Usmernenia 4/2019 týkajúce sa článku 25

Špecificky navrhnutá a štandardná ochrana údajov

Verzia 2.0

Prijaté 20. októbra 2020

História verzií

Verzia 1.0	13. november 2019	Prijatie usmernení na účely verejnej konzultácie
Verzia 2.0	20. októbra 2020	Prijatie usmernení EDPB po verejnej konzultácii

Obsah

Európsky výbor pre ochranu údajov

so zreteľom na článok 70 ods. 1 písm. e) nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“),

so zreteľom na Dohodu o EHP, najmä na jej prílohu XI a protokol 37 k nej, ktoré boli zmenené rozhodnutím Spoločného výboru EHP č. 154/2018 zo 6. júla 2018,

so zreteľom na článok 12 a článok 22 svojho rokovacieho poriadku,

PRIJAL TIETO USMERNENIA:

Zhrnutie

Dodržiavanie požiadaviek špecificky navrhnutej a štandardnej ochrany údajov zohráva v tomto čoraz digitalizovanejšom svete kľúčovú úlohu pri presadzovaní ochrany súkromia a údajov v spoločnosti. Preto je nevyhnutné, aby prevádzkovatelia brali túto zodpovednosť vážne a pri navrhovaní spracovateľských operácií plnili povinnosti vyplývajúce zo všeobecného nariadenia o ochrane údajov.

Tieto usmernenia poskytujú všeobecné usmernenia k povinnosti týkajúcej sa špecificky navrhnutej a štandardnej ochrany údajov (ďalej len „ŠNaŠOÚ“) uvedenej v článku 25 všeobecného nariadenia o ochrane údajov. Špecificky navrhnutá a štandardná ochrana údajov predstavuje povinnosť pre všetkých prevádzkovateľov bez ohľadu na rozsah a rozličnú zložitosť spracúvania. Na to, aby prevádzkovateľ mohol plniť požiadavky ŠNaŠOÚ, je veľmi dôležité, aby rozumel zásadám ochrany údajov a právam a slobodám dotknutej osoby.

Hlavnou povinnosťou je prijať *primerané* [appropriate] opatrenia a nevyhnutné záruky, ktoré zabezpečia *účinné vykonávanie zásad ochrany údajov* a následne *práv a slobôd dotknutých osôb špecificky navrhnutou a štandardnou ochranou údajov*. Článok 25 stanovuje prvky špecificky navrhnutej aj štandardnej ochrany údajov, ktoré je potrebné zohľadniť. Tieto prvky budú podrobnejšie opísané v týchto usmerneniach.

Článok 25 ods. 1 ustanovuje, že prevádzkovatelia by mali ŠNaŠOÚ zvážiť už keď plánujú novú spracovateľskú operáciu. Prevádzkovatelia musia vykonávať ŠNaŠOÚ *pred* spracúvaním a aj *neustále* počas spracúvania, a to pravidelným prehodnocovaním účinnosti vybraných opatrení a záruk. Špecificky navrhnutá a štandardná ochrana údajov sa vzťahuje aj na existujúce systémy, ktoré spracúvajú osobné údaje.

Tieto usmernenia obsahujú aj usmernenia k tomu, ako účinne vykonávať zásady ochrany údajov uvedené v článku 5, a uvádzajú kľúčové prvky špecificky navrhnutej a štandardnej ochrany údajov, ako aj praktické názorné príklady. Prevádzkovateľ by mal zvážiť primeranosť [appropriateness] navrhovaných opatrení v kontexte konkrétneho spracúvania.

Európsky výbor pre ochranu údajov (ďalej len „EDPB“) poskytuje odporúčania k tomu, ako môžu prevádzkovatelia, sprostredkovatelia a výrobcovia spolupracovať na dosahovaní ŠNaŠOÚ. Nabáda prevádzkovateľov v odvetví, sprostredkovateľov a výrobcov, aby používali ŠNaŠOÚ ako prostriedok na

dosiahnutie konkurenčnej výhody pri uvádzaní svojich produktov na trh pre prevádzkovateľov a dotknuté osoby. Takisto nabáda všetkých prevádzkovateľov, aby využívali certifikáciu a kódexy správania.

