# Ochrana osobních údajů v kriminologickém výzkumu[1]

KAROLÍNA NOVÁ[2]
JAKUB DRÁPAL
Ústav státu a práva Akademie věd ČR, Právnická fakulta Univerzity Karlovy

**Personal data protection in criminological research**

**Abstract**: Empirical researchers often use secondary data collected by others, especially state institutions. Due to the increasing availability of data online and the ever-growing ease of merging various datasets, the protection of personal data and adherence to the principles of data processing is becoming increasingly important for researchers. In criminal justice research, the protection of personal data is especially important, as information on convictions or criminal proceedings is under special protection. This article presents the basic principles for conducting research using personal data, focusing on their application in criminological research and especially on the use of secondary data. The article further discusses the responsibilities of personal data administrators and their role in the context of processing data for research purposes, data security, creating databases and their various forms, and the process of anonymization and pseudonymization. The article concludes with practical recommendations for ensuring ethical and legal practices in the field of criminological research vis-à-vis personal data protection.
**Keywords:** GDPR; criminology; research ethic; personal data; data protection

## Úvod

Kriminologický výzkum se neobejde bez práce s citlivými, zejména osobními, údaji. Nastává tak konflikt mezi ochrannou citlivých dat a potřebou realizovat kvalitní výzkum, který často vyžaduje práci s osobními údaji. Neregulované prostředí by zejména v čím dál více digitalizované společnosti mohlo vést k častému porušování práva na soukromí. Přílišná regulace zpracování osobních údajů by na druhou stranu

[1] Tento článek je výsledkem badatelské činnosti finančně podporované Grantovou agenturou ČR v rámci grantu GA ČR č. 19-15077S „Rozdíly při ukládání trestů v postkomunistických kontinentálních právních systémech“, řešeného na Ústavu státu a práva Akademie věd ČR.
[2] Případnou korespondenci zasílejte na e-mailovou adresu: karolina.nova95@gmail.com.

měla za následek snížení flexibility výzkumu, a ve svém důsledku i ohrožení naplnění jeho cíle – získávání nových poznatků. Proto jsou přijímána pravidla pro práci s osobními údaji, která umožňují realizaci výzkumů využívajících je, ale přitom zajišťují dostatečnou míru jejich ochrany. Z důvodu důležitého zájmu společnosti na získávání nových znalostí jsou práva subjektu osobních údajů ve výzkumu vyvažována zcela v jiném kontextu, než tomu je u běžného zpracování osobních údajů. Vědcům je tak poskytováno zvláštní postavení, kterého by si měli vážit a které by neměli zneužívat. Kriminologický výzkum je pak specifický tím, že existuje speciální trestněprávní směrnice, která upravuje nakládání s údaji z trestního řízení. Jak tyto výjimky ovlivňují práci kriminologů, nemusí být zřejmé ani odborníkovi seznámenému s problematikou práva na ochranu osobních údajů.

Tento článek odpovídá na základní otázky, na které se kriminolog pracující s daty může ptát. Často totiž nemusí být zřejmé, která ze získaných dat jsou osobními údaji, a podléhají tak právní regulaci práva na ochranu osobních údajů. Ty, kteří se v ochraně osobních údajů neorientují, zaujme úvodní pasáž rozebírající ochranu osobních údajů obecně, tedy právní předpisy, kterými se tato oblast řídí, co se považuje za osobní údaj a jak lze docílit toho, aby osobní údaj přestal být osobním údajem. Těm, kteří se rozhodnou shromažďovat osobní údaje za účelem vedení kriminologického výzkumu, je věnována další část článku, která popisuje, jak zajistit ochranu osobních údajů a jak je skladovat. Vzhledem k častému užití sekundárních dat ve výzkumu se následně článek zabývá opětovným užitím osobních údajů. Závěrečná část článku pak představuje jednoduchý seznam praktických opatření, která je třeba přijmout pro co nejlepší ochranu osobních údajů při realizaci kriminologického výzkumu.

## Právní předpisy upravující ochranu osobních údajů

Mezi tři základní předpisy, na které lze v souvislosti se zpracováním osobních údajů v kriminologickém výzkumu narazit, patří: (i) nařízení Evropského parlamentu a Rady EU č. 2016/679, známé také jako Obecné nařízení, nebo GDPR, (ii) směrnice Evropského parlamentu a Rady EU č. 2016/680, známá také jako trestněprávní směrnice, a (iii) zákon č. 110/2019 Sb., o zpracování osobních údajů, který byl přijat v návaznosti na přijetí Obecného nařízení a trestněprávní směrnice (dále též „zákon o zpracování“).

Obecné nařízení požaduje, aby osobní údaje byly zpracovávány mimo jiné zákonným, transparentním a účelově omezeným[3] způsobem tak, aby data zůstala

[3] Podle článku 4 odst. 3 GDPR se omezením zpracování rozumí dostatečné vymezení důvodu pro zpracování vymezených osobních údajů, a to již před zahájením daného zpracování. Cílem je především zajistit, aby subjekt údajů, kterého se osobní údaje týkají, věděl, k čemu přesně dané zpracování slouží. Pokud by se měl tento účel v průběhu zpracování osobních údajů změnit, nelze údaje nadále zpracovávat bez dalšího – k tomu blíže k testu slučitelnosti níže.

důvěrná (Pormeister, 2017). Na zpracování osobních údajů výzkumníky se vztahují speciální pravidla vzhledem k povaze procesu vedení výzkumu či vytváření statistik a jejich nezbytnosti k rozšiřování nových poznatků, který opravňuje oslabení práv subjektů údajů v oblasti výkonů jejich práv. Tato specifičnost se odráží v existenci výjimek z působnosti některých ustanovení Obecného nařízení. Důvodem pro tuto úpravu je především snaha zajistit dostatečnou ochranu osobních údajů pomocí řady různých opatření a záruk, aniž by došlo ke svazujícím povinnostem při realizaci výzkumu.[4]

Výjimky a záruky jsou stanovované na dvou úrovních: Obecně na úrovni EU pomocí GDPR a následně právními předpisy jednotlivými členskými státy. První stupeň výjimek a záruk se odvolává přímo na jednotlivá ustanovení nařízení GDPR, a to za podmínky, že při uplatnění výjimky pro vědecký výzkum jsou současně zajištěny dostatečné záruky spočívající v technických a organizačních opatřeních. Těmto výjimkám a zárukám se věnujeme níže.

Druhý stupeň pak představují právní předpisy členského státu, ve kterém je výzkum prováděn, přičemž se tímto předpisem pro Českou republiku rozumí zákon o zpracování osobních údajů. Ten se v hlavě druhé věnuje zpracovávání osobních údajů dle GDPR a pro oblast výzkumu uvádí příklady vhodných opatření.[5] Hlava třetí se věnuje zpracování osobních údajů v souvislosti s trestním řízením, a to včetně předcházení trestné činnosti, stíhání trestných činů či výkonu trestů. Zpracovává tak trestněprávní směrnici, která se sice přímo zabývá osobními údaji v oblasti kriminologie a trestního práva, jedná se však o oblast vyňatou z působnosti GDPR, jelikož se týká pouze zpracování osobních údajů orgány činnými v trestním řízení. Pouze v případě, kdy by došlo ke zpracování osobních údajů na základě souhlasu dle tuzemského práva (např. by osoba dala souhlas se zveřejněním odposlechu telekomunikačního provozu[6]), by se zpracování na základě souhlasu řídilo podle GDPR. Stejně tak se budou orgány činné v trestním řízení řídit Obecným nařízením, pokud by vedly samostatný výzkum.[7]

I pokud vědec dodrží zákonná pravidla pro ochranu osobních údajů, neznamená to, že může s osobními údaji nakládat dle své libosti. Na rozdíl od ostatních odvětví se vědec musí řídit i dalšími omezeními, a to zejména zavedenými etickými standardy, které jsou běžně stanovovány v rámci jednotlivých vědeckých

