Metodika aplikace GDPR na výzkumná data v prostředí vysokých škol v ČR

Radim Polčák, Leoš Ševčík, Michal Koščík,
Jakub Klodwig, Petr Holub

Masarykova univerzita

2018

Název: Metodika aplikace GDPR na výzkumná data v prostředí vysokých škol v ČR

Autoři:

doc. JUDr. Radim Polčák, Ph.D. Ústav práva a technologií, Právnická fakulta, Masarykova univerzita. ORCID 0000-0002-5295-0855

Mgr. Leoš Ševčík Ústav výpočetní techniky, Masarykova univerzita a International Clinical Research Center (ICRC), Fakultní nemocnice u sv. Anny. ORCID 0000-0002-6726-8656

Mgr. Bc. Michal Koščík, Ph.D. Lékařská fakulta, Masarykova univerzita. ORCID 0000-0002-9243-6391

Jakub Klodwig Ústav výpočetní techniky a Právnická fakulta, Masarykova univerzita. ORCID 0000-0002-9599-2043

doc. RNDr. Petr Holub, Ph.D. Ústav výpočetní techniky, Masarykova univerzita. ORCID 0000-0002-5358-616X

Vedoucí skupiny: doc. RNDr. Petr Holub, Ph.D., doc. JUDr. Radim Polčák, Ph.D.

Vydání: první, opravené

DOI: `10.5281/zenodo.2533865`

Poděkování:

CRP-GDPR 2018

Tato metodika byla vytvořena v rámci projektu Komplexní řešení ochrany osobních údajů v prostředí vysokých škol (ROZV/C11/2018).

Obsah

Úvod

Obecné nařízení o ochraně osobních údajů klade na vysoké školy a veřejné výzkumné instituce značné nároky po materiální i organizační stránce. Publikace je zaměřena na ochranu soukromí a osobních údajů v oblasti výzkumu. Hlavním účelem této publikace je poskytnout metodickou podporu pro výzkumné organizace, etické komise i jednotlivé výzkumníky. Publikace záměrně nepokrývá ochranu osobních údajů v oblastech vysokých škol, jakými jsou kupříkladu studijní či personální agenda, a to z důvodu snahy o co nejpřehledněji zpracovaný, úzce zaměřený text.

Zpracování osobních dat pro vědecké účely je poměrně specifickou problematikou, které se i v rámci GDPR dostává zvláštního zřetele. Publikace identifikuje ustanovení obecného nařízení (GDPR), která jsou relevantní pro oblast výzkumu a podává jejich koncentrovaný výklad ve vztahu k výzkumným činnostem. Díky prvním dvěma kapitolám je publikace přístupná i pro osoby, které doposud nejsou obeznámeny s regulací v oblasti ochrany osobních údajů. Pro čtenáře s pokročilou znalostí je určen zejména výklad následujících kapitol. Snahou autorského je poskytnout metodickou podporu zejména vedoucím výzkumných týmů, při plánování a realizaci výzkumných projektů a navazujících procesech správy výzkumných dat.

Tato příručka vznikla v rámci Centrální rozvojového projektu VŠ zaměřujícího se na podporu konzistentní implementace GDPR v prostředí českých veřejných vysokých škol a klade si za cíl poskytnout vodítka pro korektní implementaci GDPR s maximálním využitím výjimek a možností, které jsou pro vědecké účely a akademický projev k dispozici.

V čem je vědecké zpracování dat „jiné“?

- *Potřeba integrovat datové sady napříč institucemi a zeměmi.* Špičkový vědecký výzkum je dnes již obtížně představitelný a realizovatelný bez mezinárodní spolupráce na různých úrovních. Pro zpracování vědeckých dat to znamená, že k dosažení statistické významnosti bývá potřeba spojovat datové sady pocházející z různých zemí Špičkový vědecký výzkum je dnes již obtížně představitelný a realizovatelný bez mezinárodní spolupráce na různých úrovních. K dosažení statistické významnosti bývá potřeba spojovat datové sady pocházející z různých zemí, kdy nekompatibilita omezení na data kladená bývá často překážkou pro realizaci výzkumu.

- *Potřeba zpracovávat data mezinárodně.* Mezinárodní spolupráce se netýká jen integrace datových sad, ale mezinárodní multicentrický výzkum přirozeně vytváří i další scénáře: *(a)* potřeba přenášet data mezi zeměmi, protože expertíza ve zpracování dat je k dispozici v jiné zemi, než ve které jsou data sbírána; *(b)* deponování dat (včetně dat velmi citlivých, kupříkladu genomických) v mezinárodních depozitářích za účelem ověření reprodukovatelnosti výzkumu a pro jejich opakovanou upotřebitelnost.

- *Potřeba zajistit kompatibilitu rozhodování etických komisí s požadavky na ochranu osobních dat.* Vědecké projekty ve většině oblastí pracujících s osobními daty podléhají přezkoumání etickými komisemi ve snaze zajistit vysokou a nepopiratelnou kvalitu výzkumu. Tyto etické komise se také vyjadřují k různým aspektům ochrany účastníků výzkumu (např. pacientů v případě medicínského výzkumu) a nezřídka mívají ve svých požadavcích velmi striktní interpretaci zákonných požadavků. Různé etické komise se pak také často systematicky liší v benevolenci svého rozhodování, což pro mezinárodní výzkumné prostředí představuje další úroveň komplikací. Problematická bývá také akceptace rozhodnutí jiných etických komisí, kdy řada institucí vyžaduje přezkoumání vlastní etickou komisí, byť by existující etické schválení po-

cházelo ze stejného evropského kontextu. Z těchto důvodů je důležité, aby i u etických komisí docházelo ke konvergenci rozhodovacích procesů v oblasti ochrany osobních dat na národní i mezinárodní úrovni.

- *Potřeba efektivního opětovného upotřebení dat.* Získávání kvalitních a reprodukovatelných vědeckých dat a jejich validace je proces velmi náročný na čas i finanční a lidské zdroje. Z tohoto důvodu vznikají mezinárodní výzkumné infrastruktury, které se o tyto data dlouhodobě starají a poskytují je vědcům. Zvyšování překážek pro opětovné upotřebení dat pak komplikuje přístup vědců k těmto infrastrukturám a efektivně je popouzí „levnému sběru dat nízké kvality". Vědecká data jsou často sbírána na základě úzce specifikovaných informovaných souhlasů a v případě jejich opětovného získávání (re-consenting) dochází ke ztrátě zájmu účastníků v čase, přičemž v některých případě je i samotné opětovné získávání souhlasu eticky problematické (např. zákonný zástupce dětského pacienta si nechce neustále připomínat, že jeho dítě prodělalo rakovinu).

- *Požadavky na publikování otevřených nebo FAIR dat.* Vzhledem k výše uvedeným nákladům na tvorbu kvalitních dat se ve vědecké světě zvyšuje tlak na publikování dat tak, aby byly znovu upotřebitelné – a to nejen přes vědecké infrastruktury, ale až na úroveň jednotlivých vědců a vědeckých týmů. Pokud data byla vytvořena za účasti veřejného financování, jaký je důvod aby data zůstávala v „soukromém vlastnictví" vědce? Navíc i velké farmaceutické firmy pod tlakem rostoucích nákladů uvažují o sdílení dat s konkurenty s vidinou zefektivnění výzkumných procesů.

- *Výzkum ve veřejném zájmu vs. komerční výzkum.* Výzkum je možno dělat jak na akademickém tak na komerčním základě, což může být důležitým kriteriem pro rozhodnutí o dalším postupu z hlediska ochrany osobních dat – např. využití výjimek a pro specifické formy informovaných souhlasů, v nichž si účastník

výzkumu může vybrat, zda jeho data mohou být upotřebena pro komerční výzkum či nikoli. V některých oblastech lze poměrně dobře rozlišit čistě akademický a čistě komerční výzkum, nicméně v některých významných oblastech je toto rozlišení obtížnější: vývoj nových léků a léčebných postupů bývá často jak ve veřejném zájmu, avšak současně se provádí za účelem zisku farmaceutických firem.

- *Rozvoj „citizen science" – aneb do je vlastně vědec?* V poslední dekádě se stále více skloňuje „občanská věda", v níž výzkum není výsadou vědců z institucí k tomu určených, ale v podstatě kterýkoli občan má mít možnost dělat výzkum, má-li k tomu zdroje. Tato demokratizace vědy ale přináší důležité otázky ohledně kontroly kvality i toho, které výjimky pro vědecké účely jsou v takové případě uplatnitelné (kdo kontroluje, zda je výzkum dělán ve veřejném zájmu?, kdo zajišťuje povinnosti k datům v případě úmrtí konkrétního občana–vědce?)

- *Potřeba harmonizace s dalšími regulacemi.* Vědecký výzkum je v některých oblastech upraven dalšími regulacemi: např. v oblasti klinického výzkumu se jedná o zákony o klinickém hodnocení. Pokud tyto regulace nejsou harmonizovány se regulacemi na ochranu osobních dat, mohou vznikat vdaných doménách neřešitelné požadavky nebo konflikty.

Co dál? Z výše uvedených specifik vyplývá jednoznačně *potřeba mezinárodní harmonizace pravidel.* V rámci GDPR v době vytváření této příručky již probíhá tvorba Kodexu chování pro opětovné využití zdravotních dat pro výzkum a Kodex chování pro klinická hodnocení. Díky mnoha vlivům, různorodým zájmům i procesním komplikacím je tato tvorba relativně pomalá a schválení kodexů se neočekává dříve jak ke konci roku 2019 a realisticky spíše až v roce 2020. *Text také odráží právní stav v ČR k 31. 12. 2018*, tedy před schválením a nabytí účinnosti Zákon o zpracování osobních údajů (ZZOÚ, národní implementace GDPR). Po schválení ZZOÚ a případném schválení relevantních kodexů

bude vhodná doba pro aktualizaci předkládané metodiky tak, aby maximálně využívala jak flexibilitu GDPR na národní úrovni tak i možnosti poskytované relevantními kodexy.

Dalším důležitým aspektem, o němž je do budoucna třeba uvažovat, je právní potřeba ošetření zbytkového rizika při výzkumu. Vědecké studie ukazují, že požadavky na vysokou míru ochrany soukromí vedou ke snížení kvality vědeckého výsledku (např. modely dávkování léků vykazují výrazně horšící se kvalitu predikce správného dávkování s rostoucími požadavky na ochranu soukromí[1]). I studie v oblasti jedné z nejnadějnějších metod ochrany soukromí, tzv. diferenčního soukromí,[2] ukazují, že nelze mít současně dokonalou ochranu osobních údajů a dokonale užitečná a spolehlivá data. Tento konflikt se zdá že nebude vyřešen na úrovni technických prostředků a s rostoucím rozsahem strojového zpracování dat pro výzkumné účely bude důležité zvažovat dodatečnou i právní ochranu účastníků výzkumu, jejichž soukromí bude ohroženo v důsledku nahodilé příp. zlovolné publikace dat.

Struktura příručky Příručka je strukturována následujícím způsobem:

- úvod vysvětlující *logiku regulatorní metody GDPR* (principy performativních regulací) a *prameny práva*, umožňujícím vhled do problematiky pro nezasvěcené čtenáře z řad vědců (kapitoly 1–2);
- doporučení ohledně využívání *právních titulů*, pro specifikaci *účelu* zpracování a sdílení dat (kapitola 3);
- vysvětlení *výjimek pro vědecké užití dat* při uplatňování hmotných práv subjektů (kapitoly 4–7);
- vysvětlení *role pověřence* vzhledem k vědeckým datům (kapitola 8);

[1] Matthew Fredrikson et al. „Privacy in Pharmacogenetics: An End-to-End Case Study of Personalized Warfarin Dosing." In: *USENIX Security Symposium*. 2014, s. 17–32.

[2] Cynthia Dwork a Aaron Roth. „The algorithmic foundations of differential privacy". In: *Theoretical Computer Science* 9.3-4 (2013), s. 211–407.

- *procesní diagramy* (česky i anglicky), vysvětlující vhodné uchopení procesů týkajících se vědeckých dat (kapitola 9):
  - příprava projektu zahrnujícího zpracování osobních dat,
  - správa dat v průběhu realizace a po skončení projektu (vč. opětovné upotřebitelnosti dat),
  - reakce na události;
- doporučená *struktura dokumentace* zpracování osobních dat pro vědecké účely (kapitola 10);
- *vzor DPIA* (česky i anglicky) a příklad jejího vyplnění (kapitola 11 a příloha B).

Slovník

DPO Data Protection Officer (Pověřenec pro ochranu osobních údajů). 4, 50, 82, 89

FAIR Findable, Accessible, Interoperable, Reusable – paradigma publikování vědeckých dat. 9

GDPR General Data Protection Regulation (Obecné nařízení o ochraně osobních údajů). 3, 4, 7, 10, 11, 13, 15–24, 29, 30, 35, 36, 38, 46, 49, 52, 53, 56–61, 63–68, 70, 71, 73–77, 79, 81–84, 86, 89, 92, 96

NIS Směrnice o síťové bezpečnosti – Network Information Security. 17

ObčZ Občanský zákoník. 23, 33
OSŘ Občanský soudní řád. 81, 85

SFEU Smlouvy o fungování Evropské unie. 85
SŘ Správní řád. 83
SŘS Soudní řád správní. 84, 85

ZOOÚ Zákon č. 101/2000 Sb. o ochraně osobních údajů. 33, 56
ZZOÚ Zákon o zpracování osobních údajů – nadcházející národní implementace GDPR (v době publikace příručky ještě nenabyla platnosti). 10, 49, 53, 56–60, 70, 71, 73, 75–77, 84, 85, 87

ÚOOÚ Úřad na ochranu osobních údajů. 21–24, 55, 60, 84, 90

1. Logika a regulatorní metoda GDPR

1.1. GDPR a nižší standard ochrany osobních údajů

Zpracování dat ve vědě a výzkumu představuje jedno z nejobtížnějších zadání z agendy ochrany osobních údajů. Pro účely výzkumu a vývoje se totiž zpracovává bezprecedentně široké spektrum různých typů osobních dat, která často mají vysokou individuální nebo společenskou citlivost. Typicky sbíraná data, například o zdravotním stavu, genetickém profilu, osobní historii nebo politických názorech či náboženském přesvědčení mají vzhledem k životu konkrétního člověka vysokou vypovídací hodnotu. Z toho pak plyne i zvýšená poptávka po jejich právní ochraně.

Oproti všeobecnému společenskému přesvědčení lze konstatovat, že z normativního hlediska nepřináší GDPR v porovnání s dříve účinnou úpravou evropských směrnic a českého zákona o ochraně osobních údajů vyšší standard ochrany osobních údajů. Právě naopak je v GDPR v porovnání s dřívější úpravou zmírněna řada omezení. S osobnímu údaji je tím pádem možno právně konformním způsobem provádět i operace, které byly dříve zákonem zapovězeny.

Jedním z institutů ilustrujících shora uvedené tvrzení a nově vyjímajícím zpracování osobních dat z jinak rigorózního ochranného režimu je institut zpracování osobních dat pro vědecké účely doplněný institutem zpracování osobních dat pro účely akademického projevu. Obě generální

výjimky mají nově v právu ochrany osobních údajů takový význam, že na základě konkrétních společensko-politických podmínek (k tomu dále) umožňují vědeckým, resp. akademickým, institucím zpracovávat pro vědecké účely osobní údaje v takovém rozsahu, který byl doposud de iure nemyslitelný.

Zatímco je *de iure* ochrana osobních údajů dle GDPR mírnější než v dosavadní právní úpravě, objevuje se v GDPR řada nových institutů, které mají v porovnání se současnou situací zajistit vyšší míru ochrany osobních údajů *de facto*. Problémem dosavadního ochranného režimu totiž bylo jeho rozdílné uplatňování v různých členských státech a dále pak skutečnost, že jeho reálná vynutitelnost byla v řadě zemí často spíše teoretická. Rozdílné uplatňování ochrany osobních údajů pak přinášelo problémy v řadě vědeckých oblastí, kde integrace dat z více zemí představuje nedílnou součást výzkumného procesu (např. personalizovaná medicína a problematika vzácných nemocí).

Lze říct, že v České republice nikoho doposud ochrana osobních údajů příliš nezajímala. Na rozdíl od jiných podobně velkých členských států u nás prakticky neexistovala judikatura vyšších soudů ve věcech ochrany osobních údajů a tato problematika obvykle nebývala ani předmětem vnitro-organizačních compliance procesů. Případů, v nichž správcům nebo zpracovatelům stálo za to žalovat postup nebo rozhodovací praxi úřadu, bylo totiž jen absolutní minimum a případy, kdy by se proti liknavému postupu úřadu bránily subjekty údajů, u nás prakticky neexistovaly.

Problém faktické impotence úřadu u nás měl daleko závažnější důsledky, než se může na první pohled jevit. Kvůli absenci poptávky se totiž u nás nemohla v oboru ochrany osobních údajů vytvořit profesionální právní praxe, tj. specializovaní podnikoví právníci nebo advokáti. Ani na soudech nebylo možno nalézt soudce, kteří by se problematice ochrany osobních údajů odborně věnovali, neboť by jim taková profesní specializace nebyla k ničemu dobrá.

1.2. Performativní a chytrá pravidla

Hloubka shora naznačeného problému se projevila u nás s příchodem GDPR. Nové nařízení totiž kromě přímé působnosti přináší řadu institutů, které mají pragmaticky (prakticky) přinést vyšší míru skutečné ochrany osobních údajů, tj. vyšší míru přiblížení reálné situace zákonnému ideálu. Tyto nové instituty tedy mají přiblížit *"law in action"* ideálu *"law in books"* a zajistit vyšší míru skutečné ochrany osobních údajů, dokonce přesto, že normativní úroveň ochrany se v porovnání s minulým stavem platného práva relativně snížila. Konkrétně se jedná o následující nové nástroje (tj. nástroje, které předchozí úprava neobsahovala):

- Regulace prostřednictvím performativních pravidel
- Nástroje chytré (informované) regulace
- Přímé nároky subjektů údajů

Performativní pravidla (angl. *performance-based regulation*) se neobjevují v evropské právní úpravě poprvé a lze očekávat, že tato regulatorní metoda zdomácní i v jiných agendách. Prvním případem plošného uplatnění metody performativních pravidel byla tzv. směrnice o síťové bezpečnosti (označovaná zkratkou jako směrnice NIS). V české republice se ještě před harmonizací směrnice NIS jednalo o zákon o kybernetické bezpečnosti. Performativních pravidel bylo u kybernetické bezpečnosti i ochrany osobních údajů užito z toho důvodu, že obě regulatorní agendy vykazují následující společné rysy:

- Zájem právotvůrce je v základních rysech synergický se zájmem regulovaného subjektu (stát má zájem na tom, aby byla osobní data bezpečně zpracovávána a správce či zpracovatel mají zájem na tomtéž). Lze tedy předpokládat, že regulovaný subjekt nebude mít a priorit zájem na absolutním sabotování příslušného regulatorního účelu.
- Konkrétní podoba regulovaných systémů je extrémně různorodá (osobní data se zpracovávají v ohromném spektru různých apli-

kací, za užití široké palety různých technologií a k nepřebernému množství účelů). Z toho důvodu nelze z pohledu právotvůrce určit typický use-case a na něj mapovat konkrétní povinnosti. Žádný typický use-case totiž neexistuje.

- Regulovaný subjekt nejlépe ví, co je konkrétně třeba dělat k tomu, aby bylo v jeho případě účelu regulace dosaženo nejefektivnějším způsobem (na rozdíl třeba od medicíny je tedy v tomto případě pacient tím, kdo je nejlépe schopen určit vlastní diagnózu a nejefektivnější indikaci).

Podstata performativních pravidel spočívá v tom, že právotvůrce metaforickým způsobem stanoví pouze základní účelové kategorie a *přikáže regulovanému subjektu, aby si sám určil konkrétní pravidla, podle nichž bude k dosažení příslušného účelu postupovat.* Vztah mezi zákonem a regulovaným subjektem je v tomto případě obdobný, jako je vztah mezi zákonem a orgánem veřejné moci, kterému je svěřeno provádět zákon formou podzákonného předpisu. Zákonodárce tedy nemá v tomto případě konkrétní představu ohledně toho, co přesně znamenají obecné zákonné kategorie, ale nechává na regulovaném subjektu jejich autoritativní interpretaci pro určitou konkrétní situaci.

Rozdíl mezi tímto způsobem performativní regulace a standardní právní regulací konkrétními pravidly lze demonstrovat na příkladu rychlostních omezeních na dálnicích. V České republice je rychlost omezena právním předpisem na 130 km/h. V Německu je rychlost na dálnici omezena performativním pravidlem – není přitom pravdou, že by v Německu rychlost nebyla omezena vůbec, ale omezení je provedeno v tom směru, že každý může jet tak rychle, jak je to za daných okolností (typ vozu, jeho technický stav, schopnosti řidiče, hustota provozu, stav vozovky a počasí apod.) bezpečné. Každý řidič tedy musí zhodnotit svoji vlastní situaci a stanovit si dle ní rychlostní limit sám pro sebe.

Pokud jde **o metodu chytré regulace**, nelze již z pochopitelných důvodů shora uvedenou analogii s rychlostním limitem použít. Je totiž založena na maximální informovanosti veřejné moci ohledně stavu

regulovaného substrátu. V případě spojení s metodou performativních pravidel to navíc předpokládá explicitní informovanost regulovaného subjektu ohledně jeho vlastní situace. Shora uvedenou analogií by tedy chytrá regulace na německé dálnici nutila řidiče, aby sami pro sebe popsali stav svého vozidla, svých řidičských schopností, vozovky, počasí apod. a aby zároveň explicitně zdokumentovali, jakou nejvyšší povolenou rychlost si pro sebe stanovili.

V případě ochrany osobních údajů se chytrá regulace projevuje následujícími povinnostmi:

- Správce je povinen vědět (a zdokumentovat), jaké osobní údaje, proč a jak zpracovává
- Správce je povinen zdokumentovat bezpečnostní rizika a stanovit si vlastní povinnosti k ochraně osobních údajů
- Správce je povinen hlásit případy porušení ochrany osobních údajů vrchnosti a subjektům údajů
- Správce je povinen spolupracovat s vrchností při kontrole souladu vlastní dokumentace a bezpečnostních opatření s obecným zákonným standardem (za tímto účelem byl zaveden jinde v Evropě již úspěšně využívaný institut pověřence).

1.3. Autonomní regulace a důležitost experta

Z právě uvedeného nepřímo plyne též největší problém přechodu z předchozího právního režimu do režimu GDPR v České republice. V současné době je každý druhý český advokát expertem na ochranu osobních údajů, a to přesto, že ještě před dvěma lety o této problematice téměř žádný člen advokátní komory nevěděl zhola nic. Stejně tak se experti na ochranu osobních údajů rekrutují prakticky ze všech možných více či méně obskurních profesí, přičemž kvalifikaci pro tento druh specializace jim obvykle zajišťuje přečtení textu GDPR a

doposud vydaných doporučení WP29. Jsou to však právě tito ‚experti', kdo de facto určuje konkrétní podobu pravidel, jimiž se regulované subjekty (správci a zpracovatelé) budou při zpracování osobních údajů řídit.

Když správce potřebuje splnit nové typy povinností, potřebuje experta především k tomu, aby zhodnotil ad hoc technickou a právní situaci správce a na míru mu stanovil takové konkrétní povinnosti, které zajistí naplnění zákonných maxim, a přitom budou pro fungování správce co nejefektivnější. Analogicky se shora uvedeným příkladem tedy správce potřebuje, aby expert zhodnotil jeho řidičské schopnosti, typ a stav jeho vozu, stav vozovky a všech ostatních okolností a pak mu předepsal, jakou rychlostí může na dálnici cestovat.

Tam, kde expert nemá dostatek odborných znalostí, praktických zkušeností i mezinárodního přehledu o problematice (což je v ČR na rozdíl od jiných členských států bez nadsázky standardní situace), může být výsledkem nesoulad se zákonem nebo častěji zásadní neefektivita příslušného řešení. Český expert shora zmíněného střihu tedy při užití dálniční analogie nejprve prohlédne velký technický průkaz supersportovního vozu schopného zastavit z třísetkilometrové rychlosti na pětníku a zdravotní dokumentaci zcela zdravého řidiče v nejlepších letech, opíše příslušná data do složitě vypadající tabulky (za kterýžto úkon si naúčtuje zpravidla šestimístnou sumu) a následně konstatuje, že dle GDPR je příslušný řidič s příslušným autem povinen jezdit po dálnici rychlostí maximálně 55 km/h (následuje pak obvykle svorné nadávání experta a správce na to, jak je Evropská unie povýšená a hloupá, že stanoví lidem takto hloupé povinnosti).

S vyšším zájmem veřejnosti a podniků o otázky ochrany osobních údajů se objevilo větší množství kurzů nabízejících „certifikované" vzděláváni pro pověřence osobních údajů, případně další zaměstnance pracující s osobními údaji. Byť je jakékoliv zvyšování kvalifikace bohulibou aktivitou, je nutno poznamenat, že předpisy EU ani vnitrostátní předpisy žádnou konkrétní certifikaci nevyžadují.

1.4. Sankční režim

Hodnocení relevantních faktorů a výběr konkrétních pravidel k maximálně efektivnímu řešení ochrany osobních údajů je v jednotlivých případech samozřejmě možno provést i typově pro určitý use-case (např. pro řemeslníka-živnostníka zpracovávajícího data svých klientů) a správce se tím pádem může spolehnout i na nějaké standardizované řešení dokumentace či bezpečnostních opatření (k tomu viz např. výklad ke kodexům v části 2). U zpracování výzkumných dat je ale situace poněkud složitější, neboť typické use-cases nejsou v pravém smyslu slova typické (vyskytují se v řádově menších frekvencích) a parametry, které je nutno vzít v potaz, jsou nesrovnatelně složitější. Z toho plyne, že při dokumentaci a definici bezpečnostních opatření pro zpracování osobních údajů pro vědecké účely existuje i větší riziko autonomní nezákonnosti na jedné straně a současně i riziko fatální neefektivity na straně druhé.

Problém potenciální nezákonnosti autonomního řešení ochrany osobních údajů je samozřejmě z pohledu regulovaného subjektu (v tomto případě výzkumné instituce) z více důvodů nepříjemný. Problematická je pro regulovaný subjekt, nota bene financovaný z veřejných zdrojů, už i sama kontrolní činnost vrchnosti – u nás Úřad na ochranu osobních údajů (ÚOOÚ) – a nezanedbatelné jsou i teoretické možnosti postihu formou pokut nebo opatření k nápravě.

Je však zásadní chybnou vnímat sankční režim GDPR analogicky se sankčním režimem regulatorních nástrojů postavených na standardním modelu konkrétních behaviorálních (nikoli performativních) pravidel. Národní úřady pro ochranu osobních údajů totiž v tomto případě nemají postavení regulátora a nejsou tedy vybaveny oprávněním konkretizovat obecná ustanovení zákonného práva. Národní úřady pro ochranu osobních údajů tedy nejsou v obdobné pozici, jako například úřady na úseku elektronických komunikací nebo elektroenergetiky, které formou prováděcích předpisů konkretizují v mezinárodním právu členského státu obsah zákonných metafor. ÚOOÚ tudíž nemá právo formou prováděcího

cího předpisu vymyslet nějakou svoji ideální interpretaci zákonné metafory a tu pak vymáhat, ale je oprávněn uplatnit sankci pouze tam, kde bude možno prokázat, že zákonná metafora absolutně nebyla naplněna (tj. dojde k prokázání logického opaku dispozice příslušné právní normy).

Typicky tedy např. u informačních povinností stanoví GDPR požadavek na srozumitelnost příslušného sdělovacího prostředku. Tato velmi obecně stanovená povinnost může být sankcionována pouze za předpokladu, že správce prokazatelně informoval povinný subjekt nesrozumitelně (nikoli tehdy, pokud bude pouze mezi správcem a ÚOOÚ spor o to, zda mohla být informace o zpracování osobních údajů podána povinnému subjektu nějak jinak či lépe). *Nemůže být tedy předmětem sankce postup správce, který je pouze diskutabilní nebo u kterého lze najít nějakou lepší alternativu – sankci bude podléhat pouze takové jednání, které bude prokazatelně v rozporu se zákonnou povinností.* Určitou formou konkretizace metaforických zákonných povinností budou kodexy chování dle čl. 40 GDPR,(srov. výklad níže). Ani v tomto případě ale nepůjde o produkty regulátora, ale pouze o dobrovolné opční nástroje, kdy si profesní, zájmová nebo jinak zastřešující organizace schválí doporučená pravidla pro zpracování v jednotlivých případech, aby fakticky vykompenzovala chybějící podzákonnou legislativu. Takovýto kodex pak následně může být posvěcen úřadem a přinese členům právní jistotu v tom smyslu, že nebudou sankcionováni, pokud se doporučených postupů přidrží.

2. Prameny práva ochrany osobních údajů

2.1. Mnohost a hierarchie pramenů ochrany osobních údajů

Všeobecné nařízení je důležitým pramenem práva ochrany osobních údajů. Zdaleka však není pramenem jediným, a dokonce nemusí být z praktického hlediska ani pramenem nejdůležitějším. Pro správce, zpracovatele i subjekty údajů totiž všeobecné nařízení často představuje pouze nástroj k základní orientaci nebo dokonce jen zdroj obecných informací k prvotnímu přiblížení se k příslušné regulatorní materii.

Chápání GDPR jako kuchařky či návodu k tomu, jak chránit osobní údaje, je z mnoha důvodů vadné. Předně je totiž třeba GDPR chápat jako součást systému národního zákonného práva, jehož realizace probíhá zcela v mezích ústavní proporcionality. Příkladně se tedy na potenciální škodu z porušení povinností založených na základě GDPR může vztahovat prevenční povinnost dle Občanský zákoník (ObčZ), nebo může být kontrolní a sankční činnost ÚOOÚ uplatňována pouze v mezích ohraničených principy dobré správy, principem rovnosti nebo principem právní jistoty. Z toho plyne, že skutečný rozsah (často silně metaforicky formulovaných) povinností založených GDPR je v obecné rovině možno určit až systematickou interpretací za užití všech možných souvisejících pramenů zákonného práva. Přitom je třeba vyloučit takové interpretační závěry, které by ve smyslu stávající judikatury Ústavního soudu vybočovaly z mezí aktuální doktríny ústavní proporcionality.

Druhým důvodem, proč nelze příslušná práva a povinnosti k ochraně osobních údajů bez dalšího dovozovat z GDPR, je skutečnost, že nařízení až na výjimky neobsahuje konkrétní pravidla chování. Namísto toho je struktura nařízení tvořena soustavou performativních pravidel regulujících autonomní normotvorbu na úrovni regulovaných subjektů (zpracovatelů a správců). Konkrétní pravidla chování k ochraně osobních údajů tedy mají buďto charakter individuálních autonomně vytvořených norem nebo autonomních norem svépomocně vytvořených třídou regulovaných subjektů pro typické situace.

Z pohledu správce nebo zpracovatele se může shora naznačená struktura pramenů práva zdát složitou a těžko přístupnou. Při hodnocení srozumitelnosti právní úpravy však je třeba vzít v potaz, že už její samotná teleologie není triviální a že rozsah situací, na které má dopadat, je extrémně široký. Přestože tedy právo obecně nemá být psáno pro právníky, počítá všeobecné nařízení s tím, že bude přímo aplikováno především profesionály (což, jak uvedeno výše, zdaleka neznamená člověka, který si nařízení přečte a pak si nechává platit za to, že jej předčítá ostatním). Povinným subjektům jsou tak přímo určena až konkrétní autonomní pravidla tvořená na míru (resp. typově) dle jejich situace. Subjektům údajů pak slouží k orientaci v jejich právech především další autonomně tvořené nástroje, typicky informace mandatorně poskytované povinnými subjekty. V obou případech (tj. u autonomních pravidel povinných subjektů i návodů pro subjekty údajů) přitom platí, že neexistuje ideální nebo jediné správné konkrétní řešení – prameny, o kterých je dále stručně pojednáno, tedy povinné subjekty využívat mohou, avšak nemusí.

2.2. Osvědčené postupy a kodexy

Z typových fakultativních pramenů práva ochrany osobních údajů si zaslouží zvláštní pozornost různá výkladová stanoviska WP29, Evropského sboru pro ochranu osobních údajů (dále jen Sbor) nebo ÚOOÚ. Ve vztahu k nim je třeba předně upozornit na to, že Sbor ani národní úřady

pro ochranu osobních údajů nejsou regulátory, tj. nemají regulační pravomoci. Úlohou národních úřadů je pouze podporovat autonomní normotvorbu a dohlížet na dodržování zákonných pravidel. Podobně pak je úkolem Sboru především koordinace aktivit národních úřadů a sjednocování praxe při správní interpretaci obecného nařízení. Sbor ani národní úřady tedy nedisponují legislativní kompetencí k pravé delegované právotvorbě.

Obecné nařízení užívá pro to, co bylo u nás běžně označováno jako výkladové stanovisko, pojmu „pokyn", „doporučení" nebo „osvědčený postup" (pojem „stanovisko" je obecným nařízením používán především pro formu autoritativního přezkumu autonomního pravidla, tj. např. kodexu – viz dále). *Přestože byla u nás dosavadním doporučením WP29 připisována velká důležitost, je jejich skutečný význam relativně malý.* Nejde ani tak o to, že tyto neautoritativní formy de iure nezavazují téměř nikoho (de facto zavazují prostřednictvím principu právní jistoty pouze Sbor a národní úřady pro ochranu osobních údajů), ale o praktickou použitelnost jejich obsahu. Doporučení či pokyny totiž obvykle vycházejí z velmi obecně formulovaných performativních pravidel obecného nařízení a nezaměřují se zpravidla na konkrétní oblast zpracování osobních údajů. Prakticky nejcennější částí doporučení a pokynů jsou tedy poněkud paradoxně pasáže, kde jsou uvedeny hypotetické příklady správně nebo vadné praxe.

Z právě uvedeného důvodu je za pragmaticky (prakticky) daleko významnější prameny poznání právní úpravy ochrany osobních údajů nutno považovat osvědčené postupy, a především pak kodexy. V obou případech se totiž jedná o vysoce konkrétní pravidla ochrany osobních údajů vytvořená pro určité typy praktických aplikací (např. pro určitý obor). Nejde o pravidla performativní, ale o konkrétní (standardní) pravidla chování, která mohou bezprostředně aplikovat příslušné povinné subjekty a jejichž dodržení nebo naopak porušení lze relativně snadno identifikovat.

V případě *osvědčených postupů* jde o konkrétní funkční řešení ochrany osobních údajů, jejichž kvalita založí v očích Sboru dobrou praxi. Po-

vinné subjekty mohou z osvědčených postupů získat vysoce konkrétní informaci ohledně praxe, kterou Sbor považuje vzhledem k obecnému nařízení za správnou, a upravit podle toho vlastní postupy a ochranné nástroje. Nemusí přitom jít na straně povinných subjektů o přímou implementaci osvědčeného postupu, ale osvědčené postupy lze využít také k pouhé inspiraci. Jde tedy vlastně o obdobu shora zmíněných pokynů a doporučení tam, kde tyto materiály obsahují praktické příklady.

Právní důsledky adaptace osvědčených postupů jsou každopádně pouze zprostředkované. Inspiruje-li se povinný subjekt osvědčeným postupem, zakládá tím pouze důvod k obdobnému posouzení souladnosti příslušného řešení s platným právem v míře odpovídající ad hoc analogii se situací u osvědčeného postupu. Národní úřad na ochranu osobních údajů ale každopádně bude při kontrole i v případě aplikace osvědčeného postupu pozitivně hodnotit praxi příslušného povinného subjektu a konfrontovat ji s požadavky zákonné úpravy.

Formální struktura i proces vzniku *kodexu* jsou v porovnání s osvědčeným postupem složitější a jeho výsledný právní efekt je též mnohem závažnější. Předmětem autoritativní aprobace kodexu je totiž komplexní struktura povinností týkajících se ochrany osobních údajů v definovaném procesu zpracování. Kodex tedy v porovnání s osvědčeným postupem obsahuje jednak precizní vymezení procesu zpracování osobních údajů, a kromě toho i systematický, komplexní a vyčerpávající popis souvisejících povinností.

Aprobace kodexu generuje na straně úřadů pro ochranu osobních údajů presumpci compliance (jednání v souladu s právem). Znamená to, že *povinný subjekt, který implementuje kodex, nemusí prokazovat soulad vlastní praxe s nařízením, ale prokazuje pouze soulad vlastní praxe s kodexem* (to je samozřejmě vzhledem ke konkrétní povaze kodexu mnohem jednodušší). Kontrola tedy není v takovém případě orientována na pozitivní ověření teze ohledně souladnosti příslušné praxe s nařízením, ale úřad se může pouze negativně zaměřit na to, co schválenému kodexu případně neodpovídá. Kodex se přitom může týkat

i tak zásadních otázek, jako je předávání dat ke zpracování mimo území EU.

