Související literatura:

NONNEMANN, F. Náležitosti souhlasu se zpracováním osobních údajů. *Právní rozhledy*, 2011, roč. 19, č. 9, s. 520.

NONNEMANN, F. Odvolání souhlasu se zpracováním osobních údajů. *Právní rozhledy*, 2011, roč. 19, č. 24, s. 871.

Názory a rozhodovací praxe ÚOOÚ:

stanovisko ÚOOÚ č. 4/2013 – K pojetí zpracování osobních údajů

stanovisko ÚOOÚ č. 3/2012 – K pojmu osobní údaj (ve znění aktualizovaném v únoru 2014)

Stanoviska WP29:

WP 136, Opinion 4/2007 on the concept of personal data, adopted on 20th June 2007

WP 169, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010

KAPITOLA II
Zásady

Článek 5
Zásady zpracování osobních údajů

1. Osobní údaje musí být:

a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“);

b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely („účelové omezení“);

c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“);

d) přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny („přesnost“);

e) uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, a to za předpokladu provedení příslušných technických a organizačních opatření po-

žadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů („omezení uložení“);

f) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („integrita a důvěrnost“);

2. Správce odpovídá za dodržení odstavce 1 a musí být schopen toto dodržení souladu doložit („odpovědnost“).

K čl. 5

Základní zásady zpracování jsou do GDPR převzaty bez podstatných změn ze směrnice 95/46/ES. Nově je doplněn pouze princip odpovědnosti dle čl. 5 GDPR, který zdůrazňuje odpovědnost správce nejen za dodržení GDPR ale i za doložení souladu svých činností s požadavky GDPR.

Základní zásady pochází již ze směrnice OECD o ochraně soukromí a přeshraničních tocích osobních údajů z roku 1980 a dále ze směrnice 95/46/ES v čl. 6.[1]

Předchozí úprava v ZOOÚ neobsahovala výčet principů, ale stejné principy v něm byly obsaženy ve formě obdobných povinností pro správce.

Kontinuitu základních principů potvrzuje i ZOOÚ v následujícím vyjádření: *„Je nutné zdůraznit, že základní zásady, principy a klíčové instrumenty zůstávají de facto neměnné, resp. byly detailněji pouze rozpracovány a zpřesněny (např. nutnost disponovat pro zpracování právním důvodem, zabezpečení osobních údajů, transparentnost vůči subjektu údajů atd.)“*.[2]

Zásady zpracování dle čl. 5 GDPR jsou nejen obecnými interpretačními principy pro ostatní ustanovení GDPR ale přímo vynutitelnými ustanoveními, jejichž porušení podléhá sankci dle čl. 83 odst. 5 písm. a) GDPR. K tomu je však třeba uvést, že pokud správce poruší některé konkrétní ustanovení GDPR a zároveň stejným jednáním i některou ze zásad uvedených v čl. 5 GDPR, bude se na případné sankce vztahovat omezení kumulace sankcí dle čl. 83 odst. 3 GDPR.

Odpovědnost za dodržení zásad zpracování nese podle čl. 5 odst. 2 GDPR správce, nikoli zpracovatel. Lze se tedy domnívat, že i pokud by zpracovatel porušil např. zásadu integrity a důvěrnosti dle čl. 5 odst. 2. písm. f) GDPR, odpovědnost za toto porušení ponese správce.

---

[1] Part Two of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; čl. 6 směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

[2] Úřad pro ochranu osobních údajů. Nové přístupy a povinnosti [online]. Dostupné z: https://www.uoou.cz/2-nove-p-istupy-a-povinnosti/d-27268.

K odst. 1

K písm. a) (zákonnost, korektnost, transparentnost)

Oproti čl. 6 odst. 1 písm. a) směrnice 95/46/ES přidává GDPR požadavek zpracovávání *transparentním způsobem*.

Zásada zákonnosti se nejvýznamněji projevuje v čl. 6 a čl. 9 GDPR. Zásady korektnosti a transparentnosti se nejvýznamněji projevují v čl. 12–22 GDPR.

Britský regulátor ICO shrnul následující požadavky na dodržení zásad zákonnosti a korektnosti zpracování:

- oprávněný důvod pro shromažďování a uchovávání údajů;
- správce nepoužívá údaje způsobem, který má neodůvodněné nepříznivé důsledky na subjekty údajů;
- transparentnost o tom, jak správce hodlá údaje využívat, prostřednictvím informací zpřístupněných subjektům údajů při převzetí údajů;
- zpracovávat osobní údaje způsobem, který mohou subjekty údajů rozumně očekávat;
- zajistit, že správce nenakládá s údaji nezákonným způsobem.[3]

V tomto shrnutí ICO je specificky uveden i princip zpracování na základě legitimního očekávání subjektů údajů. Tento princip není samostatnou zásadou GDPR a běžně se proto test legitimního očekávání subjektů údajů dle GDPR neprovádí. Lze se však domnívat, že tento test je podpůrně zahrnut v zásadě korektnosti zpracování. Z toho by mohlo vyplývat určité omezení pro zpracování na základě souhlasu dle čl. 6 odst. 1 písm. a) GDPR nebo zpracování na základě oprávněného zájmu dle odst. 6 písm. f) GDPR, kdy by zásada korektnosti zpracování omezovala možnost zpracování pro účely, které subjekt údajů nemohl legitimně očekávat. Test legitimního očekávání subjektů údajů je částečně také zahrnut v principu slučitelnosti údajů a požadavků na vyjádření účelu v rámci zásady účelového omezení dle čl. 5 odst. 1 písm. b) GDPR.