[4] Čl. 89 GDPR, bod odůvodnění 156 GDPR.
[5] § 16 odst. 1 z. č. 110/2019 Sb., o zpracování údajů, uvádí např. jmenování pověřence, pseudonymizace a šifrování osobních údajů, vedení záznamů o veškerém zpracování včetně jejich uchování po dobu aspoň dvou let, dostatečné zabezpečení technického vybavení včetně pravidelného ověřování, zda je toto zabezpečení dostatečné, omezení přístupu k osobním údajům a procesy obnovy dat v případě bezpečnostního incidentu.
[6] § 8c z. č. 141/1961 Sb., trestního řádu.
[7] Čl. 9 odst. 2 trestněprávní směrnice.

odvětví například odbornými společnostmi,[8] což potvrzuje i stanovisko Evropského inspektora ochrany údajů (2020, s. 13).[9] V tomto článku se jimi primárně nezabýváme, nicméně i v následujícím textu naznačujeme na příkladu opětovného zpracování již jednou získaných osobních údajů, jak tyto etické standardy mohou ovlivnit přístup vědce k otázce ochrany osobních údajů.

## Obecně k ochraně osobních údajů ve výzkumu

Abychom se vůbec mohli zabývat otázkou, jak chránit osobní údaje při realizaci výzkumu, je vhodné krátce zmínit, v jakém případě se jedná o vědecký výzkum ve smyslu GDPR. V bodu odůvodnění 159 Obecného nařízení je zdůrazněno, že pojem „vědecký výzkum" je nutno chápat spíše šířeji, a obsahuje proto nejen aplikovaný či technologický výzkum, ale i výzkum hrazený ze soukromých zdrojů. Výzkum, ačkoli financovaný ze soukromých zdrojů, by měl být přinejmenším alespoň zčásti veden za účelem veřejného zájmu. Pokud tomu tak není, výjimka z běžného režimu zpracování se neuplatní.

Pro lepší pochopení základních pojmů ochrany osobních údajů ve výzkumu je vhodné vysvětlit, co se jednotlivými pojmy myslí. Za **osobní údaj**[10] je třeba považovat jakoukoli informaci, která umožní, sama nebo ve spojení s jinými informacemi (např. jméno + IP adresa), určit, koho se týká – tato osoba je **subjektem údajů**. Co se týče informací o **trestných činech**[11], požívají údaje o odsouzení, ale i údaje s odsouzením související, zvláštní ochrany, jelikož jejich náhodné šíření může mít negativní dopad na jejich zaměstnání či soukromí.[12] Z toho důvodu je třeba s těmito údaji nakládat s větší péčí a opatrností, nežli tomu je u jiných osobních údajů. Některé údaje jsou

[8] Pro kriminology nejbližší oborově i geograficky budou např. dokumenty britské kriminologické či sociologické společnosti (The British Society of Criminology, n.d., British Sociological Association n.d.). V kriminologii lze předvídat např. rozšíření etických komisí projednávajících návrhy výzkumů, běžné v zahraničí či v medicinských vědách.

[9] Podobně i Evropská komise rozlišuje mezi GDPR a H2020 etickými standardy (European Commission, 2018, s. 5).

[10] Teorie rozlišuje definici tzv. subjektivního a objektivního pojetí pojmu osobní údaj. Dle objektivního přístupu se jedná o osobní údaj v případě, kdy někde objektivně existuje další informace, která může pomoci vytvořit potřebné prostředí a kontext pro opětovnou identifikaci údajů. Subjektivní pojetí však vnímá situaci tak, že o osobní údaj se nejedná tehdy, pokud správce osobních údajů nemá potřebné informace k identifikaci, přestože může potřebná informace někde, mimo jeho dosah (objektivně) existovat. Jelikož je subjektivní přístup příliš zužující, k objektivnímu pojetí se připojil také Soudní dvůr Evropské Unie v rozsudku ze dne 19. 10. 2016 ve věci C582/14 - Breyer.

[11] Pod tento pojem spadají i údaje o podezřelém, zahlazení odsouzení a obětech trestných činů. K tomu blíže viz https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/criminal-offence-data/what-is-criminal-offence-data/.

[12] Bod odůvodnění 75 GDPR.

označené jako **zvláštní kategorie**[13] nebo **citlivé**[14], jelikož se týkají rasy, přesvědčení, zdravotního stavu či sexuální orientace. Nároky na zpracování těchto údajů jsou proto vyšší.[15] Důvodem, proč údaje o trestných činech nejsou údaji citlivými, je dán především zájmem společnosti[16] na jejich případném šíření za účelem veřejného zájmu, což by u citlivých údajů nebylo možné.[17] Můžeme si proto údaje o trestné činnosti z hlediska nutnosti ochrany představit jako jakýsi mezičlánek mezi „běžným" a citlivým osobním údajem.[18]

Pokud z údajů nelze osobu identifikovat, Obecné nařízení se neaplikuje, jelikož se nejedná o osobní údaje. Stejně tak povinnosti vyplývající z Obecného nařízení zanikají okamžikem **anonymizace** údajů, tedy uskutečněním operace, po které již subjekt nelze identifikovat. Pokud lze identifikovat subjekt údajů pouze prostřednictvím číselného identifikátoru, který je uložen separátně od sady anonymizovaných dat, jedná se o **pseudonymizaci**[19], která představuje jedno z opatření napomáhajících zajištění souladu výzkumu pracujícího s osobními údaji s Obecným nařízením, avšak na rozdíl od anonymizace nadále zůstávají údaje po pseudonymizace nadále osobními.

**Zpracováním** se rozumí jakákoli operace s osobními údaji – od jejich získání, uspořádání, pozměnění, smazání či předání třetí osobě.[20] **Správcem** se v souladu s článkem 4 odst. 7 GDPR rozumí osoba, která samostatně určuje, za jakým účelem a jakými prostředky budou osobní údaje zpracovávány. Zároveň je tato osoba (ať už fyzická, nebo právnická) odpovědná za splnění veškerých požadavků na zpracování osobních údajů od doby jejich získání po jejich zničení či úplnou anonymizaci. Může jím být samostatný výzkumník, nebo častěji jeho zaměstnavatel, tedy vědecká instituce. **Zpracovatel** dle článku 4 odst. 8 GDPR zpracovává osobní údaje pro správce, tedy na základě jeho pokynů. Jedná se například o externího brigádníka, který na základě pokynů výzkumníka vede rozhovory, během kterých získává předem

[13] Pro zpracování zvláštní kategorie osobních údajů musí být vzhledem k jejich charakteru dostatečně dobrý důvod – Obecné nařízení mezi ně zařazuje vědecký výzkum, avšak pouze, pokud je pro účel jeho vedení zpracování takových údajů nezbytné.

[14] Ačkoli je pojem „citlivé údaje" upraven směrnicí 95/46/ES, kterou GDPR nahradilo spolu s novým pojmem „zvláštní kategorie údajů", pro svoji zavedenost se často nadále používá, a odkazuje na něj i GDPR v bodu odůvodnění 10.

[15] Čl. 9 GDPR.

[16] Srov. § 6 odst. 2 písm. b) z. č. 110/2019 Sb., o zpracování osobních údajů.

[17] K tomu blíže spolu se seznamem možných opatření blíže zde: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/.

[18] Velká Británie proto vzhledem k specifickému postavení dat o trestné činnosti přijala předpis, který zahrnuje úpravu údajů o trestné činnosti spolu s citlivými údaji, blíže viz: https://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted.

[19] Až užitím identifikátoru lze propojit pseudonymizovaná data a separátně uložené osobní údaje.

[20] Čl. 4 odst. 2 GDPR.

stanovené osobní údaje, a to za předem stanoveným účelem, který určil výzkumník samostatně, či prostřednictvím vědecké instituce – správce.

