Pokyny 4/2019 k článku 25

Záměrná a standardní ochrana osobních údajů

Verze 2.0

Přijato dne 20. října 2020

Historie verzí

Verze 1.0	13. listopadu 2019	Přijetí pokynů k veřejné konzultaci
Verze 2.0	úterý 20. října 2020	Přijetí pokynů EDPB po veřejné konzultaci

Obsah

Evropský sbor pro ochranu osobních údajů

s ohledem na čl. 70 odst. 1 písm. e) nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“),

s ohledem na Dohodu o EHP, a zejména na přílohu XI a protokol 37 k této dohodě ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018,

s ohledem na články 12 a 22 svého jednacího řádu,

PŘIJAL TYTO POKYNY

Shrnutí

Ve světě, který je stále více digitální, hraje dodržování požadavků na záměrnou a standardní ochranu osobních údajů stěžejní úlohu při prosazování ochrany soukromí a osobních údajů ve společnosti. Je proto zásadní, aby správci brali svou odpovědnost vážně a při navrhování operací zpracování plnili povinnosti stanovené GDPR.

Pokyny poskytují obecné vodítko ohledně povinnosti týkající se záměrné a standardní ochrany osobních údajů stanovené v článku 25 GDPR. Záměrná a standardní ochrana osobních údajů je povinností všech správců bez ohledu na velikost a různou složitost zpracování. Aby správce mohl plnit požadavky týkající se záměrné a standardní ochrany osobních údajů, je důležité, aby porozuměl zásadám ochrany údajů a právům a svobodám subjektu údajů.

Hlavní povinností je zavedení *vhodných* opatření a nezbytných záruk, které zajistí *účinné provádění zásad ochrany osobních údajů* a v důsledku dodržování *práv a svobod subjektů údajů pomocí záměrné a standardní ochrany*. Článek 25 předepisuje jak koncepční, tak standardní prvky, které by měly být vzaty v úvahu. Zmíněné prvky budou v těchto pokynech blíže rozvedeny.

V čl. 25 odst. 1 se stanoví, že by správci měli při plánování nové operace zpracování včas zvážit záměrnou a standardní ochranu osobních údajů. Správci zajišťují záměrnou a standardní ochranu osobních údajů *před* zpracováním a rovněž *průběžně* v době zpracování tím, že pravidelně přezkoumávají účinnost zvolených opatření a záruk. Záměrná a standardní ochrana osobních údajů se vztahuje rovněž na stávající systémy, které zpracovávají osobní údaje.

Pokyny obsahují také vodítka ohledně účinného provádění zásad ochrany údajů stanovených v článku 5 a uvádějí klíčové koncepční a standardní prvky, jakož i praktické názorné příklady. Správce by měl zvážit vhodnost navrhovaných opatření v rámci daného konkrétního zpracování.

EDPB podává doporučení ohledně toho, jak mohou správci, zpracovatelé a zhotovitelé spolupracovat na dosažení záměrné a standardní ochrany osobních údajů. Vybízí správce v odvětví, zpracovatele a zhotovitele, aby používali záměrnou a standardní ochranu osobních údajů jako prostředek k dosažení konkurenční výhody při propagování svých produktů vůči správcům a subjektům údajů na trhu. Rovněž všechny správce vybízí k tomu, aby využívali osvědčení a kodexů chování.

1 OBLAST PŮSOBNOSTI

1. Tyto pokyny se zaměřují na provádění záměrné a standardní ochrany osobních údajů ze strany správců na základě povinnosti stanovené v článku 25 GDPR.[1] Tyto pokyny mohou být užitečné i pro jiné subjekty, jako jsou zpracovatelé a zhotovitelé produktů, služeb a aplikací (dále jen „zhotovitelé“), na něž se článek 25 přímo nevztahuje, při vytváření produktů a služeb, které jsou v souladu s GDPR a které správcům umožňují plnit jejich povinnosti v oblasti ochrany údajů.[2] V 78. bodě odůvodnění GDPR se upozorňuje na to, že by záměrná a standardní ochrana osobních údajů měla být zohledněna i v souvislosti s veřejnými zakázkami. Navzdory tomu, že povinnost začlenit záměrnou a standardní ochranu osobních údajů do svých činností zpracování mají všichni správci, toto ustanovení podporuje přijímání zásad ochrany údajů v případech, kdy by orgány veřejné správy měly jít příkladem. Správce je odpovědný za plnění povinností týkajících se záměrné a standardní ochrany osobních údajů při zpracování prováděném jeho zpracovateli a dílčími zpracovateli, měl by proto tuto skutečnost zohlednit při uzavírání smluv s těmito stranami.

2. Požadavek popsaný v článku 25 spočívá v tom, že správci mají ochranu údajů koncipovanou v rámci zpracování osobních údajů a jako standardní nastavení, což platí po celou dobu zpracování. Záměrná a standardní ochrana osobních údajů je rovněž požadavkem na systémy zpracování, které existovaly již před vstupem GDPR v platnost. Správci musí zpracování důsledně aktualizovat v souladu s GDPR. Více informací o tom, jak zachovat stávající systém v souladu se záměrnou a standardní ochranou osobních údajů, je uvedeno v podkapitole 2.1.4 těchto pokynů. Podstatou tohoto ustanovení je zajistit *přiměřenou* a *účinnou* ochranu údajů, a to jak *záměrnou*, tak *standardní*, což znamená, že by správci měli být schopni prokázat, že v rámci zpracování mají zavedena vhodná opatření a záruky, aby byly zajištěny účinné zásady ochrany údajů a práva a svobody subjektů údajů.

3. Kapitola 2 pokynů se zaměřuje na výklad požadavků stanovených v článku 25 a zkoumá právní povinnosti, které toto ustanovení zavádí. Příklady toho, jak se záměrná a standardní ochrana osobních údajů použije v souvislosti s jednotlivými zásadami ochrany údajů, jsou uvedeny v kapitole 3.

4. Pokyny se rovněž zabývají možností vytvořit mechanismus pro vydávání osvědčení za účelem prokázání souladu s článkem 25, a to v kapitole 4. V kapitole 5 je posouzen možný způsob prosazování dozorovými úřady. Závěrem pokyny podávají zúčastněným stranám další doporučení, jak úspěšně provádět záměrnou a standardní ochranu osobních údajů. EDPB uznává, že pro malé a střední podniky je obtížné plnit povinnosti vyplývající ze záměrné a standardní ochrany osobních údajů v plném rozsahu, a v kapitole 6 poskytuje další doporučení konkrétně malým a středním podnikům.

[1] Zde uvedený výklad platí stejnou měrou i pro článek 20 směrnice (EU) 2016/680 a článek 27 nařízení 2018/1725.

[2] V 78. bodě odůvodnění GDPR je tato nutnost jasně zmíněna: *„Pokud jde o vývoj, koncepci, výběr a používání aplikací, služeb a produktů, které jsou založeny na zpracování osobních údajů nebo osobní údaje za účelem plnění svých funkcí zpracovávají, je třeba zhotovitele těchto produktů, služeb a aplikací vybízet k tomu, aby při vývoji a koncipování těchto produktů, služeb a aplikací zohledňovali právo na ochranu údajů a brali náležitý ohled na stav techniky s cílem zajistit, aby správci a zpracovatelé mohli plnit své povinnosti v oblasti ochrany údajů.“*

2 ANALÝZA ČL. 25 ODST. 1 A 2 – ZÁMĚRNÁ A STANDARDNÍ OCHRANA OSOBNÍCH ÚDAJŮ

5. Cílem této kapitoly je prozkoumat požadavky na záměrnou ochranu osobních údajů uvedené v čl. 25 odst. 1 resp. požadavky na standardní ochranu osobních údajů uvedené v čl. 25 odst. 2 a poskytnout k nim vodítko. Záměrná a standardní ochrana osobních údajů jsou vzájemně se doplňující koncepty, které se synergeticky podporují. Subjekty údajů budou mít větší prospěch ze standardní ochrany osobních údajů, bude-li souběžně prováděna záměrná ochrana osobních údajů, a naopak.

6. Záměrná a standardní ochrana osobních údajů je povinností všech správců, včetně malých podniků i nadnárodních společností. Vzhledem k tomu se složitost provádění záměrné a standardní ochrany osobních údajů může lišit v závislosti na jednotlivých operacích zpracování. Bez ohledu na velikost však může být ve všech případech prováděním záměrné a standardní ochrany osobních údajů dosaženo pozitivních přínosů pro správce i subjekt údajů.

2.1 Ustanovení čl. 25 odst. 1: Záměrná ochrana osobních údajů

2.1.1 Povinnost správce zavést do procesu zpracování vhodná technická a organizační opatření a nezbytné záruky

7. V souladu s čl. 25 odst. 1 správce zavede *vhodná* technická a organizační *opatření*, která jsou navržena za účelem provádění zásad ochrany osobních údajů, a začlení do zpracování *nezbytné záruky*, aby splnil požadavky a ochránil práva a svobody subjektů údajů. Vhodná opatření i nezbytné záruky mají sloužit témuž účelu, a sice chránit práva subjektů údajů a zajistit, aby byla do procesu zpracování začleněna ochrana jejich osobních údajů.

8. Pod pojmy *technická a organizační opatření* a nezbytné *záruky* lze chápat obecně jakoukoliv metodu nebo prostředek, které může správce při zpracování použít. *Vhodným* se rozumí to, že by opatření a nezbytné záruky měly být způsobilé k dosažení zamýšleného účelu, tj. musí *účinně* provádět zásady ochrany osobních údajů[3]. Požadavek na vhodnost proto úzce souvisí s požadavkem na účinnost.

9. Technickým nebo organizačním opatřením a zárukou může být cokoliv od používání vyspělých technologických řešení až po základní školení zaměstnanců. Příklady, které mohou být vhodné v závislosti na kontextu a rizicích spojených s daným zpracováním, zahrnují pseudonymizaci osobních údajů[4]; uchovávání osobních údajů ve strukturovaném, běžně strojově čitelném formátu; možnost subjektů údajů zasahovat do zpracování; poskytování informací o uchovávání osobních údajů; existence systémů detekce malwaru; školení zaměstnanců o základní „kybernetické hygieně“; vytváření systémů řízení ochrany soukromí a bezpečnosti informací; smluvní zavázání zpracovatelů k zavedení konkrétních postupů minimalizace údajů atd.

10. Při určování vhodných opatření mohou být užitečné normy, osvědčené postupy a kodexy chování, které uznávají sdružení a jiné subjekty zastupující kategorie správců. Správce však musí ověřit vhodnost opatření pro dotyčné konkrétní zpracování.

[3] „Účinností“ se zabývá podkapitola 2.1.2.
[4] Jak je definováno v čl. 4 bodu 5) GDPR.

2.1.2 Účelem je provádět zásady ochrany údajů účinným způsobem a ochránit práva a svobody subjektů údajů

11. *Zásady ochrany osobních údajů* jsou uvedeny v článku 5 (dále jen „zásady“), *právy a svobodami subjektů údajů* jsou základní práva a svobody fyzických osob, a zejména jejich právo na ochranu osobních údajů, jejichž ochrana je v čl. 1 odst. 2 uvedena jako cíl GDPR (dále jen „práva“)[5]. Jejich přesnou formulaci lze nalézt v Listině základních práv EU. Je nezbytné, aby správce rozuměl významu *zásad* a *práv* jako základu pro ochranu, kterou poskytuje GDPR, konkrétně v rámci povinnosti týkající se záměrné a standardní ochrany osobních údajů.

12. Při zavádění vhodných technických a organizačních opatření je třeba postupovat s ohledem na účinné provádění každé z výše zmíněných zásad a z toho plynoucí ochranu práv a svobod, aby opatření a záruky byly *záměrné*.

Zajištění účinnosti

13. Účinnost je základním prvkem koncepce záměrné ochrany osobních údajů. Požadavek na účinné provádění zásad znamená, že správci musí zavést nezbytná opatření a záruky na ochranu těchto zásad, aby byla zajištěna práva subjektů údajů. Každé zavedené opatření by mělo přinést zamýšlené výsledky pro správcem plánované zpracování. Z tohoto konstatování vyplývají dva důsledky.

