyber-risks-what-impact-insurance-industry.
[47] EIOPA. *Cyber risk for insurers – challenges and opportunities* [online]. Luxembourg: Publications Office of the European Union, 2019 [cit. 16. 2. 2022]. ISBN 978-92-9473-213-2. Dostupné z: https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf.
[48] EIOPA. *Eiopa strategy on cyber underwriting* [online]. EIOPA, © 2020 [cit. 16. 2. 2022]. ISBN 978-92-9473--225-5. Dostupné z: https://www.eiopa.europa.eu/document-library/strategy/cyber-underwriting-strategy_en.
[49] SMEJKAL, 2018, op. cit., s. 252.

I když spolu předpisy GDPR a NIS úzce souvisejí, není záběr jejich dopadu stejný. GDPR je specifičtější – zakotvuje ochranu OÚ a bezpečnostními hledisky se po technické stránce nezaobírá. Vzájemná propojenost GDPR a NIS je ale znatelná v prioritizaci prevence vymezením požadavků na zavedení TOO a notifikační povinnosti. Zároveň oba předpisy zakotvují povinnost ohlašování incidentů DPA na národní úrovni (dle GDPR ÚOOÚ, dle NIS NÚKIB), popř. za určitých okolností i dotčeným subjektům. Specifikem NIS je zavedení možnosti dobrovolného ohlašování incidentů ze strany subjektů.

Koncem roku 2020 byla ukončena veřejná konzultace EK k revizi NIS (NIS2), kterou je potřeba vnímat v kontextu DORA. Vztah DORA k NIS je totiž *lex specialis*. NIS už brzy nebude osamoceným KB předpisem.

EK na začátku mandátu vyhlásila prioritizaci digitální a kybernetické agendy[50]. V roce 2020 došlo k veřejným konzultacím a publikacím ESD[51], *Bílé knihy k umělé inteligenci*[52], DFS[53] a *Strategie kybernetické bezpečnosti EU pro digitální dekádu*[54]. Na koncepční dokumenty navazují konkrétní legislativní návrhy, např. právě NIS2, a návrhy nařízení pro oblast správy a recipročního sdílení dat na evropské úrovni či pro etické a odpovědnostní aspekty úpravy UI, kterým je věnována předposlední kapitola této práce.

Páteřním předpisem s výrazným dopadem i na pojistný sektor je principově a rizikově formulovaná DORA. Ten pojistným sektorem již od veřejné konzultace EK výrazně rezonuje. Považuji za relevantní zmínit, že tento rámec nedopadne jen na stabilní, tradiční instituce, ale také na fintech, start-upy či obchodníky s kryptoaktivy, u kterých tak může dojít k radikálnějším změnám v oblasti zabezpečení KB. Ze strany pojistného sektoru je zdůrazňována[55] nutnost kompatibility a prevence duplicity s existujícím právním rámcem, a to

[50] DIGITALEUROPE. *Von der Leyen is right: Digital is the 'make-or-break' issue* [online]. 15. 9. 2021 [cit. 16. 2. 2022]. Dostupné z: https://www.digitaleurope.org/news/von-der-leyen-is-right-digital-is-the-make-or-break-issue/.
[51] EK. *Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů. Evropská strategie pro data* [online]. V Bruselu: 19. 2. 2020 [cit. 16. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52020DC0066.
[52] European commision. *White Paper on Artificial Intelligence: a European approach to excellence and trust* [online]. Brussels: 19. 2. 2020 [cit. 16. 2. 2022]. Dostupné z: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.
[53] EK. S*dělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů o strategii EU v oblasti digitálních financí* [online]. V Bruselu: 24. 9. 2020 [cit. 16. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0591.
[54] EK. *Společné sdělení Evropskému parlamentu a Radě*. *Strategie kybernetické bezpečnosti EU pro digitální dekádu* [online]. V Bruselu: 16. 12. 2020 [cit. 19. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52020JC0018.
[55] IE. *Position on the European Commission proposal for a Digital Operational Resilience Act* [online]. Brussels: IE, 22. 2. 2021 [cit. 16. 2. 2022]. Dostupné z:

např. NIS, GDPR, SII, ale i stávajícími mezinárodními normami a pokyny Agentury EU pro KB (ENISA) či EIOPA, prozatím *Obecnými pokyny k outsourcingu u poskytovatelů cloudových služeb*[56] a pokyny pro bezpečnost a řízení a kontrolu ICT[57].

Není zde prostor detailně rozebírat obsah DORA. Ten pokryje oblasti ICT rizikového managementu, testování, úpravy vztahů s ICT TPPs, sdílení dat, dohledu a také ohlašování. Zaměřím se proto pouze na oblasti dle mého názoru relevantní k GDPR.

Cílem DORA není v přímočaré rovině úprava OÚ. Dle mého názoru je však z faktického hlediska podmínka nejvyššího možného zajištění KB fundamentálním předpokladem ke splnění předpokladů pro vytvoření prostředí, v jehož rámci lze GDPR následně aplikovat. To ostatně deklarovala i EK ve *Zprávě,* viz kapitola 6 této práce. Pojistný sektor iniciativu EK vítá, jelikož registruje potřebu posílení právní jistoty i odstranění fragmentace a přeshraničních překážek. Toho lze dle mého názoru smysluplně dosáhnout zavedením proporcionální, rizikově a principově orientované úpravy (např. u ICT managementu či testování, ohlašování incidentů dle závažnosti, počtu prováděcích regulatorních technických standardů), která nebude nadbytečně preskriptivní co do technických metod. Proporcionalitu požadavků je vhodné zohlednit jak ve vztahu k velikosti, tak míře rizikovosti dotčených subjektů. Tyto faktory zároveň umožní *pro futuro* stabilitu regulace a neomezí budoucí inovace.

Dohledovým orgánem na národní úrovni bude dle DORA ČNB. Tak je tomu i podle SII. Ohlašovací povinnosti v režimu GDPR, NIS, SII a DORA vůči různým autoritám je tak třeba nastavit efektivně, aby nedocházelo ke zbytečné administrativní zátěži povinných subjektů a dohledových orgánů, jak bylo naznačeno výše.

Přesah do GDPR spatřuji v několika dalších oblastech. V první řadě je to úprava vztahů k ICT TPPs, kdy pojišťovny i další subjekty registrují výraznou míru omezené vyjednávací a

---

https://www.insuranceeurope.eu/publications/1646/position-on-the-european-commission-proposal-for-a-digital-operational-resilience-act/download/Position+on%20the%20European%20Commission%20proposal%20for%20a%20Digital%20Operational%20Resilience%20Act.pdf.

[56] EIOPA. *Obecné pokyny k outsourcingu u poskytovatelů cloudových služeb* [online]. Frankfurt nad Mohanem: EIOPA, 2020 [cit. 16. 2. 2022]. Dostupné z: https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_cz_0.pdf.

[57] EIOPA. *Guidelines on information and communication technology security and governance* [online]. Frankfurt: EIOPA, 8. 10. 2020 [cit. 16. 2. 2022]. Dostupné z: https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/eiopa-bos-20-600-guidelines-ict-security-and-governance.pdf?source=search.

smluvní svobody a následné exit strategie. To je způsobeno patovou situací, kdy omezený počet ICT TPPs na trhu v podstatě jednostranně určuje předem standardizované podmínky poskytování služeb. Proto by DORA měla obsáhnout řešení asymetrických smluvních vztahů a pevně odkázat na nutnost nakládání s OÚ dle standardu GDPR, a to i v častých situacích, kdy mají ICT TPPs přeshraniční či mezinárodní povahu. Na hledisko asymetrie smluvních vztahů mezi technologickými giganty a spotřebiteli či jinými podnikatelskými subjekty upozorňuje také Zuboff[58]. Ta varuje před negativními konsekvencemi adhezních smluv, kdy v rámci přístupu „*take it or leave it"* nemá subjekt v postavení slabší smluvní strany reálnou možnost ovlivnit obsah smluvních podmínek. Právě zde je ale zvýšena koncentrace rizik i pro ochranu OÚ, což zohledňuje i DORA v čl. 27 odst. 2 písm. c). Proto je nutné nezapomínat na kapitolu 5 GDPR a Schrems II. DORA se kladně věnoval také EDPS ve svém názoru 7/2021[59]. Zdůraznil důležitost zpracování OÚ na právních základech dle čl. 6 GDPR a jasného vymezení rolí a povinností správců a zpracovatelů. Jako základní předpoklad kybernetické ochrany OÚ stanovil také zakotvení vhodných TOO, DPIA a systému ohlašování porušení.

DORA upravuje i dobrovolné sdílení dat a zkušeností s kybernetickými hrozbami. Z důvodu předvídání této legislativní iniciativy i faktického vývoje v oblasti KB v rámci mého působení v PS Kybernetická bezpečnost ČAP vypracovala v průběhu roku 2021 *Samoregulační standard pro sdílení informací o kybernetické bezpečnosti*. Ten není vzhledem ke své povaze veřejně přístupný. Opětovně je vyjádřením dobrovolného závazku pojišťovny připojit se k systému výměny informací o KB. V kontextu GDPR uvádím, že sdílené informace obsahují OÚ v souladu s principem minimalizace, a tedy pouze v rozsahu nutném k identifikaci původce a incidentu. Ke sdílení OÚ dochází na základě právního titulu oprávněného zájmu dle čl. 6 odst. 1 písm. f) GDPR, kterým je prevence protiprávního jednání a ochrana majetku a KB ČAP a pojišťoven. Tento závěr byl následně potvrzen zmíněným názorem EDPS, který ve věci dobrovolného sdílení dat a zkušeností o kybernetických hrozbách neidentifikoval z pohledu GDPR překážky. Jako primární právní základ také vymezil oprávněný zájem, je-li splněna podmínka balančnosti s ochranou individuálních práv. Standard dnes upravuje pouze postupy pojistného sektoru, ale do budoucna se zvažuje mezisektorové rozšíření, což je v souladu s evropskými tendencemi. EIOPA opakovaně proklamuje centralizovanou,

[58] ZUBOFF, 2019, op. cit., s. 236–237.
[59] EDPS. *Opinion 7/2021 on the Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) 1060/2009, (EU) 648/2012, (EU) 600/2014 and (EU) 909/2014* [online]. Brussels: EDPS, 10. 5. 2021 [cit. 16. 2. 2022]. Dostupné z: https://edps.europa.eu/system/files/2021-05/2021-0203_d0943_opinion_digital_operational_resilience_for_the_financial_sector_en.pdf.

anonymizovanou databázi incidentů. Podle mě by spolupráce v této oblasti měla být zahájena na dobrovolné bázi a inspirována by měla být povinností ohlašování podle NIS a GDPR. Ideální by byla jednotná, strukturovaná, anonymizovaná podoba za zachování granularity, jejíž výhody analyzuji v této práci u šablony, která je přílohu *Standardů*. Je však samozřejmé, že tyto předpisy upravují a podchycují pouze zlomek kybernetických incidentů. GDPR sice reguluje incidenty, které mohou přinést negativní konsekvence vůči právům subjektů OÚ, kybernetické hrozby jsou však mnohem širší a dopad může být i nepřímý. Proto považuji za nezbytnou spolupráci napříč odvětvími na národní i evropské úrovni. Významnou roli v této věci může sehrávat ENISA a načrtnutý rámec DORA. Komplikací však může být nejednotná taxonomie, vedoucí ke komparačním a statistickým potížím.

Závěrem je nutno podotknut, že má stanoviska vycházejí z verzí návrhů NIS2 a DORA EK, EP a Rady dostupných k datu vyhotovení této práce. Finální verzi zvolených formulací proto nelze predikovat.

3 Ochrana OÚ

3.1 Historický exkurz

Při pohledu na obsah GDPR lze vidět, že se jedná o relativně širokou úpravu výrazně unifikující ochranu OÚ. Co však přijetí tohoto nařízení předcházelo? A na jaké existující podmínky pojistné odvětví navázalo při jeho implementaci?

GDPR pochopitelně nevzniklo na zelené louce. Jedná se o výsledek dlouhotrvající iniciativy pro posílení a sjednocování rámce ochrany OÚ, kterou se povedlo uvést v život. Dovolím si tvrdit, že tím byl vytvořen velmi solidní legislativní základ, který EU posunul na 1. místo v dané oblasti a vytvořil globální vzor. Proces evoluce ochrany OÚ ovšem není předmětem této práce. Považuji však za vhodné nejdříve krátce nastínit cestu od prvotní zmínky o důležitosti práva na soukromí v článku „Právo na soukromí“[60] z 19. století až k GDPR, reflektujícímu offline i online život v 21. století.

Jako reakce na druhou světovou válku byly přijaty multilaterální lidskoprávní úmluvy, např. právně nezávazná VDLP a EÚLP Rady Evropy. Právo na přístup k informacím, vymezené např. čl. 10 EÚLP, respektuje základní vlastnost informací a předpokládá jejich rozšiřování v souladu se zásadou publicity, ochrany soukromí a OÚ. To platí zejména pro ochranu OÚ, jejíž systém stojí na prevenci škody, kontrole dat a zajištění toho, že nebudou použity v rozporu s právy subjektů OÚ.[61] EÚLP tak budoucí praxi výrazně posunula nejen díky svému obsahu, ale také zřízením ESLP, jehož judikatura se stala určujícím výkladovým nástrojem celoevropských rozměrů. Dále uvedu LZPEU, která je na základě *Lisabonské smlouvy*, platné od roku 2009, inkorporována do evropského právního rámce a dle čl. 6 odst. 1 SEU je nadána identickou právní silou jako smlouvy. Oblast ochrany OÚ nepomíjí ani primární evropská legislativa; čl. 16 SFEU garantuje každému právo na ochranu OÚ, které se jej týkají.

[60] WARREN, Samuel D. a BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review* [online]. 1890, 4(5) [cit. 16. 2. 2022]. Dostupné z: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

[61] GELLERT, Raphaël. Understanding Data Protection as Risk Regulation. *Journal of Internet Law* [online]. 2015, 18(11) [cit. 15. 2. 2022]. Dostupné z: https://www.researchgate.net/publication/301552462_Understanding_Data_Protection_As_Risk_Regulation.

Během 20. století docházelo v souvislosti s tržním rozvojem k formování množství databází OÚ. OECD v roce 1980 přijala nezávaznou směrnici[62]. Následně došlo k přijetí *Úmluvy 108*[63], modernizované v roce 2018. V té době se však jednalo o první evropský právně závazný nástroj pro ochranu OÚ.

Co však právo na soukromí znamená v kontextu této práce? Filozofických směrů je několik, společným základem je v obecné rovině právo na soukromý život. Centrálním pojmem je v tomto směru „informační sebeurčení" (*informationelle Selbstbestimmung*[64]).

Pasivní komponentou informačního sebeurčení je informační soukromí a ochrana OÚ. Aktivní komponentu tvoří to, co by se dalo označit za „právo na soukromou informační interakci".[65] Jedná se tedy o kontrolu nad hranicí soukromí. To např. Clarke dělí do pěti kategorií. Čtvrtou dimenzí je právě soukromí OÚ projevované kontrolou nad obsahem a zpracováním. Pátou dimenzí, následkem technologických a společenských změn, je pak soukromí osobního zážitku a zkušeností v kontextu profilování a dalších aktivit podobného charakteru.[66]

Předmětem této práce je tedy pouze zlomek relativně širokého pojmu „soukromí", tedy proporcionální ochrana OÚ s dopadem na specifické odvětví – pojišťovnictví. Hranice soukromí jsou nabourávány nejen v kyberprostoru, ale skrze inovativní uplatnění technologií také v mnoha instancích běžného světa kolem nás. Příklady lze nalézt v dnes již tradičních, všudypřítomných kamerových systémech, GPS lokátorech v mobilních telefonech, tělesných skenerech na letištích, identifikaci na základě biometrických údajů, IoT či dronech.[67] Nejen tyto faktory přispěly k nutnosti zakotvení minimálního rámce ochrany OÚ na evropské úrovni.

---

[62] OECD. *Přehled: směrnice OECD o ochraně soukromí a přeshraničních tocích osobních údajů* [online]. © OECD, 2003 [cit. 16. 2. 2022]. Dostupné z: https://www.oecd.org/digital/ieconomy/15589535.pdf.

[63] ÚOOÚ. *Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat ve znění jejího protokolu CETS č. 223: pracovní překlad* [online]. ÚOOÚ, 28. 1. 1981 [cit. 16. 2. 2022]. Dostupné z: https://rm.coe.int/1680994818.

[64] Pojem užíván bez ohledu na jurisdikci; je připisován Spolkovému ústavnímu soudu, který jej použil v rozhodnutí ze dne 15. 12. 1983, o právní úpravě sčítání lidu, *Volkszählung*, sp. zn. Az 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/ 83, bod 172–175. Dostupné z: https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BVerfG&Datum=15.12.1983&Aktenzeichen=1%20BvR%20209%2F83.

[65] POLČÁK et al., 2018, op. cit., s. 21.

[66] CLARKE, Roger. Introduction to Dataveillance and Information Privacy, and Definitions of Terms. In: *Roger Clarke's Website* [online]. Canberra: Xamax Consultancy Pty Ltd, 15. 8. 1997. 24. 7. 2016 [cit. 16. 2. 2022]. Dostupné z: http://www.rogerclarke.com/DV/Intro.html.

[67] POLČÁK et al., 2018, op. cit., s. 427.

Před účinností GDPR byla základním předpisem směrnice EP a Rady 95/46/ES ze dne 24. 10. 1995, o ochraně FO v souvislosti se zpracováním OÚ a o volném pohybu těchto údajů. Tento model de Azevedo Cunha popisuje jako vyrovnaný, stimulující volný pohyb služeb a zboží bez omezení individuálních základních práv, především práva na soukromí a OÚ. Na druhé straně přiznává existenci prostoru pro hlubší harmonizaci vzhledem k výrazným rozdílům v úpravách jednotlivých ČS[68]. Vyjma marginální změny z roku 2003[69], nemající dopad na samotné zpracování OÚ, totiž nebyla směrnice novelizována.

GDPR na základě čl. 94 směrnici zrušilo a dne 25. 5. 2018 vstoupilo v účinnost. Fragmentace mezi ČS sice přetrvává v některých klíčových oblastech, jako je např. přístup dohledových orgánů, právní titul pro zpracování zdravotních OÚ nebo postavení dětí, obecně však došlo k posílení harmonizačního rámce.

3.2 GDPR

3.2.1 Forma

V rámci fragmentace ochrany OÚ a z důvodu nutnosti jednotného postupu pro rozvoj vnitřního trhu byla u předpisu k vymezení standardů ochrany OÚ v EU, GDPR, nově zvolena forma nařízení. To je závazné v celém rozsahu a přímo použitelné ve všech ČS a je určené nespecifickému množství subjektů. Z hlediska funkce je hlavním sjednocujícím nástrojem rozvoje práva EU, který platí unitárně a bezprostředně, tj. i bez prováděcího vnitrostátního aktu. Je integrální součástí právních řádů a automaticky potlačuje aplikaci jemu odporujícího vnitrostátního práva. Jednotlivci se ho mohou dovolávat stejným způsobem jako předpisu práva národního. Nařízení je tak nejúplnějším a nejvíce bezprostředním opatřením v rámci arzenálu nástrojů sbližování práva. Přímý účinek nařízení se tak presumuje[70], což potvrdil SDEU, když uvedl, že „díky své povaze a funkci v systému pramenu práva Společenství mají

[68] DE AZEVEDO CUNHA, 2013, op. cit., s. 18.
[69] Nařízení EP a Rady (ES) č. 1882/2003 ze dne 29. 9. 2003, o přizpůsobení ustanovení týkajících se výborů, které jsou nápomocny EK při výkonu jejích prováděcích pravomocí stanovených v právních aktech Rady a přijatých postupem podle čl. 251 *Smlouvy o ES*, ustanovením rozhodnutí 1999/468/ES. In: *Úřední věstník* [online]. L 284, 31. 10. 2003, s. 1–53 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32003R1882&from=EN.
[70] BOBEK, Michal, BŘÍZA, Petr a KOMÁREK, Jan. *Vnitrostátní aplikace práva Evropské unie*. Praha: C. H. Beck, 2011, s. 56. Beckova edice Právo. ISBN 978-80-7400-377-6.

nařízení přímý účinek a jako taková jsou způsobilá vytvářet individuální práva“[71]. Obecný zákaz transpozice nařízení SDEU potvrdil ve věci Variola[72]. Výjimka je přípustná za situace, kdy určitou materii nebo její aspekty upravují vzájemně propojeným, ovšem nepřehledným způsobem jedno či více nařízení a vnitrostátní předpisy[73] a nedojde k zastření unijního původu, povahy ani právních účinků obsahu nařízení.

3.2.2 Účel

Ratio legis řady forem nakládání s OÚ, které obsahují výpovědní hodnotu o FO, je nutno vnímat i ve světle rostoucího vlivu dění v kyberprostoru na každodenní fungování většiny z nás. Digitální ekonomika a společnost stojí na nakládání s daty, které často obsahují informace o osobních projevech či složkách osobnosti identifikovatelné FO. S razantně narůstajícím množstvím těchto datových toků roste také míra jejich využitelnosti s kladnými i zápornými důsledky pro dotčené osoby. Zásahy do osobnostních či jiných základních práv a svobod skrze zpracování OÚ mohou nabývat různé intenzity.[74]

Tato práce je věnována aktuální úpravě v souvislostech pojišťovnictví, jakožto i komplexně oboru finančních služeb, kde jsou tyto tendence patrné. Data obecně, OÚ ještě o to více, bývají označována jako „nové zlato“. Proto je relevance OÚ pro pojišťovnictví a kompatibilita s právním rámcem GDPR nosným tématem této práce.

Přijetí GDPR předcházela silná mediální kampaň. Mluvilo se o revoluci v oblasti ochrany OÚ. Já se přikláním spíše k evoluci. Byla medializována především rozšířená práva subjektů OÚ a výše možných sankcí, častokrát s přívlastkem „drakonické“. Právní *compliance* týmy tak společně s IT experty stáli před úkolem implementace. Přínos GDPR v oblasti regulace zacházení s neustále podstatnější kategorií údajů – OÚ – však nelze popřít. Jeho význam průběžně vyzdvihuje např. Zuboff v díle *The age of surveillance capitalism* nebo Nulíček

[71] SDEU. *Rozsudek Soudního dvora ze dne 14. prosince 1971. Politi s.a.s. proti Ministero delle Finanze della Republica Italiana*, C43/71 [online]. 14. 12. 1971 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX:61971CJ0043.
[72] SDEU. *Rozsudek Soudního dvora ze dne 10. října 1973. Fratelli Variola S.p.A. proti Amministrazione italiana delle Finanze*, C34/73 [online]. 10. 10. 1973 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:61973CJ0034.
[73] SDEU. *Rozsudek Soudního dvora ze dne 28. března 1985. Komise Evropských společenství proti Italské republice*, C272/83 [online]. 28. 3. 1985 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:61983CJ0272.
[74] POLČÁK et al., 2018, op. cit., s. 434.

a kol. ve svém komentáři[75], kde ho charakterizuje jako „nejvýznamnější legislativní počin v oblasti ochrany OÚ za posledních 20 let“.

3.2.3 Obsah

Unifikující předpis je strukturován do preambule, která obsahuje 173 ustanovení a 99 článků nařízení. Krátce rozeberu úvodní ustanovení i další instituty a jejich dopad pak vykreslím v pojistném kontextu na základě modelové samoregulační úpravy.

GDPR vzhledem k svému univerzálnímu rázu vymezuje obecně platná, sjednocující pravidla neboli principy pro zpracování OÚ, včetně práv subjektu OÚ. Předmět a cíle jsou popsány hned v čl. 1 GDPR. Jedná se o pravidla týkající se ochrany FO (na rozdíl třeba od ePrivacy) v souvislosti se zpracováním OÚ a volného pohybu OÚ; GDPR je vnímáno jako horizontální předpis zakotvující princip předběžné opatrnosti ve věci ochrany OÚ.

OÚ rozumím dle dikce čl. 4 odst. 1 GDPR veškeré informace o identifikované nebo identifikovatelné FO (subjektu OÚ), tedy takové, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, např. jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této FO. Nepřímou identifikací je kombinace několika složek, které samy o sobě identifikátory nejsou, ale jejich spojování identifikaci umožňuje. GDPR se nevztahuje na anonymní informace ani na OÚ anonymizované tak, že subjekt OÚ již přestal být identifikovatelným. I když jsou známy techniky reidentifikace či vzájemného propojení anonymizovaných údajů za účelem identifikace, nebudu se jimi zde zaobírat.

S rostoucí podrobností naší digitální stopy roste spektrum informací, které lze považovat za nepřímé identifikátory, a tudíž OÚ. Pojem „osobní údaje“ se stává zásadním určovatelem hranic naší virtuální (a reálné) identity. Na základě rozhodnutí ESLP vycházejícího z definice OÚ v čl. 2 *Úmluvy 108* ve věci S. a Marper vs. Spojené království[76] bylo rozhodnuto, že i

[75] NULÍČEK, Michal et al. *GDPR – obecné nařízení o ochraně osobních údajů.* Praha: Wolters Kluwer, 2017. 580 s. Praktický komentář. ISBN 978-80-7552-765-3.
[76] ESLP. *Rozhodnutí velkého senátu Evropského soudu pro lidská práva ze dne 4. prosince 2008 ve věci S. a Marper proti Spojenému království* [online]. Wolters Kluwer, 4. 12. 2008 [cit. 20. 2. 2022]. Dostupné z: http://eslp.justice.cz/justice/judikatura_eslp.nsf/0/EA8CFA7D862952D2C1258487002E9626/$file/S.%20a%20Marper%20proti%20Spojen%C3%A9mu%20kr%C3%A1lovstv%C3%AD_rozsudek.pdf?open&.

otisky prstů, buněčné vzorky a profily DNA zasluhují míru ochrany jako OÚ, které je z nich možné dovodit. Je tomu tak třeba i u dynamické IP adresy[77].

Následně je čl. 2 definována věcná působnost předpisu. Dopadá na zcela nebo částečně automatizované zpracování OÚ a na neautomatizované zpracování těch OÚ, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.

Zpracováním rozumím dle čl. 4 odst. 2 operace, při kterých je s OÚ nakládáno ze strany zpracovatele, podle pokynů správce, nebo samotného správce, který určuje účel a formu zpracování a nese primární odpovědnost. Výjimkou jsou situace, kdy zpracovatel z vlastní iniciativy určuje účel a prostředky zpracování a kdy je ve vztahu k tomuto zpracování považován za správce. O zpracování v tomto smyslu se nejedná v případech osobní či domácí činnosti, jako je např. seznam kontaktů.

Univerzální místní působnost zakotvuje čl. 3 nařízení. GDPR se vztahuje na zpracování OÚ v souvislosti s činnostmi provozovny správce nebo zpracovatele v EU a EHP, tedy na Islandu, v Norsku a Lichtenštejnsku, bez ohledu na to, zda v ní zpracování probíhá, což specifikuje bod 22 preambule GDPR. Vzhledem k radikálně vzrůstajícímu významu elektronické formy OÚ a outsourcingu služeb je teritorialita významným aspektem. Hlouběji je problematika analyzována pokyny EDPB 3/2018[78] a kapitolou 5.6 této práce.

Čl. 3 odst. 2 GDPR dále uvádí, že tento právní rámec se vztahuje na zpracování OÚ subjektů, které se nacházejí v EU, správcem nebo zpracovatelem, jenž není usazen v EU, pokud činnosti zpracování souvisejí s nabídkou zboží nebo služeb těmto subjektům OÚ v EU, bez ohledu na to, zda je od subjektů OÚ požadována platba, nebo souvisejí s monitorováním jejich chování, pokud k němu dochází v rámci EU. Pro tyto situace je podpůrně aplikován čl. 27 GDPR, kdy správce nebo zpracovatel písemně jmenuje svého zástupce v EU. I zde platí odpovědnost, jak je definována v čl.24 a násl. GDPR, příp. výkon pravomocí DPA podle čl. 58 a násl. i čl. 83 GDPR.

Výjimka je použitelná pro případy příležitostného zpracování, zpracování nezahrnujícího ve velkém měřítku zvláštní kategorie OÚ podle čl. 9 odst. 1 GDPR nebo OÚ týkajících se

[77] SDEU. *Rozsudek Soudního dvora (velkého senátu) ze dne 18. července 2017. Evropská komise vs. Patrick Breyer,* C213/15 P [online]. 18. 7. 2017 [20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A62015CJ0213.

[78] EDPB. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* [online]. Version 2.1. Brussels: EDPB, 12. 11. 2019 [16. 2. 2022]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

rozsudku v trestních věcech a trestných činů podle čl. 10 GDPR a takového zpracování, u něhož je nepravděpodobné, že by s ohledem na svou povahu, kontext, rozsah a účely představovalo riziko pro práva a svobody FO.

Pro úplnost uvádím, že GDPR se taktéž vztahuje na zpracování OÚ správcem, který není usazen v EU, ale na místě, kde se právo ČS uplatňuje na základě mezinárodního práva veřejného. Teritorialitu výstižně komentuje Smejkal[79], podle kterého i když žijeme v době globálního, propojeného světa a všeobecného opojení cloudem (jedná se o způsob používání počítačových technologií [služeb, programů] uložených na serverech na internetu s tím, že uživatelé k nim mohou přistupovat prakticky odkudkoli[80]), lze se domnívat, že GDPR pokrývá všechny možnosti nakládání s OÚ z hlediska místní působnosti. Resp. opačně – nepokrývá pouze zpracování OÚ, které se nacházejí mimo EU, subjekty se sídlem (či provozovnou) rovněž mimo EU.

Časová působnost navazuje na datum účinnosti a vynutitelnosti, tj. 25. 5. 2018.

Čl. 4 vymezuje taxonomii. Z rozsahového hlediska se nejrůznějším definicím, kromě pojmů „osobní údaje“ a „zpracování“, vymezených výše, v této práci blíže nevěnuji, nicméně při jejím psaní i při tvorbě *Standardů* byly plně zohledněny a doplněny o příklady z praxe.

[79] SMEJKAL, 2018, op. cit., s. 244–245.
[80] SMEJKAL, 2018, op. cit., s. 60.

4 Samoregulační standardy ČAP k uplatňování GDPR v pojišťovnictví v obecné rovině

4.1 Vývoj

Jelikož je zpracovávání OÚ za splnění podmínek ochrany subjektů OÚ klíčem k úspěšnému a efektivnímu výkonu pojišťovací činnosti, členské pojišťovny ČAP se rozhodly zdůraznit význam připisovaný ochraně soukromí a bezpečnosti OÚ přijetím dokumentu *soft law* povahy, který zde blíže představím.

PS GDPR ČAP byla založena s cílem připravit pojistný trh na implementaci GDPR a uchopit mezery a nedostatky, které existovaly mezi dosavadní praxí a novými podmínkami či ve výkladovém vakuu. V průběhu tvorby dokumentu PS reagovala na vyvíjející se národní i evropské interpretační požadavky. Inspirovala se také zahraničními předlohami, např. německou, francouzskou či irskou. Textace byly konzultovány s ÚOOÚ, který ocenil přístup pojistného sektoru. Tento komunikační kanál je udržován i během pravidelných revizí dokumentu.

První verze *Standardů* nabyla účinnosti dne 4. 4. 2019, a to schválením prezidiem ČAP. Pro pojišťovny se staly závaznými okamžikem přistoupení. Přistoupení ke *Standardům* je dobrovolné, formou oznámení o přistoupení, avšak nemá jenom deklaratorní povahu. Pojišťovna se zavazuje zajistit dodržování pravidel stanovených *Standardy* i do budoucna a je povinna provádět vyhodnocení souladu na roční bázi, které předkládá ČAP. Pojišťovny, jež ke *Standardům* přistoupily, o této skutečnosti vhodným způsobem informují své klienty.

Pokud by docházelo k opakovanému porušování *Standardů* zjištěnému ČAP na základě vlastní činnosti či podnětu, může být pojišťovna vyškrtnuta z evidence pojišťoven dodržujících *Standardy*, kterou ČAP vede na svých webových stránkách. ČAP není oprávněna k vydávání sankčních opatření *stricto sensu*, za zvážení ale samozřejmě stojí možné reputační riziko pojišťovny.

Co se týká řešení stížností subjektů OÚ na nedodržování *Standardů* ze strany pojišťovny, ČAP není oprávněna je vyřizovat. Obdrženou stížnost předá ČAP dané pojišťovně. ČAP tedy vůči pojišťovnám není v dozorovém, dohledovém ani kontrolním postavení.

V současnosti tak z tohoto dokumentu vychází 93 % pojistného trhu ČR[81], což je nepochybně solidní údaj, a dovolím si tvrdit, že dokládá kvalitní úroveň zpracování dokumentu nejen v obecné rovině, ale právě s důrazem na pojistná specifika. Tím vytváří vhodný podklad pro implementaci v jednotlivých pojišťovnách a zodpovězení případných interpretačních nebo i praktických otázek.