Z výše uvedeného plyne, že pro praxi zpracování osobních údajů ve vědě a výzkumu budou mít ve střednědobé perspektivě největší praktický význam právě kodexy. Nelze totiž očekávat, že by se vysoce komplexní a procedurálně i subjektivně složité typické formy zpracování dat pro vědecké účely dočkaly obecných interpretací ve formě doporučení nebo pokynů. Ze zkušenosti nelze zřejmě čekat ani to, že se zpracování dat pro vědecké účely stane záhy předmětem rozhodovací praxe národních úřadů na ochranu osobních údajů, národních soudů a Soudního dvora. Čekání na judikaturu se tedy v tomto směru rovněž nejeví jako příliš účelné. Velké naděje konečně nelze vkládat ani do osvědčených postupů. Pokud už dojde k jejichž masivnějšímu vydávání, není příliš pravděpodobné, že budou bez dalšího použitelné na často velmi specifické situace výzkumných organizací. Krom toho jejich partikulární charakter a právní efekt neposkytují ve složitých případech vysoce riziky exponovaného zpracování osobních údajů (které jsou především v biomedicínském výzkumu či společenských vědách běžné) kýženou právní jistotu.

3. Právní titul, účel zpracování a sdílení dat

3.1. Právní titul a účel zpracování

Logika ochrany osobních údajů stojí na předpokladu, že zpracování osobních údajů je obecně zakázáno. Zákon, resp. nařízení, pak z tohoto zákazu stanoví řadu různých výjimek. Obecně se tyto výjimky zakládající možnost zpracovávat osobní údaje označují jako právní důvody zpracování (užívá se též pojmu právní titul zpracování). Správce musí být vždy schopen prokázat, že příslušný proces zpracování spadá pod některý z těchto právních důvodů (titulů).

Výčet titulů je proveden v čl. 6 GDPR následovně:

a) souhlas,
b) plnění smlouvy,
c) plnění právní povinnosti,
d) životně důležitý zájem,
e) plnění úkolu ve veřejném zájmu,
f) oprávněný zájem.

Tituly představují obecné zákonné důvody ke zpracování osobních údajů. Od titulu je třeba odlišit účel zpracování, který má konkrétní charakter a vztahuje se vždycky k určitému procesu zpracování osobních údajů u příslušného správce. Platí přitom, že konkrétní účel zpracování tak, jak jej vymezí správce, musí spadat pod rozsah některého ze zákonných titulů. Ověřením konkrétního účelu zpracování tedy můžeme učinit

závěr ohledně toho, zda je zpracování osobních údajů v příslušném případě z hlediska zákona důvodné.

Titulem ke zpracování osobních údajů bude u výzkumné organizace zpravidla plnění úkolu ve veřejném zájmu, plnění právní povinnosti nebo oprávněný zájem výzkumné organizace. V případě zpracování výzkumných dat např. v komerčním projektu může být titulem ke zpracování též plnění smlouvy.

Ve vědě a výzkumu je běžným a y pohledu práva nijak závadným jevem, když jeden konkrétní účel zpracování naplňuje skutkovou podstatu více než jednoho titulu. Příkladem může být situace, kdy univerzita získá projekt z veřejného financování ke zmapování účinnosti určitého léčebného postupu. V takovém případě je účelem zpracování příslušné projektové zadání tj. výzkum účinnosti konkrétního léčebného postupu. Titulem ke zpracování je současně plnění úkolu ve veřejném zájmu, plnění smlouvy (tj. smlouvy o dotaci) i oprávněný zájem univerzity.

GDPR obsahuje v čl. 9 zvláštní úpravu týkající se údajů dříve označovaných za citlivé (nyní jsou to zvláštní kategorie osobních údajů). Jde o údaje, „které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby." GDPR obecně zakazuje tyto údaje zpracovávat a v čl. 9(2) taxativně vypočítává případy, kdy tento zákaz neplatí. Jedná se tedy vlastně o specifický zákaz v rámci obecného zákazu – nařízení totiž obecně zakazuje zpracování osobních údajů vyjma případů krytých tituly dle čl. 6. I tam, kde by zpracování osobních údajů odpovídalo některému z obecných titulů dle čl. 6, platí pro zvláštní kategorie osobních údajů specifický zákaz zpracování stanovený čl. 9(1).

Pokud tedy má správce zájem zpracovávat některou ze zvláštních kategorií osobních údajů, musí být jednak naplněn některý ze zákonných titulů dle čl. 6 a k tomu musí přistoupit některá z následujících výjimek uvedených v čl. 9(2):

a) subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že zákaz uvedený v odstavci 1 nemůže být subjektem údajů zrušen;
b) zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu nebo kolektivní dohodou podle práva členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů;
c) zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;
d) zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt;
e) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;
f) zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí;
g) zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů;
h) zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na zá-

kladě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem a při splnění podmínek a záruk uvedených v odstavci 4 článku 9 GDPR [1];

i) zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství;

j) *zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely v souladu s čl. 89 odst. 1 na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.*

Stejně jako v případě titulů mají i výjimky dle čl. 9(2) obecný charakter a jejich skutková podstata musí být naplněna konkrétním účelem zpracování. Ve shora zmíněném příkladu výzkumného projektu univerzity týkajícího se veřejného zdraví a financovaného ministerstvem bude účel projektu současně naplňovat skutkovou podstatu výjimky ze zákazu ve smyslu písm. i) a písm. j). Univerzita tedy v tomto případě stanoví konkrétní účel zpracování odpovídající projektovému zadání a z něj pak vyplyne jednak zákonná důvodnost zpracování osobních údajů jako takových ve smyslu čl. 6 a jednak neaplikovatelnost zákazu zpracovávat zvláštní kategorie osobních údajů ve smyslu čl. 9.

K výše uvedenému je třeba doplnit poznámku týkající se souhlasu se zpracováním osobních údajů. Ten je v obecné formě (včetně nevýslovného, tj. konkludentního souhlasu) jedním ze zákonných důvodů zpracování osobních údajů dle čl. 6(1)(a) a je též v explicitní (výslovné) formě

[1] GDPR požaduje, aby národní právní úprava respektovala záruky před zneužitím genetických a biometrických údajů

výjimkou ze zákazu zpracovávat zvláštní kategorie osobních údajů dle čl. 9(2)(a).

3.1.1. Informovaný souhlas jako právní základ

V praxi je sice souhlasu subjektu údajů přikládán velký význam, avšak z právního hlediska bývá souhlas při zpracování dat pro vědecké účely důvodem zpracování osobních údajů nezbytný jen výjimečně. Před účinností GDPR nebyl vědecký výzkum sám o sobě dle Zákon o ochraně osobních údajů (ZOOÚ) zákonným důvodem pro zpracování osobních údajů, což přispělo k zakořenění představy, že souhlas subjektu údajů je jediným možným způsobem jak zákonně zpracovávat neanonymizovaná výzkumná data. Správci, kteří neuvažují o jiných právních důvodech zpracování osobních údajů, tak v důsledku nepochopení rozsahu jiných titulů dle čl. 6(1) a výjimek dle čl. 9(2) GDPR často žádají o souhlas zbytečně a zatěžují tak subjekt údajů i sebe sama zbytečnou administrativou. Pokud navíc považuje správce údajů souhlas za jediný titul ke zpracování osobních údajů, znamená to, že při odvolání souhlasu se zpracováním (na které má subjekt údajů zákonné právo) má správce povinnost údaje dále nezpracovávat.

Navzdory výše uvedenému, je souhlas legitimním právním důvodem zpracování a daná instituce může dojít k legitimnímu závěru, že bude v rámci některých projektů zpracovávat pouze ta data, k nimž má výslovný souhlas. Souhlas je z pohledu tuzemského práva právním jednáním a váže se na něj obecný požadavek na jeho vážnost, určitost a srozumitelnost,[2] přičemž kritéria uložená ZOOÚ[3] a GDPR jsou vůči ObčZ zvláštní úpravou. Právě otázka určitosti bývá v oblasti výzkumu často zdrojem právní nejistoty. Pokud subjekt údajů dává souhlas se zpracováním svých osobních údajů pro účely jednoho konkrétního projektu,

[2] Srov. §551–553 ObčZ.

[3] Například požadavek výslovnosti souhlasu se zpracováním citlivých osobních údajů dle §9 ZOOÚ.

který je vymezen svými cíli i časem, problém s určitostí souhlasu nevzniká. Mnohem složitější je však formulovat dostatečně určitý a srozumitelný souhlas k sekundárnímu užití dat pro budoucí výzkumné projekty, včetně těch, které ještě nejsou ani naplánované, nebo souhlas k budoucímu sdílení výzkumných dat s dalšími výzkumnými institucemi. Problém spočívající v neznámých budoucích možnostech zpracování osobních údajů se výzkumné instituce často snaží pokrývat tzv. **otevřenými souhlasy**, které se snaží účel specifikovat právě tím, že stanoví souhlas se zpracováním za jakýmkoli účelem, tím, že jako účel stanovuje vědecký výzkum obecně.[4] Použití otevřeného souhlasu je pro instituci zdánlivě pohodlným řešením, jež umožní sesbírané osobní údaje maximálně vytěžit, sdílet a nijak zásadně se neomezovat. Tato praxe je ale problematická z důvodu nedostatečné specifičnosti souhlasu, ale také i z hlediska nedostatečně určitě vymezenému účelu zpracování. Pracovní skupina evropské komise WP29 ve svém stanovisku č. 03/2013 výslovně uvádí, že používání slovního spojení „budoucí výzkum" (angl. "future research") je typickým příkladem nedostatečně určitého vymezení účelu[5],[6] a lze se tedy domnívat, že bude takové vymezení v mnoha případech důvodem i pro konstatování nedostatečně určitého souhlasu se zpracováním.

[4] Dara Hallinan a Michael Friedewald. „Open consent, biobanking and data protection law: can open consent be 'informed' under the forthcoming data protection regulation?" In: *Life sciences, society and policy* 11.1 (2015), s. 1, analyzují problematiku otevřeného souhlasu se zaměřením na nové nařízení, ale v některých částech i jako retrospektivní ohlédnutí za směrnicí 95/46.

[5] Article 29 Data Protection Working Party. *Opinion 03/2013 on purpose limitation*. The European Commission, 2013. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, s. 16, dále také s. 52.

[6] Olof Nyrén, Magnus Stenbeck a Henrik Grönberg. „The European Parliament proposal for the new EU General Data Protection Regulation may severely restrict European epidemiological research". In: *European journal of epidemiology* 29.4 (2014), s. 227–230; Mette Rye Andersen, Hans H Storm et al. „Cancer registration, public health and the reform of the European data protection framework: abandoning or improving European public health research?" In: *European Journal of Cancer* 51.9 (2015), s. 1028–1038.

Na druhé straně pak stojí reálná společenská potřeba zachovat a dále sdílet data získaná během konkrétního výzkumného projektu. Výzkum totiž zpravidla pokračuje i po splnění konkrétního účelu a ne všechna data lze anonymizovat, aniž by ztratila podstatnou část své hodnoty. Zároveň není možné předvídat veškeré směry budoucího výzkumu nebo identifikovat všechny budoucí partnery. Uspokojení vyřešení otázky, jak poskytnout dostatečně určitý otevřený souhlas má extrémní význam zejména v oblasti medicínského výzkumu, farmaceutického výzkumu a ochrany veřejného zdraví, jež těží z dlouhodobě budovaných zdravotních registrů.

GDPR přináší v otázkách udělování souhlasů se zpracováním osobních údajů několik konkrétních ustanovení, jež napomáhají překlenout interpretační nejasnosti při získávání souhlasů. První je obecný požadavek jednoznačnosti a informovanosti souhlasu[7] a požadavek na to, aby byl dán aktivním jednáním subjektu. Souhlas je definován v čl. 4 odst. 11) jako jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. GDPR problém neurčitosti budoucího směřování výzkumu explicitně zmiňuje v recitálu č. 33, když uvádí, že *„Často není možné v době shromažďování osobních údajů v plném rozsahu stanovit účel zpracování osobních údajů pro účely vědeckého výzkumu. Subjektům údajů by proto mělo být umožněno, aby udělily svůj souhlas ohledně určitých oblastí vědeckého výzkumu v souladu s uznávanými etickými normami pro vědecký výzkum. Subjekty údajů by měly mít možnost udělit svůj souhlas pouze pro některé oblasti výzkumu nebo části výzkumných projektů v rozsahu přípustném pro zamýšlený účel.“* Interpretační pravidlo tedy je, že pokud se subjekt účastní výzkumného projektu zabývající se kupříkladu Crohnovou nemocí, může dát dostatečně určitý souhlas k dalšímu použití jeho osobních údajů za účelem výzkumu Crohnovy nemoci i po ukončení daného projektu, aniž by bylo nutné uvádět záměry budoucích a v dané chvíli ještě neznámých projektů. S ohledem na další ustanovení GDPR však lze doporučit, aby měl subjekt údajů možnost aktivně vybírat z obou možností – tedy zpraco-

[7] Srov. recitál (32) GDPR.

vání osobních údajů pouze v rámci daného projektu, nebo dlouhodobému zpracování osobních údajů v konkrétních výzkumných oblastech. Dále je nutno upozornit, že samotné udělení otevřeného souhlasu ještě neznamená, že pro zpracování těchto dat neplatí další limity spočívající zejména v účelovém omezení a minimalizaci údajů.[8]

Dalším problémem běžně se vyskytujícím v praxi a souvisejícím se souhlasem ke zpracování osobních údajů, je považování tzv. informovaného souhlasu pacienta za souhlas se zpracováním osobních údajů ve smyslu čl. 6(1)(a) a čl. 9(2)(a). Informace uvedené v informovaném souhlasu pacienta však často neobsahují náležitosti zákonného výslovného souhlasu se zpracováním osobních údajů. V takovém případě to však ještě nemusí automaticky znamenat, že jsou data pacienta zpracovávána nezákonně. I v případě absence souhlasu, nebo formálním pochybení při jeho archivaci může být zákonným důvodem zpravidla plnění právní povinnosti zdravotnického zařízení ve smyslu čl. 6(1)(f), životně důležitý zájem subjektu údajů ve smyslu čl. 6(1)(d), plnění úkolu ve veřejném zájmu ve smyslu čl. 6(1)(e) nebo oprávněný zájem zdravotnického zařízení ve smyslu čl. 6(1)(f) GDPR. Často přitom může jít o kumulaci více těchto důvodů současně.

Informovaný souhlas s poskytováním zdravotní služby ve formě běžně používané zdravotnickými zařízeními obvykle neplní funkce souhlasu se zpracováním osobních údajů ve smyslu čl. 6(1)(a) nebo čl. 9(2)(a) GDPR. Za tímto účelem navíc souhlasu ani v praxi nebývá třeba, neboť zpracování spadá pod rozsah některého ze zákonných titulů ve smyslu čl. 6(1) a zákonných výjimek ve smyslu čl. 9(2). Pokud však obsah informovaného souhlasu s poskytováním zdravotní služby zároveň nesplňuje veškeré formální požadavky na obsah informovaného souhlasu se zpracováním osobních údajů, může plnit přinejmenším roli srozumitelné informace podané pacientovi ve smyslu čl. 13 GDPR.

[8] Srov. čl. 5 GDPR

3.1.2. Výzkum jako právní základ zpracování

Samotný pojem „vědeckého výzkumu“ je nejasný a ÚOOÚ měl v minulosti za to, že k tomu aby se jednalo o vědecký výzkum musí být splněny dvě podmínky, a to existence výzkumného úkolu a kvalifikovanost subjektu.[9] Toto stanovisko však vychází z předchozí právní úpravy a je velmi pravděpodobné, že po přijetí GDPR bude definice vědeckého výzkumu značně ovlivněna jeho pojetím v rámci evropských výzkumných struktur. V recitálu 159 nabízí interpretační pravidlo, v rámci něhož má být výzkum chápán velmi široce.[10]

3.1.3. Oprávněný zájem instituce jako právní základ

Ze zákonných titulů pro zpracování osobních údajů bývá v praxi špatně pochopen především oprávněný zájem správce. Oprávněný zájem není nějakou absolutní kategorií s taxativním výčtem situací, na které se vztahuje. Správce musí vždy posuzovat oprávněnost svého zájmu vzhledem k procesu zpracování a důvodnému očekávání subjektu údajů. Je tedy třeba při hodnocení oprávněnosti zájmu správce rozlišovat například mezi získáním dat (včetně zohlednění způsobu jejich získání a jejich zdroje), jejich uložením, pořízením jejich kopie, nebo například jejich předáním dalšímu příjemci.

Druhým určujícím kritériem pro posouzení oprávněnosti zájmu správce je pak **oprávněné očekávání subjektu údajů**. To vždy vyplývá z konkrétní situace a správce tak musí na základě příslušných okolností posoudit, zda může subjekt údajů důvodně předpokládat, že jeho data mohou být za příslušným konkrétním účelem ze strany správce zpracovávána.

[9] Srov. stanovisko ÚOOÚ č. 2/2006 – Zpracování osobních údajů v rámci vědy (aktualizace duben 2013) https://www.uoou.cz/stanovisko-c-2-2006-zpracovani-osobnich-udaju-v-ramci-vedy/d-1485.

[10] *A zahrnovat například technologický vývoj a technologické demonstrace, základní výzkum, aplikovaný výzkum a výzkum financovaný ze soukromých zdrojů. K účelům vědeckého výzkumu by rovněž měly patřit studie prováděné ve veřejném zájmu v oblasti veřejného zdraví.* Srov. recitál 159 GDPR.

Interpretační vodítko v tomto směru dávají odst. 47 a 48 preambule ke GDPR následovně:

> *(47) Oprávněné zájmy správce, včetně správce, jemuž mohou být osobní údaje poskytnuty, nebo třetí strany se mohou stát právním základem zpracování za předpokladu, že nepřevažují zájmy nebo základní práva a svobody subjektu údajů, a to při zohlednění přiměřeného očekávání subjektu údajů na základě jeho vztahu se správcem. Tento oprávněný zájem by mohl být dán například v situaci, kdy existuje relevantní a odpovídající vztah mezi subjektem údajů a správcem, například pokud je subjekt údajů zákazníkem správce nebo mu naopak poskytuje služby. Existenci oprávněného zájmu je v každém případě třeba pečlivě posoudit, včetně toho, zda subjekt údajů může v okamžiku a v kontextu shromažďování osobních údajů důvodně očekávat, že ke zpracování pro tento účel může dojít. Zájmy a základní práva subjektu údajů by mohly převážit nad zájmy správce údajů zejména tehdy, jestliže ke zpracování osobních údajů dochází za okolností, kdy subjekt údajů jejich další zpracování důvodně neočekává. Jelikož právní základ pro zpracování osobních údajů orgány veřejné moci má upravit zákonodárce právním předpisem, neměl by se tento právní základ vztahovat na zpracování prováděné orgány veřejné moci při plnění jejich úkolů. Oprávněným zájmem dotčeného správce údajů je rovněž zpracování osobních údajů nezbytně nutné pro účely zamezení podvodům. Zpracování osobních údajů pro účely přímého marketingu lze považovat za zpracování prováděné z důvodu oprávněného zájmu.*
>
> *(48) Správci, kteří jsou součástí skupiny podniků nebo instituce přidružené k ústřednímu orgánu, mohou mít oprávněný zájem na předání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely, včetně zpracování osobních údajů zákazníků či zaměstnanců. Obecné zásady pro předávání osobních údajů v rámci skupiny podniků do podniku nacházejícího se ve třetí zemi zůstávají nedotčeny.*

Z výše uvedeného tedy plyne, že výzkum je sice v obecné rovině možno pokládat za oprávněný zájem výzkumné organizace, ale v konkrétním případě bude vždy třeba posoudit, zda je příslušný konkrétní účel dostatečně legitimní vzhledem k určitému způsobu zpracování dat a dále pak zda mohou subjekty údajů takové zpracování důvodně očekávat. Lze očekávat, že většina výzkumných organizací tedy bude využívat oprávněný zájem spíše jako podpůrný argument pro zákonnost zpracování, vedle jiných právních titulů kterými jsou veřejný zájem nebo souhlas subjektu údajů.

V tomto směru se jedná o jeden z typických případů, kdy GDPR nedává jednoznačnou odpověď a namísto konkrétního stanovení práv a povinností jen obecně odkazuje na kategorie jako „důvodné očekávání subjektu údajů". Tato konstrukce je sice z pohledu správce extrémně obecná a nepředvídatelná, na straně druhé ale umožňuje relativně efektivní postup v konkrétních případech. Tam, kde by bez těchto metafor následoval zákaz, je tedy správci umožněno, najde-li ve shora uvedených obecných kategoriích argumenty oprávněného zájmu, data zpracovávat. Je jen třeba, aby správce realisticky vyhodnotil okolnosti konkrétní situace (kterou nikdo jiný než správce z logiky věci ani lépe znát nemůže). Vedle obecného DPIA je v tomto směru z pohledu správce vhodným nástrojem především konzultace s pověřencem.

V situacích, kdy správci nesvědčí jiný zákonný důvod ke zpracování osobních údajů, je tedy třeba, aby správce konfrontoval konkrétní účel zpracování dat s příslušnými okolnostmi (tj. typ zpracování a důvodné očekávání subjektu údajů) a pokud, typicky na základě konzultace s pověřencem, konstatuje důvodné očekávání subjektu údajů, aby tento postup zdokumentoval pro případ kontroly.

3.2. Sdílení dat vs. právní titul

3.2.1. Výzkumná data v kontextu otevřeného přístupu a otevřené vědy

Otázky otevřeného přístupu k výzkumným výsledkům, doktríny Open Access, volných licencí není potřeba v době vydání této publikace podrobněji představovat. Ranní fáze Open Access se soustředila spíše na zpřístupňování publikovaných článků, v současné době se však klade větší důraz na sdílení a propojování výzkumných dat. Pravidla otevřeného přístupu ERC ve vztahu k výzkumným datům pouze doporučují výzkumníkům, aby si uchovávali soubory obsahující jejich veškeré výzkumné údaje, které použili v průběhu své práce, a aby byli připraveni sdílet tato data s dalšími výzkumníky.[11] Doporučení RVVI z roku 2014 již pod otevřeným přístupem k vědeckým informacím rozumí nejen přístup k finálním publikacím ale již i data, která mohou sloužit k ověření výsledků.[12] Doporučení Evropské komise o přístupu k vědeckým informacím a jejich uchovávání členským státům explicitně doporučuje, aby vymezily *jasné politiky pro šíření výzkumných údajů, které vznikly v rámci výzkumu financovaného z veřejných prostředků, a otevřený přístup k nim.*[13] **Amsterdamská výzva pro otevřenou vědu** , právně nezávazný dokument zpracovaný panelem odborníků na podnět Rady Evropské unie, se otázkám zacházení s daty věnuje v několika rovinách a formuluje požadavek na přehodnocení přístupu k opakovanému využívání (re-use) výzkumných dat jako jeden ze čtyř klíčových cílů pro

[11] European Research Council, Scientific Council. *Opean Access Guidelines for researchers funded by ERC*. revised October 2013. Říj. 2013. URL: http://erc.europa.eu/sites/default/files/document/file/ERC_Open_Access_Guidelines-revised_2013.pdf.

[12] *Zápis z 291. zasedání Rady pro výzkum, vývoj a inovace konaného 28. února 2014 na Úřadu vlády*. 2014. URL: http://www.vyzkum.cz/FrontClanek.aspx?idsekce=711410&ad=1&attid=714365, str. 9.

[13] Evropská komise. *Doporučení Komise ze dne 17. července 2012 o přístupu k vědeckým informacím a jejich uchovávání (2012/417/EU)*. Úřední věstník Evropské unie L 194/39. 2012. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012H0417, čl. 3.

zvýšení výkonu výzkumného sektoru do roku 2020.[14] Dokument volá po tom, aby se požadavek na otevření výzkumných dat stal standardním požadavkem pro veškerý dotovaný výzkum ve veřejném sektoru a zároveň klade důraz na zvýšení standardů při práci s výzkumnými daty a lepší správu výzkumných dat.[15] Z klíčových dokumentů je na místě zmínit rovněž publikovaná doporučení Evropské univerzitní asociace k zavedení otevřeného přístupu z roku 2017,[16] jež své členy nabádají k vytváření publikačních platforem na bázi Open Access, ale také k vypracování institucionálních pravidel pro koloběh výzkumných dat. Dobré správy výzkumných dat by měla vycházet z tzv. FAIR data principů, což je anglický akronym pro Findable (dohledatelná), Accessible (přístupná), Interoperable (propojitelná), and Re-usable (opakovaně použitelná) data.[17] Oba dokumenty akcentují institucionální či sdílené repositáře jako primární nástroj pro lepší správu dat. V rámci příprav *Národní strategie otevřeného přístupu k vědeckým informacím v ČR 2016–2020* (jejíž příprava a schválení se protáhla o rok) již Vláda ČR identifikuje otevřený přístup k vědeckým informacím jako nástroj pro podporu kvality a efektivity výzkumu, urychlení inovací a ekonomického růstu a povědomí o českých výzkumných institucích a o jejich významu.[18] Dá se předpokládat,

[14] Experts and stakeholders of the Amsterdam Conference 'Open Science – From Vision to Action', hosted by the Netherlands' EU Presidency on 4 and 5 April 2016. *Amsterdam Call for Action on Open Science*. 2016. URL: http://openaccess.nl/sites/www.openaccess.nl/files/documenten/amsterdam-call-for-action-on-open-science.pdf, str. 4.

[15] Ibid., str. 14.

[16] European University Association. *Toward Full Opean Access in 2020. Aims and recommendations for university leaders and National Rectors' Conferences*. Červ. 2017. URL: https://eua.eu/resources/publications/417:towards-full-open-access-in-2020.html, str. 6.

[17] Mark D. Wilkinson et al. „The FAIR Guiding Principles for scientific data management and stewardship". In: *Scientific Data* 3.160018 (2016). URL: http://www.nature.com/articles/sdata201618.

[18] Průběžná sebehodnotící zpráva Akčního plánu České republiky Partnerství pro otevřené vládnutí na období let 2016 až 2018, 2017. Praha: Úřad vlády České republiky, Ministr pro lidská práva, rovné příležitosti a legislativu. Dostupné také z: http://www.korupce.cz/assets/partnerstvi-pro-otevrene-vladnuti/Prubezna-sebehodnotici-zprava-Akcniho-planu-Ceske-republiky-Partnerstvi-pro-

že změna přístupu poskytovatelů grantů, zvýší zájem výzkumných institucí o sdílení dat na otevřeném principu.

Pokud výzkumná data obsahují osobní údaje, je jejich sdílení i analýzou dat převzatých z jiných institucí považováno za zpracování a je nutno k nim mít vyřešen jak titul tak legitimitu účelu zpracování.

3.2.2. Specifika sekundárního užití (nevýzkumných) dat pro výzkumné účely

O sekundární užití dat se může jednat v případě druhotného využití výzkumných dat, ale také o zpracování dat, která nebyla sesbírána přímo výzkumnou organizací, nýbrž třetím subjektem za zcela jiným účelem (poskytování služeb, poskytování zdravotní péče, plnění zákonné povinnosti při sběru statistických údajů). Obecné nařízení o ochraně osobních údajů (GDPR) do reflektuje a zohledňuje společenskou potřebu sekundárního využití osobních dat k výzkumným účelům a přináší několik důležitých pravidel, která zvyšují právní jistotu při realizaci legitimních výzkumných postupů.

V recitálu 33 GDPR zohledňuje skutečnost, že v mnoha případech není možné v době shromažďování osobních údajů v plném rozsahu stanovit účel zpracování osobních údajů pro účely vědeckého výzkumu, a deklaruje, že by k platnému souhlasu s dalším zpracováním výzkumných dat mělo postačovat obecnější vymezení oblastí výzkumu nebo části výzkumných projektů.GDPR pro sekundární užití dat používá termín „další zpracování“, přičemž toto další zpracování explicitně legitimizuje pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely,[19] a to i v případě tzv. zvláštních

otevrene-vladnuti-na-obdobi-let-2016-az-2018.pdf [cit. 2017-12-15] s. 23–24

[19] Srov. čl. 5 GDPR.

kategorií osobních údajů. GDPR legitimizuje i analýzu dat v rámci tzv. zdravotních registrů.[20]

Skutečnost, že při sekundárním užití lze aplikovat výzkumnou výjimku, neznamená bezbřehou možnost dispozice s těmito údaji. Pořád se bude jednat o zpracování osobních údajů, na něž se vztahují obecné zásady zpracování a další ustanovení a nařízení, z nichž není výslovně uvedena výjimka.[21] Sběr a zpracování těchto osobních údajů bude podléhat požadavkům na jasné stanovení účelu a z toho vyplývajících účelových omezení, požadavků na minimalizaci údajů a zachování její integrity a důvěrnosti. V souladu s článkem 89 GDPR se bude muset každá instituce zabývat tím, jak zajistit záruky práv subjektů údajů, přičemž se doporučuje pseudonymizace údajů všude tam, kde je to možné.

GDPR je tedy na jednu stranu k výzkumným institucím velmi vstřícné tím, že jim poskytuje značnou legitimitu pro sekundární zpracování osobních údajů, na druhou stranu požaduje, aby se velmi seriózně zabývaly ochranou i těch dat, které byly doposud považovány za anonymní, byť jsou ve skutečnosti pseudonymní.

3.2.3. Specifika spolupráce několika výzkumných týmů

Výzkumná data často vznikají ve spolupráci výzkumných týmů z několika institucí. Původci dat se stávají doktorští studenti bez pracovního poměru k instituci, nebo osoby, které nejsou zaměstnáni v žádné výzkumné instituci (typicky například lékař podílející se na klinické studii). Multicentrická výzkumná spolupráce navíc přináší problémy v podobě obtížného určení osoby, jíž náleží právo rozhodovat o zveřejnění či dalším využití výzkumných dat. Osoby fakticky rozhodující o zveřejnění či sdílení dat nemusí být de iure osobami, kterým skutečně náležejí práva rozhodovat o dispozici s daty. Překročení oprávnění jednotlivého zaměstnance a neoprávněné sdílení dat jiné výzkumné instituci znamená pro

[20] Srov. recitál GDPR č. 157.
[21] Srov. recitál GDPR č. 156.

jeho mateřskou instituci „incident“, neboli případ porušení zabezpečení osobních údajů, ale zároveň oslabuje legitimitu zpracování u instituce, která data přijala.

Čerpání dat z nespolehlivého zdroje, nebo nesprávná manipulace při sdílení dat ohrožuje jak instituci sdílející, tak instituci přebírající. V současné době však neexistuje jednoduchý způsob, jak v případě potřeby prokázat, že instituce, od níž data vysoká škola přebírá je právě tím spolehlivým zdrojem, jež má právo data předat. Jistým řešením by mohly být kodexy chování pro správu výzkumných dat, které by umožnily hladké a důvěryhodné sdílení a přebírání dat mezi výzkumnými organizacemi. Jak již bylo uvedeno ve výkladu výše, článek 40 obecného nařízení o ochraně osobních údajů (GDPR) nabádá subjekty zastupující kategorie správců v různých sektorech hospodářského i společenského života vytvářet kodexy chování vztahující se ke zpracování osobních údajů ve vybraných odvětvích. Účelem těchto kodexů je pomoct institucím z daného odvětví dodržovat pravidla zavedená GDPR a do jisté míry tato pravidla přetavovat do ustálených a obecně akceptovaných vzorců chování. Článek 40 předpokládá, že tyto kodexy chování budou vypracovávány zájmovými nebo profesními organizacemi a následně předkládány ke schválení národnímu[22] dozorovému úřadu k autorizaci a zveřejnění. Kodex chování se zveřejněním nestává podzákonným předpisem. Předpokládá se, že se k jeho dodržování jednotlivé instituce zaváží dobrovolně.[23] Přihlášením se ke kodexu může dát instituce veřejnosti jednoduchý a srozumitelný signál o nastaveném standardu ochrany osobních údajů. Ke stejnému účelu mohou sloužit certifikace, pečetě a osvědčení vydané nezávislou institucí na základě čl. 42 GDPR.

Výchozí pozice vysokých škol a výzkumných institucí v procesu zavádění požadavků GDPR je docela výhodná, protože výzkumné instituce

[22] V souladu se sedmým odstavcem je možné předložit kodex, jehož význam přesahuje hranice jednoho členského státu, Evropské komisi, a to prostřednictvím tzv. Evropského sboru pro ochranu osobních údajů, nově založeného orgánu, jehož kompetence jsou popsány v článku 68.

[23] A to buď na základě smlouvy se zájmovou organizací, jež kodex vytvořila, nebo na základě jednostranného prohlášení.

věnovaly ochraně soukromí velkou pozornost i před přijetím obecného nařízení. Univerzity běžně školí své zaměstnance a studenty o zásadách ochrany soukromí a výzkumné etiky. Grantové agentury, redakční rady časopisů i vedení výzkumných institucí vyvíjejí tlak na to, aby se výzkumné projekty posuzovaly ještě před svým zahájením v rámci etických komisí. Empirickým důkazem o tom, že se pokusy o kodexy chování stanou trendem nejbližších let, je rovněž nedávná iniciativa evropské výzkumné infrastruktury BBMRI-ERIC, která se zabývá biobankami. BBMRI-ERIC na svých webových stránkách v roce 2017 oznámila zahájení prací na *„Kodexu chování pro zpracování osobních údajů pro účely vědeckého výzkumu v oblasti zdravotnictví“*,[24] jenž má ambici stát se univerzálním kodexem pro sdílení výzkumných dat v oblasti zdravotnictví (BBMRI-ERIC, 2017).

Kodexy chování mohou mít obrovský význam v oblasti sdílení dat. Jestliže výzkumná úloha vyžaduje agregaci dat z více výzkumných center, je nezbytné, aby měl subjekt, jež data sbírá, jistotu, že ostatní centra shromažďují a zpracovávají údaje v souladu se zákonnými normami. Výzkumné instituce, které shromažďují data nesdílená jinými subjekty, však budou mít problém kupříkladu prokázat, že subjekt údajů dal se sběrem dat souhlas. S ohledem na textaci článku 24 GDPR, který stanovuje, že *dodržování schválených zásad chování, jak je uvedeno v článku 40, nebo schválených certifikačních mechanismů uvedených v článku 42 může být použito jako prvek prokazující splnění povinností správce.* Jsme toho názoru, že kodexy chování, spolu s certifikačními mechanismy, mohou prokázat dodržování pravidel nejen vůči kontrolnímu orgánu, ale i vůči jiným správcům a zpracovatelům. Pokud agregující instituce nemůže prokázat, že příslušná data byla sesbírána a zpracována v souladu se zákonem, protože důkazy o zpracování drží jiný správce údajů, může k prokázání souladu postačit, že data sbírá od instituce, které dodržuje schválený kodex chování, a je certifikována podle článku 42 GDPR.

[24] BBMRI-ERIC, „Group mulls guidance on use of personal data“, 3. února 2017, dostupné z: http://www.bbmri-eric.eu/news-events/code-of-conduct-for-using-personal-data-in-health-research/ citováno 31. 10.2017

Mezinárodní spolupráce mezi výzkumnými týmy není omezena hranicemi Evropské unie. Kodexy chování v konkrétních oblastech výzkumu by mohly být přijaty v souladu s právními předpisy EU a následně dobrovolně převzaty i výzkumnými institucemi mimo Evropskou unii, což by mohlo v souladu s čl. 40 (3) GDPR ulehčit nebo přímo umožnit výměnu dat s těmito institucemi. Pro přijímání případných kodexů dle čl. 40 ve výzkumné oblasti však existují i poměrně závažné překážky. Jsou jimi zejména nedostatek jediného orgánu nebo sdružení, které skutečně zastupuje všechny výzkumné instituce na mezinárodní úrovni, protichůdné potřeby jednotlivých odvětví vědy a překrývání výzkumu s jinými sektory, které mohou vyžadovat vlastní kodexy chování.