14. Za prvé to znamená, že článek 25 nevyžaduje zavedení žádných konkrétních technických a organizačních opatření, nýbrž že by zvolená opatření a záruky měly být specifické vzhledem k provádění zásad ochrany údajů při konkrétním zpracování. Přitom by opatření a záruky měly být navrženy tak, aby byly spolehlivé, a správce by měl mít možnost provádět další opatření s cílem rozšířit je s ohledem na případné zvýšení rizika[6]. To, zda opatření jsou či nejsou účinná, bude proto záviset na kontextu dotyčného zpracování a na posouzení určitých prvků, jež je nutné zohlednit při určování prostředků zpracování. Výše uvedenými prvky se zabývá podkapitola 2.1.3.

15. Správci by za druhé měli být schopni prokázat dodržení zásad.

16. Zavedená opatření a záruky by měly dosáhnout požadovaného účinku, pokud jde o ochranu údajů, a správce by měl mít dokumentaci o zavedených technických a organizačních opatřeních[7]. Za tímto účelem může správce určit vhodné klíčové ukazatele výkonnosti k prokázání účinnosti. Klíčový ukazatel výkonnosti je měřitelná hodnota zvolená správcem, která prokazuje, jak účinně správce plní cíl týkající se ochrany údajů. Tyto ukazatele mohou být *kvantitativní*, například procentní podíl falešně pozitivních nebo falešně negativních výstupů, pokles počtu stížností, zkrácení doby reakce, pokud subjekty údajů uplatňují svá práva, nebo *kvalitativní*, jako jsou hodnocení výkonnosti, používání hodnotících stupnic nebo odborné posudky. Alternativně ke klíčovým ukazatelům výkonnosti mohou být správci schopni

[5] Viz 4. bod odůvodnění GDPR.

[6] „Základní zásady, kterými se správci musí řídit (tj. zákonnost, minimalizace údajů, účelové omezení, transparentnost, integrita údajů a přesnost údajů), by měly zůstat beze změny, ať už jde o jakékoliv zpracování a subjektům údajů hrozí jakákoliv rizika. Nedílnou součástí uplatňování těchto zásad je však vždy náležité zohlednění povahy a rozsahu takového zpracování, tudíž jejich inherentní vlastností je možnost rozšíření.“ Pracovní skupina zřízená podle článku 29. „Statement on the role of a risk-based approach in data protection legal frameworks“ (Prohlášení o úloze přístupu založeného na rizicích v právních rámcích pro ochranu údajů). WP 218, 30. května 2014, s. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[7] Viz 74. a 78. bod odůvodnění.

prokázat účinné uplatňování zásad tím, že své posouzení účinnosti zvolených opatření a záruk odůvodní.

2.1.3 Prvky, které je třeba vzít v úvahu

17. V čl. 25 odst. 1 jsou uvedeny prvky, které správce musí vzít v úvahu při určování opatření pro konkrétní operaci zpracování. V následujících odstavcích poskytneme vodítka ohledně toho, jak tyto prvky uplatňovat v procesu navrhování, který zahrnuje návrh standardního nastavení. Všechny tyto prvky přispívají k určení toho, zda je opatření vhodné k účinnému provádění zásad. Každý z těchto prvků tudíž není cílem sám o sobě, nýbrž se jedná o faktory, které je třeba pro dosažení tohoto cíle posuzovat společně.

2.1.3.1 „stav techniky“

18. Pojem „stav techniky“ figuruje v různých dokumentech acquis EU, např. v souvislosti s ochranou životního prostředí a bezpečností výrobků. V GDPR je „stav techniky“[8] zmíněn nejen v článku 32 v souvislosti s bezpečnostními opatřeními[9][10], nýbrž také v článku 25, čímž se toto referenční kritérium rozšiřuje na veškerá technická a organizační opatření, jež jsou součástí zpracování.

19. V souvislosti s článkem 25 ukládá zmínka o „stavu techniky“ správcům při určování vhodných technických a organizačních opatření povinnost **zohlednit soudobý pokrok v oblasti technologií**, které jsou k dispozici na trhu. To znamená, že správci musí mít povědomí o technologickém pokroku a držet s ním krok. Musí rovněž vědět, jaká rizika nebo příležitosti mohou technologie představovat pro ochranu údajů při operacích zpracování a jak zavádět a aktualizovat opatření a záruky, které *zabezpečí účinné provádění* zásad a práv subjektů údajů s ohledem na měnící se technologie.

20. „Stav techniky“ je dynamický pojem, který nelze definovat staticky v daný časový okamžik, ale je třeba jej posuzovat *průběžně* v souvislosti s technologickým pokrokem. Vzhledem k technologickému pokroku je možné, že správce zjistí, že opatření, které kdysi zajišťovalo odpovídající úroveň ochrany, již tuto ochranu neposkytuje. Pokud nebude držet krok s technologickými změnami, může se proto dopustit jednání v rozporu s článkem 25.

21. Kritérium „stav techniky“ se nevztahuje pouze na technologická opatření, nýbrž také na organizační opatření. Nedostatečná organizační opatření mohou snížit, nebo dokonce zcela narušit účinnost zvolené technologie. K příkladům organizačních opatření může patřit přijetí interních strategií; aktuální odborná příprava v oblasti technologií, bezpečnosti a ochrany údajů a zásady správy a řízení bezpečnosti IT.

22. Při udávání současného „stavu techniky“ v dané oblasti použití mohou hrát roli stávající a uznávané rámce, normy, certifikace, kodexy chování atd. v různých oblastech. Pokud takové normy existují a poskytují subjektu údajů vysokou úroveň ochrany v souladu s právními požadavky nebo jdou nad

[8] Viz rozhodnutí německého Spolkového ústavního soudu ve věci „Kalkar“ z roku 1978: https://germanlawarchive.iuscomp.org/?p=67, které může sloužit jako základ pro metodiku objektivního definování tohoto pojmu. Technologická úroveň „stavu techniky“ by tudíž měla být vymezena jako technologická úroveň nacházející se mezi „současnou úrovní vědeckých poznatků a výzkumu“ a zavedenějšími „obecně přijímanými pravidly technologií“. „Stav techniky“ je tudíž možné vymezit jako technologickou úroveň služeb, technologií nebo produktů, které existují na trhu a nejúčinněji dosahují stanovených cílů.
[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security
[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

rámec těchto požadavků, měli by je správci zohlednit při navrhování a provádění opatření na ochranu údajů.

2.1.3.2 „náklady na provedení“

23. Správce může při výběru a uplatňování vhodných technických a organizačních opatření a nezbytných záruk, které účinně provádějí zásady za účelem ochrany práv subjektů údajů, zohlednit náklady na provedení. Náklady se v této souvislosti rozumějí zdroje obecně, včetně času a lidských zdrojů.

24. Prvek nákladovosti nevyžaduje, aby správce vynaložil neúměrné množství zdrojů, pokud existují alternativní opatření, méně náročná na zdroje a přesto účinná. Náklady na provedení jsou však spíše faktorem, který je třeba brát v úvahu při provádění záměrné ochrany osobních údajů, než důvodem jejího neuskutečnění.

25. Zvolená opatření mají tudíž zajistit, že správce v rámci plánované činnosti nebude zpracovávat osobní údaje v rozporu se zásadami, a to bez ohledu na náklady. Správci by měli mít možnost řídit celkové náklady, aby byli schopni účinně uplatňovat všechny zásady a chránit tak práva.

2.1.3.3 „povaha, rozsah, kontext a účel zpracování“

26. Správci musí při určování potřebných opatření vzít v úvahu povahu, rozsah, kontext a účel zpracování.

27. Tyto faktory by měly být vykládány v souladu s jejich úlohou v jiných ustanoveních GDPR, jako jsou články 24, 32 a 35, s cílem navrhnout zásady ochrany údajů při zpracování.

28. Stručně řečeno, pojem **povaha** je možno chápat jako nedílnou[11] vlastnost zpracování. **Rozsahem** se rozumí velikost a šíře zpracování. **Kontext** se týká okolností zpracování, které mohou ovlivnit očekávání subjektu údajů, zatímco **účel** se vztahuje k cílům zpracování.

2.1.3.4 „různě pravděpodobná a různě závažná rizika pro práva a svobody fyzických osob, jež s sebou zpracování nese“

29. GDPR zaujímá soudržný přístup založený na rizicích v rámci mnoha svých ustanovení, v článcích 24, 25, 32 a 35, s cílem určit vhodná technická a organizační opatření za účelem ochrany fyzických osob, jejich osobních údajů a splnění požadavků GDPR. Aktiva, která se chrání, jsou vždy tatáž (fyzické osoby prostřednictvím ochrany jejich osobních údajů), chrání se vždy před týmiž riziky (pro práva fyzických osob) s ohledem na tytéž podmínky (povaha, rozsah, kontext a účel zpracování).

30. Při provádění analýzy rizik pro účely souladu s článkem 25 musí správce určit rizika pro práva subjektů údajů, která představuje porušení zásad, a určit jejich pravděpodobnost a závažnost, aby mohl zavést opatření k účinnému zmírnění zjištěných rizik. Při posuzování rizik má zásadní význam systematické a důkladné hodnocení zpracování. Správce například posuzuje konkrétní rizika spojená s neexistencí svobodně uděleného souhlasu, což představuje porušení zásady zákonnosti, v průběhu zpracování osobních údajů dětí a osob mladších 18 let jako zranitelné skupiny v případě, že neexistuje jiný právní základ, a zavádí vhodná opatření k řešení a účinnému zmírnění zjištěných rizik spojených s touto skupinou subjektů údajů.

[11] Příkladem jsou zvláštní kategorie osobních údajů, automatizované rozhodování, nerovnovážné mocenské vztahy, nepředvídatelné zpracování, obtíže subjektu údajů při výkonu práv atd.

31. „Pokyny EDPB pro posouzení vlivu na ochranu údajů“[12], které se zaměřují na určení, zda je pravděpodobné, že operace zpracování povede k vysokému riziku pro subjekt údajů, či nikoliv, rovněž nabízejí vodítka k tomu, jak posuzovat rizika pro ochranu údajů a jak provádět posouzení vlivu na ochranu osobních údajů. Tyto pokyny mohou být užitečné také při posuzování rizik ve všech článcích uvedených výše, včetně článku 25.

32. Přístup založený na rizicích nevylučuje použití základních scénářů, osvědčených postupů a norem. Ty se mohou ukázat jako osvědčený soubor nástrojů, kterými mohou správci zvládat podobná rizika v podobných situacích (povaha, rozsah, kontext a účel zpracování). Přesto nadále platí povinnost uvedená v článku 25 (jakož i v článcích 24, 32 a čl. 35 odst. 7 písm. c)), tj. vzít v úvahu *„různě pravděpodobná a různě závažná rizika pro práva a svobody fyzických osob, jež s sebou zpracování nese“*. Proto i když se správci opírají o takovéto nástroje, musí pro danou činnost zpracování vždy provést posouzení vlivu na ochranu osobních údajů v každém jednotlivém případě a ověřit účinnost navrhovaných vhodných opatření a záruk. Dodatečně se pak může vyžadovat posouzení vlivu na ochranu osobních údajů nebo aktualizace stávajícího posouzení vlivu na ochranu osobních údajů.

2.1.4 Aspekt času

2.1.4.1 V době určení prostředků pro zpracování

33. Záměrná ochrana osobních údajů musí být zavedena *„v době určení prostředků pro zpracování“*.

34. *„Prostředky pro zpracování“* sahají od obecných prvků po podrobné prvky návrhu zpracování, jako je architektura, postupy, protokoly, rozvržení a vzhled.