Standardy nadto představují obecně pojatou minimální míru ochrany subjektů OÚ, kdy není jednotlivým členům bráněno zvolit si v konkrétních případech vyšší míru ochrany na základě jejich specifických potřeb a postupů.

Pro účely této práce zároveň slouží jako ideální podklad pro názornou ilustraci specifik implementace GDPR v pojistném odvětví.

V průběhu činnosti PS bylo rozebíráno také vypracování kodexu chování dle čl. 40 a násl. GDPR. Ve světle vydávání výkladových pokynů WP29 i EDPB a v té době nedostatečně určitě vymezených kritérií a později spíše bariér pro tvorbu kodexu, kterým se věnuji níže, se členské pojišťovny domluvily na sepsání dokumentu samoregulační povahy. Podobný a přetrvávající přístup registruji v rámci svého působení v IE i na dalších trzích.

4.2 Struktura

Struktura *Standardů* je tvořena preambulí, vymezující výchozí zásady, hodnoty a cíle přijetí *Standardů*, seznamem definic a zkratek a dvěma hlavními kapitolami, jež stanovují požadavky na zpracování OÚ v pojišťovnictví a správu a monitorování ČAP. Mnou sepsaná preambule uvádí, že za účelem zpracování velkého množství OÚ pro řádný a korektní výkon pojistné činnosti byly přijaty *Standardy*, které přispívají k řádnému uplatňování GDPR a zároveň reflektují specifickou povahu pojišťovnictví a konkrétní potřeby členů ČAP při zpracování OÚ. Idea, která prostupuje též celou tuto práci, vychází z předpokladu, že pojišťovny při výkonu své činnosti musí nezbytně zpracovávat značné množství OÚ, které slouží ke správnému zhodnocení rizika a nastavení odpovídajícího pojistného a podmínek smlouvy klientům, stejně tak i plnění legislativních povinností. Dokument je doplněn třemi přílohami:

[81] Dobrovolně se zavázalo *Standardy* dodržovat 20 členských pojišťoven ČAP, které tvoří 93 % trhu. Dostupné z: https://www.cap.cz/odborna-verejnost/samoregulacni-standardy#:~:text=Dlouhodob%C3%BDm%20c%C3%ADlem%20%C4%8CAP%20je%20transformace,%2C%20kter%C3%A9%20tvo%C5%99%C3%AD%2093%20%25%20trhu.

a) *Oznámením členské pojišťovny ČAP o přistoupení*, zakotvujícím úmysl pojišťovny připojit se k dodržování *Standardů*;

b) *Šablonou pro ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 GDPR*;

c) každoročním *Oznámením členské pojišťovny o vyhodnocení souladu se* Standardy.

4.3 Obsah

Obsah *Standardů* je strukturován obdobně jako GDPR, tj. od hlavních principů až po práva, TOO a postupy při porušení zabezpečení OÚ.

Standardy se vztahují na zpracování OÚ klientů a pojišťovacích zprostředkovatelů, které pojišťovny zpracovávají při výkonu pojišťovací činnosti a souvisejících činností v ČR.

V souladu s požadavky ÚOOÚ a EDPB je text doplněn o příklady, které lépe znázorňují souvislosti, jež nemusí být vzhledem k časté složitosti prováděných pojistných procesů *prima facie* evidentní, a to jak ze strany subjektů OÚ, tak i pojišťoven a jejich zaměstnanců.

Záměrem je kromě proklamace ochrany OÚ i vymezení specifik pojišťovacího sektoru formou srozumitelnou i osobám bez právního vzdělání či zkušeností.

5 Samoregulační standardy ČAP k uplatňování GDPR v pojišťovnictví v konkrétní rovině

5.1 Základní principy

První kapitola *Standardů* je tvořena principy neboli zásady zpracování OÚ, které navazují na čl. 5 GDPR. Tato obecnější část slouží k vykreslení limitů, ve kterých se pojišťovny při zpracovávání OÚ pohybují. Aby byl srozumitelnější konkrétní dopad na výkon pojišťovací činnosti a následně vliv na subjekt OÚ, jsou principy dopodrobna rozebrány.

Jedná se nejen o principy zákonnosti, korektnosti, transparentnosti a odpovědnosti, ale také účelového omezení, kdy pojišťovna zpracovává OÚ pouze pro určité, explicitně vyjádřené a legitimní účely, přičemž OÚ nejsou dále zpracovávány způsobem, který je s těmito účely neslučitelný.

Kromě toho je nutno dodržovat zásadu minimalizace, kdy pojišťovna zpracovává přiměřené, relevantní a na nezbytný rozsah omezené OÚ ve vztahu k účelu, pro který jsou zpracovávány.

Dále pojišťovna zpracovává přesné a aktualizované OÚ.

O nic méně důležitý je časový princip omezení uložení, dle kterého pojišťovna nezpracovává OÚ, kterými je možné identifikovat subjekt OÚ, po dobu delší, než je nezbytné pro účely zpracování. Pojišťovna tak nezpracovává OÚ, pokud pomine účel (právní titul).

V neposlední řadě se členské pojišťovny zavázaly ke zpracování způsobem, který zajistí náležité zabezpečení a ochranu OÚ, což má přesah na TOO a KB ochranu.

5.1.1 Zákonnost

Zákonnost jako jedna ze základních zásad zpracování OÚ je představena v čl. 5 odst. 1 písm. a) GDPR a následně důkladněji čl. 6 GDPR, zakotvujícím možné právní základy pro zpracování OÚ, jejž doplňují body 10, 44, 45, 46, 50, 51 a s přesahem na spravedlnost a transparentnost i bod 60 preambule.

Pro dodržení maximální úrovně zákonnosti je nutné posuzovat kombinaci tří aspektů. Je potřeba určit účel, pro který dochází ke zpracování, nalézt či zajistit právní základ daného zpracování a vymezit okruh dotčených OÚ, který musí být přiměřený tomuto účelu a podložený právním základem. Vzhledem k dynamice operací je třeba tyto tři složky vnímat

jako spojené nádoby –rozšíření účelu zpracování tedy vyžaduje revizi adekvátnosti právního základu i přiměřenosti okruhu dotčených OÚ.[82]

Pro pojišťovací činnosti jsou relevantní zejména právní základy zpracování nezbytné pro plnění smlouvy, zákonné povinnosti správce, oprávněný zájem anebo zpracování na základě souhlasu subjektu OÚ. V případě citlivých údajů je vedle stanovení právního základu dle čl. 6 GDPR třeba naplnit i jednu z podmínek uvedených v čl. 9 GDPR, čemuž se podrobněji věnuji níže.

5.1.2 Korektnost a transparentnost

Pojišťovna v souladu s čl. 12 GDPR a pokyny EDPB[83] transparentně informuje subjekt OÚ, které OÚ o něm zpracovává, v jakém rozsahu a jakým způsobem a o právech, jejichž výkonu napomáhá. Subjekt OÚ by měl být také informován o provádění AR a o jeho důsledcích, viz kapitola 5.10 této práce. Všechny informace poskytuje pojišťovna stručně, snadno přístupným způsobem a srozumitelně, viz informační povinnost.

5.1.3 Odpovědnost

Princip odpovědnosti chápu ve dvou rovinách. Vztahuje se k doložitelnému dodržování ostatních principů a odpovědnosti za případnou újmu. Za tímto účelem pojišťovna zavede vhodná opatření, která pravidelně aktualizuje a u nichž je schopna demonstrovat jejich existenci a aplikaci.

Co se týče odpovědnosti, rozlišuje se mezi pojišťovnou v pozici správce dle čl. 4 odst. 7 a zpracovatele dle čl. 4 odst. 8 GDPR. V postavení správce je pojišťovna odpovědná za újmu, kterou způsobí zpracováním *contra legem*. V postavení zpracovatele je za újmu způsobenou zpracováním odpovědná pouze v případě, že nesplní povinnosti stanovené právními předpisy pro zpracovatele, nebo pokud jednala nad rámec či v rozporu se zákonnými pokyny správce. *Standardy* dále uvádějí, že pojišťovna může být odpovědnosti za újmu zproštěna, pokud prokáže, že žádným způsobem nenese odpovědnost za událost, která ke vzniku újmy vedla, a to dle čl. 82 odst. 3 a bodu 146 preambule GDPR.

[82] POLČÁK et al., 2018, op. cit., s. 437.
[83] Article 29 Data Protection Working Party. *Guidelines on Transparency under Regulation 2016/679* [online]. Brussels: Article 29 Data Protection Working Party, 11. 4. 2018 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

5.1.4 Přesnost a aktuálnost

Pro výkon pojišťovací činnosti je maximálně podstatné disponovat přesnými a aktuálními OÚ, což analyzuji níže. Objeví-li se při nebo po uzavření smlouvy konkrétní indikace o opaku, pojišťovna učiní nezbytný výmaz nebo opravu. K tomuto pojišťovna může vyžadovat součinnost subjektu OÚ, jelikož je to i v jeho zájmu. To je vykresleno na konkrétním příkladu, který uvádí, že neohlášení změny příjmení, např. z důvodu změny osobního stavu klienta, může mít vliv na rychlost a efektivnost pojistného plnění a řešení pojistné události, neboť pojišťovna bude nejprve muset provést identifikaci subjektu OÚ, a to např. dožádáním oddacího listu. Identifikace je však v souladu s čl. 11 a bodem 57 preambule GDPR umožněna pouze vyžaduje-li to daný účel zpracování.

5.2 Kategorie OÚ

Jelikož bylo během tvorby *Standardů* zakotveno, že dokument má sloužit k bližšímu pochopení zpracovávání OÚ v sektoru pojišťovnictví, byly některé typy OÚ upraveny samostatně. Hlavní příčinou je jejich specifičtější povaha, na kterou je vázán i odlišný režim zacházení. Vlastní podkapitola tak dle mého názoru správně náleží nejen citlivým údajům, ale také OÚ týkajícím se rozsudků v trestních věcech a trestných činech a vzhledem ke svému výjimečnému postavení i přístupu k RČ.

5.2.1 OÚ

Obecnou definici OÚ dle čl. 4 odst. 1 GDPR uvádím v kapitole 3.2.3 této práce. Při aplikaci na pojišťovnictví se v souladu s proporcionalitou jedná zejména o: identifikační a kontaktní údaje (např. jméno, příjmení, datum narození, RČ, adresu, telefon, e-mail, státní příslušnost); OÚ týkající se rozsudků v trestních věcech a trestných činech; údaje pro účely underwritingu (např. u ŽP povolání, vzdělání, sporty); údaje vztahující se k předmětu pojištění (např. velký technický průkaz vozidla); dále také údaje pro zjištění potřeb a požadavků klienta, jelikož na základě § 77 ZDPZ je pojišťovna povinna před sjednáním nebo podstatnou změnou pojištění získat od klienta informace týkající se jeho požadavků, cílů a potřeb; údaje pro test vhodnosti, protože na základě § 78 ZDPZ je pojišťovna povinna před sjednáním nebo podstatnou změnou rezervotvorného pojištění poskytnout klientovi radu týkající se vhodnosti; pak také např. finanční situace klienta, znalosti a zkušenosti v investicích; údaje z monitoringu (např. ze záznamů z jednání, telefonických hovorů, online služeb); údaje zpracovávané v souvislosti

s plněním pojistné smlouvy a využíváním služeb (např. o sjednání a využívání služeb či o nastavení smluv a parametrech pojištění, informace k řešení pojistné události čili likvidace).

5.2.2 Citlivé OÚ

Citlivé údaje, dle české terminologie „zvláštní kategorie OÚ dle dikce čl. 9 a bodu 51 preambule GDPR“, nesou vzhledem ke svému charakteru (ochrany obzvlášť hodnému) speciální míru pozornosti, jelikož by při jejich zpracování mohla vzniknout závažná rizika pro základní práva a svobody.

Jsou zde zahrnuty údaje o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, genetické, biometrické a zdravotní údaje či údaje o sexuálním životě nebo orientaci.

Do této kategorie náleží i gender, kterému se budu věnovat blíže, protože se v rámci GDPR jedná o výrazné specifikum pojišťovnictví. Z hlediska pojišťovnictví a přístupu k OÚ této povahy byl průlomovým rozsudek SDEU Test-Achats[84], navazující na žádosti o rozhodnutí o předběžné otázce podle čl. 234 Smlouvy o ES (dnes čl. 267 SFEU) k platnosti čl. 5 odst. 2 směrnice k rovnému zacházení s muži a ženami[85].

Ten zakotvil, že kalkulace pojistného a pojistného plnění podle pohlaví je diskriminující – v rozporu s čl. 21 a 23 LZPEU, a dotčený článek zrušil. Výjimka pro aplikaci skončila dne 21. 12. 2012. To se netýká účelů pojistně matematických, výpočtu technických rezerv v souladu s SII apod., což poté EK vysvětlila svými pokyny[86]. Zde bylo také objasněno, že ohledně prevence genderové diskriminace by se tato směrnice měla vztahovat na přímou i nepřímou diskriminaci. K přímé diskriminaci dochází pouze tehdy, pokud se s osobou z důvodu pohlaví zachází ve srovnatelné situaci méně příznivým způsobem.

Dle ČSpA pravidlo stejného přístupu k oběma pohlavím znamená, že pojistné a pojistné plnění se nesmí lišit u dvou různých osob se stejnou pojistnou smlouvou pouze z genderových

---

[84] SDEU. *Rozsudek Soudního dvora (velkého senátu) ze dne 1. března 2011. Association belge des Consommateurs Test-Achats ASBL, Yann van Vugt, Charles Basselier proti Conseil des ministres*, C236/09 [online]. V Bruselu: 1. 3. 2011 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:62009CJ0236&from=EN.

[85] Směrnice Rady 2004/113/ES ze dne 13. 12. 2004, kterou se zavádí zásada rovného zacházení s muži a ženami v přístupu ke zboží a službám a jejich poskytování. In: *Úřední věstník* [online], L 373, 21. 12. 2004, s. 37–43 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX:32004L0113.

[86] European Commission. Guidelines on the application of Council Directive 2004/113/EC to insurance, in the light of the judgment of the Court of Justice of the European Union in Case C-236/09 (Test-Achats) (Text with EEA relevance). *Official Journal of the European Union* [online]. 13 January 2012, 11(1) [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012XC0113(01)&from=EN.

důvodů. Existují však jiné rizikové faktory, např. zdravotní stav či rodinná anamnéza, na jejichž základě je rozlišení možné a při jejichž posuzování musí pojistitelé s ohledem na určité fyziologické rozdíly mezi muži a ženami vzít pohlavní identitu v úvahu[87]. To uvádí také § 59 odst. 2 ZPOJ v souladu se zákonem č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací, a je to podmíněno efektivním underwritingem, což není v rozporu s principem rovnosti dle např. čl. 1 VDLP. Rozdílům mezi diskriminací a diferenciací se věnuji v této práci i níže – u AR a UI.

Zpracování citlivých OÚ je dle čl. 9 GDPR v obecné rovině zakázáno, avšak je možno aplikovat některou z výjimek z odst. 2. Pro pojistný sektor je relevantní zejména výjimka založená primárně na souhlasu dle písm. a), hlouběji analyzovaná níže, a na určení, výkonu nebo obhajobě právních nároků nebo v rámci soudních pravomocí dle písm. f). Výčet právních základů je zde však užší a chybí např. plnění smlouvy.

Bod 10 preambule GDPR umožňuje diskreci ČS nad rámec minimální roviny vymezené GDPR, což upřesňuje čl. 9 odst. 4, dopadající na zpracování genetických, biometrických a zdravotních údajů.

5.2.2.1 Genetické údaje

Podle definice čl. 4 odst. 13 GDPR se jedná o OÚ týkající se zděděných nebo získaných genetických znaků FO, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy jejího biologického vzorku.

Využívání tohoto typu údajů je častým předmětem diskuzí nejen mezi zástupci pojistného sektoru. Důvodem je jejich značný potenciál pro budoucí zdravotní vývoj klienta, ale také nebezpečí adverzní selekce, což by bylo v přímém rozporu se zákazem diskriminace vymezené např. čl. 21 LZPEU a čl. 11 úmluvy Rady Evropy[88]. Komplikovanost vymezení jednoznačného přístupu lze dovodit i z nízkého počtu zemí, které ratifikovaly dodatkový

[87] ČSpA. *Odborné doporučení ČSpA č. 2* [online]. Praha: ČSpA, 1. 11. 2012 [cit. 16. 2. 2022]. Dostupné z: https://www.actuaria.cz/doporuceni-2.html.
[88] Úmluva na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie a medicíny. Úmluva o lidských právech a biomedicíně. In: *Série evropských úmluv* [online]. Č. 164 [cit. 22. 2. 2022]. Dostupné také z: https://www.lf3.cuni.cz/3LF-426-version1-umluva_o_lidskych_pravech_a_biomedicine.pdf.

protokol o genetickém testování pro zdravotní účely sjednaný k *Úmluvě na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie a medicíny*[89].

Co se týká pojišťovnictví, v ČR není použití genové analýzy pojišťovnami využíváno. Přímý zákaz je zakotven např. v Rakousku, Belgii a Irsku.

5.2.2.2 Biometrické údaje

Dle čl. 4 odst. 14 GDPR jde o OÚ vyplývající z konkrétního technického zpracování a týkající se fyzických či fyziologických znaků nebo znaků chování FO, které umožňují nebo potvrzují jedinečnou identifikaci, např. zobrazení obličeje nebo daktyloskopie.

Zpracování fotografií by dle bodu 51 preambule GDPR nemělo být systematicky považováno za zpracování zvláštních kategorií OÚ, neboť na fotografie se definice biometrických údajů vztahuje pouze v případech, kdy jsou zpracovávány zvláštními technickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci FO.

Ve finančních službách je toto téma v současnosti velice aktuální. I v rámci pojišťovnictví dochází k posuzování vhodnosti zakomponování prvku biometriky, především 3D biometrického podpisu. Z tohoto důvodu jsem z pověření ČAP realizovala celoevropské mapovací cvičení, ze kterého vyplynulo, že i kolegové ze zahraničí se potýkají s nedostatkem interpretačních vodítek. Ve světle těchto zjištění a výkladu ÚOOÚ[90] bylo od aktivního rozvoje v této oblasti prozatím upuštěno.

Dalšími, v ČR zatím neaplikovanými instituty jsou kontroverzní techniky rozpoznávání hlasů či obličejů, jež nepochybně přinesou mnohé výzvy nejen v rámci GDPR, ale i etických mantinelů, *per analogiam* v kapitole 7.2 této práce.

5.2.2.3 Údaje o zdravotním stavu

Dle čl. 4 odst. 15 GDPR se jedná o údaje týkající se tělesného nebo duševního zdraví, včetně údajů o poskytnutí zdravotních služeb, vypovídajících o zdravotním stavu FO. Pod tento pojem lze v pojišťovnictví zařadit i údaje poskytnuté přímo subjektem prostřednictvím

[89] Dodatkový protokol k úmluvě o lidských právech a biomedicíně, o genetickém testování pro zdravotní účely. In: *Sbírka mezinárodních smluv* [online]. Č. 41/2019, částka 27, s. 7597–7606 [cit. 22. 2. 2022]. Dostupné také z: https://www.mzcr.cz/ratifikace-dodatkoveho-protokolu-o-genetickem-testovani-pro-zdravotni-ucely/.
[90] ÚOOÚ. *Kontrola využití biometriky u klientů (UOOU-09654/18)* [online]. [cit. 22. 2. 2022]. Dostupné z: https://www.uoou.cz/kontrola-vyuziti-biometriky-u-klientu-uoou-09654-18/ds-6546.

dotazníku, údaje z karty pacienta, od zdravotních pojišťoven nebo ze zdravotní dokumentace a informace o nemoci, anamnéze či postižení.

Zpracovávání této kategorie citlivých OÚ je nezbytné pro výkon pojišťovnictví, např. ŽP, zdravotního pojištění, dlouhodobé péče nebo invalidního pojištění. Na jejich základě dochází kromě posouzení pojistného rizika k vypracování návrhu a uzavření nebo ukončení pojistné smlouvy, popř. likvidaci. Absence relevantních podkladů by vedla k nemožnosti posoudit žádost zájemce o pojištění a v širší rovině pak ke změnám pojistného a limitů pojistného krytí, s komplexnějším negativním přesahem. O těchto konsekvencích pojednávám u souhlasů níže a v kapitole 7.2 této práce. GDPR umožněná diskrece přirozeně vede k nejednotným přístupům v EU. To může dle mého názoru zkomplikovat i aktuální iniciativu EK ve věci vytvoření Evropského prostoru pro zdravotní údaje. Systém by vytvořil právní rámec, který by se vztahoval na přístup k údajům o zdravotním stavu a jejich výměně, např. pro účely poskytování zdravotní péče a služeb. Je třeba vzít v úvahu nutnost zachovat rovnost podmínek, kontrolu subjektů OÚ a portabilitu, a to i v souladu s čl. 20, bodem 68 preambule GDPR.

5.2.3 OÚ týkající se rozsudků v trestních věcech a trestných činů

Pojišťovna zpracovává tyto OÚ v souladu s čl. 10 GDPR, který uvádí, že zpracování OÚ tohoto typu na základě čl. 6 odst. 1 se může provádět pouze pod dozorem orgánu veřejné moci nebo pokud je oprávněné podle práva EU nebo ČS.

V kontextu pojistného odvětví je rámec aplikován, je-li to nezbytné pro: ochranu bezpečnosti a integrity, včetně prevence, odhalování a vyšetřování trestných činů; ověřování důvěryhodnosti distributorů pojištění podle ZDPZ; evidenci pro účely AML/CFT a plnění dalších zákonných povinností. Tím není dotčena povinnost pojišťovny dle § 129 b ZPOJ, který upravuje sdílení informací mezi pojišťovnami v oblasti PPP.

5.2.4 RČ

RČ patří dle GDPR do kategorie zvláštních situací, při nichž dochází ke zpracování, a vztahuje se na ně jakožto národní identifikační čísla čl. 87 GDPR. Nepatří však do kategorie citlivých OÚ[91].

[91] NULÍČEK et al., 2017, op. cit., s. 500.

Využívání tohoto druhu jedinečného a jednoznačného identifikátoru je v ČR časově omezeno a bude nahrazeno principem tzv. „dělené identity“ dle sektorů. Dle mých informací se v pojišťovnictví bude jednat o identifikátor z Agendového IS České kanceláře pojistitelů, což ale nenahrazuje fyzickou identifikaci. To dle mého názoru přinese z hlediska GDPR výhody. Z RČ lze totiž vyčíst další OÚ, jako gender nebo datum narození.

V současnosti je však jejich zpracování třeba, a to nejen k provozování pojišťovací činnosti, což se považuje za zpracování nezbytné pro dodržení právní povinnosti správce dle § 6 odst. 6 ZPOJ. Samozřejmě v souladu se zásadou minimalizace zpracovává pojišťovna RČ pouze v rozsahu nezbytně nutném pro výkon činnosti.

5.3 Účely zpracování

Pojišťovna zpracovává OÚ pro konkrétní, jednoznačné a legitimní účely vyplývající z její činnosti v souladu s právními předpisy, které stanoví již v okamžiku jejich shromažďování nebo nakládání s nimi. Každý účel potřebuje právní základ zpracování.

V souladu s principem účelového omezení nelze OÚ bez dalšího užívat k jinému účelu. Proto pokud pojišťovna zjistí, že je potřebuje zpracovávat pro jiné účely, může tak učinit, pouze pokud je to právně umožněno, na základě souhlasu subjektu OÚ, anebo je-li zpracování pro jiný účel slučitelné s původními účely, dle čl. 6 odst. 4 GDPR. V takovém případě pojišťovna vždy mj. zohlední vazbu mezi účely, povahu OÚ, okolnosti shromáždění, možné důsledky dalšího zpracování apod. To je relevantní především z pohledu nepřímého marketingu. Např. e-mail anebo telefon klienta poskytnuté při uzavření smlouvy pro účely jejího plnění nesmí být bez dalšího užity k marketingovým účelům, u kterých je vyžadován jako právní základ souhlas. Nejedná se tedy o přímý marketing, kde je právním základem oprávněný zájem.

V souladu se zásadou minimalizace pojišťovna zpracovává OÚ v rozsahu přiměřeném, relevantním a omezeném na to, co je nezbytné z hlediska účelů. To je ve *Standardech* vysvětleno na příkladu, dle kterého není důvodné od klienta vyžadovat předložení výpisu z trestního rejstříku pro účely sjednání smlouvy o havarijním pojištění.

Je taktéž důležité, že před dalším zpracováním pojišťovna poskytne subjektu OÚ informace o jiném účelu a jeho právech. Pro bližší představu účelů uvádí *Standardy* demonstrativní výčet, jenž mezi nejčastěji aplikované účely řadí např. jednání o smluvním vztahu, zjišťování

potřeb a požadavků klienta a dalších údajů potřebných pro test vhodnosti, underwriting, likvidaci, PPP apod.

5.4 Právní základy zpracování

Zpracování je zákonné, pokud je prováděno v odpovídajícím rozsahu za splnění nejméně jedné z podmínek – právních základů dle taxativního výčtu čl. 6 odst. 1 GDPR. Pro účely v pojišťovnictví uvedené výše se zejména uplatní níže zkoumané právní základy.

Právní základy ochrany životně důležitých zájmů subjektu OÚ nebo jiné FO dle písm. d) a splnění úkolu prováděných ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce dle písm. e), nejsou v pojišťovnictví využívány. Nebudu se jim zde tedy věnovat.

5.4.1 Smlouva

Plnění smlouvy, jejíž stranou je subjekt OÚ, nebo provedení opatření přijatých před uzavřením smlouvy na žádost subjektu OÚ v souladu s čl. 6 odst. 1 písm. b) GDPR, popř. pokynů EDPB 2/2019[92], lze označit za primární účel aplikovaný v kontextu pojišťovnictví. I proto je jeho zařazení do revidované ePrivacy tak relevantní.

Pojišťovna zpracovává OÚ již od doby jednání o uzavření pojistné smlouvy a v případě uzavření smlouvy po dobu trvání pojištění. Konkrétně dochází ke zpracování identifikačních a kontaktních údajů klienta, OÚ vztahujících se k předmětu pojištění (např. velký technický průkaz vozidla), ale i citlivých OÚ a údajů pro underwriting či likvidaci.

5.4.2 Právní povinnost

Plnění právní povinnosti správce je upraveno čl. 6 odst. 1 písm. c) GDPR. Pojišťovna při provozování pojišťovací činnosti musí zpracovávat OÚ pro plnění povinností dle právních předpisů, v souladu s čl. 6 odst. 3 GDPR. Jak je patrné z názorného výčtu v kapitole 2 této práce, optikou pojišťovnictví se skutečně nejedná o zanedbatelnou kategorii.

[92] EDPB. *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* [online]. Version 2.0. Brussels: 8. 10. 2019 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.

5.4.3 Oprávněný zájem

Oprávněný zájem správce či třetí strany, kromě případů, kdy mají přednost zájmy nebo základní práva a svobody subjektu OÚ, zejména dítěte, je aplikován v souladu s čl. 6 odst. 1 písm. f) a bodem 47 preambule GDPR.

V případě, že ke zpracování nedochází na základech uvedených výše a nejsou splněny podmínky udělení souhlasu, lze použít právní základ oprávněného zájmu, který musí být podložený a proporcionální. To *Standardy* vykreslují na faktických příkladech, jako je např. zpracování OÚ nesmluvních stran (zejména pojištěných osob v rámci individuálního i skupinového pojištění, osob obmyšlených, oprávněných, poškozených), přímý marketing, ochrana práv a právem chráněných zájmů pojišťovny, PPP a jiná protiprávní jednání, např. kybernetická rizika, jak bylo aplikováno v souladu s názorem EDPS vysvětleným v kapitole 2.2.3.3 této práce.

5.4.4 Souhlas

Nejvíce diskutovaný je právní základ opírající se o souhlas dle čl. 6 odst. 1 písm. a), 7, 9 odst. 2 písm. a) a bodů 32, 33, 42, 43 preambule GDPR, které v této práci proto podrobím důkladnějšímu zkoumání.

Diskreci související se souhlasem umožňuje čl. 8, na co navazují čl. 12 odst. 1 a body 38, 58, 65 preambule GDPR ve věci věkové hranice nezletilého pro jeho udělení, což vede k fragmentaci úprav mezi ČS.

Dle definice obsažené v čl. 4 odst. 11 GDPR je souhlasem subjektu OÚ jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt OÚ dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování OÚ. Význam souhlasu v oblasti ochrany OÚ potvrzuje i čl. 8 LZPEU.

Tato problematika je také předmětem výše uvedených pokynů EDPB, kde je souhlas hodnocen jako poslední možná, a určitě ne doporučovaná varianta. Proto je tento právní základ pojišťovnou aplikován pouze za situace, že nelze využít jiného právního základu. Zde opět připomínám analogii k revizi ePrivacy.

I když jsou požadavky vymezené na evropské úrovni k souhlasům určující, ráda bych vymezila národní specifika ve vztahu ke genetickým, biometrickým a zdravotním údajům, dle

čl. 9 odst. 4 GDPR, jelikož v rámci pojišťovnictví je nutno zohlednit veřejnoprávní i soukromoprávní přístup.

U GDPR jakožto veřejnoprávní úpravy je v rámci pojišťovnictví aplikován implicitní souhlas ke zpracování OÚ o zdravotním stavu u vstupu do pojištění z důvodu ocenění pojistného rizika. Následně, po uzavření pojistné smlouvy dochází k překlopení na alternativní právní titul nezbytnosti pro určení, výkon nebo obhajobu právních nároků v souladu s čl. 9 odst. 2 písm. f) GDPR. To umožňuje kontinuitu smlouvy i pro případné odvolání souhlasu. Tohoto specifického dopadu na provozování pojišťovací činnosti si byl vědom i zákonodárce, a proto bez souhlasové řešení zakomponoval do důvodové zprávy k adaptačnímu zákonu[93].

Souběžná je úprava soukromoprávní, OZ, která ale nespadá pod diskreci dle GDPR a má tradičnější povahu. Vedle GDPR tak platí i § 2828 a 2864 OZ. Odmítne-li pojištěný/poškozený v době trvání pojistné smlouvy sdělit další zdravotní OÚ relevantní např. pro šetření pojistné události a určení výše plnění (dle souhlasu OZ), dochází ke kontraproduktivní situaci, kdy objektivně nemůže dojít k plnění ze smlouvy. To je zapříčiněno neudělením souhlasu dle OZ ze strany pojištěného/poškozeného, což je v rozporu s jeho zájmem[94].

Zároveň toto výkladové řešení přináší ulehčení pro staré smlouvy (založené na souhlasech dle předchozího zákona č. 37/2004 Sb., o pojistné smlouvě, nebo OZ za účinnosti předešlého zákona č. 101/2000 Sb., o ochraně OÚ), kde není nutné získávat nový souhlas, pokud nedošlo k její změně a souhlas byl udělen dle podmínek GDPR, což praví i bod 171 preambule GDPR. To samozřejmě neplatí u všech typů zpracování OÚ, např. u předávání údajů ve skupině k jiným než administrativním účelům, AR či nepřímého marketingu, kde se vyžaduje souhlas.

U nepřímého marketingu bylo oříškem vymezení minimálních požadavků pro oslovování potenciálních klientů, jelikož se praxe napříč trhem liší a bylo potřeba vymezit hranici, kdy se již jedná o předsmluvní jednání, na které je aplikován právní základ smlouvy. Nakonec bylo domluveno, že realizuje-li pojišťovna prostřednictvím elektronické pošty oslovování subjektů OÚ, které nejsou klienty, činí tak na základě předchozího souhlasu uděleného přímo pojišťovně (např. online formulář) nebo získaného prostřednictvím doporučující osoby (např. souhlas na formuláři, který doporučující předá pojišťovně). Nicméně ve chvíli, kdy

[93] Parlament ČR. *Sněmovní tisk 138/0. Vládní návrh zákona o zpracování osobních údajů* [online]. 28. 3. 2018, s. 34–57 [cit. 20. 2. 2022]. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?o=8&ct=138&ct1=0.
[94] PETROV, Jan et al. *Občanský zákoník: komentář*. První vydání. Praha: C. H. Beck, 2017, s. 2792. Beckova edice Komentované zákony. ISBN 978-80-7400-653-1.

potenciální klient požádá o zpracování nabídky, se již jedná o právní základ zpracování nezbytný k uzavření smlouvy realizované na žádost subjektu OÚ. V tu chvíli se stává klientem a souhlas pro další marketingové nabídky není vyžadován.

