FAKULTA DOPRAVNÍ ČVUT V PRAZE

ROWAN LEGAL

TL03000691

Ochrana soukromí a osobních údajů v systémech autonomního řízení

Certifikovaná metodika nastavení vhodných opatření snižujících rizika nepřiměřeného zásahu do soukromí

Řešitelé projektu:

ČVUT v Praze, Fakulta dopravní, Konviktská 20, 110 00 Praha 1

ROWAL LEGAL, advokátní kancelář s.r.o., Na Pankráci 1683/127, 140 00 Praha 4

Vypracovali:

doc. Ing. Zdeněk Lokaj, Ph.D., LL.M.

prof. Ing. Tomáš Zelinka, CSc.

Ing. Martin Šrotýř, Ph.D.

Ing. Miroslav Vaniš, Ph.D.

JUDr. Martin Flaškár

Mgr. Jakub Jirovský

Obsah

1 Seznam zkratek

Zkratka	Český význam	Anglický význam
ABS	Protiblokovací systém	Anti-lock Brake System
C-ITS	Kooperativní inteligentní dopravní systém	Cooperative Intelligent Transport System
ČVUT	České vysoké učení technické v Praze	Czech Technical University in Prague
DENM	Typ zprávy používaný v rámci kooperativních systémů	Decentralized Environmental Notification Message
DPIA	Posouzení vlivu na ochranu osobních údajů	Data Protection Impact Assessment
eCall	Automatický systém tísňového volání	Electronic Emergency Call
EDPB	Evropský sbor pro ochranu osobních údajů	European Data Protection Board
EDR	Záznamové zařízení událostí	Event Data Recorder
EN	Evropská norma	European standard
ESP	Elektronický stabilizační program	Electronic Stability Program
EU	Evropská unie	European Union
GDPR	Obecné nařízení ochrany osobních údajů	General Data Protection Regulation
GNSS	Globální navigační satelitní systém	Global Navigation Satellite System
OBU	Palubní jednotka	On-board unit
RL	ROWAN LEGAL	
SAE	Společnost automobilových inženýrů	Society of Automotive Engineers
SMS	Služba krátkých textových zpráv	Short Message Service
V2I	Komunikace mezi vozidlem a infrastrukturou	Vehicle-2-Infrastructure
V2X	Komunikace mezi vozidlem a dalším zařízením	Vehicle-2-X

2 Shrnutí metodiky

Základním cílem této metodiky je subjektům, pro které je tato metodika určena, poskytnout informace o vybraných povinnostech vyplývajících z aktuální právní regulace v oblasti ochrany osobních údajů v autonomních vozidlech. Konkrétně tato metodika obsahuje návrh opatření a doporučení na základě vstupních definovaných parametrů, která mají pro uživatele metodiky představovat určitá vodítka a možné kroky za účelem zajištění plnění daných povinností dle právních předpisů na ochranu osobních údajů.

Tato certifikovaná metodika vznikla jako jeden z výsledků výzkumného projektu „TL03000691 Ochrana soukromí a osobních údajů v systémech autonomního řízení“, v rámci kterého byla rovněž zpracována necertifikovaná metodika „Metodika analýzy zpracování osobních údajů a hodnocení míry zásahu do soukromí“, která je komplementární k tomuto dokumentu a na kterou je v textu několikrát odkazováno, neboť jejím hlavním obsahem je výpočet rizikovosti včetně jeho detailního popisu a zhodnocení zásahu do soukromí.

Struktura této certifikované metodiky je rozdělena do 8 kapitol. Po tomto shrnutí jsou v kapitole 3 popsány hlavní cíle certifikované metodiky.

V kapitole 4 je popsán celý metodický postup k získání doporučení pro implementaci vhodných opatření pro zajištění odpovídající míry ochrany osobních údajů a eliminaci rizika nepřiměřeného zásahu do soukromí v rámci systémů autonomního řízení. Nejprve je nutné stanovit, jaká data jsou zpracovávána v rámci autonomního systému či zařízení. V rámci této metodiky jsou tato data rozdělena do několika oblastí (např. lokalizační data, audiovizuální data apod.). Přesnější popis těchto skupin dat lze nalézt v kapitole 4.1.1. Kromě toho by měl uživatel metodiky u všech výše zmíněných oblastí dat stanovit některé doplňující parametry těchto dat, jako např. doba zpracování či rozsah dat. Popis těchto parametrů je předmětem kapitoly 4.1.2.

Z legislativního hlediska rozlišujeme několik typů subjektů zpracovávající osobní údaje, přičemž pro každý z nich platí částečně jiné povinnosti. Popis těchto subjektů včetně jejich povinností jsou součástí kapitoly 4.2 včetně jejich podkapitol. Cílem této metodiky není stanovit typ tohoto subjektu, ale zároveň je nutné, aby si uživatel této metodiky tento subjekt určil.

Aby subjekt zpracovávající osobní údaje byl v souladu s povinnostmi dle právních předpisů ochrany osobních údajů, zejm. pak dle GDPR, musí mimo jiné stanovit i konkrétní účel zpracování osobních údajů. Specifikace tohoto účelu závisí na jeho rozhodnutí, a tudíž nedochází k výběru z uzavřeného a předdefinovaného seznamu, jak je tomu například u právního titulu. Typické příklady stanovení účelu zpracování osobních údajů v rámci systémů autonomního řízení lze nalézt v kapitole 4.3 a stanovení odpovídajícího právního titulu je předmětem kapitoly 4.4.

Kapitola 4.5 se pak zabývá zhodnocením míry zásadu do soukromí subjektu údajů, kdy představuje jednotlivé úrovně takového zásahu a variantnost dílčích vstupů, na základě kterých je příslušná úroveň zásahu do soukromí stanovena.

Stěžejní částí této metodiky je kapitola 4.6 zabývající se návrhem samotných opatření. Na základě konkrétních vstupů od uživatelů této metodiky, spočívajících ve specifikaci konkrétních parametrů a atributů příslušného zpracování, mu budou doporučena pro něj vhodná opatření. Zajištění takových opatření rovněž pomůže plnit další povinnost dle GDPR, kterou je zavedení technických a organizačních opatření v takovém rozsahu, aby byla zaručena odpovídající úroveň zabezpečení v souladu s příslušnými riziky zpracování osobních údajů.

Speciálně pro účely této metodiky byla také vytvořena webová aplikace, která je přímo určena uživatelům metodiky, kteří budou osobní údaje zpracovávat. V jejím rámci je možné zadat vstupy z podkapitol 4.1.1 Kategorie osobních údajů a 4.1.2 Parametry osobních údajů. Na základě příslušných parametrů a stanovené úrovni rizikovosti aplikace automatizovaně identifikuje a doporučí možná opatření. Popis této aplikace lze nalézt v kapitole 5.

Kapitola 6 má za cíl srovnat přístup k problematice osobních údajů v autonomní vozidle s již zpracovanými dostupnými materiály. Kapitola 7 potom shrnuje hlavní přínosy této metodiky a kapitola 8 se zabývá ekonomickými aspekty v této oblasti. Poslední kapitola již jen pouze uvádí seznam použitých zdrojů.

2.1 Publikace související s metodikou

Přípravě a certifikaci této metodiky předcházela odborná publikace

Lokaj, Z., Šrotýř, M., Flaškár, M., Jirovský, J. Ochrana osobních údajů v systémech autonomního řízení. Co je nezbytné pro bezpečné fungování a jak toho dosáhnout? In. Revue pro právo a technologie, č. 24, Brno: Masarykova univerzita, 2021, ISSN: 1804-5383

3 Úvod

V dnešní době je odvětví autonomní mobility velmi rychle se rozvíjející, a to hlavně z hlediska technologického. Řeší se vývoj a zdokonalování systémů na rozpoznávání obrazu, rozvoj matematických modelů, podle kterých se autonomní vozidlo pohybuje atd.

Pokud se na tuto problematiku podíváme z legislativního hlediska, zjistíme, že obecně se řeší hlavně oblasti související s provozem autonomních vozidel a případnou odpovědností za způsobenou škodu. Mediální zájem budí speciálně řešení nehod autonomních vozidel a také etické otázky související s případnými úmrtími či těžkými zraněními na základě rozhodnutí algoritmu autonomního vozidla.

Z druhé strany ochrana osobních údajů se začala řešit hlavně v návaznosti na účinnost přímo aplikovatelného nařízení GDPR z května roku 2018. Na internetu lze nalézt mnoho návodů pojednávajících o tom, jak by měla malá firma či e-shop zpracovávat osobní údaje tak, aby zajistila soulad s GDPR.

Trochu stranou však zatím zůstává oblast osobních údajů v oblasti autonomní mobility. Každé autonomní vozidlo, resp. jeho součásti budou zpracovávat velké objemy dat, kdy řada z těchto dat bude splňovat definici osobního údaje dle čl. 4 GDPR. Pro ukládání a zpracování těchto dat ovšem platí stejné legislativní předpisy jako v jiných oblastech, jinými slovy i zpracování osobních údajů v autonomním vozidle, resp. jeho součásti, musí být v souladu s GDPR.

Je proto na místě řešit, jak správně nakládat s osobními údaji získanými v rámci provozu autonomních vozidel. Tato metodika by měla být určena právě pro tyto účely, tj. měla by poskytovat dílčí doporučení pro budoucí výrobce autonomních vozidel, jejich dodavatele či provozovatele služeb, jak správně nakládat s osobními údaji v případech, kdy se budou touto oblastí zabývat.

3.1 Stanovení cílů metodiky

Nařízení GDPR obsahuje řadu zásadních povinností, které musí příslušné subjekty při zpracování osobních údajů plnit. Pro popisovanou oblast této metodiky je zásadní článek 25 GDPR, dle kterého má správce osobních údajů zavést vhodná technická a organizační opatření, a to jak v době určení prostředků pro zpracování, tak i v průběhu zpracování daného opatření.