35. *„Doba určení prostředků pro zpracování“* označuje dobu, kdy správce rozhoduje o tom, jak bude zpracování provedeno, o způsobu, jakým bude zpracování provedeno, a o mechanismech, které budou použity k provedení takového zpracování. Během tohoto rozhodování musí správce posoudit vhodná opatření a záruky pro účinné uplatnění zásad a práv subjektů údajů do zpracování a zohlednit prvky, jako je stav techniky, náklady na provedení, povaha, rozsah, kontext a účel zpracování a také rizika. To zahrnuje dobu pořízení a zavedení softwaru, hardwaru a služeb pro zpracování údajů.

36. Včasné posouzení záměrné a standardní ochrany osobních údajů má zásadní význam pro úspěšné provádění zásad a ochranu práv subjektů údajů. Z hlediska nákladů a přínosů bude mimoto v zájmu správců zohlednit záměrnou a standardní ochranu osobních údajů spíše dříve než později, neboť by mohlo být náročné a nákladné měnit již hotové plány a již navržené operace zpracování.

2.1.4.2 V době samotného zpracování (zachování a přezkum požadavků na ochranu údajů)

37. Jakmile je zpracování zahájeno, má správce trvalou povinnost zachovávat záměrnou a standardní ochranu osobních údajů, tj. setrvalé účinné provádění zásad za účelem ochrany práv, zohledňovat nejnovější stav techniky, přehodnocovat úrovně rizika atd. Povaha, rozsah a kontext operací zpracování, jakož i riziko se mohou v průběhu zpracování měnit, což znamená, že správce musí své operace zpracování přehodnocovat prostřednictvím pravidelných přezkumů a hodnocení účinnosti zvolených opatření a záruk.

38. Povinnost zachovávat, přezkoumávat a v případě potřeby aktualizovat operaci zpracování se vztahuje i na již existující systémy. To znamená, že starší systémy navržené před vstupem GDPR v platnost musí

[12] Pracovní skupina zřízená podle článku 29, „Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679“. WP 248 rev.01, 4. října 2017. ec.europa.eu/newsroom/document.cfm?doc_id=47711 – schváleno EDPB.

být podrobeny přezkumu a údržbě, aby se zajistilo zavedení opatření a záruk, které účinně provádějí zásady a práva subjektů údajů, jak je uvedeno v těchto pokynech.

39. Tato povinnost platí rovněž pro veškerá zpracování prováděná zpracovateli. Operace zpracování by měli správci pravidelně přezkoumávat a posuzovat, aby bylo zajištěno, že průběžně umožňují dodržování zásad a správci údajů usnadňují plnění jeho povinností v tomto ohledu.

2.2 Ustanovení čl. 25 odst. 2: Standardní ochrana osobních údajů

2.2.1 Standardně se zpracovávají pouze osobní údaje, které jsou nezbytné pro každý konkrétní účel zpracování.

40. „Standardním“ (nastavením), jak je běžně definuje počítačová věda, se rozumí již existující nebo předem zvolená hodnota konfigurovatelného nastavení, jež je přiřazena softwarové aplikaci, počítačovému programu nebo zařízení. Tato nastavení se také označují jako „přednastavení“ nebo „tovární nastavení“, zejména u elektronických zařízení.

41. Pojmem „standardní“ se při zpracování osobních údajů tudíž rozumí volba týkající se konfiguračních hodnot nebo možností zpracování, které jsou nastaveny nebo předepsány v systému zpracování, jako je softwarová aplikace, služba nebo zařízení, nebo manuální způsob zpracování, jež ovlivňuje množství shromážděných osobních údajů, rozsah jejich zpracování, dobu jejich uchovávání a jejich dostupnost.

42. Správce by měl zvolit zavedení standardního nastavení a možností zpracování tak, aby se provádělo pouze zpracování, které je nezbytně nutné k dosažení stanoveného zákonného účelu, a nést za ně odpovědnost. V takovém případě by se správci měli spoléhat na své posouzení nezbytnosti zpracování s ohledem na právní důvody uvedené v čl. 6 odst. 1. To znamená, že správce standardně neshromažďuje více údajů, než je nezbytné, nezpracovává shromážděné údaje více, než je pro dané účely nezbytné, ani neuchovává údaje déle, než je nezbytné. Základním požadavkem je, aby ochrana údajů byla začleněna do standardního zpracování.

43. Správce je povinen předem stanovit, pro které určité, výslovně vyjádřené a legitimní účely se osobní údaje shromažďují a zpracovávají[13]. Opatření musí být standardně nastavena tak, aby byla vhodná k zajištění toho, že se zpracovávají pouze osobní údaje, které jsou nezbytné pro jednotlivý konkrétní účel zpracování. Při rozhodování, které údaje jsou nezbytné pro zpracování k dosažení konkrétního účelu, mohou být užitečné rovněž pokyny Evropského inspektora ochrany údajů (EIOÚ) k posouzení nezbytnosti a přiměřenosti opatření, která omezují právo na ochranu osobních údajů[14] [15] [16].

[13] Čl. 5 odst. 1 písm. b), c), d) a e) GDPR.
[14] EIOÚ. „Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection“ (Pokyny k posouzení nezbytnosti a přiměřenosti opatření, která omezují právo na ochranu údajů). 25. února 2019. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf
[15] Viz také EIOÚ. „Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit“ (Posouzení nezbytnosti opatření, která omezují základní právo na ochranu osobních údajů: soubor nástrojů) https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en
[16] Více informací o nezbytnosti viz: pracovní skupina zřízená podle článku 29. „Stanovisko č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES“. WP 217, 9. dubna 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf

44. Pokud správce používá software třetí strany nebo komerčně dostupný software, měl by provést posouzení rizik dotyčného produktu a zajistit, aby byly funkce, které nemají právní základ nebo které nejsou slučitelné se zamýšlenými účely zpracování, vypnuty.

45. Tytéž úvahy platí i pro organizační opatření na podporu operací zpracování. Měla by být navržena tak, aby se od začátku zpracovávalo pouze minimální množství osobních údajů nezbytných pro dané operace. Tuto zásadu je třeba zohlednit zejména při udělování přístupu k údajům zaměstnancům plnícím odlišné úlohy a s různou potřebou přístupu.

46. Vhodná „technická a organizační opatření“ v souvislosti se standardní ochranou osobních údajů je proto třeba chápat stejně, jak bylo projednáno výše v podkapitole 2.1.1, avšak ve vztahu konkrétně k provádění zásady minimalizace údajů.

47. Výše uvedená povinnost zpracovávat pouze osobní údaje, které jsou nezbytné pro jednotlivé konkrétní účely, se týká níže uvedených prvků.

2.2.2 Rozsah povinnosti týkající se minimalizace údajů

48. V čl. 25 odst. 2 je stanoven rozsah povinnosti týkající se minimalizace údajů při standardním zpracování, přičemž se uvádí, že se tato povinnost vztahuje na množství shromážděných osobních údajů, rozsah jejich zpracování, dobu jejich uložení a dostupnost.

2.2.2.1 „množství shromážděných osobních údajů“

49. Správci by měli zvážit jak objem osobních údajů, tak i druhy, kategorie a míru podrobnosti osobních údajů, která je nutná pro účely zpracování. Jejich rozhodnutí při navrhování by měla zohlednit vyšší rizika, pokud jde o zásady integrity a důvěrnosti, minimalizace údajů a omezení uložení, při shromažďování velkého množství podrobných osobních údajů a porovnat je s nižšími riziky plynoucími ze shromažďování menšího množství a/nebo méně podrobných informací o subjektech údajů. Standardní nastavení nesmí každopádně zahrnovat sběr osobních údajů, které nejsou nezbytné pro konkrétní účel zpracování. Jinými slovy, pokud některé kategorie osobních údajů nejsou nezbytné nebo pokud nejsou zapotřebí podrobné údaje, protože stačí méně detailní údaje, pak nesmí být shromažďovány žádné nadbytečné osobní údaje.

50. Stejné standardní požadavky se vztahují na služby nezávislé na tom, jaká platforma nebo zařízení se používá, shromažďovány mohou být pouze osobní údaje nezbytné pro daný účel.

2.2.2.2 „rozsah jejich zpracování“

51. Operace zpracování[17] osobních údajů se omezí na to, co je nezbytné. K naplnění účelu zpracování může přispět mnoho operací zpracování. Skutečnost, že ke splnění účelu zpracování jsou zapotřebí určité osobní údaje, neznamená, že v souvislosti s těmito údaji mohou být prováděny veškeré druhy operací zpracování a s jakoukoliv četností. Správci by také měli k posouvání hranic „slučitelných účelů“ podle čl. 6 odst. 4 přistupovat opatrně a mít na paměti, jaké zpracování mohou subjekty údajů rozumně očekávat.

[17] Podle čl. 4 bodu 2) GDPR tyto operace zahrnují shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

2.2.2.3 „doba jejich uložení“

52. Shromážděné osobní údaje se neuchovávají, pokud nejsou nezbytné pro účel zpracování a neexistuje jiný slučitelný účel a právní důvod podle čl. 6 odst. 4. Jejich uchovávání by měl správce údajů objektivně odůvodnit jako nezbytné v souladu se zásadou odpovědnosti.

53. Správce omezí dobu uchovávání údajů na to, co je pro daný účel nezbytné. Nejsou-li osobní údaje nadále nezbytné pro účel zpracování, musí být standardně vymazány nebo anonymizovány. Délka doby uchovávání bude proto záviset na účelu dotyčného zpracování. Tato povinnost přímo souvisí se zásadou omezení uložení uvedenou v čl. 5 odst. 1 písm. e) a je zavedena standardně, tj. správce by měl do zpracování začlenit systematické postupy pro výmaz nebo anonymizaci údajů.

54. Anonymizace[18] osobních údajů je alternativou výmazu, pokud jsou zohledněny veškeré relevantní kontextové prvky a pravidelně se hodnotí pravděpodobnost a závažnost rizika, včetně rizika zpětné identifikace[19].

2.2.2.4 „jejich dostupnost“

55. Správce by měl na základě posouzení nezbytnosti omezit počet osob, které mají přístup k osobním údajům, a rovněž typy přístupu a zajistit, aby osobní údaje byly skutečně přístupné těm, kteří přístup k nim potřebují, například v kritických situacích. V rámci celého toku údajů během zpracování je třeba provádět kontroly přístupu.

56. V čl. 25 odst. 2 se dále uvádí, že osobní údaje nesmí být bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob. Správce musí standardně omezit přístupnost a umožnit subjektu údajů zasáhnout předtím, než zveřejní nebo jinak zpřístupní osobní údaje o subjektu údajů neomezenému počtu fyzických osob.

57. Zpřístupnění osobních údajů neomezenému počtu osob může vést k dalšímu šíření údajů, než bylo původně zamýšleno. To je relevantní zejména v souvislosti s internetem a vyhledávači. To znamená, že by správci měli standardně subjektům údajů umožnit zasáhnout dříve, než budou osobní údaje zpřístupněny na otevřeném internetu. To je obzvláště důležité, pokud jde o děti a zranitelné skupiny.

58. V závislosti na právních důvodech zpracování by se možnost zásahu mohla lišit podle kontextu zpracování. Například požádat o souhlas se zpřístupněním osobních údajů veřejnosti nebo o nastavení ochrany soukromí, aby subjekty údajů mohly samy kontrolovat přístup veřejnosti.

59. Ani v případě, kdy se osobní údaje zpřístupní veřejnosti se svolením a vědomím subjektu údajů, to neznamená, že tyto údaje může sám svobodně zpracovávat jakýkoliv jiný správce, který k nim má přístup, pro své vlastní účely – musí mít samostatný právní základ[20].

[18] Pracovní skupina zřízená podle článku 29. „Stanovisko č. 5/2014 k technikám anonymizace“. WP 216, čtvrtek 10. dubna 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf

[19] Viz čl. 4 bod 1) GDPR, 26. bod odůvodnění GDPR, pracovní skupina zřízená podle článku 29, „stanovisko č. 5/2014 k technikám anonymizace“. Viz také pododdíl o „omezení uložení“ v oddíle 3 tohoto dokumentu, který se týká toho, že správce musí zajistit účinnost zavedené techniky (technik) anonymizace.