Pokud tedy pro zpracování OÚ neexistuje jiný právní základ, lze vyžadovat souhlas. To má přesah zejména v případě citlivých údajů, dle čl. 9 odst. 2 písm. a) GDPR. Pojišťovna v takovém případě vždy zváží, zda existuje přímá spojitost mezi určitými OÚ a potřebou jejich zpracování pro uzavření nebo plnění smlouvy, a tedy samotné poskytnutí služby. V takovém případě informuje subjekt OÚ o smluvním požadavku OÚ poskytnout a o možných důsledcích, nebude--li tak učiněno – jak vysvětluji výše. Souhlas je tedy svobodný, avšak bez něj nelze sjednat pojištění – uzavřít smlouvu, u níž pojišťovna potřebuje znát např. údaje o zdravotním stavu (u ŽP). Vyžadování takového souhlasu není v rozporu s čl. 7 odst. 4 GDPR a bodem 43 preambule, kdy při posuzování svobodnosti souhlasu musí být zohledněna skutečnost, zda je mj. plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem, který není pro plnění dané smlouvy nutné. Z uvedeného lze *a contrario* výkladem dovodit, že s ohledem na skutečnost, že bez zpracování OÚ nelze žádanou službu v podobě pojištění poskytnout, jsou tyto OÚ relevantní, jinou výjimku dle čl. 9 odst. 2 GDPR nelze pro řadu účelů aplikovat a udělení souhlasu subjektem OÚ je nezbytné a nutné pro plnění smlouvy.

Jelikož problematika právních základů je nejen v českém právním prostředí mírně zamotaná, jsou *Standardy* doplněny o konkrétní ukázky vysvětlující jejich rozdílnou aplikaci. Např. správu pojistné smlouvy ani zpracování zdravotních údajů poškozených osob, které uplatnily svůj nárok na náhradu újmy na zdraví z pojištění odpovědnosti, nelze podmínit udělením souhlasu, neboť se použije právní základ plnění smlouvy. Uvedené se netýká tzv. „necitlivých“ OÚ, jelikož pro ty je možné využít právní základ nezbytnosti pro plnění smlouvy.

Za zmínku stojí, že aplikace vhodných právních základů není napříč EU vykládána totožně. Dle mých zjištění z IE se o souhlas plně, bez prostoru pro aplikaci jiného právního základu, opírá např. belgická, rakouská, kyperská, portugalská a norská úprava. Stejný přístup jako v ČR byl zvolen v Dánsku, Maďarsku i Řecku. Německo zvolilo úpravu, která se opírá primárně o souhlas. U zpracování citlivých údajů třetích stran v případech jejich odpovědnosti je možno aplikovat čl. 9 odst. 2 písm. f) GDPR. V potaz připadala i aplikace čl. 9 odst. 2 písm. h), tj. nezbytnost pro zdravotní účely. To však není využitelné ze strany soukromého

pojistného sektoru. Francie kromě souhlasu umožňuje využití čl. 9 odst. 2 písm. b) z důvodu zajištění sociální ochrany, což dopadá především na doplňkové zdravotní pojištění nebo pokrytí úmrtí. Naopak souhlas není pro výkon pojišťovací činnosti v oblastech cestovního pojištění, ŽP, zdravotního pojištění a pojištění odpovědnosti vyžadován v Bulharsku.

Pro futuro je pak potřeba myslet na rychlý vývoj v oblasti sdílení dat, medicíny, implantátů, robotiky a biotechnologií či na výzvy, které tyto dosud nepoznané instrumenty přinesou do praxe i do výkladu nejen v pojišťovnictví.

5.4.4.1 Svobodný

Souhlas se poskytuje ke konkrétnímu, jednoznačnému a legitimnímu účelu. Pojišťovna tedy nemůže podmiňovat poskytnutí služeb souhlasem se zpracováním OÚ, které nejsou nezbytné, jak je vysvětleno výše v souladu s pokyny EDPB. Ty uvádějí, že souhlas není svobodný, pokud subjekt OÚ nemá možnost volby, je donucen okolnostmi nebo vystaven negativním důsledkům neudělení.

V kontextu pojišťovnictví je tak relevantní především pokyny EDPB vymezená nevhodnost vázání souhlasu na plnění v rámci smlouvy či nevhodnost duplicitních právních základů – dochází-li tedy ke zpracování na základě smlouvy, je vyžadování souhlasu nadbytečné.

5.4.4.2 Jednoznačný

Udělený písemný souhlas je jednoznačným projevem vůle, pokud je text souhlasu oddělitelný od ostatních smluvních ujednání, zejména vizuálně. Toto vymezení bylo důležité pro prevenci nežádoucí praxe spojování, či dokonce podmiňování souhlasu s uzavřením samotné smlouvy a dalších praktik, jako absence nesouhlasu v první vrstvě, méně rozeznatelného linku místo tlačítka nesouhlasu, barevného zvýraznění souhlasu či opt-out souhlasů, tj. předem zaškrtnutých políček, která opačně, než je vyžadováno, musel subjekt OÚ aktivně vyškrtnout.

To ostatně odsoudila WP29 již v roce 2007[95] i SDEU[96] v kontextu autorizace cookies a informační povinnosti. To se odrazilo i v českém právním prostředí, a to v zákonu

[95] Article 29 Data Protection Working Party. *Working Document on the processing of personal data relating to health in electronic health records (EHR)* [online]. Brussels: Article 29 Data Protection Working Party, 15. 2. 2007 [cit. 20. 2. 2022]. Dostupné z*:* https://www.dataprotection.ro/servlet/ViewDocument?id=228.
[96] SDEU. *Rozsudek Soudního dvora (velkého senátu) ze dne 1. října 2019. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. vs. Planet49 GmbH*, C-673/17 [online]. 1. 10. 2019 [cit. 20. 2. 2022]. Dostupné z: http://curia.europa.eu/juris/liste.jsf?num=C-673/17.

č. 127/2005 Sb., o elektronických komunikacích. Od začátku roku 2022 platí pro použití cookies povinnost opt-in souhlasu.

O jednoznačný souhlas se tedy jedná u podpisu listiny, zaškrtnutí příslušného pole, písemného, ale i ústního prohlášení (např. svědecká výpověď nebo záznam telefonického hovoru), popř. u jiného dostatečně zjevného a prokazatelného způsobu.

5.4.4.3 Granulární, určitý, konkrétní a informovaný

Konkrétnost souhlasu souvisí s jeho transparentností a požadavkem informovanosti subjektu OÚ.[97] Jeden souhlas může být udělen pro zpracování více kategorií OÚ a může zahrnovat více skutečných kroků zpracování, pokud tyto operace sledují stejný účel. Pokud pojišťovna hodlá využít OÚ pro jiný účel s potřebným souhlasem, musí ho obdržet předem.

V každém případě tedy platí zásada oddělenosti souhlasů dle konkrétních účelů v souladu s požadavky čl. 7 a bodů 32, 33, 42, 43 preambule GDPR. Na základě těchto principů není podporováno využití komplexních souhlasů (tzv. „na jeden klik“). Je aplikován aktivní opt-in, samostatná volba pro každý z účelů, např. ke zpracování OÚ pro zařazení do soutěží a předávání údajů třetí osobě.

Subjekt OÚ je informován o tom, k jakým účelům zpracování poskytuje souhlas, a o svých právech, viz kapitola 5.8 této práce.

5.4.4.4 Odvolatelný

V souladu s bodem 42 preambule GDPR má subjekt OÚ právo souhlas kdykoli odmítnout nebo odvolat, a to stejným způsobem, jakým jej poskytl. To je důležité pro prevenci nežádoucích postupů, kdy byl např. souhlas udělen elektronicky, ale pro odvolání je nutné osobně se dostavit na pobočku a podepsat listinný dokument.

V případě odvolání souhlasu by pojišťovna měla být bez ohledu na formu udělení schopna prokázat, zda a kdy byl souhlas odvolán.

Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu před jeho odvoláním. Odvolání souhlasu neznamená vždy povinnost pojišťovny OÚ zlikvidovat, neboť pojišťovně může příslušet jiný právní základ, pro který může pojišťovna nadále držet či

[97] POLČÁK et al., 2018, op. cit., s. 438.

aktivně zpracovávat OÚ pro jiný účel, např. ochrana práv a právem chráněných zájmů pojišťovny nebo plnění právních povinností.

Odvolání souhlasu, stejně jako jeho neposkytnutí, v první řadě nesmí jít k tíži subjektu OÚ ani mít příliš zatěžující důsledky. To ostatně pokyny EDPB zdůrazňují a *Standardy* doplňují příklady. Pokud klient odvolá souhlas se zpracováním OÚ pro marketingové účely, nemůže to vést k ukončení celé pojistné smlouvy ani k odmítání pojišťovny nadále poskytovat plnění. Nebo subjekt OÚ udělí výslovný souhlas se zpracováním OÚ o zdravotním stavu pro účely uzavření pojistné smlouvy ŽP. Tento souhlas ještě před uzavřením smlouvy odvolá. Pojišťovna není z důvodů vysvětlených výše nucena uzavřít s klientem smlouvu ŽP a toto neuzavření není považováno za jinak zakázaný škodlivý důsledek odvolání souhlasu.

5.5 Předávání OÚ ve skupině podniků

Z praktického pohledu se během formulace *Standardů* ukázala být velice významnou právě oblast předávání OÚ v rámci skupiny podniků definovaného čl. 4 odst. 19 a body 37, 48 preambule GDPR.

Pojišťovna nemusí pro předávání OÚ ve skupině podniků vyžadovat zvlášť souhlas pro každou společnost, která byla uvedena jako příjemce, pokud jim OÚ předává za stejným účelem zpracování. Např. subjekt OÚ projevil zájem o uzavření pojistné smlouvy telefonicky a při sjednání smlouvy projevil souhlas se zpracováním OÚ za účelem nabízení služeb třetích osob. Tento ústní souhlas má pojišťovna zdokumentovaný. Klient ale nemusí znovu udělovat souhlas s předáváním OÚ ve skupině pokaždé, kdy dojde ke změně členů skupiny, pokud zároveň nedochází ke změně účelů nebo charakteru zpracování OÚ a klient je o možnosti takové změny informován. Opačný postup by byl prakticky velice obtížně realizovatelný. Navíc pro zajištění plné informovanosti klienta pojišťovna pravidelně aktualizuje seznam členů skupiny podniků (např. na webových stránkách).

Souhlas není vyžadován ani pro předání OÚ v rámci skupiny podniků z důvodu interních administrativních účelů skupiny, kde dochází ke zpracování OÚ na základě oprávněného zájmu.

Pro případné předávání OÚ v rámci skupiny podniků mimo EHP platí pravidla pro předávání OÚ do třetích zemí.

5.6 Předávání OÚ do třetích zemí

5.6.1 Aktuální stav

Navzdory tomu, že předávání OÚ do třetích zemí není v kontextu české pojišťovací praxe dennodenním chlebem, je tato problematika ve *Standardech* obsažena, a to v návaznosti na čl. 44 a násl. GDPR a její sílící relevanci, např. u outsourcování ICT služeb, jak bylo popsáno u DORA.

Pojišťovna předává OÚ do třetích zemí v minimálním rozsahu nebo pseudonymizované podobě. V ojedinělých případech může docházet k předání většího množství OÚ, např. v případě potřeby sjednat nadlimitní zajištění a u ICT služeb, kdy pojišťovna využívá např. datové centrum či cloudové služby. Dle režimu předávání OÚ do třetích zemí je to umožněno, pouze pokud pojišťovna disponuje právním základem:

a) rozhodnutím EK o odpovídající ochraně v zemích hodnocených jako bezpečné dle čl. 45 a bodů 103–108, 169 preambule GDPR a referenčním rámcem pro odpovídající ochranu WP29[98], kdy není vyžadováno žádné zvláštní povolení ÚOOÚ. Vzhledem k brexitu je i Velká Británie třetí zemí, kdy je od roku 2021 účinná *Dohoda*[99], a EK rozhodla o odpovídající úrovni ochrany[100], což bude v budoucnu předmětem přezkumu;

b) vhodnými zárukami správce a zpracovatele dle čl. 46 a bodů 108–110, 114 preambule GDPR a *sub conditione*, že jsou k dispozici vymahatelná práva a účinná právní ochrana subjektu OÚ, kdy lze OÚ předat bez povolení ÚOOÚ. Jedná se zejména o:

- závazná podniková pravidla dle požadavků čl. 47 GDPR, v souladu s mechanismem jednotnosti dle čl. 63 a bodu 135 GDPR, schválená příslušným DPA, která ale platí pouze pro přenos OÚ v rámci jedné nadnárodní skupiny podniků;

[98] EDPB. *Doporučení 01/2021 o referenčním rámci pro odpovídající ochranu podle směrnice o prosazování práva* [online]. Brussels: EDPB, 2. 2. 2021 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_cs.
[99] Dohoda o obchodu a spolupráci mezi EU a Spojeným královstvím. In: *Úřední věstník* [online], L 149/10, 30. 4. 2021 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/info/strategy/relations-non-eu-countries/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_cs.
[100] European Commission. *Commission implementing decision of 28. 6. 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (Text with EEA relevance)* [online]. Brussels: 28. 6. 2021 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

- SCCs, tj. uzavření smlouvy o zpracování OÚ, prostřednictvím které se zpracovatel ve třetí zemi zaváže dodržovat úroveň ochrany OÚ v EU. SCCs, vzorové texty, může stanovit EK přezkumným postupem podle čl. 93 odst. 2 GDPR nebo je může přijmout DPA v souladu s mechanismem jednotnosti;

- schválený kodex chování dle čl. 40 GDPR;

- schválený mechanismus pro vydávání osvědčení od DPA nebo vnitrostátního akreditačního orgánu nejvýše na tři roky, které může být obnovováno;

c) ke specifické situaci, kdy není možné uplatnit a) ani b) výše, může dojít při splnění podmínek čl. 49 odst. 1 GDPR a bodů 111–116 preambule GDPR a taktéž pokynů EDPB 2/2018[101]. Zde je nutné požádat o souhlas DPA, jestliže správce hodlá předání realizovat na základě nestandardních nástrojů pro vytvoření vhodných záruk podle čl. 46 odst. 3 písm. a) a b) GDPR (tzn. nestandardní smluvní doložky, správních ujednání mezi orgány veřejné moci nebo veřejnými subjekty, která zahrnují vymahatelná a účinná práva subjektů OÚ) nebo hodlá informovat DPA dle čl. 49 odst. 1 GDPR v případě jednorázového předání OÚ omezeného počtu subjektů OÚ do třetích zemí, pokud je to nezbytné pro účely závažných oprávněných zájmů správce, jež nepřeváží nad zájmy, právy ani svobodami subjektů OÚ, a pokud nelze uplatnit žádnou z výjimek podle čl. 49 odst. 1 písm. a–g) GDPR, nebo hodlá požádat o schválení závazných podnikových pravidel příslušný DPA dle čl. 47. To se ale děje výjimečně.

Pro úplnost doplňuji, že dle čl. 48 GDPR rozhodnutí soudního a správního orgánu třetí země, jež po správci nebo zpracovateli požadují předání nebo zpřístupnění OÚ, lze uznat nebo vymáhat, pouze pokud vycházejí z mezinárodní dohody, která je v platnosti mezi žádající třetí zemí a EU nebo ČS.

5.6.2 Schrems II

Do roku 2020 byl vztah mezi EU a USA upraven programem Privacy Shield, na základě prováděcího rozhodnutí EK 2016/1250. Ten byl následkem zrušení systému Safe Harbour ze

[101] EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679* [online]. Brussels: EDPB, 25. 5. 2018 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_en.

strany SDEU (Schrems I)[102], který argumentoval nedostatečnou úrovní ochrany předávaných OÚ. Na to společnosti reagovaly textací SCCs a následně registrací v rámci Privacy Shield.

Max Schrems v rozhovoru pro Index Privacy Shield komentoval již s několikaročním předstihem: „Je to v podstatě to samé, co býval Safe Harbour, jen s novým jménem.“[103] To víceméně potvrdil i SDEU ve věci Schrems II[104], když Privacy Shield zrušil. Dále je obsahem rozsudku stanovisko, že SCCs pro přenos OÚ do třetích zemí zůstávají v platnosti, avšak národní dohledové orgány mohou platnost pozastavit nebo zrušit za situace, že vyhodnotí, že jejich dodržování v souladu s evropským standardem není v dané třetí zemi možné. SDEU tedy aproboval využití SCCs za stanovených podmínek a testu proporcionality v oblasti přezkumu rizik.

Zastaralé znění SCCs k předávání OÚ do třetích zemí je na základě prováděcích rozhodnutí EK (EU) 2021/914 a 2021/915 potřeba nahradit do konce roku 2022.

Na neaktuálnost SCCs byla EK pojistným sektorem upozorněna i během hodnocení dle čl. 97. K předávání OÚ do třetích zemí byly v GDPR obsažené nástroje vyhodnoceny jako nedostačující. Rozhodnutím EK byla vyčtena nízká flexibilita, která neodráží dynamický rozvoj globálních ekonomických vztahů. Závazná podniková pravidla se zase týkají předávání údajů v rámci skupiny. Kodexy chování a certifikační mechanismy jsou kapitolou samou pro sebe.

5.7 Doba zpracování

U doby zpracování postupuje pojišťovna v souladu se zásadou minimalizace, zejména stanoví lhůty pro výmaz OÚ, které se budou vázat k jednotlivým typům a účelům zpracování. Pojišťovna vyhodnotí povinnost uchovávat nebo jinak zpracovávat OÚ po dobu vyplývající z právních předpisů a zda oprávněnost zpracování převáží nad ochranou zájmů a práv

[102] SDEU. *Rozsudek Soudního dvora (velkého senátu) ze dne 6. října 2015. Maximillian Schrems vs. Data Protection Commissioner*, C-362/14 [online]. 6. 10. 2015 [cit. 20. 2. 2022]. Dostupné z: https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=112515.
[103] Internet nemůže být divoký západ. *Index LN 06/2017*, Praha, 2017, s. 12–17, ISSN 2464-6911.
[104] SDEU. *Rozsudek Soudního dvora ze dne 16. července 2020. Data Protection Commissioner vs. Facebook Ireland Limited a Maximillian Schrems*, C-311/18 [online]. 16. 7. 2020 [cit. 20. 2. 2022]. Dostupné z: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=541779.

subjektů OÚ a také možnost anonymizace, pokud již není nutné OÚ zpracovávat s vazbou na jednotlivé subjekty OÚ, např. u statistiky, cenotvorby – big dat.

Standardy obsahují přehled dob zpracování s ohledem na specifické účely v pojišťovnictví. Obecným pravidlem je, že pojišťovna zpracovává OÚ do jejich rozsahu a časovosti jen tak, jak je nezbytné ve vztahu k účelu zpracování, konkrétně např. u výkonu pojišťovací činnosti u potenciálního klienta do konce druhého kalendářního roku od poslední komunikace; v případě uzavření pojistné smlouvy nejméně po dobu trvání smluvního vztahu a 10 let po jeho ukončení, pokud ZDPZ nebo jiné předpisy nestanoví déle; u přímého marketingu po dobu trvání smluvního vztahu.

5.8 Informování o zpracování

S plnohodnotným přístupem k výkonu práv v rámci ochrany OÚ úzce souvisí poskytnutí podkladů v dostatečné míře a vyhovující formě. Jedná se o základní předpoklad k učinění plnohodnotného, skutečně informovaného rozhodnutí. V kontextu GDPR je to relevantní především u uzavírání smlouvy a samozřejmě i udělení, popř. odnětí souhlasu. Tento požadavek stoupá na významu s rostoucí tendencí ochrany spotřebitele.

GDPR je pouze zlomkem souboru informačních povinností, které v současnosti pojišťovny nesou. Podle analýzy, jež ČAP uskutečnila ke stavu národních a evropských legislativních předpisů účinných k roku 2018, je řada povinností duplikována. Počet zveřejňovaných údajů v pojistných smlouvách se tak např. v případě pojistných produktů s investiční složkou v roce 2018 zvýšil v porovnání se situací v 90. letech o 705 %.[105] Dále Mesršmíd uvádí, že pojišťovnictví se dotklo za posledních pět let – přímo či nepřímo – celkem 130 inciativ EK, tj. více než dvě měsíčně. Z toho ve 40 případech jde o návrhy právních aktů, z nichž některé jsou již v platnosti, nebo dokonce účinné. Vyplývá z toho logicky obava, že může dojít k nezamýšleným efektům – větší administrativě, nákladům a překrývání některých ustanovení právních aktů apod.[106] I když byla daná publikace vydána v roce 2015, zůstává pořád aktuální. To akcentovala taktéž Michaela Koller, ředitelka IE, která uvedla[107], že SII, PRIIPs, IDD

[105] Komentář ČAP: Pojišťovny svazuje evropská regulace. In: *Opojištění.cz* [online]. 26. 9. 2017 [cit. 20. 2. 2022]. Dostupné z: https://www.opojisteni.cz/spektrum/komentar-cap-pojistovny-svazuje-evropska-regulace/c:13193/.
[106] MESRŠMÍD, 2015, op. cit., s. 156.
[107] DURSKA, Agnieszka. Insurance Europe: Working together to ensure the voices of Europe's insurers are heard in EU policymaking. In: *Piu.org.pl* [online]. 27. 1. 2021 [cit. 20. 2. 2022]. Dostupné z:

a GDPR vedly ke 250 % (z 33 na 115) nárůstu poskytování předsmluvních informací u prodeje pojistného produktu s investiční složkou. U online prodeje se jedná o 161 informací. To má patrně celoevropský rozměr.

Konkrétně u GDPR vyplývá informační povinnost z čl. 13 a násl. a bodů 60, 61, 62 preambule. *Standardy* popisují konkrétní postup pojišťovny, která v okamžiku, kdy získává OÚ ke zpracování, poskytne např. informace o totožnosti a kontaktech pojišťovny, včetně DPO; o účelech a právních základech zpracování, včetně souhlasu; případných dalších příjemcích; právech; případném plně AR a o tom, zda je poskytnutí OÚ zákonným, či smluvním požadavkem, popř. požadavkem nutným pro uzavření smlouvy. Bude-li to možné, pojišťovna informuje také o době zpracování nebo kritériích jejího stanovení.

Standardy berou v potaz také situace, kdy pojišťovna získala OÚ nepřímo, např. od jiných správců, z veřejně dostupných zdrojů či od datových brokerů. Za této okolnosti nejpozději do jednoho měsíce po získání anebo nejpozději v okamžiku první komunikace nebo při prvním zpřístupnění OÚ, podle toho, co nastane dříve, poskytne informace dle výčtu výše a charakteru OÚ i zdroji.

Informace je možné subjektu OÚ předat prostřednictvím třetí osoby (pojišťovacího zprostředkovatele nebo pojistníka u skupinových smluv ŽP nebo leasingových smluv) za podmínky, že se k tomu smluvně zaváže.

Následkem nastíněné regulatorní zátěže vůči pojistnému odvětví v oblasti informačních povinností dochází k informačnímu přetížení spotřebitele, který obdrží enormní množství podkladových materiálů[108]. To může být matoucí. Např. jak uvádí Zuboff u zaklikávání souhlasu u smluvních podmínek obecně, včetně rámce ochrany OÚ, které většina uživatelů nečte. Kromě obsahu je proto podstatná i forma.

Ta by v ideálním případě měla splňovat kritéria strukturovanosti a přehlednosti a měla by se vyhýbat duplicitě. Jedná se o kroky k posílení pravděpodobnosti učinění informovaného rozhodnutí, které ve své činnosti potvrdil i soudní výklad[109] a přístup ČNB[110]. Důležitým

---

https://piu.org.pl/blogpiu/insurance-europe-working-together-to-ensure-the-voices-of-europes-insurers-are-heard-in-eu-policymaking/.

[108] IE. *Making EU insurance regulation that works and benefits consumers* [online]. Brussels: IE aisbl, December 2019 [cit. 20. 2. 2022]. Dostupné z: https://www.insuranceeurope.eu/publications/498/making-eu-regulation-that-works-and-benefits-consumers/download/Making+EU%20regulation%20that%20works%20and%20benefits%20consumers.pdf.

[109] ČR. *Nález Ústavního soudu ze dne 11. listopadu 2013 sp. zn. I. ÚS 3512/11* [online]. 11. 11. 2013 [cit. 20. 2. 2022]. Dostupné z: http://nalus.usoud.cz/Search/GetText.aspx?sz=1-3512-11.

aspektem je zvolení jazykových prostředků, které umožní reálné pochopení obsahu. Proto *Standardy* uvádějí, že pojišťovna bude všechny informace poskytovat ve stručné formě a zajistí, aby byly snadno přístupné a srozumitelné. Pojišťovna může využít tzv. „vrstveného přístupu“ pomocí stručného shrnutí základních informací s odkazy na detailnější informace. Tento krok je dobrým předpokladem pro hlubší pochopení materie.

Za zmínku také stojí fakt, že dané informace jsou poskytovány bezplatně. Výjimkou jsou případy zjevně nedůvodné nebo nepřiměřené žádosti, typicky žádosti tzv. „notorických stěžovatelů“.

Z důvodu ústupu papírové formy dokumentů mohou být informace určené subjektům OÚ poskytovány i v elektronické podobě, zejména prostřednictvím webových stránek.

Pojišťovna nemusí poskytovat výše uvedené informace v případě, že jimi subjekt OÚ již disponuje. Pokud se jedná o OÚ získané z jiných zdrojů než od subjektu OÚ, nemusí pojišťovna v souladu s čl. 14 GDPR navíc poskytnout výše uvedené informace v situaci, kdy jejich poskytnutí není možné nebo by vyžadovalo neúměrné úsilí nebo je získávání či zpřístupnění výslovně stanoveno právem EU nebo ČR anebo OÚ musí zůstat důvěrné s ohledem na zákonnou povinnost mlčenlivosti. To *Standardy* doplňují příkladem pro neúměrné úsilí, za které je možno považovat případy zpracování OÚ osob účastných na likvidaci pojistné události, kdy s touto třetí osobou nemá pojišťovna žádný kontakt ani vztah, např. se svědkem dopravní nehody.

5.9 Práva subjektu údajů

5.9.1 Obecně

Jelikož celková koncepce ochrany OÚ směřuje k bilancování nerovného postavení mezi subjektem OÚ a správcem či zpracovatelem ve vztahu k nakládání s informacemi o jeho osobě, jsou její neopominutelnou součástí, vedle povinností tvořících mantinely přípustného zpracování OÚ, také specifická práva, kterými subjekt OÚ vůči správci, příp. zpracovateli disponuje. Ta mají za cíl především zvýšit jeho informovanost o operacích týkajících se OÚ

[110] ČNB. *Dohledový benchmark č. 4/2018 k určitosti stanovení rozsahu pojištění včetně výluk z pojištění* [online]. Praha: 13. 12. 2018 [cit. 20. 2. 2022]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-trh/.galleries/vykon_dohledu/dohledove_benchmarky/download/dohledovy_benchmark_2018_04.pdf.

a příp. mu dát možnost určité míry kontroly nad formou a rozsahem nakládání. Jde tedy o formu posílení jeho faktické možnosti informačního sebeurčení v digitálním věku.[111]

Shodně s GDPR proto věnují *Standardy* samostatnou kapitolu právům subjektů OÚ. GDPR oblast upravuje v čl. 12 a násl. Ten kromě informační povinnosti správce v odst. 1 specifikuje v odst. 2, že tento vyhoví žádosti subjektů OÚ za účelem výkonu práv, ledaže není splněna podmínka proveditelné identifikace dle čl. 11 odst. 2 GDPR. Zde platí, že při posuzování identifikovatelnosti je namístě brát v potaz objektivní faktory, jakými jsou volná dostupnost referenčních údajů, stav techniky, náklady na identifikaci či časová a systematická náročnost této operace.[112] U pojišťovny by metoda měla být úměrná rizikovosti uplatněného práva. Jedná se např. o komunikaci s klientem prostřednictvím ověřeného kanálu, jako je prostředí uživatelského účtu nebo sada otázek s předem definovanými odpověďmi, které subjekt OÚ sám uvedl při prvotní identifikaci.

Primárním krokem pro výkon práva je ale podání žádosti ze strany subjektu OÚ. Dle čl. 12 odst. 3 GDPR správce žádosti vyhoví bez odkladu, ve lhůtě jednoho měsíce od obdržení. Lhůta může být v případech nadměrné složitosti či velkého počtu žádostí prodloužena o dva měsíce, o čemž je subjekt informován. GDPR zde zakotvuje i požadavek na formu. Je-li žádost podána elektronicky, poskytnou se tak i informace, je-li to možné a pokud subjekt nepožádá o jiný způsob.

V případě, že žádosti o OÚ není možné vyhovět, v souladu s odst. 4 správce či pojišťovna informuje bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti subjekt OÚ o důvodech a možnosti podat stížnost u DPA a žádat o soudní ochranu. Tento proces je dle odst. 5 bezplatný. To, ostatně jako u informační povinnosti, nemusí platit v neodůvodněných či nepřiměřených případech.

Standardy v obecné rovině zakotvují, že pojišťovna stanoví postupy, které usnadní výkon práv, např. mechanismy pro podávání žádostí, uplatnění práva vznést námitku apod. Také uvádějí, že v souladu s informační povinností pojišťovna informuje o právech a způsobech uplatnění. Informace o výkonu práv mohou být dle odst. 7 doplněny standardizovanými ikonami kvůli jednoduššímu pochopení.

[111] POLČÁK et al., 2018, op. cit., s. 448.
[112] POLČÁK et al., 2018, op. cit., s. 399.

5.9.2 Právo na přístup

Právo na přístup vycházející z obecnějšího práva na informace upravuje čl. 15 a body 63, 64 preambule GDPR. Právo na informace chápu ve dvou rovinách, na základě toho, zda se jedná o OÚ získané přímo od subjektu OÚ dle čl. 13 GDPR, nebo od třetí osoby dle čl. 14 GDPR.

Podle *Standardů* má subjekt OÚ právo požadovat po pojišťovně, aby mu sdělila, zda a jaké OÚ o něm zpracovává, viz kapitola 5.8 této práce. Právo na přístup se naopak nevztahuje na OÚ, které by mohly ohrozit PPP, vyšetřování trestných činů nebo aktivity týkající se AML/CFT; mlčenlivost; nepříznivě zasáhnout práva a svobody jiných osob. Do poslední kategorie spadají *Standardy* explicitně vymezené příklady, tj. že pojišťovna nebude poskytovat zdravotní údaje třetích osob ani není povinna poskytnout právo na přístup jednotlivci za účelem zjištění, zda byl určen subjektem OÚ jako obmyšlená osoba v pojistné smlouvě.

5.9.3 Právo na opravu a omezení zpracování

Právo na opravu vycházející ze zásady přesnosti je v GDPR vymezeno čl. 16 a bodem 65 preambule. Subjekt OÚ má právo požádat pojišťovnu o opravu nepřesných OÚ. Pojišťovna ověří jejich přesnost a aktuálnost. Než tak učiní, je jejich zpracování omezeno v souladu s dikcí čl. 18 a bodem 67 preambule GDPR. To je provedeno dle technických možností pojišťovny např. pozastavením generování následných předpisů či procesu vymáhání pohledávek na dobu potřebnou k ověření nebo za situace, že zpracování je protiprávní, subjekt odmítá výmaz OÚ a žádá místo toho omezení použití, nebo že správce již OÚ nepotřebuje pro účely zpracování, ale subjekt je požaduje pro určení, výkon nebo obhajobu právních nároků apod.

Po úspěšném ověření OÚ dochází k opětovnému zahájení zpracování, o kterém je subjekt OÚ před započetím informován. Pojišťovna zajistí, že uplatněné právo na opravu bude zohledněno i při případné obnově dat ze záložních zdrojů či archivů.

Čl. 16 GDPR je následně rozveden čl. 19, upravujícím oznamovací povinnost ohledně opravy nebo výmazu OÚ nebo omezení zpracování. Na základě tohoto ustanovení správce oznamuje jednotlivým příjemcům, jimž byly OÚ zpřístupněny, veškeré opravy nebo výmazy OÚ nebo omezení zpracování provedené v souladu s čl. 16, 17, 18, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Správce také informuje subjekt OÚ o těchto příjemcích, pokud to subjekt OÚ požaduje.

Právo na opravu se opětovně netýká obdobných OÚ jako právo na přístup.

5.9.4 Právo na výmaz a být zapomenut

Právo na výmaz je v GDPR upraveno čl. 17 a body 65, 66 preambule. Společně s právem být zapomenut vychází z myšlenky, že subjekt OÚ má právo, aby pojišťovna jeho OÚ v určitých případech dále nezpracovávala.

Subjekt OÚ může požádat pojišťovnu o výmaz např. v případech, kdy pojišťovna již nepotřebuje OÚ pro účel, ke kterému je zpracovávala, a to v souladu s výše rozebranými lhůtami, nebo kdy došlo k odvolání souhlasu nebo kdy podal úspěšnou námitku proti zpracování na základě oprávněného zájmu.