ICO také zdůrazňuje, že zásada korektnosti musí být splněna ve vztahu ke každému jednotlivému subjektů údajů, nestačí její splnění ve vztahu k většině subjektů údajů. Pokud je zpracování sice vůči většině subjektů údajů korektní, ale vůči některým subjektům údajů nekorektní, jedná se o porušení zásady zpracování podle čl. 5 odst. 1 písm. a) GDPR.[4] Tak by tomu mohlo být např. u zpracování na základě souhlasu, pokud by sice většina subjektů údajů souhlas udělila, ale s některými subjekty údajů by se správci nepodařilo spojit a rozhodl se zpracovávat jejich údaje bez souhlasu, protože se jedná o zanedbatelnou skupinu subjektů údajů.

---

[3] ICO. Processing personal data fairly and lawfully (Principle 1). Dostupné z: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/.

[4] Tamtéž.

K písm. b) (účelové omezení)

Oproti čl. 6 odst. 1 písm. b) směrnice 95/46/ES přidává GDPR možnost dalšího zpracování *pro účely archivace ve veřejném zájmu*.

Zásada účelového omezení požaduje, aby správce již při shromáždění údajů měl jasně stanoveno, pro jaký účel jsou údaje shromažďovány, a zároveň klade na tento účel konkrétní požadavky, a to konkrétně požadavek (i) určitosti, (ii) výslovného vyjádření a (iii) legitimního charakteru.

– Určitost účelu

Určitost účelu brání zejména tomu, aby správce shromažďoval osobní údaje, aniž by byl schopen přesně stanovit jejich budoucí využití. To klade požadavky zejména na plnění informační povinnosti dle čl. 13 odst. 1 písm. a) GDPR. Obecné účely jako „datová analytika", „budoucí využití" apod. budou v rozporu s tímto požadavkem určitosti účelu zpracování. I účel specifikovaný jako „marketingové účely" může být v rozporu s požadavkem určitosti účelu, zejména pokud z kontextu není zjevné, jaké formy marketingu správce provádí a pokud tyto formy nemůže subjekt údajů legitimně očekávat.

– Výslovné vyjádření účelu

Požadavek výslovného vyjádření především omezuje možnost implicitních účelů zpracování. Tento požadavek brání správci v argumentaci, že některé další účely byly implicitně obsaženy v účelu vyjádřeném např. v informační povinnosti dle čl. 13 odst. 1 písm. a) GDPR či v souhlasu subjektu údajů dle čl. 7 GDPR. Správce by tak např. nemohl tvrdit, že v účelu „zasílání marketingové komunikace" je implicitně zahrnuto i profilování subjektů údajů, aby tato marketingová komunikace byla efektivní. Takový další účel by měl být výslovně vyjádřen. To potvrzuje i WP29, která uvádí, že správci by neměli uvést jeden široký účel zahrnující řadu zpracovatelských operací, které s tímto účelem jen vzdáleně souvisí.[5]

WP29 k tomuto požadavku upřesňuje, že účel musí být vyjádřen takovým způsobem, aby byl srozumitelný nejen pro správce a zpracovatele, ale i pro dozorové orgány a dotčené subjekty údajů. Subjektům údajů musí být účel srozumitelný bez ohledu na jejich odlišné kulturní a jazykové zázemí, úroveň pochopení a specifické potřeby. WP29 zdůrazňuje, že správce přitom musí vzít v úvahu všeobecné chápání a rozumná očekávání subjektů údajů.[6] Specifické požadavky na srozumitelnost stanoví bod odůvodnění 58 ve vztahu ke zpracování údajů dětí. Všechny

[5] Stanovisko WP29 č. 3/2013 on purpose limitation, WP203, s. 15–16. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[6] Stanovisko WP29 č. 3/2013 on purpose limitation, WP203, s. 17–19. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

informace a sdělení musí být dětem podávány za použití jasných a jednoduchých jazykových prostředků, aby jim děti snadno porozuměly.

Na základě tohoto výkladu jsou na správce kladeny velmi vysoké a v mnoha případech obtížně splnitelné požadavky. U komplexních technologických a softwarových produktů může být splnění informační povinnosti v tomto standardu velmi obtížné, zejména pokud jsou subjekty údajů i děti. V takové situaci by správce mohl zvážit nad rámec splnění informační povinnosti v podobě textu i jinou doprovodnou formu vysvětlení, která bude subjektům údajů přístupnější a zaměří se pouze na hlavní aspekty účelů zpracování (např. v podobě zkráceného shrnutí, videa apod.). Často se používají též vrstvené dokumenty, které subjektům údajů umožňují snazší navigaci v hlavních informacích a možnost zjistit detailnější informace v rozklikávacích oknech. Vrstvené dokumenty doporučuje pro informace dostupné online i WP29.[7]

– Požadavek legitimního charakteru účelu

Dle WP29 znamená požadavek legitimního charakteru účelu, že tento účel musí být v souladu se zákonem v nejširším slova smyslu. Zahrnuje to soulad se všemi zákonnými a podzákonnými normami, vyhláškami měst a obcí, soudními rozhodnutími, ústavními principy, základními právy a svobodami jakož i jinými principy, které by soudy aplikovaly a interpretovaly jako „právo". V legitimním charakteru zpracování mohou být podle WP29 zohledněny i zvyklosti, kodexy chování, etická pravidla, smluvní ujednání a obecný kontext.[8]

Komplexním aspektem zásady účelového omezení je požadavek, že *„údaje nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný"*, potvrzený i v čl. 6 odst. 4 GDPR. Z tohoto požadavku lze dovozovat, že bez ohledu na obecný princip účelového omezení mohou být osobní údaje později zpracovávány jiným způsobem, pokud takový způsob zpracování bude s původním účelem slučitelný. Lze se domnívat, že test slučitelnosti účelů nemá za cíl omezit požadavek výslovného vyjádření účelu zpracování, ale připouští, že následně mohou vzniknout nové účely zpracování, které v době shromáždění údajů nebyly správci známy. Na takovéto nově vzniklé účely se následně uplatní požadavek slučitelnosti s původními účely, pro které byly údaje shromážděny.