V současnosti nejsou dostupná závazná doporučení, která by se zabývala opatřeními GDPR v oblasti autonomních vozidel. Správcům jsou dostupné informace o obecných postupech a zásadách, kterých by se měl v případě používání GDPR dat držet.

Hlavními cíli metodiky je na základě definovaných vstupů identifikovat rizikovost popsaného zpracování osobních údajů a doporučit implementaci konkrétních technických a organizačních opatření, aby konkrétní správce zajistil plnění jeho povinností dle článku 25 GDPR. Doporučení obsažená v této metodice mohou správci rovněž využít při přípravě na provedení posouzení vlivu na ochranu osobních údajů dle článku 35 GDPR.

Opatření navržená metodikou není možné garantovat v obecné rovině. Zákonnost zpracování osobních údajů je nutné ověřit vždy na konkrétním případě a zohlednit veškerá specifika, která není možné obecným postupem postihnout.

3.2 Východiska a best practices

Zpracování osobních údajů v systémech autonomního řízení je poměrně novou oblastí odborného bádání, což v konečném důsledku znamená, že doposud nejsou dostupné hlubší zkušenosti. Tato metodika proto mj. vychází z dosud publikovaných výstupů a doporučení Evropského sboru pro ochranu osobních údajů (European Data Protection Board), který se již zabýval problematikou zpracování osobních údajů v dopravních systémech, mj. v dokumentech:

- Stanovisko 13/2011 ke geolokalizačním službám u inteligentních mobilních zařízení; [1]
- Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Systems (C-ITS)[2];
- Guidlines 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[3];
- Guidlines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications[4].

Současně bylo možné využít také dokumenty Car2Car Communication Consortium, které se rovněž problematikou ochrany osobních údajů a právní konformitu jejich zpracování zabývalo[5]. V neposlední řadě se oblastí zpracování osobních údajů v C-ITS systémech zabývala pracovní skupina Data Protection v rámci C-ITS platformy.

Při hodnocení parametrů a rizikovosti zpracování jednotlivých typů, resp. skupin osobních údajů se dále brala v úvahu kybernetická bezpečnost, která je již podstatně dále a disponuje mnoho postupy a ověřených metodami, jak objektivně zhodnotit rizikovost daného systému či řešení. [6]

---

[1] PARTY, A. D. P. W. Opinion 13/2011 on geolocation services on smart mobile devices. Opgeroepen op August, 2011, 7: 2013.

2 PARTY, A. D. P. W. Opinion 03/2017 on processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS).

[3] EUROPEAN DATA PROTECTION BOARD. 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. 2019.

[4] EUROPEAN DATA PROTECTION BOARD. Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications. 2020.

[5] Privacy. *Car-2-car communication consortium* [online]. Braunschweig, Germany, 2018 [cit. 2023-01-18]. Dostupné z: https://www.car-2-car.org/service/privacy

[6] MANSON, C. G.; GORNIAK, S. Recommendations for a methodology of the assessment of severity of personal data breaches. *ENISA (European Union Agency for Network and Inform. Security) Working Document, v1. 0*, 2013.

4 Popis metodiky

K naplnění cílů této metodiky stanovených v předchozí kapitole, tj. doporučení odpovídajících technických a organizačních opatření, je ze strany subjektu nezbytné provést několik kroků. Jedná se především o identifikaci, jaká data budou zpracovávána, za jakým účelem, z jakého právního titulu atd. Tyto informace jsou nutnou podmínkou pro možnost posouzení rizik zpracování dat a navržení příslušného opatření.

Následující podkapitoly se věnují popisu tohoto procesu. Důležitý podpůrným nástrojem této metodiky je vytvořený software, který provází celým procesem sběru informací od subjektu a je schopen na základě zjištění stanovit rizikovost zpracování údajů a stanovit doporučení. Popis nástroje je obsahem kapitoly 5).

4.1 Analýza osobních údajů, které jsou v rámci systému autonomního řízení zpracovávány

Jako první krok musí zapojený subjekt v pozici potenciálního správce zhodnotit, zda a v jakém případě bude v systému zpracovávat osobní údaje. Metodika pro ten účel uvádí:

1. výčet kategorií osobních údajů, které by potenciální správce mohl zpracovávat,
2. možnost určení, zda daný subjekt modelově jako správce osobních údajů vystupuje,
3. katalog určení účelu pro zpracování, a
4. zákonné důvody pro zpracování osobních údajů.

Je nad rámec této metodiky zkoumat každý jednotlivý datový záznam, a proto k nim metodika přistupuje formou kategorií osobních údajů. Tato kategorizace byla zvolena na základě již dříve provedených analýz prováděných v rámci tohoto projektu a vycházela ze společných znaků jednotlivých datových záznamů, které bylo možné sdružit.

4.1.1 Kategorie osobních údajů a jejich výčet

Data zpracovávaná v rámci vozidlových systémů a systémů autonomního řízení můžeme popsat dle použitých technologií:

1) Data podporující řízení motorového vozidla
   a) Senzorové jednotky (senzory, radary, kamery, lidar, ABS, ESP) – na tyto senzory vozidla spoléhají při řízení vozidla, jejich počet a kvalita musí odpovídat požadavkům na kvalitu a četnost vstupních dat pro algoritmy a systémy autonomního řízení.
   b) Elektronické řídící jednotky (či obdobná zařízení) – zpracovávají informace ze senzorů, provádějí diagnostiku, detekují chyby, vydávají povely (aktory) apod.

2) Obrazová data

a) Kamery zachycující okolí vozidla – pomáhají vlastnímu řízení vozidla, mohou ale i identifikovat okolní vozidla a kolemjdoucí osoby;
b) Kamery zachycující vnitřek vozidla – například systémy na sledování únavy řidiče, pro zabezpečení apod.

3) Data o řízení vozidla (a o nehodách)
   a) EDR jednotka – záznam dat pro analýzu jízdy a forenzní analýzy v případě dopravní nehody či nestandardního stavu systému. U systémů autonomního řízení je možný sběr i dalších dat, než jen ze senzorů a řídích jednotek, ale rovněž data o uživateli vozidla, počtu pasažérů, styl jízdy apod.

4) Lokalizační a polohová data
   a) Navigační systémy – primárně data z GNSS systémů a již běžných doplňkových systémů jako například elektronický kompas, napojení na mobilní sítě apod. U systémů autonomního řízení se předpokládá potřeba většího rozlišení a také spojení například s akcelerometry, laserovými gyroskopy, lidary a 4G/5G sítěmi. Současně bude nutné mít velmi kvalitní mapové podklady s vysokým rozlišením, podle kterých budou algoritmy vyhodnocovat aktuální pozici a směr jízdy.
   b) V2X komunikace – polohu vozidla je možné zpřesňovat i s využitím komunikačních systémů krátkého dosahu, především se jedná o V2I komunikaci, kde komunikační zařízení na infrastruktuře má svou pevnou polohu a může poskytovat aktuální chybu detekce geografické pozice, případně mohou vozidlové systémy polohu dopočítat na základě zpoždění komunikačního kanálu.

5) Data z biometrických, biologických nebo zdravotních senzorů
   a) Biometrické, biologické nebo zdravotní senzory – data pro účely jednoznačné identifikace osob, pro které se používají otisky prstu, dlaně, scan obličeje, oční duhovka, charakteristika hlasu apod. V systémech autonomního řízení je možné sledovat stav identifikovaného řidiče, jeho chování či reflexy a na základě toho upravovat parametry systému. Současně je možné personalizovat různé služby a funkce systémů ve vozidlech, které se spouštějí na základě identifikace osob.

6) Audio data
   a) Vnitřní mikrofony – jsou určeny pro hlasové ovládání systémů a funkcí, případně ve spojení s telefonem i pro hlasové volání či diktování krátkých zpráv.
   b) Externí mikrofony – autonomní vozidla používají externí mikrofony jako dodatečné vstupy pro scanování svého okolí, tím pádem ale mohou detekovat i hovor náhodných kolemjdoucích.

7) Personalizovaná data
   a) Paměť ve vozidle – vozidla uchovávají data, která jsou využívána například pro tzv. infotainment, který může obsahovat řadu osobních údajů týkajících se subjektu údajů nebo například data z uživatelských zařízení a aplikací, získaná např. prostřednictvím propojení mobilních zařízení se systémem vozidla a využíváním specifických aplikací (jako je Apple CarPlay, Android Auto). Právě

napojení na mobilní zařízení je zásadním rizikem, neboť obsahují velké množství dat, spojených se subjektem údajů – seznam realizovaných hovorů, telefonní seznam, krátké textové zprávy (SMS, smart messaging aplikace), emaily apod.

Není možné vyjmenovat všechna data, která v autonomním vozidle budou proudit. Princip je takový, že subjekt identifikuje ty kategorie dat (může jich být samozřejmě i více), které zpracovává a s těmi pak bude pracovat i v dalších krocích.

4.1.2 Parametry kategorií osobních údajů

Ke každé kategorii z minulé podkapitoly je potřeba určit parametry, které poskytnou více informací pro zhodnocení rizikovosti a dále pro navrhnutí příslušných opatření. Nyní následuje jejich výčet:

1. Aktuálnost dat – jedná se o parametr toho, jak často jsou data aktualizována. Můžou být např. aktualizována průběžně (realtime) nebo pouze jednou za čas (každou hodinu, každý den apod.)