3.3. Studentské práce v prostředí VŠ

Výzkum v prostředí vysokých škol přirozeně probíhá za více, či méně angažované přítomnosti studentů. Často je však prohlížena skutečnost, že studenti nejsou nevyhnutně také zaměstnanci instituce, co nemá dopady pouze na to, že nedochází k přesunu oprávnění k výkonu autorských práv, ale také na to, že student je z pohledu přístupu k osobním údajům třetí osobou. Zpracování studentských prací (bakalářských, diplomových, disertačních či prací jinak zpracovaných v rámci výuky) v prostředí vysokých škol je třeba rozdělit do dvou skupin:

1. **Zpracování v zájmu studenta,** kdy instituce do procesu zpracování nevstupuje ani nemá na práci zájem s výjimkou toho, že práce se podmínkou k postupu studiem nebo k jeho absolvování a jako taková je pak také institucí může zveřejněna za účelem. Zde se jedná o soukromé resp. nahodilé *zpracování dat studentem jakožto fyzickou osobou, pro svou osobní potřebu, na něž se GDPR nevztahuje.* V tomto případě je nutné ošetřit pouze ty případy, kdy student pro vlastní výzkum přistupuje k osobním údajům, které již vysoká škola spravuje. Pokud student v rámci své diplomové práce nahodile uvede údaje vztahující se ke konkrétním osobám, nestává

se univerzita správcem osobních údajů pouze proto, že danou práci archivuje, nebo zveřejňuje v souladu s požadavky zákona.

2. **Zpracování v zájmu instituce**, kdy je studentská práce součást řešení vědeckého/výzkumného projektu neseného institucí nebo jejím zaměstnancem. V takovém případě se jedná o práci, na níž *se vztahuje GDPR a obsahově i tato příručka.* V tuto chvíli je potřeba se studentem uzavřít zvláštní smlouvu v níž bude vystupovat jako zpracovatel pověřený institucí. Nejpraktičtějším řešením však ve většině případů bude studenta „internalizovat“ pomocí pracovněprávního vztahu s odpovídající doložkou o mlčenlivosti a ochraně osobních údajů.

4. Hmotná práva subjektu údajů

4.1. Právo na Informace o zpracování osobních údajů

Relevantní ustanovení: Čl. 13, 14 GDPR a § 8, 17, 18, 26 ZZOÚ

Právo na informace je zakotvené v článcích 13 a 14 GDPR. Právu subjektu údajů odpovídá povinnost správce poskytovat jistou množinu informací, která se liší podle toho, zda jsou osobní údaje získávány od subjektu údajů (čl. 13 GDPR) nebo od třetí strany (čl. 14 GDPR). V zásadě se ale vždy jedná o poskytnutí základních informací o identitě správce a plánovaném režimu zpracování osobních údajů.

Informační povinnost lze splnit různou formou a volba je v tomto případě na správci. Jedná se o typický případ performativního pravidla, za jehož porušení hrozí sankce pouze při prokázání negativní dispozice, tj. že subjekt údajů nebyl informován. Zvláštní režim informování subjektu údajů je upraven pouze pro informace poskytnuté ústně – v takovém případě je třeba, aby správce prokázal, že si ústní poskytnutí informací subjekt údajů vyžádal (to bude typické např. při kvalitativním výzkumu, kde jsou data získávána formou zvukové nebo audiovizuální nahrávky).

Prvním logickým krokem při plnění povinností dle čl. 13 a 14 bude zpravidla vytvoření webové stránky, kde subjekt údajů zjistí přinejmenším následující skutečnosti (není vhodné tento okruh nějak výrazně iniciativně rozšiřovat, neboť by to ve výsledku mohlo mít negativní dopad na jednoduchost a srozumitelnost):

Pokud se údaje získávají od subjektu údajů:

- jasné označení správce, včetně sídla, identifikačního čísla osoby, případně dalších údajů
- kontaktní údaje případného DPO
- účely zpracování a právní základ pro zpracování
- oprávněné zájmy správce nebo třetí strany
- příjemce nebo kategorie příjemců osobních údajů
- úmysl předat osobní údaje do třetí země nebo mezinárodní organizaci a informaci o tom, jestli se jedná o zemi, u níž Evropská komise rozhodla, že chrání osobní údaje odpovídajícím způsobem
- doba uložení osobních údajů, příp. kritéria pro určení doby
- existenci práva na přístup k osobním údajům, opravu, výmaz, omezení zpracování, odvolání souhlasu, podat stížnost, důsledky neposkytnutí, zda dochází k automatizovanému zpracování
- úmysl zpracování pro jiný účel, než pro který byly shromážděny

Pokud osobní údaje nepochází od subjektu údajů (tj. správce je legitimně získal z jiného zdroje, než kterým je subjekt údajů – např. v rámci konsorcionální spolupráce, nákupem apod.):

- totožnost a kontaktní údaje správce a jeho případné zástupce,
- kontaktní údaje případného DPO,
- účely zpracování a právní základ pro zpracování,
- kategorie dotčených osobních údajů,
- příjemce nebo kategorie příjemců osobních údajů,
- úmysl předat osobní údaje do třetí země nebo mezinárodní organizaci a související údaje o bezpečnostní situaci osobních údajů v daném subjektu,

- doba uložení osobních údajů, příp. kritéria pro určení doby,
- oprávněné zájmy správce či třetí osoby,
- existenci práva na přístup k osobním údajům, opravu, výmaz, omezení zpracování, vznést námitku, přenositelnost údajů,
- úmysl zpracování pro jiný účel, než pro který byly shromážděny, odvolání souhlasu, podání stížnosti, zdroj, automatizované rozhodování.

Obsah informačního webu není rigorózně upraven (viz kapitola 10 pro příklady dokumentace). Platí tedy, že sankcí bude stiženo pouze takové jednání správce, na jehož základě bude možno z pohledu vrchnosti konstatovat, že subjekt údajů např. nebyl informován o totožnosti správce.

Konkrétní forma informování subjektu údajů rovněž není předmětem úpravy. Čl. 12 odst. 1 pouze nařizuje, aby informace byly poskytnuty „stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků". Jedná se přitom trochu o chucpe právotvůrce, neboť samotné nařízení je na mnoha místech nesrozumitelné a zbytečně upovídané.

Čl. 12 odst. 7 umožňuje alternativní použití standardizovaných ikon. I když použití standardizovaných ikon teoreticky nelze vyloučit i v případě zpracování dat k vědeckým účelům, nutno říct, že žádné univerzálně rozpoznávané a standardizované ikony pro zpracování dat za vědeckým účelem nejsou k dispozici. Lze opatrně předpokládat, že standardizované ikony mohou být na základě delegovaných aktů Komise předmětem kodexů – v dohledné době však nic takového zřejmě nebude k dispozici.

Pro zpracování dat k vědeckým účelům je důležité ustanovení čl. 12 odst. 3 a čl. 13 odst. 4, tj. povinnost informovat subjekt údajů o zpracování dat za jiným účelem než pro účel, k němuž byla data původně získána. Zpracování dat k vědeckým účelům je totiž typickým zákonným důvodem zpracování osobních údajů bez souhlasu subjektu údajů (to platí i pro

zvláštní kategorie údajů). Je tedy běžné, že data získaná za jedním účelem jsou později bez souhlasu subjektu údajů legitimně vědecky využívána k jiným účelům (např. data získaná pro účely jednoho projektu jsou dále zpracovávána dalšími projekty).

„Vědecké účely" přitom sice jsou zákonným důvodem zpracování, ale nepředstavují per se účel např. ve smyslu čl. 13 odst. 1 písm. c) nebo čl. 14 odst. 1 písm. c) GDPR. Na informační web tedy nelze umístit pouze informaci ohledně toho, že jsou určité údaje zpracovávány „k vědeckým účelům" – namísto toho je nutno účel konkrétně specifikovat, tj. na informační web uvést, že data budou užita k výzkumu konkrétního vědeckého zadání (např. specifikovaného vědeckým projektem), nebo k výzkumu konkrétní vědecké problematiky (například vymezení skupiny nemocí). Pokud budou dříve získaná data použita k jinému výzkumnému úkolu, než v jehož rámci byla původně získána, je třeba na informačním webu identifikovat nový účel zpracování, tj. například napsat, že data získaná pro účely jednoho projektu jsou nyní využívána v jiném projektu.

Plnění informačních povinností dle čl. 13 a 14 nelze na rozdíl od čl. 15, 16, 18 a 21 omezit u zpracování pro vědecké účely evropským ani národním zákonným právem. Zatímco tedy mohou být práva subjektů podle cit. článků různě limitována (tj. např. mohou být data pro vědecké účely zpracovávána i přes námitky subjektu údajů), má subjekt údajů právo na informace bez omezení. Jedinou výjimkou jsou případy, kdy nejsou údaje získány od subjektu údajů a bylo by neúměrně složité subjekt údajů informovat. K tomu dochází např. tehdy, pokud subjekt nelze ztotožnit, nebo je extrémně složité příslušné údaje zpracovat (např. při získání rozsáhlého papírového archivu z pozůstalosti by i jen zjištění toho, zda, čí a jaké osobní údaje obsahuje, představovalo značné úsilí a vysoké náklady). Zároveň je nutno vzít v úvahu, že snahou o ztotožnění subjektu může dojít k oslabení jeho práv. Snaha o ztotožnění subjektu v pseudonymizované nebo anonymizované sadě dat pouze za účelem jeho informace může vést k oslabení ochrany jeho osobních údajů a také i k oslabení ochrany osobních údajů dalších subjektů v datové sadě.

4.2. Právo na přístup k osobním údajům

Relevantní ustanovení: Čl. 15 a rec. 47 GDPR a § 11, 18 ZZOÚ

Toto právo vychází z článku 15 GDPR a lze jej považovat za základní právo při uplatňování práv pro ochranu osobních údajů. Právo na přístup k osobním údajům se skládá ze dvou souvisejících částí. Na jedné straně stojí povinnost správce potvrdit či vyvrátit subjektu údajů, zda o něm zpracovává osobní údaje. Tento první krok je esenciální pro uplatňování dalších práv, jelikož subjekt údajů zjistí, zda o něm vůbec nějaké údaje správce zpracovává.

Po získání potvrzení, že správce zpracovává osobní údaje daného subjektu, si může subjekt v rámci svého práva na přístup vyžádat kopii těchto dat. Poskytnutí kopie je apriori zdarma. Pokud by ovšem docházelo k opakovaným žádostem o poskytnutí kopií, může si správce účtovat přiměřený poplatek na pokrytí jeho administrativních nákladů.

Forma, v jaké je kopie dat poskytována, je do velké míry determinována formou žádosti subjektu. Pokud subjekt sám požádá v elektronické formě, může mu být poskytnuta informace rovněž v elektronické formě. V každém případě je ale nutné dbát o řádnou identifikaci a autentizaci subjektu. Právo na přístup a pořízení kopie dat lze splnit i tím, že uživatel dostane data k dispozici pro nahlédnutí a zkopírování v rámci zabezpečeného informačního systému.

Kromě potvrzení a poskytnutí výše zmíněné kopie, správce poskytne subjektu údajů také informace o:

- účelu zpracování,
- kategoriích dotčených osobních údajů,
- příjemcích, kterým byly údaje zpřístupněny včetně jejich kategorizace (příjemci ve třetích zemích nebo v mezinárodních organizacích),

- plánované době či kritérium ke stanovení doby zpracování,
- existenci práva na opravu, výmaz nebo omezení zpracování včetně námitky proti tomuto zpracování,
- právu podat stížnost u dozorového úřadu,
- veškerých dostupných informacích o zdroji osobních údajů, pokud nejsou získány přímo od subjektu údajů,
- skutečnosti, zda dochází k automatizovanému rozhodování, včetně profilování, nebo alespoň informace o předpokládaných důsledcích takového zpracování pro subjekt údajů.

Vzhledem k tomu, že při zpracování za účelem vědeckého výzkumu dochází často k předávání osobních údajů do třetích zemí mimo EHS či do mezinárodních organizací, má v takových situacích subjekt údajů nárok také na informace o vhodných zárukách o bezpečnosti předání, jež byly přijaty a jež zaručují subjektu účinnou právní ochranu.

Samotné nařízení ovšem umožňuje národním státům přijmout výjimky a slevit tak z nároků na zpracování osobních údajů mimo jiné i pro zpracování za účelem vědy a výzkumu. Tyto výjimky jsou zapracovány do návrhu českého zákona hned ve dvou ustanoveních § 11 odst. 3 a § 18 odst. 3, přičemž každé ustanovení míří na jiný druh výzkumu.

Prvně zmíněný § 11 odst. 3 poskytuje cílenou výjimku umožňující v přiměřeném rozsahu odložení, přiměřené použití nebo dokonce úplně vynětí z práva na přístup, pokud oprávněné zájmy správce (včetně výzkumné organizace, jíž jsou osobní údaje poskytnuty nebo třetí strany) převáží nad zájmy nebo základními právy subjektu údajů. Při vážení zájmů správce vůči zájmu subjektu se přitom přihlíží zejména k přiměřenému očekávání subjektu na základě jeho vztahu se správcem. Situací, kdy v případě vědeckého výzkumu na člověku veřejný zájem, nebo zájem správce převáží nad zájmem jednotlivce bude v praxi poskrovnu. Jedním

z myslitelných případů je třeba informace o tom, zda byla subjektu zaslepeného klinického hodnocení podána léčivá látka nebo placebo,[1] případně ochrana připravované patentové přihlášky. I v těchto případech však nemůže jít o úplné omezení práva na poskytnutí informace, je však možné poskytnutí informace oddálit.

Druhá forma vynětí z práva na přístup týkající se výzkumných dat pak zohledňuje zejména legitimní potřebu chránit informace v době před jejich dalším zpracováním. To může zahrnovat zejména typicky případy ochrany před zveřejněním, ale také další situace, kdy by realizací práva na přístup došlo ke zmaření účelu jejich zpracování. Tato výjimka však není absolutní, příkladem může být § 18 odst. 3, který podmiňuje omezení či vyloučení pouze na dobu potřebnou k dosažení účelu, nebo dobu nutnou na ochranu zdroje informace ve vědeckém výzkumu, pokud by realizací práva na přístup k osobním údajům došlo ke zmaření účelu jejího zpracování.

V samotné praxi tak lze právo na přístup omezit buď dlouhodobě za účelem efektivního výkonu vědeckého výzkumu, či dočasně za účelem ochrany zdroje. Konkrétní situaci je tedy vždy nutné individuálně posoudit co do charakteru ale také rozsahu omezení. Lze si tedy představit omezení práv na přístup subjektů údajů ke kopii dat či poskytnutí informací o jednotlivých příjemcích zpracování při převážení oprávněného zájmu výzkumné instituce na efektivním běhu výzkumu. Na druhou stranu ale bude zřídka docházet k situacím, kdy bude možné trvale odmítnout první fázi práva na přístup, a tedy pouhé sdělení, zda instituce zpracovává o subjektu osobní údaje.

O omezení práva na přístupu rozhoduje správce osobního údaje, na své riziko. Subjekt údajů se následně může obrátit na ÚOOÚ se stížností.

[1] „Od-zaslepení" klinické studie je umožněno pouze na základě bezpečnostních důvodů v souladu s přílohou č. 3 nařízení č. 536/2014 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

4.3. Právo na opravu

Relevantní ustanovení: Čl. 16, 89 GDPR a § 19 ZZOÚ

Právo na opravu osobních údajů je právo, zakotvené ve čl. 16 GDPR. Jeho uplatnění je na rozdíl od ostatních práv subjektů údajů i v bezprostředním zájmu správce. Jako takové totiž garantuje opravu nepřesných osobních údajů, s nimiž správce nakládá, pokud o to subjekt požádá. Vedle opravy chyby, jež se v osobních údajích může vyskytnout, však toto právo pokrývá i případy doplnění neúplných osobních údajů, čehož subjekt může dosáhnout např. poskytnutím dodatečného prohlášení.

Právo na opravu doplňuje obecnou povinnost správce zpracovávat osobní údaje přesné a přiměřeně aktualizované, jak stanoví zásada přesnosti v čl. 5 odst. 1 písm. d). Ve své podstatě tak výkon tohoto práva usnadňuje správci výkon jeho obecných povinností a přispívá k řádnému zpracování založeném na pravdivých údajích, což je pro výzkumné účely více než žádoucí.

Byť je právo na opravu jedním z práv, jehož omezení pro vědecké účely přímo nabízí čl. 89 GDPR, český zákonodárce na rozdíl od omezování ostatních práv, ponechal toto právo bez výjimky. V tuzemském ZOOÚ jsou upraveny pouze omezení související s oznamovací povinností při provedení opravy. Kromě informování subjektu musí správce oznámit provedení opravy všem, komu osobní údaje předal, aby tak zaručil přesnost zpracovávaných údajů.

Nutno však zdůraznit, že ztráta několika jednotlivců z většího sledovaného celku, která pouze ovlivňuje statistickou sílu výsledků, ne však povahu objevu nebo validitu výsledků neznamená zmaření celého výzkumu. Tam, kde smazání údajů o jednom výzkumném subjektu v zásadní míře neovlivní výsledek celého statistického měření, se o danou výjimku nelze opírat.

Při režimu zpracování osobních údajů za účelem vědy a výzkumu nebude zřejmě možné příliš kontrolovat správnost osobních údajů z vnějšku.

O to spíše, ale správce musí dbát na správnost a úplnost osobních údajů, jež zpracovává a pokud zjistí nepřesnost, opravit ji bez zbytečného odkladu. Provedení opravy pak správce oznamuje nejen subjektu údajů, ale také všem, komu osobní údaje předal.

4.4. Právo na výmaz

Relevantní ustanovení: Čl. 17 GDPR a § 9 ZZOÚ

Právo na výmaz, jež je široké veřejnosti známé jako „právo být zapomenut" je právo subjektu údajů na smazání některých osobních údajů. Jako takové se snaží suplovat neschopnost virtuálního světa zapomínat a ve formě čl. 17 GDPR je toto právo přiznáno z těchto taxativně uvedených důvodů:

- osobní údaje již nejsou potřeba pro účely, pro které byly shromážděny,
- subjekt údajů odvolal souhlas jakožto jediný právní důvod pro zpracování,
- na základě námitky subjektu nebyly zjištěny převažující oprávněné důvody pro zpracování,
- osobní údaje byly zpracovány protiprávně,
- osobní údaje musí být vymazány na základě právní povinnosti,
- osobní údaje byly shromážděny s nabídkou služeb informační společnosti dítěti.

Pokud je dán alespoň jeden z výše uvedených důvodů má správce povinnost údaje smazat a v případě, že údaje zveřejnil, pak přijmout cenově a technologicky přiměřené kroky k informování správců, kteří údaje také zpracovávají. I na ty se pak vztahuje povinnost nejen osobní údaje ale i odkazy, kopie a replikace těchto údajů vymazat.

Vzhledem k invazivním dopadům, jež uplatnění práva na výmaz správcům způsobuje, se výjimka pro účely vědeckého výzkumu objevila již přímo v třetím odstavci daného článku. Ten stanoví, že pokud je veřejný zájem na vědeckém výzkumu a je pravděpodobné, že by uplatnění práva na výmaz znemožnilo, nebo vážně ohrozilo splnění cílů takového zpracování, pak se právo na výmaz neuplatní. Pokud tedy zpracování pro vědecké účely probíhá ve veřejném zájmu, nemusí správce vyhovět žádostem o výmaz, ale musí zvážit, zda by pro vědecké účely nepostačil méně intenzivní zásah do práv jednotlivce, například anonymizací, nebo pseudonymizací dat. V případech zvlášť regulovaného výzkumu ještě může nastat situace, kdy se veřejný zájem nebo povinnost plnit právní povinnost nebude vztahovat pouze na dosažení výsledku samotného, ale také na zajištění hodnověrnosti výzkumu a možnosti zpětné kontroly průběhu výzkumu. Nemusí tedy platit, že ukončením výzkumu končí i právní titul výzkumná data zpracovávat.

4.5. Právo na omezení zpracování

Relevantní ustanovení: Čl. 18 GDPR a § 13, 19 ZZOÚ

Právo na omezení zpracování je sekundární institut, který prozatímně upravuje režim zpracování, zatímco je rozhodnuto o primárním nároku. Samotné omezení zpracování přitom může spočívat v dočasném znepřístupnění osobních údajů, přesunu do jiného systému zpracování, nebo dočasném skrytí údajů na webové stránce. Tento institut, který se použije, pokud:

- subjekt popírá přesnost údajů, a to po dobu, než správce posoudí přesnost osobních údajů,
- zpracování je protiprávní a subjekt o omezení požádá místo jejich výmazu,
- správce již údaje nepotřebuje, ale subjekt je požaduje pro určení, výkon nebo obhajobu právních nároků,

- po dobu posouzení, čí oprávněné důvody převáží, pokud subjekt vznesl námitku proti zpracování.

Jak je vidět z výčtu, všechny tyto situace vždy souvisejí s předcházející aktivitou subjektu údajů, který uplatnil svá práva.

Skutečnost, že jsou dané údaje postiženy aktuálním omezením zpracování, by měla být u údajů zřetelně uvedena. Údaje postižené omezením mohou být, s výjimkou jejich uložení, zpracovány pouze z důvodu určení, výkonu či obhajoby právních nároků, ochrany práv jiné fyzické osoby, z důvodu zájmu Unie nebo členského státu, jinak pouze se souhlasem subjektu údajů. Pakliže by mělo být omezení zrušeno, musí o tom být subjekt údajů předem informován.

Je třeba ovšem poznamenat, že pokud jsou správci údajů dočasně omezeni v jejich zpracování, nezbavuje je to povinnosti tyto osobní údaje předat či zpřístupnit, pokud tuto povinnost stanoví jiný právní předpis. Při uskutečnění takového předání budou osobní údaje opět příznačným způsobem označeny jako údaje uvedené v čl. 18 odst. 1 GDPR.

I výkon práva na omezení zpracování patří mezi ty práva, jež je možné národní legislativou omezit, pokud je zpracování činěno pro účely vědeckého výzkumu. Ke zúžení použití práva na omezení zpracování se český zákonodárce pustil v § 19 ZZOÚ kde stanoví, že omezení zpracování pro účely vědeckého výzkumu je možné pouze tehdy pokud správce, již osobní údaje nepotřebuje pro účely zpracování a subjekt tyto údaje požaduje pro určení, výkon nebo uplatnění právních nároků. Pokud jsou tyto podmínky splněny kumulativně, nemusí správce zasahovat do dosavadního průběhu zpracování a při splnění informační povinnosti, může pokračovat ve výzkumu. Ve svém důsledku tedy nebude právo na omezení zpracování častou překážkou při zpracování osobních údajů pro vědecký výzkum, jelikož dokud bude daný údaj potřebný pro probíhající výzkum, nelze naplnit zužující požadavky pro omezení zpracování.

Nutno však zdůraznit, že ztráta několika jednotlivců z většího sledovaného celku, která pouze ovlivňuje statistickou sílu výsledků, ne však povahu objevu, nebo validitu výsledků neznamená zmaření celého výzkumu. Tam kde smazání údajů o jednom výzkumném subjektu v zásadní míře neovlivní výsledek celého statistického měření se o danou výjimku nelze opírat.

Stejně jako u o omezení práva na přístup, i v tomto případě rozhoduje o uplatnění výjimky správce osobního údaje na své riziko. Subjekt údajů se následně může obrátit na ÚOOÚ se stížností.

4.6. Právo na přenositelnost údajů

Relevantní ustanovení: Čl. 20 GDPR

Právo na přenositelnost osobních údajů je jedna z novinek, jež s GDPR přichází. Díky jeho novosti a úzce nastaveným podmínkám pro použití se právu na přenositelnost v GDPR nevěnuje mnoho prostoru a český ZZOÚ jej upravuje jen okrajově. Ve své podstatě se jedná o rozšíření práva na přístup, jelikož umožňuje při splnění dvou níže uvedených podmínek zpřístupnit subjektem poskytnuté osobní údaje ve strukturovaném, běžně používaném, strojově čitelném a interoperabilním formátu třetí osobě, dle výběru subjektu. To má za cíl zvýšit kontrolu subjektu nad jeho automatizovaně zpracovanými údaji, které může snadněji přenést k jinému správci.

V praxi se výkon práva na přenositelnost uskuteční tak, že správce, který je požádán o přenesení údajů subjektem vytvoří kopii těchto údajů a ve výše definovaném formátu ji poskytne požadované osobě, rozdílné od subjektu údajů. To však neznamená, že musí takto přenesené údaje u sebe vymazat či omezit jejich zpracování. Naopak jeho nakládání s danými osobními údaji není uplatněním práva na přenositelnost dotčeno.

Podmínkou uplatnění práva na přenositelnost je:

1. automatizované zpracování údajů správcem,
2. založené na souhlasu nebo plnění smlouvy.

Pokud zpracování nesplňuje obě tyto podmínky kumulativně, právo na přenositelnost se nedá uplatnit.

Výzkumná instituce může žádost o přenositelnost odmítnout, pokud data získala na základě jiného právního titulu než souhlasu subjektů, nebo data nejsou uloženy v digitální podobě. Výjimkou je i zpracování prováděné ve veřejném zájmu, nebo ochrana práv jiných osob. I zde musí být uplatněn test proporcionality a není možné veškeré žádosti zamítat jen s odkazem na veřejnou prospěšnost výzkumu. Žádosti o přenos osobních údajů tak musí být vyhověno v případě, že přenos osobních údajů úkoly ve veřejném zájmu neohrozí.

V případě, že by toto právo bylo uplatněno, je žádoucí data předat ve formátu definovaném vhodným *otevřeným standardem*, tedy jehož specifikace je volně dostupná kterémukoli příjemci dat (příklady dat jsou např. XML, JSON, RDF, JSON-LD, … a veřejně publikovaným schématem). Otevřený formát dat neimplikuje, že by samotná data měla být otevřená (tj. bez šifrování) – pouze že samotný formát dat je zdokumentovaný a je k dispozici komukoli.

4.7. Právo nebýt předmětem automatizovaného rozhodování

Relevantní ustanovení: Čl. 22 GDPR

Právo nebýt předmětem žádného rozhodnutí založeném výhradně na automatizovaném zpracování včetně profilování je moderní právo, související s technologickým vývojem. Jeho účelem je zaručit subjektu údajů spravedlivý a nediskriminační přístup, založený na zohlednění všech relevantních okolností, a nikoliv pouze strojové rozhodnutí založeném na algoritmickém zpracování dat. S ohledem na skutečnost, že ve výzkumné

praxi vůbec nedochází k rozhodování o právech či povinnostech subjektů, je obtížné si představit situaci, kde by automatizované rozhodnutí mohlo nějak ovlivnit další osud subjektu. Z těchto důvodů se nebudeme právem nebýt předmětem automatizovaného rozhodnutí hlouběji zabývat.

5. Výjimky z GDPR pro vědecký výzkum

5.1. Obecné pojednání k fungování výjimek

Obecné nařízení explicitně reflektuje problematiku zpracování dat ve vědě a výzkumu, a to formou dvou specifických kategorií výjimek. Obě tyto kategorie jsou účelově definovány, tj. výjimky z ochrany osobních údajů se vážou na prokazatelný účel jejich zpracování. Tím je u první kategorie výjimek „účel vědeckého výzkumu," u druhé kategorie pak se jedná o „účel akademického projevu."

GDPR není v tomto ohledu zcela jednotné co do terminologie, neboť preambule též na dvou místech hovoří ještě o „vědeckých účelech" (nikoli tedy pouze o „účelech vědeckého výzkumu"). Normativní text však již pracuje pouze se shora zmíněnou explicitní teleologickou dichotomií účelů vědeckého výzkumu[1] a akademického projevu.[2]

Obě kategorie výjimek mají zcela odlišný regulatorní základ a zásadně se liší též konstrukce jejich normativní úpravy. Základem výjimek za účelem vědeckého výzkumu je v obecné rovině svoboda vědeckého bádání. Smyslem těchto výjimek je usnadnit vědeckou činnost, to však samozřejmě za současného respektování oprávněných zájmů subjektů údajů.

Výjimky za účelem vědeckého výzkumu jsou v obecném nařízení konstruovány relativně konkrétně a jejich rozsah je pro členské státy

[1] Srov. čl. 5(1)(b), 5(1)(e), 9(2)(j), 14(5)(b), 17(3)(d) nebo 21(6).

[2] Viz čl. 85.

z hmotněprávního hlediska jednotný. Členské státy tedy sice mohou vlastními právními předpisy upravovat konkrétní povinnosti správců např. při zabezpečení vědeckých dat, ale nemohou národními právními úpravami zasahovat do rozsahu toho, co se ve smyslu nařízení považuje za zpracování dat pro účely vědeckého výzkumu.

GDPR tím pádem nereflektuje vzájemné rozdíly mezi členskými státy co do rozsahu svobody vědeckého bádání. Některé členské státy totiž za různými účely (veřejný pořádek, veřejné zdraví apod.) omezují v některých oborech svobodu vědeckého bádání, typicky např. v oblasti genetiky. Zatímco se však rozsah svobody vědeckého bádání může mezi jednotlivými členskými státy odlišovat, rozsah výjimek z ochrany osobních údajů se neliší. To samozřejmě neznamená legalizaci výzkumu, který by byl prováděn v rozporu s národním právním řádem členského státu – důsledkem jednoty výjimek v GDPR je pouze nepostižitelnost správce nebo zpracovatele příslušných dat z důvodu nenaplnění definice účelu vědeckého výzkumu tam, kde příslušný členský stát takový účel za vědecký neuznává.

Příkladem dopadu jednotného věcného rozsahu výjimek za účelem vědeckého výzkumu je situace, kdy si výzkumný tým ukládá data na datové úložiště spravované poskytovatelem služby informační společnosti usazeném ve členském státě, v němž je provádění příslušného výzkumu protiprávní. Jednotný rozsah výjimek v tomto případě zajišťuje, že poskytovatel služby informační společnosti nebude na základě ochrany osobních údajů postižitelný místním dozorovým orgánem za to, že zpracovává mimo zákonný účel data, která příslušný členský stát kvůli své vnitrostátní úpravě nepovažuje za zdroje nebo výsledky vědeckého výzkumu.

Rozsah pojmu zpracování za účelem vědeckého výzkumu je každopádně třeba vykládat extenzivně. K takové interpretaci ostatně přímo vybízí i preambule obecného nařízení mj. v odst. 159.[3] Otázkou samozřejmě je,

[3] (159) preambule GDPR: „Pro účely tohoto nařízení by zpracování osobních údajů pro účely vědeckého výzkumu mělo být chápáno v širokém smyslu a zahrnovat například technologický vývoj a technologické demonstrace, základní výzkum, aplikovaný vý-

jak bude takto extenzivní přístup uplatňován dozorovými orgány při reálných kontrolách. Pojem účelu vědeckého výzkumu totiž nedává ani v náznaku vodítka vzhledem k tomu, zda má být chápán materiálně (tj. vzhledem ke kvalitě dat), institucionálně (tj. vzhledem ke kvalitě instituce) nebo třeba procesně (tj. vzhledem k typu procesu zpracování dat). Můžeme v tomto směru opatrně spekulovat, že základem pro pragmatické uchopení účelu vědeckého výzkumu bude zřejmě institucionální hledisko v kombinaci s hlediskem procesním. U subjektů, které lze označit jako výzkumné instituce (tj. výzkumné univerzity, ústavy Akademie věd apod.), tedy bude zřejmě možno pracovat u dat zpracovávaných při jejich hlavní činnosti (tj. nikoli při např. organizačních činnostech) s presumpcí zpracování dat za účelem vědeckého výzkumu. Výzkumné organizaci by tedy mělo k prokázání hypotézy účelu vědeckého výzkumu ve smyslu GDPR postačovat, pokud prokáže, že příslušná data byla zpracovávána v rámci činnosti této organizace. V případě ostatních subjektů lze naopak očekávat, že bude dozorový orgán požadovat konkrétní pozitivní důkaz skutečnosti, že předmětná data byla zpracovávána za účelem vědeckého výzkumu.

Zvláštní kategorií účelu v rámci zpracování dat za účelem vědeckého výzkumu pak je zpracování dat za účelem vědeckého výzkumu prováděného ve veřejném zájmu. Tento partikulární účel se objevuje v textu obecného nařízení v souvislosti s omezením práva na námitku. Výzkum ve veřejném zájmu v tomto případě přímo vylučuje právo na námitku, což významným způsobem omezuje subjekt údajů v možnosti protestovat proti zpracování osobních údajů správcem nebo zpracovatelem.

Zavedení kategorie veřejného zájmu v tomto případě samozřejmě neznamená, že by měl správce zpracovávající osobní údaje za účelem vědeckého výzkumu ve vztahu k subjektu údajů oslabené postavení. Při zpracování pro účely vědeckého výzkumu nikoli ve veřejném zájmu se

zkum a výzkum financovaný ze soukromých zdrojů. Kromě toho by mělo zohledňovat cíl Unie podle čl. 179 odst. 1 Smlouvy o fungování EU, jímž je vytvoření evropského výzkumného prostoru. K účelům vědeckého výzkumu by rovněž měly patřit studie prováděné ve veřejném zájmu v oblasti veřejného zdraví."

pouze uplatní standardní procedura, kdy bude muset příslušný správce proti námitce posoudit, zda má ke zpracování osobních údajů „závažné oprávněné důvody." Naproti tomu správce, který data zpracovává za účelem vědeckého výzkumu ve veřejném zájmu žádné podobné posouzení nemusí provádět a námitku může en bloc odmítnout.

Vzhledem k tomu, že ani v tomto případě neexistuje interpretační vodítko, můžeme o adekvátním rozsahu pojmu veřejného zájmu pouze spekulovat. Je evidentní, že tímto zájmem může být zájem členského státu nebo i zájem Unie. Podobně jako u shora diskutované kvalifikace účelu zpracování se však i zde nabízí otázka, jaké hledisko bude při posuzování veřejného zájmu dominantní či relevantní.

Nabízela by se sice analogie se shora diskutovanou extenzivní interpretací účelu vědeckého výzkumu. V tomto případě ale přílišné interpretační extenzi brání jednak absence explicitního interpretačního vodítka v preambuli a jednak skutečnost, že kvalifikace veřejného zájmu zde en bloc vylučuje velmi významné právo subjektu údajů.

Z tohoto důvodu a také z důvodu užití konstrukce „pro splnění úkolu prováděného z důvodů veřejného zájmu" považujeme za nepravděpodobné, že by při hodnocení veřejného zájmu mohlo být postupováno jako ve shora diskutovaném případě institucionálně, tj. předjímat veřejný zájem na základě skutečnosti, že zpracování provádí např. veřejná vysoká škola. Namísto toho bude třeba proti námitce konstatovat jako účel zpracování konkrétní „úkol" a argumentovat veřejný zájem na jeho splnění.

Z procesních charakteristik použitelných k prokázání veřejného zájmu bude zřejmě možno aplikovat především užití veřejných prostředků – ty totiž vzhledem k požadavkům na finanční kontrolu nelze užít jinak než pro veřejný zájem. Současně lze z dikce obecného nařízení usuzovat, že nebude nutno prokazovat dokonalý nebo převažující veřejný zájem, ale že postačí, pokud bude veřejný zájem i jen jedním z aspektů příslušného „úkolu," k jehož splnění je zpracování dat za účelem vědeckého výzkumu nezbytné. Tím pádem by mělo být možno konstatovat veřejný zájem

například v případě vědeckých projektů kofinancovaných z veřejných rozpočtů.

Konkrétní kvalifikaci veřejného zájmu každopádně považujeme za vysoce problematickou otázku. V hraničních případech je tedy z pohledu výzkumné instituce bezpečnější, pokud bude proti námitce argumentovat závažnými oprávněnými důvody ke zpracování osobních údajů spíše, než aby námitku odmítla s poukazem na veřejný zájem.

Na rozdíl od výjimek za účelem vědeckého výzkumu vycházejí výjimky za účelem akademického projevu z práva na svobodu projevu. Toto právo je z politického hlediska poměrně citlivé a v konkrétních svých aspektech vykazuje jeho ochrana v různých členských státech poměrně podstatné odchylky. Legální projev v jednom členském státě tedy může být v konkrétním případě dokonce v jiném členském státě postižen trestněprávní sankcí.

GDPR tuto skutečnost reflektuje, když dává členským státům možnost a povinnost upravit rozsah těchto výjimek nejen z práv subjektů údajů, ale též např. z kontrolních pravomocí dozorových úřadů. Základním obecným parametrem pro tyto výjimky je nezbytnost k zachování standardu ochrany svobody projevu v příslušném členském státě.

Vzhledem k tomu, že Česká republika doposud nesplnila svoji povinnost upravit si výjimky za účelem ochrany svobody projevu (včetně akademického projevu) vnitrostátním právem a že se tyto výjimky již u nás staly předmětem zjitřené politické debaty, můžeme jejich výhledovou podobu pouze odhadovat. Z dosavadních náznaků považujeme za pravděpodobné, že budou u nás tyto výjimky definovány velmi široce. Jejich aplikace však bude muset být vzhledem k dikci nařízení každopádně omezena na případy, kdy je jejich uplatnění nezbytné k realizaci svobody projevu. Podmínkou nastoupení těchto výjimek tedy jednak bude přímá příčinná souvislost mezi zpracováním osobních údajů a veřejným projevem. Kromě toho bude možno se jich dovolávat pouze v době, kdy bude svoboda projevu skutečně realizována a nebudou tedy např. krýt zpracování zdrojových dat pro již vydaný vědecký text.