Zjevným příkladem, který uvádí samotné znění čl. 5 odst. 1 písm. b) GDPR, jsou účely archivace ve veřejném zájmu, např. u archiválií, nebo vědecký a histo-

[7] Stanovisko WP29 č. 3/2013 on purpose limitation, WP203, s. 15–16. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[8] Stanovisko WP29 č. 3/2013 on purpose limitation, WP203, s. 20. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

rický výzkum. Dále by se mohlo jednat o některé oprávněné zájmy správce, které správci v době shromáždění údajů nebyly známy.

V některých případech by oprávněný zájem správce využít údaje jako důkaz v soudním sporu mohl být neslučitelný s účelem, pro který byly údaje získány. Pokud byly např. údaje získány pro ochranu životně důležitých zájmů subjektů údajů, bude s tímto účelem pravděpodobně neslučitelné využití údajů jako důkazní prostředek ve sporu se subjektem údajů. Naopak využití údajů v soudním sporu se subjektem údajů bude slučitelné s původním účelem zpracování pro splnění smlouvy, které se spor týká.

Lze se domnívat, že test slučitelnosti nelze provádět ve vztahu ke zpracování pro účely splnění právní povinnosti správce. Pokud správci vznikne nová právní povinnost, pro jejíž splnění musí zpracovat osobní údaje získané původně za jiným účelem, nemůže správce provádět test slučitelnosti účelů a zvažovat, zda v závislosti na výsledku tohoto testu svoji právní povinnost splní či nikoli. Typickým příkladem je poskytnutí osobních údajů orgánům činným v trestním řízení. Tento účel bude neslučitelný s většinou účelů, pro který byly údaje získány, správce však musí přesto svou zákonnou povinnost splnit.

K písm. c) (minimalizace údajů)

Oproti předchozí úpravě ve směrnici 95/46/ES, která omezovala zpracování na *„přiměřené, podstatné a nepřesahující míru s ohledem na účely“* dochází v GDPR k drobné úpravě terminologie na *„přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu“*.

Požadavek minimalizace údajů není požadavkem na omezení dat na absolutní minimum nezbytné k činnosti správce, ale spíše požadavkem na omezení shromažďování údajů na rozsah přiměřený účelu zpracování.[9] Posouzení souladu se zásadou minimalizace údajů by tedy mělo vycházet z testu přiměřenosti zpracování ve vztahu k účelu, stanovenému v souladu s požadavky zásady účelového omezení dle písm. b) tohoto článku.

Zásada minimalizace údajů se aplikuje na zpracování na základě všech titulů zpracování podle čl. 6 odst. 1 GDPR. Pro zpracování na základě oprávněného zájmu dle čl. 6 odst. 1 písm. f) GDPR je stanoven přísnější test „nezbytnosti“ pro účely oprávněných zájmů, doplněný balančním testem, ve kterém se porovnávají oprávněné zájmy správce s právy a svobodami subjektů údajů. Důvody zpracování dle čl. 6 odst. 1 písm. b) až e) GDPR předvídají přísnější test „nezbytnosti“. Rovněž důvody zpracování pro zvláštní kategorie údajů dle čl. 9 odst. 2 GDPR předvídají ve většině případů přísnější test „nezbytnosti“ pro stanovený důvod zpracování.

[9] VOIGT, P., VON DEM BUSSCHE, A. The EU general data protection regulation (GDPR). New York, NY: Springer Berlin Heidelberg, 2017. s. 90.

V praxi bude mít zásada minimalizace zpracování největší dopad na zpracování údajů na základě souhlasu dle čl. 6 odst. 1 písm. f) GDPR, případně dle čl. 9 odst. 2 písm. a) GDPR. Dle zásady minimalizace by správce neměl žádat subjekt údajů o souhlas se zpracováním jakýchkoli údajů, ale jen údajů přiměřených účelu zpracování. Pokud např. správce žádá o souhlas se zasíláním marketingových sdělení formou e-mailu či sms, neměl by za tímto účelem žádat o zpracování údajů o čísle platební karty či rodném čísle, neboť tyto údaje zpravidla nebudou přiměřené k účelu zasílání marketingových sdělení. Nelze vyloučit, že tyto údaje správce zpracovává za jiným účelem, např. číslo platební karty za účelem splnění smluvní povinnosti.