2. Doba uchování dat – z GDPR vyplývá, že osobní údaje mají být uchovávány pouze po dobu nezbytnou k naplnění účelu (délka doby uchování se tak může lišit v návaznosti na konkrétní účel). Čím je delší doba uchovávání, tím je větší riziko, že by mohlo dojít ke ztrátě či zneužití dat.

3. Rozsah dat – souvisí s rozmanitostí a i samotným objemem dat. Opět platí, čím větší rozsah dat, tím větší riziko.

4. Propojení k dalším datům – je parametr, který určuje, jak moc jsou data napojena na jiný datový soubor a zároveň se zvyšuje riziko zneužití ve chvíli, kdy by propojením dat vznikly další osobní údaje.

5. Třetí strana – zdrojem osobních údajů může být také třetí strana. V tu chvíli je stěžejní, v jakém postavení se tato třetí strana nachází, a jaké má vazby na další správce a zpracovatele (jestli vůbec).

6. Právní základ – souvisí s tím, na jakém právním titulu základě je zpracování osobních údajů prováděno.

7. Přenos dat – subjekt musí brát také v potaz, jaký rozsah dat je z celkového objemu přenášen a zároveň, jaké je přenosové médium toho přenosu.

Více o parametrech kategorií osobních údajů lze nalézt v metodice „Metodika analýzy zpracování osobních údajů a hodnocení míry zásahu do soukromí“, která je komplementární k tomuto dokumentu a kde jsou uvedeny i varianty těchto parametrů včetně informací o tom, jak tyto varianty ovlivňují celkovou rizikovost.

4.2 Určení subjektu z legislativního pohledu

Dalším krokem je určení postavení subjektu. Pro něj je stěžejní, jakým způsobem se podílí na zpracování osobních údajů, tedy např. zda rozhoduje o účelech a prostředcích zpracování sám, společně s jinými, či zda provádí zpracování pouze na základě pokynu a dle požadavků někoho jiného. Postavení subjektu je třeba vyhodnocovat ve vztahu ke konkrétním činnostem zpracování (při jedné činnosti může být subjekt správcem, zatímco při druhé činnosti může být v postavení zpracovatele):

a) Správce standardně sám určuje účely a prostředky zpracování, tj. důvod a způsob zpracování. Pokud tedy zapojený subjekt určí „proč“ a „jak“ by se osobní údaje měly zpracovávat, je správcem údajů. Postavení správce osobních údajů samozřejmě nevylučuje možnost využívat pro dílčí aspekty zpracování třetí osobu (zpracovatele).
b) Společný správce účely a prostředky zpracování, tedy „proč“ a „jak“ by se osobní údaje měly zpracovávat, určuje společně s dalším subjektem. Zastřešujícím kritériem existence společné správy je tedy společný podíl dvou nebo více subjektů na určení účelů a prostředků operace zpracování.
c) Zpracovatelem údajů bude subjekt v případě, že splňuje dvě základní podmínky: jedná se o samostatný subjekt ve vztahu ke správci a osobní údaje zpracovává jménem správce. Zpracovatel nesmí údaje zpracovávat jinak než podle pokynů správce, tzn., nesmí sám rozhodovat o zpracování či zpracovávat osobní údaje pro své vlastní účely nad rámec pokynů správce.

Podrobnější popis těchto subjektů včetně jejich povinností je předmětem následujících podkapitol.

4.2.1 Správce osobních údajů

Správcem se dle čl. 4 odst. 7 nařízení GDPR rozumí entita, která sama nebo společně s jinými určuje účely a prostředky zpracování osobních údajů, či které jsou účely a prostředky určeny právem členského státu. Základní povinností správce je pak zejména zavést v souvislosti se zpracováním osobních údajů taková technická a organizační opatření, která zajistí a umožní správci doložit, že zpracování je prováděno v souladu s nařízením GDPR. Těmito opatřeními by mělo být zejména zajištěno zabezpečení dat před neoprávněným přístupem nebo minimalizace údajů a rozsahu jejich zpracování s ohledem na účel zpracování. Tohle všechno jsou výzvy, se kterými se správci osobních údajů v rámci autonomního řízení budou muset vypořádat.

Veškerá opatření k ochraně osobních údajů a zajištění souladu správce s požadavky nařízení GDPR je nezbytné řádně dokládat v záznamech o činnostech zpracování, vedených u správce, resp. případně i doložit dozorovému úřadu. Jednou ze základních povinností správce dle nařízení GDPR je totiž povinnost umět prokázat, že postupuje v souladu s nařízením GDPR.

Za významnou je třeba považovat rovněž povinnost hlásit specifické incidenty dozorovému úřadu či v jistých případech dokonce samotným dotčeným subjektům údajů. Součástí ohlášení narušení jsou povinně popis povahy daného případu narušení, popis

pravděpodobných důsledků narušení, popis opatření přijatých či navržených s cílem vyřešit dané narušení apod.

4.2.2 Společní správci osobních údajů

Společnými správci jsou podle čl. 26 odst. 1 nařízení GDPR takoví správci, kteří pro dané zpracování společně stanoví jeho účely a prostředky. Současně platí, že v postavení společných správců jsou i takoví správci, kteří jsou jako společní správci určeni právními předpisy, které jim stanoví účely a prostředky zpracování.[7]

Pro účely společného správcovství je tedy nutné analyzovat, zda jsou údaje jednotlivými subjekty zpracovávány za totožným účelem. V případě, že více subjektů zpracovává stejné údaje, avšak za odlišným účelem, nebude se jednat o společné správcovství. Účel zpracování je totožný i v případě, že navazující operace zpracování prováděné jednotlivými správci mají odlišné dílčí cíle, avšak vždy směřují k jednotnému společnému účelu.[8]

Dále je nutné poukázat na skutečnost, že ke zpracování osobních údajů společnými správci nemusí standardně docházet zároveň. Obdobně účast jednotlivých společných správců na zpracování nemusí být rovnoměrná. To, zda se jedná o společné správce či nikoli, zcela závisí na faktickém stavu dané situace. Společné správcovství tedy zejména nelze vyloučit smluvně.

Obecnou nevýhodou postavení společných správců je nutnost umožnit subjektu údajů uplatnit svá práva u kteréhokoli z nich. Jako komplikované může na první pohled působit rovněž rozlišení, zdali subjekt údajů uplatňuje svá práva proti zpracování v souvislosti se systémem, kde jednotlivé subjekty vystupují jako společní správci, či pouze k danému konkrétnímu subjektu vůči zpracování, ve kterém subjekt vystupuje jako samostatný správce. V souvislosti s působením subjektu jako společného správce zároveň vzniká riziko vzniku odpovědnosti za porušení povinnosti stanovené Nařízením, ačkoli se takového porušení dopustil jiný společný správce. S tím souvisí i riziko vzniku společné a nerozdílné odpovědnosti v případě nejasného rozdělení jejích podílů v uzavřené dohodě. Poslední identifikovanou nevýhodou postavení subjektů jako společných správců je možnost jednoho subjektu vyjadřovat se k nakládání s osobními údaji jiným subjektem, pokud k takovému nakládání dochází v rámci vztahu společných správců.

4.2.3 Zpracovatel osobních údajů

Správce může pověřit zpracováním osobních údajů další entitu, tzv. zpracovatele, který bude zpracovávat osobní údaje na základě pokynu správce. Odpovědnými za ochranu

[7] V opačném případě by správci, jimž jsou účely a prostředky zpracování stanoveny právními předpisy, nikdy nemohli být společnými správci; rozpor mezi čl. 4 odst. 7 a čl. 26 odst. 1 nařízení GDPR v tomto směru lze mít spíše za legislativní nepřesnost než za záměr.

[8] PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29, Stanovisko č. 1/2010 k pojmům „správce“ a „zpracovatel“, 16. února 2010. [online]. *Internetové stránky Úřadu pro ochranu osobních údajů*. [cit. 26. 11. 2020]. Dostupné z: https://www.uoou.cz/files/wp169.pdf

osobních údajů bude primárně správce, který je povinen ovšem zavázat si zpracovatele v takovém rozsahu, že lze v případě porušení povinností plynoucích z nařízení GDPR lze na zpracovatele uplatnit sekundární odpovědnost. Nařízení GDPR však i na zpracovatele klade požadavky, které mají zajistit bezpečnost zpracování a skutečnou ochranu subjektů údajů a jejich práv. Proto také bude muset být mezi správci a zpracovateli uzavřena speciální zpracovatelská smlouva či řádná zpracovatelská doložka v rámci jiné smluvní dokumentace. Zpracovatelé nicméně nejsou oprávněni zpracovávat osobní údaje pro své vlastní účely či v rozporu s pokyny, které jim udělí správce: pokud by tak učinili, považují se ve vztahu k takovému zpracování za správce.

4.3 Určení účelu zpracování osobních údajů

Osobní údaje lze zpracovávat pouze pro určité, výslovně vyjádřené a legitimní účely. S ohledem na výslovný požadavek nařízení GDPR je nutné přesně definovat **účely**, včetně jejich konkrétního a sjednoceného pojmenování, a vést jejich katalog. Tyto účely lze vhodně dělit podle následujících demonstrativně uvedených usecasů v rámci kterých dochází ke zpracování osobních údajů:

a) bezpečnost, a to zejména v podobě zajištění funkčnosti asistenčních systémů;
b) poskytování služeb s přidanou hodnotou vztahujících se k danému vozidlu;
c) vývoj a rozvoj technického řešení, tj. výzkumné a rozvojové činnosti vedoucí k dalšímu rozvoji systémů autonomního řízení, užívaných technologií apod;
d) pojištění;
e) servisní účely;
f) infotainment.