Každé zpracování osobních údajů musí být zákonné, tedy každé jednotlivé zpracování musí být podloženo **právním titulem**, který představuje oprávnění správce tyto údaje zpracovávat. Jedním z příkladů nepochopení Obecného nařízení je představa, že ke každému zpracování osobních údajů je zapotřebí souhlas. Ten je však pouze jedním z šesti právních titulů a aplikuje se pouze v případě, kdy nelze zpracovat údaje na základě jiného titulu – nadužívání požadování souhlasů je pro subjekty údajů zbytečně zatěžující. Mezi typické právní tituly při zpracování osobních údajů ve výzkumu bude patřit souhlas, zpracování ve veřejném zájmu a oprávněný zájem správce (Summers & Woollard, 2020, s. 163).

**Splnění úkolu prováděného ve veřejném zájmu** bude jedním z nejčastějších právních titulů, který budou vědci uvádět. V ČR se budou vysoké školy odkazovat na zákon o vysokých školách, jejichž úloha je uchování a rozhojňování dosaženého poznání a pěstování vědecké, výzkumné, vývojové a inovační činnosti,[21] ústavy Akademie věd ČR na zákon o Akademii věd ČR, dle kterého jednotlivá pracoviště uskutečňují vědecký výzkum, přispívají ke zvýšení úrovně poznání a vzdělanosti a k využití výsledků vědeckého výzkumu a získávají, zpracovávají a rozšiřují vědecké informace.[22] **Souhlas subjektu údajů** bude titulem (případně dalším titulem) ve vybraných oblastech výzkumu, například typicky při vedení rozhovorů. Titul **oprávněného zájmu správce**[23] je pak nejproblematičtější kategorií.[24] Pokud správce tvrdí, že zpracování daných osobních údajů potřebuje z určitého významného důvodu, který se jej týká, nesmí zájem správce převážit práva a očekávání subjektu údajů,[25] a nelze tak tuto kategorii chápat jako extenzivní, sběrnou kategorii (Pattynová, 2019). Nesprávné užití tohoto právního titulu má totiž za následek nezákonnost zpracování. Jelikož je správce vzhledem ke své odpovědnosti za zajištění veškerých aspektů zpracování jím spravovaných údajů, je vhodné se této chybě vyvarovat.

Mezi tituly jen zřídka využitelné v oblasti výzkumu patří nezbytnost zpracování pro splnění smlouvy (např. pro realizaci objednávky), splnění právní povinnosti (např. odvádění dávek sociálního pojištění zaměstnavatelem, jehož

[21] § 1 písm. a).
[22] § 13 písm. a).
[23] Oprávněným zájmem se především rozumí, že správce má dostatečně dobrý důvod ke zpracování osobních údajů, aniž by k tomu potřeboval výslovný souhlas. Jedná se například o ochranu majetkových zájmů pomocí užití kamery.
[24] Příkladům aplikace tohoto právnímu titulu ve vědeckém výzkumu se věnuje stanovisko WP 29 k pojmu oprávněného zájmu správce údajů podle čl. 7 směrnice 95/46/ES ze dne 9. dubna 2014, dostupné zde:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.
[25] Typickým příkladem je umístění bezpečnostních kamer v prostorách vědecké instituce za účelem ochrany majetku.

uplatnění ve výzkumu je nepravděpodobné, ledaže např. předání těchto údajů orgánům veřejné moci předpokládá právní předpis) a pro ochranu životně důležitých zájmů subjektu údajů či jiné osoby, tedy např. identifikaci pacienta v bezvědomí, což je ve výzkumu velice nepravděpodobné.

Jedním ze základních principů zpracovávání osobních údajů je **zásada minimalizace**, dle které by mělo docházet k co nejmenšímu zásahu do práv subjektů údajů, přičemž míra zásahu je určována zejména účelem zpracování a shromáždění osobních údajů.[26] Výjimkami opětovného užití dat pro výzkum se zabýváme níže. V případě, že by měly být osobní údaje zpracovávány ve větším rozsahu, než byl původně vymezen, nejsou zpracovávány na základě platného právního titulu. Ve vztahu ke každému zpracování musí správce subjekt údajů informovat o veškerých náležitostech zpracování, a teprve pokud se správce drží těchto mantinelů, může být takové zpracování v souladu s obecnými principy zpracování dle GDPR.

Odlišnost zpracování osobních údajů ve výzkumu se nejvýrazněji projevuje v omezení práv subjektů ve prospěch zájmu společnosti na vedení výzkumu, a tím i získávání nových poznatků. Omezena jsou zejména práva na plnění informační povinnosti, na výmaz osobních údajů a práva vznést námitku proti zpracování, přičemž však musí být dodrženy další dostatečné záruky řádného zpracování. Konkrétně při zpracování osobních údajů ve výzkumu není nutné plnit informační povinnosti, pokud osobní údaje byly získány jinak, než na základě souhlasu subjektu údajů (např. od jiné instituce), a to za předpokladu, že splnění této povinnosti by (i) vyžadovalo nepřiměřené úsilí, nebo (ii) by její realizace znemožnila či ztížila dosažení cíle výzkumu.[27] Podobně není možné vyhovět žádosti subjektu na výmaz osobních údajů, pokud by uplatnění tohoto práva znemožnilo naplnění cíle výzkumu,[28] a subjekt nemůže vznést námitku, pokud je výzkum veden jako splnění úkolu prováděného z důvodu veřejného zájmu.[29]

**Anonymizace kvantitativních dat, textu a audiovizuálních záznamů**

Jak jsme uvedli v úvodu, jsou-li data anonymizovaná, není třeba se zabývat ochranou osobních údajů. Anonymizace lze dosáhnout, pokud již neexistuje způsob, jak osobu na základě získaných dat identifikovat. Dosažení anonymizace tak, aby naplnila svou definici, je však velmi individuální. Bohužel platí, že nástroje, které byly využity v minulosti jinými subjekty pro dosažení anonymizace údajů, nemusí vést ke

[26] Čl. 5 odst. 1 písm. c) GDPR, bod odůvodnění 29 GDPR.
[27] Čl. 14 odst. 5 písm. b) GDPR.
[28] Je ovšem nutno posoudit, zda je smazání jednoho žadatele o smazání osobních údajů dostatečně způsobilé omezit výzkum. Pokud existuje dostatečný důvod, který spočívá především ve změně statistiky, může správce – výzkumník s ohledem na čl. 17 odst. 3 písm. d) GDPR odmítnout již prvního žadatele o výmaz. Pokud tomu tak není, může být takto odmítnut až např. padesátý žadatel.
[29] Čl. 21 odst. 5 GDPR.

stejnému výsledku i v současnosti či pokud s daty pracují jiní výzkumníci, kteří disponují dalšími daty. Blíže si proto přiblížíme logiku, s jakou při zajištění co nejvyšší ochrany údajů postupovat.

Evropský inspektor ochrany osobních údajů (EDPS) spolu se španělským Úřadem pro ochranu osobních údajů (AEPD) vydal přehledné stanovisko (2021) věnující se nejčastějším nesrovnalostem při procesu anonymizace. V něm uvádí, že ne vždy je možné anonymizace vůbec dosáhnout. Typicky se bude jednat o případ, kdy okruh potenciálních dotčených subjektů je natolik malý, že je možné dosáhnout identifikace pouze na základě vymezení skutkového vymezení zkoumaného trestného činu, například velezrady. V takovém případě je nutno nahlížet na data jako na osobní údaje a tím pádem splňovat kritéria GDPR.