ÚOOÚ se podle předchozí právní úpravy vyjádřil k minimalizaci osobních údajů ve vztahu k identifikaci osob následovně: *„Subjekt údajů nemusí být identifikován pouze jménem, příjmením a adresou (přímá identifikace). Jakákoliv jiná kombinace osobních údajů, která umožní odlišit od sebe jednotlivé fyzické osoby (subjekty údajů), musí být považována za identifikaci subjektu údajů (nepřímá identifikace). Je však nutno vždy posoudit minimální kombinaci osobních údajů, která již identifikaci umožní. Nicméně např. kombinace osobních údajů jméno, příjmení, adresa a datum narození téměř vždy jednoznačně subjekt údajů identifikují. Ve většině případů zpracování osobních údajů je však znalost jména, příjmení a adresy dostatečným předpokladem pro určenost nebo určitelnost subjektu údajů“*.[10]

ÚOOÚ se podle předchozí právní úpravy dále vyjádřil k minimalizaci osobních údajů ve vztahu k identifikaci osob pro účely evidence ubytovaných následovně: *„Obec může v souladu s ust. § 5 odst. 1 písm. d) ZOOÚ (minimalizace údajů) v obecně závazné vyhlášce stanovit ubytovateli vedení řádné evidence ubytovaných osob pro kontrolu placení poplatku, do níž lze zapsat jméno a příjmení, datum narození a adresu trvalého bydliště poplatníka, druh a číslo jeho dokladu totožnosti, den příchodu a odchodu, a tedy počet dní pro stanovení základu poplatku. Údaje, které zákonem o místních poplatcích stanoveny nejsou, tedy datum narození a rodné číslo ubytovaného, ubytovatel ani obecní úřad vyžadovat pro zápis do knihy nemůže.“*[11] Podobný závěr by bylo možné učinit i na základě testu „nezbytnosti“ aplikovaném podle GDPR na zpracování údajů pro splnění právní povinnosti dle čl. 6 odst. 1 písm. c) GDPR.

[10] Úřad pro ochranu osobních údajů. Stanovisko č. 3/2012 – K pojmu osobní údaj [online]. Dostupné z: https://www.uoou.cz/stanovisko-c-3-2012-k-pojmu-osobni-udaj/d-1535.

[11] Úřad pro ochranu osobních údajů. Místní poplatky za lázeňský nebo rekreační pobyt [online]. Dostupné z: https://www.uoou.cz/c-3-2002-mistni-poplatky-za-lazensky-nebo-rekreacni-pobyt/ds-2537/archiv=0&p1=3109. Citováno v NOVÁK, M. Zákon o ochraně osobních údajů a předpisy související. Komentář. Praha: Wolters Kluwer, 2014, s. 145.

K písm. d) (přesnost)

Dle zásady přesnosti má správce povinnost přijmout rozumná opatření, aby údaje byly přesné a aktualizované. Podle vyjádření ÚOOU k předchozí právní úpravě je v rámci zásady přesnosti vyžadována nejen formální správnost údajů, ale i jejich faktická správnost: *„Zpracováním nepřesných osobních údajů není pouze zpracování nesprávných údajů vzniklých např. gramatickou chybou, ale i zpracování formálně správných údajů v souvislosti s nesprávnou informací. Např. zpracování přesných identifikačních údajů spolu s informací o tom, že daná osoba je dlužníkem, ačkoli tomu tak ve skutečnosti není.*"[12]

Povinnost aktualizace osobních údajů není absolutní povinností a aplikuje se pouze v případech, že z účelu zpracování vyplývá nutnost aktualizace údajů. Pokud naopak z účelu zpracování vyplývá, že je nutné zpracovávat historické údaje, nemá správce povinnost údaje aktualizovat.

Rozumná opatření směřující k zajištění správnosti a aktuálnosti údajů budou zahrnovat zejména aktualizaci interních databází a zajištění, že pokud správce získal informaci o změně osobních údajů, je tato informace reflektována ve všech informačních systémech a jiných nástrojích zpracování údajů vedených správcem. Tato opatření budou také zahrnovat opatření zajišťující, že osobní údaje jsou ve všech zdrojích aktualizovány o skutečnosti vzniklé činností samotného správce. Britský dozorový orgán k tomuto jako příklad uvádí, že pokud zaměstnavatel jako správce údajů zaměstnance sjednal se zaměstnancem zvýšení mzdy, je povinností správce v rámci zásady přesnosti údajů tuto informaci aktualizovat u všech osobních údajů zaměstnance.[13]

Je sporné, do jaké míry by měl správce ověřovat správnost a aktuálnost osobních údajů z externích zdrojů, protože taková činnost zpravidla vyžaduje zpracování dalších osobních údajů. Lze se domnívat, že zásada přesnosti nebude právní povinností ve smyslu čl. 6 odst. 1 písm. c) GDPR, která by bez omezení odůvodňovala jakékoli zpracování dalších osobních údajů za účelem ověření správnosti a aktuálnosti údajů již zpracovávaných správcem.

Zpracování údajů z externích zdrojů z důvodu zajištění přesnosti zpracovávaných údajů může být v omezené míře přípustné v situacích, kdy nepřesnost údajů může mít negativní dopad na subjekt údajů. Tak tomu bude např. u údajů využívaných k automatizovanému individuálnímu rozhodování, včetně profilování dle čl. 22 GDPR. Lze předpokládat, že robustnější opatření směřující k zajištění

[12] Úřad pro ochranu osobních údajů. K problematice aktualizace zpracovávaných osobních údajů [online]. Dostupné z: https://www.uoou.cz/k-problematice-aktualizace-zpracovavanych-osobnich-udaju/d-1595.

[13] ICO. Keeping personal data accurate and up to date (Principle 4). Dostupné z: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/.

správnosti a aktuálnosti údajů budou součástí opatření na ochranu práv a svobod a oprávněných zájmů subjektů údajů dle čl. 22 odst. 3 GDPR.