Pojišťovna v případech odůvodněných žádostí vymaže nebo anonymizuje OÚ bez zbytečného odkladu. V souladu s odst. 3 však nevymaže OÚ v případě, kdy je oprávněna nebo povinna je zpracovávat na základě jiného právního základu, jako je ochrana právních nároků či plnění právní povinnosti správce, nebo pro jiný účel, kterým může opětovně být např. PPP, AML/CFT. Pokud je výmaz OÚ pojišťovnou odmítnut, informuje o tomto subjekt OÚ, včetně důvodu a poučení o možnosti podat stížnost u DPA a bránit se proti takovému rozhodnutí u soudu.

Vzhledem k vzájemným souvislostem a struktuře GDPR došlo během tvorby *Standardů* k podřazení práva být zapomenut. Jedná se o právo, na základě kterého může subjekt OÚ požadovat, aby pojišťovna jeho OÚ v určitých případech dále nezpracovávala.

5.9.5 Právo na přenositelnost

Právo na přenositelnost je vyjádřením zvýšené kontroly nad OÚ a vytvořením možnosti učinit v této věci rozhodnutí. To má zejména význam v případech automatizovaného zpracování OÚ, tedy bez ingerence lidského faktoru. Portabilitu nově zakotvuje čl. 20, bod 68 preambule GDPR a pokyny[113], které *Standardy* zohledňují.

Portabilita se uplatní pouze za splnění předem daných podmínek. Pojišťovna zpracovává OÚ pouze automatizovaně (nejedná se např. o vedení fyzického spisu); anebo je právním základem zpracování souhlas nebo plnění smlouvy a výkonem práva nebudou nepříznivě

[113] Article 29 Data Protection Working Party. *Guidelines on the right to "data portability"* [online]. Brussels: Article 29 Data Protection Working Party, 13. 12. 2016 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/newsroom/article29/items/611233/en.

dotčena práva ani svobody třetích osob (např. anamnéza třetích osob ve zdravotní dokumentaci) v souladu s požadavkem odst. 4.

Důležitost podoby informací je tak ve *Standardech* zohledněna i při výkonu práv. Subjekt OÚ má v rámci práva na přenositelnost nárok získat své OÚ ve strukturovaném, běžně používaném a strojově čitelném formátu a dále má právo požádat, aby je pojišťovna přímo předala jinému správci, pokud je to technicky proveditelné.

Právo se vztahuje pouze na původní OÚ, tj. ty, které subjekt OÚ předal správci (např. na formuláři o oznámení pojistné události, na klientem zaslané lékařské zprávě). Z přenositelnosti jsou vyloučeny OÚ odvozené nebo vyvozené z údajů poskytnutých (např. výsledky revizní prohlídky provedené na objednávku pojišťovny, výsledky profilování) a OÚ zpracovávané ve veřejném zájmu či orgány veřejné moci. Logickou podmínkou je také to, že správce dotčené OÚ ještě zpracovává.

Využití práva na přenositelnost neznamená automatický výmaz, jak je zakotveno i odst. 3.

Pojišťovna dále neodpovídá za zpracování provedené subjektem OÚ nebo přijímajícímu správci, který nemá povinnost OÚ přijmout. Podle mých informací však k praktickým potížím nedochází.

5.9.6 Právo na námitku

GDPR se právu na námitku věnuje v čl. 21 a bodech 69, 70 preambule. I na toto právo má být subjekt OÚ výslovně upozorněn.

Konkrétně proti zpracování OÚ pojišťovnou na právním základě oprávněného zájmu může subjekt OÚ vznést námitku. V pojišťovnictví může jít zejména o účely přímého marketingu zahrnující profilování. Po vznesení námitky je přestane pojišťovna zpracovávat. U ostatních účelů pojišťovna námitce vyhoví, ledaže prokáže, že oprávněné důvody, veřejný zájem či oprávněný zájem správce nebo třetí strany převažují nad základními právy a svobodami subjektu OÚ anebo že je další zpracování nezbytné pro určení, výkon nebo obhajobu právních nároků pojišťovny. Do té doby je zpracování omezeno.

Toto právo se nevztahuje na zpracování OÚ prováděná pojišťovnou na základě jiných právních základů, než je oprávněný zájem, např. plnění právní povinnosti.

5.10 AR a profilování

S narůstající efektivitou a mírou použití nových technologických řešení ve finančních službách GDPR v souladu s deklarovaným *pro futuro* přístupem zahrnulo v čl. 22 a bodech 68, 71, 72 preambule i oblast AR, popř. profilování. Úprava je doplněna pokyny[114] a *Úmluvou 108*.

Míra použití AR se i v souvislosti s dále rozebíranou UI bude zvyšovat. Proto je v této práci podrobím důkladnější analýze a pokusím se vymezit i dle mého názoru vhodné *check and balances*.

Profilováním rozumím dle čl. 4 odst. 4 GDPR jakoukoliv formu automatizovaného zpracování OÚ hodnotící osobní aspekty a vztahující se k FO, zejména za účelem analýzy či předvídání aspektů souvisejících s pracovním výkonem subjektu OÚ, jeho ekonomickou situací, zdravotním stavem, osobními preferencemi nebo zájmy, spolehlivostí nebo chováním a s místem pobytu či pohybu, pokud má pro něj právní účinky nebo se ho podobným způsobem významně dotýká. Polčák takto autonomně tvořená pravidla přibližuje mj. na příkladu pojišťovnictví jako nejvyšší formy chytré regulace, kdy dispozice příslušné normy nemá předem definované stavy a její konstrukce je plně v režii autonomního algoritmu. Autonomní systém tak vyhodnocuje data z cílového systému a na jejich základě nevolí jen z předem definovaných variant, ale sám tyto varianty originálně vytváří (a následně díky datům z regulovaného prostředí okamžitě vyhodnocuje jejich úspěšnost)[115]. Zde hovořím o plně automatizovaném zpracování, tj. takovém, kde není do rozhodovacího procesu zahrnuta lidská intervence.

K posílenému postavení AR Polčák dále uvádí, že s rozvojem strojového učení, UI a vytěžování big dat přichází stále častěji ke slovu podnikatelské či analytické modely, které využívají maximum dostupných informací k profilování.[116] To souvisí také s rozmachem behaviorální predikce, které se kriticky věnuje Zuboff v *The age of surveillance capitalism*. Popisuje, že mechanismy a ekonomické imperativy prvotně aplikované především internetovými mega společnostmi pro oblast marketingu si postupně našly cestu i do offline a dalších odvětví. Jako jeden z příkladů aplikace prediktivních modelů Zuboff uvádí právě

[114] Article 29 Data Protection Working Party. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* [online]. Brussels: Article 29 Data Protection Working Party, 3. 10. 2017 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/newsroom/article29/items/612053/en.
[115] POLČÁK et al., 2018, op. cit., s. 18.
[116] POLČÁK et al., 2018, op. cit., s. 460.

pojišťovnictví a tzv. „behaviorální underwriting“, využívaný např. u tzv. „*smart* domácností“[117] a hlavně u telematiky v rámci pojištění motorových vozidel při stanovování výše pojistného a příp. i vyplácení plnění[118]. Další potenciálně zajímavou oblastí je ŽP v kontextu *wearables* apod., ve kterých jsou shromažďovány zdravotní OÚ. Tyto konstrukty rozebírám optikou pojistné praxe právě u UI.

Co se však týká AR jako takového, pojišťovna potřebné údaje zpracuje dle klasifikace pojistných rizik, což je proces kategorizace zájemců o pojištění na základě rozdílů v očekávaných rizicích. Nejuváděnější příklady zahrnují rozlišování na základě věku v případě ŽP, zdravotního stavu v případě zdravotního pojištění a povahy majetku v případě pojištění majetku[119]. Minimalizace rizika a jeho správné vyhodnocení jsou tak relevantní nejen pro naplnění zájmů pojišťovny, ale také jako prevence pro splnění povinností vůči klientům či z obecného hlediska cenově přístupného pojištění. To se samozřejmě netýká všech OÚ. V souladu se zákazem diskriminace by selekce na základě vysoce citlivých informací, jako např. o rase, národnosti a zkušenosti s domácím násilím, která vede k vyšší pravděpodobnosti uplatnění nároků z ŽP a pojištění zdravotního či invalidity, disproporčně omezila možnosti těchto osob, a to pouze na základě příslušnosti k určité znevýhodněné skupině. Proto argumenty informační asymetrie a adverzní selekce nejsou dostatečně silné pro legitimizaci zpracování všech OÚ v rámci analýzy rizik[120]. To je v souladu s požadavky zásad týkajících se pojistných smluv[121], ale i s faktickým pohledem ČSpA identifikovaným u UI.

Co platí pro UI, platí i zde – navzdory tomu, že definice profilování je obecně uznávaná, nadále existují praktické výzvy. Hodnocení profilování se opírá pouze o obecné principy vymezené čl. 6 GDPR, ale charakter profilování a jeho fundamentální význam pro kontinuitu poskytování služeb v rámci pojistného sektoru by si žádaly vymezení konkrétnějších pravidel a limitů pro použití OÚ. Dle *Standardů* má subjekt OÚ právo nebýt předmětem AR, které by na něj mělo právní účinky nebo by se ho *per analogiam* významně dotklo. Na příkladu je

[117] ZUBOFF, 2019, op. cit., s. 10.
[118] ZUBOFF, 2019, op. cit., s. 211–212.
[119] BAKER, Tom. *Containing the Promise of Insurance: adverse selection and risk classification* [online]. Philadephia: University of Pennsylvania Carey Law School, 2002, s. 7 [cit. 20. 2. 2022]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=322581.
[120] Independent German Federal and State Data Protection Supervisory Authorities. *Report on Experience Gained in the Implementation of the GDPR* [online]. Independent German Federal and State Data Protection Supervisory Authorities, November 2019, s. 6 [cit. 20. 2. 2022]. Dostupné z: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/Evaluation-Report-German-DPAs-Clean.pdf.
[121] HEISS, Helmut. *The Principles of European Insurance Contract Law: an optional instrument?* [online]. Brussels: © European Parliament, 2010 [cit. 20. 2. 2022]. Dostupné z: http://www.europarl.europa.eu/document/activities/cont/201004/20100430ATT73919/20100430ATT73919EN.pdf.

dovysvětleno, že pojišťovna může využívat plně automatizované zpracování pro marketingové účely. To *Standardy* následně rozvádějí na konkrétnějším příkladu, kdy pojišťovna provádí marketingovou kampaň a automaticky oslovuje pouze klienty, kteří by o nabízený typ pojištění mohli mít zájem.

Dále pojišťovna může plně AR použít, avšak pouze za splnění podmínek dle čl. 22 odst. 2 GDPR. Hlavně se může jednat o nezbytnost k uzavření nebo plnění pojistné smlouvy, tj. o oprávněný zájem. Jde např. o aplikaci AR při online sjednávání pojištění v rámci kalkulace, dnes běžně např. u cestovního pojištění. S rostoucí digitalizací lze důvodně předpokládat stoupající tendenci tohoto trendu, což uvádí i Tereszkiewicz[122].

Výklad nezbytnosti ze strany EDPB však vytváří bariéry pro praktické využití v pojišťovnictví. Na s. 23 pokyny vymezují, že „správce musí být schopen prokázat, že tento druh zpracování je nezbytný, a musí zvážit, zda by nebylo možné použít metodu, která méně zasahuje do soukromí. Existují-li účinné a méně rušivé prostředky k dosažení stejného cíle, pak nejde o ‚nezbytnost'". To v praxi znamená, že každé toto použití musí být individuálně zdůvodňováno a tím přináší neúměrnou zátěž pro pojistitele. Kromě toho se jedná o brzdu budoucího technologického vývoje, kdy jsou inovativní produkty založeny právě na automatizaci, která může přinést pozitivní dopady nejen na samotné pojistitele, ale především na spotřebitele v postavení subjektů OÚ. Podrobněji to řeším níže, avšak pro vykreslení se jedná např. o nabídku pojištění vozidel prostřednictvím mobilní aplikace, kdy zájemce o pojištění zašle fotografii vozidla a uvede požadované informace, na základě čehož je mu pak zaslána nabídka pojištění s automatizovaně vypočtenou výší pojistného. V případě akceptace nabude smlouva platnosti zaplacením tohoto pojistného. Úzký výklad „nezbytnosti" je zde překážkou poskytování služby v reálném čase, kdy není možno prokázat tuto „nezbytnost" pro uzavření smlouvy. Podobně může být argumentováno u nabídek cestovního pojištění nebo vyřizování pohledávek. Z tohoto důvodu bylo během hodnocení dle čl. 97 pojistným sektorem doporučeno revidovat zmíněné pokyny ve smyslu výmazu ustanovení o „nezbytnosti"[123].

[122] TERESZKIEWICZ, Piotr. Digitalisation of Insurance Contract Law: preliminary thoughts with special regard to insurer's duty to advise. In: MARANO, Pierpaolo a NOUSSIA, Kyriaki. *InsurTech: a legal and regulatory view*. První vydání. Cham: Springer, 2020, s. 127. AIDA Europe Research Series on Insurance Law and Regulation. ISBN 978-3-030-27385-9.
[123] ANDRAŠČIKOVÁ, Jana. Kompatibilita *Standardů* s požadavky pokynů [tabulka]. In: *Opojištění.cz* [online]. [cit. 20. 2. 2022]. Dostupné z: https://www.opojisteni.cz/legislativa/evropska-legislativa/krok-za-krokem-ke-kodexu-chovani-podle-gdpr/c:17456/.

Dále je-li AR povoleno právem EU nebo ČS anebo pokud subjekt OÚ udělil výslovný souhlas, souhlas je i zde, nepřekvapivě, kamenem úrazu. Může být předmětem diskuzí, zda souhlas s AR pro ŽP a zdravotní pojištění je svobodně udělen; je-li uzavření smlouvy na něm závislé, tj. není-li souhlas pro AR udělen, vede to k objektivní nemožnosti uzavření pojistné smlouvy, jak bylo analyzováno u souhlasu v kapitole 5.4.4 této práce. Zde se opětovně vracím k podmíněnosti dle čl. 7 odst. 4 GDPR a pokynů EDPB 5/2020.

Dle mého názoru je v dnešní době proporcionálně aplikované AR skvělou pomůckou pro poskytování pojistných služeb, a to až do té míry, že spadá pod nezbytnost. Není-li však výklad jednotný, vidím řešení v oddělení souhlasů – k AR a k hodnocení rizik a likvidaci pojistných událostí. To by umožnilo odmítnout AR, ale zároveň by to nelimitovalo přístup k pojištění. V neposlední řadě musí být o aplikaci tohoto prostředku a jeho důsledcích subjekt OÚ v souladu s čl. 13 odst. 2 písm. f) GDPR informován. Především mu musí být umožněno jednoduchou cestou požádat o lidský zásah a rozhodnutí napadnout, což považuji za dostačující záruku. Právo na lidský zásah, a tedy i vysvětlení často velice složitých algoritmů, rozebírám níže u UI.

Mám za to, že jsou-li tedy v praxi důsledně aplikována *compliance* s racionálně formulovanými legislativními požadavky, jako např. GDPR, ale *pro futuro* třeba (snad) i nové ePrivacy, DORA nebo AIA, je v evropském pojistně právním ekosystému splněna podmínka dostatečných *check and balances* a nehrozí Harariho predikce, kdy technická revoluce možná potvrdí nadvládu algoritmů velkých dat a ty pak podkopají osobní svobodu.[124] Zdůrazňuji však, že tento závěr nesdílím pro všechny ekonomicky významné sektory.

Pro úplnost, automatizovaným zpracováním není dotčen výkon jiných práv. Je zaveden omezený režim pro případy, kdy je subjektem OÚ dítě a dochází ke zpracování citlivých OÚ. To je v souladu s požadavky bodů 38 a 71 preambule GDPR.

[124] HARARI, Yuval N. *21 lekcí pro 21. století*. Přeložila Z. GUBALOVÁ. Praha: Leda, 2019, s. 66. ISBN 978--80-7335-612-5.

5.11 Postavení správců a zpracovatelů

Standardy uvádějí, že pojišťovny mohou vystupovat v roli správce i zpracovatele OÚ. *Standardy* se vysvětlení odlišnosti jejich postavení explicitně nevěnují, proto problematiku analyzuji zde, jelikož během fáze implementace GDPR byla významná.

Správcem je podle čl. 4 odst. 7 GDPR a v kontextu *Standardů* pojišťovna, která sama nebo společně s jinými určuje účely a prostředky zpracování OÚ. Dle čl. 24 odst. 1 GDPR nese odpovědnost zavést vhodná TOO, aby zajistila a doložila, že zpracování je v souladu s GDPR. Opatření vycházejí z požadavků na záměrnou a standardní ochranu dle čl. 25, bodu 78 preambule GDPR. Tok dat v prostředí ICT je totiž nejsnáze regulovatelný při jejich prvotním vzniku. Nejlépe zabezpečeny jsou pak OÚ, se kterými není nakládáno vůbec, proto je v rámci standardní ochrany OÚ kladen důraz na minimalizaci rozsahu, množství i doby zpracování OÚ. Smyslem záměrné ochrany OÚ je pak od úvodní fáze procesu zpracování účinně chránit OÚ, např. formou pseudonymizace.[125] V čl. 24 odst. 3 se uvádí, že plnění příslušných povinností může být doloženo i dodržováním schválených kodexů chování dle čl. 40 GDPR nebo schválených mechanismů pro vydávání osvědčení v rámci čl. 42 GDPR. To může být dle čl. 28 odst. 5 aplikováno i na zpracovatele.

V případě společného správcovství podle úpravy čl. 26 GDPR si společní správci transparentním ujednáním vymezí podíly na odpovědnosti za plnění povinností. Bez ohledu na jimi domluvené podmínky může subjekt OÚ vykonávat svá práva u každého i vůči každému z nich.

Zpracovatelem je podle čl. 4 odst. 8 GDPR FO nebo PO, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává OÚ pro správce. Platí premisa čl. 29 GDPR, že zpracovatel a jakákoliv osoba, která jedná z pověření správce nebo zpracovatele a má přístup k OÚ, je mohou zpracovávat pouze na pokyn správce, ledaže jim jejich zpracování ukládá právo EU nebo ČS. Zpracovatelovo postavení je blíže upraveno čl. 28 GDPR. Je povinen poskytnout dostatečné záruky zavedením vhodných TOO.

Mezi správcem a zpracovatelem vzniká vztah na základě smlouvy stanovující: předmět, dobu trvání, povahu a účel zpracování, typy OÚ a povinnosti a práva správce. Dále se vymezí: zpracování pouze na základě doložených pokynů správce, mlčenlivost osob oprávněných ke zpracování, přijetí opatření k zabezpečení zpracování podle čl. 32 GDPR, případné povolení

[125] POLČÁK et al., 2018, op. cit., s. 447.

sub zpracovatele a součinnost se správcem. Nad rámec individuálních smluv mezi správcem a zpracovatelem mohou být písemné smlouvy nebo jiné právní akty založeny zcela nebo částečně na SCCs, mj. i v případě, že jsou součástí osvědčení uděleného správci či zpracovateli podle čl. 42 a 43 GDPR.

Pro pojišťovnu v pozici správce je nejvýznamnějším zpracovatelem zprostředkovatel dle IDD a ZDPZ. Také se může jednat o: poskytovatele ICT, smluvní lékaře, externí likvidátory, poskytovatele asistenčních služeb, ale třeba také marketingové agentury. Zprostředkovatelská síť je však kardinálním prvkem výkonu pojišťovnictví. Následující digitalizační roky ukážou, do jaké míry bude tento distribuční kanál ovlivněn distanční, především online formou distribuce.

Podnětem k zamyšlení je i moment změny postavení, kterému se věnoval NSS[126]. Pojišťovna se správcem nemůže stát dříve než v okamžiku, kdy OÚ dojdou do sféry její dispozice. A tedy zprostředkovatel bude správcem v době, kdy OÚ získává a zpracovává v rámci vlastního obchodního vztahu s klientem. Okamžikem jejich poskytnutí pojišťovně a nadále v rámci úkonů souvisejících s administrací pojistné smlouvy bude již vystupovat jako zpracovatel.

Zvláštní režim je v čl. 27 GDPR zaveden pro zástupce správců nebo zpracovatelů, kteří nejsou usazeni v EU. V pojišťovnictví se zejména jedná o případy, kdy je pojišťovna součástí mezinárodní skupiny podniků anebo služby odebírá od dodavatelů usazených ve třetích zemích. Tato spolupráce funguje dle GDPR ve dvou rovinách: buď dojde k naplnění podmínky pro místní příslušnost dle čl. 3 odst. 2 GDPR, kdy správce nebo zpracovatel písemně jmenuje svého zástupce v EU, čímž ale nedochází k přenesení odpovědnosti, nebo je aplikována některá z výjimek popsaných čl. 27 odst. 2 GDPR, tedy příležitostné zpracování, které nezahrnuje ve velkém měřítku zvláštní kategorie OÚ uvedených v čl. 9 odst. 1 GDPR nebo OÚ týkajících se rozsudků v trestních věcech a trestných činech uvedených v čl. 10 GDPR a u něhož je nepravděpodobné, že by s ohledem na svou povahu, kontext, rozsah a účely představovalo riziko pro práva a svobody FO, nebo jde o orgán veřejné moci nebo veřejný subjekt.

[126] ČR. *Rozsudek NSS 9 As 34/2008–68* [online]. V Brně: 12. 2. 2009 [cit. 22. 2. 2022]. Dostupné z: http://www.nssoud.cz/files/SOUDNI_VYKON/2008/0034_9As__0800068A_prevedeno.pdf.

5.12 TOO

Zde načrtnutá TOO je skutečně nutné pojímat jako minimální, protože během diskuzí v PS GDPR ČAP vyplynulo, že každá z pojišťoven aplikuje řešení vyhovující její činnosti a kapacitám, která nejsou nutně totožná. *Pro futuro* bude oblast třeba posoudit i optikou DORA. *Standardy* uvádějí deklaratorní výčet opatření, zejména pravidelné testování, postupy pro důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování a taktéž pseudonymizaci, anonymizaci či šifrování OÚ. Poslední zmíněné kategorii je ve *Standardech* dedikována samostatná kapitola, kde je zdůrazněno, že pseudonymizované OÚ nicméně nejsou anonymizovanými údaji, proto se na ně stále vztahuje GDPR. Nadále platí, že pokud pojišťovna nemá účel ani právní základ ke zpracování, např. po uplynutí doby, příslušné OÚ vymaže anebo anonymizuje.

I pseudonymizovaná nebo anonymizovaná data jsou nezbytná pro fungování klíčových systémů pojišťovny, a to např. u pojistně matematických kalkulací, analytických modelů, výzkumu a vývoje produktů, služeb a trhu, jak objasňuji u big dat.

5.13 Porušení zabezpečení OÚ

GDPR zakotvuje zvýšenou míru ochrany a související informovanosti subjektů OÚ napříč EU. Zavádí tak nejen práva subjektů OÚ, ale i nové povinnosti správců či zpracovatelů. Mezi povinnosti správce kromě jiného náleží i nahlásit případy porušení zabezpečení OÚ DPA dle čl. 33 a 34 GDPR. Problematice se detailněji věnují i pokyny WP29[127], jež EDPB schválil.

Porušením zabezpečení OÚ se rozumí porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně, neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných OÚ.

Pojišťovna v pozici správce OÚ je povinna ohlásit DPA pouze takové porušení zabezpečení OÚ, které pravděpodobně představuje riziko pro práva a svobody FO, a to bez zbytečného odkladu. Byla stanovena lhůta 72 hodin od okamžiku, kdy se pojišťovna o porušení zabezpečení dozví, resp. získá rozumný stupeň jistoty, že došlo k porušení zabezpečení OÚ. Ohlášení může předcházet krátké prošetření s cílem zjistit, zda událost skutečně naplňuje

[127] Article 29 Data Protection Working Party. *Ohlášení případů porušení zabezpečení osobních údajů* [online]. Brussels: Article 29 Data Protection Working Party, 25. 5. 2018 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guideline/personal-data-breach-notifications_cs.

patřičné znaky, aniž by začala plynout lhůta. To se ale nevztahuje na případy, kdy je porušení evidentní. Pokud dojde k překročení této lhůty, je v souladu s recitálem 85 GDPR nezbytné, aby to správce odůvodnil.

Ohlášení nemusí být realizováno, pokud správce může v souladu s GDPR proklamovanou zásadou odpovědnosti doložit, že je nepravděpodobné, že by porušení mělo za následek riziko pro práva a svobody FO.

Z důvodu efektivnějšího způsobu plnění povinnosti ohlašování případů porušení zabezpečení OÚ byla ze strany IE a ČAP vypracována standardizovaná šablona, publikovaná ještě před nabytím účinnosti GDPR a formulářem ÚOOÚ[128]. Tuto šablonu jsem z pozice gestora PS GDPR ČAP přepracovala do české verze, jež je přílohou *Standardů*.

ČAP podporuje rozšíření jejího preventivního zavedení do GDPR dokumentace nejen v rámci sektoru pojišťovnictví[129] za účelem standardizace ohlašování. Dle mého názoru a zkušeností plyne ze zakomponování šablony do interní dokumentace pro eventuální použití řada výhod. V první řadě šablona splňuje požadavky GDPR. Při jejím řádném využití správce naplní své povinnosti vymezené pro situace porušení zabezpečení OÚ. V opačném případě totiž může být sankcionován v souladu s čl. 83 GDPR. Navíc může dojít ke kombinaci správní pokuty a dalšího opatření v souladu s čl. 58 odst. 2 GDPR. Dále je výhodou jednotného používání šablony nejen přehledná dokumentace incidentů v souladu s požadavky GDPR, ale i možnost použití pro komparaci, analýzy či statistické účely. V neposlední řadě se může jednat o vhodný nástroj pro studium a prevenci rapidně stoupajících kybernetických rizik s možným dopadem na OÚ. Sjednocená evidence kybernetických událostí nese nepochybné výhody, ještě znatelnější v případě přítomnosti OÚ. Ostatně toho jsou si vědomy i evropské orgány, které např. do DORA zakomponovaly prozatím dobrovolné sdílení dat relevantních z hlediska KB, a také ČAP, výsledkem čehož je *Samoregulační standard pro sdílení informací o kybernetické bezpečnosti*, zmíněný v kapitole 2.2.3.3 této práce.

[128] ÚOOÚ. *Ohlášení porušení zabezpečení osobních údajů dle GDPR* [online]. [cit. 22. 2. 2022]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=46004.
[129] ANDRAŠČIKOVÁ, Jana. Šablona pro ohlašování případů porušení zabezpečení osobních údajů. *Pojistný obzor: časopis českého pojišťovnictví* [online]. Praha: ČAP, 2018, č. 2, s. 12–13. ISSN 2464-7381 [cit. 22. 2. 2022]. Dostupné z: https://www.pojistnyobzor.cz/images/archiv/2018-2/casopis.pdf.

5.14 DPO

V závěrečné kapitole *Standardy* zakotvují požadavky na DPO dle čl. 37, 38, 39 bodu 97 preambule GDPR a pokynů EDPB[130].

Pojišťovna v případě naplnění podmínek pro nutnost zajistí brzké jmenování DPO, aby mohl být řádně a včas zapojen do procesů a operací zpracování OÚ. V souladu s čl. 37 odst. 2 GDPR se může skupina podniků rozhodnout, že jmenuje jednoho DPO. V případě, kdy pojišťovna jmenuje zahraničního DPO, na svůj náklad a odpovědnost zajistí překlad jeho vyjádření do českého jazyka.

DPO je v souladu s GDPR zaměstnanec pojišťovny či externí pracovník (FO či PO), jehož úkolem je dohlížet na dodržování předpisů. DPO ale nenese osobní odpovědnost za nesoulad zpracování pojišťovnou se *Standardy*, GDPR a dalšími předpisy o ochraně OÚ. Je jmenován na základě profesních kvalit, spolehlivosti, zodpovědnosti a trestní bezúhonnosti.

Mezi jeho hlavní úkoly patří dle čl. 39 GDPR např. poskytování informací a poradenství o povinnostech plynoucích z GDPR, monitorování souladu a návrh opatření, spolupráce a kontakt s DPA či řešení případů porušení zabezpečení v souladu s výše popsaným postupem.

Při výkonu činnosti je DPO vázán mlčenlivostí, nachází se v nezávislém postavení, není vázán pokyny správce ani zpracovatele a nemůže být v případě plnění svých povinností sankcionován. To platí i pro jiné úkoly a povinnosti, které může DPO dle dikce čl. 38 odst. 6 GDPR plnit, avšak pokyny doporučují vymezit pozice neslučitelné s funkcí DPO a zavést interní pravidla k prevenci střetu zájmů.

Pojišťovna dále včas a vhodnou formou zveřejní kontaktní údaje DPO a sdělí je DPA. Všechny subjekty, jejichž OÚ pojišťovna zpracovává, se mohou na DPO kdykoliv obrátit a předložit mu své návrhy, dotazy či stížnosti. Komunikace je považována za důvěrnou.

[130] Article 29 Data Protection Working Party. *Guidelines on Data Protection Officers ('DPOs')* [online]. Brussels: Article 29 Data Protection Working Party, 13. 12. 2016 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

5.15 DPIA

DPIA je upraveno čl. 35 a 36, body 75, 84, 89–96 preambule GDPR, ale také pokyny WP29, schválenými EDPB[131], a stanoviskem ÚOOÚ[132].

Pojišťovna vyhodnotí nutnost provedení DPIA pro druhy zpracování OÚ a vyžádá si posudek DPO, je-li jmenován. V neposlední řadě je DPIA vhodným podkladem pro zavedení přiměřených TOO v rámci standardní a záměrné ochrany, jak je popsáno výše. Dle s. 14 pokynů se jedná o interní nástroj, který má doplnit správu rizik a umožnit vhodné nastavení operací ještě před jejich zahájením. Pojem „riziko“ není GDPR přímo definován. Bod 83 preambule přináší výčet: náhodné nebo protiprávní zničení, ztráta, pozměnění, neoprávněné zpřístupnění nebo zpřístupnění předaných, uložených nebo jiným způsobem zpracovaných OÚ, které by mohly zejména vést k fyzické, hmotné nebo nehmotné újmě. *Standardy* uvádějí konkrétní příklad, podle kterého mezi kritéria pro stanovení vysoké rizikovosti zpracování OÚ patří provádění hodnocení bonity FO, včetně profilování a predikce (viz AR), zpracování zvláštních kategorií či velkého rozsahu OÚ apod.

Dále na s. 18 pokyny uvádějí, že tato dokumentace může sloužit jako doklad pro prokázání souladu vůči DPA či v rámci dobré praxe a transparentnosti.

Z mé zkušenosti je DPIA kontinuálním procesem. Pojišťovna provádí posouzení ve vztahu k nově zaváděným postupům, systémům a jejich změnám, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody FO.

5.16 Potenciál kodexu chování

Jak již bylo naznačeno, *Standardy* byly vytvořeny jako samoregulační nástroj pojišťoven z důvodu vůle deklarovat důležitost ochrany OÚ.

[131] Article 29 Data Protection Working Party. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* [online]. Brussels: Article 29 Data Protection Working Party, 4. 4. 2017 [cit. 19. 2. 2022]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
[132] ÚOOÚ. K povinnosti provádět posouzení vlivu na ochranu osobních údajů. In: *Uoou.cz* [online]. 7. 2. 2018 [cit. 19. 2. 2022]. Dostupné z: https://www.uoou.cz/k-nbsp-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385.

Samotné GDPR předvídá samoregulaci pro jednotlivé sektory v podobě kodexů chování dle čl. 40 a 41 GDPR, a to s ohledem na jejich konkrétní povahu a specifikace. Zmínka se nachází např. i u úpravy odpovědnosti správce v čl. 24 odst. 3 GDPR či dodržování povinností zpracovatele v čl. 28 odst. 5 GDPR. Podle čl. 32 odst. 3 GDPR k zabezpečení zpracování může být dodržování kodexu chování jedním z prvků, jimiž lze doložit soulad s požadavky. Dle čl. 35 odst. 8 GDPR je kodex zohledňován i při DPIA.

Vytvoření kodexu chování je formalizovaný postup obsahující i schválení ze strany ÚOOÚ. Jak dokládám níže, *Standardy* jsou považovány za vhodný základ pro pozdější potenciální transformaci v kodex chování, a to jak z obsahového, tak formálního hlediska.