Nástrojem, který lze využít, pokud anonymizace nelze dosáhnout, je pseudonymizace osobních údajů. Ta umožňuje, aby osobní údaje mohly být přiřazeny ke konkrétnímu subjektu, ale pouze za pomocí identifikátoru, který je uchováván odděleně. Pokud tedy vedeme anonymizovanou tabulku, která obsahuje pouze číslo účastníka, a nikoli jeho jméno, a zároveň je odděleně uchovávaná tabulka, která číslo účastníka přiřazuje ke konkrétním osobním údajům, ke kterým má však přístup mnohem užší okruh osob, jedná se o pseudonymizaci. Ta je podstatná proto, že zmenšuje riziko případného zneužití dat. Pokud však výzkumník změní jména a všechny další údaje umožňující identifikaci a neuchová si tabulku propojující původní a pozměněné údaje, tedy pokud žádný z dalších údajů není schopen identifikovat subjekt údajů, jedná se o anonymizaci a nikoli o pseudonymizaci.

Stejně tak nelze spoléhat na to, že anonymizace je trvalý proces. Spolu s vývojem kvantových počítačů přináší technika neustále další možnosti, jak odhalit data, která nyní odhalit nedokážeme. Ačkoliv se tato informace může zdát jako příliš daleká budoucnost, je třeba ji mít na paměti a být na možnost aplikace GDPR v polovině výzkumu připraven. Anonymizace proto zcela nevylučuje možnost opětovné identifikace v budoucnosti, i přesto je nejlepším nástrojem v oblasti zajištění práva na ochranu osobních údajů. Je však nutno brát v potaz skutečnost, že náklady vynaložené na identifikaci mohou být nepatrné v porovnání s hodnotou získaného osobního údaje. Anonymní jsou proto jen ta data, jejichž následná identifikace by vyžadovala nepřiměřeně mnoho úsilí a práce (Koščík et al., 2017, kap. Anonymizace a pseudonymizace – od binárního ke škálovatelnému).

Stanovisko dále upozorňuje na to, že anonymizaci nelze popsat pouze tak, že je, či není; vždy lze analyzovat a měřit její stupeň, a tím i pravděpodobnost opětovné identifikace. Není proto možné jednoznačně stanovit hranici, dokdy je míra natolik nízká, že lze údaj brát za anonymizovaný. Existuje široká šedá zóna, která se průběžně proměňuje. Z hlediska výzkumu je podstatné, že anonymizace nemůže vést k tomu, že by se data stala nepoužitelnými pro předem definovaný účel.

Jedním z nástrojů anonymizace dat v písemné podobě je znemožnění přečtení osobních údajů. Nestačí však text pouze černě zabarvit v textu, jelikož je text možno

v počítači zvýraznit, a tím i přečíst. Vhodným nástrojem je proto jejich smazání, nebo nahrazení jinými znaky (např. XXX). Rozsahu anonymizovaných údajů se věnuje tabulka níže.

Další možností, jak anonymizace mimo jiné docílit, je užití pseudonymů či jiných vágních označení, které neumožní následnou identifikaci konkrétních osob, za současného nezaznamenání údajů propojujících pseudonymy a označení s dalšími údaji identifikující osobu. Vždy je však třeba vzít v potaz, jak byla nastavena kritéria zpracování již před zahájením výzkumu. Domluva s účastníky na tom, jaké informace mohou či nemohou být nahrávány či přepisovány do záznamů, totiž představují vhodnější postup nejen z hlediska následné jednodušší revize dat, ale i pro naplnění očekávání účastníků z hlediska kontroly nad poskytovanými daty a tím i větší ochotu se výzkumu účastnit.

Pokud je z vedeného rozhovoru vytvářen audiovizuální záznam, je následná korekce poměrně složitá. Příliš časté „vypípávání" či střih by mělo za následek nižší srozumitelnost nahrávky, a je proto pro výzkumníka vhodnější zajistit před provedením rozhovoru informovaný souhlas se zpracováním osobních údajů.

Při anonymizaci psaného textu je dále třeba mít na paměti, že přílišné odstraňování dat ve snaze zajištění souladu s GDPR může znemožnit vedení výzkumu. Je proto podstatné vždy zohlednit, (i) jaká data bude skutečně potřeba získat a proč (což je třeba zaznamenat do záznamu o činnostech zpracování[30]), (ii) identifikovat přímé a nepřímé identifikátory, (iii) užít pseudonymy či vyvarování se samotnému sběru těchto dat (viz výše), (iv) ponechat si původní, neanonymní verzi a zajistit její zabezpečení, (v) učinit záznam o provedené anonymizaci. Pro lepší představu vedení záznamu zpracování, včetně možného řešení, uvádíme základní možnosti anonymizace v Tabulce 1. Pokud by nebyl uchován klíč propojující původní a upravený záznam a ostatní údaje neumožňovaly identifikaci konkrétní osoby, jednalo by se o anonymizaci. Pokud by naopak propojující klíč byl odděleně uložen, resp. by bylo možné propojit upravené a původní záznamy, pak by se jednalo jen o pseudonymizaci.

**Tabulka 1. Možnosti anonymizace**

| | |
|---|---|
| narozen 7. 3. 1985 | Věková skupina 35–40 let / věk 35 let |
| Jan Novák | Jan / obžalovaný č. 4 / Roman (pseudonym) / oběť TČ |
| Most | město v Ústeckém kraji / město nad 50 tis. obyvatel |

[30] Hlavním cílem těchto záznamů je zjednodušení komunikace s Úřadem pro ochranu osobních údajů v případě zahájení šetření, a zároveň usnadňuje a zpřehledňuje organizační aspekt zpracování. Úřad pro ochranu osobních údajů nabízí vzor záznamu o činnostech zpracování zde: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30188.

Co je a co není osobním údajem, není jednoznačně dané – šedá zóna je široká a záleží na okolnostech: Může být tedy například závislá i na konkrétním období. Příkladem může být spisová značka, která může být považována za osobní údaj, pokud jsou k dispozici nástroje, které umožňují přiřazení spisové značky společně s dalšími údaji o osobě a trestním řízení ke jménu osoby, jako třeba webová stránka Právnické výpočty, kde je možné dohledat jméno ke konkrétní spisové značce.[31] Vzhledem k omezenému rozsahu v Právnických výpočtech lze však považovat za osobní údaje pouze spisové značky z vybraných let (např. nikoli již od března 2020, kdy jména účastníků přestala být zveřejňována v InfoJednání,[32] které sloužilo jako zdroj údajů pro tuto databázi). Ačkoliv se nejedná o oficiální databázi, jedná se o způsob, jakým je identifikace možné dosáhnout, a spisová značka se proto může jednoduše stát osobním údajem.

Prvek identifikace proto musí být posuzován do určité míry individuálně. Zatímco GPS lokace spáchání trestné činnosti zaznamenaná jako sto metrový rádius v Praze neumožňuje určení konkrétního místa spáchání trestného činu, stejný rádius ve venkovských oblastech už konkretizaci umožňuje výrazně častěji. V tomto lze spatřit jeden z hlavních problémů pochopení ochrany osobních údajů: Neexistuje univerzální postup, který by zajistil správné řešení. Namísto toho je nabídnut systém pravidel a principů, nad kterými je potřeba se při individuální aplikaci zamyslet. Zajímavým z tohoto pohledu je například rozsudek Nejvyššího správního soudu z roku 2009, dle kterého ani jméno ve spojení s číslem občanského průkazu není osobním údajem, jelikož za zásadní považuje možnost osobu kontaktovat na základě poskytnutých údajů.[33] Jednalo se nicméně o překvapivé rozhodnutí, jelikož zpochybnilo nezbytnost jejich ochrany (Zahumenská & Zahumenský, 2013), a je do určité míry vnímáno jako exces.

Zároveň je třeba vyvarovat se přehnané snahy o ochranu osobních údajů. Pokud údaje zveřejňované v publikacích samy o sobě nejsou schopny identifikovat konkrétního pachatele se skutky, není zapotřebí další anonymizace, například: muž, nar. 1995, vykradl prodejnu potravin v Jeseníku (Gealfow & May, 2019), jelikož v případě nemožnosti identifikace se nejedná o osobní údaj, a není proto chráněn GDPR.