Z výše uvedeného plyne, že při běžném zpracování osobních údajů ve vědě a výzkumu bude zřejmě správce v praxi spoléhat především na výjimky za účelem vědeckého výzkumu. Otázka po tom, zda se dovolávat jedné nebo druhé kategorie výjimek, které se věcně mohou překrývat (vědecká činnost totiž samozřejmě často směřuje k publikacím), bude mít zpravidla pragmatické řešení. Vědec nebo vědecká instituce bránící své právo zpracovávat osobní údaje může v takovém případě extrapolovat svoji argumentaci do úrovně ústavního práva a vybrat výjimku podle toho, jakého svého ústavním pořádkem zaručeného práva by se dovolávali u Ústavního soudu nebo Evropského soudu pro lidská práva. V případech, kdy by vědec v řízení před Ústavním soudem bránil své právo zpracovávat osobní údaje poukazem na svobodu vědeckého bádání, je na místě použít výjimku pro účely vědeckého výzkumu. Naopak v případě, kdy by vědec argumentoval svobodou projevu, je i v úrovní zákonného práva na místě užití výjimky za účelem akademického projevu.

5.2. Shrnutí výjimek pro vědecké účely u jednotlivých práv

Výzkumné instituce se mohou při výzkumu spolehnout na několik výjimek, kdy ve veřejném zájmu nebo s odvoláním na výzkumné účely nemusí respektovat obecné pravidlo. Možné výjimky z jednotlivých práv subjektu jsou shrnuty v tabulce níže. O aplikaci jednotlivých výjimek je podrobně pojednáno v dalším výkladu o konkrétních právech subjektu v kapitole č. 3.

Právo subjektu osobních údajů, z něhož může subjekt uplatnit výjimku
Typ výjimky

Právo na informace o zpracování osobních údajů - čl. 13, 14
Plnění informačních povinností dle čl. 13 a 14 nelze na rozdíl od čl. 15, 16, 18 a 21 omezit u zpracování pro vědecké účely evropským ani

národním zákonným právem. Subjekt údajů má tedy právo na informace bez omezení. Jedinou výjimkou jsou případy, kdy nejsou údaje získány od subjektu údajů a bylo by neúměrně složité subjekt údajů informovat. K tomu dochází např. tehdy, pokud subjekt nelze ztotožnit, nebo je extrémně složité příslušné údaje zpracovat, typicky v důsledku aplikace technologií na ochranu soukromí.

V praxi se tak toto performativní právo může plnit prostřednictvím webových stránek, kde budou uvedeny nařízením požadované informace s ohledem na zdroj získání osobních údajů. V budoucnu pak lze předpokládat užití standardizovaných ikon (pokud vzniknou a budou standardizovány).

Právo na přístup – čl. 15 Právo na přístup je možné při zpracování výzkumných údajů omezit dvěma způsoby. První výjimka, která se pravděpodobně bude častěji využívat, umožňuje omezit, odložit anebo dokonce úplně vyloučit právo na přístup, v případě, že oprávněné zájmy správce převáží nad zájmy nebo základními právy subjektu údajů. Při posuzování proporcionality práv musí správce přihlédnout zejména k přiměřenému očekávání subjektu údajů vzhledem ke vztahu se správcem osobních údajů.

Druhá výjimka dle § 18 odst. 3 umožňuje vynětí z práva na přístup pouze po dobu potřebnou k dosažení účelu v případech, kdy by zveřejněním nebo také realizací práva na přístup došlo ke zmaření účelu jejího zpracování. Jedná se tedy o dočasnou ochranu zdroje osobních údajů.

Právo na opravu – čl. 16 Existuje obecná povinnost zpracovávat data správná a aktuální, byť se nicméně odhaduje, že podněty k opravě výzkumných dat nebudou časté. Z tohoto důvodu český zákonodárce nevyužil zmocnění ke stanovení zákonné výjimky a nezakotvil ji do českého zákona. Právo na opravu se tedy může teoreticky uplatňovat při zpracování výzkumných údajů v plném rozsahu.

Právo na výmaz – čl. 17 Právo na výmaz je při zpracování výzkumných údajů omezeno nejvíce. Omezení tohoto práva českým zákonem není nutné, jelikož je obsažené již přímo v samotném článku 17 GDPR. Pokud vědecký výzkum probíhá ve veřejném zájmu a je pravděpodobné, že by uplatnění práva na výmaz znemožnilo, nebo vážně ohrozilo splnění cílů takového zpracování, pak se právo na výmaz neuplatní.

Právo na omezení zpracování – čl. 18 Jelikož je právo na omezení zpracování způsobilé ve svém plném rozsahu vážně narušit výkon zpracování výzkumných dat, využil český zákonodárce zmocnění k výjimkám v § 17 ZZOÚ. To zužuje toto právo při zpracování výzkumných dat pouze na případy, kdy správce již nepotřebuje osobní údaje pro původní účel a zároveň je subjekt údajů požaduje pro výkon, určení nebo uplatnění právních nároků. V ostatních případech než v tomto výše uvedeném případě tedy nelze úspěšně žádat omezení zpracování výzkumných údajů.

Oznamovací povinnost při opravě, omezení, nebo výmazu – čl. 19 Oznamovací povinnost vůči všem příjemcům, kterým byly osobní údaje zpřístupněny, probíhá vždy s výjimkou případů, kdy se to ukáže jako nemožné, nebo pokud by to pro správce znamenalo nepřiměřené úsilí. Oznámení je možné také pouhou změnou údaje v evidenci, pokud správce provozuje evidenci, která je příjemcům pravidelně zpřístupňována. Při zpracování výzkumných údajů se nabízí ještě jedna alternativa splnění této povinnosti, a sice uvedením údaje o verzi datové sady (která musí být s každou změnou inkrementována), případně o okamžiku poslední aktualizace obsahu, pokud je zpracování prováděno způsobem umožňujícím dálkový přístup.

Právo na přenositelnost – čl. 20 Právo na přenositelnost se vztahuje pouze na automatizovaně zpracovávané osobní údaje, u nichž je právním základem souhlas či plnění smlouvy. Výjimka pro vědu a výzkum

není zakotvena, lze se dovolat obecné výjimky ochrany práv třetích stran.

Právo vznést námitku – čl. 21 Právo vznést námitku je jedním z práv, které mají výjimku pro výzkumné údaje zakotvenou přímo ve svém definičním článku v GDPR. Ten stanoví možnost námitku odmítnout, pokud je namítané zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu. Druhou výjimku přidal ovšem i český zákonodárce, který stanovil, že po podání námitky správce nezpracovává osobní údaje pouze tehdy, když subjekt uplatní námitku proti zveřejnění konkrétních osobních údajů a zároveň prokáže, že jeho zájem na ochraně práv převažuje nad zájmem na zveřejnění těchto osobních údajů.

To v praxi znamená, že při podání námitky subjektu údajů proti konkrétnímu zpracování v režimu zpracování pro účely vědy a výzkumu se dle českého ZZOÚ může apriori pokračovat ve zpracování, dokud subjekt údajů neprokáže, že v konkrétním případě převažuje jeho oprávněný zájem na ochraně jeho práv a svobod. Pokud by toto subjekt prokázal, pak musí správce konkrétně vymezené osobní údaje přestat zpracovávat, ledaže sám prokáže, že je zpracování nezbytné pro splnění úkolu prováděného z důvodu veřejného zájmu.

Právo nebýt předmětem automatizovaného rozhodování– čl. 22 Výjimka pro zpracování za účelem vědy a výzkumu není pro toto právo stanovena čl. 89 a nevyskytuje se ani v jiné podobě. Důvodem je zřejmě povaha tohoto práva, spočívající v pasivním oprávnění subjektu a z toho plynoucí preventivní povinnosti pro správce upravit své procesy zpracování v souladu s tímto právem. Naplnění požadavků tohoto práva tak není natolik problematické vzhledem k možnosti řešit jeho požadavky výlučně předem, systematicky, a nikoliv reaktivně a individuálně.

6. Procesní postup správce při uplatnění práva subjektů údajů

6.1. Zajištění transparentnosti a postup při žádosti o informace

Relevantní ustanovení: Čl. 12, 89 GDPR a § 16 - 21 ZZOÚ

GDPR v obecné rovině nařizuje správcům přijmout taková opatření, aby v co největší míře usnadňoval subjektům údajů výkon jejich práv popsaných v předchozí kapitole. V čl. 12 GDPR jsou uvedeny obecná pravidla, zásady a postupy pro jejich vyřizování. Zákonodárce požaduje stručná, transparentní a snadno přístupná řešení za použití jasných a jednoduchých jazykových prostředků, a to zejména pokud se jedná o informace určené dětem.

Reakce či výstup se poskytuje elektronicky, pokud byla tímto způsobem uplatněna i příslušná žádost. Pokud nikoliv, pak písemně nebo jinými vhodnými prostředky. Pokud si to subjekt údajů vyžádá, je možné sdělit informace i ústně za předpokladu, že bude totožnost subjektu údajů dostatečně prokázána.

Žádosti je nutné vyřizovat bez zbytečného odkladu, nejpozději však do jednoho měsíce od obdržení žádosti. Pokud se bude jednat nárazově o vysoký počet žádostí, nebo o velmi složité žádosti, je možné lhůtu přiměřeně prodloužit až o dva další měsíce. Nejzazší termín vyřízení tedy musí být bezpodmínečně 3 měsíce od podání žádosti. O takovém

prodloužení je však nutné subjekt údajů vždy informovat v původní lhůtě a vysvětlit důvody takového prodloužení.

Pokud by správce nepřijal opatření, o něž subjekt oprávněně žádal, informuje správce bezodkladně subjekt údajů též nejpozději do jednoho měsíce o důvodech takového odmítnutí. Zároveň jej také poučí o možnosti podat stížnost u dozorového úřadu.

Veškeré úkony související s uplatněním práv z GDPR (viz níže) musí být činěny bezplatně. Možnost účtovat si za vyřízení žádosti peníze je možné pouze pokud jsou žádosti subjektu zjevně nedůvodné či nepřiměřené, zejména proto že se opakují. V takovém případě může správce požadovat poplatek dle svých administrativních nákladů, nebo také odmítnout žádosti vyhovět. Přičemž je třeba pamatovat na to, že nedůvodnost žádosti je povinný doložit správce.

Správce by měl postupovat velmi obezřetně a mít vždy zdravé pochybnosti o totožnosti fyzické osoby, která podává žádost a zabezpečit důvěrnost přenášených informací. Na písemné žádosti reagovat přinejmenším doporučeným dopisem, u elektronických žádosti je na místě vyžadovat elektronický podpis, nebo požadovat, ať se žadatel dostaví osobně. V případě, že subjekt není při elektronické komunikaci nebo osobní komunikaci schopen prokázat svoji totožnost, nemusí správce žádosti vyhovět.

Zpracování dat za účelem vědy a výzkumu požívá vzhledem k vysoké míře veřejného zájmu na jeho trvání výjimky z řady povinností uvedených buď přímo u konkrétního práva, nebo v národní zákonné úpravě v případě, že k tomu dostal národní zákonodárce zmocnění v článku 89 GDPR. Ten nejprve stanoví vhodné záruky, za jakých by měl zmírněný režim výzkumných údajů probíhat a dále umožní národnímu zákonodárci stanovit odchylky od práva na přístup, opravu, omezení zpracování a práva na námitku.

Vhodné záruky jsou pro zpracování výzkumných dat stanoveny obecně, aby si každý správce a zpracovatel výzkumných údajů nastavil opatření individuálně, a tedy úměrně ke své situaci. Výslovně je ovšem zmíněna

zásada minimalizace údajů a pseudonymizace dat, jako základní opatření, která by měla být zavedena a k nímž by mělo být přihlíženo v každém případě. Taktéž pokud by bylo možné ve vědeckém výzkumu pokračovat způsobem, který by nevyžadoval identifikaci osob při splnění sledovaných účelů, pak musí být tyto účely splněny tímto způsobem. Zákonodárce se tak snaží omezit zpracování osobních údajů pro vědecké účely tam, kde není identifikace nutná, čímž by se výzkum dostal z režimu ochrany osobních údajů a GDPR.

6.2. Právo vznést námitku

Relevantní ustanovení: Čl. 21 GDPR a § 21 ZZOÚ

Právo vznést námitku proti zpracování osobních údajů umožňuje subjektu údajů vyžádat si přezkum oprávněnosti zpracování osobních údajů v jeho konkrétní situaci, pokud:

- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce, či třetí strany nebo;
- zpracování probíhá za účelem přímého marketingu (včetně profilování pro účely přímého marketingu).

Námitka v režimu přímého marketingu má speciální povahu, jež spočívá v tom, že pouhé její uplatnění automaticky znamená ukončení zpracování pro účel přímého marketingu. Přímý marketing ovšem není relevantní z hlediska vědy a výzkumu, a tedy budeme nadále pojednávat pouze o prvních dvou výše zmíněných případech.

O právu na vznesení námitky musí být subjekt údajů výslovně upozorněn, a to zřetelným způsobem, odděleně od jakýchkoliv jiných informací, nejpozději v okamžiku první komunikace se subjektem údajů. Právo

vznést námitku se tedy promítá i do informační povinnosti správce. Pokud se zpracování uskutečňuje pomocí služby informačních společností, může subjekt údajů.

V případě, že při vznesení námitky dojde k omezení zpracování, jakožto k provizornímu opatření, než se rozhodne, zda je možné ve zpracování pokračovat či nikoliv. A tedy podání jakékoliv námitky, byť by se nakonec ukázala jako neoprávněná, má za následek omezení zpracování a další důsledky dle čl. 18 GDPR.

V posledním odstavci čl. 21 je zakotvena výjimka pro zpracování osobních údajů pro účely vědeckého výzkumu, která umožňuje odmítnout námitku, pokud je namítané zpracování nezbytné pro splnění úkolu prováděného z důvodů veřejného zájmu. Další výjimku přidal tentokrát český zákonodárce do § 21 ZZOÚ. Tato druhá výjimka pak odstraňuje provizorní omezení zpracování při podání námitky a částečně otáčí důkazní břemeno u případů, spadajících do Dílu 2, Hlavy II., mezi které patří i zpracování za účely vědy a výzkumu. To znamená, že po podání námitky subjektem správce nezpracovává osobní údaje jen pokud subjekt:

1. konkrétně označí, jaké osobní údaje namítá;
2. námitka směřuje proti jejich zveřejnění;
3. subjekt osvědčí, že jeho zájem na ochranu jeho práv převažuje nad zájmem na zveřejnění osobních údajů.

To v praxi znamená, že při podání námitky subjektu údajů proti konkrétnímu zpracování v režimu zpracování pro účely vědy a výzkumu se dle českého ZZOÚ může apriori pokračovat ve zpracování, dokud subjekt údajů neprokáže, že v konkrétním případě převažuje jeho oprávněný zájem na ochraně jeho práv a svobod. Pokud by toto subjekt prokázal pak, musí správce tyto konkrétně vymezené osobní údaje přestat zpracovávat, ledaže sám prokáže, že je zpracování nezbytné pro splnění úkolu prováděného z důvodu veřejného zájmu. Zpracování osobních údajů za účelem vědy a výzkumu ve veřejném zájmu je tedy absolutní důvod,

který vylučuje úspěch při podání námitky proti zpracování. V případě výzkumu v soukromém zájmu se však lze námitce také vyhnout, pokud převáží oprávněné důvody pro zpracování nad zájmy a svobodami subjektu údajů. Zpracování osobních údajů za účelem vědy a výzkumu však v každém případě disponuje provizorní ochranou proti omezení zpracování postihující běžné uplatnění práva na námitku, spočívající v otočení důkazního břemene, dle § 21 ZZOÚ.

6.3. Oznamovací povinnost při opravě, výmazu nebo omezení zpracování osobních údajů

Relevantní ustanovení: Čl. 19 a 16, 17, 18 GDPR a § 9, 20 ZZOÚ

Oznamovací povinnost správce při provedení opravy, výmazu, nebo omezení zpracování osobních údajů odpovídá právu subjektu údajů být informován o těch skutečnostech, jež se dotýkají zpracování jeho osobních údajů. Touto formou je tak garantována potřebná komunikace mezi správcem a subjektem tak, aby se relevantní informace a reakce správce na uplatněná práva spolehlivě dostala zpět k subjektu údajů.

Oznamovací povinnosti podléhá provedení:

- opravy osobních údajů,
- výmazu osobních údajů,
- omezení zpracování osobních údajů.

Kromě těchto obecných povinností však identifikujeme i některé jiné dílčí informační povinnosti dané v konkrétních situacích, jako je např. upozornění, že bude zrušeno omezení zpracování (čl. 18 odst. 3). Tyto dílčí informační doplňky plní obdobnou funkci jako oznamovací povinnost, ale jejich provedení není předmětem širší úpravy a pod oznamovací povinnost se obecně nepodřazují.

Obecné informování probíhá vůči všem jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny s výjimkou případů, kdy se to ukáže jako nemožné, nebo pokud by to pro správce znamenalo nepřiměřené úsilí. Takové oznámení je ovšem značně usnadněno těm, kteří provozují evidenci, která je příjemcům pravidelně zpřístupňována. V takovém případě lze totiž oznamovací povinnosti učinit za dost pouhou změnou osobních údajů v této evidenci. Tato možnost není povinná, ale zejména u situací, kdy správce poskytuje příjemci přístup k databázi, a tedy změna zdrojové databáze povede k žádoucím úpravám i u příjemce, se tento způsob jeví jako vhodný pro správce i pro subjekt údajů.

Pozice výzkumných organizací je v tomto ohledu zvýhodněna ještě více. Existuje totiž speciální výjimka pro zpracování osobních údajů za vědeckými a jinými účely ve veřejném zájmu, pokud jsou uskutečňovány způsobem umožňujícím dálkový přístup. V takovém případě je totiž možné splnit oznamovací povinnost uvedením údaje o okamžiku poslední aktualizace obsahu, v němž jsou nebo byly osobní údaje uvedeny. Samotný fakt, že je změněný údaj přístupný, totiž subjektu údajů umožní zjistit, zda mu bylo vyhověno, a to především díky informaci o datu poslední aktualizace. Požadavek na sdílení informace o uskutečnění opravy či výmazu s dalšími subjekty, kterým správce osobní údaje předal ovšem zůstává zachován i pro výzkumné instituce.

7. Vymahatelnost práv subjektů údajů v případě pochybení správce či zpracovatele

Jednou z podstatných změn, které GDPR přináší do našeho právního řádu je přímá vymahatelnost práv, která jsou subjektům údajů přiznávána. Subjekty údajů již nemusí spoléhat na dozorový Úřad pro ochranu osobních údajů (dále jen „úřad"), aby vyřídil jejich podnět, ale mohou svá práva realizovat osobně přímo vůči příslušným správcům a zpracovatelům. Od této právní úpravy lze očekávat zvýšení souladu law in books a law in action. Doposud totiž úřad nebyl důsledný při vymáhání právní úpravy ochrany osobních údajů, a ne vždy dbal výkladu pracovní skupiny WP 29, nebo jiných těles zabývajících se problematikou ochrany osobních údajů. Nezřídka se tedy stávalo, že úřad zaujal stanovisko, které ignorovalo publikovaný výklad WP 29, sporně jej aplikoval či dokonce byl v jeho přímém rozporu (např. souhlas s cookies prostřednictvím nastavení prohlížeče).[1] Tato praxe úřadu ve spojení s nízkou výší ukládaných pokut, vedla k minorizaci této právní agendy a k prohlubování nesouladu mezí právní teorií a běžnou praxí v České republice před GDPR.

Poskytnutím možnosti subjektu údajů domáhat se svých nároků přímo, se zvýšila pravděpodobnost argumentace relevantními výklady WP 29 před soudem. Subjekty údajů tak ve svém zájmu způsobí častější

[1] Srov. Doporučení k zpracování cookies a obdobných prostředků sledování od 25. května 2018, [online]. [vid. 14. červenec 2018], Získáno z: https://www.uoou.cz/cookies-a-nbsp-gdpr/d-29966

promítání právní teorie do rozhodovací praxe. Poskytnutím této zbraně subjektům údajů tak evropský orgán sám získává na relevanci. Při aplikaci právní zásady „Vigilantibus iura“[2] se budou jeho vyjádření spíše objevovat v argumentaci stran a bude s jeho příslušnými vyjádřeními pracováno alespoň jednou ze stran. Tímto způsobem budou eliminovány situace, kdy by jeho vyjádření nebylo uplatněno záměrně. Subjekty údajů totiž ve svém sporu budou ve svém vlastním zájmu vyhledávat veškeré zmínky o relevantních právních institutech a teoretických pojednáních, jež budou svědčit v jejich prospěch.

Je si třeba také uvědomit, že skrze jednotnou právní úpravu bez zásadních národních odchylek již bude ve velké míře použitelná také soudní judikatura jiných členských států. Nebude tak již teoreticky možná deviace jednoho úřadu členského státu při výkladu těch stejných právních norem. Subjekty údajů by totiž v případném soudním sporu mohly argumentovat judikaturou z ostatních členských států a sami ve svém zájmu tak pomoci sjednotit také právní praxi napříč členskými státy. Právní teorií přiznávaný výklad tak již nebude čistě akademický, ale dá se očekávat, že strany soudního sporu jím budou argumentovat při uplatňování svých práv, a tedy bude tímto způsobem možné je lépe promítnout do praxe.

Doposud mohly subjekty údajů podávat v členských zemích přímo správci pouze námitky, pokud nesouhlasily s některými formami zpracování. Pokud ovšem správce i po podání námitky ignoroval toto nebo i jiná práva subjektu údajů, vyplývající z právní úpravy ochrany osobních údajů, nezbývalo subjektu než svoji záležitost nahlásit na úřad a vyčkat, jak jeho podnět úřad posoudí a zda bude správce následně efektivně donucen k nápravě. I tato nemožnost přímé vymahatelnosti práv ochrany osobních údajů, kdy by se subjekt mohl sám bránil před soudem, přispěla k nedodržování práv ochrany osobních údajů.

[2] *Vigilantibus iura scripta sunt* (zkráceně *vigilantibus iura*) je klasická římskoprávní zásada, která říká že práva patří bdělým. Neboli, že právo přeje bdělým, nechť si tedy každý střeží svá práva.

Dnes však subjekty údajů mají možností mnohem více. Konkrétně mohou:

1. Obrátit se na správce
2. Obrátit se na zpracovatele
3. Obrátit se na úřad
4. Obrátit se na soud
    a) Civilní žalobou o soukromoprávním nároku
    b) Trestním podáním
    c) Zásahovou žalobou
    d) Žalobou proti rozhodnutí správního orgánu
    e) Žalobou proti nečinnost správního orgánu
    f) Žalobou podle části V. Občanský soudní řád (OSŘ)

7.1. Postup správce a zpracovatele při vyřizování stížností

Subjekt, který je příslušný k vyřizování žádostí subjektů údajů, je primárně správce osobních údajů. Správce je odpovědným subjektem, který určuje účel a zákonný důvod zpracování. Je tedy logické, že bude tím prvním, na koho by se měl subjekt údajů obrátit při uplatňování svých práv podle GDPR. Až při potížích v bezprostřední komunikaci, nebo v uplatňování práv se správcem přichází v úvahu použití jiné cesty k dosažení zákonných práv subjektu údajů. Správce totiž může nebo nemusí vyhovět individuálním žádostem subjektu, které budou nejčastěji zahrnovat uplatnění práv na přístup, informace, omezení zpracování nebo i na výmaz. Samotnou formu realizace těchto práv a možná omezení, kdy může správce odmítnout vyhovět subjektu údajů

definuje čl. 12 GDPR, o kterém je pojednáno v kap. 6. Tuto agendu budou mít na starosti typicky pověřenci DPO, nebo jiné pověřené osoby u subjektů jež tuto pozici nezavedou.

Pokud by se subjekt údajů obrátil na zpracovatele, pak záleží na konkrétních smluvních ujednáních, ale zpravidla bývá proces podobný, pouze s tím rozdílem, že zpracovatel předá tuto žádost správci k vyřízení v předem definované lhůtě, aby ten měl dostatek času na ni včas a kvalitně odpovědět. Tyto situace jsou ovšem běžně upraveny dispozitivně ve smlouvách či dodatcích o zpracování osobních údajů mezi správcem a zpracovatelem, a proto je nelze paušalizovat.

7.2. Úřad pro ochranu osobních údajů

Ke třetí cestě, jakou se může subjekt vydat, zpravidla dochází až po absolvování jedné z dvojice výše zmíněných. Je totiž kýžené, aby si subjekty údajů a správci jejich osobních údajů vyřešili své záležitosti mezi sebou a neangažovali úřad či dokonce soud, pokud to není nutné. Podat podnět k úřadu je na místě až u případů, kdy subjekt není schopen se svých práv domoci sám, nebo pokud potřebuje odbornou konzultaci. Úřad provádí náhodné kontroly dodržování ochrany osobních údajů, podle vlastního Kontrolního plánu ex offo. Velkou částí jeho činnosti je ale také vyřizování a zkoumání, zda nedochází k porušení ochrany osobních údajů na základě podnětů, nebo stížností. K podání podnětu slouží internetový formulář, obsahující všechny potřebné informace k tomu, aby se věcí mohl úřad začít zabývat. Úřad může na základě podnětu subjektu údajů ověřit zákonnost zpracování osobních údajů, ale také nemusí, pokud doloží že podnět je zřejmě nedůvodný nebo nepřiměřený (zejména pokud se podnět opakuje). Úřad do čtyř měsíců ode dne podání podnětu informuje podatele o tom, zda ověřil zákonnost zpracování a seznámí jej s výsledky svého šetření, anebo odůvodní, proč k prověření zákonnosti nepřistoupil. Nově musí být k těmto informacím připojeno poučení o možnosti žádat o soudní ochranu přezkumem věci nezávislým soudním orgánem.

Při činnosti úřadu je nutné rozlišovat mezi podnětem a stížností. Zatímco podnět lze obecně chápat jako iniciaci přezkumu určité činnosti správce související, se zpracováním osobních údajů, stížnost je typizovaná forma podání, se kterou pracuje i správní řád ve svém § 175 a kterou je možné podat proti postupu správního orgánu. Subjekt tedy disponuje možností podat podnět na úřad proti určité praxi při zpracování osobních údajů se kterou se setkal. Pokud ten mu nevyhoví, nebo není s vyřízením podnětu úřadem spokojený, může podat stížnost. Stížnost se podává u stejného správního orgánu, který řízení vede. V našem případě by tak úřad měl povinnost znovu prošetřit skutečnosti uvedené ve stížnosti a informovat stěžovatele o výsledku šetření do šedesáti dní ode dne doručení stížnosti úřadu.

Vzhledem k tomu, že nařízení na různých místech pracuje s některými novými prostředky ochrany, jež nejsou zakotveny v procesní úpravě českého procesního práva, použije se pro tyto prostředky ochrany subsidiárně procesní úprava stížnosti dle § 175 správního řádu (SŘ). Pokud tedy subjekt podá námitku proti zpracování nezbytného pro splnění úkolu prováděného ve veřejném zájmu, nebo třeba při nesprávnosti údajů o výši započitatelných příjmů orgánem sociálního zabezpečení, bude procesní režim této námitky odpovídat procesní úpravě stížnosti. Při jiných prostředcích ochrany vedle námitky jsou porušení projednávána obecně podle zákona č. 500/2004 Sb. správní řád a dále podle zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich.

GDPR prostřednictví svého článku 83 odst. 8 přímo stanoví, že porušení nařízení v čl. 83 odst. 4 až 6 jsou přestupky ve smyslu vnitrostátního práva. Tím je požadován režim správního trestání pro projednávání a ukládání sankcí dle GDPR. Návrh zákona za tímto účelem stanoví, že sankce jsou projednávány jako přestupky, při zachování garance všech práv vyplývajících z Úmluvy o ochraně lidských práv a základních svobod. Uložené pokuty přitom nejsou příjmem úřadu, ale jsou příjmem státního rozpočtu, ačkoliv je úřad vybírá. V případě, že není pravomocně uložená pokuta uhrazena dobrovolně, předá úřad pokutu k vymáhání celnímu úřadu. Spravedlivé řízení je zajištěno také skrze přezkum nezávislým správním soudem, jež umožňuje osobám pravomocně odsouzeným

ze spáchání přestupku podle GDPR podat ke správnímu soudu žalobu proti pravomocnému rozhodnutí úřadu. Možností soudního přezkumu, však zde máme mnohem více.

7.3. Soudní přezkum

První a nejpřirozenější cestu, kterou předpovídá už i samotná důvodová zpráva k ZZOÚ je přezkum rozhodnutí úřadu správním soudem. Jelikož má správní sankce podobu přestupku, bude proti sankci uložené úřadem možné podat žalobu proti rozhodnutí správního orgánu, dle § 65 soudního řádu správního (SŘS). Účastníkem tohoto řízení by byl dle § 69 SŘS kromě žalobce i úřad. Oba přitom budou mít rovné postavení i možnosti přesvědčit soud o svém názoru. Rovnost v daném postavení však zahrnuje například i možnost úřadu podat kasační opravný prostředek v případě, že úřad nebude s prvostupňovým rozhodnutím soudu souhlasit. A tak právo na spravedlivý proces je garantováno nejen možností přezkumu rozhodnutí správního orgánu v širší slova smyslu nezávislým soudem, ale i skrze plnou možnost úřadu zapojovat se do soudního řízení s cílem vymoci GDPR.

Soudní řád správní ovšem umožňuje bránit se i jinými typy žalob. Vedle výslovně zmíněné žalobě proti pravomocnému rozhodnutí správního orgánu, která bude pravděpodobně nejčastějším způsobem ochrany subjektu, jelikož se rozhodnutí ÚOOÚ bude projednávat jako přestupek, není vyloučené v některých případech, jež nesplňují podmínku povahy správního rozhodnutí použít zásahovou žalobou podle § 82 SŘS. Tato žaloba je zbytkovou kategorií, kdy byl subjekt údajů zkrácen na svých právech nezákonným zásahem, pokynem nebo donucením, který není rozhodnutím a byl zaměřen přímo proti němu nebo v jeho důsledku bylo proti němu zasaženo. Mohlo by se tak jednat například o případy, kdy úřad nedoručí rozhodnutí, nebo vyrozumění, a to tedy nenabude právní moci, nebo jiného neformálního jednání úřadu, které nepředstavuje rozhodnutí ve smyslu § 65 SŘS.

Třetí žalobou podle § 79 SŘS, je žaloba proti nečinnosti správního orgánu. Tato žaloba doplňuje předchozí dvě žaloby a používá se v případech, kdy subjekt vyčerpal všechny prostředky nápravy, které procesní předpis umožňuje při nečinnosti správního orgánu. Žalobou proti nečinnosti se tak lze domáhat, aby soud uložil správnímu orgánu povinnost vydat rozhodnutí ve věci samé nebo jiné osvědčení. Tato třetí žaloba by tak typicky měla uplatnění při nečinnosti úřadu na podnět, nebo námitku podanou subjektem údajů nejpozději do jednoho roku ode dne, kdy v dané věci marně proběhla lhůta stanovená zákonem k vydání rozhodnutí nebo jiného osvědčení.

Vedle soudního přezkumu veřejných subjektivních nároků v režimu SŘS je však možné, že vznikne také nárok ze subjektivních soukromých práv. Typicky rozhodnutí úřadu o udělení pokuty správci osobních údajů může být důvodem vzniku subjektivních soukromých práv, které bude české soudnictví projednávat v režimu části V. OSŘ. Žalobce se v tomto případě bude domáhat, aby soud nově projednal a rozhodl věc, která byla pravomocně rozhodnuta před tím jiným než soudním orgánem v obnoveném nalézacím řízení. Účel tohoto režimu tak bude jiný než podle SŘS, jelikož se jedná o nové posouzení věci kdy, pokud se zjistí, že úřad věc posoudil správně, tak se žaloba zamítne. V opačném případě rozhodne soud rozsudkem, jímž se nahrazuje rozhodnutí správního orgánu v takovém rozsahu, v jakém je rozsudkem dotčeno.

Absence paragrafu v ZZOÚ, jež by se zabýval určením jednoho procesního postupu před soudem způsobila, že nově uvolněnou agendu ochrany osobních údajů mohou subjekty řešit také v civilním soudním řízení. Civilní žalobou podle OSŘ tak lze řešit nejen širokou škálu porušení smluvních ustanovení ochrany osobních údajů například mezi správci, nebo správcem a zpracovatelem, nebo v rámci žaloby na náhradu újmy způsobené porušením ochrany osobních údajů, ale také proti předávání jejich osobních údajů do třetích zemí. Pomocí negatorní žaloby se jedinci v civilním řízení sporném dle OSŘ mohou domoci také toho, aby soud podal předběžnou otázku dle čl. 267 Smlouvy o fungování Evropské unie (SFEU) a přezkoumal rozhodnutí Komise o odpovídající ochraně, podle vzoru judikátu Schrems vs. Facebook Ireland.

Aby byla procesní paleta českého soudního systému kompletní, tak nelze vyloučit ani utváření judikatury ochrany osobních údajů prostřednictvím trestního práva. Trestní právo jakožto ultima ratio , chrání také nakládání s osobními údaji, a to zejména skrze trestný čin neoprávněného nakládání s osobními údaji, za nějž hrozí v kvalifikované skutkové podstatě až osmileté vězení. Tento trestný čin ve svém prvním odstavci stanoví, že: „Kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti." Ve svém druhém odstavci nicméně tento trestný čin skrývá druhou skutkovou podstatu, chránící povinnost mlčenlivosti a sice: „Stejně bude potrestán, kdo, byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají." Skrze tyto dvě skutkové podstaty lze předpokládat tvorbu judikatury k těm nejzávažnějším činům, ohrožující ochranu osobních údajů. Je totiž pravda, že tento trestný čin existoval již před účinností GDPR, ale vzhledem k medializaci právní úpravy osobních údajů a celkové tvorbě širšího povědomí ve společnosti lze očekávat také nárůst této agendy v režimu trestního řádu.

Lze tedy shrnout, že nová právní úprava GDPR uvolnila subjektům údajů mnoho možností k uplatňování jejich práv z ochrany osobních údajů. Díky těmto novým možnostem lze očekávat nárůst této agendy nejen před úřadem ale zejména před nezávislými soudy. Nedávný zájem médií přispěl k informovanosti široké veřejností o této problematice, což stimuluje uplatňování práv subjektů údajů a tímto způsobem i genezi nové agendy. Mediální zájmem o GDPR, přímá vymahatelnost těchto práv a strašidelně vysoké pokuty jsou jevy, které bezpochyby přispívají k dodržování práv z ochrany osobních údajů.

Praktickou překážkou, kterou však přímá vymahatelnost práv přináší v důsledku opomenutí výslovné úpravy v českém ZZOÚ, je definovaný procesní postup uplatnění práv ochrany osobních údajů před soudem. Ignorováním skutečnosti, že ochranu osobních údajů lze v různých situacích uplatňovat všemi procesními postupy, které český právní řád zná, může způsobit zmatek a mnoho nepříjemností, než po letech soudních sporů tuto chybu zákonodárce překoná až judikatura. Z kontextu důvodové zprávy se lze domnívat, že český zákonodárce předpokládal uplatňování práv před správními soudy, zejména pomocí žaloby proti rozhodnutí správního orgánu. Absence vyjádření této vůle v textu předpisu však umožňuje v praxi využít i ostatní procesní cesty v různých kontextech ochrany osobních údajů.

8. Role pověřence pro ochranu osobních údajů a jeho relevance v kontextu výzkumných dat

8.1. Povinnost vysoké školy ustanovit pověřence (DPO)

Obecné nařízení o ochraně osobních údajů vymezuje okruh subjektů, jež mají povinnost ustanovit pověřence pro ochranu osobních údajů a do jisté míry se tak stát sami sobě malým úřadem pro ochranu osobních údajů. Jak bude uvedeno níže, většina tuzemských vysokých škol tuto povinnost má už jen z toho důvodu, že jsou veřejnými subjekty, neboť plní úkoly ve veřejném zájmu a působí vůči svým studentům jako orgán veřejné moci (srov. Čl. 37 GDPR).

I kdyby tato podmínka nebyla u některé z vysokých škol naplněna, nebo byla zpochybněna odlišným výkladem pojmu „veřejná instituce", je nutno upozornit, že existují i další skupiny osob, které jsou dle GDPR povinny ustanovit pověřence. Z článku 37 GDPR mimo jiné vyplývá, že pověřence musí jmenovat každý subjekt, který vykonává výzkum na datech spadajících do okruhu „tzv. zvláštních kategorií údajů",[1]

[1] Zvláštní kategorie osobních údajů jsou osobní údaje, pro něž se v praxi vžil pojem „citlivé osobní údaje". Ve výzkumu se bude jednat zejména o údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických

nebo výzkum spočívající v opakovaném či systematickém monitorování osobních údajů.