1 ROZSAH PÔSOBNOSTI

1. Tieto usmernenia sa zameriavajú na to, ako prevádzkovatelia vykonávajú ŠNaŠOÚ na základe povinnosti stanovenej v článku 25 všeobecného nariadenia o ochrane údajov.[1] Aj pre ďalšie subjekty, ako sú sprostredkovatelia a výrobcovia produktov, služieb a aplikácií (ďalej len „výrobcovia"), na ktorých sa článok 25 priamo nevzťahuje, môžu byť tieto usmernenia užitočné pri vytváraní produktov a služieb, ktoré sú v súlade so všeobecným nariadením o ochrane údajov a ktoré prevádzkovateľom umožňujú plniť ich povinnosti v oblasti ochrany údajov.[2] Odôvodnenie 78 všeobecného nariadenia o ochrane údajov uvádza, že špecificky navrhnutá a štandardná ochrana údajov by sa mala zohľadniť aj v súvislosti s verejným obstarávaním. Napriek tomu, že všetci prevádzkovatelia majú povinnosť začleniť ŠNaŠOÚ do svojich spracovateľských činností, v tomto ustanovení sa podporuje prijatie zásad ochrany osobných údajov, pri ktorých by verejná správa mala ísť príkladom. Prevádzkovateľ je zodpovedný za plnenie povinností v oblasti špecificky navrhnutej a štandardnej ochrany údajov, pokiaľ ide o spracúvanie vykonávané jeho sprostredkovateľmi a sub-sprostredkovateľmi, a preto by to mal zohľadniť pri uzatváraní zmlúv s týmito stranami.

2. Požiadavka opísaná v článku 25 sa vzťahuje na prevádzkovateľov, aby mali navrhnutú ochranu údajov pri spracúvaní osobných údajov a ako štandardné nastavenie a uplatňovali ju počas celého životného cyklu spracúvania. Požiadavka ŠNaŠOÚ sa vzťahuje aj na systémy spracúvania, ktoré existovali pred nadobudnutím účinnosti všeobecného nariadenia o ochrane údajov. Prevádzkovatelia musia spracúvanie neustále aktualizovať v súlade so všeobecným nariadením o ochrane údajov. Ďalšie informácie o tom, ako udržiavať existujúci systém v súlade so ŠNaŠOÚ, sa nachádzajú v podkapitole 2.1.4 týchto usmernení. Podstatou tohto ustanovenia je zabezpečiť *primeranú* a *účinnú* ochranu osobných údajov pri *špecificky navrhnutej* aj *štandardnej* ochrane údajov, čo znamená, že prevádzkovatelia by mali byť schopní preukázať, že majú v rámci spracúvania zavedené primerané opatrenia a záruky, aby sa zabezpečilo, že sa účinne uplatňujú zásady ochrany údajov a práva a slobody dotknutých osôb.

3. Druhá kapitola týchto usmernení sa zameriava na výklad požiadaviek stanovených v článku 25 a skúmajú sa v nej právne záväzky zavedené týmto ustanovením. Príklady spôsobov uplatňovania ŠNaŠOÚ v súvislosti s osobitnými zásadami ochrany údajov sú uvedené v kapitole 3.

4. V kapitole 4 týchto usmernení sa rieši možnosť zavedenia certifikačného mechanizmu na preukázanie súladu s článkom 25 a v kapitole 5 sa pozornosť zameriava na spôsob, ako môžu dozorné orgány tento článok presadzovať. V usmerneniach sa na záver poskytujú zainteresovaným stranám ďalšie odporúčania, ako úspešne implementovať ŠNaŠOÚ. EDPB uznáva výzvy, ktorým čelia malé a stredné

[1] Uvedené výklady sa vzťahujú aj na článok 20 smernice (EÚ) 2016/680 a článok 27 nariadenia 2018/1725.

[2] V odôvodnení 78 všeobecného nariadenia o ochrane údajov sa jasne uvádza táto potreba: *„Pri vypracovaní, navrhovaní, výbere a používaní aplikácií, služieb a produktov, ktoré sú založené na spracúvaní osobných údajov alebo spracúvajú osobné údaje, aby splnili svoju úlohu, by sa výrobcovia týchto produktov, služieb a aplikácií mali vyzvať, aby pri vypracovaní a navrhovaní takýchto produktov, služieb a aplikácií zohľadnili právo na ochranu údajov, pričom náležite zohľadnia najnovšie poznatky, aby sa zabezpečilo, že prevádzkovatelia a sprostredkovatelia môžu plniť svoje povinnosti týkajúce sa ochrany údajov."*

podniky (ďalej len „MSP“) pri plnom dodržiavaní povinností v oblasti ŠNaŠOÚ, a v kapitole 6 poskytuje doplňujúce odporúčania osobitne pre MSP.