Čl. 41 GDPR upravuje možnost monitorování schválených kodexů chování dle čl. 40, které nemusí nutně náležet do pravomocí příslušného DPA podle čl. 57 a 58 GDPR, v českém prostředí tedy ÚOOÚ. Tuto funkci může přebrat jiný, interní nebo externí, subjekt splňující požadavky na odbornost a nezávislost, jemuž se povedlo získat akreditaci udělenou ÚOOÚ. Ten předloží návrh kritérií pro akreditaci subjektu EDPB podle mechanismu jednotnosti v čl. 63 GDPR. Obdobně jako u DPO, monitorovací orgán by měl být oprávněn jednat samostatně, bez hrozby sankce nebo přímých či nepřímých zásahů ze strany držitele kodexu, jeho členů či jiného externího subjektu.

Výrazný vliv na problematiku i počáteční nadšení měly pokyny EDPB[133] publikované až po více než roce účinnosti GDPR. K přijetí finální verze došlo po ukončení veřejné konzultace, do které se ČAP vzhledem k očekávané relevanci dokumentu pro vývoj *Standardů* zapojila. Nejpodstatnějším bodem připomínek nejen ze strany pojistného odvětví byl nesoulad mezi level 1 textem nařízení, jež v čl. 41 odst. 1 GDPR stanovuje vytvoření monitorovacího orgánu jako možnost, a textem návrhu pokynů, diametrálně odlišně pojímajících ustanovení monitorovacího orgánu jako povinnost. To naneštěstí EDPB nezohlednil. Nekoherentním vztahem mezi GDPR a pokyny tak zkomplikoval uvádění kodexů chování v život. Už v samotném textu pokynů je sice, podobně jako ve stanovisku ÚOOÚ, proklamována podpora vzniku kodexů obsahujících specifika různých odvětví a zdůrazňujících pozitiva společných *best practice*s. Na druhé straně praktické dopady formulace pokynů jsou v rozporu s prohlašovanou podporou a konzistentní aplikací GDPR. Pokyny se pak věnují

[133] EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* [online]. Brussels: EDPB, 12. 2. 2019 [cit. 19. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under-0_en.

konkrétnějšímu vymezení podmínek pro kodexy a zřízení a fungování monitorovacího orgánu akreditovaného DPA.

Pokyny nadále charakterizují kodex jako jeden z nástrojů dobrovolného prohlášení a přijetí odpovědnosti dle GDPR. Upozorňují také na v některých případech povinné DPIA a vydávání osvědčení, pečetí a známek prokazujících soulad s GDPR. Dále tvrdí, že ke schválenému kodexu by mělo být přihlíženo i ze strany DPA v případě evaluace, řešení bezpečnostních situací, DPIA nebo při ukládání pokut. Není přímo obsažena možnost konzultací s DPA, kterému je ale umožněno poskytovat rady či doporučení k obsahové i formální stránce dokumentu. Principiálně by k tomu ale nemělo docházet ve fázi podání kodexu ke schválení. To je sice docela pochopitelné, DPA v této fázi již dokument akceptoval, ale na druhé straně to může vést k opakování celého procesu a opětovnému zatížení kapacit DPA i podávajícího subjektu. Tomu by se dle mého názoru dalo předejít akceptací vyžádaných dodatků i v tomto stadiu. Bohužel tato argumentace pojistného odvětví ve fázi veřejné konzultace k dokumentu taktéž nebyla zohledněna.

Plynulost procesu pokulhává rovněž u vymezení, kdy nedošlo během veřejné konzultace k akceptaci připomínek ke stanovení maximálního časového rámce pro posouzení kodexů. To může vést k řadě nesrovnalostí v praxi jednotlivých národních dozorových orgánů. Dovozuji, že podle § 50 adaptačního zákona se jedná o ústřední správní úřad a bude aplikována obecná úprava zákona č. 500/ 2004 Sb., správního řádu.

Z hlediska transparentnosti je relevantní, že EDPB všechny schválené kodexy chování a jejich úpravy či rozšíření shromáždí v registru a zveřejní.

Co tedy z pokynů plyne pro budoucí vývoj textu *Standardů*? Do jaké míry splňuje jejich současná podoba EDPB vymezená kritéria? Které požadavky pokynů budou největší výzvou? Přehledné zodpovězení těchto otázek ulehčuje již zmíněná tabulka „Kompatibilita *Standardů* s požadavky pokynů“. Současná verze *Standardů* tak téměř splňuje podmínky EDPB. Deficit kompatibility je shledáván především u monitorovacího orgánu. Zde se ale nachází začarovaný kruh, kdy EDPB ve vymezení jeho ustanovení jako povinnosti výrazně překročil své možnosti a zpřísnil dikci GDPR. Úkolem level 3 textu – pokynů není a nesmí být stanovení nových povinností. Jedná se pouze o nástroj detailnějšího vymezení a specifikace požadavků právně závazného level 1 textu – nařízení, což důkladněji rozebírám v další kapitole. Zde to může v podstatné míře vést k navýšení organizační, administrativní a finanční

zátěže zainteresovaných subjektů, např. oddělení od běžné organizační struktury nebo posouzení odbornosti. To má potenciální odrazující dopad.

Navzdory dlouhé době přípravy, očekáváním i aktivnímu vymezení zásadních připomínek jsou pokyny zklamáním, jež do praxe nevnáší mnoho pozitivního. Spíše naopak. Místo krystalizace požadavků zavádějí náročná kritéria nad rámec nařízení a zesilují nejistotu subjektů i DPA při posuzování náležitostí návrhů kodexů.

Z informací, které mám k dispozici od IE, je znát, že i ostatní evropské asociace pojistného odvětví přistupují k problematice opatrně. Cestu samoregulačního mechanismu tak zvolilo např. Slovensko, Německo, Španělsko, Nizozemsko či Finsko.

Ať už v současné, samoregulační verzi, nebo jako kodex chování *stricto sensu*, vidím ve *Standardech* potenciál pro obsahové rozšíření navazující na legislativní i faktický vývoj. To by dle mého názoru mohlo v přijetí vycházet z revidované ePrivacy, ale také dalších předpisů. Specificky DORA ze své horizontální povahy může být faktorem pro sjednocení minimálně principů TOO relevantních pro GDPR nebo pro úpravu vztahu pojišťoven a ICT TPPs. Z perspektivy subjektů OÚ bude stát za zvážení i zakomponování přístupu k mezisektorovému sdílení dat a insurtechu, především UI. Podle mých zkušeností mohou být právě *Standardy* vhodným nástrojem pro v rámci možností srozumitelné vysvětlení aplikace UI v pojistném sektoru.

6 Hodnotící zpráva EK

Očekávaná *Zpráva o hodnocení a přezkumu GDPR*, kterou byla EK povinna vydat v souladu s čl. 97 GDPR do 25. 5. 2020, byla o měsíc opožděna. Dle ustanovení je EK povinna dokument předložit EP a Radě, nejprve se zaměřením na transfer OÚ do třetích zemí a mechanismus jednotnosti a poté v pravidelných intervalech, každé čtyři roky. Následně EK v případě potřeby předloží návrhy na změnu GDPR, zvláště s přihlédnutím k vývoji ICT a dosaženému pokroku. To úzce souvisí s plánovaným rozšířením záběru EDPB i na tuto oblast, což plyne z *Výroční zprávy EDPB 2019*[134] nebo také např. *Pracovního programu EDPB 2021–2022*[135] a dynamického vývoje v oblasti legislativní úpravy inovativních technologií, např. UI či sdílení dat, jak průběžně zmiňuji a v kontextu pojišťovnictví analyzuji níže.

ČAP prostřednictvím IE komunikovala s EK stanovisko pojistného trhu ke dvěma letům účinnosti GDPR. Jednalo se o jedinečnou příležitost souhrnně vymezit nedostatky. Obsahem sdělení bylo, že vzhledem ke krátké době účinnosti není důvod otevírat samotný text nařízení. Tento krok by byl předčasný a kontraproduktivní. Dosud nevyjasněné výkladové otázky by měly být i nadále řešeny EDPB formou pokynů. K záběru připravované *Zprávy* IE doporučila rozšíření na další oblasti, jako je role EDPB a dopad jeho pokynů, se zaměřením na možné překročení jeho pravomocí podle čl. 70 GDPR rozšířením požadavků level 1 textu nebo zúžením výkladu požadavků GDPR, jak uvádím na příkladu kodexu chování výše. Dopodrobna byla tato aktivita analyzována v oblastech vymezených v příloze č. 1 této práce: „Kompatibilita GDPR a pokynů EDPB“. Jedná se např. o rozšíření definic a aplikace DPIA, citlivých údajů, informací z profilování a další. Toto téma, identifikované napříč evropskými pojistnými trhy, EK ve *Zprávě* naneštěstí neobsáhla. V navazujícím pracovním dokumentu pouze vágně uvádí, že požadavky k vyjasnění aplikace GDPR a poskytnutí právní jistoty nemohou jít na úkor vymezení dalších povinností.

Stejně neurčitě se postavila k jednotnosti právních základů GDPR a ePrivacy.

Dále byla zmíněna prohloubená fragmentace výkladu z důvodu činnosti DPA, např. u přístupu nizozemského dohledového orgánu k oprávněnému zájmu, který není možné

[134] EDPB. *EDPB Annual Report 2019* [online]. Brussels: EDPB, 18. 5. 2020 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/publication-type/annual-report_en.
[135] EDPB. *EDPB Work Programme 2021/2022* [online]. Brussels: EDPB, 16. 3. 2021 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-work-programme-20212022_cs.

využívat pro komerční účely ani za účelem zisku, což je v rozporu s bodem 47 preambule GDPR a může vést k právní nejistotě[136]. Unifikovaný přístup je základním kritériem efektivní aplikace nařízení. EK tento stav sice uznala, ale detailněji se mu nevěnovala. Fragmentace v oblasti zvláštních kategorií OÚ také nebyla předmětem hodnocení. Bylo upozorněno na propastné rozdíly mezi zázemím poskytnutým jednotlivým DPA, což znemožňuje jejich činnost v rovných podmínkách.

Mezi hlavní zjištění EK patří přetrvávání fragmentace GDPR implementace mezi ČS, což ztěžuje přeshraniční byznys a inovace. Dále považuji za relevantní upozornit na zaměření EK na předávání OÚ do třetích zemí (viz výše) a aspekt technologického vývoje (viz AR a níže), kde se zavázala k monitorování aplikace GDPR v kontextu nových technologií, jelikož souhlasí s důležitostí těchto výzev a podporuje konzistentní aplikaci GDPR rámce. EDPB je proto podporován ve vydávání pokynů k technologickému vývoji (včetně UI a blockchainu) a revizi existujících pokynů. Jak je zmíněno výše, zdá se, že EDPB se s tím ztotožňuje. To pojistný sektor vítá, jelikož přesnější klarifikace je přínosná pro právní jistotu pojistitelů i subjektů OÚ.

Mám-li být kritická, po publikaci *Zprávy* však nebylo těžké všimnout si její nicneříkající povahy. EK se mnohým oblastem věnovala okrajově, nebo dokonce vůbec. Pozitivní ale je, že nedošlo k otevření GDPR a byla potvrzena předčasnost tohoto postupu. Zároveň však byla vymezena tato možnost do budoucna (např. v oblastech sjednocení věku nezletilého u udělování souhlasu).

Následně došlo k přijetí usnesení k implementaci GDPR[137], kterým EP navázal na zjištění *Zprávy*. Další fáze, snad obsahově praktičtějšího hodnocení ze strany EK, nastane v roce 2024.

[136] Autoriteit Persoonsgegevens. *Normuitleg grondslag 'gerechtvaardigd belang'* [online]. 1. 11. 2019 [cit. 20. 2. 2022]. Dostupné z: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf.

[137] Hodnotící zpráva EK o provádění obecného nařízení a o ochraně osobních údajů dva roky od začátku jeho uplatňování. Usnesení EP ze dne 25. 3. 2021, o hodnotící zprávě EK, o provádění obecného nařízení, o ochraně osobních údajů dva roky od začátku jeho uplatňování (2020/2717(RSP)) [online]. In: *Úřední věstník* [online], C 494/11, 25. 3. 2021 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52021IP0111&from=EN.

7 Inovace v mezích regulace

7.1 Insurtech

Provázanost GDPR a nových technologií transformujících pojišťovnictví, insurtech, považuji za vysoce aktuální téma jak na základě vlastní praxe v českém i bruselském prostředí, tak na základě avizovaných kroků evropských orgánů, včetně EDPB, EIOPA či ENISA. I proto je v této práci tato problematika, možná i výzva, průběžně zmiňována.

Rapidní faktický vývoj společně s prioritizaci agend digitalizace a KB pod heslem „Fit for digital decade“ ze strany evropských institucí se odráží ve značném množství legislativních iniciativ.

EK již na počátku svého mandátu vydala v rámci ambiciózní strategie *Shaping Europe's Digital Future*[138], ESD, DFS, *Bílou knihu k umělé inteligenci*, *Strategii kybernetické bezpečnosti EU pro digitální dekádu* a další. Na tyto strategie navazují početné legislativní návrhy EK, např. ePrivacy, NIS2, DORA, AIA, návrhy pro reciproční sdílení dat atd.

Významnou roli sehrává také EDPB. Z *Pracovního programu EDPB 2021–2022,* navazujícího na dříve publikovanou strategii[139], lze vyčíst orientaci na nové technologie, což bylo ostatně naznačeno již ve *Zprávě*. Zde je proklamována nutnost vyhodnocení GDPR v kontextu technologických inovací, nevyjímaje insurtech a vymezení potenciálně kritických ustanovení.

Tento nový multilevelový rámec, jenž může výrazně změnit poskytování nejen finančních služeb, je pro pojistný trh vysoce aktuální. Ve hře je jak konkurenceschopnost EU jako celku, tak jednotlivých odvětví, ve vztahu k ostatním globálním hráčům – ve smyslu států, především Číny a USA, i ve smyslu technologických gigantů, *gatekeepers*, u kterých se očekává byznysový přesah do dosud neřešených oborů. Konkrétní dopady pro rozvoj v oblasti pojišťovnictví rozebírám níže, a to i v návaznosti na inciativy evropských orgánů v dosud neupravených rovinách i na potřeby modernizace legislativního rámce odpovědnosti za škodu.

[138] European Commission. Shaping Europe's Digital Future. In: *Ec.europa.eu* [online]. 19. 2. 2020 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en.
[139] EDPB. *EDPB Strategy 2021–2023* [online]. EDPB, 15. 12. 2020 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/work-program/edpb-strategy-2021-2023_en.

Mým základním předpokladem je stanovisko, že je nezbytné používat GDPR tak, aby nařízení tvořilo spíše standard aplikace i pro nové technologie, ale nebylo bariérou pro jejich další rozvoj a implementaci. GDPR je nezbytnou normou, ze které je vhodné vycházet při zavádění inovací, jelikož zde upravené zásady, povinnosti a práva subjektů údajů tvoří mantinely pro jejich proporcionální využití. Aplikace nových technologií tak může výrazně pozitivně ovlivnit fungování pojišťoven a zároveň poskytování kvalitnějších služeb spotřebitelům i v postavení subjektů OÚ.

S právní nejistotou se dnes evropské trhy potýkají např. u GDPR principu minimalizace dat, přičemž požadavky na efektivní fungování UI jsou opačné – k vývoji algoritmu je potřeba velké množství dat. To má také význam u prevence podjatosti či diskriminace. K této věci expertní skupina EK k regulatorním překážkám ve finančních inovacích navrhuje vydat speciální pokyny pro aplikaci GDPR ve vztahu k novým technologiím ve finančních službách. Dalším příkladem je GDPR úprava AR, viz výše.

V kontextu GDPR je posouzení hodná i kompatibilita s blockchainem, distribuovanou databází, v níž jsou navždy uloženy veškeré záznamy, které jsme do ní vložili, *per analogiam* nekonečná kniha účetních záznamů. Ani jeden z těchto popisů však zdaleka nevystihuje, proč je blockchain tak jedinečný. Vlastně ani není tak úplně novou, revoluční technologií. Revoluční je především způsob, jakým blockchain přistupuje k využití technologií.[140] Obecně je potenciál pro pojišťovnictví spatřován v umožnění růstu, zvyšování efektivnosti a snižování nákladů prostřednictvím automatizace klíčových procesů.[141] Konkrétně se může jednat o PPP, automatizaci underwritingu, zvyšování transparentnosti či rozvoj chytrých smluv.

Základní potenciální nesoulad s GDPR však plyne přímo z permanentní povahy blockchainu ve vztahu k výkonu práva být zapomenut nebo práva na výmaz. To bude nezbytné interpretovat tak, aby se nejednalo o regulatorní překážku blokující další vývoj.

---

[140] WOLF, Karel. Proč svět touží po blockchainu? In: *Marwick.cz* [online]. 1. 10. 2018 [cit. 16. 2. 2022]. Dostupné z: https://www.marwick.cz/tema/svet-na-blockchainu.

[141] *Blockchain in insurance – opportunity or threat?* [online]. New York: © McKinsey&Company, July 2016 [cit. 20. 2. 2022]. Dostupné z: https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/blockchain%20in%20insurance%20opportunity%20or%20threat/blockchain-in-insurance-opportunity-or-threat.ashx.
BRAUN, Alexander a SCHREIBER, Florian. *The Current InsurTech Landscape: business models and disruptive potential* [online]. St. Gallen: Institute of Insurance Economics I.VW-HSG, University of St. Gallen, 2017 [cit. 20. 2. 2022]. ISBN 978-3-7297-2009-1. Dostupné z: https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/abinsurtech_2017.pdf.

Dalším příkladem je *cloud computing*, který zase zachovává konzistenci a spolehlivost zdrojů, centralizuje data, redukuje náklady a tím zlepšuje operační efektivitu. Jak bylo vykresleno výše, vzhledem k jeho globální povaze je vhodné brát v potaz úpravu GDPR regulovaných vztahů ke třetím zemím a v neposlední řadě i faktor KB, což by měla regulovat DORA.

Finanční sektor tedy prochází turbulentním vývojem, na který reagují jak etablovaní tržní hráči, tak nové subjekty. Tyto aspekty povedou k vůbec první nebo důkladnější úpravě některých institutů; uvedené příklady nejsou uzavřeným výčtem všech aktuálních insurtechů. I zde totiž platí, že mezi technologickým a legislativním vývojem se jedná o závod zajíce a želvy, na což upozorňuje třeba i Harari[142].

Navzdory určité rigiditě, která v pojistném sektoru panuje v důsledku detailních legislativních a regulatorních požadavků, dochází v posledních letech k postupné modernizaci, digitalizaci a zavádění technologicky inovativních postupů a řešení, což má nepochybně i tržní důvody.

Nelehkým úkolem je tak zakotvení proporcionálního principu *de lege ferenda*. Kromě eventuálně sporných příkladů na následujících stránkách detailněji zkoumám institut nesoucí potenciál pro pojišťovnictví, UI, a to včetně IoT a big dat.

7.2 UI, IoT a GDPR

7.2.1 Aplikace v pojišťovnictví

Perspektivou pojišťovnictví je znatelná transformační kapacita UI, popř. strojového učení. UI je sofistikovaným, konektivním, autonomním systémem založeným na algoritmech, které závisejí na datech. Obrovskou byznysovou kapacitu služeb aplikujících UI lze dedukovat z odhadů, podle kterých od roku 2016 do roku 2025 dojde k 56násobnému nárůstu, z 644 mil. USD na 35 mld. USD[143]. Potenciál je vázán na existenci a analýzu velkých množství dat splňujících kvalitativní a kvantitativní předpoklady.

V této oblasti dochází k enormně rychlému vývoji, kdy podle Světového ekonomického fóra UI pojišťovnám umožní predikovat a reagovat na rizika s lepší přesností, PPP či

[142] HARARI, Yuval N. *Homo deus: stručné dějiny zítřka*. Praha: Leda, 2017, s. 374. ISBN 978-80-7335-502-9.

1 [143] FELDMAN, Michael. Market for Artificial Intelligence Projected to Hit $36 Billion by 2025. In: *Top500.org* [online]. 29. 8. 2016 [20. 2. 2022]. Dostupné z: https://www.top500.org/news/market-for-artificial-intelligence-projected-to-hit-36-billion-by-2025/.

přizpůsobovat produkty[144]. Samostatnou rovinou je právě vývoj nových pojistných produktů (např. v oblasti přírodních katastrof, pandemických rizik, ztráty dat či KB), ale i personalizace produktů a cen (např. ŽP nebo pojištění vozidel), komunikace se spotřebiteli (např. chatbot, voicebot, virtuální asistenti), zpracování žádostí, vyhodnocování spokojenosti, vyřizování pojistných událostí, underwriting či prediktivní analýzy. Nové techniky a přístup k většímu množství dat tak umožňují nejen důkladnější personalizaci nabízeného produktu, ale také přesnější vyhodnocení rizik či pojištění dosud nepojistitelných rizik z důvodu nedostatku podkladových údajů.

Pojišťovnictví však nese datacentrickou povahu již mnohem déle, než je znám fenomén big dat. Z hlediska podkladových dat v pojišťovnictví neplatilo ani v minulosti, že méně je někdy více. Více je prostě více. Big data by se dala popsat jako vysoce objemná, rychlá a různorodá informační aktiva, která vyžadují nákladově efektivní, inovativní formy zpracování informací pro posílení dovedností a rozhodování[145]. Big data jsou svým charakterem v podstatě syrové údaje, ale při vhodných, stále více sofistikovaných technikách *data miningu* mohou přinést hodnotné informace. Pro úplnost je potřeba dodat, že velké množství big dat využívaných v pojišťovnictví nese anonymizovanou podobu.

Tyto nové modely však dle mého názoru pouze modernizují a recyklují tradiční vzorce pojišťovnictví. Následně tato optimalizace přináší výhody pro samotné pojišťovny i spotřebitele v postavení subjektů OÚ, protože se jedná o nutný požadavek pro analýzu rizik, hodnocení minulých událostí a predikci jejich výskytu v budoucnu. Takto to vnímá i EIOPA ve *Zprávě k umělé inteligenci*[146] a OECD ve *Zprávě k dopadům umělé inteligence a big dat na pojišťovnictví*[147], kde se uvádí, že granularita dat může vést i k prohloubení klasifikace rizik, kdy se pojistné stanoví na základě skupiny osob, které mají podobné rizikové profily. Podrobnější soubory dat umožňují zpřesnit klasifikaci rizik, což by mohlo vést ke snížení

[144] *The New Physics of Financial Services: understanding how artificial intelligence is transforming the financial ecosystem* [online]. World Economic Forum, August 2018 [cit. 20. 2. 2022]. Dostupné z: http://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf.
[145] IE. *Q&A on the use of big data in insurance* [online]. Brussels: © IE aisbl, January 2019 [cit. 21. 2. 2022]. Dostupné z: https://www.insuranceeurope.eu/publications/504/qas-on-the-use-of-big-data-in-insurance/download/QAs+on%20the%20use%20of%20big%20data%20in%20insurance.pdf.
[146] EIOPA, 2021. *Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector. A report from EIOPA's Consultative Expert Group on Digital Ethics in insurance* [online]. Luxembourg: Publications Office of the European union, 2021 [cit. 21. 2. 2022]. ISBN 978-92-9473-303-0. Dostupné z: https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa-ai-governance-principles-june-2021.pdf.
[147] OECD. *The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector* [online]. © OECD 2020, 28. 1. 2020 [cit. 21. 2. 2022]. Dostupné z: https://www.oecd.org/finance/Impact-Big-Data-AI-in-the-Insurance-Sector.htm.

pojistného pro některé spotřebitele na jedné straně, ale upozorňuje se na možné negativní konsekvence, jako např. na exkluzi nabídky pojištění pro jiné spotřebitele.

Proto jedná-li se o OÚ, je samozřejmě nutné rozlišovat míru rizikovosti jednotlivých aplikací a také související odpovědnosti za škodu. Nastíním kategorizaci typických aplikací UI v pojišťovnictví dle míry GDPR rizikovosti. Mezi nízce rizikové aplikace se řadí: UI vytvořená k efektivnímu plnění jednoduchého úkolu, např. automatizace interních procesů či konverzační a asistenční UI poskytující informace; dále i automatické vyřizování žádostí, např. u pojištění motorových vozidel dle zaslaných fotografií, což přináší časovou úsporu a zvyšuje komfort klienta; taktéž PPP, kde by se mohlo jednat o jeden z nástrojů snížení enormní částky 13 mld. EUR v EU[148] prostřednictvím analýz dat z různých zdrojů k detekci podvodných znaků. Specifický potenciál vidím také v analýze názorů a postojů klientů, kdy u telefonického hovoru UI přepisuje dialog do textové podoby a dle obsahu vyhodnotí spokojenost klienta, který obdrží kopii. Tím zároveň dojde k méně pracnému naplnění požadavků IDD. Pro případné etické otázky vidím jako řešení právo na lidské posouzení, a to nejen u UI orientované na klienta, ale také u PPP.

Do kategorie nesoucí vyšší rizikový potenciál patří underwriting a výpočet pojistného. Údaje poskytnuté v souhlasovém režimu mohou být podkladem pro přesnější výpočty (např. u ŽP, pojištění motorových vozidel), což může vyústit v kvalitnější obecnou predikci a následně celkové snížení pojistného (např. u povodní). To analyzuji u IoT. Mezi rizikovější aplikace náleží i behaviorálně prediktivní analýzy, kdy samoučící se UI hodnotí chování klienta, předvídá jeho vývoj a dle toho nabízí služby individuální a personalizované povahy (např. u narození dítěte, rozvoje nemoci).

Právě zde existuje potenciální riziko rozevírání nůžek v přístupu k finančním službám – reverzní selekce neboli výše zmíněné exkluze, kdy někteří zájemci z objektivních příčin na službu pojištění nedosáhnou. To sice není požadovaným stavem, ale nepovažuji za pobuřující tvrdit, že pojišťovnictví není charita. Jedná se o odvětví finančních služeb, které reaguje na tržní a společenský vývoj. Navzdory tomu, že funguje na principu solidarity, není prakticky možné vykládat to nesmyslně extenzivně, jelikož pojišťovna je povinna dodržovat i solventností kapitálové požadavky dle SII a další povinnosti.

[148] IE. *Insurance fraud: not a victimless crime* [online]. Brussels: © IE aisbl, November 2019 [cit. 20. 2. 2022]. Dostupné z: https://www.insuranceeurope.eu/mediaitem/2bf88e16-0fe2-4476-8512-7492f5007f3c/Insurance%20fraud%20-%20not%20a%20victimless%20crime.pdf.

Specifickou kategorií UI je IoT. Definice pojmu není sjednocena, avšak EK IoT vymezuje jako „rozsáhlý ekosystém fyzických objektů připojených k internetu, které jsou schopny samy sebe identifikovat a sdělovat data ostatním objektům pomocí komunikační sítě pro digitální zpracování“[149]. U IoT tak pro pojišťovnictví plynou výhody obdobné jako u telematiky, a to z hlediska dostupnosti údajů v reálném čase. Dalším příkladem jsou *wearables* apod. Data z těchto zařízení mohou být základem pro hodnocení rizikovosti daného klienta a mohou ovlivnit následně stanovenou výši pojistného. Z toho samozřejmě plynou individuální underwritingové výhody pro nízkorizikové klienty, např. sportující u ŽP, pojištění domácnosti nebo stabilní řidiče u pojištění motorových vozidel; za aplikace big dat analýz pak i v obecné rovině u tvorby, poradenství a distribuce produktů dle (v reakci na technologický rozvoj v budoucnu revidované) IDD.

V neposlední řadě sdílení takových dat a predikce ze strany pojistného sektoru mohou být excelentním podkladem např. pro medicínu či posílení prevence a bezpečnosti na silnicích. Nicméně v obecné rovině existuje riziko identifikace, monitorování chování, lokace, ovlivňování rozhodování jednotlivce a dnes už ne až tak absurdní představy „bodování“ podle dystopického „vzoru“ čínského sociálního kreditového systému. Smejkal to vnímá jako další módní fenomén dneška, jehož prognózy jsou úžasné, leč rizika rovněž.[150] Upozorňuje především na riziko zneužití, kdy na příkladu inteligentní budovy uvádí, že ta může být naším hlídačem, ale i věznitelem a udavačem. Obdobné příklady jsou již známé z nedaleké minulosti, např. Google „spy-fi“ skandál týkající se extrakce nezašifrovaných údajů z domácností ze strany Google *street* aut byl odhalen německou Federální komisí pro ochranu dat. To vyústilo v opt-out z této služby ze strany téměř 250 000 německých domácností a pokuty pro Google.[151] Zde se rovněž vybaví analogie ke známému dílu Orwella *1984* či opomíjenému dílu Burgesse *1985*. Ztotožňuji se s komentářem Smejkala[152]. Podle něho čím více věcí bude připojeno (stane se součástí kyberprostoru), s tím větším rizikem zneužití se musí počítat. Oblast ochrany OÚ tak čekají nelehké výzvy sloučené i s vývojem tohoto technologického výdobytku a prevencí nežádoucích důsledků.

[149] European Commission. *Commission staff working document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy* [online]. Brussels: 10. 1. 2017 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0002.
[150] SMEJKAL, 2018, op. cit., s. 860.
[151] ZUBOFF, 2019, op. cit., s. 143–148.
[152] SMEJKAL, 2018, op. cit., s. 897.

7.2.2 Legislativní vývoj

7.2.2.1 AIA

První krok k regulaci je známý z Kalifornie, USA, kde v roce 2018 došlo k přijetí zákona upravujícího IoT[153], jenž je účinný od roku 2020 a zavádí povinnost výrobce vybavit připojené zařízení zákonně stanovenými bezpečnostními prvky. Jedná se o první úpravu této oblasti na světě, která může být inspirací snaze o horizontální legislativní úpravu UI v EU. EK zdůrazňuje, že dosáhne dalšího „bruselského efektu" *per analogiam* GDPR, čímž by vytvoření prvního regulačního rámce UI na světě skutečně mohlo získat výhodu prvního tahu při stanovování mezinárodních standardů v oblasti UI založených na evropských hodnotách, jakož i úspěšně vyvážet „důvěryhodnou UI" do celého světa.

U legislativního podchycení těchto složitých fenoménů je důležité zohlednění toho, že prvotním krokem k řádnému praktickému fungování UI je dostatečný datový vzorek, přičemž pro analýzu dat je nezbytná jednotná metodologie sběru. Z hlediska právní jistoty je pak nezbytností jasný rámec vycházející z principů proporcionality, rizikové založenosti, transparentnosti a vysvětlitelnosti složitého řetězce UI, možnosti lidského zásahu a prevence diskriminace, zajištění KB atd., v souladu s právně nezávaznými, ale definujícími principově založenými *Etickými pokyny pro zajištění důvěryhodnosti umělé inteligence*, na které navazuje *Bílá kniha k umělé inteligenci*, a robotickými Asimovovými dogmaty či doporučením OECD[154]. Zároveň je potřeba vycházet také ze zásad zakotvených v čl. 5 GDPR, které by se měly odrazit v aplikovaných TOO dle čl. 25 GDPR. K obdobnému závěru nezbytnosti kompatibility UI a GDPR dospěly také německé dohledové orgány pro oblast ochrany OÚ[155].

K datu vyhotovení této práce byl již publikován horizontální návrh AIA EK. Jeho základem je rozdělení typů aplikací UI dle rizikovosti, a to z pohledu základních práv a svobod, včetně ochrany OÚ. Ve verzi Rady je nešťastným řazení pojišťovnictví, konkrétně underwritingu a vyřizování pohledávek, mezi vysoce rizikové aplikace. Důvody nevhodnosti tohoto přístupu

[153] STATE OF CALIFORNIA. *Senate Bill No. 327/886, An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy* [online]. 28. 9. 2018 [cit. 22. 2. 2022]. Dostupné z: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.
[154] OECD. *Recommendation of the Council on Artificial Intelligence* [online]. Paris: OECD Legal Instruments, 22. 5. 2019 [cit. 20. 2. 2022]. Dostupné z: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
[155] *Report on Experience Gained in the Implementation of the GDPR* [online]. Independent German Federal and State Data Protection Supervisory Authorities, November 2019 [cit. 20. 2. 2022]. Dostupné z: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/Evaluation-Report-German-DPAs-Clean.pdf.

jsem uvedla výše. Je potřeba je chápat i v kontextu prevenčního mechanismu, jímž je právo na lidský zásah, a sofistikace, nikoli změny modelů posuzování rizik aplikovaných v pojišťovnictví, či v rozdílech mezi diskriminací a diferenciací analyzovaných níže. Jelikož trialogy se nacházejí v úvodní fázi, je dnes nemožné odhadovat finální znění. Evropské orgány tak čeká komplexní úkol vymezení vůbec první evropské legislativní úpravy UI, a to za zohlednění praktické aplikace a složité predikce budoucího technologického vývoje i stávajících pravidel.