Pověřence může dobrovolně ustanovit i organizace, které to zákon přímo neukládá. Právní úprava umožňuje rovněž ustanovení jednoho pověřence pro několik veřejných institucí, nicméně v prostředí vysokých škol je tato možnost poměrně sporná, protože vzhledem k jejich samosprávě chybí orgán schopný jmenovat pověřence pro několik vysokých škol současně. Lze si však představit pověřence jmenovaného společně pro několik ústavů akademie věd, nebo výzkumných ústavů zřízených centrálními orgány státní správy.

Shrnutí: Organizace, která provádí výzkum na člověku, nebo výzkum dotýkající se většího množství lidí, bude s velmi vysokou pravděpodobností muset ustanovit pověřence, a to i v případě, že není veřejnou institucí.

8.2. Odbornost pověřence ve vztahu k výzkumu

Při jmenování pověřence je povinností Organizace zajistit, aby byl pověřenec dostatečně způsobilý k plnění svých úkolů. Jsme v souladu s názorem ÚOOÚ,[2] že k výkonu funkce pověřence není obecně předepsaná žádná certifikace. Avšak dle vodítek WP 29 se musí organizace před jmenováním ubezpečit, že správce osobních údajů má dostatečnou úroveň odborných znalostí, náležité profesní a osobní kvality (schopnosti) k řádnému plnění svých úkolů.

Vodítka WP 29 k profesním kvalitám pověřence uvádějí: „Užitečná je znalost oboru podnikání a chodu organizace, která je správcem. Pověřenec by také měl mít dobrou znalost prováděných operací zpracování, stejně

údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

[2] `https://www.uoou.cz/poverenec-pro-nbsp-ochranu-osobnich-udaju/d-27307/p1=3938` cit. 16. června 2018

jako informačních systémů, bezpečnosti dat a správcových potřeb v oblasti ochrany osobních údajů."

Na veřejných vysokých školách je výzkum jednou z hlavních činností, a proto je nezbytné, aby jmenovaný pověřenec dokázal doložit nejen znalost platných předpisů, ale také orientaci a zkušenosti v oblasti provádění či řízení výzkumných aktivit. Z tohoto důvodu se domníváme, že na výzkumně zaměřené organizaci profesní kvality stěží splní člověk, jež nemá vzdělání přinejmenším magisterského, ideálně však doktorského stupně.

Shrnutí: Vysoká škola se musí mít před jmenováním ubezpečit, že pověřenec je odborně schopen vykonávat dohled i v oblasti výzkumných činností.

8.3. Role pověřence a jeho zapojení do výzkumných procesů

Tento materiál vychází z předpokladu, že je role pověřence podrobněji popsána v příloze A tohoto projektu. Pro účely tohoto modulu vycházíme ze zjednodušené definice, že pověřenec je nezávislým odborníkem v oblasti ochrany osobních údajů, který má instituci napomoci k dodržování právních předpisů a působit jako zprostředkovatel mezi organizací, subjekty osobních údajů a dozorovými orgány. Úkolem pověřence je především být účasten posouzení vlivu na ochranu osobních údajů a dále monitorovat dodržování pravidel v průběhu zpracování těchto údajů.[3]

Pověřenec navzdory jazyku směrnice, která zmiňuje „jmenování pověřence", není jmenovanou funkcí ve smyslu § 33 zákoníku práce a není bez dalšího považován za vedoucího zaměstnance ve smyslu zákoníku práce. Pověřenec nemá právo ukládat jiným zaměstnancům pracovní pokyny a

[3] Úkoly pověřence jsou podrobně popsány v článku 39.

nenese v případě nedodržování souladu s obecným nařízením o ochraně osobních údajů osobní odpovědnost.[4]

Při zapojování role pověřence do výzkumných procesů tak nesmí být zapomínáno na to, že pověřenec není výkonným orgánem instituce, ale orgánem kontrolním. Správce musí zajistit nezávislý výkon funkce pověřence. To znamená, že pověřenec pro ochranu osobních údajů nesmí dostávat žádné pokyny týkající se toho, jak svou práci vykonává. Organizace musí nastavit procesy tak, aby měl pověřenec možnost se do výzkumných procesů včas zapojit nebo je zpětně kontrolovat, běh těchto procesů však nesmí být podmíněn jakýmikoli vstupy či výstupy ze strany pověřence. Odpovědnost za dodržování pravidel a ochranu soukromí však v konečném důsledku nese vždy vedení výzkumné instituce a jednotliví výzkumní pracovníci.

Závěr: Pověřenec se nesmí stát součástí žádných „schvalovacích koleček". Jeho úkolem je být účasten vytváření schvalovacích a kontrolních mechanizmů a monitorovat jejich dodržování.

8.4. Konflikt zájmů pověřence ve výzkumné činnosti

GDPR umožňuje pověřencům „plnit i jiné úkoly a povinnosti", je však nezbytné zabezpečit, aby žádné z těchto úkolů a povinností nevedly ke střetu zájmů.[5]

I když pověřenec může být pověřen i dalšími úkoly, než úkoly vymezenými v článku 39, jeho požadavky na nezávislost a neexistenci konfliktu zájmů jsou prakticky neslučitelné s výkonem funkce v řídících a výkonných orgánech vysoké školy. Souhlasíme s vodítky WP 29 jež

[4] Srov. Vodítko WP 29 ze dne 13. prosince 2016 k pověřencům str. 6
[5] Srov. Vodítko WP 29 ze dne 13. prosince 2016 k pověřencům str. 10

doporučují mít určena pracovní místa, která jsou neslučitelná s výkonem funkce pověřence. Ve vztahu k výzkumným činnostem je nežádoucí, aby byl pověřenec vedoucím výzkumné skupiny, v níž dochází k systematickému zpracování osobních údajů, nebo jiným způsobem koordinoval výzkumné činnosti, v nichž a dochází k výzkumu na člověku. Rovněž není dle našeho názoru vhodná účast pověřence v etických komisích posuzujících etickou přípustnost a legálnost výzkumného záměru.

Pověřenec se však dle našeho názoru může věnovat svému vlastnímu výzkumu. Opačný výklad by byl nedůvodným zásahem do ústavně garantované svobody vědeckého bádání. Pověřenec může být školitelem v doktorském studiu a vedoucím závěrečných prací, protože samotné školitelství není řídící ani výkonnou činností.

Závěr: Funkce pověřence je slučitelná s výkonem funkce akademického/výzkumného pracovníka, pokud není vedoucím výzkumné skupiny, v níž dochází k systematickému zpracování osobních údajů. Při výkonu řídící funkce však musí organizace zkoumat, zda je výkon jakékoliv jiné funkce slučitelný s rolí pověřence.

8.5. Spolupráce s orgány vysoké školy a vstup pověřence do jednotlivých fází výzkumu

Jak bylo uvedeno výše, je funkce pověřence neslučitelná s členstvím v řadě orgánů a komisí uvnitř výzkumné organizace. To však neznamená, že se pověřenec nemůže jednání těchto orgánů účastnit s hlasem poradním. Právě naopak. Je povinností správce zajistit, aby byl pověřenec náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů. Je proto vhodné pověřence informovat a zvát na jednání orgánů, jež může mít dopady na způsob zpracování osobních údajů. Ve vztahu k výzkumu se jedná zejména o jednání etických komisí posuzujících výzkumné přihlášky nebo jednání orgánů odpovědných za provoz výzkumných infrastruktur.

Před zahájením výzkumu může etická komise, vedení ústavu nebo řešitel výzkumného týmu vyžádat od pověřence stanovisko, zda je potřeba k výzkumnému záměru nebo zamýšlené činnosti vypracovat posouzení vlivu na ochranu osobních údajů. Úkolem pověřence však není toto posouzení provádět, pouze vypracovat svůj posudek a poskytnout případné poradenství. Názor pověřence není pro řešitele úkolu závazný, pokud se od něj chce odchýlit, musí v dokumentaci posouzení vlivu konkrétně odůvodnit, proč posudek nebyl vzat v úvahu.

V průběhu výzkumu se může výzkumník na pověřence obrátit s žádostí o stanovisko prakticky k jakémukoliv problému. Dané stanovisko však opět není právně závazné a je na odpovědnosti řešitele/vedoucího pracovníka, zda se stanoviskem bude řídit.

Pro výkon kontrolní funkce pověřence v průběhu výzkumu nejsou specifická pravidla a je nutno vycházet z obecných principů. Pověřenec je vázán mlčenlivostí a lze si představit přístup na žádost k veškerým údajům týkajících se řízení výzkumných činností, nelze však bez dalšího dovodit automatické právo pověřence na přístup k výzkumným datům konkrétního subjektu výzkumu. Je nepochybné, že k efektivnímu výkonu činností pověřence je nezbytné, aby měl pověřenec přístup k evidenci všech výzkumných záměrů, realizovaných projektů a ukončených projektů tak, aby mohl monitorovat plnění jednotlivých povinností v rámci výzkumu.

9. Procesní diagramy

Tato kapitola zahrnuje přehled procesů, s nimiž vědci a administrativa univerzit přichází do styku při práci s osobními daty pro výzkumné účely. Cílem přiložených diagramů je provést příslušného pracovníka krok za krokem nejdůležitějšími rozhodovacími a procesními kroky. Diagramy jsou přiloženy dvojjazyčně a to z důvodu jejich relativní unikátnosti v evropském kontextu. Diagramy pokrývají následující oblasti životního cyklu osobních dat využitých pro výzkumné účely:

- **návrh nových vědeckých projektů** – tedy prvotní fáze před podáním a realizací projektu, během níž se předkladatel rozhoduje o tom, jaká data budou získána a použita, jak bude zajištěna adekvátní úrovneň ochrany dat, i jak se připravit na realizační fázi projektu;
- **správa osobních dat** – kdy jsou již data pro projekt využita a instituce řeší jejich další správu a případně další využití;
- **řešení událostí – incidentů** – kdy musí instituce reagovat na podněty subjektu údajů, případně na podněty z relevantních institucí.

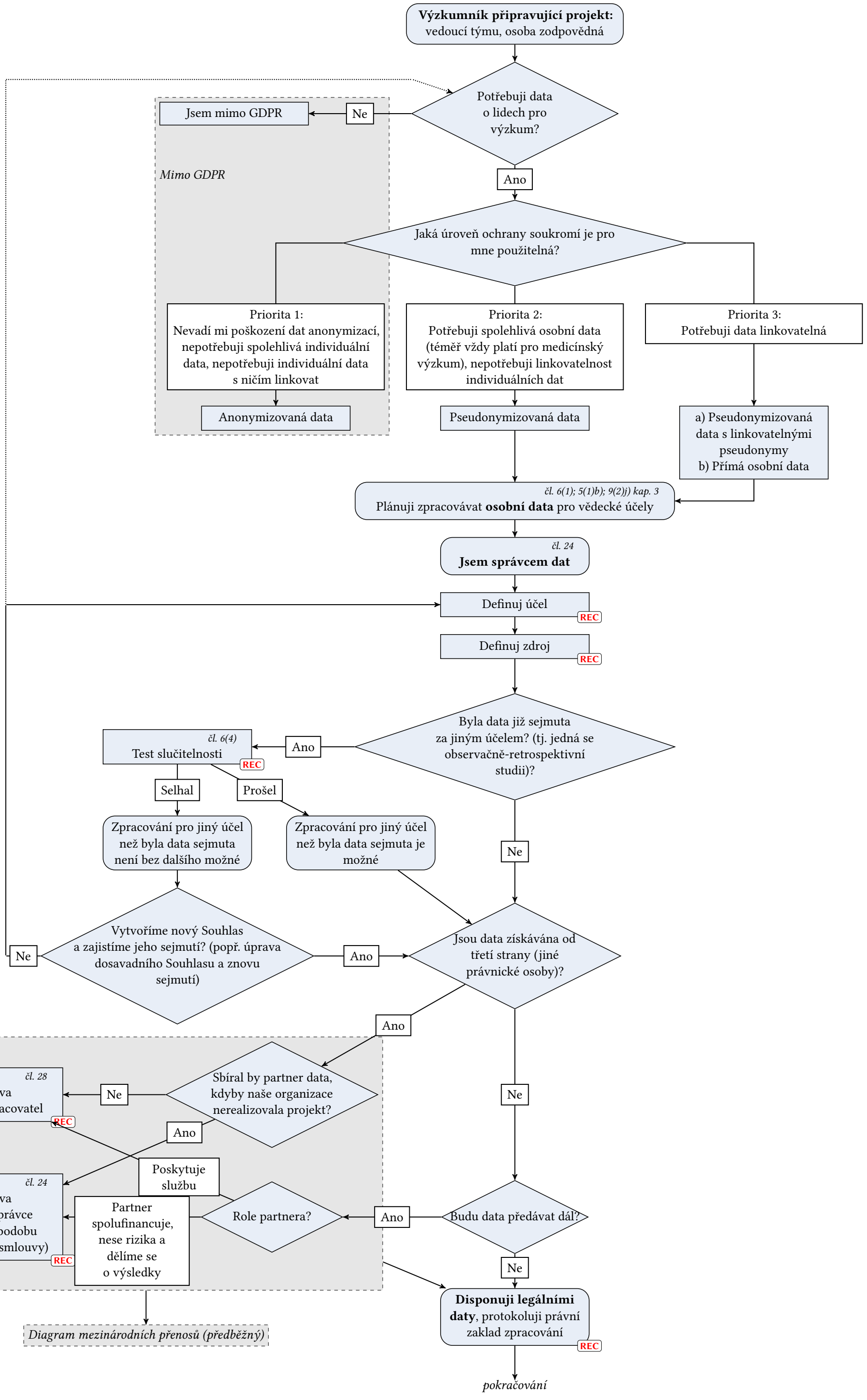
Všechny procesy zohledňují specifika použití dat pro výzkum a snaží se v maximální formě využít dostupných výjimek.

Diagram mezinárodních přenosů je zatím pouze předběžný, s ohledem na vyvíjející se situaci na mezinárodní scéně v této oblasti.

Legenda k diagramům

- Diagramy používají symboly rozhodovacích diagramů: obdélníky jsou procesy, kosodélníky body rozhodnutí, zakulacené boxy jsou terminály.
- V pravém horním rohu rámečků mohou být odkazy:
  - Čl. 1 odst. 2 (anglicky Art. 1(2)) odkazuje na příslušný článek/odstavec GDPR;
  - § 4 odkazuje na příslušný odstavec Zákona o zpracování osobních údajů (ZZOÚ);
  - Str. 8 (anglicky p. 8) odkazuje na příslušnou stránku této příručky.
- REC – označuje momenty, kdy je nezbytné pořídit záznam do protokolu o provedení akce.

Příprava nového projektu



Příprava nového projektu (pokračování)

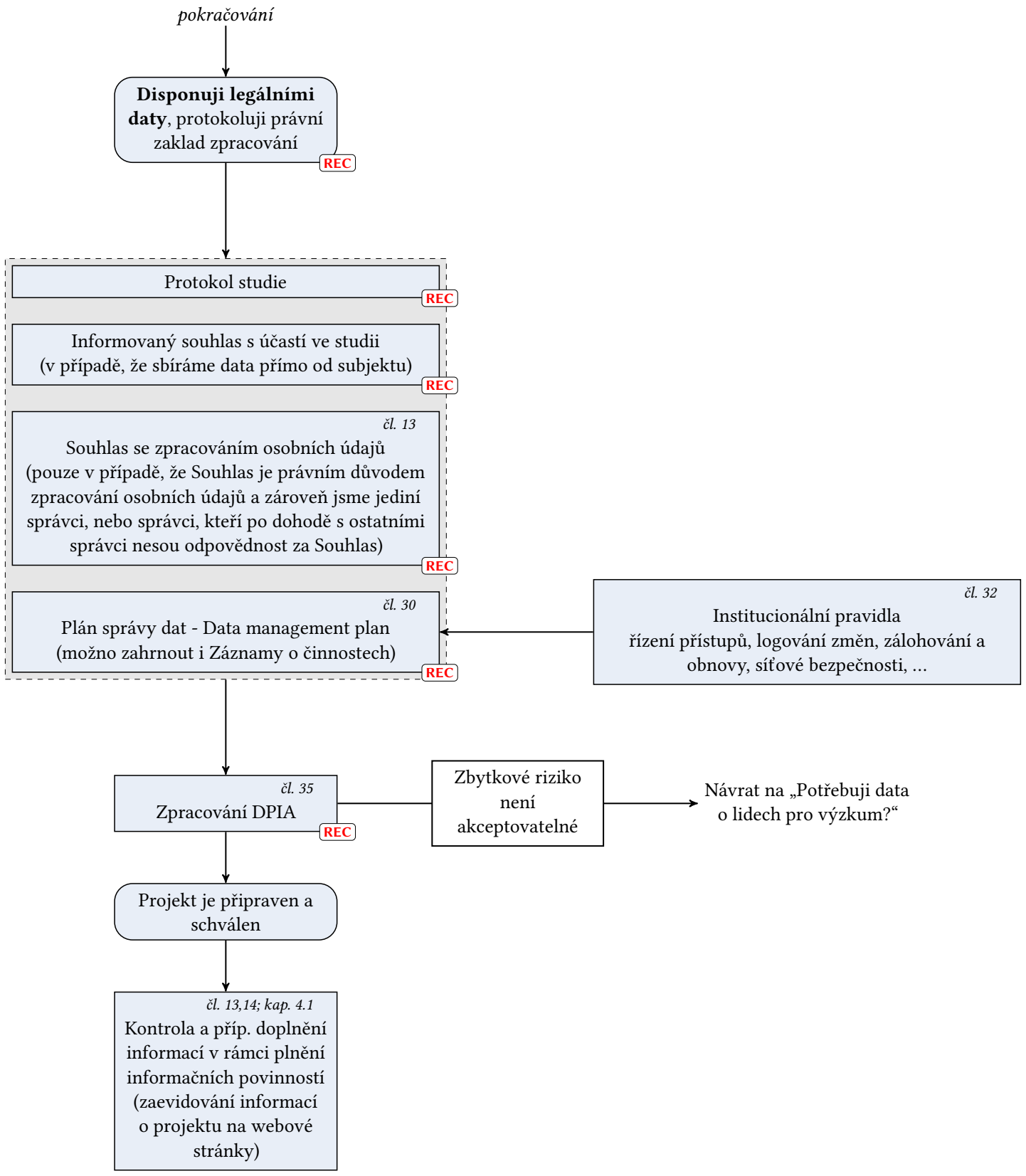
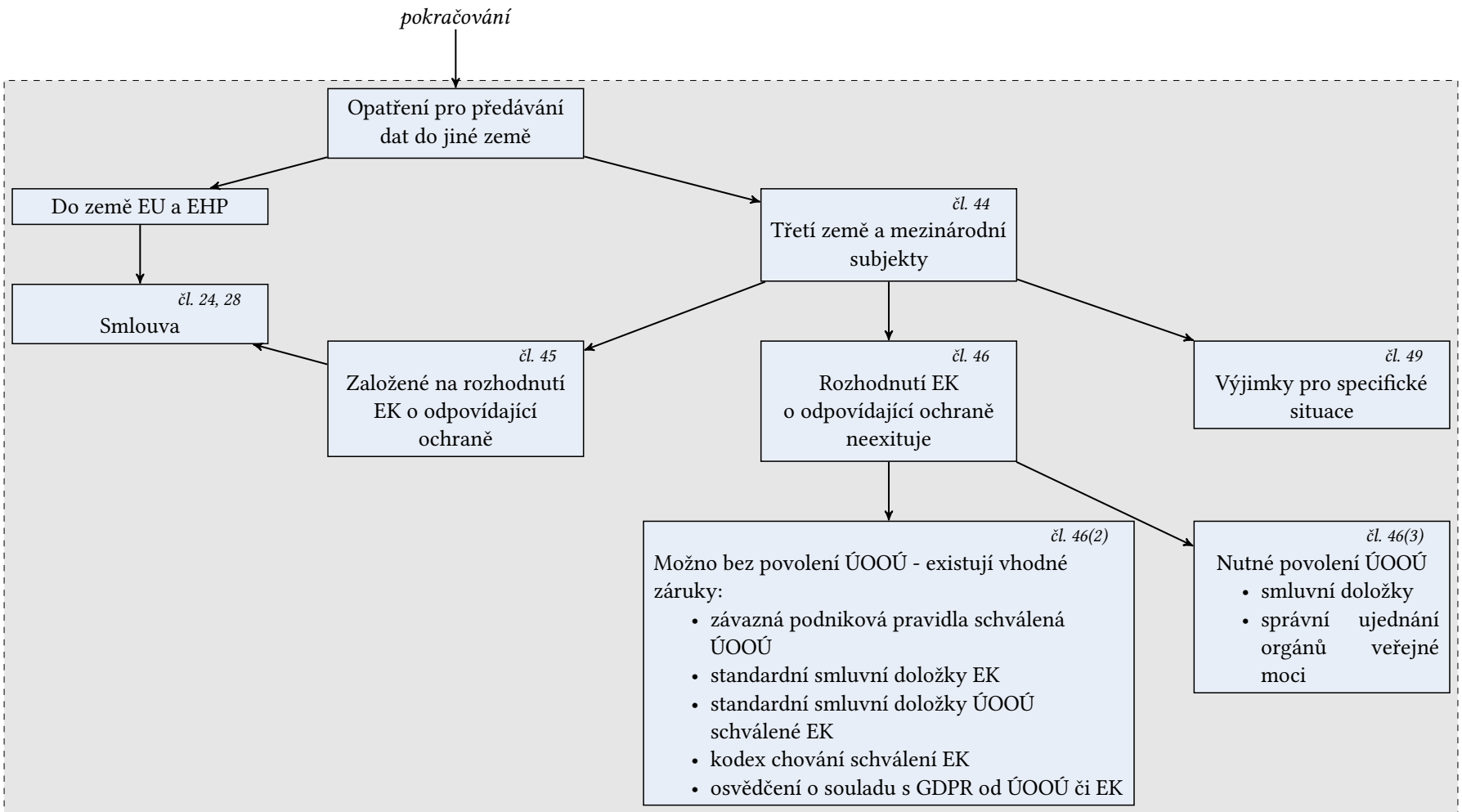
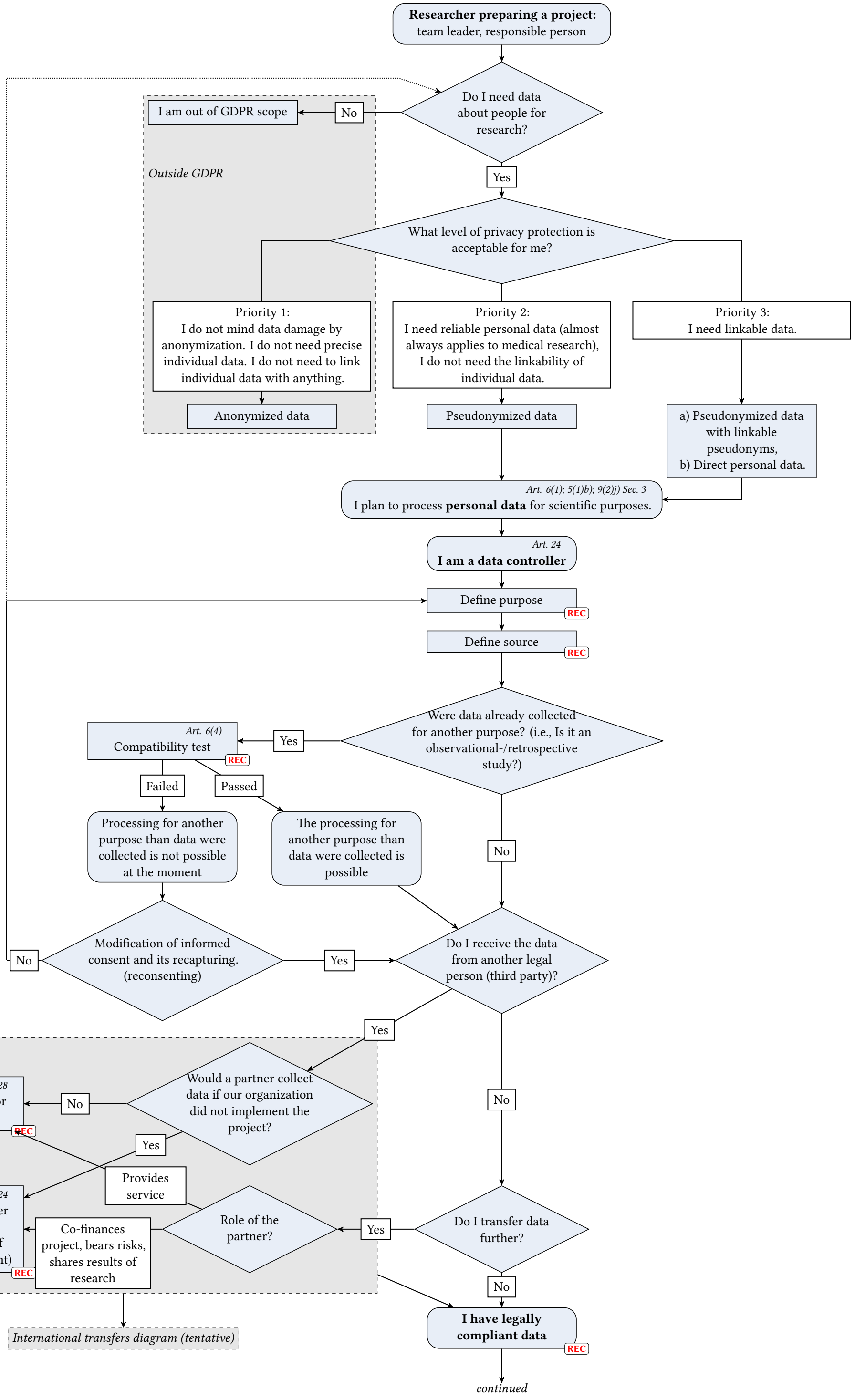


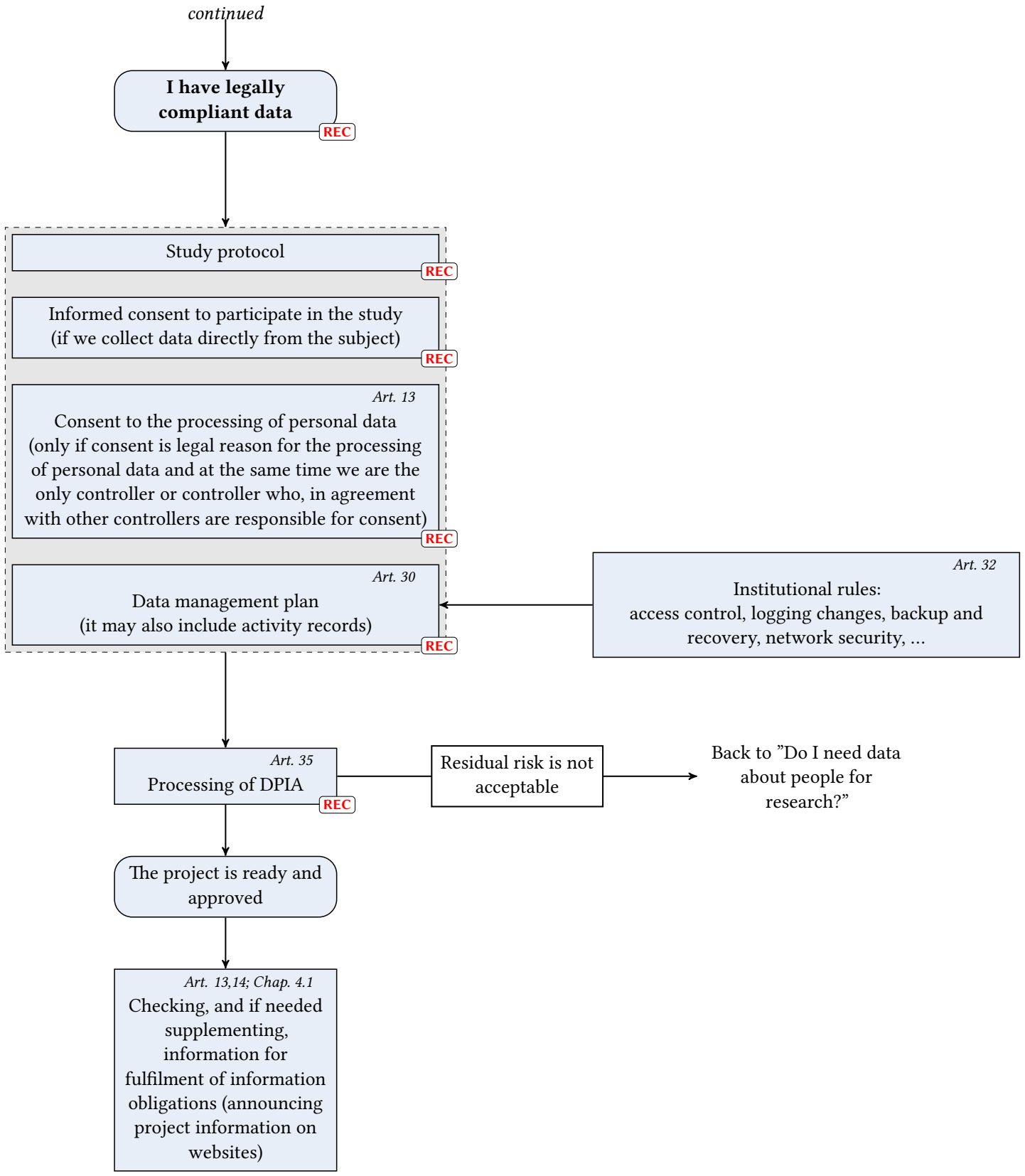
Diagram mezinárodních přenosů (předběžný)



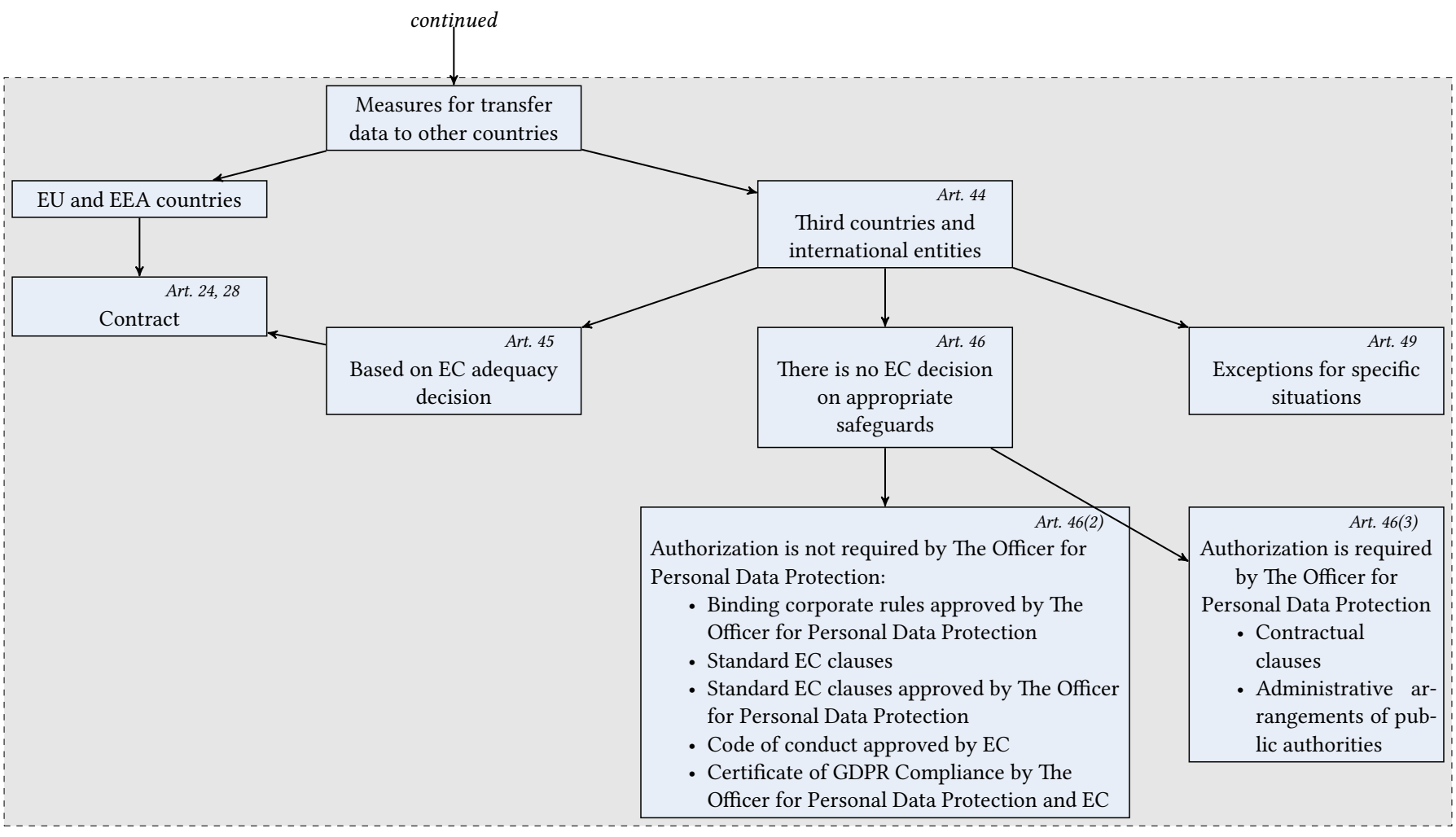
Preparation of a New Project



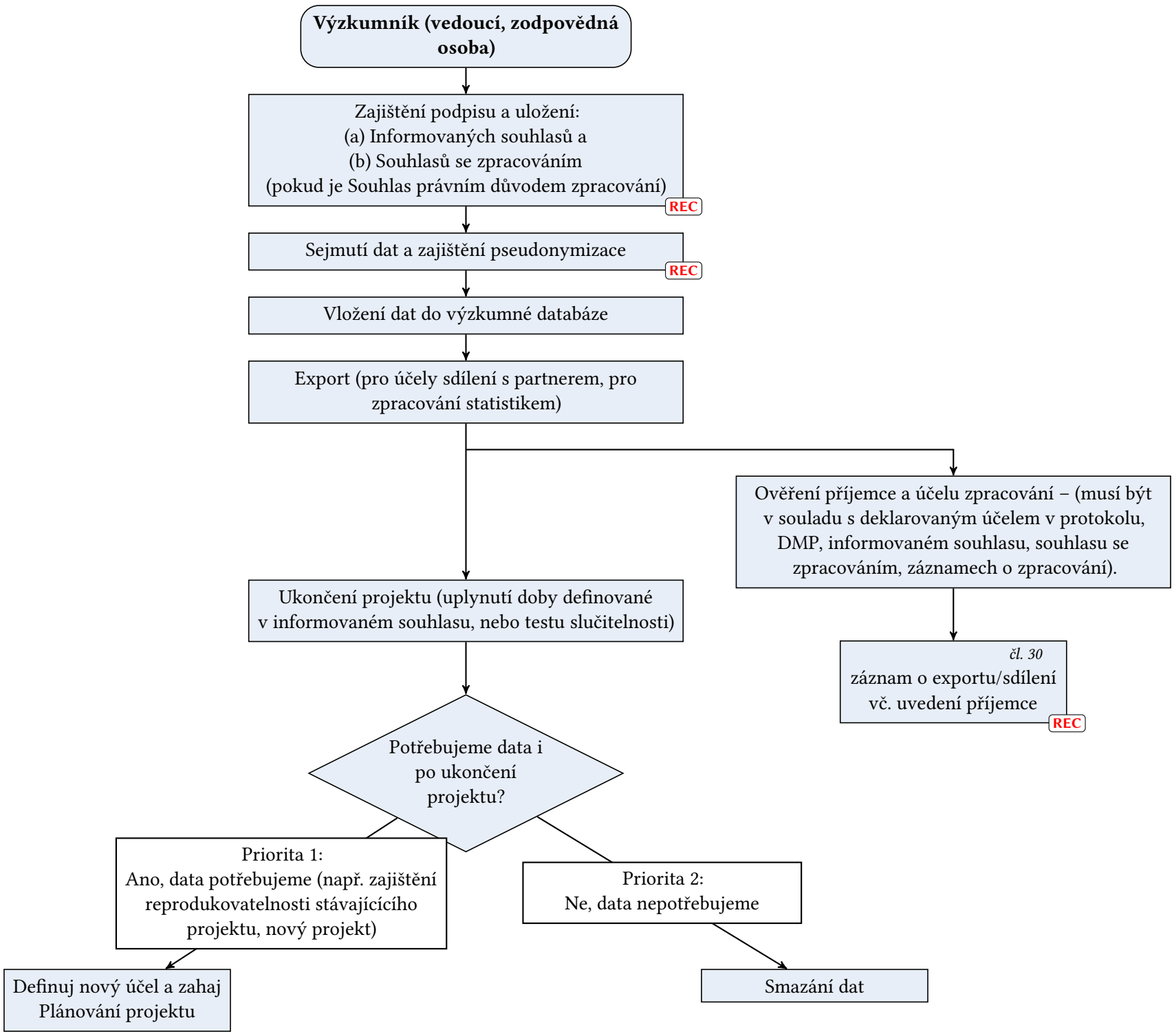
Preparation of a new project (continued)