2 ANALÝZA ČLÁNKU 25 ODS. 1 A 2 ŠPECIFICKY NAVRHNUTÁ A ŠTANDARDNÁ OCHRANA ÚDAJOV

5. Cieľom tejto kapitoly je preskúmať a poskytnúť usmernenia k požiadavkám na špecificky navrhnutú ochranu údajov podľa článku 25 ods. 1 a na štandardnú ochranu údajov podľa článku 25 ods. 2. Špecificky navrhnutá ochrana údajov a štandardná ochrana údajov sú vzájomne sa dopĺňajúce koncepcie, ktoré sa navzájom posilňujú. Dotknuté osoby budú mať väčší prospech zo štandardnej ochrany údajov, ak sa súbežne vykonáva špecificky navrhnutá ochrana údajov, a naopak.

6. Požiadavka ŠNaŠOÚ sa vzťahuje na všetkých prevádzkovateľov vrátane malých podnikov a nadnárodných spoločností. Vzhľadom na uvedené sa zložitosť vykonávania ŠNaŠOÚ pri jednotlivých spracovateľských operáciách môže líšiť. Vykonávaním ŠNaŠOÚ však možno bez ohľadu na veľkosť podniku vo všetkých prípadoch dosiahnuť pozitívny prínos pre prevádzkovateľa a dotknutú osobu.

2.1 Článok 25 ods. 1: Špecificky navrhnutá ochrana údajov

2.1.1 Povinnosť prevádzkovateľa prijať primerané technické a organizačné opatrenia a začleniť nevyhnutné záruky do spracúvania

7. Podľa článku 25 ods. 1 prevádzkovateľ prijme *primerané* technické a organizačné *opatrenia*, ktoré sú určené na účinné zavedenie zásad ochrany údajov, a začlení do spracúvania *nevyhnutné záruky* s cieľom splniť požiadavky a chrániť práva a slobody dotknutých osôb. Primerané opatrenia, ako aj nevyhnutné záruky slúžia na ochranu práv dotknutých osôb a zabezpečenie toho, aby bola ochrana ich osobných údajov súčasťou spracúvania.

8. Pojem *technické a organizačné opatrenia* a nevyhnutné *záruky* možno v širšom zmysle chápať ako akúkoľvek metódu alebo prostriedky, ktoré môže prevádzkovateľ pri spracúvaní použiť. *Primeranosť* znamená, že opatrenia a nevyhnutné záruky by mali byť prispôsobené dosiahnutiu zamýšľaného účelu, t. j. musia sa nimi *účinne*[3] uplatňovať zásady ochrany údajov. Požiadavka primeranosti je teda úzko spojená s požiadavkou účinnosti.

9. Technickým alebo organizačným opatrením a zárukou môže byť akékoľvek opatrenie od používania pokročilých technických riešení až po základnú odbornú prípravu personálu. K príkladom, ktoré môžu byť vhodné podľa kontextu a rizík súvisiacich s konkrétnym spracúvaním, patrí pseudonymizácia osobných údajov,[4] uchovávanie dostupných osobných údajov v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte, umožnenie dotknutým osobám zasiahnuť do spracúvania, poskytovanie informácií o uchovávaní osobných údajov, používanie systémov na odhaľovanie malvéru, odborná príprava zamestnancov o základnej „kybernetickej hygiene“, zavedenie systémov riadenia bezpečnosti súkromia a osobných údajov, uloženie zmluvnej povinnosti sprostredkovateľom vykonávať osobitné postupy minimalizácie údajov, atď.

[3] Otázka „účinnosti“ sa rieši v podkapitole 2.1.2.
[4] Vymedzená v článku 4 ods. 5 všeobecného nariadenia o ochrane údajov.

10. Pri určovaní primeraných opatrení môžu byť nápomocné normy, najlepšie postupy a kódexy správania, ktoré uznávajú združenia a iné orgány zastupujúce kategórie prevádzkovateľov. Prevádzkovateľ však musí overiť primeranosť opatrení pre konkrétne spracúvanie.

2.1.2 Určené na účinné zavedenie zásad ochrany údajov a ochrany práv a slobôd dotknutých osôb

11. *Zásady ochrany údajov* sú v článku 5 (ďalej len ako „zásady"), *práva a slobody dotknutých osôb* sú základné práva a slobody fyzických osôb, najmä právo na ochranu osobných údajov, ktorých ochrana je uvedená v článku 1 ods. 2 ako cieľ všeobecného nariadenia o ochrane údajov (ďalej len ako „práva")[5]. Ich presné znenie sa nachádza v Charte základných práv Európskej únie. Je mimoriadne dôležité, aby prevádzkovateľ chápal význam *zásad* a *práv* ako základ ochrany, ktorú poskytuje všeobecné nariadenie o ochrane údajov, konkrétne povinnosť ŠNaŠOÚ.