Na následujících řádcích se proto věnuji výzvám a možným řešením chystané legislativní úpravy v kontextu pojišťovnictví. Budu vycházet jak z AIA, revidované PLD, GDPR, DORA, sektorově specifické legislativy, *Zprávy k bezpečnosti a odpovědnosti umělé inteligence, IoT a robotiky* EK[156] a taktéž z návrhu zprávy o UI zveřejněné AIDA[157]. Tento návrh zprávy klade velký důraz na posílení evropského odvětví UI a zdůrazňuje, že naprostá většina případů využití UI je málo riziková a nevyžaduje legislativní záruky. Takový přístup by právě u výčtu z pojišťovnictví uvedeného výše umožnil další inovace. Kromě jiného se věnuje i přesahům na GDPR. Překvapivě kriticky zdůrazňuje, že GDPR a rozdílné výklady v jednotlivých ČS vedly k právní nejistotě a nedostatečné spolupráci v odvětví zdravotnictví. V této věci vidím i přesah na vágní *Zprávu* EK i chystanou iniciativu Evropského prostoru pro zdravotní údaje, jelikož AIDA uvádí, že specifický souhlasový režim s poskytováním informací brání zpracování zdravotních údajů pro další analýzy a studie, což vede ke zpoždění vědeckých objevů a zpracování dat a vytváří byrokratickou zátěž ve zdravotnickém výzkumu. Dále AIDA u regulace UI deklaruje, že ústředním prvkem regulačního přístupu EU je emfáze na etiku v souladu se základními hodnotami lidských práv a demokratickými zásadami.

Z perspektivy GDPR je relevantní kompatibilita aplikace UI. Nadto je nutné brát ohled i na kontradikci GDPR proklamované minimalizace dat a požadavky na kvalitu i kvantitu dat pro efektivní fungování algoritmů v rámci UI. Nedostatky spatřuji i v kontextu nízké využitelnosti anonymizovaných údajů pro účely UI dle dikce čl. 9 GDPR. Výše zmíněné příklady aplikace UI v pojistném sektoru je dle mého názoru nutné vnímat nejen optikou nové, specifické regulace, ale již i optikou principu *de lege lata*. Nejedná se pouze o GDPR, ale i SII, PRIIPs či IDD. Tyto základní předpisy detailně regulují transparentnost a zveřejňování či tvorbu

[156] EK. *Zpráva Komise Evropskému parlamentu, Radě a Evropskému hospodářskému a sociálnímu výboru. Zpráva o dopadech umělé inteligence, internetu věcí a robotiky na bezpečnost a odpovědnost* [online]. V Bruselu: 19. 2. 2020 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020DC0064&from=en.

[157] EP. *Návrh zprávy o umělé inteligenci v digitálním věku (2020/2266(INI))* [online]. Štrasburk: 2. 11. 2021 [cit. 20. 2. 2022]. Dostupné z: https://www.europarl.europa.eu/doceo/document/AIDA-PR-680928_CS.pdf.

produktů, a to bez ohledu na použité technologické řešení. Konkrétně je to vidět na poradenství, primárně upravené IDD, z hlediska ochrany OÚ GDPR. IDD vymezuje striktní požadavky, které musí být dodrženy, a to bez ohledu na to, zda je poradenství poskytováno člověkem, nebo UI. To opětovně potvrzuje tezi o pouhé sofistikaci, nikoli zavádění neznámých institutů.

Detailněji vymezím nebezpečí negativních konsekvencí na konkrétní subjekt OÚ na příkladu AR u underwritingu. Důležitost práva na lidský zásah je nutné chápat v dle mého názoru sice malé, ale existující chybovosti algoritmů. Jak píše Harari: *Počítačové algoritmy za sebou nemají dějiny přirozeného výběru a nevládnou emocemi ani pudy, proto se v krizové situaci řídí zakódovanou etikou mnohem důsledněji než lidé. Stačí morální předpisy Kanta, Milla a Rawlse vyjádřit čísly.*[158] Návod však v praxi nemusí být tak lehce aplikovatelný a nedostupnost práva na lidský zásah by mohla vést k diskriminaci a prohlubovat nerovnost i v dostupnosti finančních služeb.

Nebezpečí exkluze ale nevychází z aplikace UI jako takové. Složité pojistně matematické metody by právě naopak byly zdokonaleny větším a kvalitnějším objemem dat, který by v konečném důsledku vedl spíše ke spravedlivějšímu hodnocení rizik a nabízení produktů s personalizovanou a individualizovanou vložkou. Dle mých zkušeností je v pojistném kontextu nezbytné odlišit diskriminaci a diferenciaci, což má smysl pro pochopení fungování pojišťovnictví obecně i konkrétně třeba u AR a následně využitého práva na lidský zásah, kdy realizace vysvětlení vůči průměrnému spotřebiteli může být vzhledem k složitosti algoritmů náročným úkolem v rovině obsahové i volby jazykových prostředků, a to v mezích obchodního tajemství či duševního vlastnictví. O diskriminaci *stricto sensu*, charakterizovanou v úvodu této práce, se nejedná, jsou-li rozdílné služby (např. rozsah krytí nebo cena) poskytovány na základě objektivně rozdílných rizikových faktorů.

Nesprávný postup zvýhodňující určité klienty by se negativně odrazil na celkově poskytovaných službách i solventnostních požadavcích. To ostatně zmiňuje i již uvedené stanovisko ČSpA: *Pokud budou málo a vysoce rizikoví jedinci v jedné skupině se stejným pojistným, stanoveným podle průměrného rizika ve skupině, jedinci s nízkým rizikem budou platit vyšší pojistné, než by odpovídalo jejich riziku. Kvůli vysoké ceně mohou následně tito málo rizikoví jedinci odejít ze skupiny. Průměrné riziko skupiny se zvýší a může nepříznivě ovlivnit výsledky pojistitele.*

[158] HARARI, 2019, op. cit., s. 77.

De lege ferenda regulace pojišťovnictví musí překonat paradigma tradičního pojistitele, který je jediným designérem hotového hromadného produktu, a uvědomit si, že klienti budou pořád více vyzýváni k aktivní roli u produktů na míru, a to za pomoci technologicky založených nástrojů[159].

7.2.2.2 Odpovědnost

Dále ze strany pojistného sektoru a spotřebitelů považuji za nutné nastavení odpovědnostního režimu. Podle informací dostupných v době tvorby této práce jsou ve hře dvě varianty úpravy odpovědnosti u UI na evropské úrovni, a to v rámci samostatného nového předpisu, nebo revidované PLD, k čemuž se pojistné odvětví přiklání.

Revize PLD navazuje na hodnocení, z kterého vyplynula terminologická i obsahová zastaralost směrnice, např. v kontextu insurtechu už *de facto* není určujícím bodem pro hodnocení odpovědnosti uvedení výrobku do oběhu. Taxonomická nejednotnost může vést k budoucí právní nejistotě a limitaci vývoje. Nejednotným vnímáním terminologie se zaobírá i Smejkal[160], který popisuje absenci právních definic relevantních pojmů. Odkazuje na *Občanskoprávní pravidla pro robotiku*[161], kterými EP vyzval EK k navržení jednotných definic, což se snad povede právě v AIA.

Modernizace PLD by dle mého názoru stačila k dosažení kýženého cíle v rámci odpovědnosti UI, jelikož principy PLD v kombinaci s národním principem *de lege lata* jsou vyváženým systémem tím, že poskytují vysokou úroveň ochrany poškozeným osobám a zároveň zohledňují oprávněné zájmy výrobců. V této věci je však třeba přizpůsobení odpovědnosti za škodu způsobenou vadou výrobku i odškodnění v digitálním světě. Cílem EK je modernizovat pravidla odpovědnosti tak, aby zohledňovala vlastnosti a rizika insurtechu, komplexních digitálních a obchodních modelů, včetně produktů a služeb vybavených UI.

Škoda je dnes vnímána nejen hmotně, ale i z pohledu ochrany soukromí a OÚ. Polčák v kontextu „virtualizace prakticky všeho“ upozorňuje na rovnocennost fyzického a virtuálního majetku, mají-li reálnou hodnotu. Stejně tak neexistuje rozdíl mezi fyzickou a virtuální

[159] REGO, Madriga L. a CARVAHLO, Joana C. Insurance in Today's Sharing Economy: New Challenges Ahead or a Return to the Origins of Insurance? In: MARANO, Pierpaolo a NOUSSIA, Kyriaki. *InsurTech: a legal and regulatory view*. První vydání. Cham: Springer, 2020, s. 46. AIDA Europe Research Series on Insurance Law and Regulation. ISBN 978-3-030-27385-9.
[160] SMEJKAL, 2018, op. cit., s. 88.
[161] Usnesení EP ze dne 16. února 2017 obsahující doporučení EK o občanskoprávních pravidlech pro robotiku (2015/2103[INL]). In: *Úřední věstník* [online], C252/239, 18. 7. 2018, s. 239–257 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52017IP0051.

škodou, došlo-li ke skutečné škodě, v národním režimu dle § 2952 OZ.[162] O odpovědnostním režimu pojednává von Westphalen[163]. U PLD se jedná o zákonnou objektivní odpovědnost, zavinění je tedy irelevantní. Co je zde však předmětem diskuzí, je, jak vymezit příčinnou souvislost, vadu a v první řadě výrobek. Od toho se pak odvine hodnocení škody. Zdá se ale být složité vymezit odpovědný subjekt, alokovat odpovědnost v rámci řetězce dodavatelů vůči koncovému uživateli. Na to odkazuje i Smejkal, který uvádí, že se stále vzrůstající složitostí IS a ICT se dostáváme do situace, kdy je velmi obtížné diagnostikovat, co a proč se v určitém IS odehrálo, a tedy i stanovit odpovědnost za případný incident[164]. To je zapříčiněno hlavně dvěma faktory:

Zaprvé spletitostí dodavatelského řetězce. Hardware, software a služby tvoří technologické ekosystémy, což je ještě komplexnější u IoT, kde dochází k interakcím mnoha propojených zařízení, služeb a subjektů (designér, programátor, výrobce, poskytovatel, poskytovatel připojení, poskytovatel finální služby atd.). Zároveň se jedná o vyvíjející se systémy, takže modernizace může zamíchat kartami k posuzování původní a aktualizované verze. Von Westphalen zde odkazuje na judikaturu německého Spolkového nejvyššího soudu, kde bylo konstatováno, že spotřebitel – i v roli poškozeného – nemůže očekávat žádnou absolutní bezpečnost. Požadavky na výrobce u bezpečnosti by měly vycházet z přiměřenosti a v případě nepředvídatelné vady je aplikována povinnost odvrácení nebezpečí či sledování výrobku.[165]

Další rovinou, kterou u složitosti dodavatelského řetězce není vhodné podcenit, jsou kompetence vhodných dohledových orgánů, jelikož samotný poskytovatel ICT ani finanční instituce spíše nebudou tím samým subjektem. Vzhledem k povaze ICT se navíc častokrát jedná o globálně poskytované služby; decentralizovaná regulace zde může být komplikací pro právní jistotu. Dohledové orgány tak čelí výzvě přizpůsobení se novým tržním podmínkám, přičemž je od nich vyžadováno, aby svoje pravomoci využívaly za aplikace balančního přístupu mezi ochranou finanční stability a spotřebitelů a podporou inovací a volné soutěže.[166]

[162] POLČÁK, Radim. Protiprávní jednání a škoda on-line. In: *XXVIII. Karlovarské právnické dny*. Praha: Leges, 2021, s. 518–519. ISBN 978-80-7502-462-6.
[163] GRAF VON WESTPHALEN, Friedrich. Náhrada škody ve virtuálním světě s důrazem na umělou inteligenci. In: *XXVIII. Karlovarské právnické dny*. Praha: Leges, 2021, s. 427. ISBN 978-80-7502-462-6.
[164] SMEJKAL, 2020, op. cit.
[165] GRAF VON WESTPHALEN, Friedrich. Náhrada škody ve virtuálním světě s důrazem na umělou inteligenci. In: ZOUFALÝ, Vladimír, ed. *XXVIII. Karlovarské právnické dny*. Praha: Leges, 2021, s. 431. ISBN 978-80--7502-462-6.
[166] CHATZARA, Viktoria. FinTech, InsurTech, and the Regulators. In: MARANO, Pierpaolo a NOUSSIA, Kyriaki. *InsurTech: a legal and regulatory view*. První vydání. Cham: Springer, 2020, s. 21–22. AIDA Europe Research Series on Insurance Law and Regulation. ISBN 978-3-030-27385-9.

Zadruhé již načrtnutou složitostí algoritmů. To naráží nejen na limitovanou vysvětlitelnost, ale i na možnou neprůhlednost. To nemusí být závislé pouze na primárně vložených datech (když vycházím z předpokladu, že se jedná o data, u kterých nehrozí riziko diskriminačního posouzení), ale jak hodnotí i EK ve *Zprávě k bezpečnosti a odpovědnosti umělé inteligence, IoT a robotiky*, na základě efektu samostatného učení UI se může stát, že stroj učiní rozhodnutí odlišné od původně zamýšleného výrobcem nebo očekávaného uživatelem. Von Westphalen také upozorňuje na nutnost chybové marže a kauzality škody samoučící UI vycházející z inherentního probabilistického chování. To vede k důsledku, že *ex ante* je omezena předvídatelnost UI a *ex post* je omezena vysvětlitelnost. Což nás opětovně dostává k důkaznímu břemenu. To je na straně subjektu OÚ dle mého názoru v praxi velmi těžce realizovatelné, a to jak z hlediska samotného pochopení fungování algoritmu, tak z hlediska ochrany obchodního tajemství apod. Jako průchodnější variantu vnímám kauzální odpovědnost za chybné chování UI, které vede ke vzniku škody.

Problematika odpovědnosti je ze zřetele pojišťovnictví relevantní i v další rovině. Dle mých informací je evropským zákonodárcem zvažována i varianta povinného pojištění vysoce rizikových aplikací UI. Zde ale není zohledněna realita. Systémy přísné odpovědnosti fungují pouze tehdy, když jsou rizika, která mají být kryta, dostatečně podobná a když jsou splněny specifické tržní předpoklady. To není případ insurtechu, který zahrnuje velmi širokou škálu různých zařízení a použití. Navíc chybí historická nebo analogicky použitelná data. Bez splnění těchto podmínek by zavedení povinného pojištění odpovědnosti za škodu způsobenou vadou výrobku mohlo způsobit více škody než užitku, s následkem nedostatku upisovací a smluvní svobody či potlačení inovací pojistných produktů. Dále by mohlo mít nepříznivý vliv na pronikání na trh, pokud by pojistný trh nebyl schopen poskytnout dostatečné krytí, a také negativně ovlivnit výši pojistného a prevenci, protože pojistníci by mohli mít pocit, že břemeno je na pojistiteli. Můj názor v této intervenci shodně kritizuje i Bugra.[167]

Povahou UI daná konektivita, autonomie a otevřenost mohou vést k vyššímu riziku ohrožení základních práv, práv subjektů OÚ i KB. Při formulování horizontálního, nikoli sektorově specifického rámce AIA a vymezení odpovědnostního režimu je tak potřeba vzít v potaz řadu faktických aspektů a zajistit, aby již *prima facie* byla AIA nadstavbou kompatibilní *de lege lata*. Pro oblast pojišťovnictví se jedná o sektorové předpisy, ale i GDPR či DORA.

[167] BUGRA, Aysegul. Room for Compulsory Product Liability Insurance in the European Union for Smart Robots? Reflections on the compelling challenges. In: MARANO, Pierpaolo a NOUSSIA, Kyriaki. *InsurTech: a legal and regulatory view*. První vydání. Cham: Springer, 2020, s. 193. AIDA Europe Research Series on Insurance Law and Regulation. ISBN 978-3-030-27385-9.

Z výše nastíněných dokumentů dedukuji odůvodněnou obavu z rizik spojených s UI. Jako ultimátní instanci prevence potenciálních nedostatků proto ze zkušeností s GDPR vnímám v praxi umožněné právo na lidskou intervenci. To považuji za řešení případné chybovosti UI, která může být zapříčiněna nevhodným algoritmem nebo autonomním procesem. Zde si dovolím analogii k Čapkovi, který to vyjádřil sice nikoli technicky či právně, ale navzdory tomu výstižně: *Roboti nejsou lidé. Jsou mechanicky dokonalejší než my, mají úžasnou rozumovou inteligenci, ale nemají duši.*[168] A bude-li tento aspekt podchycen, není dle mého názoru důvod se aplikacím UI i jiných insurtechů do interních a externích procesů nejen pojišťoven bránit.

[168] ČAPEK, Karel. *Dramata: Loupežník: R.U.R.: Věc Makropulos: Bílá nemoc: Matka* [online]. První vydání. Praha: Československý spisovatel, 1994, s. 10. Spisy, sv. 7 [cit. 16. 2. 2022]. Dostupné z: https://web2.mlp.cz/koweb/00/03/34/75/81/rur.pdf.

8 Závěr – ozvěny budoucnosti

Hlavním cílem této práce bylo analyzovat průběh a dopady implementace evropského právního rámce GDPR na pojistný sektor ČR a prokázat úvodní tezi, že GDPR není izolovaným předpisem, nýbrž že společně s dalšími tvoří komplexní, vzájemně provázanou syntézu.

K pokrytí relevantních teoretických i praktických aspektů významných a charakteristických pro pojistný sektor byla zvolena forma rozboru *Standardů*, jelikož tento dokument, který jsem spoluvytvářela, vnímám jako ideální podklad pro vymezení perspektivy pojišťovnictví k GDPR. Tato jedinečná zkušenost společně s informacemi a postřehy získanými během kooperace v rámci ČAP i s ostatními evropskými asociacemi pojistného trhu v rámci IE mi umožnila pohlížet na GDPR nikoli pouze z obecného hlediska, ale se zaměřením na specifičnosti pojistného trhu, a to jak ze strany pojišťoven, tak ze strany jejich klientů či dalších osob v postavení subjektů OÚ.

Standardy tak posloužily pro účely této práce jako základní osa pro definici a analýzu institutů GDPR a jejich implementaci v kontextu pojišťovnictví. Otevřené interpretační otázky i možné okruhy budoucí revize GDPR byly charakterizovány v souvislosti s přístupem evropských orgánů v rámci hodnocení legislativního rámce GDPR i přístupu EDPB. Pojistný sektor využil jedinečné příležitosti a v předchozí fázi veřejné konzultace komunikoval identifikované nedostatky. Tyto, ale i další postřehy jsem vzala v potaz u koncentrace na některé významné GDPR instituty a explikovala jsem nebo jsem navrhla řešení implementačně náročných situací specifických pro pojišťovnictví, jako např. u OÚ o zdravotním stavu, genderu v kontextu hodnocení rizik, AR, rovněž v kontextu UI, či právních základů s orientací obzvláště na souhlas a informační přetížení v kontextu informačních povinností dle souhrnných legislativních požadavků.

Nejednotnost přístupů v rámci EU byla prokázána u některých klíčových institutů, např. u citlivých OÚ, právních základů s orientací zejména na souhlas a přístupu ke kodexům chování, které byly komparovány s úpravou přijatou v dalších ČS.

Také byla vysvětlena a prokázána teze o vysoké míře regulace pojišťovnictví, což bylo analyzováno na vztahu nejvíce relevantních evropských předpisů, popř. jejich národních protějšků k GDPR.

Ve druhé rovině bylo záměrem této práce právě poukázat na nedostatky současné úpravy především ve vztahu k přetrvávající praktické a interpretační fragmentaci v EU. Zde jsem se orientovala na konkrétní důkazy výkladu EDPB nad rámec textu samotného GDPR, jenž je v rozporu z gramatického i logického hlediska, a na jeho dopady pro pojišťovnictví. Proto jsem navrhla dle mého názoru vhodná řešení *de lege ferenda* a obecně i doplnění obsahu *Standardů*, za kritického objasnění limitací pro možnou vyšší formu evoluce na kodex chování *stricto sensu* dle čl. 40 GDPR právě v kontextu diskutabilní intepretace ze strany EDPB. I tak v GDPR existuje prostor pro zdokonalení; navzdory obecnému pozitivnímu hodnocení je nutno brát v potaz např. čím dál běžnější aplikaci insurtechu, pro který může být soulad s GDPR *compliance* minovým polem.

Ve třetí rovině byl proto naznačen i přesah do blízké budoucnosti. Zaměřila jsem se na souvislosti GDPR a nové evropské legislativní regulace týkající se hromadných žalob či očekávaných předpisů ve věcech soukromí v odvětví elektronických komunikací, KB či insurtechu, především UI. Zde jsem analyzovala a v konkrétních návaznostech dovodila, že legislativní úpravu nových institutů je potřeba brát jako nadstavbu GDPR. Z toho jsem vycházela i u dalších navrhovaných kroků, potenciálně možných, s ambicí zakomponování do *Standardů*, a zohledňujících hledisko rozšíření ochrany subjektů OÚ, pojišťoven, legislativní základny, digitalizace a technologického vývoje.

Jak bylo charakterizováno v předchozí kapitole této práce, rapidní vývoj ICT přináší nový, pozitivní potenciál pro subjekty OÚ i pojišťovny, ale na druhé straně může vést ke zvýšené míře ohrožení OÚ. Potřebu, ale i nejednoduchost jejich podchycení zmiňuje i Polčák, který je popisuje jako oblasti, které se v právu ICT objevují zcela nově, typicky v návaznosti na technologický vývoj nebo doposud nevídané společenské využití stávajících technologií. V případech doposud nepoznaných technologických a společenských fenoménů je totiž třeba definovat relativně nové základní parametry příslušné regulatorní agendy a k tomu je nutno vycházet z vysoce abstraktních fundamentálních maxim[169]. Tento nelehký úkol aktuálně čeká EK a další dotčené subjekty. I zde bude nutné vyhodnotit vhodnou míru formalismu, aby nedošlo k opačnému než zamýšlenému následku, tedy brzdě technologického rozvoje pod tlakem legislativních požadavků. Proto je proklamována technologická neutralita a u této oblasti je vhodné aplikovat pragmatický přístup, který ale nebude na úkor GDPR jakožto minimálního standardu a rovného zatížení subjektů.

[169] POLČÁK et al., 2018, op. cit., s. 1.

Neméně významné potenciální kroky ale predikuji optikou vztahů k poskytovatelům služeb ze třetích zemí nebo u asymetrie smluvních vztahů s technologickými giganty, což i s rozvojem insurtechu přímo souvisí. Např. disproporci minimálních standardů v oblasti ochrany OÚ mezi EU a USA je nutné důkladně upravit pro stav po Schrems II a je třeba neopomenout ani pobrexitový stav pro úpravu přenosu OÚ mezi Spojeným královstvím a EU.

Účelem těchto rovin bylo poukázat na spletitý systém, kterým je pojistný sektor vázán ve svém přístupu k GDPR. Mým úmyslem byla nejen deskripce hodnoty OÚ jako takových a jejich ochrany pro pojišťovnictví, i když premisa o jejich významu se ukázala být pravdivá. Jednalo se ale i o cíl analyzovat a na konkrétních příkladech potvrdit, že se jedná o spojené nádoby z pohledu historického, současného a nepochybně i budoucího. Rovinu aktuálního stavu i předpokládaného *pro futuro* rámce jakožto provázaného organizmu proto aplikuji na eventuální návrh rozšíření *Standardů*.

Co se týká hodnocení dopadu GDPR na pojišťovnictví, považuji za vhodné zdůraznit význam této přelomové legislativní úpravy, kterou by bylo dobré vnímat jako globální standard. Jak plyne ze sice krátké, ale v celosvětovém měřítku unikátní evropské zkušenosti, posílení ochrany OÚ je důležitým integračním nástrojem, protože umožňuje volný pohyb OÚ mezi ČS, vytváří dobrou atmosféru pro volný pohyb služeb a zboží, snižuje náklady na poskytování služeb a zboží v přeshraniční perspektivě a zvyšuje kompetitivnost trhů ČS jako celku, ve stejném čase ochraňujíc soukromí jednotlivců z hlediska použití jejich OÚ[170].

Na základě výše uvedeného lze zmínit, že GDPR přineslo nejen do evropského právního prostředí výrazný posun v oblasti ochrany OÚ. To může být inspirací i pro další legislativní formulace, např. práva na lidský dohled u regulace UI právě po vzoru GDPR. GDPR jako norma by tak mělo ovlivnit i další legislativní počiny na evropském poli, poněvadž v této práci zmiňovaná teze o dvoukolejnosti technologického a legislativního vývoje by neměla být opomenuta. Právě zde predikuji obdobný význam návrhů DORA nebo AIA, a to minimálně na dvou úrovních: Zaprvé, je-li smyslem komplexní ochrana OÚ, v této práci dokazuji, že GDPR nelze chápat jako separovanou úpravu. To dle mého názoru platí nejen pro sektor pojišťovnictví. Zadruhé, extenzivnější, i tyto legislativní počiny mohou být inspirací celosvětových rozměrů.

Zároveň tedy bylo mým úmyslem vyzdvihnout esenciální význam legislativního rámce GDPR nejen pro evropské prostředí a zdůraznit, že toto přelomové nařízení a navazující praxe se

[170] DE AZEVEDO CUNHA, 2013, op. cit., s. 206.

nadále vyvíjejí, ať už formou reakcí na praxi, technologických mílových kroků, pokynů EDPB, nebo také judikatury SDEU.

Je tak patrné, že všechny tyto aspekty tvoří, resp. v blízkém časovém horizontu budou tvořit provázaný rámec vyžadující implementaci. Dle mého názoru bylo v této práci prokázáno úvodní tvrzení, že GDPR rámec skutečně není jenom o GDPR. Po skloubení i tak deklaratorního výčtu souvisejících faktických a právních rovin v sektoru pojišťovnictví není složité představit si situaci, kdy např. v důsledku nedostatečné KB ochrany aplikované UI dojde k úniku OÚ s následkem vzniku škody, což vyústí v hromadnou žalobu.

Na základě kritické analýzy, komparace a dedukce jsem dospěla k podloženému závěru, že sektoru pojišťovnictví se v ČR povedlo proces implementace GDPR řádně naplnit. Proaktivní přístup zastřešený ČAP se osvědčil; *Standardy* jsou prakticky použitelné nejen pro *compliance*, experty, ale také pro zaměstnance pojišťoven a subjekty OÚ při pochopení a výkonu jejich práv. Svým přehledným pojetím a volbou jazykových prostředků přibližují složitou problematiku GDPR a aplikují ji na pojistný sektor.

Tuto zdařilou implementaci posuzuji jako ideální základní kámen pro potenciální rozšíření *Standardů* po formální a/nebo obsahové stránce, se zaměřením na přesah s právními základy zpracování OÚ dle ePrivacy, na zakotvení minimálních požadavků na KB v návaznosti na DORA (např. TOO), iniciativy k výměně dat a insurtechu, z důvodu GDPR relevance především UI, v návaznosti na AIA a úpravu odpovědnosti. Právě z důvodu prozatím proklamovaného principu *ratio legis* nikoli nesmyslně preskriptivní, ale principově a rizikově formulované očekávané legislativy lze *Standardy* využít k přiblížení přesahů a souvislostí. I zde však platí „One size does not fit all“, a proto je nutné brát v potaz specifika jednotlivých odvětví.

Na GDPR by mělo být pohlíženo jako na mantinel, na navazující úpravy pak jako na nadstavbu, přičemž společně se jedná o kompatibilní, rovnovážnou úpravu zakotvující právní jistotu pro všechny zúčastněné subjekty, formulující podmínky pro další růst, a především vytvářející ekvilibrium pro subjekty OÚ.

Jak bylo v této práci ukázáno, jedná se o komplexní balíček, který nelze vnímat odděleně, a právní vakuum v těchto oblastech, rapidně nabývajících na významu, by bylo kontraproduktivní. Finanční sektor je jedním z nejvíce narušených odvětví v globální ekonomice. Technologické změny a vysoká míra regulace jsou považovány za nejvíce

narušující faktory.[171] Právě proto bylo mým cílem na tyto faktory poukázat a v závěru analýzy relevantního rámce obhájit nevyhnutelnou adaptaci pojistného sektoru na legislativní novum a dynamické, faktické, tržní, spotřebitelské i technologické požadavky.

I proto datacentrický charakter pojišťovnictví pojímám jako tradiční, výchozí úroveň a GDPR, oblasti KB či insurtech pak chápu spíše jako další evoluční stadium, kdy v silně konkurenčním prostředí není příhodné stagnovat. Ani z hlediska ochrany práv subjektů OÚ dle GDPR tak nepovažuji nové technologické výdobytky, za dodržení podmínek popsaných výše, za hrozby, nýbrž za další podněty ke sofistikaci, modernizaci a optimalizaci.

Status quo tak není udržitelný ani ve spíše rigidním pojistném sektoru, který tak za prognózy inovace v mezích snad konstruktivní a proporcionální regulace čeká nezbytná adaptace *stricto sensu* s prostorem pro potenciální hlubší formu samoregulace inspirované přístupem k GDPR. I zde totiž platí proslulé tvrzení, že jediné, co je konstantní, je změna.

[171] CHRISTOFILOU, Alkistis a CHATZARA, Viktoria. The Internet of Things and Insturance. In: MARANO, Pierpaolo a NOUSSIA, Kyriaki. *InsurTech: a legal and regulatory view*. První vydání. Cham: Springer, 2020, s. 55. AIDA Europe Research Series on Insurance Law and Regulation. ISBN 978-3-030--27385-9.

9 Přílohy

Příloha č. 1: Kompatibilita GDPR a pokynů EDPB

Pokyny EDPB	Požadavky pokynů nad rámec nařízení	Názor pojistného odvětví	Doporučení pojistného odvětví
Pokyny k posouzení vlivu na ochranu OÚ, revidované roku 2017	**Povinné DPIA:** Pokyny rozšiřují povinné provedení DPIA i na situace, kdy není jednoznačné, že DPIA je vyžadováno (s. 8). **Citlivé údaje:** Lokalizační a finanční údaje zařazeny mezi citlivé údaje nebo údaje vysoce osobní povahy (s. 9–10).	**Povinné DPIA:** Požadavek nad rámec nařízení způsobuje právní nejistotu a zvyšuje náklady na DPIA. Společnosti tak preventivně provedou DPIA, aby nedošlo k výtkám v oblasti *compliance* a riziku vzniku právních nároků. **Citlivé údaje:** Rozpor s čl. 9 a 10 GDPR, obsahujícími taxativní výčet.	Pokyny jsou nad rámec požadavků nařízení, což zvyšuje právní nejistotu, *compliance* náklady a riziko vzniku právních nároků. Je doporučeno revidovat text pokynů do znění v souladu s nařízením.
Pokyny k ohlašování případů porušení zabezpečení OÚ, revidované roku 2018	**Komunikace porušení zabezpečení OÚ:** Pokyny uvádějí, že v případě pochybností o porušení a míře rizika by správce měl provést ohlášení (s. 26). **Povinnost dokumentovat porušení zabezpečení OÚ:** Kromě požadavků dle čl. 33 odst. 5 GDPR by správce měl zdokumentovat i zdůvodnění přijatých kroků (s. 27).	**Komunikace porušení zabezpečení OÚ:** Doslovný výklad pokynů vede správce i k ohlašování případů nad rámec povinností dle čl. 33 a 34 GDPR. Dochází k dalšímu zatížení dozorového orgánu a administrativnímu zatížení ohlašovatele. **Povinnost dokumentovat porušení zabezpečení OÚ:** Povinnost zahrnout zdůvodnění je nad rámec požadavku dle čl. 33 odst. 5 GDPR.	Je doporučeno revidovat text pokynů do znění v souladu s nařízením.