[31] Viz https://www.pravnicke-vypocty.com/psj/.

[32] Srov. diskuzi v usnesení sp. zn. III. ÚS 1017/20 ze dne 19. 6. 2020.

[33] „Za osobní údaj však zdejší soud nepovažuje ani jméno a příjmení osoby (návštěvníka) ve spojení s číslem jeho občanského průkazu. Ani na základě těchto údajů totiž není možné konkrétní osobu určit nebo kontaktovat. Neexistuje totiž žádný veřejně dostupný registr čísel občanských průkazů, v němž by bylo možné zjistit identitu osoby podle čísla průkazu." Rozsudek Nejvyššího správního soudu ze dne 29.7.2009, čj. 1 As 98/2008 - 148, č. 1944/2009 Sb. NSS, str. 11.

**Vyvažování dostatečné ochrany osobních údajů a přijatých opatření**

Celou úpravou Obecného nařízení prostupuje tzv. přístup založený na riziku, který spočívá v povinnosti správce a zpracovatele zajistit dostatečná organizační a technická opatření, která jsou přiměřená potenciálnímu riziku ohrožení práv subjektu údajů (ÚOOÚ, 2017). Posouzení, zda dané zpracování představuje pravděpodobné či závažné ohrožení práv účastníků výzkumu, je významné pro posouzení rizikovosti zpracování.[34]

Rizikovost daného zpracování se posuzuje především s ohledem na skutečnost, zda jsou zpracovávány citlivé údaje, jejich objem, přístup k nim, předávání těchto osobních údajů dalším subjektům či délku jejich zpracování. Nejméně rizikovým je zpracování pseudonymizovaných dat jedním výzkumníkem, zatímco zjevné riziko bude naopak představovat několikaletý výzkum zaznamenávající údaje o jménu, místě výkonu trestu a zdravotním stavu, se kterými pracuje hned řada výzkumných institucí. Většina výzkumů se však bude pohybovat mezi těmito extrémy. Obecnou radou je být spíše opatrnější. Pokud existuje podezření, že zpracování představuje vysoké riziko pro práva subjektů osobních údajů, je třeba od počátku předpokládat, že rizikové jsou, a odpovídajícím způsobem s nimi zacházet. V průběhu jejich analýzy lze posoudit, že riziko není tak vysoké, jak se zpočátku mohlo zdát, či že jsou již zajištěny dostatečné záruky ochrany práv subjektů, v návaznosti na což lze míru ochrany rozvolnit. Za tímto účelem je proto vhodné zařadit dva klíčové mechanismy pro zajištění řádného zpracování. Zaprvé, jmenování pověřence pro ochranu osobních údajů, který by měl být schopen porozumět dané oblasti a datům a navrhovat přiměřená opatření. Ten může zajistit druhý mechanismus – analýza zpracovávaných osobních údajů – známá jako posouzení vlivu na ochranu osobních údajů (takzvané „DPIA", Data Protection Impact Assessment).

Pokud hlavní činnost výzkumníka spočívá v rozsáhlém zpracování osobních údajů týkajících se rozsudků v trestních věcech, je jmenování pověřence dokonce povinné.[35] I v opačném případě je však jeho jmenování vhodné, a to především s ohledem na potřebu se poradit s odborníkem, obzvlášť pokud nemá výzkumník příliš zkušeností s úpravou práva na ochranu osobních údajů. Pokyny k funkci pověřence pro ochranu osobních údajů[36] dále uvádí, že pověřenec by měl být schopný zanalyzovat, zda správce zajistil dostatečná opatření v oblasti ochrany osobních údajů. Konkrétní poznatky a návrhy řešení jsou však vždy v rovině doporučení a konečné rozhodnutí je na správci. Praktickým problémem nicméně může být, že vzhledem k výrazné specifičnosti ochrany osobních údajů ve výzkumu se v této oblasti pověřenci pro ochranu osobních údajů zabývající se „běžnou" ochranou osobních údajů nemusí

[34] Bod odůvodnění 76 GDPR.
[35] Čl. 37 GDPR.
[36] Pokyny WP 29 k funkci pověřence pro ochranu osobních údajů ze dne 13. 12. 2016, dostupné na: https://www.mpo.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/gdpr-dokumenty/2018/1/Preklad-Metodiky-poverence-WP29.pdf.

příliš orientovat, respektive mohou k ochraně osobních údajů přistupovat příliš restriktivně a formalisticky, aniž by zohlednili specifika ochrany osobních údajů ve výzkumu. I zde je třeba dbát na výběr pověřence z hlediska jeho zkušenosti s realizací výzkumu: i GDPR předpovídá, že pro práci pověřence může být například důležitější, aby se orientoval ve výzkumné agendě profesně, než aby měl právnické vzdělání.[37]

V případě, že zpracování představuje vysoké riziko, je třeba zpracovat DPIA, jehož součástí je zhodnocení původu, povahy a závažnosti takového rizika,[38] a to již před zahájením zpracování údajů. K takové situaci typicky dochází u tvorby rozsáhlých databází, a to obzvláště pokud obsahují neanonymizovaná a citlivá data.[39] Vzhledem k tomu, že výzkumníci pravidelně operují s velkým množstvím dat, a zároveň je DPIA základním mechanismem zajištění přiměřených záruk, je vhodné DPIA zpracovat, a to i za předpokladu, že je pouze pravděpodobné, že dané zpracování může být rizikové.

Jak DPIA provést?[40] DPIA by mělo nejdříve obsahovat popis účelu zpracování dat, správce, zpracovatele a právního titulu. Následně by mělo dojít ke zhodnocení rizikových kritérií (citlivé údaje, rozsáhlost, pravděpodobnost kybernetického útoku) a určení vhodných opatření, které by bylo doprovozeno vytvořením dokumentu zhodnocujícím stav možných rizik[41] doprovozený návrhy řešení, pokud toto riziko existuje. Po implementaci takto definovaných opatření již dostačí jen s odstupem vyhodnocovat jejich efektivnost.

**Správa a skladování dat**

Speciální otázkou ochrany osobní údajů je jejich správa a skladování. Jelikož řada výzkumníků nemá k dispozici pověřence pro ochranu osobních údajů za účelem konzultace postupu, pokusíme se níže přiblížit některé nástroje a principy, které lze při práci s daty užít. Vždy však platí, že je vždy třeba poměřovat, jaká opatření jsou dostatečná k zajištění ochrany dat, a pokud si výzkumník není jistý, nakolik je riziko jejich úniku či poškození pravděpodobné, je vždy lepší jít cestou vyšší ochrany dat. Plánování postupu správy dat je klíčové z hlediska jejich dalšího zpracování. Vzhledem k tomu, že jejich životnost je často delší než samotný výzkum, je zásadní jejich řádná správa za účelem plánování jejich zpracování, dalšího užití či předávání pomocí vhodného mechanismu brzké detekce potenciálních rizik a překážek, což

[37] Srov. bod odůvodnění 97 GDPR.
[38] Bod odůvodnění 84 GDPR.
[39] Bod odůvodnění 90 GDPR.
[40] Přehledný vzor DPIA poskytuje volně k dispozici např. publikace Polčák et al. (2018).
[41] Hodnoceno buď čísly, nebo barvami od zelené (zanedbatelné či žádné riziko) přes oranžovou k červené (vysoké riziko, učinit nová opatření je zcela nezbytné, jelikož stávající je nedostačující).

umožní vyvarovat se řadě problémům.[42] Dobré praxe lze docílit zejména za použití následujících postupů:

- Užití mezinárodních standardů pro správu dat;[43] volba vhodného software pro správu dat (tzv. DMP, Amorim et al., 2017)[44], včetně stanovení pravidel pro ukládání a sdílení těchto dat a jejich zabezpečení;
- rešerše etických standardů a principů správy dat, například FAIR principy, implementované Evropskou komisí v roce 2016,[45] uplatňované v rámci The European Open Science Cloud (EOSC), podporující výzkum v rámci EU;[46]
- jasné vymezení rolí a pravomocí jednotlivých výzkumníků včetně zhodnocení toho, která opatření jsou vhodná a dostačující z hlediska výzkumné instituce, konkrétního projektu, ale i nákladů, které by bylo možné vynaložit na zajištění dalších opatření (např. softwaru na správu dat či jejich zabezpečení);
- plán správy dat[47] za pomocí check-listu (DCC, 2013) či existujícího DMP softwaru.