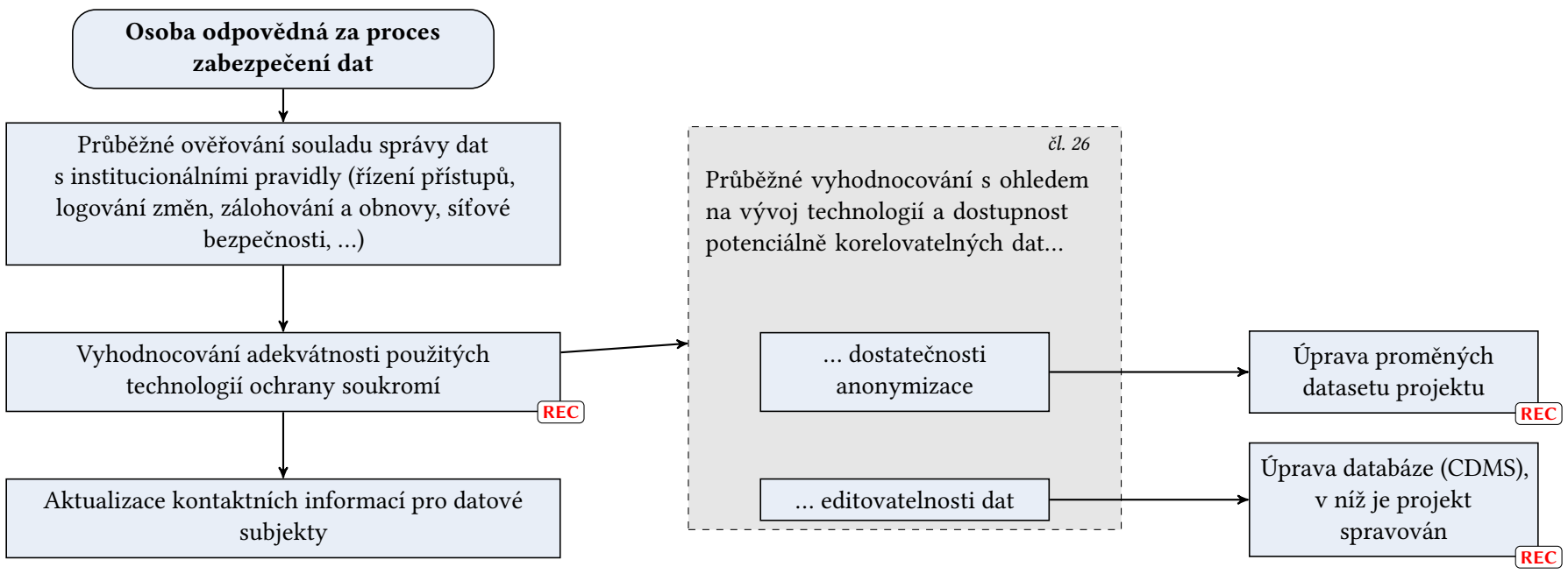


International transfers diagram (tentative)

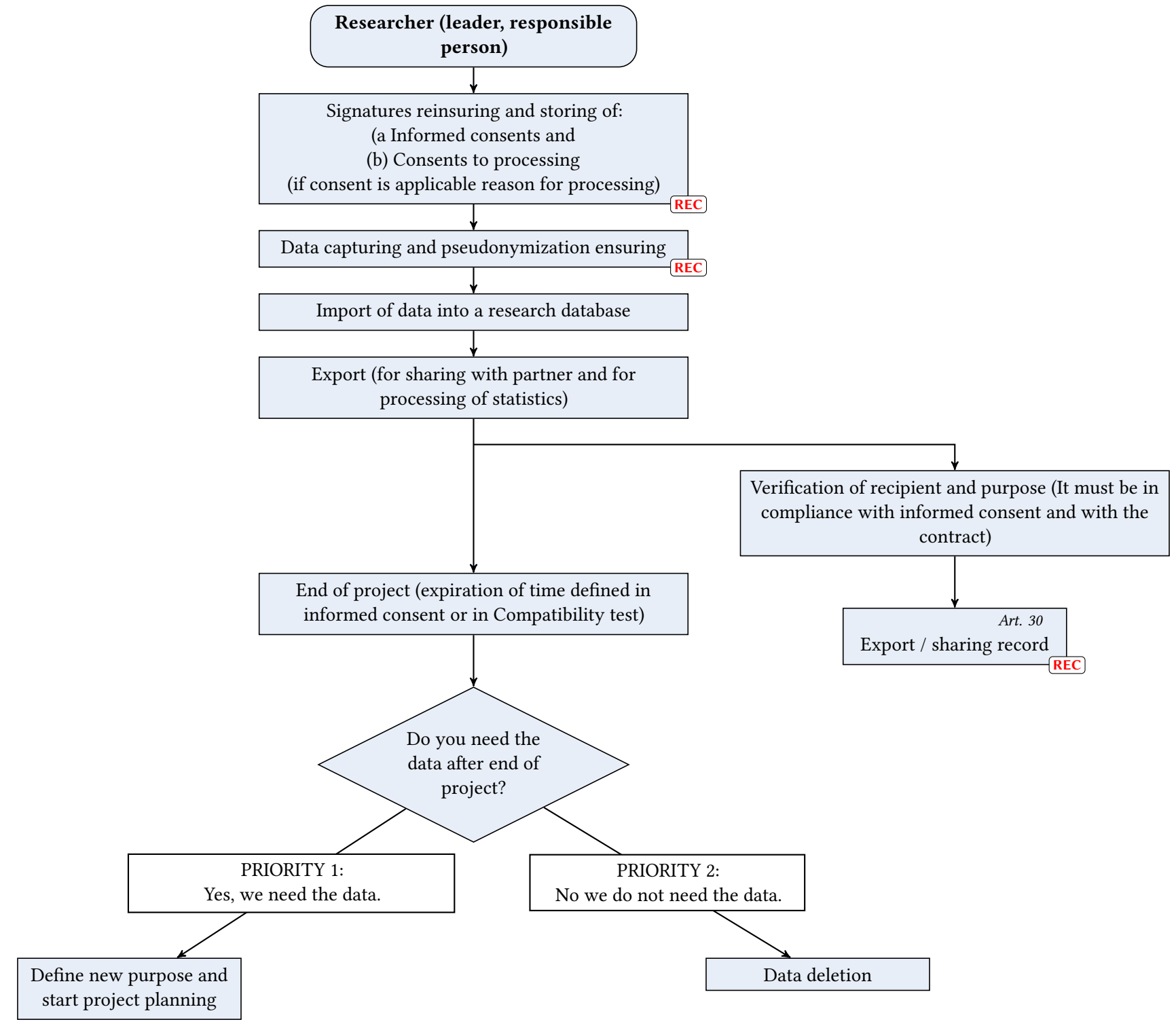


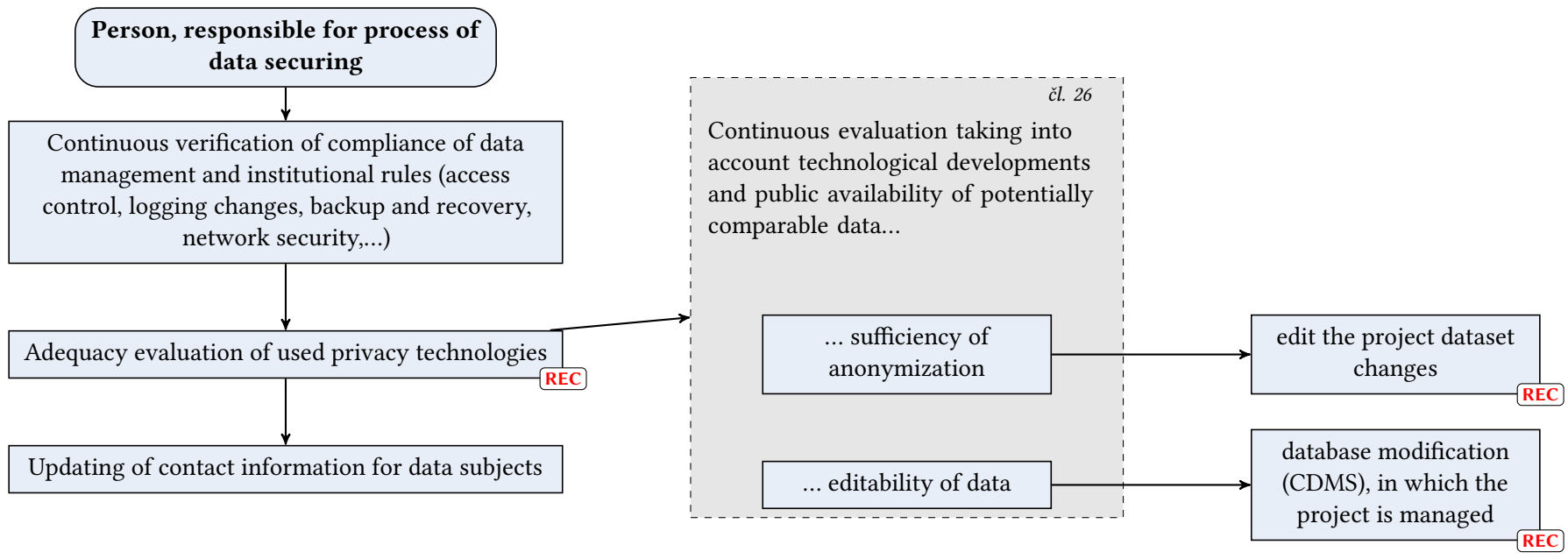
Správa dat


Výzkumník (vedoucí, zodpovědná osoba)
Zajištění podpisu a uložení:
(a) Informovaných souhlasů a
(b) Souhlasů se zpracováním
(pokud je Souhlas právním důvodem zpracování)
REC
Sejmutí dat a zajištění pseudonymizace
REC
Vložení dat do výzkumné databáze
Export (pro účely sdílení s partnerem, pro zpracování statistikem)
Ověření příjemce a účelu zpracování – (musí být v souladu s deklarovaným účelem v protokolu, DMP, informovaném souhlasu, souhlasu se zpracováním, záznamech o zpracování).
čl. 30
záznam o exportu/sdílení vč. uvedení příjemce
REC
Ukončení projektu (uplynutí doby definované v informovaném souhlasu, nebo testu slučitelnosti)
Potřebujeme data i po ukončení projektu?
Priorita 1:
Ano, data potřebujeme (např. zajištění reprodukovatelnosti stávajícího projektu, nový projekt)
Priorita 2:
Ne, data nepotřebujeme
Definuj nový účel a zahaj Plánování projektu
Smazání dat


Osoba odpovědná za proces zabezpečení dat
Průběžné ověřování souladu správy dat s institucionálními pravidly (řízení přístupů, logování změn, zálohování a obnovy, síťové bezpečnosti, ...)
Vyhodnocování adekvátnosti použitých technologií ochrany soukromí
REC
Aktualizace kontaktních informací pro datové subjekty
čl. 26
Průběžné vyhodnocování s ohledem na vývoj technologií a dostupnost potenciálně korelovatelných dat...
... dostatečnosti anonymizace
... editovatelnosti dat
Úprava proměných datasetu projektu
REC
Úprava databáze (CDMS), v níž je projekt spravován
REC

Data Management





Reakce na události

Správce výzkumných osobních údajů reaguje na požadavek REC

Kdo vznesl požadavek?

- *Čl. 12, 89; § 16-21; Kap. 4* Subjekt údajů
- *str. 81* Zpracovatel
- *str. 82* Úřad pro ochranu osobních údajů
- Police ČR
- *str. 84* Soud

Subjekt údajů

DPO komunikuje s Úřadem a poskytuje mu součinnost

Jakou formu komunikace zvolit?

- Priorita 1 → Elektronická odpověď pokud je to možné
- Priorita 2 → Písemná odpověď
- Priorita 3 → Ústně nebo jinou formou, zejména pokud si ji žadatel vyžádá

Ověření totožnosti

Jaké právo chce subjekt údajů uplatnit?

Čl. 18; § 13, 19; str. 69 **Právo na přístup**

Čí zájem je převládající?

- Ne → Oprávněné zájmy správce → Lze omezit, odložit nebo dokonce úplně vyloučit právo na přístup - úměrně k danému případu REC
- Ano → Zájem subjektu údajů na ochraně osobních údajů

Čl. 7; str. 69 **Právo na opravu**

Může požadovat plnění dle smlouvy

Čl 7; § 9; str. 70 **Právo na výmaz**

Probíhá výzkum ve veřejném zájmu?

- Ano → Je pravděpodobné, že by uplatnění práva na výmaz znemožnilo, nebo vážně ohrozilo splnění cílů takového zpracování?
  - Ano → Právo na výmaz se neuplatní REC
  - Ne
- Ne

Čl. 15; § 11, 18; str. 70 **Právo na omezení zpracování**

Potřebuje správce osobní údaje pro jejich původní účel?

- Ne → Požaduje subjekt údajů osobní údaje pro výkon, určení nebo uplatnění právních nároků?
  - Ano → Právo na omezení zpracování se neuplatní REC
  - Ne
- Ano

Úřad pro ochranu osobních údajů

DPO komunikuje s Úřadem a poskytuje mu součinnost

Prošetření podnětu

Vyšetření stížnosti

Police ČR

Vyšetřovací pravomoci

Plnění zákonné povinnosti poskytovat součinnost

Soud

Soudní řízení je zahájené na základě?

1. Žaloby proti rozhodnutí správního orgánu
2. Žaloby proti nezákonnému zásahu
3. Žaloby proti nečinnosti
4. Žaloby podle části V. OSŘ
5. Trestním oznámením
6. Civilní žalobou

Čl. 20; str. 70 **Právo na přenositelnost**

Jedná se o automatizovaně zpracované osobní údaje?

- Ano → Je právní základ souhlas nebo plnění smlouvy?
  - Ne → Právo na přenositelnost se neuplatní REC
  - Ano
- Ne

Čl. 21; § 21; str. 71 **Právo na námitku**

Je zpracování nezbytné pro splnění úkolu, prováděného ve veřejném zájmu?

- Ano → Je námitka uplatněna proti zveřejnění konkrétních osobních údajů?
  - Ano → Prokázal *žadatel*, že jeho zájem na ochraně práv převažuje nad zájmem na zveřejnění těchto osobních údajů?
    - Ano → Neuplatní se výjimky pro zpracování osobních údajů za účelem vědy a výzkumu
    - Ne → Právo na námitku se neuplatní REC
  - Ne
- Ne

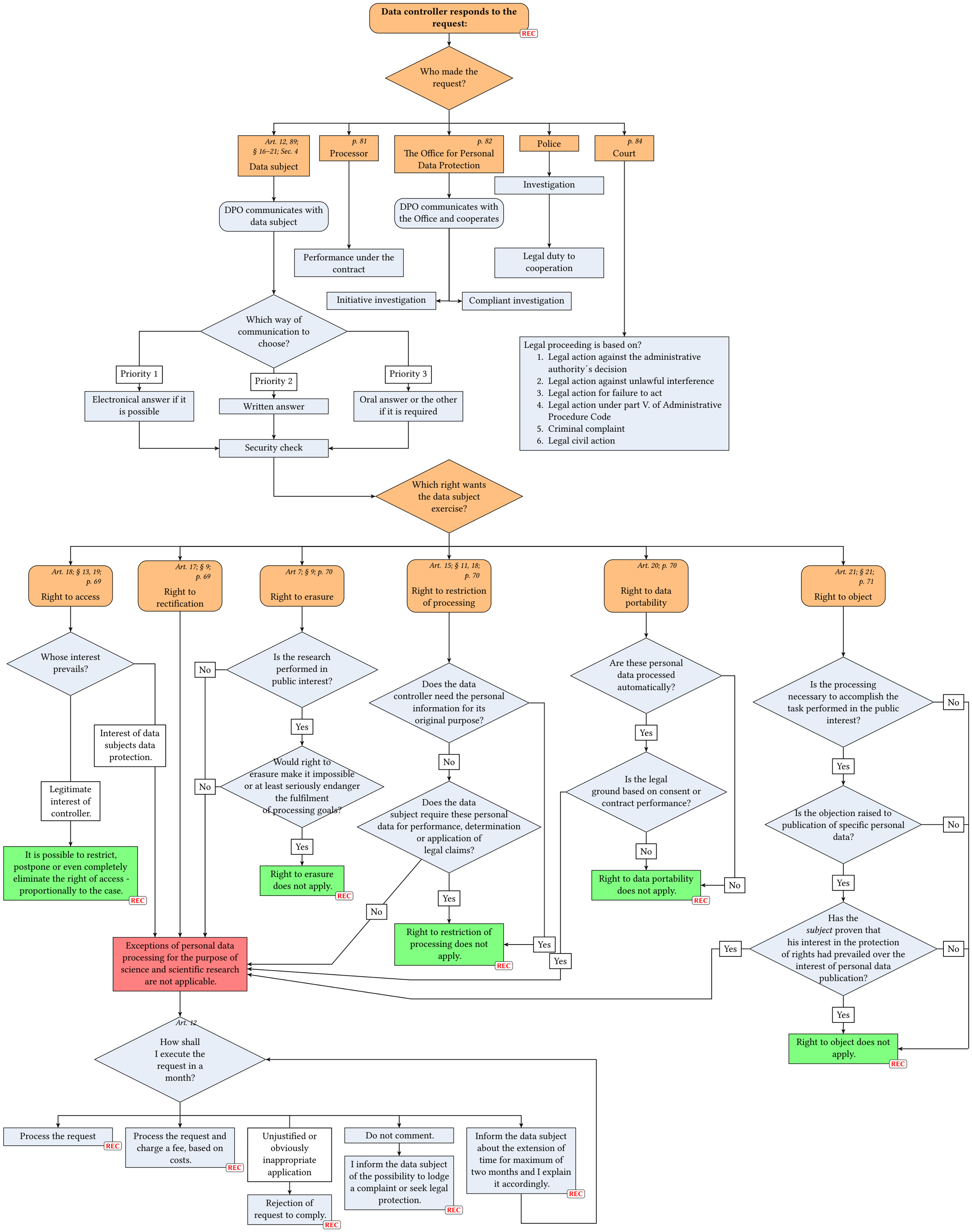
Neuplatní se výjimky pro zpracování osobních údajů za účelem vědy a výzkumu

Čl. 12

Jak během měsíce vyřídím žádost?

- Vyhovím REC
- Vyhovím a uložím poplatek dle nákladů REC
- Neodůvodněná nebo zjevně nepřiměřená žádost → Odmítnu žádosti vyhovět REC
- Nevyjádřím se → Informuji žadatele o možnosti podat stížnost nebo žádat soudní ochranu REC
- Informuji žadatele o prodloužení doby až o další dva měsíce a náležitě to zdůvodním REC

Reactions to Events



10. Dokumentace vědeckého zpracování dat

Kap. 10 na str. 105.

Dokumentaci zpracování osobních dat pro vědecké účely je vhodné provést relativně podrobněji v porovnání s rutinním zpracováním dat např. v personalistice, a to zejména s ohledem na rozmanitost toho, jaká data, za jakým účelem a jakým způsobem jsou zpracována. Tato kapitola uvádí doporučenou strukturu dokumentace.

10.1. Struktura dokumentace

Procesní dokumentace Cílem této dokumentace je zajistit systematickou institucionální dokumentaci zpracování osobních dat v rámci výzkumného projektu.

- Účel zpracování
  - ve fázi sběru dat,
  - ve fázi zpracování dat,
  - ve fázi předávání dat.
- Charakteristika sbíraných daty
  - přehled datového modelu,
  - popis prostředků zpracování,

  - úroveň technických prostředků pro ochranu soukromí (anonymizace, pseudonymizace),
  - nezbytnost a proporcionalita zpracování, vč. zdůvodnění minimalizace,
  - popis technických prostředků zabezpečení (fyzická ochrana, síťová ochrana),
  - Popis organizačních prostředků zabezpečení (řízení přístupu, pracovně-právní zodpovědnost zaměstnanců, smluvní zodpovědnost).
- Právní situace a základ zpracování
  - role,
  - právní titul zpracování (vč. informací o uložení informovaných souhlasů u správce),
  - smluvní situace (smlouvy mezi správcem a zpracovatelem, …).
- Životní cyklus dat
  - omezení doby uložení dat a evidence doby uložení,
  - Data Management Plan
  - Co se stane s daty po zániku účelu?
- Mezinárodní předávání dat
  - Předávání dat z/do zemí implementujících GDPR
  - Předávání do třetích zemí
- Práva subjektu (pouze správce dat)
  - implementace práva odvolání souhlasu a vyjádření námitky,
  - implementace dostupnosti a přenositelnost dat,
  - implementace práva subjektu na informace.

- Vyhodnocení rizik
  - identifikace hrozeb:
    - neoprávněný přístup,
    - neoprávněná modifikace,
    - ztráta dat,
  - dopady rizik na subjekt,
  - vyhodnocení zbytkového rizika.
- Dokumentace a demonstrace compliance
  - compliance s kodexy chování.
- Dozor a konzultace
  - stanovisko pověřence,
  - konzultace s dozorovým úřadem.

Přílohy Poskytují detailnější informace o důležitých podkladech, jako je smluvní situace (vč. konsorcionální smlouvy, DoW u evropských projekt a podobně) a dokumentace datového modelu.

11. Vzor DPIA

Tato kapitola obsahuje vzor DPIA (česky i anglicky) a je dostupná i jako dokument ve formátu DOCX. Konkrétní příklad provedení DPIA je v příloze B.

Posouzení vlivu zpracování na ochranu osobních údajů (DPIA)

Datum zpracování DPIA	
Označení revize DPIA	
Kdo DPIA zpracoval	
Důvod zpracování DPIA	
Datum příští revize	

Informace o zpracování

Základní informace o zpracování

Označení projektu/procesu zpracování OÚ	
Osoba/pracoviště odpovědná za zpracování OÚ	
Účel zpracování OÚ	
Právní základ zpracování OÚ	

Popis subjektů údajů a osobních údajů

Kdo je subjektem údajů?	
V jakém vztahu jsou subjekty údajů vůči správci?	
Jaký je předpokládaný počet subjektu údajů?	
Jaké osobní údaje budou zpracovávány?	
Je rozsah osobních údajů přiměřený, relevantní a omezený ve vztahu k účelu zpracování?	

Popis operací zpracování

Zdroj osobních údajů	
Způsob získání osobních údajů	
Kde a jakým způsobem jsou osobní údaje uloženy	-
Účastníci podílející se na zpracování osobních údajů	-
Předání údajů – zajištění zákonnosti předání, záruky při přeshraničním zpracování	
Doba zpracování OÚ	

Jak je zajištěna přesnost a aktuálnost dat?	
Způsob naložení s OÚ po zániku studie	

Popis organizačních a technických opatření

Použité SW, HW a jiné prostředky (plánované nebo existující)	
Jak je zajištěna pseudonymizace či anonymizace?	-
Jakým způsobem jsou OÚ případně předávány z primární databáze jiným správcům či zpracovatelům, popř. zaměstnancům bez přístupu do primární databáze?	
Jak budou řešeny bezpečnostní incidenty?	

Implementace práva subjektu

Jak jsou/budou subjekty údajů informováni o daném zpracování?	
Jak je zajištěn souhlas subjektů? (pouze pokud aplikovatelné)	
Jak je zajištěno právo na přístup subjektu a přenositelnost OÚ?	
Jak je zajištěno právo na opravu a výmaz?	
Jak je zajištěno právo na omezení zpracování a podání námitky?	

Posouzení rizik

Hrozba	Možné důsledky
Neoprávněný přístup	
Nežádoucí modifikace	
Zánik dat	

Výčet prvků systému zpracování (většinou SW	**Identifikace opatření** Způsob reakce na výše identifikované hrozby.

aplikace, listinné dokumenty, vzorky, snímky, …)	
NIS	
Listinná zdravotnická dokumentace	
SW REDCAP	
Listinné „study-specific“ dokumenty	
Elektronické „study-specific“ dokumenty	
Biologické vzorky	
Snímky zobrazovacích metod (MRI, CT, PET, ultrazvuk)	

Vyhodnocení rizik se provedlo pro jednotlivé hrozby a prvky zpracování. Pro každou hrozbu prvku se vyhodnotila pravděpodobnost výskytu a závažnost dopadu, jejichž součin tvoří výsledný skór rizika, viz:

Skór rizika	**pravděpodobnost výskytu**		
závažnost	1	2	3
3	3	6	9
2	2	4	6
1	1	2	3

Dle skóru rizik se přijme vhodná reakce, viz:

Skór rizika		**Reakce**
nízké 1-2		Riziko akceptováno
Střední 3-4		Riziko možno akceptovat. Management rozhoduje o nápravném opatření.
Vysoké 6-9		Management musí přijmout nápravné opatření.

Hrozba: Neoprávněný přístup k datům

- prvek systému zpracování:

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

- prvek systému zpracování:

pravděpodobnost výskytu	*2*
závažnost dopadu	*3*
výsledný skór	

Hrozba: Nežádoucí úpravy dat

- prvek systému zpracování:

pravděpodobnost výskytu	*1*
závažnost dopadu	*2*
výsledný skór	*2*

Hrozba: Zánik dat

- prvek systému zpracování:

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

Zhodnocení stávajících technických a organizačních opatření:

Návrh případných nových technických a organizačních opatření a jejich dopadů:

Po zavedení tohoto opatření lze snížit skóry rizika, viz:

Hrozba: Neoprávněný přístup k datům

- prvek systému zpracování:

pravděpodobnost výskytu	*1*
závažnost dopadu	*2*
výsledný skór	*2*

Hrozba: Nežádoucí úpravy dat

- prvek systému zpracování:

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

Hrozba: Zánik dat

- prvek systému zpracování:

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

Porovnání a zhodnocení variant jednotlivých opatření:

Dokumentace a demonstrace souladu

Zohlednění posudku pověřence

Stručné shrnutí posudku pověřence (viz příloha) a jeho případných doporučení.

Konzultace s dozorovým úřadem

Přílohy

Data protection impact assessment (DPIA)

Date of creation	
Revision of DPIA	
Author of DPIA	
Reason for creation of DPIA	
Date of next revision	

Information on processing

Basic information on processing

ID of personal data (PD) processing project/process	
Person/workplace responsible for PD processing	
Purpose of PD processing	
Legal basis of PD processing	

Description of data subjects and personal data

Who is data subject?	
What is the relation between data controller and data subjects?	
What is the expected amount of data subjects?	
What categories/types of PD will be processed?	
Is the scope of processing of PD adequate, relevant and limited in relation to purpose of processing?	

Description of processing operations

Source of PD	
Means of acquiring PD	
Where and how are the PD stored?	-
Personnel participating on PD processing	-
PD transfer – ensuring lawfulness of transfer, safeguards for cross-border processing	
Time period for PD processing	
How is it ensured PD are accurate and up-to-date?	

How are PD handled after cessation of the study/project/process?	

Description of organisational and technical measures

SW, HW and other means to be used to protect the PD	
How will be the pseudonymisation and anonymisation ensured?	-
How will be the PD transfered from primary database to other controllers or processors, or to employees without access to primary database?	
How would security incidents be handled?	

Implementation of data subjects rights

How are/will be data subjects informed about particular PD processing?	
How is Consent with PD processing ensured? (only if applicable)	
How is the right of access by data subject and data portability ensured?	
How is the right to rectification and erasure ensured?	
How is the right to restriction and object ensured?	

Risk assessment

Threat	Possible impacts
Illegitimate access	
Undesired modification	
Disappearance of data	

List of elements of PD processing system (mostly SW applications, paper documentation, samples, images,…)	**Identification of current threat mitigation measure**

Risk assessment has been done for each threat and element of processing system. For each pair "threat – processing element" we have evaluated probability of occurrence and severity of impact which product constitutes risk score, see:

Risk score	**Probability of occurrence**		
severity	1	2	3
3	3	6	9
2	2	4	6
1	1	2	3

Adequate measure is taken according to risk score, see:

Risk score		**Reaction**
low 1-2		Risk accepted
Medium 3-4		Risk could be accepted. Management decides on corrective/preventive measures.
High 6-9		Management must take corrective/preventive measure.

Threat: Illegitimate access to PD

- Element of PD processing: *ABC*

Probability of occurrence	
Severity of impact	
Final score	

- Element of PD processing: *XYZ*

Probability of occurrence	
Severity of impact	
Final score	

- …..

Threat: Undesired modification to data

- Element of PD processing: *ABC*

Probability of occurrence	
Severity of impact	
Final score	

- Element of PD processing: *XYZ*

Probability of occurrence	
Severity of impact	
Final score	

- .....

Threat: Disappearance of data

- Element of PD processing: *ABC*

Probability of occurrence	
Severity of impact	
Final score	

- Element of PD processing: *XYZ*

Probability of occurrence	
Severity of impact	
Final score	

- .....

Evaluation of sufficiency of current technical and organisational measures

.....

Proposal of new technical and organisational measures and their impact:

.....

After implementation of those measures the risk scored would be lowered, see:

Threat: Illegitimate access to PD

- Element of PD processing: *ABC*

Probability of occurrence	
Severity of impact	
Final score	

- Element of PD processing: *XYZ*

Probability of occurrence	
Severity of impact	
Final score	

- .....

Threat: Undesired modification to data

- Element of PD processing: *ABC*

Probability of occurrence	
Severity of impact	
Final score	

- Element of PD processing: *XYZ*

Probability of occurrence	
Severity of impact	
Final score	

- .....

Threat: Disappearance of data

- Element of PD processing: *ABC*

Probability of occurrence	
Severity of impact	
Final score	

- Element of PD processing: *XYZ*

Probability of occurrence	
Severity of impact	
Final score	

- .....

Comparison and assessment of different measures

.....

Documentation and demonstration of compliance

Links to relevant controlled and project/process documentation

DPO advice

.....

Data protection regulating authority review

.....

Annexes

.....

Přílohy

A. WP29 – Vodítka k pověřencům pro ochranu osobních údajů

Tato příloha poskytuje neoficiální překlad stanoviska WP29.

Neoficiální překlad z anglického originálu

PRACOVNÍ SKUPINA PODLE ČLÁNKU 29

16/EN
WP 243 rev.01

Vodítka k pověřencům pro ochranu osobních údajů

Schváleno dne 13. prosince 2016

Revize schválena 5. dubna 2017

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán pro otázky ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát poskytlo Generální ředitelství Spravedlnost a spotřebitelé Evropské Komise, B-1049 Brusel, Belgie, kancelář č. MO59 05/35.

Internetové stránky: http://ec.europa.eu/justice/data-protection/index_cs.htm

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na články 29 a 30 uvedené směrnice a

s ohledem na svůj jednací řád,

PŘIJALA TOTO STANOVISKO:

Obsah

1 Úvod

Obecné nařízení o ochraně osobních údajů (dále jen „Obecné nařízení“)[1], které nabude účinnosti 25. května 2018, poskytuje modernizovaný, na zásadě odpovědnosti založený rámec pro dodržování souladu se zásadami ochrany osobních údajů v Evropě. Pověřenci pro ochranu osobních údajů (dále jen „pověřenci“) budou hrát v mnoha organizacích významnou roli, napomáhaje zajišťovat soulad s ustanoveními Obecného nařízení.

Někteří správci a zpracovatelé musí podle Obecného nařízení povinně jmenovat pověřence[2]. Je to případ všech orgánů veřejné moci a veřejných subjektů (bez ohledu na to, jaká data zpracovávají) a dalších organizací, které – jako hlavní činnost – systematicky a rozsáhle monitorují jednotlivce nebo rozsáhle zpracovávají zvláštní kategorie údajů.

I v případech, kdy Obecné nařízení konkrétně nevyžaduje jmenování pověřence, mohou organizace dospět k závěru, že dobrovolné ustavení pověřence může být užitečné. Pracovní skupina podle článku 29 (dále jen „WP29“) takové dobrovolné snahy podporuje.

Koncept pověřence není nový. Přestože směrnice 95/46/ES[3] nepožadovala, aby organizace jmenovaly pověřence, rozvinula se během let tato praxe v několika členských státech.

Před přijetím Obecného nařízení argumentovala WP29, že pověřenec je úhelným kamenem zásady odpovědnosti a jeho jmenování může usnadnit dosažení právního souladu a stát se i konkurenční výhodou firmy.[4] Vedle pomoci při dosahování právní shody uplatněním nástrojů pro zajištění odpovědnosti (pomoc při posuzování vlivu na ochranu osobních údajů a provádění nebo usnadnění auditů), vystupují pověřenci jako prostředníci mezi zainteresovanými stranami (např. orgány dozoru, subjekty údajů a odděleními v rámci organizace).

Pověřenci nenesou osobní odpovědnost za nedodržování Obecného nařízení. Toto nařízení jasně stanoví, že jsou to správci nebo zpracovatelé, kteří musí zajistit a být schopni doložit, že zpracování je prováděno v souladu s jeho ustanoveními (Článek 24, odst. 1). Právní soulad v oblasti ochrany dat je odpovědností správce nebo zpracovatele.

Správce a zpracovatel mají také klíčovou roli při vytváření podmínek pověřencovi pro účinné plnění jeho úkolů. Jmenování je první krok, avšak pověřenec musí mít dostatečnou samostatnost a zdroje pro efektivní výkon funkce.

Obecné nařízení chápe pověřence jako klíčového hráče v novém systému správy dat a stanoví podmínky jeho jmenování, pracovního zařazení jakož i jeho úkoly. Cílem těchto pokynů je objasnit příslušná ustanovení Obecného nařízení a pomoci tak správcům a zpracovatelům vyrovnat se s právními předpisy a ovšem poskytnout také asistenci pověřencům při plnění jejich role. Pokyny také poskytují praktická doporučení, vycházeje ze zkušeností některých členských

---

[1] Nařízení (EU) 2016/679 Evropského parlamentu a Rady 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), (Úř. věst. L 119, 4.5.2016).

[2] Jmenovat pověřence jsou povinny také příslušné orgány ve smyslu článku 32 Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (Úř. věst. L 119, 4.5.2016, str. 89-131) a národní legislativy, která tuto směrnici implementuje. Tyto pokyny se sice zaměřují na pověřence podle Obecného nařízení, jsou však relevantní, vzhledem k obdobným ustanovením, i pro pověřence podle směrnice 2016/680.

3 Směrnice 95/46/ES Evropského parlamentu a Rady ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. L 281, 23.11.1995, str.31).

[4] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

států. WP29 bude sledovat naplňování těchto pokynů a může je v případě potřeby doplnit o další podrobnosti.

2 Jmenování pověřence

2.1. Povinné jmenování

Obecné nařízení v článku 37, odst. 1 požaduje jmenovat pověřence ve třech konkrétních případech:[5]

a) pokud zpracování provádí orgán veřejné moci či veřejný subjekt[6]
b) pokud hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů, nebo
c) pokud hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů[7] nebo[8] osobních údajů týkajících se rozsudků v trestních věcech a trestných činů[9]

V dalším textu poskytuje WP29 rady ohledně kritérií a terminologie v článku 37, odst. 1.

Není-li zřejmé, že organizace nemusí pověřence jmenovat, doporučuje WP29 správcům a zpracovatelům, aby doložili interní analýzou, zda je nebo není nutné pověřence ustavit a mohli tak prokázat, že řádně zohlednili důležité faktory.[10] Tato analýza bude součástí dokumentace pořízené podle zásady odpovědnosti. Dozorový úřad o ni může požádat a měla by být podle potřeby aktualizována, například když správce nebo zpracovatel začne vykonávat nové činnosti nebo poskytovat nové služby, jež mohou spadat mezi případy uvedené v článku 37 odst. 1.

Ustanoví-li organizace pověřence dobrovolně, podléhá jeho jmenování, postavení a úkoly článkům 37 až 39 stejně jako kdyby jmenování bylo povinné.

Nic nebrání organizaci, která není ze zákona povinná jmenovat pověřence a ani ho nechce jmenovat dobrovolně, přesto najmout zaměstnance nebo externí konzultanty pro úkoly související s ochranou osobních údajů. V takovém případě je nutné zajistit, aby nedocházelo k nedorozumění ohledně jejich funkce, postavení a úkolů. Mělo by tedy být uvnitř společnosti i navenek vůči orgánům dozoru, subjektům údajů a široké veřejnosti jasně sděleno, že takový pracovník nebo konzultant není v postavení pověřence pro ochranu osobních údajů.[11]

Pověřenec, povinný nebo dobrovolný, je jmenován pro veškeré operace zpracování prováděné správcem nebo zpracovatelem.