4.4 Určení právního titulu zpracování osobních údajů

Aby bylo možno zákonně zpracovávat osobní údaje, je nutno disponovat platným právním titulem pro zpracování osobních údajů, který definuje právě nařízení GDPR. Bez právního titulu pro zpracování osobních údajů nelze jakékoli zpracování provádět – a to ani v případě systémů autonomního řízení. Takový postup by byl v rozporu s nařízením GDPR a dle něho také postižitelný.

Nařízení GDPR výslovně vyjmenovává tyto právní tituly:

a) souhlas se zpracováním osobních údajů;
b) plnění smlouvy;
c) plnění právní povinnosti;
d) životně důležitý zájem;
e) úkol ve veřejném zájmu nebo výkon veřejné moci; a
f) oprávněný zájem.

Každý z těchto právních titulů má svá specifika a bližší podmínky jeho použití, nicméně volba konkrétního právního titulu závisí na mnoha aspektech a může se lišit u konkrétních případů zpracování osobních údajů v celém ekosystému autonomního řízení.

4.4.1.1 Checklist požadavků na určení

Souhlas lze využít v situaci, kdy si je správce jistý, že subjekt osobních údajů může svůj souhlas udělit:

a) svobodně: tedy pokud má subjekt skutečnou volbu a kontrolu nad svým souhlasem, necítí se k němu být nucen, souhlas není nevyjednatelnou součástí podmínek, v případě, že subjekt souhlas neposkytne, nepocítí negativní důsledky, a má možnost ho kdykoliv odvolat, přičemž toto odvolání povede k ukončení zpracování;
b) konkrétně: tedy pro „jeden či více konkrétních“ účelů, přičemž správce musí zajistit i) upřesněný účel jako ochranu proti rozšíření o neplánované funkce, ii) granularitu v žádostech o souhlas; a iii) jasné oddělení informací týkajících se získání souhlasu pro činnosti zpracování údajů od informací o jiných záležitostech;
c) informovaně: tedy byly subjektu před získáním souhlasu poskytnuty informace, aby bylo zjevné, že přijímá informované rozhodnutí, chápe, s čím souhlasí, a je si vědom své možnosti souhlas odvolat;
d) jednoznačným projevem své vůle: vždy tedy aktivním jednáním nebo prohlášením, aby bylo zřejmé, že subjekt údajů souhlasil s konkrétním zpracováním.

Obecně by měl být právní titul souhlasu využíván až v případě, kdy pro předmětné zpracování není možné/vhodné použít jiný právní titul. Ačkoli je v případě řádně uděleného souhlasu tento titul velice silný, je třeba pamatovat na právo subjektu údajů tento souhlas kdykoli odvolat.

Plnění smlouvy lze využít v situaci, pokud je správce schopen prokázat, že ke zpracování dochází v rámci platné smlouvy se subjektem údajů a že zpracování je nezbytné pro plnění konkrétní smlouvy se subjektem údajů. Pokud se správci nepodaří prokázat, že

a) existuje smlouva,

b) tato smlouva je platná podle příslušných vnitrostátních právních předpisů závazkového práva a

c) zpracování je objektivně nezbytné pro plnění této smlouvy,

měl by správce zvážit jiný právní základ zpracování.

Právní povinnost lze využít pouze v situaci, kdy je správce na základě mezinárodní smlouvy, zákona či prováděcích předpisů povinen provádět nezbytné zpracování, kterým tuto právní povinnost splní. Zpracování musí být rozumným a přiměřeným způsobem, jak tohoto splnění dosáhnout: správce by ho neměl využívat v situaci, kdy má možnost uvážení, zda osobní údaje zpracovávat, nebo pokud existuje jiný rozumnější a přiměřenější a méně rušivý způsob splnění povinnosti. V případě tohoto titulu je stěžejní a nezbytná identifikace konkrétní povinnosti v příslušném právním předpisu, na základě které je plnění povinnosti správci uloženo.

Ochranu životně důležitých zájmů jednotlivce lze využít, kdy je zpracování osobních údajů nezbytné k ochraně něčího života nebo ke zmírnění vážného ohrožení osoby. Lze o ní uvažovat v netypických okolnostech, kdy se žádný z ostatních právních základů jednoznačně

neuplatní. Životně důležité zájmy mohou také představovat výjimku ze zákazu zpracování zvláštní kategorie osobních údajů (např. o zdravotním stavu) dle článku 9 GDPR.

Úkol ve veřejném zájmu nebo výkon veřejné moci může správce použít, pokud je pro něj zpracování osobních údajů nezbytné buď při výkonu veřejné moci (zahrnující veřejné funkce a pravomoci stanovené zákonem), nebo pro splnění konkrétního úkolu ve veřejném zájmu (stanoveného zákonem). Tento právní základ je nejvýznamnější pro orgány veřejné moci, ale potenciálně se na něj může odvolávat i každý správce, který nějakým způsobem vykonává veřejnou moc nebo plní úkol ve veřejném zájmu. Právo, které je základem úkolu, funkce nebo pravomoci, by však mělo být jasné a přesné a jeho použití by mělo být subjektem předvídatelné.

Oprávněný zájem správce je poměrně flexibilním právním titulem, který lze využít v případě, že oprávněné zájmy správce převyšují nad zájmy nebo právy a svobodami jednotlivých subjektů údajů. Při využití tohoto titulu jsou však správcům uloženy také zvýšené povinnosti. Správci by pro dovození svého oprávněného zájmu měli provést balanční test, ve kterém by měli mimo jiné zvážit:

a) v čem tento sledovaný oprávněný zájem opravdu spočívá;
b) prokázat, že zamýšlené zpracování je nezbytné k jeho dosažení; a
c) vyvážit tento oprávněný zájem se zájmy, právy a svobodami subjektu údajů.

V případě využití právního titulu oprávněného zájmu je rovněž nezbytné pamatovat na to, že subjekt údajů musí mít právo dát proti takovému zpracování námitku – v takovém případě by správce osobní údaje dále neměl zpracovávat, pokud neprokáže závažné oprávněné důvody pro zpracování převyšující nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

4.5 Zhodnocení míry zásahu do soukromí

Volba výše uvedeného právního základu, a dále zajištění plnění všech souvisejících požadavků a náležitostí, má velmi podstatné dopady na celkové zhodnocení míry zásahu do soukromí. Například, pokud existují zpracování, která si dovozuje sám správce (na základě svého oprávněného zájmu nebo na základě toho, že v situaci spatřuje ochranu životních zájmu subjektu), lze mít takové zpracování za intruzivnější a rizikovější pro soukromí subjektu. Zvolení nevhodného právního titulu současně může vést k překročení oprávnění správce a případně až k nezákonnosti konkrétního zpracování.

V rámci této metodiky rozlišujeme 4 skupiny rizik zásahů do soukromí uživatelů:

- Minimální – kdy správce například zpracovává pouze malý objem dat, data nejsou aktualizována v reálném čase, právním titulem pro zpracování je splnění právní povinnosti, data nejsou poskytována třetím stranám, nedochází ke zpracování zvláštní kategorie osobních údajů podle GDPR,

- Malé – platí to samé, jako pro skupinu minimální s tím, že některý z vyjmenovaných bodů již představuje větší riziko (např. zpracovává se větší objem dat či data jsou poskytována třetím stranám),
- Střední – zásah do soukromí uživatelů se zvyšuje například tím, že roste počet zaznamenávaných dat o subjektu údajů, dochází k podstatnějšímu předávání údajů třetím stranám a je využíván rizikovější právní titul,
- Vysoké – kdy správce například zpracovává osobní údaje o uživateli ve velkém rozsahu, ty jsou průběžně aktualizovány, uchovává je po dlouhou dobu a údaje jsou navíc poskytovány komerční sféře či na vyžádání.

Předmětné rozdělení však není dogmatické a může se měnit na základě jednotlivých parametrů, kdy kombinace různých parametrů může mít za výsledek stejnou úroveň rizikovosti. Proto je vhodné doporučit implementovat i dodatečná opatření v návaznosti na konkrétní parametry zpracování

Zásah do soukromí uživatelů se do větších podrobností zabývá metodika „Metodika analýzy zpracování osobních údajů a hodnocení míry zásahu do soukromí“. Subjektu je na základě jeho vstupů a výpočtu stanoveno, do které z těchto oblastí zásahu patří a navržena doporučení a opatření. Ty jsou součástí podkapitoly 4.6.

I za předpokladu zcela minimálního zásahu do soukromí uživatelů (při minimální úrovni rizikovosti zpracování) je však nezbytné, aby subjekt zajistil plnění povinností dle právních předpisů ochrany osobních údajů, jak je ostatně uvedeno dále.

4.6 Návrh odpovídajících opatření a doporučení

Tato podkapitola obsahuje doporučení a opatření pro správce osobních údajů. Jsou rozdělena na opatření, která je doporučeno aplikovat bez ohledu na výpočet rizikovosti a zpracovávaná data, a potom na specifičtější doporučení související se zpracovávanými údaji a jejich parametry.