ÚOOÚ ve vyjádření k předchozí právní úpravě dovozuje, že správce by se neměl dopustit porušení zásady přesnosti, bez ohledu na to, jestli osobní údaje zpracovává za účelem neautomatizovaného či automatizovaného rozhodnutí. Příklad situace, kdy jsou osobní údaje podkladem pro automatizované rozhodování: *„Povinnost zpracovávat pouze přesné osobní údaje však neznamená, že je vždy nezbytné zpracovávat jen absolutně správné údaje, neboť nepřesnosti mohou vzniknout již při shromažďování dat od samotných subjektů údajů, z čehož nelze vyvozovat odpovědnost daného správce. […] Opatření směřující ke zjištění zpracování nesprávných osobních údajů jsou tak nezbytná zejména v systémech, jejichž provoz je zcela či do značné míry automatizovaný, a které jsou intenzivně využívány*".[14]

Se zásadou přesnosti údajů souvisí i právo subjektu údajů na opravu údajů dle čl. 16 GDPR. Důsledné zajištění práva na opravu je zjevným „rozumným opatřením" k tomu, aby údaje byly správné a aktuální. Zároveň je ale ze zásady přesnosti možné dovozovat právo správce odmítnout případné žádosti o opravu či doplnění, které by vedly k tomu, že údaje budou nesprávné, či neaktuální. Tak by tomu mohlo být např. v případě, že subjekt údajů v situaci, kdy nemá právo na výmaz údajů dle čl. 17 GDPR, usiluje o znehodnocení údajů formou jejich „opravy" na nesprávné údaje. Viz též komentář k čl. 16.

Britský dozorový orgán ICO doporučuje, aby správce s údaji spojil informaci, že údaje byly subjektem údajů rozporovány, a dovozuje, že správce nebude jednat v rozporu se zásadou přesnosti údajů, pokud správně zaznamenal údaje poskytnuté subjektem údajů, učinil za daných okolností rozumná opatření k zajištění přesnosti údajů a zajistil, že osoby přistupující k údajům jsou informovány o tom, že subjekt údajů přesnost údajů rozporoval.[15]

K písm. e) (omezení uložení)

Základním pravidlem stanoveným v této zásadě je přímá vazba účelu zpracování na dobu zpracování. Pokud tedy správce určí účel zpracování v souladu se zásadou účelového omezení [viz komentář k písm. b) výše], musí z určeného účelu též dovodit, jakou dobu zpracování tento účel odůvodňuje.

Bod odůvodnění č. 39 k tomu uvádí, že z důvodu zajištění, aby osobní údaje nebyly uchovávány déle, než je nezbytné, měl by správce stanovit lhůty pro výmaz nebo pravidelný přezkum.

[14] Úřad pro ochranu osobních údajů. K problematice aktualizace zpracovávaných osobních údajů [online]. Dostupné z: https://www.uoou.cz/k-problematice-aktualizace-zpracovavanych-osobnich-udaju/d-1595.

[15] ICO. Keeping personal data accurate and up to date (Principle 4). Dostupné z: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/.

Doba zpracování (lhůta pro výmaz) nemusí být ve všech případech určena jako konkrétní období (např. 3 roky od získání údajů). Doba zpracování bude často určena odkazem na jiné okolnosti. Tak tomu bude typicky u údajů zpracovávaných za účelem splnění smlouvy dle čl. 6 odst. 1 písm. b) GDPR, kdy doba zpracování bude často určena jako doba trvání smluvního vztahu, prodloužená případně o přiměřené období na vypořádání vzájemných práv a povinností stran.

Určení pevným obdobím by mělo být preferováno u údajů zpracovávaných na základě souhlasu dle čl. 6 odst. 1 písm. a), a to i v případě, že souhlas je poskytován v rámci registrace ke konkrétní službě. Viz též komentář k čl. 7.

ÚOOÚ se ve vztahu k předchozí právní úpravě vyjádřil k době zpracování pro účely plnění zákonné povinnosti následovně: *„Co se týče doby uchování osobních údajů, jsou uchovací lhůty dat zpracovávaných za účelem splnění právní povinnosti správce osobních údajů obvykle stanoveny právním předpisem, který danou povinnost správci ukládá. […] Překročení této doby není z hlediska zákona č. 101/2000 Sb. možné bez souhlasu subjektů údajů. Není-li doba uchování osobních údajů stanovena, je správce osobních údajů oprávněn uchovávat údaje pouze po dobu, po kterou trvá daná povinnost nebo právní vztah, popř. po jejich skončení po dobu nezbytnou pro vypořádání vzájemných práv a povinností.“*[16]

K dobám zpracování spojeným s jednotlivými právními základy zpracování viz též komentář k čl. 6 odst. 1.

Pokud není dán žádný důvod zpracování podle čl. 6 odst. 1 GDPR, připouští se další uložení a zpracování osobních údajů pro účely archivace ve veřejném zájmu, pro účely vědeckého a historického výzkumu a pro statistické účely. Podle čl. 9 odst. 2 písm. j) GDPR je pro tyto účely povoleno i zpracování zvláštních kategorií údajů.

Ke zpracování pro účely vědeckého a historického výzkumu viz též komentář k čl. 9 odst. 2 písm. j) a čl. 89 odst. 1.