2.1.1 Veřejný orgán nebo veřejný subjekt

[5] Podle článku 37, odst. 4 může Unie nebo členské státy zákonem vyžadovat jmenování pověřence i v jiných případech.
[6] S výjimkou soudů jednajících v rámci svých soudních pravomocí. Viz článek 32 Směrnice (EU) 2016/680.
[7] Podle článku 9 sem patří osobní údaje odhalující rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení či odborovou příslušnost a dále zpracování genetických a biometrických dat za účelem jednoznačné identifikace fyzické osoby, údaje týkající se zdraví nebo údaje o pohlavním životě nebo orientaci fyzické osoby.
[8] V článku 37, odst. 1, písm. c je použita spojka „a“. Použití „nebo“ namísto „a“ je vysvětleno v kapitole 2.1.5 níže.
[9] Článek 10.
[10] Viz článek 24, odst. 1.
[11] Platí to i pro členy vedení organizace pověřených ochranou soukromí (Chief Privacy Officers) a ostatní odborníky na tuto oblast již dnes působících v některých firmách, kteří nemusí vždy splňovat kritéria Obecného nařízení, například pokud jde o dostupné zdroje nebo záruky nezávislosti a pokud je skutečně nesplňují, nemohou být považováni za pověřence.

Obecné nařízení nevysvětluje, co znamená *„veřejný orgán nebo veřejný subjekt“*. WP29 se domnívá, že tento pojem by měl být definován národním právem. Veřejnými orgány a subjekty jsou národní, regionální a místní úřady, ale tento koncept podle platného národního práva typicky zahrnuje řadu dalších subjektů řídících se veřejným právem.[12] V takových případech je jmenování pověřence povinné.

Úkol ve veřejném zájmu a výkon veřejné moci může být plněn[13] nejenom veřejným orgánem nebo subjektem, ale také jinými fyzickými nebo právnickými osobami řídícími se veřejným nebo soukromým právem v oblastech specifikovaných národními předpisy členských států, jako je veřejná doprava, zásobování vodou a energiemi, silniční infrastruktura, veřejnoprávní vysílání, veřejné bydlení nebo disciplinární orgány pro vázané profese.

V těchto případech mohou být subjekty údajů v situaci velmi podobné té, kdy jejich data jsou zpracována veřejným orgánem nebo subjektem. Zvláště proto, že data mohou být zpracována pro podobné účely, přičemž jednotlivci často mají malý nebo nemají žádný vliv na to, zda a jak budou jejich data zpracována a mohou tedy požadovat dodatečnou ochranu, jakou může přinést jmenování pověřence.

Ačkoliv v těchto případech to není povinné, WP29 doporučuje jako osvědčený postup, aby soukromé organizace vykonávající úkol ve veřejném zájmu zadání nebo funkci orgánu veřejné moci jmenovaly pověřence. Činnost tohoto pověřence se vztahuje na veškeré operace zpracování včetně těch, které nesouvisí s plněním úkolu ve veřejném zájmu nebo úřední povinnosti (např. správa databáze zaměstnanců).

2.1.2 Hlavní činnosti

Obecné nařízení v článku 37, odst. 1, písm. b) a c) pojednává o *„hlavních činnostech správce nebo zpracovatele“*. Recitál 97 upřesňuje, že hlavní činnosti správce souvisejí *„s jeho základními činnostmi a nevztahují se na zpracování osobních údajů jakožto pomocnou činnost“*. *„Hlavní činnosti“* mohou být chápány jako klíčové operace nezbytné k dosažení cílů správce nebo zpracovatele.

„Hlavní činnosti“ by však neměly být interpretovány způsobem vydělujícím aktivity, při nichž zpracování dat tvoří nedílnou součást činnosti správce nebo zpracovatele. Například, hlavní činnost nemocnice je poskytovat zdravotní péči. Nemocnice však nemůže poskytovat zdravotní péči bezpečně a účinně bez zpracování zdravotních dat, jako jsou zdravotní záznamy o pacientovi. Zpracování těchto údajů by tedy mělo být považováno za jednu z hlavních činností a nemocnice proto musí jmenovat pověřence.

Jiným příkladem je soukromá bezpečnostní agentura vykonávající dohled v určitém počtu soukromých nákupních center a veřejných míst. Hlídání je hlavní činností firmy, je ovšem neoddělitelně spjato se zpracováním osobních údajů. Tato agentura musí proto jmenovat pověřence.

Na druhé straně, všechny organizace provádějí určité činnosti, například vyplácení zaměstnanců nebo poskytování standardní podpory informační a komunikační techniky. To jsou příklady potřebných funkcí podporujících hlavní činnost nebo podnikání organizace. Byť nutné nebo důležité, jsou tyto aktivity obvykle brány spíše jako pomocné funkce než hlavní činnost.

2.1.3 Rozsáhlé zpracování

[12] Viz například definice pojmů „subjekt veřejného zájmu“ a „veřejnoprávní subjekt“ v článku 2, odst. 1 a 2 směrnice 2003/98/ES Evropského parlamentu a Rady ze dne 17. listopadu 2003 o opakovaném použití informací veřejného sektoru (Úř. věst. L 345, 31.12.1995, str.90).
[13] Článek 6, odst. 1, písm. e.

Podle článku 37, odst. 1, písm. b) a c) musí být zpracování osobních údajů prováděno ve velkém rozsahu, aby to vyvolalo povinnost jmenovat pověřence. Obecné nařízení nedefinuje, co činí zpracování rozsáhlým, určitý návod poskytuje recitál 91. [14]

Vskutku není možné uvést nějaké přesné, pro všechny situace použitelné, číslo udávající množství zpracovávaných dat nebo počet dotčených jednotlivců. Není vyloučeno, že se časem vyvine standardní praxe jak přesněji určit a/nebo množstevně vyjádřit pojem „rozsáhlý" ve vztahu k určitým typům obvyklých činností zpracování. WP29 plánuje přispět k tomuto vývoji sdílením a uveřejňováním příkladů relevantních ukazatelů signalizujících nutnost jmenovat pověřence.

WP29 každopádně doporučuje vzít při určování rozsáhlosti zpracování v úvahu následující faktory:

- počet dotčených subjektů údajů – vyjádřený buď konkrétním číslem, nebo podílem na relevantní populaci
- objem dat a/nebo rozsah různých datových položek
- doba trvání nebo nepřetržitost zpracování
- územní rozsah zpracování

Příklady rozsáhlého zpracování:

- zpracování údajů o pacientech v rámci běžné činnosti nemocnice
- zpracování cestovních dat jednotlivců používajících městskou hromadnou dopravu (např. sledování prostřednictvím čipové průkazky)
- zpracování údajů o aktuální zeměpisné poloze zákazníků mezinárodních řetězců rychlého občerstvení pro statistické účely zpracovatelem zaměřeným na tuto činnost
- zpracování zákaznických dat v rámci běžné obchodní činnosti pojišťovny nebo banky
- zpracování osobních údajů vyhledávačem pro potřeby behaviorální reklamy
- zpracování dat (o obsahu, provozních, lokalizačních) poskytovatelem telefonních a internetových služeb

Příklady zpracování, která nejsou rozsáhlá:

- zpracování údajů o pacientech jednotlivým lékařem
- zpracování osobních údajů týkající se rozsudků v trestních věcech a trestných činů jednotlivým právníkem

2.1.4 Pravidelné a systematické monitorování

Pojem pravidelného a systematického monitorování subjektů údajů není v Obecném nařízení definován, avšak koncept „monitorování chování subjektů údajů" je zmíněn v recitálu 24[15] a jasně zahrnuje všechny formy sledování a profilování na internetu, i pro účely behaviorální reklamy.

---

[14] Jde především o citaci *„rozsáhlé operace zpracování, jež mají sloužit ke zpracování značného množství osobních údajů na regionální, celostátní nebo nadnárodní úrovni, jež by mohly mít dopad na velký počet subjektů údajů a u nichž je pravděpodobné, že budou představovat vysoké riziko"*. Recitál na druhé straně konkrétně stanoví, že *„zpracování osobních údajů by nemělo být považováno za zpracování velkého rozsahu, pokud se jedná o zpracování osobních údajů pacientů nebo klientů jednotlivými lékaři, zdravotníky nebo právníky".* Je třeba si uvědomit, že příklady uvedené v recitálu představují krajní body na opačných koncích pomyslné stupnice (zpracování jednotlivým lékařem v protikladu k zpracování osobních údajů za celou zemi nebo Evropu) a mezi nimi leží velká šedá zóna. Také je třeba mít na paměti, že tento recitál se týká posouzení vlivu na ochranu osobních údajů. Některé prvky mohou tedy být specifické v tomto kontextu a nemusí nutně platit stejným způsobem pro jmenování pověřenců.

[15] *„Aby se určilo, zda může být činnost zpracování považována za monitorování chování subjektů údajů, mělo by být zjištěno, zda jsou fyzické osoby sledovány na internetu, včetně případného následného použití technik zpracování osobních údajů, které spočívají v profilování fyzické osoby, zejména za účelem přijetí rozhodnutí, která se jí týkají, nebo za účelem analýzy či odhadu jejích osobních preferencí, postojů a chování."*

Pojem sledování není však omezen pouze na prostředí online, přičemž sledování na internetu by mělo být bráno jen jako jeden z příkladů monitorování chování subjektů údajů.[16]

WP29 vykládá slovo „pravidelný“ jednou nebo kombinací více následujících charakteristik:

- průběžný nebo v pravidelných intervalech a po určitou dobu se opakující
- stále se opakující nebo opakovaný ve stanoveném čase
- neustále nebo pravidelně se vyskytující

WP29 vykládá slovo „systematický“ jednou nebo kombinací více následujících charakteristik:

- vyskytující se podle určitého systému
- přednastavený, organizovaný nebo metodický
- uskutečňující se jako součást obecného plánu pro sběr dat
- vykonávaný jako součást strategie

Příklady činností, které mohou zakládat pravidelné a systematické monitorování subjektů údajů: provozování telekomunikační sítě; poskytování telekomunikačních služeb; cílení internetové reklamy pomocí e-mailu, marketing řízený daty, profilování a bodování (skórování) pro účely posouzení rizik (např. pro účely hodnocení úvěrového rizika, stanovení výše pojistného, předcházení podvodům, odhalování praní špinavých peněz), sledování polohy, například u mobilních aplikací, věrnostní programy; behaviorální reklama, sledování zdravého životního stylu, tělesné kondice a zdravotních dat pomocí na těle nositelných zařízení, kamerové systémy; propojená zařízení, např. chytré měřiče, chytrá auta, inteligentní domy, atd.

2.1.5 Zvláštní kategorie údajů a údaje týkající se rozsudků v trestních věcech a trestných činů

Článek 37, odst. 1, písm. c) se vztahuje na zpracování zvláštních kategorií údajů podle článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů podle článku 10. I když je v ustanovení užita spojka „a“, není důvod tato dvě kritéria aplikovat zároveň. Text by proto měl být chápán, jako kdyby v něm stálo „nebo“.

2.2. Pověřenec zpracovatele

Článek 37 platí pro správce[17] i zpracovatele[18] pokud jde o jmenování pověřence. V některých případech může pověřence ustanovit jen správce nebo jen zpracovatel, podle toho, kdo z nich splňuje kritéria povinného jmenování. V jiných případech musí pověřence jmenovat správce i zpracovatel (oba by pak měli vzájemně spolupracovat).

Je důležité vyzdvihnout, že i pokud správce splňuje kritéria povinného jmenování, jeho zpracovatel nemusí nutně pověřence jmenovat. Může to však být dobrou praxí.

Příklady:

- Malý rodinný podnik prodávající domácí spotřebiče v jediném městě využívá služeb zpracovatele, jehož hlavní činností je analýza webových stránek a pomoc s cílenou reklamou a marketingem. Činnost rodinného podniku ani jeho zákazníci nezavdávají důvod k rozsáhlému zpracování dat vzhledem k jejich malému počtu a poměrně omezeným aktivitám. Zato zpracovatel, maje dohromady mnoho takových klientů jako

[16] Recitál 24 se zaměřuje na extrateritoriální uplatnění Obecného nařízení. Navíc je zde rozdíl mezi formulací *„monitorování jejich chování“* (článek 3, odst. 2, písm. b) a *„pravidelné a systematické monitorování subjektů údajů“* (článek 37, odst. 1, písm. b), který by mohl vést k domněnce, že jde o dva odlišné pojmy.

[17] Správce je definován v článku 4, odst. 7 jako osoba nebo orgán, který určuje účely a prostředky zpracování.

[18] Zpracovatel je definován v článku 4, odst. 8 jako osoba nebo orgán, který zpracovává osobní údaje pro správce.

zmíněná malá firma, rozsáhlé zpracování provádí. Musí tedy jmenovat pověřence podle článku 37, odst. 1, písm. b). Naproti tomu tento rodinný podnik povinnosti jmenovat pověřence nepodléhá.

- Středně velký výrobce obkladaček zajišťuje ochranu zdraví zaměstnanců smluvně přes externí firmu, která má velký počet podobných klientů. Tato firma (zpracovatel) musí jmenovat pověřence podle článku 37, odst. 1, písm. c) za předpokladu, že se jedná o rozsáhlé zpracování. Výrobce však povinnosti jmenovat pověřence nutně nepodléhá.

Pověřenec jmenovaný zpracovatelem dohlíží rovněž na činnosti, které zpracovatelská organizace vykonává pro sebe jako správce (např. personalistika, IT, logistika).

2.3. Jmenování jediného pověřence pro více organizací

Článek 37, odst. 2 dovoluje skupině podniků jmenovat jediného pověřence, pokud bude *„snadno dosažitelný z každého podniku“*. Pojem dosažitelnosti se vztahuje k úkolům pověřence jako kontaktního bodu pro subjekty údajů[19], orgány dozoru[20], ale také uvnitř organizace, vzhledem k tomu, že jedním z úkolů pověřence je *„poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle tohoto nařízení“*.[21]

K zajištění dostupnosti pověřence, ať interního nebo externího, je důležité, aby byly k dispozici jeho kontaktní údaje v souladu s požadavky Obecného nařízení.[22]

Pověřenec, pokud nutno s pomocí týmu, musí být schopen účinně komunikovat se subjekty údajů[23] a spolupracovat[24] s příslušným dozorovým úřadem. Také to znamená, že komunikovat se musí v jazyce nebo jazycích užívaných dotčenými orgány dozoru a subjekty údajů. Dosažitelnost pověřence (fyzicky na stejném pracovišti jako zaměstnanci, přes horkou linku nebo bezpečné komunikační prostředky) je zásadní pro zajištění, že subjekty údajů budou schopny pověřence kontaktovat.

Podle článku 37, odst. 3, může jediný pověřenec být jmenován pro několik orgánů veřejné moci či veřejných subjektů při zohlednění jejich organizační struktury a velikosti. Totéž platí pro zdroje a komunikaci. V odpovědnosti pověřence jsou rozmanité úkoly, proto musí správce nebo zpracovatel zajistit, aby jediný pověřenec, s pomocí týmu, bude-li nezbytné, je zvládnul plnit efektivně i přesto, že byl jmenován pro několik orgánů veřejné moci nebo veřejných subjektů.

2.4. Dosažitelnost a sídlo pověřence

Pověřenec by měl být, podle Oddílu 4 Obecného nařízení, skutečně dostupný.

WP29 doporučuje jako obecné pravidlo, aby v zájmu dosažitelnosti pověřenec sídlil v Evropské unii, bez ohledu, zda správce nebo zpracovatel je v Evropské unii usazen.

---

[19] Článek 38, odst. 4: *„Subjekty údajů se mohou obracet na pověřence pro ochranu osobních údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle tohoto nařízení“*.

[20] Článek 39, odst. 1, písm. e): působí jako *„kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36, a případně vedení konzultací v jakékoli jiné věci“*.

[21] Článek 39, odst. 1, písm. a).

[22] Viz také oddíl 2.6. níže.

[23] Článek 12, odst. 1: *„Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 a učinil veškerá sdělení podle článků 15 až 22 a 34 o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti.“*

[24] Článek 39, odst. 1, písm. d): *„spolupráce s dozorovým úřadem“*

Nelze však vyloučit, že v některých situacích, kdy správce nebo zpracovatel nebude mít provozovnu v Evropské unii[25], může pověřenec vyvíjet činnost účinněji, bude-li sídlit mimo EU.

2.5. Odborné znalosti a schopnosti pověřence

Článek 37, odst. 5 stanoví, že pověřenec *„musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany osobních údajů a své schopnosti plnit úkoly stanovené v článku 39“*. Recitál 97 říká, že potřebná úroveň odborných znalostí by měla být určena podle prováděných operací zpracování a podle ochrany požadované pro zpracovávané osobní údaje.

- **Úroveň odborných znalostí**

Požadovaná úroveň odborných znalostí není přesně definována, musí však být úměrná citlivosti, složitosti a množství dat, které organizace zpracovává. Například tam, kde činnost zpracování dat je obzvláště složitá, nebo zahrnuje velké množství dat, bude zřejmě pověřenec potřebovat vyšší úroveň znalostí a větší podporu. Je také rozdíl, zda organizace předává osobní údaje mimo Evropskou unii systematicky nebo příležitostně. Pověřenec by tedy měl být vybrán pečlivě s náležitým zvážením specifických otázek ochrany dat, které organizace řeší.

- **Profesní kvality**

Ačkoliv článek 37, odst. 5 neupřesňuje, jaké profesní kvality by při jmenování pověřence měly být zváženy, podstatné musí být vědomosti z oblasti národní a evropské legislativy a praxe v oboru ochrany osobních údajů a důkladná znalost Obecného nařízení. Prospěšné by bylo, kdyby dozorové úřady propagovaly náležité a pravidelné školení pověřenců.

Užitečná je znalost oboru podnikání a chodu organizace, která je správcem. Pověřenec by také měl mít dobrou znalost prováděných operací zpracování, stejně jako informačních systémů, bezpečnosti dat a správcových potřeb v oblasti ochrany osobních údajů.

V případě orgánu veřejné moci nebo veřejného subjektu by pověřenec měl dobře znát také administrativní pravidla a postupy dané organizace.

- **Schopnost plnit úkoly**

Schopnost plnit úkoly přináležející pověřenci by měla být vykládána jednak ve vztahu k jeho osobním kvalitám a znalostem, ale také s ohledem na jeho postavení v organizaci. Osobní kvality by měly zahrnovat například integritu a vysokou úroveň profesionální etiky. Pověřencův prvotní zájem by měl být soulad s Obecným nařízením. Pověřenec hraje klíčovou roli při rozvoji kultury ochrany dat uvnitř organizace a pomáhá zavádět základní prvky Obecného nařízení, jako jsou zásady zpracování dat[26], práva subjektu údajů[27], záměrná a standardní ochrana osobních údajů[28], záznamy o činnostech zpracování[29], zabezpečení zpracování[30] a ohlašování a oznamování případů porušení zabezpečení ochrany osobních údajů[31].

- **Pověřenec na smlouvu o poskytování služeb**

[25] Viz článek 3 Obecného nařízení o místní působnosti
[26] Kapitola II.
[27] Kapitola III.
[28] Článek 25.
[29] Článek 30.
[30] Článek 32.
[31] Články 33 a 34.

Funkci pověřence je možné vykonávat na základě smlouvy o poskytování služeb uzavřené mezi jednotlivcem nebo externí organizací (jinou, než organizace správce nebo zpracovatele). V posledně jmenovaném případě je důležité, aby každý pracovník organizace vykonávající funkci pověřence splňoval všechny platné požadavky Oddílu 4 Obecného nařízení (například je nutné, aby nikdo nebyl ve střetu zájmů). Stejně tak je důležité, aby každý takový pracovník byl chráněn ustanoveními Obecného nařízení (například smlouva o poskytování služeb nemá být nespravedlivě vypovězena v důsledku činnosti pověřence a také žádný pracovník organizace provádějící úkoly pověřence nemá být nespravedlivě propuštěn). Je také možné kombinovat individuální schopnosti a silné stránky, takže více pracovníků pracujících jako tým může účinněji poskytovat služby svým klientům.

V zájmu právní průhlednosti a dobré organizace, jakož i v zájmu předcházení konfliktům zájmů členů týmu, se doporučuje jasně rozdělit úkoly v pověřencově týmu a určit jednoho pracovníka jako hlavní kontakt a osobu „pověřenou“ péčí o zákazníka. Obecně řečeno, užitečné by bylo vymezit tyto body ve smlouvě o poskytování služeb.

2.6. Zveřejňování a sdělování kontaktních údajů pověřence

Článek 37, odst. 7 Obecného nařízení požaduje, aby správce nebo zpracovatel:

- zveřejnil kontaktní údaje pověřence
- sdělil kontaktní údaje pověřence příslušnému dozorovému úřadu

Tyto požadavky mají zajistit, aby subjekty údajů (uvnitř i mimo organizaci) a dozorové úřady mohly snadno a přímo kontaktovat pověřence, aniž by se musely obracet na jiné složky organizace. Důvěrnost je stejně tak důležitá: zaměstnanci například se mohou zdráhat podat stížnost pověřenci, nebudou-li mít záruku, že jejich sdělení bude bráno jako důvěrné.
Pověřenec je v souvislosti s plněním svých úkolů vázán tajemstvím nebo důvěrností v souladu s právem Unie nebo členského státu (Článek 38, odst. 5).

Kontaktní údaje pověřence by měly obsahovat informaci umožňující subjektům údajů a dozorovým úřadům jednoduchým způsobem ho zastihnout (poštovní adresa, vyhrazené telefonní číslo a/nebo vyhrazená e-mailová adresa). Pro komunikaci s veřejností lze, v odpovídajících případech, poskytnout další způsoby komunikace, například vyhrazenou horkou linku nebo zvláštní kontaktní formulář určený pověřenci na webu organizace.

Článek 37, odst. 7 nevyžaduje uvádět mezi kontaktními údaji jméno pověřence. I když v rámci osvědčených postupů by to bylo vhodné, je na rozhodnutí správce nebo zpracovatele a pověřence, zda je to nezbytné nebo účelné za daných okolností.[32]

Je však důležité sdělit jméno pověřence dozorovému úřadu, aby pověřenec mohl fungovat jako kontaktní místo mezi organizací a dozorovým úřadem (Článek 39, odst.1, písm. e).

WP29 dále doporučuje, aby organizace, v souladu s osvědčenými postupy, sdělily dozorovému úřadu a zaměstnancům jméno a kontaktní údaje pověřence. Jméno a kontaktní údaje pověřence mohou například být interně oznámeny na intranetu organizace, v interním telefonním seznamu a v organigramu.

3. Postavení pověřence

3.1. Zapojení pověřence do veškerých záležitostí souvisejících s ochranou osobních údajů

[32] Stojí za zmínku, že článek 33, odst. 3, písm. b), popisující informace, které musí být poskytnuty dozorovému úřadu a subjektům údajů v případě porušení zabezpečení osobních údajů, výslovně vyžaduje, na rozdíl od článku 37, odst. 7, sdělit také jméno (a ne pouze kontaktní údaje) pověřence.

Článek 38 Obecného nařízení stanoví, že správce a zpracovatel zajistí, aby pověřenec *„byl náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů“*.

Je zásadní, aby pověřenec nebo jeho tým byl zapojen co možná nejdříve do všech záležitostí týkajících se ochrany osobních údajů. V souvislosti s posouzením vlivu na ochranu osobních údajů hovoří Obecné nařízení výslovně o včasném zapojení pověřence a stanovuje, aby si správce vyžádal posudek pověřence, když provádí posouzení vlivu na ochranu osobních údajů.[33] Informování pověřence a konzultace s ním hned na začátku procesu usnadní dosažení shody s Obecným nařízením, podpoří uplatnění přístupu podle zásady záměrné ochrany osobních údajů (Privacy by Design) a mělo by se tak stát standardním postupem v rámci řízení organizace. Důležité je, aby pověřenec byl brán jako diskusní partner uvnitř organizace a byl součástí příslušných pracovních skupin zabývajících se v organizaci zpracováním dat.

Z toho důvodu by organizace například měla zajistit, aby:

- pověřenec byl pravidelně zván na schůze vyššího a středního managementu.
- jeho přítomnost byla doporučena vždy tam, kde se dělají rozhodnutí s dopadem do ochrany osobních údajů. Pověřenec musí včas obdržet všechny podstatné informace, aby mohl poskytnout odpovídající radu.
- stanovisku pověřence byla vždy přiznána patřičná závažnost. Pro případ nesouhlasu doporučuje WP29, jako příklad dobré praxe, zadokumentovat důvody, proč pověřencova rada nebyla následována.
- pověřenec byl bezodkladně konzultován v případě porušení zabezpečení ochrany osobních údajů nebo jiné události.

Správce nebo zpracovatel může, uzná-li za vhodné, vypracovat směrnice nebo programy pro ochranu osobních údajů stanovující, kdy musí být pověřenec konzultován.

3.2. Nezbytné zdroje

Obecné nařízení v článku 38, odst. 2 požaduje, aby organizace podporovaly pověřence *„tím, že mu poskytují zdroje k plnění [těchto] úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí“*. Zvážit je potřeba hlavně tyto aspekty:

- aktivní podpora od vyššího vedení (na úrovni představenstva)
- dostatečný čas pro plnění povinností. To je především důležité v případech, kdy interní pověřenec je jmenován na částečný úvazek nebo tuto funkci vykonává externí pověřenec vedle dalších povinností. Protichůdné priority by mohly vést k zanedbávání povinností pověřence. Zcela zásadní je dostatek času věnovaný úkolům pověřence. Je dobrým zvykem stanovit pevný podíl času vyhrazený pro funkci pověřence, pokud není vykonávána na plný úvazek. Je rovněž dobrým zvykem stanovit čas potřebný k výkonu funkce, náležitou úroveň priority pověřencových povinností a sestavit plán práce pověřence (nebo organizace).
- odpovídající podpora z hlediska peněžních zdrojů, infrastruktury (prostory, vybavení, zařízení) a personálu, pokud je třeba.
- oficiální oznámení o jmenování pověřence všem zaměstnancům, aby bylo zajištěno, že jeho existence a funkce je v organizaci známa.
- nezbytný přístup do jiných útvarů v organizaci, jako personální, právní, IT, bezpečnost, atd., aby měl pověřenec nezbytnou podporu a informace z těchto útvarů
- průběžné školení. Pověřenec musí dostat příležitost udržovat své znalosti v souladu s rozvojem v oblasti ochrany dat. Cílem by mělo být neustálé zvyšování úrovně znalostí a měla by také být podporována účast pověřenců na školeních o ochraně dat a dalších formách profesního rozvoje, jako jsou fóra, semináře, atp.

[33] Článek 35, odst. 2.

- v závislosti na velikosti a struktuře organizace může se ukázat nezbytným sestavit celý tým (pověřenec a jeho personál). V takovém případě by vnitřní struktura týmu a úkoly a odpovědnosti jednotlivých členů měly být jasně stanoveny. Obdobně, pokud funkci pověřence vykonává externí poskytovatel, může skupina lidí pracujících pro tohoto poskytovatele efektivně vykonávat funkci pověřence jako tým, přičemž odpovědnost nese hlavní kontaktní osoba, které byl klient přidělen.

Obecně řečeno, čím složitější a/nebo citlivější jsou operace zpracování, tím více zdrojů musí být pověřenci dáno k dispozici. Tato funkce musí být účinným a dostatečným způsobem zabezpečena zdroji v poměru k prováděnému zpracování.

3.3. Pokyny a plnění povinností a úkolů nezávislým způsobem

Článek 38, odst. 3 stanovuje některé základní záruky napomáhající zajistit, aby pověřenec byl schopen plnit úkoly s dostatečným stupněm samostatnosti v rámci organizace. Od správců a zpracovatelů se zejména vyžaduje zajistit, aby pověřenec *„nedostával žádné pokyny týkající se výkonu [jeho] úkolů“*. V recitálu 97 je uvedeno, že pověřenci *„bez ohledu na to, zda se jedná o zaměstnance správce, by měli být schopni plnit své povinnosti a úkoly nezávislým způsobem“*.

To znamená, že při plnění úkolů podle článku 39 nesmí pověřenci dostávat pokyny jak jednat v dané oblasti, například, jakého výsledku se má dosáhnout, jak prošetřovat stížnost nebo zda konzultovat dozorový úřad. Dále jim nesmí být nařizováno přijímat určité názory v záležitostech týkajících se ochrany dat, například konkrétní výklad práva.

Autonomie pověřenců však neznamená, že mají rozhodovací pravomoci přesahující rámec jejich úkolů podle článku 39.

Za dodržení souladu s právními předpisy pro ochranu osobních údajů zůstává odpovědný správce nebo zpracovatel a musí být schopen tento soulad doložit.[34] Pokud správce nebo zpracovatel učiní rozhodnutí neslučitelná s Obecným nařízením a s radou pověřence, měl by pověřenec dostat možnost své nesouhlasné stanovisko vysvětlit nejvyššímu vedení a těm, kteří tato rozhodnutí udělali. Článek 38, odst. 1 v tomto ohledu stanoví, že pověřenec *„je přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele“.* Taková přímá podřízenost zajišťuje, že se vyšší management (např. představenstvo) dozví o radách a doporučeních pověřence coby součásti jeho poslání informovat a radit správci a zpracovateli. Dalším příkladem přímé podřízenosti je příprava výroční zprávy o činnosti pověřence pro nejvyšší úroveň řízení.

3.4. Propuštění nebo sankcionování pověřence v souvislosti s plněním jeho úkolů

Článek 38, odst. 3 stanoví, že pověřenec *„není správcem nebo zpracovatelem propuštěn ani sankcionován v souvislosti s plněním svých úkolů“*.

Tento požadavek posiluje samostatné postavení pověřenců a napomáhá zajistit, aby jednali nezávisle a požívali dostatečnou ochranu při plnění svých úkolů v oblasti ochrany dat.

Tresty podle Obecného nařízení jsou zapovězeny, jen pokud jsou uloženy jako následek výkonu povinností pověřence. Například, pověřenec může být názoru, že konkrétní zpracování by mohlo mít za následek vysoké riziko a doporučí správci nebo zpracovateli vypracovat posouzení vlivu na ochranu osobních údajů, ovšem správce nebo zpracovatel nesouhlasí s pověřencovým posudkem. V takové situaci nemůže být pověřenec za své doporučení propuštěn.

Tresty mohou nabývat řady forem a mohou být přímé nebo nepřímé. Mohou kupříkladu spočívat v zaražení nebo odkladu povýšení, bránění v kariérním postupu či odmítnutí výhod, které jiní

[34] Článek 5, odst. 2.

zaměstnanci požívají. Není nutné tyto tresty skutečně dokonat, pouhá jejich hrozba je dostatečná, pokud je užita k potrestání pověřence z důvodů souvisejících s jeho činností.

Podle běžné zásady řízení a jak by se stalo i v případě jiných zaměstnanců nebo smluvních partnerů podléhajících národnímu obchodnímu nebo pracovnímu a trestnímu právu, mohl by pověřenec být legitimně propuštěn z důvodů jiných, než v souvislosti s jeho úkoly pověřence (například v případě krádeže, fyzického, psychického nebo sexuálního obtěžování nebo podobně silně nevhodného chování).

V této souvislosti budiž řečeno, že Obecné nařízení neupřesňuje, jak a kdy může být pověřenec propuštěn nebo nahrazen jinou osobou. Nicméně, čím stabilnější bude pověřencova smlouva a čím více záruk bude mít proti nespravedlivému propuštění, tím je pravděpodobnější, že bude jednat nezávislým způsobem. WP29 proto uvítá ze strany organizací jakékoli snahy v tomto směru.

3.5. Střet zájmů

Článek 38, odst. 6 dovoluje pověřencům *„plnit i jiné úkoly a povinnosti“*. Od organizace to ovšem vyžaduje zabezpečit, aby *„žádné z těchto úkolů a povinností nevedly ke střetu zájmů“*.

Nepřítomnost konfliktu zájmů úzce souvisí s požadavkem nezávislého jednání. Byť pověřenci smějí mít i jiné funkce, mohou jim být svěřeny pouze úkoly a povinnosti, které nezakládají střet zájmů. Především z toho plyne, že pověřenec v organizaci nemůže zastávat pracovní místo, na kterém by stanovoval účely a prostředky zpracování osobních údajů. Vzhledem k organizační struktuře specifické pro každou organizaci, je potřeba tuto otázku řešit případ od případu.

V konfliktním postavení mohou typicky být pozice ve vyšším managementu (výkonný ředitel, provozní ředitel, finanční ředitel, zdravotní ředitel, vedoucí marketingového oddělení, vedoucí personálního oddělení nebo vedoucí oddělení IT), ale i pozice na nižším stupni organizační struktury, pokud v takovém postavení dochází k rozhodování o účelech a prostředcích zpracování. Konflikt zájmů může také kupříkladu vzniknout, pokud externí pověřenec bude požádán o zastupování správce nebo zpracovatele před soudem v případě týkajícím se ochrany osobních údajů.

V závislosti na činnostech, velikosti a struktuře organizace může správcům a zpracovatelům posloužit jako příklad osvědčeného postupu následující:

- určit pracovní místa neslučitelná s výkonem funkce pověřence
- sestavit vnitřní pravidla k zamezení střetu zájmů
- začlenit do pravidel obecnější vysvětlení střetu zájmů
- prohlásit, že pověřenec není ve střetu zájmů ve vztahu ke své funkci pověřence jako způsob zvyšování povědomí o tomto požadavku
- začlenit do vnitřních pravidel záruky a zajistit, aby oznámení volného místa pověřence nebo smlouvy o poskytování služeb bylo dostatečně přesné a podrobné a tím se zamezilo střetu zájmů. V této souvislosti je dobré mít na paměti, že konflikty zájmů mohou nabývat různých forem podle toho, je-li pověřenec získáván interně nebo externě.

4 Úkoly pověřence

4.1. Monitorování souladu s Obecným nařízením

Článek 39, odst. 1, písm. b) svěřuje pověřencům, kromě jiných povinností, úlohu monitorovat soulad s Obecným nařízením. Recitál 97 dále ve vztahu k pověřencům upřesňuje, že *„měla by*

být správci nebo zpracovateli při monitorování toho, zda je zajištěn vnitřní soulad s tímto [Obecným] nařízením nápomocna osoba s odbornými znalostmi".

Pověřenec, v rámci svých povinností, může zejména:

- shromažďovat informace za účelem zjišťování zpracovatelských činností
- analyzovat a prověřovat právní soulad zpracovatelských činností
- informovat, radit a vydávat doporučení správci nebo zpracovateli

Monitorování souladu neznamená, že pověřenec je osobně odpovědný za případy nesouladu. Obecné nařízení jasně stanoví, že je to správce, a nikoliv pověřenec, kdo má povinnost, že *„zavede vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto [Obecným] nařízením"*. (Článek 24, odst. 1). Soulad s předpisy o ochraně dat je podniková odpovědnost správce, ne pověřence.

4.2. Role pověřence při posuzování vlivu na ochranu osobních údajů

Podle článku 35, odst. 1 je povinností správce, nikoliv pověřence, provést, pokud je nutné, posouzení vlivu na ochranu osobních údajů (dále jen „posouzení vlivu"). Pověřenec však může sehrát velmi důležitou a užitečnou roli při pomoci správci. Vycházeje z principu záměrné ochrany osobních údajů, obsahuje článek 35, odst. 2 konkrétní požadavek, aby správce *„si vyžádal posudek"* pověřence při provádění posouzení vlivu. Naopak článek 39, odst. 1, písm. c) zadává pověřenci úkol *„poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle článku 35"*.

WP29 doporučuje správcům, aby vyžadovali posudek pověřence mimo jiné k následujícím otázkám[35]:

- zda je nebo není nutné provést posouzení vlivu
- jakou metodiku při zpracování posouzení vlivu použít
- zda posouzení vlivu vypracovat vlastními silami nebo jeho zpracování zadat externě
- jaká ochranná opatření (včetně technických a organizačních) uplatnit pro zmírnění rizik vůči právům a zájmům subjektů údajů
- zda posouzení vlivu bylo zpracováno správně a zda jeho závěry (ať už vedou či ne k pokračování zpracovatelské operace a bez ohledu na to, jaká ochranná opatření určují uplatnit) jsou v souladu s Obecným nařízením

Nesouhlasí-li správce s posudkem dodaným pověřencem, mělo by v dokumentaci posouzení vlivu být konkrétně odůvodněno, proč posudek nebyl vzat v úvahu[36].