4.6.1 Opatření a doporučení odpovídající GDPR

V následujícím seznamu jsou uvedena doporučení a opatření, která jsou možná implementovat v souvislosti se zpracováním osobních údajů podle GDPR:

a) příprava informačního dokumentu „Zásady ochrany osobních údajů“, aby obsahoval veškeré nezbytné informace, jako je například informační povinnost vůči subjektům údajů, která musí být plněna dostatečně transparentním a srozumitelným způsobem a za použití jednoduchých jazykových prostředků, zejména je-li subjektem údajů dítě. Za vhodné řešení lze považovat využívat vrstvení informací, tedy úvodní informace poskytnout například na L1 webových stránkách či přímo ve vozidle, zatímco úplné informace budou dostupné na L2 webových stránkách;

b) v souvislosti s informační povinností je třeba brát ohled na ustanovení čl. 14 nařízení GDPR, které říká, že v případě, kdy dochází ke zpracování osobních údajů, které nebyly získány od subjektu údajů, a jsou zpracovávány na základě zákona, není nutné subjekt údajů přímo informovat: informace o daném správci tohoto zpracování by však měla být veřejné (což je v některých případech přímo povinnost správce), právě třeba v „Zásadách ochrany osobních údajů“;
c) i za využití této metodiky přesně definovat účely, včetně jejich konkrétního a sjednoceného pojmenování, a vést jejich katalog. Za správný účel však není možné považovat konkrétní zákon či přímo zákonné ustanovení, jelikož z konkrétního zákona bude možno často dovodit i více účelů, resp. konkrétní účel bude upravovat více zákonných ustanovení;
d) v souvislosti s napomáháním výkonu práv subjektů údajů připravit a zveřejnit vzorové žádosti, které pak budou zpřístupněny subjektům údajů například v rámci jejich uživatelského rozhraní ve vozidle nebo na webových stránkách u daného správce dle jeho zapojení v systému autonomního řízení;
e) popsat v rámci interních směrnic proces administrace jednotlivých žádostí o výkon práv, aby bylo možno prokázat soulad s nařízením GDPR (což je jedna z povinností správce dle nařízení GDPR), a dále aby byl stanoven jasný návod a proces, jak bude s žádostmi nakládáno;
f) uchovat záznamy o aplikaci této metodiky nebo jiného správcem zvoleného přístupu v rámci interní směrnice, který prokáže splnění procesu pro zajištění minimalizace zpracování či jednoznačnost zpracování osobních údajů pouze v rámci rozsahu stanoveného zákonem, aby bylo možno prokázat soulad s nařízením GDPR;
g) vytvořit a zaznamenat proces ohlašování případu porušení ochrany a dalších incidentů, konkrétně postupy pro identifikaci bezpečnostního incidentu, aspektech posouzení jeho rizikovosti včetně následného postupu ohlašování a dokumentace incidentu dozorovému úřadu či přímo subjektům údajů, aby bylo možné prokázat soulad s nařízením GDPR; a
h) vést záznamy o zpracování osobních údajů v souladu s nařízením GDPR a evidovat v nich účely zpracování, kategorie subjektů a zpracovávaných údajů, kategorie příjemců údajů, případné předávání osobních údajů dalším správcům, plánované lhůty pro výmaz údajů a technická a organizační bezpečnostní opatření, přičemž pro obsah záznamů lze použít tuto metodiku.
i) pokud právní titul není využit správně (tzn. v případě souhlasu je svobodný, určitý, informovaný, jednoznačný a výslovný), subjekt by měl zvážit využití jiného právního titulu, či upravil zpracování – jinak totiž hrozí neplatnost právního titulu.

Tyto povinnosti je subjektu fakticky povinen plnit bez ohledu na to, jakou míru zásahu do soukromí jeho zpracování dat představuje.

4.6.2 Opatření a doporučení závislé na zpracovávaných údajích

Následující opatření jsou již specifičtější a závisí přímo na konkrétních kategoriích a parametrech dat.

Po identifikaci a posouzení rizik mohou být přijata mimo jiné následující technická opatření:

a) oddělení dat, která obsahují osobní údaje, do různých databází, aby nebylo možné je nalézt se všemi osobními údaji na jednom místě, přičemž přístup do databází je umožněn jen technickým rozhraním;
b) oddělení jednotlivých nosičů osobních údajů v různých databázích a technické zamezení jejich spojení do marketingově využitelného formátu;
c) oddělení kritických systémů od internetu;
d) zajištění fyzické bezpečnosti míst zpracování osobních údajů (řízení fyzického přístupu do prostor/objektu, ochrana perimetru míst zpracování osobních údajů);
e) zabezpečení komunikačního prostředí/sítí;
f) správa a ověřování identity určených osob;
g) řízení přístupových oprávnění;
h) monitorování a zaznamenávání činnosti určených osob;
i) detekce, řešení a vyhodnocování mimořádných událostí při zpracování osobních údajů (porušení zabezpečení osobních údajů atp.);
j) ochrana před škodlivými kódy;
k) ochrana identity subjektů údajů (pseudonymizace, anonymizace osobních údajů);
l) zajištění čitelnosti osobních údajů pouze oprávněnými osobami (kryptografie);
m) zajištění požadované úrovně dostupnosti osobních údajů;
n) zajištění zálohování a archivace; a
o) zajištění aplikační bezpečnosti.

Po identifikaci a posouzení rizik mohou být přijata mimo jiné následující organizační opatření:

p) přístup k jednotlivým databázím obsahujícím zdrojová osobní data je oddělen; všechny vrstvy IT systémů mají nastavena přístupová oprávnění a případně logování přístupů k technickým rozhraním;
q) řízení přístupu (byly definovány přístupové úrovně a oprávnění v rámci správy systému a je zavedeno logování jednotlivých přístupů k datovým analytickým modulům);
r) organizační zajištění zpracování osobních údajů (byl detailně proškolen veškerý personál, který může zejm. s OBU zařízením disponovat či k němu mít přístup);
s) zajištění systému řízení ochrany osobních údajů (bylo zamezeno manuálnímu spuštění procesu a proces byl automatizován, tj. byl vyloučen zásah osob, a bylo stanoveno provádění pravidelného kontrolního auditu nastavení procesu);
t) zajištění řízení aktiv;
u) zajištění řízení rizik;
v) řízení dodavatelů;
w) bezpečnosti lidských zdrojů;
x) zajištění požadované dokumentace zpracování osobních údajů;
y) zajištění bezpečnosti v procesech akvizice, vývoje a údržby;
z) řízení změn;
aa) řízení provozu a komunikací;
bb) řízení kontinuity činností; a

cc) řízení monitorování zpracování osobních údajů.

4.7 Doporučení dle kategorií a parametrů

Předmětem této části je pro jednotlivé kategorie dat z kapitoly 4.1 a jejich specifických parametrů[9] stanovit příslušná doporučení navrhnutá v předchozí kapitole. Nejčastější kombinace kategorií dat a jejich parametrů, a koeficientu rizikovosti[10] včetně navržených doporučení pro ně jsou uvedeny v tabulce Tabulka 1. Je jasné, že bohužel není možné postihnout všechny možné kombinace parametrů, které může správce hledat. V takových případech je nutné přistupovat ke každému případu jednotlivě, zároveň platí, že z hlediska opatření a doporučení je vždy nejvýhodnější zvolit tu nejrizikovější variantu.

Každá kategorie dat je rozdělena na několik skupin dle specifických parametrů (např. kategorie Obrazová data je rozdělena na 3 skupiny). Pokud správce nenajde přesnou shodu s příslušnou skupinou (řádkem), je doporučeno řídit se vždy podle parametru, který patří do nejrizikovější skupiny.

Příklad: Pokud zpracovávám data podporující řízení motorového vozidla a mám následující parametry:

- *Pravděpodobnost identifikace: minimální*
- *Povaha osobních údajů: běžná*
- *Zdroj osobních údajů: senzory a detektory*
- *Právní základ: plnění smlouvy*
- *Příjemci: Data jsou poskytována veřejné či komerční sféře.*
- *Vypočtený koeficient rizikovosti: R = 48.12*

Všechny parametry i vypočtený koeficient odpovídá prvnímu řádku v tabulce XX kromě příjemců, které jsou na druhém řádku (Rizikovost 2).

Pro každou skupinu jsou potom navržena doporučení odpovídající dané rizikovosti a rizikovosti nižší.

Příklad: Z předchozího příkladu (zpracování dat podporující řízení motorového vozidla) vychází, že je pro správce údajů relevantní řádek 2. Z hlediska doporučení a opatření platí, že správce by se měl řídit doporučeními z tohoto řádku a zároveň i z řádku s nižší rizikovostí. Ve výsledku jsou pro něj tedy relevantní následující doporučení:

- *d, e, i, k, m,n, p, q, t, u, v, x, bb (Rizikovost 2)*
- *a,b,c,j,l,o,s (Rizikovost 1).*

[9] blíže jsou popsány v komplementární metodice analýzy zpracování osobních údajů a hodnocení míry zásahu do soukromí v kapitole 4.4.

[10] blíže jsou popsány v komplementární metodice analýzy zpracování osobních údajů a hodnocení míry zásahu do soukromí v kapitole 4.7.