[20] Viz věc Satakunnan Markkinapörssi Oy a Satamedia Oy v. Finsko, č. 931/13.

3 PROVÁDĚNÍ ZÁSAD OCHRANY ÚDAJŮ PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ZA POUŽITÍ ZÁMĚRNÉ A STANDARDNÍ OCHRANY OSOBNÍCH ÚDAJŮ

60. Ve všech fázích návrhu činností zpracování, včetně zadávání veřejných zakázek, nabídkových řízení, externího zajišťování, vývoje, podpory, údržby, testování, uložení, výmazu atd., by měl správce zohlednit a zvážit různé prvky záměrné a standardní ochrany osobních údajů, které budou ilustrovány na příkladech uvedených v této kapitole v souvislosti s prováděním zásad[21] [22] [23].

61. Správci musí zavést zásady pro dosažení záměrné a standardní ochrany osobních údajů. K těmto zásadám patří: transparentnost, zákonnost, korektnost, účelové omezení, minimalizace údajů, přesnost, omezení uložení, integrita a důvěrnost a odpovědnost. Tyto zásady jsou uvedeny v článcích 5 a v 39. bodě odůvodnění GDPR. Aby bylo možné plně pochopit, jak provádět záměrnou a standardní ochranu osobních údajů, je zdůrazněn význam chápání významu každé z těchto zásad.

62. Při uvádění příkladů, jak zavést záměrnou a standardní ochranu osobních údajů, jsme pro každou ze zásad sestavili seznamy **klíčových prvků záměrné a standardní ochrany osobních údajů**. Příklady sice kladou důraz na konkrétní dotčenou zásadu ochrany údajů, mohou se však překrývat s úzce souvisejícími zásadami. EDPB zdůrazňuje, že klíčové prvky a příklady uvedené níže nejsou vyčerpávající ani závazné, nýbrž jsou míněny jako hlavní prvky každé z těchto zásad. Správci musí posoudit, jak zaručit soulad se zásadami v kontextu konkrétní dotčené operace zpracování.

63. Ačkoli se tento oddíl zaměřuje na provádění zásad, správce by měl rovněž zavést *vhodné* a *účinné* způsoby ochrany práv subjektů údajů, a to podle kapitoly III GDPR, pokud to již není stanoveno samotnými zásadami.

64. Zásada odpovědnosti je obecná: vyžaduje, aby správce nesl odpovědnost za výběr nezbytných technických a organizačních opatření.

3.1 Transparentnost[24]

65. Správce musí jasně a otevřeně informovat subjekt údajů o tom, jak bude shromažďovat, používat a sdílet osobní údaje. Podstatou transparentnosti je umožnit subjektům údajů porozumět jejich právům uvedeným v článcích 15 až 22 a v nezbytných případech je uplatňovat. Tato zásada je zakotvena v článcích 12, 13, 14 a 34. Provádění těchto článků by mělo být také podporováno opatřeními a zárukami zavedenými na podporu zásady transparentnosti.

66. Klíčové koncepční a standardní prvky zásady transparentnosti mohou zahrnovat:

- Jasnost – informace musí být uvedeny jasným a jednoduchým jazykem, stručně a srozumitelně.

[21] Více příkladů viz norský úřad pro ochranu osobních údajů. „Software Development with Data Protection by Design and by Default“ (Vývoj softwaru s přihlédnutím k záměrné a standardní ochraně osobních údajů). 28. listopadu 2017. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

[24] Podrobné pojednání o tom, jak chápat pojem transparentnosti, je uvedeno v dokumentu pracovní skupiny zřízené podle článku 29. „Pokyny k transparentnosti podle nařízení 2016/679“. WP 260 rev.01, středa 11. dubna 2018. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 – schváleno EDPB.

- Sémantika – komunikace by měla mít jasný obsah pro dotčené adresáty.
- Přístupnost – informace musí být pro subjekt údajů snadno přístupné.
- Kontextovost – informace musí být poskytnuty v relevantní okamžik a ve vhodné formě.
- Relevantnost – informace by měly být relevantní a vztahovat se na konkrétní subjekt údajů.
- Univerzální design – informace musí být přístupné všem subjektům údajů, včetně použití strojově čitelných jazyků s cílem usnadnit a automatizovat čitelnost a jasnost.
- Srozumitelnost – subjekty údajů by měly dobře chápat, co mohou očekávat v souvislosti se zpracováním svých osobních údajů, zejména pokud jsou subjekty údajů děti nebo jiné zranitelné skupiny.
- Použití více kanálů – informace by měly být poskytnuty prostřednictvím různých kanálů a sdělovacích prostředků, nejen textových, aby se zvýšila pravděpodobnost toho, že informace účinně osloví subjekt údajů.
- Vrstvení – informace by měly být vrstveny způsobem, který vyřeší napětí mezi úplností a porozuměním, a zároveň zohlední přiměřená očekávání subjektů údajů.

Příklad[25]

Správce navrhuje zásady ochrany soukromých údajů na internetových stránkách s cílem dodržovat požadavky na transparentnost. Zásady ochrany soukromých údajů by neměly obsahovat zdlouhavé informace, které jsou pro průměrný subjekt údajů obtížné proniknutelné a pochopitelné. Musí být napsány jasným a výstižným jazykem a uživatel internetových stránek musí snadno porozumět tomu, jak jsou jeho osobní údaje zpracovávány. Správce proto poskytuje informace ve více vrstvách, přičemž zdůrazňuje nejdůležitější body. Podrobnější informace jsou snadno dostupné. Za účelem podrobnějšího vysvětlení jednotlivých bodů a pojmů uvedených v zásadách jsou k dispozici rozbalovací nabídky a odkazy na jiné stránky. Správce rovněž zajistí, že se informace poskytují prostřednictvím více kanálů, například tím, že nabízí videoklipy vysvětlující nejdůležitější aspekty písemných informací. Zásadní význam pro zajištění toho, aby vrstvený přístup nezvyšoval zmatečnost, nýbrž ji spíše zmenšil, má součinnost mezi jednotlivými stránkami.

Přístup subjektů údajů k zásadám ochrany soukromí by neměl být složitý. Tyto zásady ochrany soukromí jsou proto zpřístupněny a jsou viditelné na všech jednotlivých stránkách dané internetové stránky, aby subjekt údajů mohl získat přístup k informacím vždy jen jedním kliknutím. Poskytované informace jsou rovněž sestaveny v souladu s osvědčenými postupy a normami univerzálního designu, aby byly přístupné všem.

Nezbytné informace musí být mimoto poskytnuty také ve správném kontextu a ve vhodné době. Jelikož správce provádí mnoho operací zpracování s použitím údajů shromážděných na internetových stránkách, obecné zásady ochrany soukromí na internetových stránkách samy o sobě nepostačují k tomu, aby správce splnil požadavky na transparentnost. Správce proto navrhuje tok informací a předkládá subjektu údajů relevantní informace ve vhodném kontextu, například za pomocí krátkých informačních sdělení nebo vyskakovacích oken. Pokud například správce žádá subjekt údajů o zadání osobních údajů, informuje ho, jak budou tyto údaje zpracovány a proč jsou tyto údaje pro dané zpracování nezbytné.

[25] Francouzský úřad pro ochranu osobních údajů zveřejnil několik příkladů dokládajících osvědčené postupy, pokud jde o informování uživatelů, i s ohledem na jiné zásady transparentnosti: https://design.cnil.fr/en/.

3.2 Zákonnost

67. Správce musí určit platný právní základ pro zpracování osobních údajů. Tento požadavek by měla podporovat opatření a záruky, aby se zajistilo, že celý cyklus zpracování je v souladu s příslušnými právními důvody pro zpracování.

68. Ke klíčovým koncepčním a standardním prvkům s ohledem na zákonnost může patřit:
- Relevantnost – na zpracování se vztahuje správný právní základ.
- Diferenciace[26] – rozlišuje se právní základ použitý pro každou činnost zpracování.
- Uvedený účel – vhodný právní základ musí jasně souviset s uvedeným účelem zpracování[27].
- Nezbytnost – zpracování musí být nezbytné a bezpodmínečné pro daný účel, má-li být zákonné.
- Autonomie – subjektu údajů by měla být přiznána co nejvyšší míra autonomie, pokud jde o jeho kontrolu nad osobními údaji v rámci právního základu.
- Získání souhlasu – souhlas musí být svobodný, konkrétní, informovaný a jednoznačný[28]. Zvláštní pozornost by měla být věnována schopnosti dětí a mladých lidí poskytnout informovaný souhlas.
- Odvolání souhlasu – je-li souhlas právním základem, mělo by zpracování usnadnit odvolání souhlasu. Odvolání musí být stejně snadné jako udělení souhlasu. Není-li tomu tak, pak mechanismus souhlasu správce není v souladu s GDPR[29].
- Vyvažování zájmů – jsou-li právním základem oprávněné zájmy, musí správce provést vážení zájmů a věnovat zvláštní pozornost nerovnováze sil, zejména v případě dětí mladších 18 let a jiných zranitelných skupin. Musí existovat opatření a záruky ke zmírnění negativního dopadu na subjekty údajů.
- Určení předem – právní základ musí být určen před zahájením zpracování.
- Ukončení – pokud právní základ již nebude platit, musí se zpracování odpovídajícím způsobem ukončit.
- Úprava – pokud došlo k platné změně právního základu zpracování, musí být vlastní zpracování upraveno v souladu s novým právním základem[30].
- Rozdělení odpovědnosti – v případě plánování společné správy si strany musí jasně a transparentně rozdělit příslušnou odpovědnost vůči subjektu údajů a navrhnout opatření k zajištění toho, aby bylo zpracování v souladu s tímto rozdělením odpovědnosti.

[26] EDPB. „Pokyny 2/2019 o zpracovávání osobních údajů podle čl. 6 odst. 1 písm. b) GDPR v souvislosti s poskytováním on-line služeb subjektům údajů“. Verze 2.0, 8. října 2019. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_cs.pdf

[27] Viz níže oddíl o účelovém omezení.

[28] Viz pokyny 5/2020 o souhlasu podle nařízení 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[29] Viz pokyny 5/2020 o souhlasu podle nařízení 2016/679, s. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[30] Je-li původním právním základem souhlas, viz pokyny 5/2020 o souhlasu podle nařízení 2016/679. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

Příklad

Banka má v plánu nabízet službu ke zvýšení účinnosti správy žádostí o úvěr. Tato služba má umožnit bance, na základě vyžádaného svolení zákazníka, získávat údaje o zákazníkovi přímo od daňových orgánů. Tento příklad nebere v úvahu zpracování osobních údajů z jiných zdrojů.

Získání osobních údajů o finanční situaci subjektu údajů je nezbytné k přijetí opatření na žádost subjektu údajů před uzavřením úvěrové smlouvy[31]. Shromažďování osobních údajů přímo od správce daně však není považováno za nezbytné, protože zákazník může uzavřít smlouvu s tím, že sám předloží informace od správce daně. Ačkoli banka může mít oprávněný zájem na přímém získání dokumentace od daňových orgánů, například v zájmu zajištění účinnosti při zpracovávání úvěrů, poskytnutí takového přímého přístupu k osobním údajům žadatelů bankám představuje riziko související s využitím nebo možným zneužitím přístupových práv.

Při provádění zásady zákonnosti si správce uvědomí, že v tomto kontextu nemůže použít základ týkající se „nezbytnosti pro uzavření smlouvy“ u té části zpracování, která zahrnuje sběr osobních údajů přímo od daňových orgánů. Skutečnost, že toto konkrétní zpracování představuje riziko v tom smyslu, že se subjekt údajů méně zapojí do zpracování svých údajů, je také relevantním faktorem při posuzování zákonnosti zpracování jako takového. Banka dospěla k závěru, že tato část zpracování se musí opírat o jiný právní základ zpracování. V konkrétním členském státě, v němž se správce nachází, existují vnitrostátní právní předpisy, jež bance umožňují získat informace přímo od daňových orgánů, pokud s tím subjekt údajů předem souhlasí.