12. Pri vykonávaní primeraných technických a organizačných opatrení by sa mali tieto opatrenia a záruky *navrhnúť* tak, aby bolo účinné vykonávanie každej z uvedených zásad a vyplývajúcej ochrany práv.

Zaručenie účinnosti

13. Účinnosť je základným prvkom pojmu špecificky navrhnutej ochrany údajov. Požiadavka účinného vykonávania zásad znamená, že prevádzkovatelia musia zaviesť potrebné opatrenia a záruky na ochranu týchto zásad s cieľom zabezpečiť práva dotknutých osôb. Každé zavedené opatrenie by malo prispievať k zamýšľaným výsledkom plánovaného spracúvania prevádzkovateľom. Z tohto tvrdenia vyplývajú dva dôsledky.

14. Po prvé to znamená, že článok 25 nevyžaduje vykonávanie žiadnych špecifických technických ani organizačných opatrení, ale že zvolené opatrenia a záruky by mali byť špecifické pre uplatňovanie zásad ochrany údajov pri konkrétnom spracúvaní. Takto navrhnuté opatrenia a záruky by mali byť pevné a prevádzkovateľ by mal vedieť zaviesť ďalšie opatrenia s cieľom prispôsobiť sa akémukoľvek nárastu rizika[6]. To, či sú opatrenia účinné, preto bude závisieť od kontextu konkrétneho spracúvania a posúdenia určitých prvkov, ktoré treba zohľadniť pri určovaní prostriedkov spracúvania. Uvedené prvky sa opisujú ďalej v podkapitole 2.1.3.

15. Po druhé, prevádzkovatelia by mali byť schopní preukázať zachovávanie zásad.

16. Zavedené opatrenia a záruky by mali dosahovať želaný účinok, pokiaľ ide o ochranu osobných údajov, a prevádzkovateľ by mal mať zdokumentované zavedené technické a organizačné opatrenia.[7] Prevádzkovateľ preto môže určiť kľúčové ukazovatele výkonnosti (KPI) vhodné na preukázanie ich účinnosti. KPI je merateľná hodnota zvolená prevádzkovateľom, ktorá preukazuje, ako účinne prevádzkovateľ dosahuje svoj cieľ ochrany údajov. Ukazovatele KPI môžu byť *kvantitatívne*, napríklad percentuálny podiel falošne pozitívnych alebo falošne negatívnych výsledkov, zníženie počtu sťažností, skrátenie času odpovede pri uplatňovaní práv dotknutých osôb; alebo *kvalitatívne*, napríklad

[5] Pozri odôvodnenie 4 všeobecného nariadenia o ochrane údajov.

[6] „Základné zásady, ktoré sa vzťahujú na prevádzkovateľov (t. j. zákonnosť, minimalizácia údajov, obmedzenie účelu, transparentnosť, integrita údajov, správnosť údajov) by mali byť rovnaké bez ohľadu na spracúvanie a riziká pre dotknuté osoby. Náležité zohľadnenie povahy a rozsahu takéhoto spracúvania však bolo vždy neoddeliteľnou súčasťou uplatňovania týchto zásad tak, aby boli inherentne prispôsobiteľné." Pracovná skupina zriadená podľa článku 29, Vyhlásenie k úlohe prístupu založeného na rizikách v právnych rámcoch ochrany údajov, WP 218, 30. máj 2014, s. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

[7] Pozri odôvodnenia 74 a 78.

hodnotenia výkonnosti, používanie hodnotiacich stupníc alebo odborné posúdenia. Namiesto využívania KPI môžu prevádzkovatelia preukázať účinné vykonávanie zásad tým, že poskytnú zdôvodnenie svojho posúdenia účinnosti zvolených opatrení a záruk.

2.1.3 Prvky, ktoré je potrebné zohľadniť

17. Článok 25 ods. 1 uvádza zoznam prvkov, ktoré musí prevádzkovateľ zohľadniť pri určovaní opatrení týkajúcich sa konkrétnej spracovateľskej operácie. V ďalšom texte poskytneme usmernenia k spôsobu využitia týchto prvkov v rámci procesu navrhovania, ktorý zahŕňa návrh štandardných nastavení. Všetky tieto prvky pomáhajú určiť, či je opatrenie primerané na účinné vykonávanie zásad. Všetky tieto prvky teda nie sú cieľom samým osebe, ale predstavujú faktory, ktoré sa majú posudzovať spoločne na dosiahnutie príslušného cieľa.