Tabulka 1 – Kategorie dat, evaluační koeficienty a přiřazená doporučení a opatření

Rizikovost	Kategorie dat	Pravděpodobnost identifikace	Povaha osobních údajů	Zdroj osobních údajů	Právní základ	Příjemci	Doporučení a opatření
1	Data podporující řízení motorového vozidla	Minimální	Běžná Ekonomická	Senzory a detektory Přímo od subjektů údajů	Zákonná povinnost Plnění smlouvy	Údaje nejsou poskytovány nikomu jinému.	a,b,c,j,l,o,s
2		Limitovaná	Behaviorální	Externí zdroj dat Zdroj systému ve vozidle	Životní zájem Veřejný zájem	Data jsou poskytována veřejné či komerční sféře.	+ d, e, i, k, m,n, p, q, t, u, v, x, bb
3,4		Vysoká Signifikantní	Behaviorální Citlivá	Audiovizuální zdroj dat Externí zdroj dat	Souhlas Oprávněný zájem	Data jsou poskytována komukoliv na požádání.	+ f, g, h, w, y, z, aa
1	Obrazová data	Minimální	Běžná	Senzory a detektory Přímo od subjektů údajů	Zákonná povinnost	Údaje nejsou poskytovány nikomu jinému.	a,b,c,i,j,k,l,o,r,s
2		Limitovaná	Behaviorální	Zdroj systému ve vozidle	Plnění smlouvy Životní zájem	Data jsou poskytována veřejné či komerční sféře.	+ d, m,n, p, q, t, u, v, x, bb
3,4		Vysoká Signifikantní	Ekonomická Behaviorální Citlivá	Audiovizuální zdroj dat Externí zdroj dat	Souhlas Veřejný zájem Oprávněný zájem	Data jsou poskytována komukoliv na požádání.	+ e,f, g, h, w, y, z, aa

Rizikovost	Kategorie dat	Pravděpodobnost identifikace	Povaha osobních údajů	Zdroj osobních údajů	Právní základ	Příjemci	Doporučení a opatření
1	Data o řízení vozidla	Minimální Limitovaná	Běžná Ekonomická	Senzory a detektory Přímo od subjektů údajů	Zákonná povinnost Plnění smlouvy	Data nejsou poskytovány nikomu jinému či jsou poskytována komerční sféře.	a, b, e, i, j, k, l, m, n, o, p, r, s, t, u, v, x, bb
2,3		Vysoká	Behaviorální	Senzory a detektory Zdroj systému ve vozidle	Souhlas Veřejný zájem Oprávněný zájem	Data jsou poskytována veřejné sféře.	+ c, d, m, n, p, q
4		Vysoká Signifikantní	Ekonomická Behaviorální Citlivá	Audiovizuální zdroj dat Externí zdroj dat	Souhlas Životní zájem Oprávněný zájem	Data jsou poskytována komukoliv na požádání.	+ f, g, h, w, y, z, aa
1	Lokalizační a polohová data	Minimální Limitovaná	Běžná Ekonomická	Senzory a detektory Přímo od subjektů údajů Zdroj systému ve vozidle	Zákonná povinnost Plnění smlouvy Souhlas	Údaje nejsou poskytovány nikomu jinému.	a, b, c, i, j, k, l, o, r, s
2		Vysoká	Behaviorální Ekonomická	Senzory a detektory Zdroj systému ve vozidle	Souhlas Životní zájem	Data jsou poskytována komukoliv na požádání.	+ d, m, n, p, q, t, u, v, x, bb
3,4		Signifikantní	Citlivá	Zdroj systému ve vozidle Audiovizuální zdroj dat Externí zdroj dat	Souhlas Veřejný zájem Oprávněný zájem	Data jsou poskytována komukoliv na požádání.	+ e, f, g, h, w, y, z, aa

Rizikovost	Kategorie dat	Pravděpodobnost identifikace	Povaha osobních údajů	Zdroj osobních údajů	Právní základ	Příjemci	Doporučení a opatření
1,2	Audio data	Minimální Limitovaná	Běžná Ekonomická	Zdroj systému ve vozidle Senzory a detektory	Souhlas Zákonná povinnost Plnění smlouvy	Data nejsou poskytovány nikomu jinému.	a, b, c, e, i, j, k, l, m, n, o, p, r, s, t, u, x, bb
3,4		Vysoká Signifikantní	Behaviorální Citlivá	Externí zdroj dat Audiovizuální zdroj dat Zdroj systému ve vozidle	Veřejný zájem Životní zájem Oprávněný zájem	Data jsou poskytována veřejné sféře.	+ f, g, h, i, q, v, w, y, z, aa
3	Data z biometrických, biologických nebo zdravotních senzorů	Vysoká	Behaviorální Citlivá	Senzory a detektory Zdroj systému ve vozidle Externí zdroj dat	Souhlas Životní zájem Plnění smlouvy	Údaje nejsou poskytovány nikomu jinému.	b, c, d, i, j, l, m, n, o, p, q, r, s, t, u, x, y
4		Signifikantní	Behaviorální Citlivá	Senzory a detektory Zdroj systému ve vozidle Externí zdroj dat	Souhlas Životní zájem Plnění smlouvy	Data jsou poskytována komukoliv na požádání.	+ a, e, f, g, h, v, w, x, z

Rizikovost	Kategorie dat	Pravděpodobnost identifikace	Povaha osobních údajů	Zdroj osobních údajů	Právní základ	Příjemci	Doporučení a opatření
1	Persona-lizovaná data	Minimální Limitovaná	Běžná Behaviorální	Senzory a detektory Přímo od subjektů údajů	Plnění smlouvy	Data nejsou poskytovány nikomu.	a, b, c, j, l, o, s
2		Limitovaná Vysoká	Behaviorální	Senzory a detektory Externí zdroj dat Zdroj systému ve vozidle	Souhlas Veřejný zájem Oprávněný zájem Životní zájem	Data jsou poskytována komukoliv na požádání.	+ d, e, i, k, m, n, p, q, t, u, v, x, bb
3,4		Vysoká Signifikantní	Behaviorální Citlivá	Audiovizuální zdroj dat Externí zdroj dat	Souhlas Oprávněný zájem	Data jsou poskytována komukoliv na požádání.	+ f, g, h, w, y, z, aa

4.8 Vyhodnocování účinnosti a efektivity zaváděných opatření

Vyhodnocování účinnosti a efektivity zaváděných opatření probíhá s ohledem na nová aktiva, nové (dosud neuvažované) hrozby, nové synergické efekty působení hrozeb, identifikace nových zranitelností, soustavně, a to buď nepřetržitě nebo v plánovaných časových krocích, v intervalech 1–3 roky s tím, že lze doporučit synchronizaci (z důvodu možnosti duplicity některých prováděných činností) termínu provedení auditu a aktualizace posouzení vlivu s audity kybernetické bezpečnosti prováděnými na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (pokud se na správce vztahují).

Může být prováděno v rámci mimořádných (po proběhlé mimořádné události, jejímž důsledkem je změna vstupních parametrů vedoucí ke zvýšené rizikovosti) nebo plánovaných auditů. V rámci auditu probíhá revize platnosti uvažovaných hrozeb a zranitelností, hodnocení správnosti a účinnosti uplatněných opatření (technických a organizačních), vliv dopadů mimořádných událostí na zpracování osobních údajů, soulad přijatých opatření s právními předpisy a závazky správce a určení případných nápravných opatření.

Je vhodné vyhodnocování účinnosti nechat zajistit na monitorovaném zpracování osobních údajů pověřencem pro ochranu osobních údajů, nebo, pokud ho správce nemá, nezávislou osobou s odbornými znalostmi a praxí.

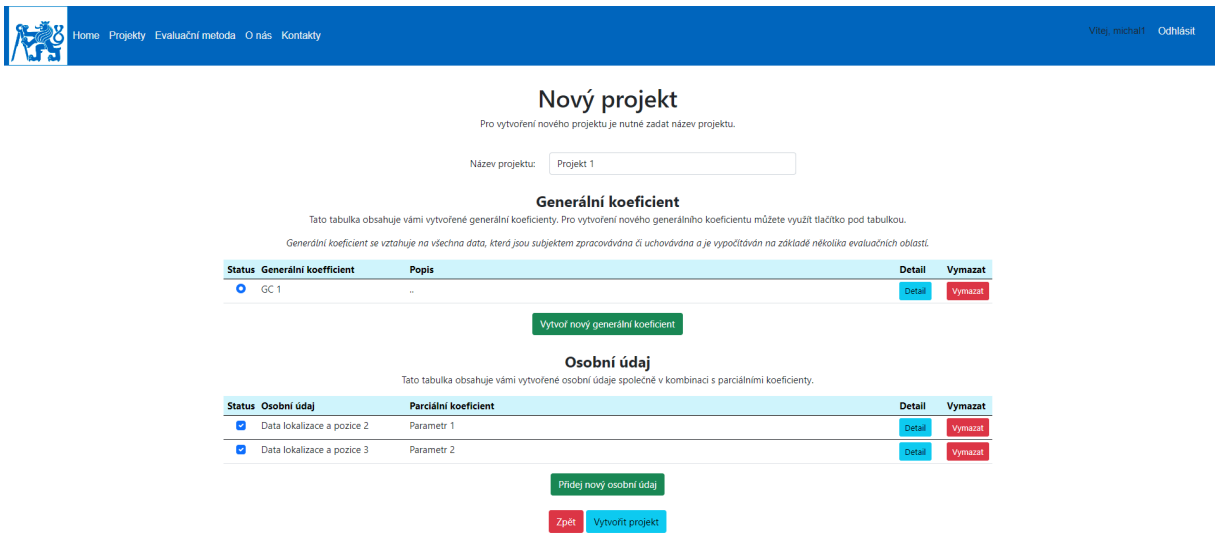
Správce ve vhodných případech, tj. zejména implementace rozsáhlého plošného opatření, si může též zajistit stanovisko zástupců subjektů údajů (vybraný vzorek v rozsahu 3-10 osob) k vyhodnocení účinnosti.

5 Popis webové aplikace

Pro účely zhodnocení rizikovosti osobních údajů, se kterými subjekt operující s daty nakládá, byla vytvořena webová aplikace. Uživatel webové aplikace má možnost vytvářet „Projekty“ ve kterých jsou osobní údaje hodnoceny na základě jejich rizikovosti. Při vytváření projektu musí uživatel nejdříve vytvořit obecný (tzv. „Generální koeficient“). Tento koeficient se vztahuje na všechny osobní údaje a je zaměřen na obecné informace vztahující se ke všem osobním údajům a na povahu subjektu, který s daty nakládá. Uživatel má dále možnost si vybrat z několika předem připravených oblastí osobních údajů a zadat doplňkové („Parciální“) parametry, které osobní údaj dále definují. Při výběru generálního koeficientu a osobních údajů uživatel vytvoří nový projekt a je mu představena stránka s výsledkem hodnocení rizikovosti.