Při skladování osobních údajů je potřeba mít na mysli několik jednoduchých principů. Pokud jsou osobní údaje uchovány rovněž ve fyzické formě (dotazníky, záznamy, ale i USB disky), musí být uchovány na takovém místě, na které má přístup pouze výzkumník, který se na daném výzkumu podílí. Pokud tedy místnost sdílí vícero výzkumníků s různorodými projekty, je zapotřebí zajistit uzamykatelnou skříňku, ke které má přístup pouze příslušný výzkumník.

Pro elektronickou formu je nutno myslet na zajištění bezpečnosti samotného zařízení, a to zejména použitím silných hesel a kvalitního antivirového programu. I v rámci databáze či sdílených disků instituce je zapotřebí, aby i v tomto případě byl přístup k těmto složkám omezen. S ohledem na povahu a rizikovost úniku dat je vhodné data rovněž šifrovat,[48] a to tak, že k nim mohou získat přístup pouze autorizované osoby.[49] Máme dobrou osobní zkušenost např. s používáním operačního systému založeného na Linuxu (Ubuntu), šifrování hard-disku pomocí nástroje VeraCrypt a šifrování záložních hard-disků či jiných zálohovacích zařízení pomocí

[42] Dobrým vodítkem mohou být již existující doporučení zavedených institucí. Více informací nabízí např. Cambridgeská univerzita zde: https://www.data.cam.ac.uk/data-management-guide.
[43] Např. The Data Documentation Intiative (DDI) či The Open Archival Information Systém (OAIS).
[44] Blíže např. https://eudat.eu/.
[45] *Go Fair*. Dostupné z: https://www.go-fair.org/fair-principles/.
[46] *European Open Science Cloud*. Dostupné z: https://ec.europa.eu/info/research-and-innovation/strategy/goals-research-and-innovation-policy/open-science/european-open-science-cloud-eosc_en.
[47] *Data Management Plan (DMP).* Dostupné z: https://openscience.cuni.cz/OSCIEN-49.html.
[48] Čl. 32 GDPR.
[49] *Encryption*. Dostupné z: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/.

stejného nástroje, byť si jsme vědomi, že některé z těchto nástrojů nebude možné jednoduše použít například v rámci státní správy.

Při předávání dat je dnes již možné ustoupit od předávání dat na CD, případně jinými formami, jelikož lze soubory zasílat dostatečně zabezpečeně skrze speciální služby umožňující šifrování od nahrání souboru po jeho stažení. Pro pracovníky v akademické sféře je například dostupný nástroj FileSender,[50] založený na principu šifrování při nahrávání a stahování a zaslání klíče k rozšifrování skrze jiný kanál (ideálně formou telefonického hovoru či případně SMS). Ten umožňuje poslat i pozvánku třetí osobě, takže se tato bezpečná komunikace nemusí omezovat na předávání dat mezi akademiky.

**Opětovné užití osobních údajů za účelem dalšího výzkumu**

Kriminologové – podobně jako mnozí jiní vědci – velmi často pracují se sekundárními daty, tedy daty vytvořenými ostatními (zejména státními institucemi) pro jiné účely než pro realizaci konkrétních výzkumů. Stejně jako zpracování ve větším rozsahu, než bylo původně vymezeno, i rozšíření účelu představuje pro zpracování osobních údajů potenciální riziko pro práva subjektu údajů. Aby k takové situaci nedošlo, jsou účely zpracování před jeho zahájením často formulovány velmi široce. V praxi však pravidelně dochází k situaci, kdy jednou získaná data je potřeba použít znovu, avšak za jiným účelem.

Takový postup je v případě běžného režimu zpracování možný pouze v případě, pokud projde tzv. testem slučitelnosti účelů. Jeho podstatou je posouzení, (a) zda mezi předchozím i novým účelem zpracování existuje souvislost,[51] (b) za jakých podmínek došlo k získání údajů, především pokud se jedná o citlivé údaje, (c) jaké může mít změna účelu dopad na subjekt údajů a (d) jaké záruky zákonného zpracování správce může zajistit (Pokorná & Dvořáková, 2020, s. 50). Pokud nový účel není slučitelný s účelem původním, musí být následné zpracování učiněno pouze na základě nového právního titulu, kterým bude typicky souhlas subjektu údajů. Získání takového souhlasu však může být například v případě longitudinálního výzkumu velmi obtížné či dokonce nemožné a ztěžovalo by jeho vedení i získávání poznatků. Obecné nařízení proto upravuje v čl. 5 odst. 1 písm. b) výjimku, kdy další zpracování pro účely vědeckého výzkumu a statistické účely se nepovažuje za neslučitelné s původním účelem za současného dodržení dostatečných záruk dle čl. 89 odst. 1 GDPR. Je však potřeba mít na paměti, že i nadále musí být pamatováno na další zásady zpracování, jakými jsou minimalizace údajů, jejich důvěrnost a integrita a požadavek na aplikaci pseudonymizace na veškerá data, kde je to možné.[52] Jak již

[50] Dostupné na https://filesender.cesnet.cz/.
[51] Typickou souvislostí bude v kontextu kriminologie především další výzkum, který je obsahově podobný, nebo na původní výzkum navazuje.
[52] Čl. 89 GDPR.

bylo poukázáno výše, etické standardy právě v tomto aspektu sehrávají klíčovou roli – následné zpracování, které je v souladu s GDPR, nemusí být totiž etické.

Etické standardy kromě požadavků na záruky zpracování dále omezují vědce v jinak volném zpracování osobních údajů, a to i při užití nevýzkumných dat za výzkumnými účely (Polčák et al., 2018). I jestliže je účel primárního zpracování slučitelný s následným zpracováním (pokud nikoli, znamená to, že původní účel je natolik odlišný, že není spravedlivé požadovat po subjektu údajů, aby s takovým zpracováním bez dalšího souhlasil), může nastat situace, kdy i přes soulad s GDPR nemusí být následné zpracování v souladu s etickými standardy.

Do hry proto vchází potřeba respektovat přání účastníků výzkumu ohledně přehledu nad účely následných zpracování. Právě jedním ze specifik v oblasti výzkumu je užití tzv. rozsáhlého souhlasu, který je specifický vágním stanovením účelu zpracování. Ten totiž často není možné v době shromáždění osobních údajů přesně určit. Obecné nařízení dle bodu odůvodnění 33 předpokládá, že by subjektu údajů mělo být umožněno, aby svůj souhlas se zpracováním vyjádřil pouze k určité části projektu či specifických oblastí výzkumu. Je však zapotřebí, aby tak bylo učiněno v souladu s účelem výzkumu tak, aby jeho průběh nemohl být znemožněn příliš úzce vymezeným souhlasem.