Pokyny k automatizovanému individuálnímu rozhodování a profilování, revidované roku 2018	**Nezbytnost:** Pokyny obsahují zatěžující a úzký výklad nezbytnosti aplikace (výhradně) automatizovaného rozhodování v souvislosti s plněním smlouvy nebo úmyslem smlouvu uzavřít (s. 13 až 23). To negativně ovlivňuje aplikaci čl. 6 odst. 1 GDPR u automatizovaného rozhodování a aplikaci čl. 22 odst. 2 písm. a) GDPR u výhradně automatizovaného rozhodování. **Výklad souhlasu dle čl. 22 odst. 2 písm. c) GDPR:** Pokyny uvádějí, že správci opírající se o souhlas jakožto právní základ profilování mají prokázat, že subjekt OÚ přesně porozumí obsahu tohoto souhlasu (s. 12–13). **Právo na informace z profilování:** Pokyny říkají, že podle čl. 15 odst. 3 GDPR má správce povinnost zpřístupnit data použitá pro vytvoření profilu a zajistit přístup k informacím v profilu (s. 17). **Algoritmický audit třetí stranou:** Pokyny obsahují *good practice* doporučení pro správce ve věci čl. 22 GDPR. Jedná se o algoritmický audit třetí stranou, které mají být poskytnuty	**Nezbytnost:** Výklad pokynů, podle kterých má správce vzít v potaz, zda existuje do soukromí méně zasahující metoda a zda je automatizované zpracování nezbytné, není v GDPR obsažen. GDPR pouze uvádí, že tyto procesy mohou být umožněny v případě nezbytnosti v souvislosti s plněním smlouvy nebo úmyslem smlouvu uzavřít. **Výklad souhlasu dle čl. 22 odst. 2 písm. c) GDPR:** Požadavek na přesné porozumění obsahu souhlasu v této věci je disproporční a prakticky nerealizovatelný, a to i v kontextu podmínek informovanosti subjektu údajů dle čl. 13–15 GDPR. **Právo na informace z profilování:** GDPR zavádí právo subjektu údajů na informace o vstupních a výstupních údajích, včetně informace o existenci procesu automatizovaného rozhodování (čl. 13 až 15 GDPR). GDPR však nezavádí právo subjektu údajů na informace o profilu samotném. **Algoritmický audit třetí stranou:** *Good practice* doporučení, i navzdory jeho povaze, může v případě neaplikování vést k vyhodnocení jako	**Nezbytnost:** Tento výklad vytváří právní nejistotu v pojistném sektoru, protože limituje používání automatizovaných procesů, což je překážkou dalšího rozvoje inovativních technologií. **Výklad souhlasu dle čl. 22 odst. 2 písm. c) GDPR:** Slovo „přesně“ by mělo být vyňato z pokynů a tato část pokynů by měla být revidována v souladu s požadavky čl. 13–15 GDPR. **Právo na informace z profilování:** GDPR nezavádí právo subjektu údajů na informace o profilu samotném. Tento požadavek by měl být z pokynů odstraněn. **Algoritmický audit třetí stranou:** Audit prováděný třetí stranou není v GDPR zahrnut. Tento požadavek by měl být z pokynů odstraněn. Je doporučeno revidovat text pokynů do znění v souladu s nařízením a smazat příklad, který nevychází z GDPR.

	všechny nezbytné informace o fungování algoritmu (s. 32).	v rozporu s *compliance* požadavky u vyšetřování během auditu DPA podle čl. 58 odst. 1 písm. b) GDPR. Audit prováděný třetí stranou není v GDPR zahrnut.	
Pokyny k transparentnosti, revidované roku 2018	**Povinnost poskytnout informace o následcích zpracování:** Pokyny uvádějí, že kromě informací poskytnutých dle čl. 13 a 14 GDPR správce odděleně jednoznačně pochopitelným jazykem poskytne informace o nejdůležitějších následcích zpracování (s. 7 odst. 10). **Výjimky z povinnosti poskytnout informace podle čl. 13 GDPR:** V souladu s čl. 13 odst. 4 GDPR může být správce vyňat z informačních povinností, pokud subjekt OÚ již těmito informacemi disponuje. Avšak pokyny (s. 27–29) obsahují příklad *best practice*, který jde nad rámec povinností dle čl. 13, neboť uvádějí, že kompletní informace mají být subjektu údajů poskytnuty opětovně. **Přiměřené nástroje k poskytnutí informací podle čl. 13 a 14 GDPR:** Pokyny říkají, že případné změny mají být komunikovány prostřednictvím	**Povinnost poskytnout informace o následcích zpracování:** Požadavek na poskytnutí informací nad rámec výčtu čl. 13 a 14 jde nad rámec GDPR. To přináší nepřiměřené a neodůvodněné zatížení správce. **Výjimky z povinnosti poskytnout informace podle čl. 13 GDPR:** Příklad jde nad rámec GDPR a vede k dalšímu informačnímu přetížení subjektu údajů. **Přiměřené nástroje k poskytnutí informací podle čl. 13 a 14 GDPR:** Tento výklad jde nad rámec čl. 12 GDPR a přináší nepřiměřené zatížení správce. Také vede k informačnímu přetížení subjektu údajů. To je v rozporu s proklamovaným principem transparentnosti. **Maximální časový limit pro poskytnutí informací podle čl. 14 GDPR:** Pokyny u písm. b) a c) zavádějí	**Povinnost poskytnout informace o následcích zpracování:** Požadavek, který jde nad rámec GDPR, by měl být vyňat z pokynů. **Výjimky z povinnosti poskytnout informace podle čl. 13 GDPR:** Příklad by měl být smazán. **Přiměřené nástroje k poskytnutí informací podle čl. 13 a 14 GDPR:** Povinnost nad rámec GDPR by měla být z pokynů odstraněna. **Maximální časový limit pro poskytnutí informací podle čl. 14 GDPR:** Rozšíření časového limitu na další ustanovení je nad rámec GDPR. Mělo by dojít k odstranění z pokynů.

	přiměřených nástrojů (e-mail, dopis atd.), ve kterých mají být obsaženy pouze tyto změny, tedy nikoli společně s dalším, např. marketingovým, obsahem. **Maximální časový limit pro poskytnutí informací podle čl. 14 GDPR:** Pokyny (s. 15) odkazují na čl. 14 odst. 3 písm. b) GDPR za situace, kdy se první komunikace se subjektem OÚ uskuteční po více než jednom měsíci od obdržení OÚ; je aplikován čl. 14 odst. 3 písm. a), takže informace dle čl. 14 mají být poskytnuty ve lhůtě jednoho měsíce. To pokyny uvádějí i pro čl. 14 odst. 3 písm. c) GDPR.	nové časové limity. Ty mají být aplikovány pouze u písm. a).	
Pokyny k souhlasu, revidované roku 2018 (k této verzi se vztahují následující informace) a 2020	**Svobodně udělený souhlas v pojistném kontextu:** Pokyny výslovně neuvádějí, že souhlas pro zpracovávání citlivých OÚ v pojistném kontextu je svobodně udělený, a tedy nepodmíněný. Avšak uvádějí několik aspektů, které vedou k závěru, že souhlas není vhodným právním základem pro situace, kdy je zpracování OÚ nezbytné pro plnění smlouvy. V těchto situacích je dle pokynů vhodným právním základem plnění smlouvy (s. 8–9, poznámka pod čarou č. 23). Pokyny uvádějí,	**Svobodně udělený souhlas v pojistném kontextu:** Výklad „svobodně uděleného“ souhlasu zůstává problematický. Pojišťovny mohou čelit situaci, kdy souhlas není vyhodnocen jako svobodně udělený, pokud subjekt OÚ nemá reálnou možnost výběru ani možnost souhlas odmítnout či vzít zpátky bez negativních následků, např. bez nemožnosti uzavření smlouvy nebo vyššího pojistného. To ztěžuje situaci pojišťoven při vymezení vhodných	**Svobodně udělený souhlas v pojistném kontextu:** Pokyny by měly být doplněny o ustanovení, že v pojistném sektoru lze tyto situace podřadit pod právní základ svobodně uděleného souhlasu. **Odmítnutí a zpětvzetí souhlasu k tíži subjektu OÚ:** Pokyny by měly obsahovat příklady (ideálně i v pojistném kontextu) vysvětlující, že k zatížení subjektu OÚ nedochází a souhlas je platný, když je služba suspendována, protože uživatel odejmul souhlas

	že souhlas je právním základem pro zpracování citlivých OÚ pouze v případech, kdy nelze aplikovat jiný právní základ uvedený v čl. 9 odst. 2 písm. b–j) (s. 19). **Odmítnutí a zpětvzetí souhlasu k tíži subjektu OÚ:** Pokyny (s. 10–11, příklad 8) vysvětlují, že když uživatel aplikace vezme zpět souhlas, což vede ke zhoršení služeb, a tyto údaje nebyly potřeba pro poskytnutí služby, jedná se o zatížení uživatele, a souhlas je neplatný. **Souhlas za třetí strany v pojistném kontextu:** Pokyny nespecifikují, jestli pojistník (rodič) může udělit souhlas za třetí strany (děti, členy rodiny) např. u cestovního pojištění. **Povinnost uvádět třetí strany:** Pokyny (s. 13) uvádějí, že pro splnění informační povinnosti dle čl. 13, 14 GDPR má správce poskytnout úplný seznam všech příjemců nebo kategorií příjemců, včetně zpracovatelů. **Souhlas v digitálním prostředí:** Pokyny reagují na početné kliky u více souhlasů, což může vést k ignoraci jejich obsahu ze strany uživatele, vyjádřením, že správce má povinnost	právních základů. **Odmítnutí a zpětvzetí souhlasu k tíži subjektu OÚ:** Podle příkladu 8 pokynů by pojišťovny mohly argumentovat, že nedochází k zatížení subjektu OÚ, a souhlas je tedy platný, když uživatel aplikace odejme souhlas se zpracováním OÚ, které jsou nezbytné pro poskytnutí služby / / výkon smlouvy. Avšak jedná se o výklad, který neposkytuje dostatečnou míru právní jistoty. **Souhlas za třetí strany v pojistném kontextu:** Absence této problematiky vede k právní nejistotě. Pojišťovny z tohoto důvodu potřebují souhlas všech zúčastněných subjektů. To znemožňuje efektivní uzavření pojistné smlouvy pro spotřebitele (především u online produktů) a je výrazně ztížena možnost pojišťoven získat a prokázat získání těchto souhlasů. **Povinnost uvádět třetí strany:** Podmínka úplného seznamu jde nad rámec informačních požadavků dle čl. 13 odst. 1 písm. e) a 14 odst. 1 písm. e) GDPR. Nedosažitelnost *compliance* s tímto požadavkem vychází z faktu, že pojišťovny	se zpracováním, které je nezbytné pro správce k poskytování služby / / výkon smlouvy. **Souhlas za třetí strany v pojistném kontextu:** Pokyny by měly obsahovat příklad, že udělení souhlasu za třetí osoby je v pojišťovnictví běžnou praxí, např. u cestovního nebo zdravotního pojištění. Takto udělený souhlas by měl být považován za platný. **Povinnost uvádět třetí strany:** Pokyny by neměly zavádět povinnosti nad rámec GDPR. Požadavek na úplnost seznamu by měl být odstraněn. **Souhlas v digitálním prostředí:** Mělo by dojít minimálně ke změně textace ve smyslu doporučení správcům najít řešení této situace. **Obnova souhlasu:** Doporučení by mělo být odstraněno.

	najít řešení této situace. **Obnova souhlasu:** Pokyny (s. 21) doporučují obnovit souhlas v přiměřených intervalech. Vycházejí z předpokladu, že opětovné poskytnutí informací zajistí plnou informovanost subjektu OÚ.	musí zasílat OÚ mnoha poskytovatelům služeb. Proto může být seznam velice obsáhlý nebo někteří příjemci OÚ nemusí být známi v momentě sběru OÚ. Např. u cestovního pojištění nemusí být předem známo, kdo bude zahraničním poskytovatelem zdravotních služeb. **Souhlas v digitálním prostředí:** GDPR nezavádí povinnost správce zajistit, že uživatel čte obsah souhlasů. Jedná se o disproporční požadavek, nejedná se o povinnost subjektu OÚ *a vice versa*. **Obnova souhlasu:** GDPR požadavek na pravidelnou obnovu souhlasu neurčuje. Tento požadavek tak jde nad rámec level 1. Dále předpoklad pokynů není podložen a vede k informačnímu přetížení subjektu údajů a administrativnímu zatížení správce. Následkem může být i právní nejistota za situace, že subjekt OÚ souhlas neobnoví, ale ani neodvolá. Není jasné, zda souhlas zůstává platný.	
Pokyny týkající se kodexů chování a subjektů pro monitorování podle nařízení, přijaté roku	**Nedostatek ekonomické životaschopnosti pro splnění kritérií subjektů pro monitorování:** Pokyny obsahují těžce	**Nedostatek ekonomické životaschopnosti pro splnění kritérií subjektů pro monitorování:** Kodexy chování mají být	**Nedostatek ekonomické životaschopnosti pro splnění kritérií subjektů pro monitorování:** Kodexy chování mají sloužit

2019	dosažitelná a finančně náročná akreditační kritéria. Málo společností je naplní. Jedná se např. o demonstraci nezávislosti oddělením zaměstnanců, managementu, rozpočtu i odpovědnosti, prevenci střetu zájmu oddělením zaměstnanců monitorovacího orgánu, odbornost za situace, kdy neexistují předchozí zkušenosti s orgánem podobného charakteru. **Nemožnost doplnit kodex chování během jeho schvalování:** Pokyny uvádějí, že okamžikem přijetí kodexu chování do schvalovacího procesu může dojít k jeho odmítnutí ze strany dohledového orgánu. To v případě úprav či doplnění kodexu chování povede k opětovnému koloběhu podání a schvalovacího procesu.	samoregulačním nástrojem, a proto by pokyny měly zohlednit proveditelnost řešení pro monitorování souladu s GDPR. To uvádí, že tyto nástroje mají být přínosné a úsporné. **Nemožnost doplnit kodex chování během jeho schvalování:** Pokyny neupravují schvalovací proces efektivním způsobem. Mělo by být umožněno vést během procesu dialog. To by mělo být posíleno možností konzultací či dotazování obou zúčastněných stran.	k lepšímu dosažení *compliance* s GDPR. Pokyny by měly být upraveny tak, aby excesivní kritéria nebránila v přijetí kodexů chování. **Nemožnost doplnit kodex chování během jeho schvalování:** Schvalování kodexu chování by mělo být efektivnější a vyhnout se nepřiměřeným administrativním a jiným nákladům. Pokyny by měly obsahovat možnost konzultace s dohledovým orgánem během schvalovací fáze.
Návrh pokynů k čl. 25, nastavení ochrany OÚ od návrhu a standardní nastavení ochrany OÚ, veřejná konzultace ukončena v lednu 2020	**Definice spojení „nejmodernější technologie“:** Pokyny (s. 7–8, poznámka pod čarou č. 6) uvádějí, že nejmodernější technologie může být identifikovatelná jako „technologická úroveň služby nebo produktu, která existuje na trhu a je nejefektivnější z hlediska dosažení požadovaných výsledků“. Dále je uvedeno, že zanedbání technologického rozvoje může vést k nedostatku	**Definice spojení „nejmodernější technologie“:** Vymezení pokynů a jeho ekonomicky náročné důsledky jdou nad rámec čl. 25 GDPR, kde nejmodernější technologie mají být hodnoceny společně s dalšími faktory, jako jsou např. náklady na implementaci. **Definice spojení „implementační**	**Definice spojení „nejmodernější technologie“:** Pokyny by měly obsahovat vysvětlení, že se nejedná o požadavek na konstantní implementování nových technologických řešení. **Definice spojení „implementační náklady“:** Pokyny by měly obsahovat požadavek na provedení balančního testu,

	compliance s čl. 25 GDPR. **Definice spojení „implementační náklady“:** Pokyny (s. 8) uvádějí, že správce má v rámci rozpočtu počítat s náklady na efektivní implementaci GDPR principů a že neschopnost nést tyto náklady není omluvou pro nedostatečnou *compliance* s GDPR. **Vyvažování zájmů v kontextu zákonnosti:** Pokyny (s. 15) zakotvují, že když je právním základem oprávněný zájem dle čl. 6 odst. 1 písm. f) GDPR, má správce povinnost zveřejnit výsledky balančního testu ke střetu zájmů. Zájmy mají být hodnoceny objektivně. Dále když správce aplikuje právní základ plnění smlouvy dle čl. 6 odst. 1 písm. b) GDPR (pokyny s. 15–16), musí být všechna data sesbírána přímo od subjektu OÚ a v případě, že některá data pocházejí od třetí strany, je jediným aplikovatelným právním základem dle čl. 6 odst. 1 písm. a) souhlas.	**náklady“:** GDPR neobsahuje tento požadavek. Požadavky dle čl. 25 GDPR by měly být hodnoceny komplexně. Úmysl EDPB by byl lépe naplněn požadavkem na provedení balančního testu. **Vyvažování zájmů v kontextu zákonnosti:** Tyto požadavky jdou na rámec GDPR. Čl. 13–15 GDPR jasně vymezují, že při zpracování OÚ na základě oprávněného zájmu má správce povinnost zveřejnit informace k zohledňovanému zájmu. Kritérium na objektivnost není v čl. 6 odst. 1 písm. f) GDPR uvedeno. Požadavek na sběr dat přímo od subjektu OÚ v případě aplikace právního základu plnění smlouvy dle čl. 6 odst. 1 písm. b) GDPR není v GDPR obsažen. To vytváří právní nejistotu a může docházet k fragmentaci praxe.	vyhodnocení rizik a posuzování jednotlivých kritérií dle čl. 25 GDPR komplexně. To by naplnilo soulad s čl. 32 i bodem 83 preambule GDPR. **Vyvažování zájmů v kontextu zákonnosti:** Pokyny by měly respektovat dikci GDPR.

Návrh pokynů ke zpracovávání OÚ v kontextu propojených vozidel, veřejná konzultace ukončena v květnu 2020	**GDPR a ePrivacy:** Podle směrnice ePrivacy není u výjimek uvedených v čl. 5 odst. 3 k přístupu k informacím uloženým v konečném zařízení potřeba souhlas. Avšak dle pokynů (odst. 18) je nutno aplikovat jeden z právních základů čl. 6 GDPR. **Souhlas:** Pokyny (odst. 46) vymezují, že správci OÚ mají být opatrní u získávání platného souhlasu zúčastněných stran, jako jsou uživatelé a vlastníci vozidel. Avšak pokyny (odst. 49) taktéž uvádějí, že v praxi může být složité získat souhlas od řidičů a pasažérů, kteří nejsou ve vztahu k majiteli vozidla. **Telemetrie:** Pokyny (odst. 52) zakotvují, že telemetrické údaje sbírané za účelem údržby nemohou být poskytnuty pojišťovnám bez souhlasu k využívání pojistného produktu založeného na chování. **Komerční partnery:** Pokyny (odst. 95) uvádějí, že souhlas subjektu OÚ má být systematicky obdržen před jejich poskytnutím komerčním partnerům v pozici správce. **Geolokalizační údaje:** Pokyny (odst. 61) uvádějí, že sběr	**GDPR a ePrivacy:** Tímto výkladem vzniká nová povinnost správců OÚ. To je v rozporu s čl. 95 a bodem 173 preambule GDPR. **Souhlas:** Pokyny by měly uvádět, že je možno alternativně aplikovat i jiný právní základ než souhlas. Dále by mělo být uvedeno, že není vyžadován souhlas pasažérů, které nelze identifikovat, a tím pádem není možné obdržet jejich souhlas. **Telemetrie:** Pokyny by zároveň měly uvádět, že telemetrické údaje jsou nezbytné pro výkon smlouvy v kontextu telematiky a pojištění vozidel, a čl. 6 odst. 1 písm. b) GDPR tedy lze aplikovat. V opačném případě může docházet k nevhodnému výkladu, že pro zpracovávání telemetrických údajů je vždy potřebný souhlas. **Komerční partneři:** Tento požadavek je nejenom prakticky nerealizovatelný, ale je i v rozporu s odst. 93, který uvádí, že správce OÚ může poskytnout OÚ komerčním partnerům, je-li takové poskytnutí podloženo některým právním základem dle čl. 6 GDPR. **Geolokalizační údaje:** Tyto principy jsou	**GDPR a ePrivacy:** Pokyny by měly obsahovat vysvětlení, že odst. 18 upravuje pouze další zpracovávání, a to po shromáždění dat z konečného zařízení. **Souhlas:** Pokyny by měly obsahovat alternativní možnost aplikace dalších právních základů. V kontextu telematiky a pojištění vozidel je nejvhodnějším právním základem dle čl. 6 odst. 1 písm. b) GDPR plnění smlouvy. **Geolokalizační údaje:** Principy by měly být přehodnoceny. **Limitace přístupu k primárním údajům:** Pokyny by měly vzít v potaz význam těchto údajů pro poskytování pojistných služeb.

	geolokalizačních údajů musí vycházet z principů, kdy k aktivaci geolokalizace dojde pouze po spuštění funkce uživatelem a že geolokaci je možno kdykoliv vypnout. **Limitace přístupu k primárním údajům:** Pokyny (odst. 74, 108) doporučují omezit přístup pojišťoven k primárním údajům z důvodu prevence přesného profilování pohybů.	v rozporu s principem spravedlnosti v pojistné telematice a v rozporu se smluvním právem. **Limitace přístupu k primárním údajům:** Přístup pojišťoven k primárním údajům je základním předpokladem férově stanovené výše pojistného. Negativní následky jsou spatřovány i v hledisku konkurenceschopnosti, inovací a regulatorních požadavků.	

10 Seznam použitých zkratek

AIA – návrh nařízení o umělé inteligenci

AIDA – zvláštní výbor Evropského parlamentu pro umělou inteligenci

AML/CFT – směrnice Evropského parlamentu a Rady (EU) 2015/849, o předcházení využívání finančního systému k praní peněz nebo financování terorismu / prevence využívání finančního systému k praní peněz nebo financování terorismu

AR – automatizované rozhodování

ČAP – Česká asociace pojišťoven

ČNB – Česká národní banka

ČR – Česká republika

ČS – členský stát / členské státy

ČSpA – Česká společnost aktuárů

DFS – *Digitální finanční strategie*

DORA – návrh nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru

DPIA – posouzení vlivu na ochranu osobních údajů

DPA – dozorový úřad (v kontextu GDPR)

DPO – pověřenec pro ochranu osobních údajů

EDPB – Evropský sbor pro ochranu osobních údajů

EDPS – evropský inspektor pro ochranu osobních údajů

EHP – Evropský hospodářský prostor

EIOPA – Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění

ENISA – Agentura Evropské unie pro kybernetickou bezpečnost

EK – Evropská komise

EP – Evropský parlament

ES – Evropské společenství

ESD – *Evropská strategie pro data*

ESLP – Evropský soud pro lidská práva

EÚLP – *Evropská úmluva o lidských právech*

EPrivacy – směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. 7. 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací

EU – Evropská unie

FO – fyzická osoba

GDPR – nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES

ICT – informační a komunikační technologie

ICT TPPs – třetí strany v postavení poskytovatelů ICT služeb

IS – informační systém / informační systémy

IDD – směrnice Evropského parlamentu a Rady (EU) 2016/97 ze dne 20. 1. 2016, o distribuci pojištění

IoT – internet věcí

IE – Insurance Europe

Insurtech – inovativní technologie v pojišťovnictví

KB – kybernetická bezpečnost

LZPEU – *Listina základních práv Evropské unie*

NIS – směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. 7. 2016, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Evropské unii

NIS2 – revize NIS

NOYB – nezisková organizace None of Your Business

NSS – Nejvyšší správní soud

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OECD – Organizace pro hospodářskou spolupráci a rozvoj

OÚ – osobní údaj / osobní údaje

OZ – zákon č. 89/2012 Sb., občanský zákoník

PLD – směrnice Rady 85/374/EHS ze dne 25. 7. 1985, o sbližování právních a správních předpisů ČS týkajících se odpovědnosti za vadné výrobky

PO – právnická osoba

PPP – prevence a odhalování pojistného podvodu

PS – pracovní skupina

PRIIPs – nařízení Evropského parlamentu a Rady (EU) č. 1286/2014 ze dne 26. 11. 2014, o sděleních klíčových informací týkajících se strukturovaných retailových investičních produktů a pojistných produktů s investiční složkou

RČ – rodné číslo / rodná čísla

SII – směrnice Evropského parlamentu a Rady 2009/138/ES ze dne 25. 11. 2009, o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu

SCCSs – standardní smluvní doložky

SDEU – Soudní dvůr Evropské unie

SEU – *Smlouva o Evropské unii*

SFEU – *Smlouva o fungování Evropské unie*

Standardy – *Samoregulační standardy ČAP k uplatňování GDPR v pojišťovnictví*

TOO – technická a organizační opatření

UI – umělá inteligence

Úmluva 108 – *Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat Rady Evropy*

ÚOOÚ – Úřad pro ochranu osobních údajů

VDLP – *Všeobecná deklarace lidských práv*

WP29 – Pracovní skupina čl. 29

ZDPZ – zákon č. 170/2018 Sb., o distribuci pojištění a zajištění

ZoKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti

ZPOJ – zákon č. 277/2009 Sb., o pojišťovnictví

Zpráva – *Hodnotící zpráva dle čl. 97 GDPR*

ŽP – životní pojištění

11 Seznam použitých zdrojů

Seznam použité literatury

BOBEK, Michal, BŘÍZA, Petr a KOMÁREK, Jan. *Vnitrostátní aplikace práva Evropské unie*. Praha: C. H. Beck, 2011. 640 s. Beckova edice Právo. ISBN 978-80-7400-377-6.

DE AZEVEDO CUNHA, Mario V. *Market integration through data protection: an analysis of the insurance and financial industries in the EU*. Dordrecht: Springer, 2013. 220 s. Law, Governance and Technology Series, Vol. 9. ISBN 978-94-007-6084-4.

HARARI, Yuval N. *21 lekcí pro 21. století*. Přeložila Z. GUBALOVÁ. Praha: Leda, 2019. 392 s. ISBN 978-80-7335-612-5.

HARARI, Yuval N. *Homo Deus: stručné dějiny zítřka*. Praha: Leda, 2017. 444 s. ISBN 978--80-7335-502-9.

MESRŠMÍD, Jaroslav. *Regulace pojišťovnictví v EU*. První vydání. Praha: Professional Publishing, 2015. 178 s. ISBN 978-80-7431-146-8.

NULÍČEK, Michal et al. *GDPR — obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. 580 s. Praktický komentář. ISBN 978-80-7552-765-3.

PETROV, Jan et al. *Občanský zákoník: komentář*. První vydání. Praha: C. H. Beck, 2017. 3120 s. Beckova edice Komentované zákony. ISBN 978-80-7400-653-1.

POLČÁK, Radim et al. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018. 656 s. Právní monografie. ISBN 978-80-7598-045-8.

POLČÁK, Radim. Protiprávní jednání a škoda on-line. In: *XXVIII. Karlovarské právnické dny*. Praha: Leges, 2021, s. 518–535. ISBN 978-80-7502-462-6.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. Druhé, rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. 936 s. ISBN 978-80-7380-720-7.

SYLLOVÁ Jindřiška et al. *Lisabonská smlouva: komentář*. První vydání. Praha: C. H. Beck, 2010. 1344 s. Beckova edice Komentované zákony. ISBN 978-80-7400-339-4.

ŠVENDOVÁ, Dagmar. *Legislativní proces EU z pohledu Evropského parlamentu: (na příkladu tzv. „Balíčku energetické účinnosti“)*. Ostrava: Key Publishing, 2011. 126 s. ISBN 978-80-7418-112-2.

ZUBOFF, Shoshana. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. London: Profile Books, 2019. 691 s. ISBN 978-1-78125-685-5.

Seznam použitých článků

BUGRA, Aysegul. Room for Compulsory Product Liability Insurance in the European Union for Smart Robots? Reflections on the compelling challenges. In: MARANO, Pierpaolo a NOUSSIA, Kyriaki. *InsurTech: a legal and regulatory view*. První vydání. Cham: Springer, 2020, s. 167–197. AIDA Europe Research Series on Insurance Law and Regulation. ISBN 978-3-030-27385-9.

GRAF VON WESTPHALEN, Friedrich. Náhrada škody ve virtuálním světě s důrazem na umělou inteligenci. In: *XXVIII. Karlovarské právnické dny*. Praha: Leges, 2021, s. 425–440. ISBN 978-80-7502-462-6.

CHATZARA, Viktoria. FinTech, InsurTech, and the Regulators. In: MARANO, Pierpaolo a NOUSSIA, Kyriaki. *InsurTech: a legal and regulatory view*. První vydání. Cham: Springer, 2020, s. 3–25. AIDA Europe Research Series on Insurance Law and Regulation. ISBN 978-3-030-27385-9.

CHRISTOFILOU, Alkistis a CHATZARA, Viktoria. The Internet of Things and Insturance. In: MARANO, Pierpaolo a NOUSSIA, Kyriaki. *InsurTech: a legal and regulatory view*. První vydání. Cham: Springer, 2020, s. 49–81. AIDA Europe Research Series on Insurance Law and Regulation. ISBN 978-3-030-27385-9.

Internet nemůže být divoký západ. *Index LN 06/2017*, Praha, 2017, s. 12–17, ISSN 2464-6911.

REGO, Madriga L. a CARVAHLO, Joana C. Insurance in Today's Sharing Economy: New Challenges Ahead or a Return to the Origins of Insurance? In: MARANO, Pierpaolo a NOUSSIA, Kyriaki. *InsurTech: a legal and regulatory view*. První vydání. Cham: Springer, 2020, s. 27–47. AIDA Europe Research Series on Insurance Law and Regulation. ISBN 978-3-030-27385-9.

TERESZKIEWICZ, Piotr. Digitalisation of Insurance Contract Law: preliminary thoughts with special regard to insurer's duty to advise. In: MARANO, Pierpaolo a NOUSSIA, Kyriaki. *InsurTech: a legal and regulatory view*. První vydání. Cham: Springer, 2020, s. 127–146. AIDA Europe Research Series on Insurance Law and Regulation. ISBN 978-3-
-030-27385-9.

Seznam použitých internetových zdrojů

ANDRAŠČIKOVÁ, Jana. Kompatibilita *Standardů* s požadavky pokynů [tabulka]. In: *Opojištění.cz* [online]. [cit. 20. 2. 2022]. Dostupné z: https://www.opojisteni.cz/legislativa/evropska-legislativa/krok-za-krokem-ke-kodexu-chovani-podle-gdpr/c:17456/.

ANDRAŠČIKOVÁ, Jana. Šablona pro ohlašování případů porušení zabezpečení osobních údajů. *Pojistný obzor: časopis českého pojišťovnictví* [online]. Praha: ČAP, 2018, č. 2, s. 12 až 13. ISSN 2464-7381 [cit. 22. 2. 2022]. Dostupné z: https://www.pojistnyobzor.cz/images/archiv/2018-2/casopis.pdf.

Autoriteit Persoonsgegevens. *Normuitleg grondslag 'gerechtvaardigd belang'* [online]. 1. 11. 2019 [cit. 20. 2. 2022]. Dostupné z: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf.

BAKER, Tom. *Containing the Promise of Insurance: adverse selection and risk classification* [online]. Philadephia: University of Pennsylvania Carey Law School, 2002, 33 s. [cit. 20. 2. 2022]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=322581.

Blockchain in insurance – opportunity or threat? [online]. New York: © McKinsey&Company, July 2016, 8 s. [cit. 20. 2. 2022]. Dostupné z: https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/blockchain%20in%20insurance%20opportunity%20or%20threat/blockchain-in-insurance-opportunity-or-threat.ashx.

BOKŠOVÁ, Jiřina. Solventnost I a II v pojišťovnictví. *Český finanční a účetní časopis* [online]. 2006, 1(3), 127–132 [cit. 15. 2. 2022]. ISSN 18022200. Dostupné z: https://cfuc.vse.cz/pdfs/cfu/2006/03/12.pdf.

BRAUN, Alexander a SCHREIBER, Florian. *The Current InsurTech Landscape: business models and disruptive potential* [online]. St. Gallen: Institute of Insurance Economics I.VW--HSG, University of St. Gallen, 2017 [cit. 20. 2. 2022]. ISBN 978-3-7297-2009-1. Dostupné z: https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/ab-insurtech_2017.pdf.

CLARKE, Roger. Introduction to Dataveillance and Information Privacy, and Definitions of Terms. In: *Roger Clarke's Website* [online]. Canberra: Xamax Consultancy Pty Ltd, 15. 8. 1997. 24. 7. 2016 [cit. 16. 2. 2022]. Dostupné z: http://www.rogerclarke.com/DV/Intro.html.

ČAP. Samoregulační standardy. In: *Čap.cz* [online]. Praha: ČAP [cit. 2. 3. 2022]. Dostupné z: https://www.cap.cz/odborna-verejnost/samoregulacni-standardy#:~:text=Dlouhodob%C3%BDm%20c%C3%ADlem%20%C4%8CAP%20je%20transformace,%2C%20kter%C3%A9%20tvo%C5%99%C3%AD%2093%20%25%20trhu.

ČAP. *Samoregulační standardy ČAP k uplatňování GDPR v pojišťovnictví* [online]. Druhé, revidované vydání. Praha: ČAP, 1. 8. 2020 [cit. 12. 2. 2022]. Dostupné z: https://www.cap.cz/images/o-nas/CAP_GDPR_standardy.PDF.

ČAPEK, Karel. *Dramata: Loupežník: R.U.R.: Věc Makropulos: Bílá nemoc: Matka* [online]. První vydání. Praha: Československý spisovatel, 1994, 89 s. Spisy, sv. 7 [cit. 16. 2. 2022]. Dostupné z: https://web2.mlp.cz/koweb/00/03/34/75/81/rur.pdf.