Banka proto uvede informace o zpracování na on-line platformě pro podávání žádostí takovým způsobem, aby umožnila subjektům údajů snadno porozumět, jaké zpracování je povinné a jaké je volitelné. Možnosti zpracování standardně neumožňují získávání údajů přímo z jiných zdrojů, než je samotný subjekt údajů, a možnost přímého získávání informací je představena způsobem, který subjekt údajů neodrazuje od nezvolení této možnosti. Každý souhlas udělený za účelem sběru údajů přímo od jiných správců je dočasným právem na přístup ke konkrétnímu souboru informací.

Každý udělený souhlas se zpracovává elektronicky způsobem, který umožňuje zdokumentování, a subjektům údajů se nabízí snadný způsob, jak kontrolovat, k čemu udělili souhlas, a jak souhlas odvolat.

Správce posoudil tyto požadavky na záměrnou a standardní ochranu osobních údajů předem a zahrne všechna tato kritéria do svých specifikací požadavků na nabídkové řízení za účelem zajištění uvedené platformy. Správce si je vědom toho, že pokud nezahrne požadavky na záměrnou a standardní ochranu osobních údajů do nabídkového řízení, může být na pozdější zavedení ochrany údajů příliš pozdě nebo může jít o velmi nákladný proces.

3.3 Korektnost

69. Korektnost je obecná zásada, která vyžaduje, aby nebyly osobní údaje zpracovány způsobem, který je pro subjekt údajů neoprávněně škodlivý, nezákonně diskriminační, neočekávaný nebo zavádějící. Opatření a záruky provádějící zásadu korektnosti rovněž podporují práva a svobody subjektů údajů, konkrétně právo na informace (transparentnost), právo na zásah (přístup, výmaz, přenositelnost údajů, oprava) a právo na omezení zpracování (právo nebýt předmětem automatizovaného individuálního rozhodování a zákaz diskriminace subjektů údajů v těchto procesech).

[31] Viz čl. 6 odst. 1 písm. b) GDPR.

70. Ke klíčovým koncepčním a standardním prvkům s ohledem na korektnost může patřit:

- Autonomie – subjektům údajů by měla být poskytnuta nejvyšší možná míra autonomie při určování využití jejich osobních údajů, jakož i pokud jde o rozsah a podmínky tohoto použití nebo zpracování.
- Interakce – subjekty údajů musí být schopny komunikovat se správcem a uplatňovat svá práva s ohledem na osobní údaje zpracovávané správcem.
- Očekávání – zpracování by mělo odpovídat přiměřeným očekáváním subjektů údajů.
- Zákaz diskriminace – správce nesmí subjekty údajů nespravedlivě diskriminovat.
- Zákaz vykořisťování – správce by neměl zneužívat potřeby nebo zranitelnost subjektů údajů.
- Volba spotřebitele – správce by neměl nespravedlivě „blokovat“ své uživatele. Je-li služba zpracovávající osobní údaje proprietární, může mít za následek „uvíznutí“ ve službě, jež nemusí být korektní, pokud je tím narušena možnost subjektů údajů uplatnit své právo na přenositelnost údajů v souladu s článkem 20.
- Rovnováha sil – rovnováha sil by měla být hlavním cílem vztahu mezi správcem a subjektem údajů. Je třeba zabránit nerovnováze sil. Není-li to možné, měla by být uznána a zohledněna prostřednictvím vhodných protiopatření.
- Žádný přenos rizika – správci by neměli přenášet na subjekty údajů rizika podniku.
- Žádné podvodné jednání – informace a možnosti týkající se zpracování údajů by měly být předkládány objektivním a neutrálním způsobem, aby se zabránilo klamavému nebo manipulativnímu jazyku či koncepci.
- Dodržování práv – správce musí dodržovat základní práva subjektů údajů a zavést vhodná opatření a záruky a nezasahovat do těchto práv, pokud to zákon výslovně neodůvodňuje.
- Etika – správce by měl sledovat širší dopad zpracování na práva a důstojnost fyzických osob.
- Pravdivost – správce musí zpřístupnit informace o tom, jak zpracovává osobní údaje, měl by jednat tak, jak prohlašuje, a neuvádět subjekty údajů v omyl.
- Lidský zásah – správce musí začlenit *kvalifikovaný* lidský zásah, který je schopen napravit předpojatost, kterou může vytvořit stroj, v souladu s právem nebýt předmětem automatizovaného individuálního rozhodování uvedeným v článku 22[32].
- Korektní algoritmy – je třeba pravidelně posuzovat, zda algoritmy fungují v souladu s účely, a upravovat algoritmy tak, aby zmírnily nezahrnutá zkreslení a zajistily korektní zpracování. Subjekty údajů by měly být informovány o zpracování osobních údajů na základě algoritmů, které je analyzují a vytvářejí související predikce, například pokud jde o pracovní výkon, ekonomickou situaci, zdraví, osobní preference, spolehlivost nebo chování, místo, kde se nacházejí, nebo jejich přesuny[33].

[32] Viz pokyny k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679. https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826.
[33] Viz 71. bod odůvodnění GDPR.

Příklad č. 1

Správce provozuje vyhledávač, který zpracovává především osobní údaje vytvářené uživateli. Správce má prospěch z toho, že vlastní velké množství osobních údajů a že tyto osobní údaje může používat pro cílenou reklamu. Chce proto ovlivnit subjekty údajů, aby umožnily rozsáhlejší shromažďování a používání svých osobních údajů. Souhlas má být získán tak, že se subjektu údajů předloží možnosti zpracování.

Při provádění zásady korektnosti vezme správce v úvahu povahu, rozsah, kontext a účel zpracování a uvědomí si, že nemůže nabízet jednotlivé možnosti způsobem, který nabádá subjekt údajů k tomu, aby správci umožnil shromažďovat více osobních údajů, než kdyby byly možnosti představeny rovnocenným nebo neutrálním způsobem. To znamená, že nemůže představit možnosti zpracování tak, aby subjektům údajů ztěžoval možnost nesdílet své údaje nebo aby subjektům údajů ztěžoval změnu nastavení ochrany soukromí a omezení zpracování. Jedná se o příklady temných vzorců, které jsou v rozporu s duchem článku 25. Standardně nastavené možnosti zpracování by měly být co nejméně invazivní a rozhodnutí týkající se dalšího zpracování je třeba předkládat způsobem, který subjekt údajů nenutí udělit souhlas. Správce proto předkládá možnosti udělení či neudělení souhlasu jako dvě stejně viditelné volby, jež přesně odrážejí důsledky každé volby pro subjekt údajů.

Příklad č. 2

Jiný správce zpracovává osobní údaje za účelem poskytování služby streamování, kdy uživatelé mají možnost rozhodnout se mezi pravidelným předplatným standardní kvality a bonusovým předplatným vyšší kvality. Jako součást bonusového předplatného získávají předplatitelé prioritní zákaznické služby.

S ohledem na zásadu korektnosti není možné, aby prioritní zákaznické služby poskytnuté bonusovým předplatitelům diskriminovaly přístup běžných předplatitelů k výkonu jejich práv podle článku 12 GDPR. To znamená, že i když bonusoví předplatitelé získávají prioritní služby, nemůže jejich upřednostňování vést k tomu, že nebudou existovat vhodná opatření týkající se neprodlené odpovědi na žádost běžných předplatitelů, a odpověď nesmí být každopádně poskytnuta více než jeden měsíc od obdržení žádostí.

Prioritní zákazníci si mohou zaplatit lepší služby, všechny subjekty údajů však musí mít rovný a nediskriminační přístup k prosazování svých práv a svobod podle článku 12.

3.4 Účelové omezení[34]

71. Správce musí shromažďovat údaje pro určité, výslovně vyjádřené a legitimní účely a nesmí je dále zpracovávat způsobem, který je neslučitelný s účely, pro které byly shromážděny[35]. Návrh zpracování by tudíž měl vycházet z toho, co je nezbytné pro dosažení uvedených účelů. Pokud má probíhat další zpracování, musí se správce nejprve ujistit, že účely tohoto zpracování jsou slučitelné s původními

[34] Pracovní skupina zřízená podle článku 29 poskytla pokyny k chápání zásady účelového omezení podle směrnice 95/46/ES. Ačkoliv toto stanovisko sbor EDPB neschválil, může být přesto relevantní, protože znění této zásady je v GDPR totožné. Pracovní skupina zřízená podle článku 29. „Opinion 03/2013 on purpose limitation" (Stanovisko č. 3/2013 k účelovému omezení). WP 203, čtvrtek úterý 2. dubna 2013. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[35] Čl. 5 odst. 1 písm. b) GDPR.

účely, a v souladu s tím zpracování navrhnout. To, zda je či není nový účel slučitelný, se posuzuje podle kritérií uvedených v čl. 6 odst. 4.

72. Ke klíčovým koncepčním a standardním prvkům s ohledem na účelové omezení může patřit:
- Určení předem – legitimní účely musí být určeny před vytvořením návrhu zpracování.
- Specifičnost – účely musí být specifikovány a musí být výslovně uvedeny důvody pro zpracovávání osobních údajů.
- Orientace na účel – účel zpracování by měl být vodítkem při navrhování zpracování a měl by stanovit meze zpracování.
- Nezbytnost – účel určuje, které osobní údaje jsou nezbytné pro dané zpracování.
- Slučitelnost – každý nový účel musí být slučitelný s původním účelem, pro který byly údaje shromážděny, a musí být vodíkem pro relevantní změny v návrhu.
- Omezení dalšího zpracování – správce by neměl propojovat soubory údajů ani provádět žádné další zpracování pro nové, neslučitelné účely.
- Omezení opětovného použití – správce by měl používat technická opatření, včetně hašování a šifrování, aby omezil možnost použití osobních údajů pro jiné účely. Správce by měl zavést rovněž organizační opatření, jako jsou zásady a smluvní závazky, jež omezují opakované použití osobních údajů.
- Přezkum – správce by měl pravidelně přezkoumávat, zda je zpracování nezbytné pro účely, pro které byly údaje shromážděny, a provést zkoušku návrhu s ohledem na účelové omezení.

Příklad

Správce zpracovává osobní údaje o svých zákaznících. Účelem zpracování je plnění smlouvy, tj. schopnost dodávat výrobky na správnou adresu a obdržet platbu. Ukládají se tyto osobní údaje: historie nákupů, jméno, adresa, e-mailová adresa a telefonní číslo.

Správce zvažuje, že zakoupí produkt pro řízení vztahů se zákazníky, který na jednom místě shromažďuje veškeré údaje o zákaznících, jako jsou tržby, marketing a zákaznické služby. Produkt nabízí možnost ukládat veškeré telefonní hovory, činnosti, dokumenty, e-maily a marketingové kampaně s cílem získat ucelený přehled o daném zákazníkovi. Systém řízení vztahů se zákazníky je mimoto schopen automaticky analyzovat kupní sílu zákazníků s použitím veřejných informací. Účelem analýzy je lépe zacílit reklamní činnosti. Tyto činnosti nejsou součástí původního zákonného účelu zpracování.

Má-li správce jednat v souladu se zásadou účelového omezení, musí od poskytovatele produktu požadovat zmapování jednotlivých činností zpracování, které využívají osobní údaje, a to s ohledem na účely relevantní pro daného správce.

Po obdržení výsledků mapování správce posoudí, zda jsou nový marketingový účel a účel cílené reklamy slučitelné s původními účely vymezenými v době, kdy byly údaje shromážděny, a zda existuje dostatečný právní základ pro příslušné zpracování. Není-li výsledek posouzení kladný, správce k použití příslušných funkcí nepřistoupí. Alternativně by se správce mohl rozhodnout, že od posouzení upustí a popsané funkce produktu jednoduše nebude využívat.