5.1 Registrace

Pro vytváření projektu ve webové aplikaci je nutné se nejprve zaregistrovat a přihlásit. Registrace je nutná z důvodu zapamatování již vytvořených projektů a ukládání specifických kombinací osobních údajů a doplňkových parametrů, pomocí kterých se následně určuje ohodnocení rizikovosti a specifických opatření, které by měl uživatel přijmout (specifická opatření jsou popsány v kapitole 4.6). Vytvoření nového projektu je vidět na Obrázek 1.

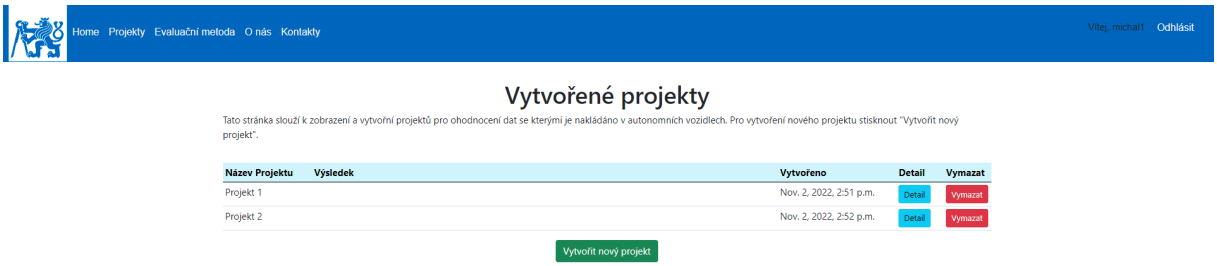


Obrázek 1 Vytvoření nového projektu, generální koeficient a osobní údaje

5.2 Projekt

Na stránce projektu je po přihlášení možné vidět seznam všech projektů, vytvořených uživatelem (Obrázek 2). Projekty lze ze seznamu mazat a zobrazit v detailu, kde je možné procházet výběr osobních údajů a jejich doplňkových parametrů, výběr generálního

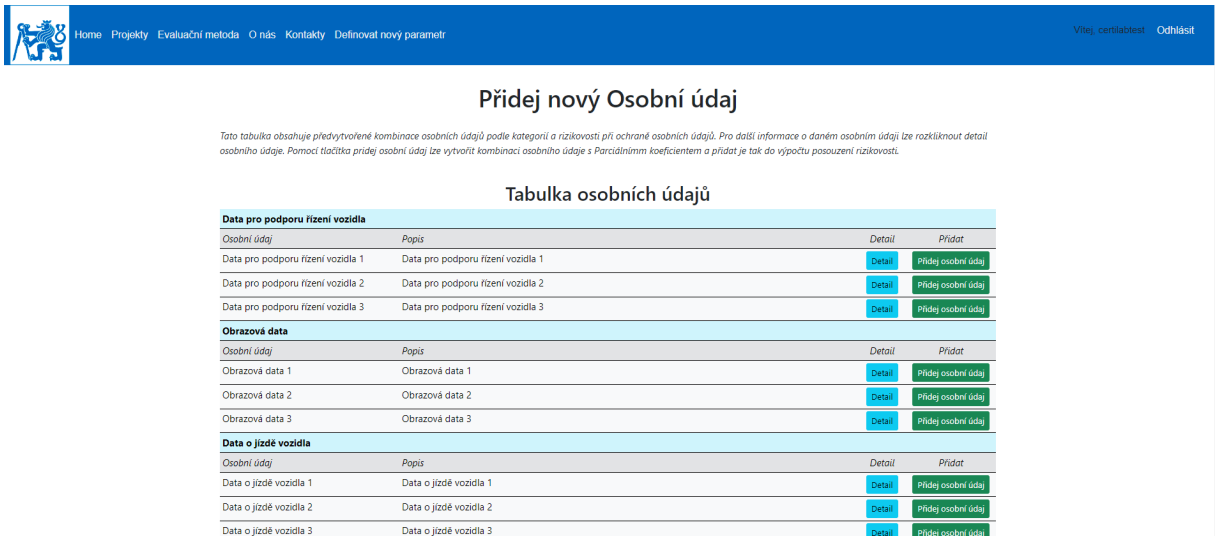
koeficientu ovlivňující veškeré osobní údaje i výsledek rizikovosti projektu a specifické opatření, které by měl subjekt přijmout.



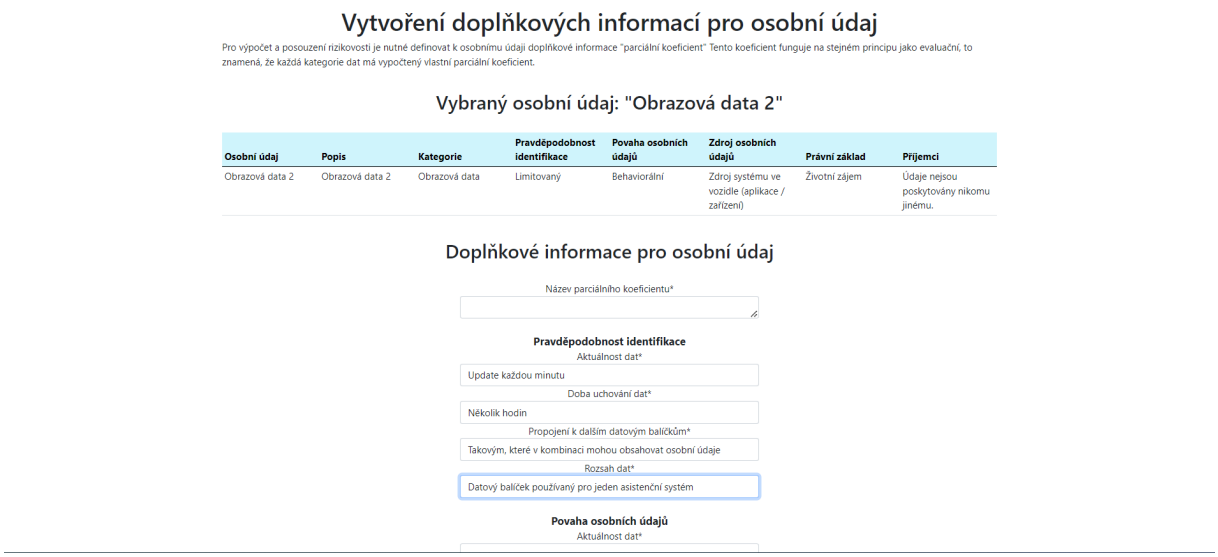
Obrázek 2 Vytvořené projekty

5.3 Přidání osobního údaje

Při vytváření projektu je nutné vybrat si z existujícího listu již vytvořených osobních údajů (Obrázek 3). Při vybrání osobního údaje je následně uživateli zobrazena stránka s dalšími parciálními parametry (Obrázek 4), které ovlivňují výsledek hodnocení rizikovosti osobních údajů. Bližší informace zabývající se výčtem a ohodnocením osobních údajích, parciálních parametrů i generálních koeficientů lze najít v komplementárním dokumentu „Metodika analýzy zpracování osobních údajů a hodnocení míry zásahu do soukromí“.



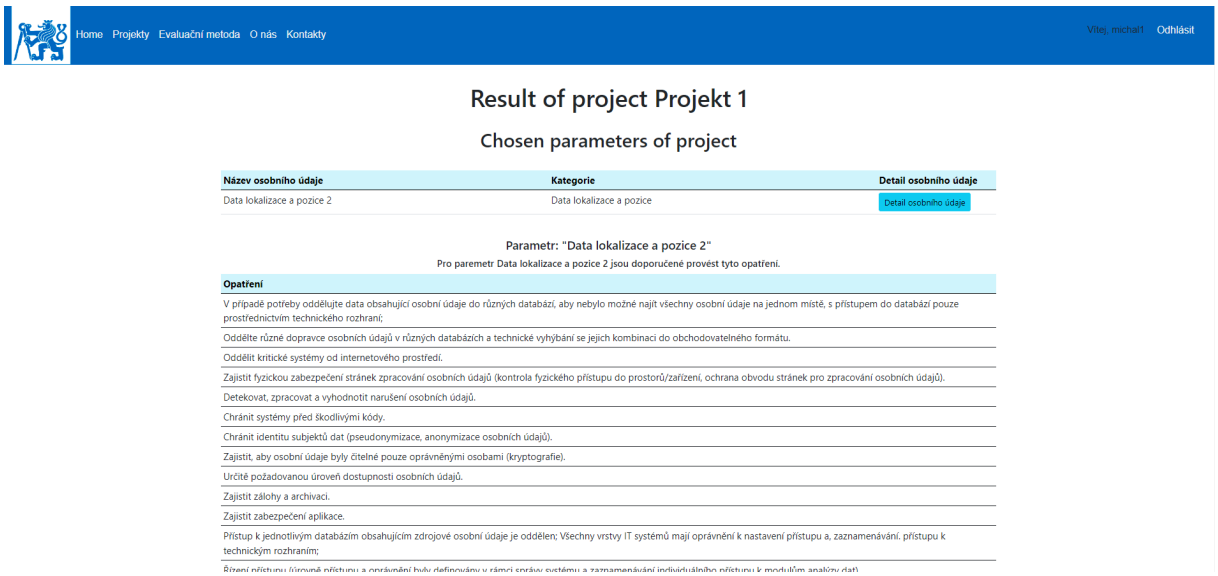
Obrázek 3 Výběr osobních údajů



Obrázek 4 Nový osobní údaj a doplňkové informace

5.4 Výsledek

Při zadání všech požadovaných údajů a vytvoření projektu je uživateli představena stránka s výsledkem hodnocení rizikovosti (Obrázek 5). Stránka obsahuje výčet všech vybraných osobních údajů a jednoho obecného koeficientu. Uživateli je představen výsledek hodnocení, tzn. jeho slovní vyjádření a dále specifické opatření, které by měl uživatel přijmout. Hodnocení rizikovosti osobních údajů je realizováno pomocí vytvořeného vzorce a individuálního ohodnocení generálního koeficientu, osobních údajů a parciálních parametrů. Veškeré informace o výpočtu rizikovosti lze nalézt v dokumentu „Metodika analýzy zpracování osobních údajů a hodnocení míry zásahu do soukromí“.