WP29 dále doporučuje, aby správce jasně vymezil, například ve smlouvě s pověřencem, ale také v informaci pro zaměstnance i vedení (a pro další zainteresované strany, pokud existují), přesné úkoly pověřence a jejich rozsah, zejména s ohledem na provádění posouzení vlivu.

[35] Článek 39, odst. 1 zmiňuje úkoly pověřence a uvádí, že pověřenec má vykonávat *„alespoň"* tyto úkoly. Nic proto nebrání správci, aby pověřenci přidělil i jiné úkoly, než ty, které jsou výslovně uvedeny v článku 39, odst. 1 nebo tyto úkoly upřesnil do většího detailu.

[36] Článek 24, odst. 1 stanoví, že *„s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována."*

4.3. Spolupráce s dozorovým úřadem a působení jako kontaktní místo

Podle článku 39, odst. 1, písm. d) a e) je úkolem pověřence *„spolupráce s dozorovým úřadem“* a *„působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36, a případně vedení konzultací v jakékoli jiné věci“*.

Tyto úkoly se týkají role pověřence coby nápomocné osoby, jak je zmíněno v úvodu těchto vodítek. Pověřenec jedná jako kontaktní osoba usnadňující dozorovému úřadu přístup k dokumentům a informacím pro výkon úkolů podle článku 57, jakož i pro uplatňování jeho vyšetřovacích, nápravných, povolovacích a poradních pravomocí podle článku 58. Jak již bylo zmíněno, pověřenec je v souvislosti s výkonem svých úkolů vázán tajemstvím a důvěrností v souladu s právem Unie nebo členského státu (Článek 38, odst. 5). Závazek tajemství, resp. důvěrnosti však pověřenci nebrání kontaktovat dozorový orgán se žádostí o radu. Článek 39, odst. 1, písm. e) stanoví, že pověřenec může případně vést konzultace s dozorovým úřadem v jakékoli věci.

4.4. Přístup založený na riziku

Článek 39, odst. 2 říká, že správce *„bere patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování.“*

Tento článek se odvolává na obecnou zásadu organizace práce a na selský rozum, tedy principy, které mohou být důležité v mnoha aspektech každodenní práce pověřence. V podstatě od pověřenců vyžaduje přiřazovat priority svým činnostem a zaměřit úsilí na záležitosti představující zvýšené riziko z hlediska ochrany osobních údajů. To neznamená, že by měli zanedbávat monitorování souladu u operací zpracování, u kterých je srovnatelně menší riziko, pouze upozorňuje, že prvotně by se měli zaměřovat na oblasti s rizikem vyšším.

Tento výběrový a pragmatický přístup by měl pověřencům pomoci při poskytování rad správci ve věci, jakou metodiku použít při provádění posouzení vlivu, které oblasti by měly být předmětem vnitřního nebo externího auditu, jaká interní školení poskytnout zaměstnancům nebo členům vedení zodpovědným za zpracovatelské činnosti a kterým operacím zpracování věnovat více času a zdrojů.

4.5. Role pověřence při vedení záznamů

Článek 30, odst. 1 a 2 stanoví, že správce nebo zpracovatel, nikoliv pověřenec, *„vede záznamy o činnostech zpracování, za něž zodpovídá“* nebo *„vede záznamy o všech kategoriích činností prováděných pro správce“*.

Pověřenci ve své praxi často vytváří přehledy a vedou registr operací zpracování na základě informací od různých oddělení jejich organizace, zodpovědných za zpracování osobních údajů. Tato praxe se ustálila podle mnoha současných národních zákonů a podle pravidel ochrany dat, kterými se řídí instituce a subjekty EU.[37]

Článek 39, odst. 1 obsahuje výčet úkolů pověřence v minimálně požadovaném rozsahu. Nic tedy nebrání správci nebo zpracovateli, aby pověřence zaúkolovali vedením záznamů o činnostech zpracování, za něž odpovídají. Takové záznamy by měly být považovány za jeden z nástrojů umožňující pověřenci plnit úkoly spočívající v monitorování souladu a informování a poskytování poradenství správci nebo zpracovateli.

Záznamy vedené podle článku 30 by také měly být brány jako nástroj umožňující správci nebo dozorovému úřadu získat na vyžádání přehled všech činností zpracování osobních údajů

[37] Článek 24, odst. 1, písm. d), Nařízení (ES) 45/2001.

v organizaci prováděných. Jsou tedy předpokladem dosažení právního souladu a jako takové i účinným opatřením směrem k odpovědnosti.

5 PŘÍLOHA – VODÍTKA K POVĚŘENCŮM: CO POTŘEBUJETE VĚDĚT

Tato příloha má organizacím poskytnout jednoduché a snadno srozumitelné odpovědi na některé klíčové otázky související se jmenováním pověřence pro ochranu osobních údajů, jak nově požaduje Obecné nařízení o ochraně osobních údajů.

Jmenování pověřence

1 Které organizace musí jmenovat pověřence?

Jmenovat pověřence je povinné, pokud:

- zpracování provádí orgán veřejné moci či veřejný subjekt (bez ohledu na to, jaká data jsou zpracovávána)
- hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Navíc, právo Unie nebo členských států může vyžadovat jmenování pověřence také v dalších situacích. I v případech, kdy Obecné nařízení nevyžaduje jmenování pověřence, mohou organizace dojít k rozhodnutí, že dobrovolné ustavení pověřence bude užitečné. WP29 takovou dobrovolnou iniciativu podporuje. Pokud organizace jmenuje pověřence dobrovolně, platí pro jeho jmenování, postavení a úkoly stejné požadavky jako kdyby byl ustaven povinně.

Zdroj: Obecné nařízení, článek 37, odst. 1

2 Co se rozumí pojmem „hlavní činnosti“?

Za „hlavní činnosti“ lze považovat klíčové operace směřující k dosažení cílů správce nebo zpracovatele. Sem také patří veškeré aktivity, kde zpracování dat je nedílnou součástí činnosti správce nebo zpracovatele. Například zpracování zdravotních dat, jako jsou zdravotní záznamy pacienta, by mělo být považováno za jednu z hlavních činností a nemocnice tak musí jmenovat pověřence.

Na druhé straně, všechny organizace vykonávají určité podpůrné činnosti, kupříkladu vyplácení zaměstnanců nebo standardní podporu výpočetní a informační techniky. Jde o nezbytné funkce podporující hlavní činnost nebo podnikání organizace. Byť nutné nebo podstatné, jsou tyto činnosti považovány spíše za pomocné funkce, než za klíčovou aktivitu.

Zdroj: Obecné nařízení, článek 37, odst. 1, písm. b) a c)

3 Co znamená „rozsáhlý“?

Obecné nařízení nedefinuje pojem rozsáhlé zpracování. WP29 doporučuje při určování, zda zpracování je rozsáhlé, vzít v úvahu zejména následující faktory:

- počet dotčených subjektů údajů – buď v absolutním vyjádření nebo podílem na relevantní populaci
- objem zpracovávaných dat a/nebo rozsah datových položek
- doba trvání nebo nepřetržitost zpracovatelské činnosti
- územní rozsah zpracovatelské činnosti

Příklady rozsáhlého zpracování:

- zpracování údajů o pacientech v rámci běžné činnosti nemocnice
- zpracování cestovních dat jednotlivců používajících městskou hromadnou dopravu (např. sledování prostřednictvím čipové tramvajenky)
- zpracování údajů o aktuální zeměpisné poloze zákazníků mezinárodních řetězců rychlého občerstvení pro statistické účely zpracovatelem zaměřeným na tuto činnost
- zpracování zákaznických dat v rámci běžné obchodní činnosti pojišťovny nebo banky
- zpracování osobních údajů vyhledávačem pro potřeby behaviorální reklamy
- zpracování dat (o obsahu, provozních, lokalizačních) poskytovatelem telefonních a internetových služeb

Příklady zpracování, která nejsou rozsáhlá:

- zpracování údajů o pacientech jednotlivým lékařem
- zpracování osobních údajů týkající se rozsudků v trestních věcech a trestných činů individuálním právníkem

Zdroj: Obecné nařízení, článek 37, odst. 1, písm. b) a c)

4 Co znamená „pravidelné a systematické monitorování“?

Pojem pravidelné a systematické monitorování subjektů údajů Obecné nařízení nedefinuje, jasně však tento výraz zahrnuje všechny formy sledování a profilování na internetu, i pro účely behaviorální reklamy. Pojem monitorování není ovšem omezen pouze na prostředí online.

Příklady činností, které mohou zakládat pravidelné a systematické monitorování subjektů údajů: provozování telekomunikační sítě; poskytování telekomunikačních služeb; cílení internetové reklamy pomocí e-mailového retargetingu, marketing řízený daty, profilování a bodování (skórování) pro účely posouzení rizik (např. pro účely hodnocení úvěrového rizika, stanovení výše pojistného, předcházení podvodům, odhalování praní špinavých peněz), sledování polohy, například u mobilních aplikací; věrnostní programy; behaviorální reklama; sledování zdravého životního stylu, tělesné kondice a zdravotních dat pomocí na těle nositelných zařízení, kamerové systémy, propojená zařízení, např. chytré měřiče, chytrá auta, inteligentní domy (domotika), atd.

WP29 vykládá slovo „pravidelný“ jednou nebo kombinací více následujících charakteristik:

- průběžný nebo v pravidelných intervalech a po určitou dobu se opakující
- stále se opakující nebo opakovaný ve stanovených časech
- neustále nebo pravidelně se vyskytující

WP29 vykládá slovo „systematický“ jednou nebo kombinací více následujících charakteristik:

- vyskytující se podle určitého systému
- přednastavený, organizovaný nebo metodický
- uskutečňující se jako součást obecného plánu pro sběr dat
- vykonávaný jako součást strategie

Zdroj: Obecné nařízení, článek 37, odst. 1, písm. b)

5 Mohou organizace jmenovat pověřence společně? Pokud ano, za jakých podmínek?

Ano. Skupina podniků může jmenovat jediného pověřence, pokud bude *„snadno dosažitelný z každého podniku“*. Pojem dosažitelnost se vztahuje k úkolům pověřence coby kontaktního místa pro subjekty údajů, dozorové úřady a platí také interně, uvnitř organizace. Pro zabezpečení dosažitelnosti pověřence, interního nebo externího, je důležité zajistit dostupnost jeho kontaktních údajů. Pověřenec, pokud nutno s pomocí týmu, musí být schopen účinně

komunikovat se subjekty údajů a spolupracovat s dotčenými dozorovými orgány. To znamená, že komunikace musí probíhat v jazyce nebo jazycích užívaných dotčenými dozorovými orgány a subjekty údajů. Dosažitelnost pověřence (fyzicky na stejném pracovišti jako zaměstnanci, přes horkou linku nebo bezpečné komunikační prostředky) je zásadní pro zajištění, že subjekty údajů budou schopny pověřence kontaktovat.

Jediný pověřenec může být jmenován pro několik orgánů veřejné moci nebo veřejných subjektů s přihlédnutím k jejich organizační struktuře a velikosti. Pro zdroje a komunikaci platí stejná kritéria. Vzhledem k tomu, že pověřenec má rozmanité úkoly, musí správce nebo zpracovatel zajistit, aby je jediný pověřenec, pokud nutno s pomocí týmu, mohl vykonávat efektivně i navzdory skutečnosti, že byl jmenován pro několik orgánů veřejné moci nebo veřejných subjektů.

Zdroj: Obecné nařízení, článek 37, odst. 2 a 3

6 Kde má pověřenec sídlit?

WP29 doporučuje, jako obecné pravidlo, aby pověřenec v zájmu dosažitelnosti sídlil v Evropské unii, bez ohledu, zda správce nebo zpracovatel je v Evropské unii usazen. Nelze však vyloučit, že v některých situacích, kdy správce nebo zpracovatel nebude mít provozovnu v Evropské unii, může pověřenec vyvíjet činnost účinněji, pokud bude sídlit mimo EU.

7 Lze jmenovat externího pověřence?

Ano. Pověřencem může být pracovník správce nebo zpracovatele (interní pověřenec) nebo může úkoly plnit na základě smlouvy o poskytování služeb. To znamená, že pověřencem může být externista a v takovém případě vykonává svoji funkci na základě smlouvy o poskytování služeb uzavřené s jednotlivcem nebo organizací.

Vykonává-li funkci pověřence externí poskytovatel, pak úkoly pověřence mohou být plněny týmově jednotlivci pracujícími pro daného externistu, přičemž odpovědnost nese určená vedoucí kontaktní osoba pověřená péčí o klienta. V tomto případě je nezbytné, aby každý člen externí organizace vykonávající funkci pověřence plnil všechny příslušné požadavky Obecného nařízení.

V zájmu právní jasnosti a dobré organizace a také kvůli prevenci konfliktu zájmů se doporučuje mít ve smlouvě o poskytování služeb jasné rozdělení úkolů v rámci týmu externího pověřence a ustanovit jednu určitou osobu jako hlavní kontakt pověřený péčí o klienta.

Zdroj: Obecné nařízení, článek 37, odst. 6

8 Jaké profesní kvality by pověřenec měl mít?

Pověřenec musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly.

Potřebná úroveň odborných znalostí by měla být určena v závislosti na prováděných zpracovatelských operacích a požadované ochraně zpracovávaných osobních údajů. Pokud například je zpracovatelská činnost zvláště složitá nebo je prováděna s velkým množstvím citlivých údajů, bude pověřenec potřebovat znalosti a podporu na vyšší úrovni.

Mezi důležité dovednosti a zkušenosti patří:

- znalost národního a unijního práva v oblasti ochrany dat a praktické zkušenosti včetně hluboké znalosti Obecného nařízení
- znalost prováděných zpracovatelských operací
- znalost informačních technologií a bezpečnosti dat

- znalost dané oblasti podnikání a organizace
- schopnost propagovat kulturu ochrany dat v organizaci

Zdroj: Obecné nařízení, článek 37, odst. 5

Postavení pověřence

9 Jaké zdroje by správce nebo zpracovatel měl pověřenci poskytnout pro plnění úkolů?

Pověřenec musí mít zdroje potřebné k výkonu svých úkolů.

V závislosti na povaze zpracovatelských operací a činností a velikosti organizace jsou zdroje, které by pověřenec měl mít k dispozici, následující:

- aktivní podpora ze strany vyššího managementu
- dostatek času k plnění úkolů
- odpovídající podpora finanční, technická (kancelářské prostory, vybavení, zařízení) a personální pokud je potřeba
- oficiální oznámení o jmenování pověřence všem zaměstnancům
- přístup do jiných útvarů v organizaci, aby měl pověřenec nezbytnou podporu a informace z těchto útvarů
- průběžné školení

Zdroj: Obecné nařízení, článek 38, odst. 2

10 Jaké jsou záruky umožňující pověřenci plnit úkoly nezávislým způsobem? Co znamená „konflikt zájmů“?

Existuje několik záruk umožňujících pověřenci konat nezávisle:

- žádné pokyny od správce nebo zpracovatele týkající se výkonu úkolů pověřence
- nemožnost propuštění nebo sankcionování v souvislosti s plněním úkolů
- zajištění správcem nebo zpracovatelem, aby žádné pověřencovy úkoly nebo povinnosti nevedly ke střetu zájmů

Jiné úkoly pověřence nesmějí vést ke konfliktu zájmů. V první řadě to znamená, že pověřenec nemůže v organizaci zastávat místo, na kterém by musel stanovovat účely a prostředky zpracování osobních údajů. Vzhledem k organizační struktuře specifické pro každou organizaci, je potřeba tuto otázku řešit případ od případu.

V konfliktním postavení uvnitř organizace mohou typicky být pozice ve vyšším managementu (výkonný ředitel, provozní ředitel, finanční ředitel, zdravotní ředitel, vedoucí marketingového oddělení, vedoucí personálního oddělení nebo vedoucí oddělení IT), ale i pozice na nižším stupni organizační struktury, pokud v takovém postavení dochází k rozhodování o účelech a prostředcích zpracování. Konflikt zájmů může také kupříkladu vzniknout, pokud externí pověřenec bude požádán o zastupování správce nebo zpracovatele před soudem v případě týkajícím se ochrany osobních údajů.

Zdroj: Obecné nařízení, článek 38, odst. 3 a článek 38, odst. 6

Úkoly pověřence

11 Co znamená „monitorování souladu“?

Pověřenec, v rámci svých povinností, může zejména:

- shromažďovat informace za účelem zjišťování zpracovatelských činností
- analyzovat a prověřovat právní soulad zpracovatelských činností
- informovat, radit a vydávat doporučení správci nebo zpracovateli

Zdroje: Obecné nařízení, článek 39, odst. 1, písm. b)

12 Je pověřenec osobně odpovědný v případě nesouladu s požadavky ohledně ochrany osobních údajů?

Ne. Pověřenci nejsou osobně odpovědni za nesoulad s požadavky ochrany osobních údajů. Je to správce nebo zpracovatel, kdo musí zajistit a doložit, že zpracování probíhá ve shodě s Obecným nařízením. Dodržování předpisů pro ochranu osobních údajů je odpovědností správce nebo zpracovatele.

13 Jaká je role pověřence v souvislosti s posudky vlivu na ochranu osobních údajů a se záznamy o činnostech zpracování?

Pokud jde o posouzení vlivu na ochranu osobních údajů, správce nebo zpracovatel by si měl nechat pověřencem poradit, mimo jiné v následujících věcech:

- zda je potřeba, případně není potřeba, vypracovat posouzení vlivu na ochranu osobních údajů (dále jen „posouzení vlivu“)
- jakou metodiku při zpracování posouzení vlivu uplatnit
- zda posouzení vlivu vypracovat vlastními silami nebo jeho zpracování zadat externě
- jaká ochranná opatření (včetně technických a organizačních) uplatnit pro zmírnění rizik vůči právům a zájmům subjektů údajů
- zda posouzení vlivu bylo zpracováno správně a zda jeho závěry (ať už vedou či ne k pokračování zpracovatelské operace a bez ohledu na to, jaká ochranná opatření určují uplatnit) jsou v souladu s požadavky na ochranu osobních údajů

V případě záznamů o činnostech zpracování má povinnost vést záznamy o zpracovatelských operacích správce nebo zpracovatel, nikoliv pověřenec. Nic ovšem nebrání správci nebo zpracovateli, aby pověřenci zadal úkol vést záznamy o operacích zpracování, přičemž odpovědnost nese správce nebo zpracovatel. Tyto záznamy by měly být chápány jako jeden z nástrojů umožňující pověřenci vykonávat úkoly spočívající v monitorování souladu, informování a poskytování rad správci nebo zpracovateli.

Zdroj: Obecné nařízení, článek 39, odst. 1, písm. c) a článek 30

V Bruselu dne 13. prosince 2016

Za pracovní skupinu
předsedkyně
Isabelle FALQUE-PIERROTIN

Posledně revidováno a schváleno 5. dubna 2017

Za pracovní skupinu
předsedkyně
Isabelle FALQUE-PIERROTIN

B. Příklad DPIA

Tato příloha obsahuje konkrétní ukázku, jak provést DPIA na základě připraveného vzoru.

itemize

Posouzení vlivu zpracování na ochranu osobních údajů (DPIA)

Datum zpracování DPIA	26.11.2018
Označení revize DPIA	1
Kdo DPIA zpracoval	Leoš Ševčík
Důvod zpracování DPIA	Výzkumný projekt zpracovává data zvláštní kategorie dle GDPR čl. 9 ve velkém objemu
Datum příští revize	26.11.2019

Pozn. Kurzívou jsou označeny instruktážní popisky, které autor DPIA nahradí vlastním textem

Informace o zpracování

Základní informace o zpracování

Označení projektu/procesu zpracování OÚ	RESEARCH-2013-01 Alzheimer
Osoba/pracoviště odpovědná za zpracování OÚ	*Vedoucí výzkumného týmu Neuro; centrální data manažer Nemocnice*
Účel zpracování OÚ	Zjistit rizikové faktory a časné příznaky Alzheimerovy choroby a dalších neuro-degenerativních onemocnění mozku. Dalším cílem je výběr preventivních opatření, která by mohla tato onemocnění ovlivnit a postupů pro lepší plánování léčby pacientů s těmito onemocněními
Právní základ zpracování OÚ	Souhlas subjektu (součástí informovaného souhlasu) Veřejný zájem (projekt hrazen z veřejných zdrojů, příjemce je výzkumná organizace)

Popis subjektů údajů a osobních údajů

Kdo je subjektem údajů?	Pacienti Nemocnice, kteří souhlasili s účastí ve studii
V jakém vztahu jsou subjekty údajů vůči správci?	Pacienti
Jaký je předpokládaný počet subjektu údajů?	600

Jaké osobní údaje budou zpracovávány?	• **Osobní a rodinná anamnéza**: jméno, příjmení, pohlaví, rok narození, vzdělání, povolání, trvalý pobyt, pobírání důchodu, rodinný stav
	• **Klinická data**: podrobné klinické údaje z neurologických a neuropsychologických vyšetření, Genetická data (APOE 4, TOMM 40)
	  ○ Odběry krve a mozkomíšního moku
	  ○ Zobrazovací metody MRI, PET, ultrazvuk cév
	Detailně v Data dictionary, které je přílohou dokumentu

Je rozsah osobních údajů přiměřený, relevantní a omezený ve vztahu k účelu zpracování?	Ano. Veškerá sbíraná data jsou v rámci projektu využívána pro vyhodnocování rizikových faktorů a dalších cílů výzkumu.

Popis operací zpracování

Zdroj osobních údajů	*Subjekt údajů*
Způsob získání osobních údajů	Výzkumník/zdravotník zaznamenává údaje prvotně do zdravotnické dokumentace na základě rozhovoru se subjektem, dotazníků vyplněných subjektem a výsledků vyšetření. Data následně vkládá do výzkumné databáze v pseudonymizované podobě.
Kde a jakým způsobem jsou osobní údaje uloženy	Databáze: - nemocniční virtuální server; SW REDCap, - Již anonymizovaná (bez jména, příjmení, rodného čísla a data narození) Podpůrná výzkumná dokumentace: - pseudonymizační klíče (pseudonym s namapovanými identifikátory, které byly odstraněny z výzkumné databáze) v papírové i elektronické podobě v místnosti a na zálohovaném PC výzkumného týmu; - listinná studijní dokumentace v zabezpečené příruční registratuře týmu Zdravotnická dokumentace: - zdravotnická dokumentace elektronicky v NIS (nemocniční virtuální server) - zdravotnická listinná dokumentace v kartotéce neurologické ambulance centra pro kognitivní poruchy
Účastníci podílející se na zpracování osobních údajů	- členové nemocničního výzkumné týmu Neuro (zaměstnanci Nemocnice) - pracovníci neurologické ambulance centra pro kognitivní poruchy (zaměstnanci Nemocnice)
Předání údajů – zajištění zákonnosti předání, záruky při přeshraničním zpracování	Data jsou předávána spolupracujícím Univerzitě v pseudonymizované podobě (bez jména, příjmení, rodného čísla a data narození). Předání pokryto smlouvou mezi dvěma samostatnými správci a v souladu s informovaným souhlasem (obsahujícím také souhlas se zpracováním OÚ)
Doba zpracování OÚ	Do doby využitelnosti dat pro výzkumné účely. Probíhá pravidelné roční přezkoumání výzkumné hodnoty dat.
Jak je zajištěna přesnost a aktuálnost dat?	Demografická data poskytuje subjekt; klinická pochází z validovaných a kalibrovaných metod. Kontinuální aktuální není pro účel zpracování nutná.
Způsob naložení s OÚ po zániku studie	Po zániku studie budou zničeny pseudonymizační klíče. Každé tři roky pak bude vyhodnocována dostatečnost takové anonymizace.

Popis organizačních a technických opatření

Použité SW, HW a jiné prostředky (plánované nebo existující)	Viz řízená dokumentace SOP_IT_02 Pravidla správy datové sítě nemocnice Viz řízená dokumentace SOP_DM_01 Databázová řešení klinického výzkumu Viz dokumentace konfigurace manažera databázového řešení REDCap (dle SOP_DM_01 na sdíleném disku NAS\DM\REDCap Viz řízená dokumentace SOP_HC_03 Zdravotnická dokumentace
Jak je zajištěna pseudonymizace či anonymizace?	Výzkumná sestra ve fázi sběru dat vytvoří pseudonymizační klíče (v papírové i elektronické podobě v místnosti a na zálohovaném PC výzkumného týmu) na jméno, příjmení, rodné číslo, datum narození a pseudonym (ID) subjektu. - Přístup má výzkumná sestra a vedoucí pracoviště Výzkumná databáze i exportované datasety již výše uvedené identifikátory neobsahují. Pro každý export z databáse se tvoří nové ID subjektu, tj. Provede opětovnou pseudonymizaci. Odpovědný datamanažer v elektronické podobě eviduje export specifické ID vs. Originální ID. - Přístup má centrální datamanažer
Jakým způsobem jsou OÚ případně předávány z primární databáze jiným správcům či zpracovatelům, popř. zaměstnancům bez přístupu do primární databáze?	Data se předávají způsobem: 1) z výzkumné databáze: Export datasetu, zašifrování datasetu, upload na FNUSA onecloud, emailem odeslání příjemci odkaz na úložiště, odeslání SMS příjemci s heslem 2) DICOM snímky: použití anonymizačního modulu SW TomoCon Viewer a odstranění identifikátorů (jména, příjmení, rodného čísla a data narození, kontaktní údaje), dále jak v případě výzkumné databáze. Datamanažer studie do databáze eviduje s jakou organizací, kdy a za jakým účelem byla data sdílena.
Jak budou řešeny bezpečnostní incidenty?	Nemocnice má svoji DPO, která je příjemcem stížnosti. Postup se řídí řízenou dokumentací SOP_DM_05 Ochrana osobních údajů v nemocnici

Implementace práva subjektu

Jak jsou/budou subjekty údajů informováni o daném zpracování?	Informace o účelu a správci viz Informovaný souhlas s účastí ve studii Další informace na webu nemocnice v sekci Ochrana osobních údajů
Jak je zajištěn souhlas subjektů? (pouze pokud aplikovatelné)	Informovaný souhlas obsahuje také právní důvod - souhlas se zpracováním OÚ

Jak je zajištěno právo na přístup subjektu a přenositelnost OÚ?	Instrukcemi na webu nemocnice v sekci Ochrana osobních údajů. Proces probíhá viz řízená dokumentace SOP_DM_05 Ochrana osobních údajů v nemocnici. Data jsou ve strojově čitelné a dokumentované podobě a v případě splnění zákonných požadavků je lze ze systému exportovat a poskytnout.
Jak je zajištěno právo na opravu a výmaz?	Instrukcemi na webu nemocnice řízená dokumentace SOP_DM_05 Ochrana osobních údajů v nemocnici.
Jak je zajištěno právo na omezení zpracování a podání námitky?	Instrukcemi na webu nemocnice Interně se proces řídí viz řízená dokumentace SOP_DM_05 Ochrana osobních údajů v nemocnici.

Posouzení rizik

Hrozba	Možné důsledky
Neoprávněný přístup	a) identifikaci jednotlivců na základě korelace s jinými databázemi, b) využití dat pro jiné účely než umožňuje informovaný souhlas, c) nežádoucí úpravy
Nežádoucí modifikace	může vyústit v a) ohrožení subjektu/pacienta na zdraví vlivem nevhodné léčby, b) nedůvěryhodnosti výsledků vědeckého výzkumu, c) ztrátu dat.
Zánik dat	by představoval a) ohrožení zdraví pacienta, b) částečnou nebo úplnou ztrátu práce výzkumného týmu, potažmo mrhání veřejnými prostředky, c) nelegitimnost zpracování osobních údajů (v případě ztráty informovaných souhlasů).

Výčet prvků systému zpracování (většinou SW aplikace, listinné dokumenty, vzorky, snímky, …)	**Identifikace opatření** Způsob reakce na výše identifikované hrozby.
NIS	zdrojová část dat se nachází ve zdravotnické dokumentaci, vč. její elektronické podoby. Přístup do NIS přes LDAP heslo pouze pro zdravotnické pracovníky nemocnice. Pracovníci proškoleni v používání hesla. Heslo vydáváno oproti identifikaci občanským průkazem či pasem.

	Veškerá data jsou denně zálohována (replikace), loguje se historie změn.
Listinná zdravotnická dokumentace	zdrojová část dat se nachází ve zdravotnické dokumentaci, vč. její listinné podoby (zdravotníci zapisují do NIS a záznamy tisknou a ručně podepisují). Dokumentace je vedena v uzamykatelné vyšetřovně, pod klíčovým režimem.
SW REDCAP	přístup do Redcapu pouze proškoleným zaměstnancům nemocnice aktivně se účastnící studie. Výzva k nastavení hesla zasílána na služební email. Heslo aplikace si uživatel nastavuje v aplikaci. Síla hesla je požadovaná dle pravidel pro LDAP hesla. Veškerá data jsou denně zálohována (replikace), loguje se historie změn.
Listinné „study-specific“ dokumenty	informované souhlasy a pseudonymizační klíče uloženy v příruční registratuře týmu, přístup do místnosti na zámek, zaveden klíčový režim dle interní směrnice.
Elektronické „study-specific“ dokumenty	pseudonymizační klíče uloženy v dokumentu na pracovním PC na lokálním disku členky týmu. PC je chráněn firewallem, (PC s aktualizovaným antivirem). Uživatelé PC seznámeni se základními pravidly chování na vnitřní síti i internetu. PC je připojen na internet. Pro přihlášení na PC je požadováno heslo. PC je v pracovně týmu, přístup do místnosti na zámek, zaveden klíčový režim dle interní směrnice.
Biologické vzorky	vzorky jsou uloženy s označením rodného čísla subjektu pro vyšetření v nemocnici, uložení je v mrazákovně s přístupem na chip (s centrálním logem osob, které odemkli místnost), kde přístup zajišťuje pouze vrchní sestra výzkumného úseku dle klíčového režimu pro veškeré týmy výzkumného úseku. Mrazáky jsou uzamykatelné, ale ne zamčené. Pro vyšetření vzorků mimo nemocnici výzkumná sestra štítky označují pouze ID subjektu, které přiděluje REDCap. Míšní likvor i krevní plazma jednoho subjektu jsou rozděleny do cca 20ti samostatných zkumavek. Vzorky se nacházejí v jednom mrazáku na elektrickém obvodu se náhradním zdrojem, monitoringem teplot a hlášením poklesu teplot.
Snímky zobrazovacích metod (MRI, CT, PET, ultrazvuk)	Snímky zobrazovacích metod (MRI, CT, PET, ultrazvuk) – součásti systému PACS ve formátu DICOM. Přístup k PACS viewer skrze centrální nemocniční heslo LDAP. PACS server je zálohovaný, přístup k němu omezen pouze na centrální administrátory, fyzicky zabezpečen jako ostatní klíčové prvky datové sítě. Pro zobrazení snímku uživatelem se stahují na jeho lokální disk. V případě nutnosti přenosu dat se de-identifikují a šifrují.

Vyhodnocení rizik se provedlo pro jednotlivé hrozby a prvky zpracování. Pro každou hrozbu prvku se vyhodnotila pravděpodobnost výskytu a závažnost dopadu, jejichž součin tvoří výsledný skór rizika, viz:

Skór rizika	**pravděpodobnost výskytu**

závažnost	1	2	3
3	3	6	9
2	2	4	6
1	1	2	3

Dle skóru rizik se přijme vhodná reakce, viz:

Skór rizika		Reakce
nízké 1-2		Riziko akceptováno
Střední 3-4		Riziko možno akceptovat. Management rozhoduje o nápravném opatření.
Vysoké 6-9		Management musí přijmout nápravné opatření.

Hrozba: Neoprávněný přístup k datům

- prvek systému zpracování: *NIS*

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

- prvek systému zpracování: Listinná zdravotnická dokumentace

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

- prvek systému zpracování: REDCap

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

- prvek systému zpracování: Listinné „study-specific“ dokumenty

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

- prvek systému zpracování: Elektronické „study-specific“ dokumenty

pravděpodobnost výskytu	*2*
závažnost dopadu	*2*
výsledný skór	*4*

- prvek systému zpracování: Vzorky

pravděpodobnost výskytu	*2*
závažnost dopadu	*3*
výsledný skór	*6*

- prvek systému zpracování: snímky zobrazovacích metod

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

Hrozba: Nežádoucí úpravy dat

- prvek systému zpracování: *NIS*

pravděpodobnost výskytu	*1*
závažnost dopadu	*2*
výsledný skór	*2*

- prvek systému zpracování: Listinná zdravotnická dokumentace

pravděpodobnost výskytu	*1*
závažnost dopadu	*2*
výsledný skór	*2*

- prvek systému zpracování: REDCap

pravděpodobnost výskytu	*1*
závažnost dopadu	*2*
výsledný skór	*2*

- prvek systému zpracování: Listinné „study-specific“ dokumenty

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

- prvek systému zpracování: Elektronické „study-specific“ dokumenty

pravděpodobnost výskytu	*2*
závažnost dopadu	*3*
výsledný skór	*6*

- prvek systému zpracování: Vzorky

pravděpodobnost výskytu	*2*
závažnost dopadu	*3*
výsledný skór	*6*

- prvek systému zpracování: snímky zobrazovacích metod

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

Hrozba: Zánik dat

- prvek systému zpracování: *NIS*

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

- prvek systému zpracování: Listinná zdravotnická dokumentace

pravděpodobnost výskytu	*1*

závažnost dopadu	*3*
výsledný skór	*3*

- prvek systému zpracování: REDCap

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

- prvek systému zpracování: Listinné „study-specific“ dokumenty

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

- prvek systému zpracování: Elektronické „study-specific“ dokumenty

pravděpodobnost výskytu	*2*
závažnost dopadu	*3*
výsledný skór	*6*

- prvek systému zpracování: Vzorky

pravděpodobnost výskytu	*2*
závažnost dopadu	*3*
výsledný skór	*6*

- prvek systému zpracování: snímky zobrazovacích metod

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

Zhodnocení stávajících technických a organizačních opatření:

Většina opatření se jeví jako dostatečná. V případě zabezpečení vzorků a elektronických study-specific dokumentů bude doporučeno posílení opatření na ochranu OÚ.

Elektronické „study-specific“ dokumenty: pracovní stanice s uloženými pseudonymizačními klíči je potenciálním rizikem, jelikož se využívá primárně při poskytování zdravotních služeb, může se na něm střídat více pracovníků a je zároveň připojený k veřejnému internetu.

Vzorky: jsou uloženy v zabezpečeném prostoru, nicméně různé výzkumné týmy mohou mít neoprávněný přístup k vzorkům, které v řadě případů jsou označeny rodným číslem a nelze je tudíž považovat ani za pseudonymní.

Návrh případných nových technických a organizačních opatření a jejich dopadů:

Elektronické „study-specific“ dokumenty: pseudonymizační klíče umístit na sdílený disk na serveru nemocnice s řízeným přístupem, omezeným pouze pro pověřené pracovníky.

Vzorky: zavést klíčový režim pro mrazáky jednotlivých týmů a uskladňovat vzorky již pod pseudonymizačním ID.

Po zavedení tohoto opatření lze snížit skóry rizika, viz:

Hrozba: Neoprávněný přístup k datům

- prvek systému zpracování: Elektronické „study-specific“ dokumenty

pravděpodobnost výskytu	*1*
závažnost dopadu	*2*
výsledný skór	*2*

- prvek systému zpracování: Vzorky

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

Hrozba: Nežádoucí úpravy dat

- prvek systému zpracování: Elektronické „study-specific“ dokumenty

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

- prvek systému zpracování: Vzorky

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

Hrozba: Zánik dat

- prvek systému zpracování: Elektronické „study-specific“ dokumenty

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

- prvek systému zpracování: Vzorky

pravděpodobnost výskytu	*1*
závažnost dopadu	*3*
výsledný skór	*3*

Porovnání a zhodnocení variant jednotlivých opatření:

Nejsou navrženy variantní řešení.

Dokumentace a demonstrace souladu

Viz řízená dokumentace SOP_IT_02 Pravidla správy datové sítě nemocnice

Viz řízená dokumentace SOP_DM_01 Databázová řešení klinického výzkumu

Viz dokumentace konfigurace manažera databázového řešení REDCap (dle SOP_DM_01 na sdíleném disku NAS\DM\REDCap

Viz řízená dokumentace SOP_HC_03 Zdravotnická dokumentace

Viz řízená dokumentace SOP_DM_05 Ochrana osobních údajů v nemocnici.

viz Informovaný souhlas s účastí ve studii

viz Další informace na webu nemocnice

Zohlednění posudku pověřence

Stručné shrnutí posudku pověřence (viz příloha) a jeho případných doporučení.

Pověřenec podpořil návrhy opatření a neměl další doporučení.

Konzultace s dozorovým úřadem

Nebyl

Přílohy

Data Dictionary

Informovaný souhlas

Posudek pověřence