3.5 Minimalizace údajů

73. Je možné zpracovávat pouze takové osobní údaje, které jsou přiměřené, relevantní a omezené na **nezbytný** rozsah ve vztahu k účelu, pro který jsou zpracovávány[36]. Správce proto musí předem určit, které prvky nebo parametry systémů zpracování a jejich podpůrné funkce jsou přípustné. Minimalizace údajů je zhmotněním zásady nezbytnosti a jejím zavedením do praxe. Při dalším zpracování by správce měl pravidelně zvažovat, zda zpracovávané osobní údaje jsou nadále přiměřené, relevantní a nezbytné, nebo zda mají být vymazány či anonymizovány.

74. Správci by měli nejprve určit, zda vůbec potřebují zpracovávat osobní údaje pro své relevantní účely. Správce by měl ověřit, zda lze příslušných účelů dosáhnout zpracováním menšího množství osobních údajů nebo méně podrobných či souhrnných osobních údajů nebo tím, že nemusí osobní údaje zpracovávat vůbec[37]. Toto ověření by se mělo uskutečnit před zpracováním, lze je však provést i kdykoli během cyklu zpracovávání. Tento postup je také v souladu s článkem 11.

75. Minimalizací se může rozumět také míra identifikace. Pokud ke splnění účelu zpracování není nutné, aby závěrečný soubor údajů označoval identifikovanou nebo identifikovatelnou fyzickou osobu (např. ve statistice), k původnímu zpracování to však nutné je (např. před agregací údajů), pak musí správce osobní údaje vymazat nebo anonymizovat, jakmile již není identifikace zapotřebí. Je-li však další identifikace zapotřebí pro jiné činnosti zpracování, měly by být osobní údaje pseudonymizovány za účelem zmírnění rizik pro práva subjektů údajů.

76. Ke klíčovým koncepčním a standardním prvkům s ohledem na minimalizaci údajů může patřit:
    - Předcházení zpracování údajů – předcházejte důsledně zpracování osobních údajů, pokud je to pro daný relevantní účel možné.
    - Omezení – omezte množství shromažďovaných osobních údajů, které jsou nezbytné pro daný účel.
    - Omezení přístupu – Navrhněte zpracování údajů tak, aby přístup k osobním údajům potřeboval k plnění svých povinností minimální počet osob, a odpovídajícím způsobem přístup omezte.
    - Relevantnost – osobní údaje by měly být relevantní pro dané zpracování a správce by měl být schopen tuto relevantnost prokázat.
    - Nezbytnost – každá kategorie osobních údajů musí být nezbytná pro určené účely a měla by být zpracovávána pouze tehdy, není-li možné splnit tento účel jinými prostředky.
    - Agregace – ve vhodných případech používejte souhrnné údaje.
    - Pseudonymizace – pseudonymizujte osobní údaje, jakmile již není nezbytné mít přímo identifikovatelné osobní údaje, a uchovávejte identifikační klíče odděleně.
    - Anonymizace a výmaz – pokud osobní údaje nejsou nebo již nejsou nezbytné pro daný účel, musí být anonymizovány nebo vymazány.
    - Tok údajů – tok údajů by měl být dostatečně efektivní, aby se nevytvářelo více kopií, než je nezbytné.
    - „Stav techniky“ – správce by měl uplatnit nejnovější a vhodné technologie za účelem vyhnutí se sběru dat a minimalizace údajů.

[36] Čl. 5 odst. 1 písm. c) GDPR.
[37] V 39. bodě odůvodnění GDPR se uvádí: „... Osobní údaje by měly být zpracovány pouze tehdy, nemůže-li být účelu zpracování přiměřeně dosaženo jinými prostředky.“

Příklad č. 1

Jisté knihkupectví chce zvýšit své příjmy prodejem knih on-line. Majitel knihkupectví chce vytvořit standardizovaný objednávkový formulář. Aby bylo zajištěno, že zákazníci vyplní veškeré požadované informace, stanoví majitel knihkupectví všechna pole ve formuláři jako povinná (pokud zákazník všechna pole nevyplní, nemůže objednávku zadat). Majitel internetového obchodu zpočátku používá standardní kontaktní formulář, který vyžaduje informace včetně data narození zákazníka, čísla mobilního telefonu a adresy bydliště. Ne všechna pole v tomto formuláři však jsou nezbytná pro zakoupení a doručení knih. Pokud v tomto konkrétním případě platí subjekt údajů za výrobek předem, nejsou datum narození a telefonní číslo subjektu údajů pro nákup výrobku nezbytné. To znamená, že tato pole nemohou být v internetovém formuláři pro objednání výrobku vyžadována, ledaže správce může jednoznačně prokázat, že je to nezbytné, a uvést důvody, proč jsou tato pole nezbytná. Mimoto existují situace, kdy nebude nezbytná ani adresa. Například při objednání elektronické knihy si zákazník může stáhnout výrobek přímo do svého zařízení.

Majitel internetového obchodu se proto rozhodl, že vytvoří dva internetové formuláře: jeden pro objednávání knih, kde bude kolonka pro adresu zákazníka, a jeden internetový formulář pro objednávání elektronických knih bez této kolonky.

Příklad č. 2

Společnost provozující veřejnou dopravu chce shromažďovat statistické informace na základě tras cestujících. Tyto informace jsou užitečné pro náležité rozhodování o změnách v jízdním řádu veřejné dopravy a o vhodných trasách vlaků. Při nástupu do dopravního prostředku nebo výstupu z něj musí cestující pokaždé přiložit jízdenku ke čtečce. Po provedení posouzení rizik v souvislosti s právy a svobodami cestujících, pokud jde o sběr údajů o trasách cestujících, správce dospěje k závěru, že je možné cestující identifikovat v případě, že žijí nebo pracují v řídce osídlených oblastech, a to na základě určení trasy díky identifikátoru na jízdence. Správce by proto neměl ukládat identifikátor na jízdence, protože to není nezbytné za účelem optimalizace jízdních řádů veřejné dopravy a tras vlaků. Jakmile jízda skončí, uloží správce pouze jednotlivé cestovní trasy, aby nebyl schopen identifikovat jízdy spojené s danou konkrétní jízdenkou, a uchová pouze informace o samostatných cestovních trasách.

V případech, kdy přetrvává riziko identifikace určité osoby výlučně na základě její cestovní trasy s využitím veřejné dopravy, zavede správce statistická opatření k snížení rizika, jako je vymazání začátku a konce trasy.

Příklad č. 3

Kurýrní společnost chce posoudit účinnost svých služeb doručování, pokud jde o dobu doručování, rozvrh pracovní zátěže a spotřebu paliva. Aby dosáhla tohoto cíle, musí kurýr zpracovávat řadu osobních údajů týkajících se jak zaměstnanců (řidičů), tak zákazníků (adresy, předměty, které mají být doručeny, atd.). Tato operace zpracování zahrnuje rizika, a to jak z hlediska sledování zaměstnanců, které vyžaduje zvláštní právní záruky, tak z hlediska sledování návyků zákazníků prostřednictvím znalostí o doručovaných předmětech v průběhu času. Tato rizika mohou být významně snížena vhodnou pseudonymizací zaměstnanců a zákazníků. Zejména pokud jsou často obměňovány pseudonymizační klíče a zohledňují se větší územní celky namísto podrobných adres, jedná se o účinnou minimalizaci údajů a správce se může zaměřit výlučně na proces doručování a na účel

optimalizace zdrojů, aniž by byla překročena únosná mez sledování chování jednotlivců (zákazníků nebo zaměstnanců).

Příklad č. 4

Nemocnice shromažďuje údaje o svých pacientech v nemocničním informačním systému (elektronický zdravotní záznam). Personál nemocnice musí mít přístup ke spisům pacientů, aby mohl rozhodovat o péči a léčbě pacientů a dokumentovat veškerá přijatá diagnostická, pečovatelská a léčebná opatření. Přístup je standardně umožněn pouze těm zdravotnickým pracovníkům, kteří jsou pověřeni léčením příslušného pacienta na specializovaném oddělení, jemuž je přidělen. Skupina osob, které mají přístup ke spisu pacienta, se rozšíří, pokud jsou do léčby zapojena další oddělení nebo diagnostické jednotky. Po propuštění pacienta a dokončení vyúčtování je přístup omezen na malou skupinu zaměstnanců specializovaného oddělení, kteří odpovídají na žádosti o lékařské informace nebo o konzultaci, které po schválení příslušným pacientem podali nebo si vyžádali jiní poskytovatelé zdravotnických služeb.

3.6 Přesnost

77. Osobní údaje musí být přesné a aktualizované a 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[38].

78. Na tyto požadavky je třeba nahlížet v souvislosti s riziky a důsledky konkrétního použití údajů. Nepřesné osobní údaje by mohly představovat riziko pro práva a svobody subjektů údajů, například pokud vedou k chybné diagnóze nebo nesprávné léčbě, jedná-li se o zdravotní záznamy, nebo nesprávný obraz o určité osobě může vést k přijetí rozhodnutí vycházejícího z chybných předpokladů, ať už manuálně, za použití automatizovaného rozhodování, nebo prostřednictvím umělé inteligence.

79. Ke klíčovým koncepčním a standardním prvkům s ohledem na přesnost může patřit:
- Zdroj údajů – zdroje osobních údajů by měly být spolehlivé, pokud jde o přesnost údajů.
- Míra přesnosti – každý prvek osobních údajů by měl být tak přesný, jak je to nezbytné pro určené účely.
- Měřitelně přesné – snížení počtu falešně pozitivních/negativních výstupů, například zkreslení v rámci automatizovaných rozhodnutí a umělé inteligence.
- Ověřování – podle povahy údajů by měl správce v souvislosti s tím, jak často se mohou měnit, ověřovat u subjektů údajů správnost osobních údajů před zahájením zpracování a v jednotlivých fázích zpracování (např. požadavky na věk).
- Výmaz/oprava – správce musí nepřesné údaje neprodleně vymazat nebo opravit. Správce to usnadní zejména v případě, že subjekty údajů jsou nebo byly dětmi, a později si přejí tyto osobní údaje odstranit[39].
- Zamezení šíření chyb – správce by měl zmírňovat účinek nahromaděných chyb v řetězci zpracování.
- Přístup – subjekty údajů by měly obdržet informace o osobních údajích a získat účinný přístup k nim v souladu s články 12 až 15 GDPR s cílem ověřovat jejich správnost a provádět případné opravy.

[38] Čl. 5 odst. 1 písm. d) GDPR.
[39] Viz 65. bod odůvodnění.

- Trvalá správnost – osobní údaje by měly být přesné ve všech fázích zpracování, v kriticky důležitých bodech je třeba provádět ověření přesnosti.
- Aktuálnost – osobní údaje musí být aktualizované, je-li to nezbytné pro daný účel.
- Návrh údajů – používání technologických a organizačních prvků návrhu ke snížení nepřesnosti, například předkládání stručných předem určených možností místo polí pro libovolný text.

Příklad č. 1

Pojišťovna chce využít umělou inteligenci k profilování zákazníků pořizujících pojištění jako základ pro rozhodování při výpočtu pojistného rizika. Při určování, jakým způsobem by měla být vyvíjena řešení v oblasti umělé inteligence, stanoví prostředky zpracování a při výběru aplikace umělé inteligence u prodejce a při rozhodování, jak umělou inteligenci vyškolit, zohlední záměrnou ochranu osobních údajů.

Při určování, jak vyškolit umělou inteligenci, by správce měl mít přesné údaje k dosažení přesných výsledků. Správce by měl proto zajistit, aby údaje použité k vyškolení umělé inteligence byly přesné.

Za podmínky, že existuje platný právní základ pro školení umělé inteligence s použitím osobních údajů od velkého okruhu stávajících zákazníků, vybere správce skupinu zákazníků, která je reprezentativní pro danou populaci, aby se předešlo předpojatosti.