Oproti čl. 6 odst. 1 písm. e) směrnice 95/46/ES přidává GDPR možnost uložení osobních údajů po delší dobu *pro účely archivace ve veřejném zájmu.* O archivaci ve veřejném zájmu by se mohlo jednat např. u tzv. archiválií. Pokud se nebude jednat o archivaci ve veřejném zájmu ale o běžnou archivaci správcem v rámci jeho zákonné povinnosti (např. archivaci účetních dokladů či zdravotnické dokumentace), lze se domnívat, že jde spíše o běžnou dobu zpracování za účelem plnění právní povinnosti dle čl. 6 odst. 1 písm. c) GDPR.

Uvozující věta ustanovení omezuje dobu zpracování na „údaje umožňující identifikaci subjektů údajů“. GDPR tak reflektuje technologickou realitu a nepožaduje absolutní výmaz všech údajů, ale pouze jejich anonymizaci.

[16] Úřad pro ochranu osobních údajů. Ke zpracování osobních údajů bývalých zaměstnanců [online]. Dostupné z: https://www.uoou.cz/ke-zpracovani-osobnich-udaju-byvalych-zamestnancu/d-1585/p1=1279.

Výmaz údajů je samozřejmě také možným řešením, pokud se pro něj správce rozhodne. V takovém případě by se mělo jednat o výmaz úplný, tak aby na nosičích dat nezůstaly žádné stopy údajů, ze kterých by bylo možné údaje rekonstruovat. Přitom je třeba vzít v úvahu technologickou realitu a připustit, že absolutní výmaz údajů tak, aby po údajích nezbyly žádné stopy, pravděpodobně není fyzicky možný jinak než zničením nosičů dat či silným magnetickým polem. Lze se domnívat, že GDPR v rámci povinnosti výmazu údajů nepožaduje např. fyzické zničení nosičů dat, mimo jiné i proto, že na stejných nosičích jsou případně uloženy jiné osobní údaje, jejichž dostupnost je správce povinen zajistit podle čl. 32 odst. 1 GDPR. Mělo by se tedy jednat o takový výmaz, aby s využitím dostupných technologií nebylo možné data znovu obnovit.

Správce se místo výmazu údajů může rozhodnout pouze pro jejich anonymizaci. Na anonymizaci jsou nicméně stanoveny velmi přísné požadavky.

GDPR rozlišuje mezi tzv. anonymizací a pseoudonymizací. Splnění povinnosti omezení uložení je možné pouze anonymizací údajů, nikoli pouze jejich pseudonymizací.

Pseudonymizace je pouze (i) možným technickým opatřením podle čl. 32 odst. 1 písm. a), čl. 25 a čl. 89 GDPR, (ii) případně technickým opatřením, které může vzhledem ke svým faktickým účinkům v některých případech omezovat rozsah oznamovací povinnosti ve smyslu čl. 33 odst. 1 a 34 odst. 3 GDPR (zejména v případě, že bude porušením zabezpečení dotčen pouze set dat, ze kterého není možné dovodit identitu žádné konkrétní fyzické osoby).

Základním rozdílem mezi anonymizací a pseudonymizací je vratnost celého procesu. Proces anonymizace i pseudonymizace je založen na oddělení tzv. „identifikátorů“ od ostatních osobních údajů. V případě anonymizace jsou „identifikátory“ nevratným způsobem vymazány, v případě pseudonymizace jsou pouze dočasně odděleny a je v moci správce je s využitím dostupných technických prostředků znovu spojit, zejména za pomoci šifrovacích klíčů.

Jedním z problémů při implementaci anonymizace splňující podmínky dle tohoto ustanovení je isolace všech identifikátorů z datového setu. Lze se domnívat, že pokud správce při sběru dat neprovedl důslednou pseudonymizaci a neoddělil všechny identifikátory od ostatních osobních údajů, bude v praxi velmi obtížné následně údaje vymazat formou anonymizace. Anonymizace tedy bude zpravidla podmíněna architekturou informačního systému, která od počátku psedonymizaci a následnou anonymizaci údajů předpokládá.

Pokud chce správce údaje smazat formou anonymizace, musí nevratně vymazat všechny identifikátory a ponechat si pouze ostatní údaje, ze kterých není možné identitu subjektu údajů zjistit. Je přitom nerozhodné, zda správce identitu subjektů údajů z datových setů aktivně zjišťuje či nikoli, zásada omezení uložení zakazuje i samotné ukládání dat umožňujících identifikaci subjektu údajů.

Identifikátory jsou přitom mnohem širší set dat než identifikační údaje subjektu jako jméno, příjmení, e-mailová adresa, telefonní číslo apod. Identifikátor je jakýkoli údaj, ze kterého je možné určit, ke kterému subjektu údajů se vztahuje. Skupina identifikátorů se přitom s vývojem technologií schopných určit ze setu dat identitu subjektu údajů postupně rozšiřuje. Rozhodovací praxe a vyjádření dozorových orgánů postupně vyjasňují, které údaje je nutné považovat za identifikátory a které nikoli.

Identifikátorem je např. i IP adresa, včetně dynamické IP adresy. Podle rozsudku SDEU i dynamická IP adresa představuje osobní údaj, jelikož může sloužit k reidentifikaci, v určitých případech tedy ani dynamická IP adresa nebude dostatečně anonymizovaným údajem.[17]

Identifikátorem jsou i iniciály ve spojení s adresou. Účastník řízení před ÚOOÚ se dopustil deliktu, neboť zveřejnil osobní údaje dlužníků v rozsahu adresy trvalého pobytu dlužníků, jejich iniciál, výše dlužných částek a identifikace. Podle iniciál XY a adresy se v seznamu neuhrazených pohledávek poznal XY bytem –, neboť na uvedené adrese s těmito iniciálami bydlí pouze on.[18]

Identifikátorem bude také každý údaj, který při zadání do internetových vyhledávačů po krátkém hledání umožní zjistit osobu, ke které se údaj vztahuje, a to i v případě, že o výsledku vyhledávání mohou být určité pochybnosti.