Obrázek 5 Výsledek

6 Srovnání novosti postupů

V dubnu 2020 byla na Ministerstvu dopravy v České republice stanovena Etická komise pro posuzování otázek spojených s provozem automatizovaných a autonomních vozidel. Tato komise vydala na podzim roku 2021 publikaci „Etická doporučení pro provoz propojených a autonomních vozidel“, která se mj. zabývá i ochranou osobních údajů.[11]

Jedno z právních doporučení má přímo název „Soukromí a ochrana dat“. Jeho základní popis je následující:

„Jakékoliv zásahy do soukromí musí být minimalizovány, zajištěna musí být práva na ochranu osobních údajů subjektů. Osobní údaje mohou být používány pouze se souhlasem subjektů. Veškerá data musí být používána transparentně a musí být přesně vymezeno, jaká data mají být uchovávána a na jak dlouho.“

Je patrné, že Etická komise MD považuje za základní právní titul zpracování osobních údajů řidičů souhlas se zpracováním osobních údajů. Tato metodika však právní tituly zpracování rozšiřuje o další možnosti na základě rozsahu osobních údajů a specifika jejich zpracování (doba a způsob uchování osobních údajů atp.). Na tomto základě také tato metodika stanovuje příslušná doporučení a opatření pro naplnění povinností vyplývajících z GDPR.

V publikaci Etické komise MD je také zmíněno, že výrobci, provozovatelé a uživatelé autonomních vozidel musí přijmout odpovědnost za zabezpečení osobních údajů po celou dobu uchovávání dat a snažit se data dostatečně chránit, např. kódováním. Konkrétní opatření zde ovšem nejsou zmíněna narozdíl od této metodiky, pro kterou je to jeden z hlavních cílů a výstupů.

[11] Dokument je dostupný na adrese: https://www.mdcr.cz/getattachment/Uzitecne-odkazy/Veda,-vyzkum,-inovace/Eticka-komise/Eticka-komise-zprava-autonomni-mobilita_.pdf.aspx

7 Popis uplatnění certifikované metodiky

Tato metodika poskytuje systematický a ucelený postup pro subjekty, zabývající se vývojem, výrobou či provozem komponent a systémů autonomního řízení, které generují a zpracovávají osobní údaje. Vzhledem k tomu, že ekosystém autonomního řízení je poměrně rozsáhlý, jedná se zejména, nikoliv však výhradně o následující subjekty:

- Výrobci motorových vozidel a jejich komponent;
- Provozovatelé vozidlových flotil (např. poskytovatelé operativního leasingu apod.);
- Poskytovatelé SW aplikací a služeb (např. provozovatelé fleet management aplikací, provozovatelé customizovaných softwarových aplikací pro řidiče apod.);
- Pojišťovny;
- Poskytovatelé servisních služeb a služeb s přidanou hodnotou;
- Správci dopravní infrastruktury;
- Správci telekomunikační infrastruktury.

Vzhledem k tomu, že v případě systémů autonomních řízení předpokládáme naplnění požadavků „privacy-by-default“, je vhodné tyto postupy aplikovat již ve fázi návrhu a vývoje prototypů tak, aby již od úvodních fází komponent autonomního řízení bylo zcela zřejmé, jaké osobní údaje jsou zpracovávány a jakým způsobem, aby bylo možné přijmout taková technická a organizační opatření, která by naplňovala požadavky GDPR a rovněž nastavit odpovídající právní titul a účel zpracování osobních údajů, včetně poskytnutí dostatku informací subjektům údajů.

Pouze absolutní transparentnost a informovanost subjektů údajů, jaký rozsah osobních údajů a jakým způsobem je zpracováván, může zajistit akceptaci těchto nových systémů ze strany uživatelů, kteří budou mít zcela logicky z počátku obavy, zda s jejich osobními údaji není nakládáno v rozporu s právní regulací.

8 Ekonomické aspekty

Tato certifikovaná metodika z ekonomického pohledu přináší zejména úspory správcům, resp. zpracovatelům osobních údajů, a to díky metodickým doporučením při návrhu organizačních, technických a právních opatření při zpracování osobní údajů v systémech a komponentách autonomního řízení. Tyto úspory lze spatřit zejména v nákladech, které by bylo nutné vynaložit na vytvoření vlastních metodických postupů a rovněž snížením rizika udělení správní pokuty ze strany kontrolních orgánů, pakliže by povinné osoby nedodržovaly závazné požadavky pro ochranu osobních údajů dle GDPR.

Z pohledu nákladů zavedení metodiky neklade žádné vysoké finanční nároky, a to s výjimkou seznámení se s jejím obsahem ze strany klíčových uživatelů u subjektů zabývajících se vývojem, výrobou a provozem systémů a komponent autonomního řízení. Zejména se bude jednat o pověřence osobních údajů a jím pověřené osoby, které budou navrhovat a implementovat organizační a technická opatření v souvislosti se zajištěním bezpečnosti a ochrany zpracovávaných a uchovávaných osobních údajů v rámci systémů autonomního řízení.

9 Seznam literatury

Internetové zdroje

1. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_201806 [online]. *SAE International.* [cit. 7.1.2021]. Dostupné z: https://www.sae.org/standards/content/j3016_201806/

2. Automated Driving Systems 2.0 A Vision for Safety [online]. *National Highway Traffic Safety Administration.* [cit. 7.1.2021]. Dostupné z: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

3. Bureš, D. Úrovně autonomních aut. Jaký je mezi nimi rozdíl? A která fáze je opravdu auto bez řidiče? [online]. *Internetové stránky auto.cz*. 27.3.2018. [cit. 7.1.2021]. Dostupné z: https://www.auto.cz/urovne-autonomnich-aut-jaky-je-mezi-nimi-rozdil-a-ktera-faze-je-opravdu-auto-bez-ridice-120259

4. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_201401 [online]. *SAE International*. [cit. 7.1.2021]. Dostupné z: https://www.sae.org/standards/content/j3016_201401/

5. SAE Standards News: J3016 automated-driving graphic update [online]. *SAE International*. [cit. 7.1.2021]. Dostupné z: https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic

6. PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29, Stanovisko č. 1/2010 k pojmům „správce“ a „zpracovatel“, 16. února 2010. [online]. *Internetové stránky Úřadu pro ochranu osobních údajů*. [cit. 26. 11. 2020]. Dostupné z: https://www.uoou.cz/files/wp169.pdf

7. The importance of data analysis in autonomous vehicle development [online]. *Internetové stránky DXC.technology*. [cit. 11.1.2021]. Dostupné z: https://www.dxc.technology/auto/insights/146742-the_importance_of_data_analysis_in_autonomous_vehicle_development

8. Butler, B. The future of auto safety is seat belts, airbags and network technology [online]. *Internetové stránky networkworld.com*. 23.5.2016. [cit. 13.1.2021]. Dostupné z: https://www.networkworld.com/article/3072486/the-future-of-auto-safety-is-seat-belts-airbags-and-network-technology.html

9. Compliance package – Connected vehicles and personal data [online]. *Internetové stránky cnil.fr*. 13.2.2018. [cit. 15.1.2021]. Dostupné z: https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf

10. Regulating government access to C-ITS and automated vehicle data [online*]. Internetové stránky National Transport Commission ntc.gov.au*. 08/2019. [cit. 15.1.2021]. Dostupné z: https://www.ntc.gov.au/sites/default/files/assets/files/NTC-Policy-Paper-Regulating-government-access-to-C-ITS-and-AV-data.pdf

11. PARTY, A. D. P. W. Opinion 13/2011 on geolocation services on smart mobile devices. *Opgeroepen op August*, 2011, 7: 2013.

12. PARTY, A. D. P. W. Opinion 03/2017 on processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS).

13. EUROPEAN DATA PROTECTION BOARD. 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. 2019.

14. EUROPEAN DATA PROTECTION BOARD. Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications. 2020.

15. MANSON, C. G.; GORNIAK, S. Recommendations for a methodology of the assessment of severity of personal data breaches. *ENISA (European Union Agency for Network and Inform. Security) Working Document, v1. 0*, 2013.

16. Privacy. *Car-2-car communication consortium* [online]. Braunschweig, Germany, 2018 [cit. 2023-01-18]. Dostupné z: https://www.car-2-car.org/service/privacy

Právní předpisy

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

18. Nařízení Komise v přenesené pravomoci (EU) č. 305/2013 ze dne 26. listopadu 2012, kterým se doplňuje směrnice Evropského parlamentu a Rady 2010/40/EU, pokud jde o harmonizované poskytování interoperabilní služby eCall v celé Unii

19. Zákon č. 110/2019 Sb., o zpracování osobních údajů

20. Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů

Seznam publikací předcházející metodice

21. MLADA, Michal, et al. Protection of personal data in autonomous vehicles and its data categorization. In: *2022 Smart City Symposium Prague (SCSP)*. IEEE, 2022. p. 1-5.

22. LOKAJ, Zdeněk, et al. Ochrana osobních údajů v systémech autonomního řízení. Co je nezbytné pro bezpečné fungování a jak toho dosáhnout?. *Revue pro právo a technologie*, 2021, 12.24: 3-37.