Údaje o zákaznících jsou poté získány z příslušného systému zpracování údajů, včetně údajů o druhu pojištění, například zdravotního pojištění, pojištění domácnosti, cestovního pojištění atd., jakož i údajů z veřejných rejstříků, k nimž existuje zákonný přístup. Před přenosem do systému určeného pro školení modelu umělé inteligence jsou všechny údaje pseudonymizovány.

Aby se zajistilo, že údaje používané ke školení umělé inteligence jsou co nejpřesnější, shromažďuje správce pouze údaje ze zdrojů údajů obsahujících správné a aktuální informace.

Pojišťovna testuje, zda je umělá inteligence spolehlivá a zda poskytuje nediskriminační výsledky jak během vývoje, tak i před konečným uvolněním produktu. Jakmile je umělá inteligence plně vyškolena a funkční, využívá pojišťovna výsledky na podporu posouzení pojistných rizik, aniž by se však při rozhodování o tom, zda poskytne pojištění, spoléhala pouze na umělou inteligenci, pokud není rozhodnutí přijato v souladu s výjimkami uvedenými v čl. 22 odst. 2 GDPR.

Pojišťovna bude rovněž pravidelně přezkoumávat výsledky umělé inteligence, aby zachovala spolehlivost a v případě potřeby algoritmus upravila.

Příklad č. 2

Správcem je zdravotnická instituce, která chce stanovit metody, jak zajistit integritu a přesnost osobních údajů v registrech klientů.

V případech, kdy do instituce přijedou dvě osoby současně a podstoupí stejnou léčbu, existuje riziko, že dojde k záměně, je-li jediným parametrem, kterým se liší, jméno. K zajištění přesnosti potřebuje správce pro každou osobu jedinečný identifikátor, a tudíž více informací než jen jméno klienta.

Instituce používá několik systémů obsahujících osobní informace klientů a musí zajistit, aby informace týkající se daného klienta byly ve všech systémech a vždy správné, přesné a jednotné. Instituce určila několik rizik, která mohou vyvstat, jestliže se informace změní v jednom systému, v jiném však nikoli.

Správce se rozhodne zmírnit riziko tím, že použije hašování, jež lze využít k zajištění integrity údajů v záznamech o léčbě. Jsou vytvořena neměnná kryptografická časová razítka pro pořizování záznamů o léčbě a o příslušném klientovi, aby bylo možné rozeznat, dát do vzájemného vztahu a případně sledovat veškeré změny.

3.7 Omezení uložení

80. Správce musí zajistit, aby byly osobní údaje uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou osobní údaje zpracovávány[40].
Je zásadní, aby správce přesně věděl, jaké osobní údaje společnost zpracovává a proč. Účel zpracování je hlavním kritériem při rozhodování o tom, jak dlouho mají být osobní údaje uloženy.

81. Opatření a záruky, které provádějí zásadu omezení uložení, musí doplňovat práva a svobody subjektů údajů, konkrétně právo na výmaz a právo vznést námitku.

82. Ke klíčovým koncepčním a standardním prvkům s ohledem na omezení uložení může patřit:
- Výmaz a anonymizace – správce by měl mít jednoznačné interní postupy a funkce pro výmaz a/nebo anonymizaci.
- Účinnost anonymizace/výmazu – správce musí zajistit, aby nebylo možné opětovně identifikovat anonymizované údaje nebo zpětně získat vymazané údaje, a měl by pokud možno provádět zkoušky.
- Automatizace – výmaz některých osobních údajů by měl být automatizován.
- Kritéria uložení – správce musí určit, jaké údaje a jaká doba uložení jsou pro daný účel nezbytné.
- Odůvodnění – správce musí být schopen odůvodnit, proč je doba uložení nezbytná pro daný účel a dotyčné osobní údaje, a musí být schopen uvést odůvodnění a právní důvody pro dobu uchovávání.
- Prosazování zásad uchovávání údajů – správce by měl prosazovat interní zásady uchovávání údajů a provádět zkoušky, zda organizace tyto zásady uplatňuje v praxi.
- Záložní soubory / protokoly – správce musí určit, které osobní údaje a jaká doba uložení jsou nezbytné pro záložní soubory a protokoly.
- Tok údajů – správci by měli mít povědomí o toku osobních údajů a ukládání jejich kopií a snažit se omezit jejich „dočasné“ uložení.

Příklad

Správce shromažďuje osobní údaje, přičemž účelem zpracování je správa členství subjektu údajů. Osobní údaje se vymažou po ukončení členství a neexistuje právní základ pro další uchovávání údajů.

Správce nejprve stanoví interní postup pro uchovávání údajů a jejich výmaz. Podle tohoto postupu musí zaměstnanci ručně smazat osobní údaje po skončení doby uchovávání. Zaměstnanec se tímto postupem řídí a pravidelně vymazává a opravuje údaje z veškerých zařízení, ze záložních souborů, protokolů, e-mailů a jiných relevantních paměťových médií.

Aby správce zajistil větší efektivnost výmazů a menší náchylnost k chybám, zavedl místo toho automatický systém, který vymazává údaje automaticky, spolehlivě a pravidelněji. Systém je nastaven tak, aby se řídil zadanými postupy pro výmaz údajů, ke kterému dochází v předem nastavených

[40] Čl. 5 odst. 1 písm. c) GDPR.

pravidelných intervalech za účelem odstranění osobních údajů ze všech paměťových médií v dané společnosti. Správce pravidelně přezkoumává a testuje postup uchovávání údajů a zajišťuje, že odpovídá aktuálním zásadám uchovávání údajů.

3.8 Integrita a důvěrnost

83. Zásada integrity a důvěrnosti zahrnuje ochranu pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Bezpečnost osobních údajů vyžaduje vhodná opatření určená k předcházení incidentům spočívajícím v porušení zabezpečení osobních údajů a jejich řešení; zaručení řádného plnění úkolů souvisejících se zpracováním údajů a dodržování ostatních zásad a usnadnění účinného výkonu práv fyzických osob.

84. V 78. bodě odůvodnění se uvádí, že by jedno z opatření v oblasti záměrné a standardní ochrany osobních údajů mohlo spočívat v umožnění správcům *„vytvářet a zlepšovat bezpečnostní prvky“*. Spolu s jinými opatřeními v oblasti záměrné a standardní ochrany osobních údajů se v 78. bodě odůvodnění uvádí, že správci mají povinnost průběžně posuzovat, zda stále používají vhodné prostředky zpracování, a hodnotit, zda zvolená opatření skutečně pomáhají odstranit stávající slabá místa. Správci by měli mimoto provádět pravidelné přezkumy opatření pro bezpečnost informací, která obklopují a chrání osobní údaje, a také postupu pro řešení případů porušení zabezpečení osobních údajů.

85. Ke klíčovým koncepčním a standardním prvkům s ohledem na integritu a důvěrnost může patřit:
    - Systém řízení bezpečnosti informací – existence operativních prostředků pro řízení strategií a postupů v oblasti bezpečnosti informací.
    - Analýza rizik – posuzování rizik s ohledem na zabezpečení osobních údajů, a to zvážením dopadu na práva fyzických osob, a přijímání opatření proti zjištěným rizikům. Pro použití při posuzování rizik vyvinout a udržovat komplexní, systematické a realistické „modelování hrozeb“ a analýzu prostoru k útoku u navrženého softwaru k omezení cest vedení útoku a příležitostí k využití slabých a zranitelných míst.
    - Bezpečnost již od fáze návrhu – zohlednění bezpečnostních požadavků co nejdříve při navrhování a vývoji systému a průběžné začleňování a provádění příslušných testů.
    - Údržba – pravidelné posuzování a testování softwaru, hardwaru, systémů a služeb atd. s cílem odhalit slabá místa systémů podporujících zpracování.
    - Řízení kontroly přístupu – pouze oprávnění pracovníci, kteří to potřebují, by měli mít přístup k osobním údajům nezbytným pro plnění úkolů v oblasti zpracování a správce by měl rozlišovat práva přístupu oprávněných pracovníků.
        - Omezení přístupu (zmocněnci) – zpracování údajů je navrženo tak, aby minimální počet osob potřeboval k plnění svých povinností přístup k osobním údajům, a přístup je odpovídajícím způsobem omezen.
        - Omezení přístupu (obsah) – v kontextu každé operace zpracování je přístup omezen pouze na atributy souboru údajů, které jsou zapotřebí k provedení této operace. Mimoto je přístup omezen na údaje týkající se těch subjektů údajů, které spadají do působnosti příslušného zaměstnance.
        - Oddělení přístupu – zpracování údajů je navrženo tak, aby žádný jednotlivec nepotřeboval komplexní přístup ke všem shromážděným údajům o subjektu údajů, a ještě méně ke všem osobním údajům určité kategorie subjektů údajů.
    - Zabezpečené předávání – předávání musí být zabezpečeno před neoprávněným náhodným a přístupem a změnami.

- Bezpečné úložiště – úložiště údajů musí být zabezpečeno před neoprávněným přístupem a změnami. Měly by existovat postupy pro posouzení rizika centralizovaného nebo decentralizovaného uložení a kategorií osobních údajů, na které se to vztahuje. Některé údaje mohou vyžadovat dodatečná bezpečnostní opatření než jiná nebo oddělení od jiných údajů.
- Pseudonymizace – osobní údaje a záložní soubory / protokoly by měly být pseudonymizovány jako bezpečnostní opatření za účelem minimalizace rizik, jež představují možné případy porušení zabezpečení osobních údajů, například pomocí hašování nebo šifrování.
- Záložní soubory / protokoly – uchovávání záložních souborů a protokolů v rozsahu, který je nezbytný pro bezpečnost informací, používání auditních stop a sledování událostí v rámci běžné bezpečnostní kontroly. Tyto soubory a protokoly jsou chráněny před neoprávněným a náhodným přístupem a změnami a jsou pravidelně přezkoumávány a incidenty by měly být řešeny neprodleně.
- Obnova po havárii / kontinuita činnosti – řešení požadavků na obnovení informačního systému po havárii a zachování kontinuity provozu k obnovení dostupnosti osobních údajů v návaznosti na závažné incidenty.
- Ochrana podle rizika – všechny kategorie osobních údajů by měly být chráněny vhodnými opatřeními, pokud jde o riziko porušení zabezpečení. Údaje představující zvláštní rizika by měly být pokud možno uchovávány odděleně od ostatních osobních údajů.
- Řízení reakce na bezpečnostní incident – zavedení rutinních procesů, postupů a zdrojů s cílem odhalit porušení zabezpečení osobních údajů, řešit je, ohlásit a vyvodit z nich důsledky.
- Řízení incidentů – správce by měl mít zavedeny postupy pro řešení případů porušení zabezpečení a incidentů, aby byl systém zpracování spolehlivější. To zahrnuje postupy oznamování, jako je řízení oznamování (dozorovému úřadu) a informování (subjektů údajů).

Příklad

Správce chce získat velké množství osobních údajů z lékařské databáze obsahující elektronické zdravotní záznamy (pacientů) pro zvláštní databázový server společnosti za účelem zpracování získaných údajů k zajištění kvality. Společnost posoudila riziko přesměrování získaných údajů na server, který je přístupný všem zaměstnancům společnosti, a dospěla k závěru, že je pravděpodobné, že riziko pro práva a svobody subjektů údajů bude vysoké. Jelikož ve společnosti existuje pouze jedno oddělení, které musí zpracovávat extrahované údaje o pacientech, správce se rozhodne omezit přístup ke zvláštnímu serveru na zaměstnance tohoto oddělení. Aby se riziko dále snížilo, budou údaje před předáním pseudonymizovány.

Společnost se v zájmu řízení přístupu a zmírnění újmy, kterou by mohl způsobit malware, rozhodne danou síť oddělit a stanovit kontroly přístupu k serveru. Kromě toho zavede systém pro monitorování zabezpečení a pro odhalování a prevenci vniknutí a oddělí jej od běžného používání. Je zaveden automatizovaný systém kontroly, který má sledovat přístup a změny. Z něj se generují zprávy a automatizovaná upozornění, pokud jsou v konfiguraci nastaveny určité události související s používáním. Správce zajistí, aby uživatelé měli přístup pouze k údajům, které potřebují znát, v souladu s vhodnou úrovní přístupu. Nevhodné použití lze rychle a snadno odhalit.