ČSpA. *Odborné doporučení ČSpA č. 2* [online]. Praha: ČSpA, 1. 11. 2012 [cit. 16. 2. 2022]. Dostupné z: https://www.actuaria.cz/doporuceni-2.html.

DIGITALEUROPE. *Von der Leyen is right: Digital is the 'make-or-break' issue* [online]. 15. 9. 2021 [cit. 16. 2. 2022]. Dostupné z: https://www.digitaleurope.org/news/von-der-leyen-is-right-digital-is-the-make-or-break-issue/.

DURSKA, Agnieszka. Insurance Europe: Working together to ensure the voices of Europe's insurers are heard in EU policymaking. In: *Piu.org.pl* [online]. 27. 1. 2021 [cit. 20. 2. 2022]. Dostupné z: https://piu.org.pl/blogpiu/insurance-europe-working-together-to-ensure-the-voices-of-europes-insurers-are-heard-in-eu-policymaking/.

EIOPA. *Obecné pokyny k outsourcingu u poskytovatelů cloudových služeb* [online]. Frankfurt nad Mohanem: EIOPA, 2020 [cit. 16. 2. 2022]. Dostupné z: https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_cz_0.pdf.

EIOPA, 2021. *Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector. A report from EIOPA's Consultative Expert Group on Digital Ethics in insurance* [online]. Luxembourg: Publications Office of the European union, 2021 [cit. 21. 2. 2022]. ISBN 978-92-9473-303-0. Dostupné z: https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa-ai-governance-principles-june-2021.pdf.

EIOPA. *Cyber risk for insurers – challenges and opportunities* [online]. Luxembourg: Publications Office of the European Union, 2019 [cit. 16. 2. 2022]. ISBN 978-92-9473-213-2. Dostupné z: https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf.

EIOPA. *Cyber risks: what is the impact on the insurance industry?* [online]. © EIOPA, 15. 10. 2021 [cit. 16. 2. 2022]. Dostupné z: https://www.eiopa.europa.eu/media/feature-article/cyber-risks-what-impact-insurance-industry.

EIOPA. *Eiopa strategy on cyber underwriting* [online]. EIOPA, © 2020 [cit. 16. 2. 2022]. ISBN 978-92-9473-225-5. Dostupné z: https://www.eiopa.europa.eu/document-library/strategy/cyber-underwriting-strategy_en.

EIOPA. *Guidelines on information and communication technology security and governance* [online]. Frankfurt: EIOPA, 8. 10. 2020 [cit. 16. 2. 2022]. Dostupné z: https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/eiopa-bos-20-600-guidelines-ict-security-and-governance.pdf?source=search.

FELDMAN, Michael. Market for Artificial Intelligence Projected to Hit $36 Billion by 2025. In: *Top500.org* [online]. 29. 8. 2016 [20. 2. 2022]. Dostupné z: https://www.top500.org/news/market-for-artificial-intelligence-projected-to-hit-36-billion-by-2025/.

GELLERT, Raphaël. Understanding Data Protection as Risk Regulation. *Journal of Internet Law* [online]. 2015, 18(11), s. 3–15 [cit. 15. 2. 2022]. Dostupné z: https://www.researchgate.net/publication/301552462_Understanding_Data_Protection_As_Risk_Regulation.

IE. *Insurance fraud: not a victimless crime* [online]. Brussels: © IE aisbl, November 2019 [cit. 20. 2. 2022]. Dostupné z: https://www.insuranceeurope.eu/mediaitem/2bf88e16-0fe2-4476-8512-7492f5007f3c/Insurance%20fraud%20-%20not%20a%20victimless%20crime.pdf.

IE. *Making EU insurance regulation that works and benefits consumers* [online]. Brussels: IE aisbl, December 2019 [cit. 20. 2. 2022]. Dostupné z: https://www.insuranceeurope.eu/publications/498/making-eu-regulation-that-works-and-benefits-consumers/download/Making+EU%20regulation%20that%20works%20and%20benefits%20consumers.pdf.

IE. *Position on the European Commission proposal for a Digital Operational Resilience Act* [online]. Brussels: IE, 22. 2. 2021 [cit. 16. 2. 2022]. Dostupné z: https://www.insuranceeurope.eu/publications/1646/position-on-the-european-commission-proposal-for-a-digital-operational-resilience-act/download/Position+on%20the%20European%20Commission%20proposal%20for%20a%20Digital%20Operational%20Resilience%20Act.pdf.

IE. *Q&A on the use of big data in insurance* [online]. Brussels: © IE aisbl, January 2019 [cit. 21. 2. 2022]. Dostupné z: https://www.insuranceeurope.eu/publications/504/qas-on-the-use-of-big-data-in-insurance/download/QAs+on%20the%20use%20of%20big%20data%20in%20insurance.pdf.

Independent German Federal and State Data Protection Supervisory Authorities. Report on Experience Gained in the Implementation of the GDPR [online]. Independent German Federal and State Data Protection Supervisory Authorities, November 2019, s. 6 [cit. 20. 2. 2022]. Dostupné z: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/Evaluation-Report-German-DPAs-Clean.pdf.

Komentář ČAP: Pojišťovny svazuje evropská regulace. In: *Opojištění.cz* [online]. 26. 9. 2017 [cit. 20. 2. 2022]. Dostupné z: https://www.opojisteni.cz/spektrum/komentar-cap-pojistovny-svazuje-evropska-regulace/c:13193/.

OECD. *The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector* [online]. © OECD 2020, 28. 1. 2020 [cit. 21. 2. 2022]. Dostupné z: https://www.oecd.org/finance/Impact-Big-Data-AI-in-the-Insurance-Sector.htm.

Parlament ČR. *Sněmovní tisk 138/0. Vládní návrh zákona o zpracování osobních údajů* [online]. 28. 3. 2018, s. 34–57 [cit. 20. 2. 2022]. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?o=8&ct=138&ct1=0.

Policie ČR, 2021. Kyberkriminalita. In: *Policie.cz* [online]. © 2021 Policie ČR [cit. 2. 3. 2022]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx.

Právnická fakulta Univerzity Palackého v Olomouci. Rigorózní řízení. In: *Pf.upol.cz* [online]. V Olomouci: Univerzita Palackého v Olomouci [cit. 16. 2. 2022]. Dostupné z: https://www.pf.upol.cz/studenti/studium/rigorozni-rizeni/.

Report on Experience Gained in the Implementation of the GDPR [online]. Independent German Federal and State Data Protection Supervisory Authorities. November 2019 [cit. 20. 2. 2022]. Dostupné z: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/Evaluation-Report-German-DPAs-Clean.pdf.

SMEJKAL, Vladimír. Formy kybernetické kriminality a jejich možný vliv na pojišťovací praxi. *Pojistný obzor: časopis českého pojišťovnictví* [online]. 2020, (2), s. 44–51 [cit. 15. 2. 2022]. ISSN 2464-7381. Dostupné z: https://www.pojistnyobzor.cz/archiv/92-2020-2.

The New Physics of Financial Services: understanding how artificial intelligence is transforming the financial ecosystem [online]. World Economic Forum, August 2018 [cit. 20. 2. 2022]. Dostupné z: http://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf.

ÚOOÚ. K povinnosti provádět posouzení vlivu na ochranu osobních údajů. In: *Uoou.cz* [online]. 7. 2. 2018 [cit. 19. 2. 2022]. Dostupné z: https://www.uoou.cz/k-nbsp-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385.

ÚOOÚ. *Kontrola využití biometriky u klientů (UOOU-09654/18)* [online]. [cit. 22. 2. 2022]. Dostupné z: https://www.uoou.cz/kontrola-vyuziti-biometriky-u-klientu-uoou-09654-18/ds-6546.

ÚOOÚ. *Ohlášení porušení zabezpečení osobních údajů dle GDPR* [online]. [cit. 22. 2. 2022]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=46004.

ÚOOÚ. *Výroční zpráva 2018* [online]. ÚOOÚ, 2018 [cit. 19. 2. 2022]. ISBN 978-80-210--9225-9. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=33526.

Verizon Communications, 2021. Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report. In: *Verizon.com* [online]. New York: 13. 5. 2021 [cit. 2. 3. 2022]. Dostupné z: https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report.

WARREN, Samuel D. a BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review* [online]. 1890, 4(5) [cit. 16. 2. 2022]. Dostupné z: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

WOLF, Karel. Proč svět touží po blockchainu? In: *Marwick.cz* [online]. 1. 10. 2018 [cit. 16. 2. 2022]. Dostupné z: https://www.marwick.cz/tema/svet-na-blockchainu.

Seznam použitých právních předpisů

Evropské a mezinárodní právní předpisy

Article 29 Data Protection Working Party. *Guidelines on Automated individual decision--making and Profiling for the purposes of Regulation 2016/679* [online]. Brussels: Article 29 Data Protection Working Party, 3. 10. 2017 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/newsroom/article29/items/612053/en.

Article 29 Data Protection Working Party. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679* [online]. Brussels: Article 29 Data Protection Working Party, 4. 4. 2017 [cit. 19. 2. 2022]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

Article 29 Data Protection Working Party. *Guidelines on Data Protection Officers ('DPOs')* [online]. Brussels: Article 29 Data Protection Working Party, 13. 12. 2016 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

Article 29 Data Protection Working Party. *Guidelines on the right to "data portability"* [online]. Brussels: Article 29 Data Protection Working Party, 13. 12. 2016 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/newsroom/article29/items/611233/en.

Article 29 Data Protection Working Party. *Guidelines on Transparency under Regulation 2016/679* [online]. Brussels: Article 29 Data Protection Working Party, 11. 4. 2018 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

Article 29 Data Protection Working Party. *Ohlášení případů porušení zabezpečení osobních údajů* [online]. Brussels: Article 29 Data Protection Working Party, 25. 5. 2018 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guideline/personal-data-breach-notifications_cs.

Article 29 Data Protection Working Party. *Opinion 4/2007 on the concept of personal data* [online]. Brussels: Article 29 Data Protection Working Party, 20. 6. 2007 [cit. 19. 2. 2022]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

Article 29 Data Protection Working Party. *Working Document on the processing of personal data relating to health in electronic health records (EHR)* [online]. Brussels: Article 29 Data Protection Working Party, 15. 2. 2007 [cit. 20. 2. 2022]. Dostupné z*:* https://www.dataprotection.ro/servlet/ViewDocument?id=228.

Dodatkový protokol k úmluvě o lidských právech a biomedicíně o genetickém testování pro zdravotní účely. In: *Sbírka mezinárodních smluv* [online]. č. 41/2019, částka 27, s. 7597–7606 [cit. 22. 2. 2022]. Dostupné také z: https://www.mzcr.cz/ratifikace-dodatkoveho-protokolu-o-genetickem-testovani-pro-zdravotni-ucely/.

Dohoda o obchodu a spolupráci mezi EU a Spojeným královstvím o obchodu a spolupráci. In: *Úřední věstník* [online], L 149/10, 30. 4. 2021 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/info/strategy/relations-non-eu-countries/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_cs.

EDPB. *Doporučení 01/2021 o referenčním rámci pro odpovídající ochranu podle směrnice o prosazování práva* [online]. Brussels: EDPB, 2. 2. 2021 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_cs.

EDPB. *EDPB Annual Report 2019* [online]. Brussels: EDPB, 18. 5. 2020 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/publication-type/annual-report_en.

EDPB. *EDPB Strategy 2021–2023* [online]. EDPB, 15. 12. 2020 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/work-program/edpb-strategy-2021-2023_en.

EDPB. *EDPB Work Programme 2021/2022* [online]. Brussels: EDPB, 16. 3. 2021 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-work-programme-20212022_cs.

EDPB. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* [online]. Brussels: EDPB, 12. 2. 2019 [cit. 19. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under-0_en.

EDPB. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679* [online]. Brussels: EDPB, 25. 5. 2018 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_en.

EDPB. *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* [online]. Version 2.0. Brussels: 8. 10. 2019 [cit. 20. 2. 2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.

EDPB. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* [online]. Version 2.1. Brussels: EDPB, 12. 11. 2019 [16. 2. 2022]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

EDPS. *Opinion 7/2021 on the Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) 1060/2009, (EU) 648/2012, (EU) 600/2014 and (EU) 909/2014* [online]. Brussels: EDPS, 10. 5. 2021 [cit. 16. 2. 2022]. Dostupné z: https://edps.europa.eu/system/files/2021-05/2021-0203_d0943_opinion_digital_operational_resilience_for_the_financial_sector_en.pdf.

EDPB. *Stanovisko č. 5/2019 ke vzájemnému působení mezi směrnicí o soukromí a elektronických komunikacích a obecným nařízením o ochraně osobních údajů (GDPR), zejména pokud jde o příslušnost, úkoly a pravomoci úřadů pro ochranu údajů* [online]. EDPB, 12. 3. 2019 [cit. 19. 2. 2022]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_cs.pdf.

EK. *Návrh nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014* [online]. V Bruselu: 24. 9. 2020 [cit. 17. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0595.

EK. *Nová politika pro spotřebitele* [online]. V Bruselu, 2. 4. 2019 [cit. 16. 2. 2022]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/cs/IP_19_1755.

EK. *Sdělení Komise Evropskému parlamentu a Radě. Ochrana osobních údajů jakožto pilíř posílení postavení občanů a přístup EU k digitální transformaci – dva roky uplatňování obecného nařízení o ochraně údajů* [online]. V Lucemburku: 24. 6. 2020 [cit. 17. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?from=EN&uri=CELEX%3A52020DC0264.

EK. *Sdělení Komise Evropskému parlamentu a Radě. Pokyny k nařízení o rámci pro volný tok neosobních údajů v Evropské unii* [online]. V Bruselu: 29. 5. 2019 [cit. 19. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A250%3AFIN.

EK. *Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů. Evropská strategie pro data* [online]. V Bruselu: 19. 2. 2020 [cit. 16. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52020DC0066.

EK. *Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů o strategii EU v oblasti digitálních financí* [online]. V Bruselu: 24. 9. 2020 [cit. 16. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0591.

EK. *Společné sdělení Evropskému parlamentu a Radě. Strategie kybernetické bezpečnosti EU pro digitální dekádu* [online]. V Bruselu: 16. 12. 2020 [cit. 19. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52020JC0018.

EK. *Zpráva Komise Evropskému parlamentu, Radě a Evropskému hospodářskému a sociálnímu výboru. Zpráva o dopadech umělé inteligence, internetu věcí a robotiky na bezpečnost a odpovědnost* [online]. V Bruselu: 19. 2. 2020 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020DC0064&from=en.

EP. *Návrh zprávy o umělé inteligenci v digitálním věku (2020/2266(INI))* [online]. Štrasburk: 2. 11. 2021 [cit. 20. 2. 2022]. Dostupné z: https://www.europarl.europa.eu/doceo/document/AIDA-PR-680928_CS.pdf.

EPrivacy. In: *Úřední věstník* [online], L 201, 31. 7. 2002, s. 37–47 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32002L0058.

European Commission. *Commission implementing decision of 28. 6. 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (Text with EEA relevance)* [online]. Brussels: 28. 6. 2021 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

European Commission. *Commission staff working document Accompanying the document Communication from the commission to the European parliament and the council Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation* [online]. Brussels: 24. 6. 2020 [cit. 19. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0115.

European Commission. *Commission staff working document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy* [online]. Brussels: 10. 1. 2017 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0002.

European Commission. Shaping Europe's Digital Future. In: *Ec.europa.eu* [online]. 19. 2. 2020 [cit. 20. 2. 2022]. Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en.

European Commision. *White Paper on Artificial Intelligence: a European approach to excellence and trust* [online]. Brussels: 19. 2. 2020 [cit. 16. 2. 2022]. Dostupné z: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

European Data Protection Board. *Guidelines 05/2020 on consent under Regulation 2016/679*. Version 1.1. [online]. Brussels: EDPB, 4. 5. 2020 [19. 2. 2022]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

Guidelines on the application of Council Directive 2004/113/EC to insurance, in the light of the judgment of the Court of Justice of the European Union in Case C-236/09 (Test-Achats) (Text with EEA relevance). *Official Journal of the European Union* [online]. 13 January 2012, 11(1) [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012XC0113(01)&from=EN.

HEISS, Helmut. *The Principles of European Insurance Contract Law: an optional instrument?* [online]. Brussels: © European Parliament, 2010 [cit. 20. 2. 2022]. Dostupné z: http://www.europarl.europa.eu/document/activities/cont/201004/20100430ATT73919/20100430ATT73919EN.pdf.

Hodnotící zpráva EK o provádění obecného nařízení o ochraně OÚ dva roky od začátku jeho uplatňování. Usnesení EP ze dne 25. 3. 2021 o hodnotící zprávě EK, o provádění obecného nařízení, o ochraně OÚ dva roky od začátku jeho uplatňování (2020/2717(RSP) [online]. In: *Úřední věstník* [online], C 494/11, 25. 3. 2021 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52021IP0111&from=EN.

IDD. In: *Úřední věstník* [online], L 352, 9. 12. 2014 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32016L0097.

LZPEU. In: *Úřední věstník* [online], C 326(2), 26. 10. 2012, s. 391–407 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex%3A12012P%2FTXT.

Nařízení EP a Rady (ES) č. 1882/2003 ze dne 29. 9. 2003, o přizpůsobení ustanovení týkajících se výborů, které jsou nápomocny EK při výkonu jejích prováděcích pravomocí, stanovených v právních aktech Rady a přijatých postupem podle čl. 251 *Smlouvy o ES*, ustanovením rozhodnutí 1999/468/ES. In: *Úřední věstník* [online]. L 284, 31. 10. 2003, s. 1 až 53 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32003R1882&from=EN.

Nařízení EP a Rady (EU) 2018/1807 ze dne 14. 11. 2018, o rámci pro volný tok neosobních údajů v EU. In: *Úřední věstník* [online]. L 303, 28. 11. 2018, s. 59–68 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32018R1807.

Nařízení EP a Rady (EU) č. 1094/2010 ze dne 24. 11. 2010, o zřízení Evropského orgánu dohledu (Evropského orgánu pro pojišťovnictví a zaměstnanecké penzijní pojištění), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí EK 2009/79/ES. In: *Úřední věstník* [online]. L 331, 15. 12. 2010, s. 48–83 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:32010R1094.

NIS. In: *Úřední věstník* [online], L 194, 19. 7. 2016, s. 1–30 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX%3A32016L1148.

PRIIPs. In: *Úřední věstník* [online]. L 352, 9. 12. 2014 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?from=EN&uri=CELEX%3A32014R1286.

SFEU (konsolidované znění). In: *Úřední věstník* [online], C 326, 26. 10. 2012, s. 47–390 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX%3A12012E%2FTXT.

OECD. *Přehled: směrnice OECD o ochraně soukromí a přeshraničních tocích osobních údajů* [online]. © OECD, 2003 [cit. 16. 2. 2022]. Dostupné z: https://www.oecd.org/digital/ieconomy/15589535.pdf.

OECD. *Recommendation of the Council on Artificial Intelligence* [online]. Paris: OECD Legal Instruments, 22. 5. 2019 [cit. 20. 2. 2022]. Dostupné z: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

SII. In: *Úřední věstník* [online], L 335, 17. 12. 2009, s. 1–155 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX%3A32009L0138.

Směrnice EP a Rady (EU) 2015/849 ze dne 20. 5. 2015, o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení EP a Rady (EU) č. 648/2012 a o zrušení směrnice EP a Rady 2005/60/ES a směrnice EK 2006/70/ES. In: *Úřední věstník* [online], L 141(73), 5. 6. 2015 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?from=EN&uri=CELEX%3A32015L0849.

Směrnice EP a Rady (EU) 2020/1828 ze dne 25. 11. 2020, o zástupných žalobách na ochranu kolektivních zájmů spotřebitelů a o zrušení směrnice 2009/22/ES. In: *Úřední věstník* [online], L 409, 4. 12. 2020, s. 1–27 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32020L1828.

Směrnice EP a Rady (EU) 2021/2118 ze dne 24. 11. 2021, kterou se mění směrnice 2009/103/ES, o pojištění občanskoprávní odpovědnosti z provozu motorových vozidel a kontrole povinnosti uzavřít pro případ takové odpovědnosti pojištění. In: *Úřední věstník* [online], L 430(64), 2. 12. 2021, s. 1–23 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:L:2021:430:FULL&from=EN.

Směrnice EP a Rady 2002/65/ES ze dne 23. 9. 2002, o uvádění finančních služeb pro spotřebitele na trh na dálku a o změně směrnice Rady 90/619/EHS a směrnic 97/7/ES a 98/27/ES. In: *Úřední věstník* [online], L 271, 9. 10. 2002, s. 16–24 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:32002L0065.

Směrnice EP a Rady 2011/83/EU ze dne 25. 10. 2011, o právech spotřebitelů, kterou se mění směrnice Rady 93/13/EHS a směrnice EP a Rady 1999/44/ES a ruší se směrnice Rady 85/577/EHS a směrnice EP a Rady 97/7/ES. In: *Úřední věstník* [online], L 304, 22. 11. 2011, s. 64–88 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:32011L0083.

Směrnice EP a Rady 2015/2302 ze dne 25. 11. 2015, o souborných cestovních službách a spojených cestovních službách, o změně nařízení EP a Rady (ES) č. 2006/2004 a směrnice EP a Rady 2011/83/EU a o zrušení směrnice Rady 90/314/EHS. In: *Úřední věstník* [online],

L 326, 11. 12. 2015 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?from=EN&uri=CELEX%3A32015L2302.

Směrnice Rady 2004/113/ES ze dne 13. 12. 2004, kterou se zavádí zásada rovného zacházení s muži a ženami v přístupu ke zboží a službám a jejich poskytování. In: *Úřední věstník* [online], L 373, 21. 12. 2004, s. 37–43 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX:32004L0113.

Směrnice Rady ze dne 25. 7. 1985, o sbližování právních a správních předpisů ČS týkajících se odpovědnosti za vadné výrobky. In: *Úřední věstník* [online], L 210, 7. 8. 1985, s. 29–33 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:31985L0374.

SEU (konsolidované znění). In: *Úřední věstník* [online], C 326, 26. 10. 2012, s. 13–390 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=celex%3A12012M%2FTXT.

STATE OF CALIFORNIA. *Senate Bill No. 327/886, An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy* [online]. 28. 9. 2018 [cit. 22. 2. 2022]. Dostupné z: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

Usnesení EP ze dne 16. 2. 2017 obsahující doporučení EK o občanskoprávních pravidlech pro robotiku (2015/2103(INL)). In: *Úřední věstník* [online], C252/239, 18. 7. 2018, s. 239–257 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52017IP0051.

Úmluva na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie a medicíny. Úmluva o lidských právech a biomedicíně. In: *Série evropských úmluv* [online], č. 164 [cit. 22. 2. 2022]. Dostupné také z: https://www.lf3.cuni.cz/3LF-426-version1-umluva_o_lidskych_pravech_a_biomedicine.pdf.

ÚOOÚ. *Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat ve znění jejího protokolu CETS č. 223: pracovní překlad* [online]. ÚOOÚ, 28. 1. 1981 [cit. 16. 2. 2022]. Dostupné z: https://rm.coe.int/1680994818.

Národní právní předpisy

ČNB. *Dohledový benchmark č. 4/2018 k určitosti stanovení rozsahu pojištění včetně výluk z pojištění* [online]. Praha: 13. 12. 2018 [cit. 20. 2. 2022]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-trh/.galleries/vykon_dohledu/dohledove_benchmarky/download/dohledovy_benchmark_2018_04.pdf.

OZ. In: *ASPI* [právní IS]. Praha: Wolters Kluwer, 2012 [cit. 3. 3. 2022]. ISSN 2336-517X. Dostupné z: https://www.aspi.cz/products/lawText/1/74907/1/2/zakon-c-89-2012-sb-obcansky-zakonik.

Zákon č. 37/2004 Sb., o pojistné smlouvě a o změně souvisejících zákonů (zákon o pojistné smlouvě). In: *ASPI* [právní IS]. Praha: Wolters Kluwer, 2004 [cit. 3. 3. 2022]. ISSN 2336-517X. Dostupné z: https://www.aspi.cz/products/lawText/1/57259/1/2/zakon-c-37-2004-sb-o-pojistne-smlouve-a-o-zmene-souvisejicich-zakonu-zakon-o-pojistne-smlouve.

Zákon č. 101/2000 Sb., o ochraně OÚ a o změně některých zákonů. In: *ASPI* [právní IS]. Praha: Wolters Kluwer, 2000 [cit. 3. 3. 2022]. ISSN 2336-517X. Dostupné z: https://www.aspi.cz/products/lawText/1/49228/1/2.

Zákon č. 110/2019 Sb., o zpracování OÚ. In: *ASPI* [právní IS]. Praha: Wolters Kluwer, 2019 [cit. 3. 3. 2022]. ISSN 2336-517X. Dostupné z: https://www.aspi.cz/products/lawText/1/91825/1/2.

Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování OÚ. In: *ASPI* [právní IS]. Praha: Wolters Kluwer, 2019 [cit. 3. 3. 2022]. ISSN 2336-517X. Dostupné z: https://www.aspi.cz/products/lawText/1/91826/0/2/zakon-c-111-2019-sb-kterym-se-meni-nektere-zakony-v-souvislosti-s-prijetim-zakona-o-zpracovani-osobnich-udaju/zakon-c-111-2019-sb-kterym-se-meni-nektere-zakony-v-souvislosti-s-prijetim-zakona-o-zpracovani-osobnich-udaju.

Zákon č. 170/2018 Sb., o distribuci pojištění a zajištění. In: *ASPI* [právní IS]. Praha: Wolters Kluwer, 2018 [cit. 3. 3. 2022]. ISSN 2336-517X. Dostupné z: https://www.aspi.cz/products/lawText/1/90613/1/2.

Zákon č. 181/2014 Sb., o KB a o změně souvisejících zákonů (zákon o KB). In: *ASPI* [právní IS]. Praha: Wolters Kluwer, 2014 [cit. 3. 3. 2022]. ISSN 2336-517X. Dostupné z: https://www.aspi.cz/products/lawText/1/82522/1/2.

Zákon č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů (antidiskriminační zákon). In: *ASPI* [právní IS]. Praha: Wolters Kluwer, 2009 [cit. 3. 3. 2022]. ISSN 2336-517X. Dostupné z: https://www.aspi.cz/products/lawText/1/68893/1/2/zakon-c-198-2009-sb-o-rovnem-zachazeni-a-o-pravnich-prostredcich-ochrany-pred-diskriminaci-a-o-zmene-nekterych-zakonu-antidiskriminacni-zakon/zakon-c-198-2009-sb-o-rovnem-zachazeni-a-o-pravnich-prostredcich-ochrany-pred-diskriminaci-a-o-zmene-nekterych-zakonu-antidiskriminacni-zakon.

Zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o KB a o změně souvisejících zákonů (zákon o KB), ve znění zákona č. 104/2017 Sb., a některé další zákony. In: *Zákony pro lidi* [online]. 1. 8. 2017 [cit. 3. 3. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205.

Zákon č. 219/2021 Sb., kterým se mění zákon č. 6/1993 Sb., o ČNB, ve znění pozdějších předpisů. In: *ASPI* [právní IS]. Praha: Wolters Kluwer, 2021 [cit. 3. 3. 2022]. ISSN 2336-517X. Dostupné z: https://www.aspi.cz/products/lawText/1/96632/1/2/zakon-c-219-2021-sb-kterym-se-meni-zakon-c-6-1993-sb-o-ceske-narodni-bance-ve-zneni-pozdejsich-predpisu.

Zákon č. 277/2009 Sb., o pojišťovnictví. In: *ASPI* [právní IS]. Praha: Wolters Kluwer, 2009 [cit. 3. 3. 2022]. ISSN 2336-517X. Dostupné z: https://www.aspi.cz/products/lawText/1/69215/1/2/zakon-c-277-2009-sb-o-pojistovnictvi/zakon-c-277-2009-sb-o-pojistovnictvi.

Zákon č. 500/2004 Sb., správní řád. In: *ASPI* [právní IS]. Praha: Wolters Kluwer, 2004 [cit. 3. 3. 2022]. ISSN 2336-517X. Dostupné z: https://www.aspi.cz/products/lawText/1/58370/1/2/zakon-c-500-2004-sb-spravni-rad.

Zákon č. 634/1992 Sb., o ochraně spotřebitele. In: *ASPI* [právní IS]. Praha: Wolters Kluwer, 1992 [cit. 3. 3. 2022]. ISSN 2336-517X. Dostupné z: https://www.aspi.cz/products/lawText/1/40431/1/2.

Judikatura

ČR. *Nález Ústavního soudu ze dne 11. listopadu 2013 sp. zn. I. ÚS 3512/11* [online]. 11. 11. 2013 [cit. 20. 2. 2022]. Dostupné z: http://nalus.usoud.cz/Search/GetText.aspx?sz=1-3512-11.

ČR. *Rozsudek NSS 1 As 238/2021–33* [online]. V Brně: 11. 11. 2021 [cit. 19. 2. 2022]. Dostupné z: http://www.nssoud.cz/files/SOUDNI_VYKON/2021/0238_1As__2100033S_20211111111159.pdf.

ČR. *Rozsudek NSS 9 As 34/2008–68* [online]. V Brně: 12. 2. 2009 [cit. 22. 2. 2022]. Dostupné z: http://www.nssoud.cz/files/SOUDNI_VYKON/2008/0034_9As__0800068A_prevedeno.pdf.

ESLP. *Rozhodnutí velkého senátu Evropského soudu pro lidská práva ze dne 4. prosince 2008 ve věci S. a Marper proti Spojenému království* [online]. Wolters Kluwer, 4. 12. 2008 [cit. 20. 2. 2022]. Dostupné z: http://eslp.justice.cz/justice/judikatura_eslp.nsf/0/EA8CFA7D862952D2C1258487002E9626/$file/S.%20a%20Marper%20proti%20Spojen%C3%A9mu%20kr%C3%A1lovstv%C3%AD_rozsudek.pdf?open&.

SDEU. *Rozsudek Soudního dvora (velkého senátu) ze dne 1. března 2011. Association belge des Consommateurs Test-Achats ASBL, Yann van Vugt, Charles Basselier proti Conseil des ministres*, C-236/09 [online]. V Bruselu: 1. 3. 2011 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:62009CJ0236&from=EN.

SDEU. *Rozsudek Soudního dvora (velkého senátu) ze dne 1. října 2019. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. vs. Planet49 GmbH*, C-673/17 [online]. 1. 10. 2019 [cit. 20. 2. 2022]. Dostupné z: http://curia.europa.eu/juris/liste.jsf?num=C-673/17.

SDEU. *Rozsudek Soudního dvora (velkého senátu) ze dne 6. října 2015. Maximillian Schrems vs. Data Protection Commissioner*, C-362/14 [online]. 6. 10. 2015 [cit. 20. 2. 2022]. Dostupné z: https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=112515.

SDEU. *Rozsudek Soudního dvora (velkého senátu) ze dne 18. července 2017. Evropská komise vs. Patrick Breyer*, C-213/15 P [online]. 18. 7. 2017 [20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A62015CJ0213.

SDEU. *Rozsudek Soudního dvora ze dne 4. října 2018, Société Colas Est vs. France*, C-416/17 [online]. 4. 10. 2018 [cit. 19. 2. 2022]. Dostupné z: https://curia.europa.eu/juris/document/document.jsf?text=&docid=206426&pageIndex=0&doclang=EN&.

SDEU. *Rozsudek Soudního dvora ze dne 5. února 1963*, C-26/62 [online]. V Lucemburku: 5. 2. 1963 [cit. 16. 2. 2022]. Dostupné z: https://curia.europa.eu/arrets/TRA-DOC-CS-ARRET-C-0026-1962-200406974-05_01.html.

SDEU. *Rozsudek Soudního dvora ze dne 10. října 1973. Fratelli Variola S.p.A. proti Amministrazione italiana delle Finanze*, C-34/73 [online]. 10. 10. 1973 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:61973CJ0034.

SDEU. *Rozsudek Soudního dvora ze dne 14. prosince 1971. Politi s.a.s. proti Ministero delle Finanze della Republica Italiana*, C-43/71 [online]. 14. 12. 1971 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX:61971CJ0043.

SDEU. *Rozsudek Soudního dvora ze dne 16. července 2020. Data Protection Commissioner vs. Facebook Ireland Limited a Maximillian Schrems*, C-311/18 [online]. 16. 7. 2020 [cit. 20. 2. 2022]. Dostupné z: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=541779.

SDEU. *Rozsudek Soudního dvora ze dne 28. března 1985. Komise Evropských společenství proti Italské republice*, C-272/83 [online]. 28. 3. 1985 [cit. 20. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:61983CJ0272.

Volkszählung, sp. zn. Az 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/ 83, bod 172–175. Dostupné z: https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BVerfG&Datum=15.12.1983&Aktenzeichen=1%20BvR%20209%2F83.