Obdobně bude identifikátorem každý údaj umožňující vyhledání osoby ve veřejně dostupném rejstříku, bez ohledu na to, zda je takový rejstřík zřízen dle zákona či nikoli.

Objevují se i úvahy, že některé dostatečně velké sety dat mohou být identifikátorem samy o sobě, i pokud neobsahují žádné konkrétní informace, ke kterým osobám se vztahují. Takto lze uvažovat o setech dat, ze kterých je možné ne příliš náročnou analýzou osobu určit. Takto je možno uvažovat např. o údajích z GPS či jiných geolokačních nástrojů, protože analýzou informací o tom, kde se osoba pravidelně a příležitostně zdržuje, je možné identitu osoby dovodit.

Identifikátorem zpravidla naopak nebudou údaje o jednotlivých nákupech či jiném uživatelském chování subjektu údajů, pokud je není možné spojit s identitou subjektu údajů. Nicméně do budoucna lze předpokládat, že s rozvíjejícími se možnostmi datové analytiky se bude skupina identifikátorů rozšiřovat a skupina údajů, ze kterých nelze identitu subjektů údajů dostupnými technologiemi zjistit, se bude naopak zužovat, a to zejména pokud správce disponuje velkými sety dat.

Podobný závěr potvrzuje i WP29. Ve svém stanovisku k anonymizačním technikám WP29 uvádí, že správci by se měli zaměřit na konkrétní prostředky, kte-

[17] Rozsudek SDEU ze dne 19. října 2016 Patrick Breyer proti Bundesrepublik Deutschland, věc C-582/14.

[18] Rozhodnutí VER-3280/08.

ré by případně umožnily vratnost anonymizace, a vzít v potaz zejména náklady a know-how potřebné k implementaci těchto prostředků, jakož i pravděpodobnost jejich využití a závažnost dopadu. Podle WP29 by správci měli např. porovnat úsilí, které sami vynaloží na anonymizaci (pokud jde o čas a náklady), se stále se zvyšující dostupností cenově nenáročných prostředků, jak identifikovat jednotlivce ve velkých setech dat ve spojení se zvyšující se dostupností jiných datových setů (i.e. prostřednictvím open data). WP29 také upozorňuje na to, že existuje řada příkladů neúplné anonymizace s často nevratnými důsledky pro subjekty údajů.[19]

Do budoucna se tedy anonymizace může blížit výmazu údajů.

Lze se domnívat, že způsob výmazu či anonymizace osobních údajů by měl být součástí hodnocení rizik pro práva a subjekty údajů podle čl. 35 GDPR, zejména pokud jde o rizika případně vyplývající ze skutečnosti, že údaje mohou být při použití zvolené technologie výmazu či anonymizace zpětně zrekonstruovány.

Ve svém stanovisku k anonymizačním technikám uvádí WP29 tři hlavní rizika anonymizačních technologií (tedy rizika, že údaje mohou být zpětně zrekonstruovány navzdory použité anonymizační technologii): (i) isolace údajů (tzv. „*singling out*"), propojení údajů (tzv. „*linkability*") a dovození údajů (tzv. „*inference*").[20] Tato rizika mohou mít dopad na práva a svobody subjektů údajů, i pokud nevedou ke zcela přesným závěrům ale jen k závěrům přibližným, s určitou mírou chybovosti.

WP29 také doporučuje prostředky ke snížení těchto rizik (*noise addition, permutation, difefrential privacy*, generalizační techniky jako *aggregation* a *K-anonymity* případně doplněné o *L-diversity/T-closeness*).[21]

K písm. f) (integrita a důvěrnost)

Konkrétní požadavky na splnění povinností integrity a důvěrnosti údajů jsou stanoveny oddíle 2 GDPR, zejména v čl. 32 GDPR. Povinnosti správce související s vyhodnocováním rizik zpracování jsou stanoveny v oddíle 3 GDPR.

[19] Stanovisko WP29 č. 05/2014 on Anonymisation Techniques, WP216, s. 8–9 Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Citováno v NULÍČEK, GDPR. s. 115.

[20] Stanovisko WP29 č. 05/2014 on Anonymisation Techniques, WP216, s. 11–12 Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[21] Stanovisko WP29 č. 05/2014 on Anonymisation Techniques, WP216, s. 12–18 Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Citováno v NULÍČEK, GDPR. s. 115.

K odst. 2 (odpovědnost)

Podle tohoto ustanovení má správce povinnost doložit soulad s hlavními zásadami zpracování osobních údajů dle čl. 5 odst. 1 GDPR. Tato povinnost nebyla v předchozí úpravě ZOOÚ a směrnice 95/46/ES obsažena.

Zásadu blíže rozvádí zejména čl. 24 GDPR.