Některé extrahované údaje musí být porovnávány s novými extrahovanými údaji, a proto musí být uloženy po dobu tří měsíců. Správce se rozhodne vložit je do samostatných databází na témže serveru a k jejich uložení použít jak transparentní šifrování, tak i šifrování na úrovni sloupců. Klíče pro dešifrování sloupců jsou uloženy ve speciálních bezpečnostních modulech, které mohou použít pouze oprávnění zaměstnanci, nelze je však extrahovat.

Řešení nadcházejících incidentů činí systém důkladnějším a spolehlivějším. Správce údajů chápe, že by do všech případů zpracování osobních údajů, které provádí a bude provádět, měla být začleněna

preventivní a účinná opatření a záruky a že tím může v budoucnu pomoci zabránit takovýmto případům porušení zabezpečení osobních údajů.

Správce tato bezpečnostní opatření zavádí jednak proto, aby zajistil přesnost, integritu a důvěrnost, a jednak proto, aby zabránil šíření malwaru při kybernetických útocích a posílil tak robustnost řešení. Existence důkladných bezpečnostních opatření přispívá k budování důvěry se subjekty údajů.

3.9 Odpovědnost[41]

86. Zásada odpovědnosti stanoví, že správce odpovídá za dodržování všech výše uvedených zásad a je schopen toto dodržování prokázat.

87. Správce musí být schopen prokázat soulad se zásadami. Správce přitom může prokázat účinky opatření přijatých na ochranu práv subjektů údajů a důvody, proč jsou tato opatření považována za vhodná a účinná. Například prokázání toho, proč je opatření vhodné k účinnému zajištění zásady omezení uložení.

88. Aby mohl správce osobní údaje zodpovědně zpracovávat, měl by mít znalosti o ochraně údajů i schopnost tuto ochranu provádět. To znamená, že by správce měl chápat své povinnosti v oblasti ochrany údajů vyplývající z GDPR a být schopen tyto povinnosti plnit.

4 USTANOVENÍ ČL. 25 ODST. 3 TÝKAJÍCÍ SE VYDÁVÁNÍ OSVĚDČENÍ

89. Podle čl. 25 odst. 3 lze jako jeden z prvků, jimiž lze doložit soulad se záměrnou a standardní ochranou osobních údajů, použít vydávání osvědčení podle článku 42. V procesu vydávání osvědčení mohou být užitečné dokumenty prokazující soulad se záměrnou a standardní ochranou osobních údajů. To znamená, že pokud bylo operaci zpracování správcem nebo zpracovatelem vydáno osvědčení podle článku 42, dozorové úřady to zohlední ve svém celkovém posouzení souladu s GDPR, konkrétně pak s ohledem na záměrnou a standardní ochranu osobních údajů.

90. Je-li pro operaci zpracování správcem nebo zpracovatelem vydáno osvědčení podle článku 42, patří k prvkům, které přispívají k prokázání souladu s čl. 25 odst. 1 a 2, procesy navrhování, tj. postup určování prostředků zpracování, správy a technických a organizačních opatření k provádění zásad ochrany údajů. Kritéria pro vydávání osvědčení o ochraně údajů stanoví subjekty pro vydávání osvědčení nebo vlastníci systémů pro vydávání osvědčení a poté je schválí příslušný dozorový úřad nebo EDPB. Pokud jde o další informace o mechanismech pro vydávání osvědčení, odkazujeme čtenáře na pokyn EDPB k vydávání osvědčení[42] a jiné příslušné pokyny, které jsou zveřejněny na internetových stránkách EDPB.

91. I v případě, že je pro zpracování uděleno osvědčení v souladu s článkem 42, má správce stále odpovědnost za průběžné sledování a zlepšování souladu s kritérii záměrné a standardní ochrany osobních údajů stanovenými v článku 25.

[41] Viz 74. bod odůvodnění, v němž se vyžaduje, aby správci prokázali účinnost svých opatření.
[42] EDPB. „Pokyny 1/2018 týkající se vydávání osvědčení a určování kritérií pro vydávání osvědčení podle článků 42 a 43 nařízení“. Verze 3.0, 4. června 2019.
edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_cs.pdf

5 PROSAZOVÁNÍ ČLÁNKU 25 A DŮSLEDKY

92. Dozorové úřady mohou posoudit dodržování článku 25 v souladu s postupy uvedenými v článku 58. V čl. 58 odst. 2 jsou uvedeny nápravné pravomoci, mezi něž patří upozornění, napomenutí, nařízení dodržovat práva subjektů údajů, omezení nebo zákaz zpracování, správní pokuty atd.

93. Záměrná a standardní ochrana osobních údajů je také jedním z faktorů při určování výše peněžitých pokut za porušení GDPR, viz čl. 83 odst. 4[43] [44].

6 DOPORUČENÍ

94. Ačkoli se jimi článek 25 přímo nezabývá, zpracovatelé a zhotovitelé jsou rovněž považováni za klíčové aktéry umožňující záměrnou a standardní ochranu osobních údajů a měli by si být vědomi toho, že správci jsou povinni zpracovávat osobní údaje pouze pomocí systémů a technologií, které zahrnují ochranu osobních údajů.

95. Při provádění zpracování jménem správců nebo při poskytování řešení správcům by zpracovatelé a zhotovitelé měli využít své odborné znalosti k budování důvěry a pomoci svým zákazníkům, včetně malých a středních podniků, při navrhování/pořizování řešení, která začleňují do procesu zpracování ochranu údajů. To znamená, že by koncepce produktů a služeb měla usnadnit uspokojování potřeb správců.

96. Při provádění článku 25 je třeba mít na paměti, že hlavním cílem návrhu je *účinné provádění* zásad a *ochrana* práv subjektů údajů v rámci vhodných opatření zpracování. S cílem usnadnit a posílit přijetí zásad záměrné a standardní ochrany osobních údajů předkládáme správcům, zhotovitelům a zpracovatelům tato doporučení:
    - Správci by měli pamatovat na ochranu osobních údajů od *počátečních fází* plánování operace zpracování, dokonce ještě před určením prostředků zpracování.
    - Pokud má správce pověřence pro ochranu osobních údajů, EDPB podporuje aktivní zapojení pověřence pro ochranu osobních údajů do začlenění zásad záměrné a standardní ochrany osobních údajů do postupů zadávání zakázek a vývoje, jakož i do celého cyklu zpracování.
    - Pro operaci zpracování je možné vydat *osvědčení*. Možnost získat pro operaci zpracování osvědčení poskytuje správci přidanou hodnotu při výběru mezi různým softwarem, hardwarem, službami a/nebo systémy pro zpracování od zhotovitelů nebo zpracovatelů. Zhotovitelé by proto měli usilovat o prokázání záměrné a standardní ochrany osobních údajů v celém cyklu vývoje řešení pro zpracování. Certifikační značka může být rovněž vodítkem pro subjekty údajů při výběru mezi různými druhy zboží a služeb. Možnost získat pro zpracování osvědčení slouží jako konkurenční výhoda pro zhotovitele, zpracovatele i správce, a může dokonce posílit důvěru subjektů údajů ve zpracování jejich osobních údajů. Pokud se osvědčení nevydává, měli by se správci snažit poskytnout jiné *záruky*, že zhotovitelé nebo zpracovatelé dodržují požadavky záměrné a standardní ochrany osobních údajů.

[43] V čl. 83 odst. 2 písm. d) GDPR se stanoví, že při rozhodování o uložení pokut za porušení GDPR *„se řádně zohlední“ [...] „míra odpovědnosti správce či zpracovatele s přihlédnutím k technickým a organizačním opatřením jimi zavedeným podle článků 25 a 32“.*

[44] Více informací o pokutách je uvedeno v dokumentu pracovní skupiny zřízené podle článku 29. „Pokyny k uplatňování a stanovování správních pokut pro účely nařízení 2016/679“. WP 253, 3. října 2017. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 – schváleno EDPB.

- Správci, zpracovatelé a zhotovitelé by měli zvážit své povinnosti poskytovat dětem mladším 18 let a dalším zranitelným skupinám zvláštní ochranu při dodržování zásad záměrné a standardní ochrany osobních údajů.
- Zhotovitelé a zpracovatelé by se měli snažit usnadnit provádění zásad záměrné a standardní ochrany osobních údajů s cílem podpořit schopnost správce plnit povinnosti podle článku 25. Správci by na druhé straně neměli vybírat zhotovitele nebo zpracovatele, kteří nenabízejí systémy, jež správci umožňují být v souladu s článkem 25 nebo jej přitom podporují, neboť za nedostatečné provedení ustanovení tohoto článku nesou odpovědnost správci.
- Zhotovitelé a zpracovatelé by měli hrát aktivní úlohu při zajišťování toho, že jsou splněna kritéria „stavu techniky“, a uvědomit správce o veškerých změnách „stavu techniky“, jež mohou mít vliv na účinnost opatření, která zavedli. Správci by také měli zahrnout tento požadavek jako smluvní doložku, aby byla zajištěna aktuálnost.
- EDPB správcům doporučuje, aby od zhotovitelů a zpracovatelů požadovali doložení toho, jak jejich hardware, software, služby nebo systémy umožní správci plnit požadavky na odpovědnost v souladu se zásadami záměrné a standardní ochrany osobních údajů, například použitím klíčových ukazatelů výkonnosti k prokázání účinnosti opatření a záruk při provádění zásad a práv.
- EDPB zdůrazňuje, že je nutné zaujmout harmonizovaný přístup k účinnému provádění zásad, a vybízí sdružení nebo subjekty, které vypracovávají kodexy chování v souladu s článkem 40, aby do nich začlenily rovněž odvětvové pokyny k záměrné a standardní ochraně osobních údajů.
- Správci by měli být korektní vůči subjektům údajů a transparentní, pokud jde o to, jak posuzují a prokazují účinné provádění záměrné a standardní ochrany osobních údajů, a postupovat stejným způsobem, jakým prokazují soulad s GDPR podle zásady odpovědnosti.
- Jako opatření v souladu s požadavky na záměrnou a standardní ochranu osobních údajů v rámci přístupu založeného na posouzení rizik mohou být případně použity technologie zvyšující ochranu soukromí, které dosáhly dostatečné vyspělosti. Technologie zvyšující ochranu soukromí samy o sobě nemusí nutně zahrnovat povinnosti podle článku 25. Správci posoudí, zda je opatření vhodné a účinné při provádění zásad ochrany údajů a práv subjektů údajů.
- Na existující starší systémy se vztahují stejné povinnosti týkající se záměrné a standardní ochrany osobních údajů jako na nové systémy. Pokud starší systémy již nejsou v souladu se zásadami záměrné a standardní ochrany osobních údajů a nelze provést změny za účelem splnění povinností, pak starší systém jednoduše nesplňuje povinnosti vyplývající z GDPR a nelze jej použít ke zpracování osobních údajů.
- Článek 25 nesnižuje práh požadavků pro malé a střední podniky. Dodržování článku 25 malými a středními podniky mohou usnadnit tyto body:
    - provést včasné posouzení rizik
    - začít malým zpracováním – poté rozšířit jeho rozsah a důkladnost
    - vyhledat záruky zhotovitelů a zpracovatelů týkající se záměrné a standardní ochrany osobních údajů, jako je vydávání osvědčení a dodržování kodexů chování
    - využívat partnery s dobrými výsledky
    - hovořit s orgány pro ochranu údajů
    - prostudovat pokyny orgánů pro ochranu údajů a EDPB
    - dodržovat kodexy chování, jsou-li k dispozici
    - vyžádat si odbornou pomoc a poradenství

Za Evropský sbor pro ochranu osobních údajů

předsedkyně

(Andrea Jelinek)