Právě úvaha, zda případná realizace práva subjektu práv nemá za následek ztížení či znemožnění výzkumu či statistiky, je klíčová pro vysvětlení výjimek z běžného režimu zpracování, jak bude popsáno níže. Jelikož tento rozsáhlý souhlas musí být udělen v souladu s etickými standardy, není možné uplatnit výjimku tam, kde by se dle GDPR uplatnit mohla, avšak podle etických standardů nikoliv. Právě tento aspekt činí tuto problematiku velmi složitou, jelikož si výzkumníci nemusí být vědomi existence všech závazných etických standardů, a při aplikaci musí ověřovat, zda je s nimi plánovaný výzkum v souladu.[53] Cílem ochrany účastníka výzkumu není pouze ochrana před jeho možnou identifikací, která vyplývá z práva na ochranu soukromí a zajištění důvěrnosti předávaných údajů (Negrouk & Lacombe, 2018). Vědec musí zkoumat i to, zda by subjekty údajů udělily či neudělily souhlas, pokud by jim byl konkrétní aspekt výzkumu znám, přičemž udělený rozsáhlý souhlas nebyl účelově dostatečně vymezen, nebo se jedná o zpracování za jiným účelem, než byl zprvu definován.

Při běžném zpracování je prováděn tzv. test slučitelnosti účelů, jehož cílem je zjistit, zda účel, který byl na začátku zpracování udělen, je v souladu s přiměřeným očekáváním subjektu údajů k dalším zpracováním. Tato otázka je významná pro posouzení, jaká mohou být očekávání účastníka výzkumu. Ochota subjektu údajů se do něj zapojit, pokud jsou údaje získávány díky jeho souhlasu, je často vázána na důvěru v danou vědeckou instituci, a je proto významné detekovat možné

[53] *The Research Ethics Guidebook*. Dostupné z: http://www.ethicsguidebook.ac.uk/index.html.

kontroverzní aspekty tak, aby je mohl subjektu výzkumu patřičně osvětlit a zároveň umožnit, aby se k nim mohl vyjádřit již před jeho zahájením (Peloquin et al., 2020).

Možný způsob řešení představuje tzv. dynamický souhlas, představující strategii průběžné oboustranné komunikace mezi výzkumníky a účastníky. Účastníci jsou tedy po prvotním udělení nadále informováni v případě nutnosti změny účelu vedení výzkumu pomocí předem určené platformy (např. webová aplikace), prostřednictvím které je usnadněn proces opětovného získávání souhlasu (Budin-Ljøsne et al., 2017). Tento způsob udržování účastníků je nejen efektivní z hlediska udržování účastníků, snížení nákladů na vedení výzkumu a zvýšení transparentnosti, ale rovněž zajištění etického aspektu respektování volby účastníka, na jakém druhu výzkumu je ochoten se podílet, jak je uvedeno níže. Ačkoliv zavedení komunikační platformy a její spravování představuje jistý náklad, dynamický souhlas je vhodnou a etickou formou právního titulu v případě vedení dlouhodobého výzkumu, který umožňuje vést transparentně dialog s účastníky výzkumu, a to pro obměňující se účely (Dankar et al., 2020).

**Praktická aplikace ochrany osobních údajů v kriminologickém výzkumu**

Jak má tedy jednat kriminolog, když by rád dodržel zásady ochrany osobních údajů? Nejprve si potřebuje stanovit, zda vůbec pracuje s osobními údaji. Obecné nařízení je aplikováno pouze v případě zpracování osobních údajů, tedy údajů o fyzických osobách, které jsou způsobilé je samy o sobě či v kombinaci s jinými identifikovat. Pokud se údaje například týkají pouze dat o spáchaném trestném činu a výši sazby, nejedná se o osobní údaje. O ty by se jednalo, pokud by obsahovaly rovněž jméno a adresu pobytu či spisovou značku, kterou by bylo možné jednoduše propojit s dalšími databázemi, umožňujícími identifikovat osobu.

Pracuje-li výzkumník s osobními údaji (např. zpracovává-li rozhovory s odsouzenými), jednou ze základních možností je data pseudonymizovat, jelikož takový přístup v mnohém zajistí ochranu osobních údajů (Mourby et al., 2018). Pseudonymizace obnáší vytvoření určitého klíče, kterým je unikátně identifikována určitá osoba a který sám o sobě nemá žádný význam, nicméně s jeho pomocí lze spojit původní databázi s další databází obsahující osobní údaje. Takto lze řešit situace, mělo-li by být možné třeba ve výjimečných případech účastníka kontaktovat (např. z důvodu potřeby upřesnění určitého výroku).

Jakmile kriminolog začne pracovat s osobními daty, je třeba, aby si výzkumník ujasnil, kdo je v rámci jeho výzkumu správcem a kdo zpracovatelem. Jak již bylo zmíněno výše, za sběr a uložení dat je často odpovědná přímo vědecká instituce, a je proto i správcem osobních údajů. Zpracovatelem pak bude typicky externí spolupracovník, který například na pokyny výzkumného pracovníka vede rozhovory s obžalovanými.

Jednotlivým právním titulům se článek věnoval výše, je však nutné podotknout, že při zpracování na základě souhlasu případné odvolání souhlasu se zpracováním neznamená automaticky odvolání souhlasu s účastí na výzkumu. Je proto vhodné osobní údaje získané na základě souhlasu anonymizovat, jelikož i v takovém případě výzkumník bude moci pracovat se získanými daty. Při získávání souhlasu od subjektu údajů je zapotřebí identifikovat správce osobních údajů spolu se subjektem údajů, za současného vysvětlení základních náležitostí souhlasu, jakými je stanovený účel zpracování (např. účast na kriminologickém výzkumu zabývající se recidivou), dobu zpracování a uvedení kontaktní osoby pro případ uplatnění některého z práv (např. právo na výmaz). Účel zpracování musí být natolik konkrétní, aby subjekt věděl, čím se výzkum vzhledem k poskytovaným údajům zabývá. Uvedení názvu konkrétního projektu by však znemožňovalo slučitelnost se sekundárním zpracováním s ohledem na etické standardy. Ujasnění si, na základě jakého právního titulu, za jakým účelem je výzkum veden, jakým způsobem (dotazníky, rozhovory) a po jakou dobu budou údaje zpracovávány, je klíčové pro splnění informační povinnosti (ÚOOÚ, 2013) ve vztahu k účastníkům výzkumu. Výzkumník by měl zároveň vzít v potaz etické a právní požadavky na transparentnost, a zahrnout rovněž informování o možných rizicích účasti na výzkumu (British Sociological Association, n.d.).

Při předávání dat jinému subjektu či osobě je vždy třeba zvážit, v jakém je postavení. Pokud se jedná o zpracování spočívající například v zajištění části výzkumu, a to na pokyny výzkumníka, je zapotřebí s tímto subjektem – zpracovatelem – uzavřít smlouvu o zpracování osobních údajů. V případě spolupráce na výsledcích výzkumu jsou oba subjekty v postavení správce, s čímž jsou spojena především rizika za řádné zpracování a samostatné rozhodování o účelech a prostředcích zpracování. V tomto případě bude proto zapotřebí uzavřít smlouvu o spolupráci v oblasti předávání osobních údajů.

V průběhu výzkumu nelze opomenout stručně zaznamenat veškerý cyklus zpracování dat,[54] od jejich získání (spolu s definováním zdroje, účelů, splnění informační povinnosti) a jejich případné anonymizování či pseudonymizaci přes tvorbu databáze (spolu s informacemi, kdo k ní má přístup) až po předání či smazání.