Podle vyjádření ÚOOU budou k prokazování souladu s těmito zásadami sloužit záznamy o činnostech zpracování a též kodexy a osvědčení.[22]

Britský dozorový organ ICO uvádí širší výčet možností, jak může správce doložit soulad se zásadami zpracování. Podle ICO by měl správce (i) přijmout vhodná technická a organizační opatření, která zajišťují a dokládají soulad s GDPR, což může zahrnovat interní směrnice na ochranu osobních údajů, školicí program pro zaměstnance, program interních auditů činností zpracování a pravidelných revizí interních směrnic pro zaměstnance, (ii) vést relevantní dokumentaci k záznamům činností zpracování**,** (iii) v relevantních případech jmenovat pověřence pro ochranu osobních údajů, (iv) implementovat opatření naplňující požadavky záměrné a standardní ochrany osobních údajů, (v) v relevantních případech provést posouzení vlivu na ochranu osobních údajů a (vi) řídit se schválenými kodexy chování a pravidly pro schválené procesy vydávání osvědčení.[23]

WP29 ve svém stanovisku k zásadě odpovědnosti uvádí obecnější principy, zdůrazňuje povinnost vyhodnotit účinnost přijatých opatření a mj. doporučuje školení zaměstnanců a jmenování pověřence pro ochranu osobních údajů. Podle WP29 by správci měli zajistit, že přijatá opatření k zajištění souladu s GDPR jsou účinná. V případě rozsáhlejšího nebo komplexnějšího zpracování a zpracování zahrnujícího vysoká rizika doporučuje WP29 pravidelně účinnost přijatých opatření ověřovat, např. interními a externími audity.[24]

Zásada odpovědnosti se podle znění ustanovení čl. 5 odst. 2 vztahuje pouze na doložení souladu s obecnými zásadami zpracování dle čl. 5 odst. 1 GDPR a nikoli na doložení souladu s jinými ustanoveními GDPR. Nicméně řada zásad zpracování je dále podrobněji upravena v jiných ustanoveních GDPR a tato ustanovení tak mohou být nepřímo zahrnuta do povinnosti odpovědnosti.

Přestože se nejedná o plné procesní obrácení důkazního břemene, přenáší toto ustanovení podstatnou část důkazního břemene v případném správním řízení na správce.

---

[22] Úřad pro ochranu osobních údajů. Zásady a právní důvody zpracování [online]. Dostupné z: https://www.uoou.cz/4-zasady-a-pravni-d-vody-zpracovani/d-27271.

[23] ICO. Accountability and governance. Dostupné z: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/.

[24] Stanovisko WP29 č. 3/2010 on the principle of accountability, WP173, s. 9. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

Ve vztahu k sankcím je velmi relevantní, zda odpovědnost upravená v čl. 5 odst. 2 GDPR je sama o sobě základní zásadou zpracování a může být předmětem sankce dle čl. 83 odst. 5 písm. a) GDPR, či zda se jedná pouze o dodatečnou povinnost související se zásadami zpracování dle odst. 1, jejíž porušení samo o sobě nemůže být předmětem sankce jako porušení základní zásady zpracování. Oddělení do samostatného odstavce by mohlo svědčit o tom, že zákonodárce zamýšlel povinnost odpovědnosti stanovit jen jako dodatečnou povinnost, která zajišťuje plnění základních zásad zpracování, a nikoli jako samostatnou zásadu zpracování. Nicméně existuje řada zdrojů, ve kterých je odpovědnost uváděna jako jedna ze základních zásad zpracování, i když bez specifické úvahy o interpretaci sankcí dle čl. 83 odst. 5 písm. a) GDPR.

Související judikatura:

Judikatura evropských soudů:

rozsudek SDEU ze dne 19. 10. 2016, ***C-582/14***, Patrick Breyer proti Bundesrepublik Deutschland.

Související ustanovení:

čl. 6, čl. 9, čl. 12–14, čl. 32, čl. 83 odst. 5 písm. a)
Body odůvodnění: 39

Související předpisy:

§ 5 zákona č. 101/2000 Sb., o ochraně osobních údajů
čl. 6 směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Související literatura:

NOVÁK, M. *Zákon o ochraně osobních údajů a předpisy související.* Komentář. Praha: Wolters Kluwer, 2014
VOIGT, P., VON DEM BUSSCHE, A., *The EU general data protection regulation (GDPR).* New York, NY: Springer Berlin Heidelberg, 2017.

Názory a rozhodovací praxe ÚOOÚ:

rozhodnutí ÚOOÚ, č. j. VER-3280/08
ÚOOÚ. Nové přístupy a povinnosti, vytvořeno/změněno: 27. 10. 2017
ÚOOÚ. Zásady a právní důvody zpracování, vytvořeno/změněno: 27. 10. 2017
ÚOOÚ. Ke zpracování osobních údajů bývalých zaměstnanců, vytvořeno/změněno: 21. 3. 2013
ÚOOÚ. K problematice aktualizace zpracovávaných osobních údajů, vytvořeno/změněno: 21. 3. 2013
stanovisko ÚOOÚ č. 3/2012 k pojmu osobní údaj, poslední aktualizace únor 2014

Stanoviska WP29:
WP173, Opinion 3/2010 on the principle of accountability, adopted on 13 July 2010
WP203, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013
WP216, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014

Další dokumenty:
OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
ICO. Processing personal data fairly and lawfully (Principle 1)
ICO. Keeping personal data accurate and up to date (Principle 4)
ICO. Accountability and governance

Článek 6
Zákonnost zpracování

1. Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

První pododstavec písm. f) se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů.

2. Členské státy mohou zachovat nebo zavést konkrétnější ustanovení, aby přizpůsobily používání pravidel tohoto nařízení ohledně zpracování ke splnění odst. 1 písm. c) a e) tím, že přesněji určí konkrétní požadavky na zpracování a jiná opatření k zajištění zákonného a spravedlivého zpracování, a to i u jiných zvláštních situací, při nichž dochází ke zpracování, jak stanoví kapitola IX.