Pokud dle povahy výzkumu nelze mít údaje ani pseudonymizované, jedná se o potenciální riziko. Pokud se jedná o rozsáhlé zpracování, a to obzvláště, pokud se jedná o citlivé osobní údaje nebo o údaje související s trestnou činností, bude zapotřebí zpracovat DPIA, které pomůže zhodnotit, jak vysoké je riziko například úniku takových dat (především s ohledem na stav zabezpečení či jejich rozsáhlost), a na základě takové úvahy provést vhodná opatření, která budou způsobilá vyvážit zvýšené riziko oproti zpracování pseudonymizovaných dat (Alter & Gonzalez, 2018). V úvahu je nutno zahrnout kybernetickou bezpečnost, včetně bezpečnosti hesel,

[54] Bod odůvodnění 82 a čl. 30 GDPR.

softwaru a limitování přístupu, a to zejména ke kompletním, nezanonymizovaným datům. Vzor DPIA a procesů zpracování lze nalézt ve volně dostupné publikaci Metodika aplikace GDPR na výzkumná data v prostředí vysokých škol v ČR (Polčák et al., 2018), a může proto vedle tohoto článku napomoci při zajištění vhodných záruk při vedení (nejen) kriminologického výzkumu.

## Závěr

Klíčová fáze při zajištění ochrany osobních údajů nastává ještě před zahájením samotného výzkumu, a to učiněním takových bezpečnostních opatření, díky kterým nemusí dojít k jakémukoli pochybení či bezpečnostnímu incidentu. Toto pochybení může spočívat jednak v nerespektování zásad zpracování Obecného nařízení, a jednak v porušení etických standardů, které může ohrozit důvěru účastníků v samotný výzkum. Cílem tohoto článku bylo pomoci porozumět postupu zajištění ochrany osobních údajů tak, aby byla reálná a zároveň neomezující původní účel, za kterými byly získány. Nelze totiž podat technický postup, který by mohl být aplikovatelný pro každé jednotlivé případy stejně. Individuální a poučený přístup k nakládání s osobními údaji je proto ku prospěchu všem – účastníkům výzkumu, jejichž data jsou chráněna a nad kterými mají alespoň částečnou kontrolu spočívající v omezené možnosti uplatnění práv subjektu údajů, ale i výzkumníkům, kteří se nemusí bát případné kontroly ze strany Úřadu pro ochranu osobních údajů, nebo zdiskreditování výzkumu z důvodu nesprávného nakládání s daty, a tím i důvěryhodnosti příslušné vědecké instituce a výzkumníka.

*KAROLÍNA NOVÁ je absolventkou Právnické fakulty Univerzity Karlovy a pověřenkyní pro ochranu osobních údajů pro grantový projekt na Ústavu státu a práva Akademie věd ČR.*

*JAKUB DRÁPAL je výzkumníkem na Ústavu státu a práva Akademie věd ČR a na Právnické fakultě Univerzity Karlovy. Zabývá se ukládáním trestů a jejich výkonem, přičemž se zaměřuje na empirické studium soudních rozhodnutí. Je hlavním řešitelem grantů GA ČR „Rozdíly při ukládání trestů v postkomunistických právních systémech“ a „Podmíněně odložené tresty odnětí svobody v postkomunistické Evropě“.*

## Literatura

AEPD a EDPS. (2021). *10 misunderstandings related to anonymisation. EDPS* (online, cit. 1. 6. 2021), dostupné na adrese: https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf.

Alter, G., & Gonzalez, R. (2018). Responsible practices for data sharing. *American Psychologist*, *73*(2), 146–156. https://doi.org/10.1037/amp0000258

Amorim, R. C., Castro, J. A., Rocha da Silva, J., & Ribeiro, C. (2017). A comparison of research data management platforms: Architecture, flexible metadata and interoperability. *Universal Access in the Information Society*, *16*(4), 851–862. https://doi.org/10.1007/s10209-016-0475-y

British Society of Criminology. (n.d.) *Statement of Ethic*. http://www.britsoccrim.org/ethics/

British Sociological Association. (n.d.) *Guidelines on ethical research*. *BSA EDPS* (online, cit. 1. 6. 2021), dostupné na adrese: https://www.britsoc.co.uk/ethics.

Budin-Ljøsne, I., Teare, H. J. A., Kaye, J., Beck, S., Bentzen, H. B., Caenazzo, L., … Mascalzoni, D. (2017). Dynamic Consent: A potential solution to some of the challenges of modern biomedical research. *BMC Medical Ethics*, *18*(1), 4. https://doi.org/10.1186/s12910-016-0162-9

Dankar, F. K., Gergely, M., Malin, B., Badji, R., Dankar, S. K., & Shuaib, K. (2020). Dynamic-informed consent: A potential solution for ethical dilemmas in population sequencing initiatives. *Computational and Structural Biotechnology Journal*, *18*, 913–921. https://doi.org/10.1016/j.csbj.2020.03.027

DCC. (2013). *Checklist for a data management plan. v. 4.0*. *DCC* (online, cit. 1. 6. 2021), dostupné na adrese: http://www.dcc.ac.uk/resources/data-management-plans.

EDPS. (2020). *Preliminary Opinion on data protection and scientific research*. *EDPS* (online, cit. 1. 6. 2021), dostupné na adrese: https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en.

European Commission (2018). *Ethics and data protection*. *EC* (online, cit. 1. 6. 2021), dostupné na adrese: https://ec.europa.eu/info/sites/info/files/5._h2020_ethics_and_data_protection_0.pdf.

Gealfow, J., & May, C. (2019). Anonymizace osobních údajů v soudních rozhodnutích. *Revue pro právo a technologie*, *19*, 3–39.

Koščík, M., Polčák, R., Myška, M. & Harašta, J. (2017). *Výzkumná data a výzkumné databáze. Právní rámec zpracování a sdílení vědeckých poznatků*. Praha: Wolters Kluwer.

Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., … Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review*, *34*(2), 222–233. https://doi.org/10.1016/j.clsr.2018.01.002

Negrouk, A., & Lacombe, D. (2018). Does GDPR harm or benefit research participants? An EORTC point of view. *The Lancet Oncology*, *19*(10), 1278–1280. https://doi.org/10.1016/S1470-2045(18)30620-X

Pattynová, J. (2019). Článek 6 [Zákonnost zpracování]. In: J. Pattynová, L. Suchánková, J. Černý (Eds.), *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě. Komentář.* 2. aktualizované vydání. Ostrava: CODEXIS publishing.

Peloquin, D., DiMaio, M., Bierer, B., & Barnes, M. (2020). Disruptive and avoidable: GDPR challenges to secondary research uses of data. *European Journal of Human Genetics*, *28*(6), 697–705. https://doi.org/10.1038/s41431-020-0596-x

Pokorná, A., & Dvořáková, H. (2020). *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek: stěžejní judikatura SDEU a vybraná judikatura ESLP výkladové pokyny a stanoviska skupiny WP29 a EBDP: zákon o zpracování osobních údajů*. Praha: Wolters Kluwer.

Polčák, R., Ševčík, L., Koščík, M., Klodwig, J., & Holub, P. (2018). Metodika aplikace GDPR na výzkumná data v prostředí vysokých škol v ČR. https://doi.org/10.5281/zenodo.2532860

Pormeister, K. (2017). Genetic data and the research exemption: is the GDPR going too far? *International Data Privacy Law*, *7*(2), 137–146. https://doi.org/10.1093/idpl/ipx006

Summers, S., & Woollard, M. (2020). Legal and Ethical Considerations in Sharing Data. In: L. Corti, V. Van den Eyden, L. Bishop (Eds.), *Managing and sharing research data.* 2nd ed. Los Angeles: SAGE.

ÚOOÚ. (2013). *K plnění informační povinnosti*. *ÚOOÚ* (online, cit. 1. 6. 2021), dostupné na adrese: https://www.uoou.cz/k-plneni-informacni-povinnosti/d-1596/p1=0.

ÚOOÚ. (2017). *Nové přístupy a povinnosti*. *ÚOOÚ* (online, cit. 1. 6. 2021), dostupné na adrese: https://www.uoou.cz/2-nove-pristupy-a-nbsp-povinnosti/d-27268/p1=4744.

Zahumenská, V., & Zahumenský, D. (2013). Zvukové záznamy z veřejných projednání a ochrana osobních údajů. *Časopis pro právní vědu a praxi.* 3, 414–423.