2.1.3.1 „najnovšie poznatky“

18. Pojem „najnovšie poznatky“ [state of art] sa vyskytuje v rôznych *acquis* EÚ, napr. v oblasti ochrany životného prostredia a bezpečnosti výrobkov. Vo všeobecnom nariadení o ochrane údajov sa odkaz na „najnovšie poznatky“[8] uvádza nielen v článku 32 vo vzťahu k bezpečnostným opatreniam,[9] [10] ale aj v článku 25, čím sa toto referenčné kritérium rozširuje na všetky technické a organizačné opatrenia, ktoré sú súčasťou spracúvania.

19. V súvislosti s článkom 25 sa odkazom na „najnovšie poznatky“ ukladá prevádzkovateľom povinnosť, aby pri určovaní primeraných technických a organizačných opatrení **zohľadnili súčasný technologický pokrok**, ktorý je dostupný na trhu. Od prevádzkovateľov sa požaduje, aby boli informovaní o technologickom pokroku a držali s ním krok. Musia vedieť, aké riziká alebo príležitosti môžu technológie predstavovať v oblasti ochrany údajov pri spracovateľskej operácii a ako prijať a aktualizovať opatrenia a záruky, ktoré *zabezpečujú účinné uplatňovanie* zásad a práv dotknutých osôb vzhľadom na vyvíjajúci sa stav technológie.

20. Pojem „najnovšie poznatky“ je dynamickým pojmom, ktorý nie je možné pevne vymedziť v konkrétnom čase, ale mal by sa posudzovať *priebežne* v kontexte technologického pokroku. Vzhľadom na technologický pokrok prevádzkovateľ môže zistiť, že opatrenie, ktorým sa v minulosti poskytovala primeraná úroveň ochrany, už túto ochranu neposkytuje. Zanedbanie udržiavania kroku s technologickými zmenami by preto mohlo viesť k nesúladu s článkom 25.

21. Kritérium „najnovších poznatkov“ sa nevzťahuje len na technologické, ale aj na organizačné opatrenia. Nedostatok primeraných organizačných opatrení môže znížiť alebo dokonca úplne ohroziť účinnosť vybranej technológie. Príkladom organizačných opatrení môže byť prijatie vnútorných politík, aktuálna odborná príprava v oblasti technológií, bezpečnosti a ochrany údajov, ako aj politiky správy a riadenia bezpečnosti informačných technológií.

---

[8] Pozri rozhodnutie nemeckého Spolkového ústavného súdu vo veci Kalkar z roku 1978: https://germanlawarchive.iuscomp.org/?p=67, ktoré môže byť východiskom pre metodiku objektívneho vymedzenia tohto pojmu. Technologická úroveň „najnovších poznatkov“ by sa tu mala vymedziť ako technologická úroveň medzi „existujúcou úrovňou vedomostí a výskumu“ a zaužívanejšími „všeobecne akceptovanými technickými normami“. „Najnovšie poznatky“ je preto možné vymedziť ako technologickú úroveň služby alebo technológie alebo výrobku, ktorá existuje na trhu a je najúčinnejšia pri dosahovaní stanovených cieľov.

[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/.

22. Existujúce a uznané rámce, normy, certifikácie, kódexy správania atď. v rôznych oblastiach môžu hrať dôležitú úlohu pri identifikácii súčasných „najnovších poznatkov“ v danej oblasti používania. Ak takéto normy existujú a zabezpečujú vysokú úroveň ochrany dotknutej osoby v súlade s právnymi požiadavkami alebo nad ich rámec, prevádzkovatelia by ich mali zohľadniť pri navrhovaní a vykonávaní opatrení na ochranu údajov.

2.1.3.2 „náklady na vykonanie opatrení“

23. Prevádzkovateľ môže zohľadniť náklady na vykonanie pri výbere a uplatňovaní primeraných technických a organizačných opatrení a potrebných záruk, ktorými sa účinne vykonávajú zásady s cieľom chrániť práva dotknutých osôb. Náklady znamenajú zdroje vo všeobecnosti vrátane času a ľudských zdrojov.

24. V rámci prvku nákladov sa nevyžaduje, aby prevádzkovateľ vynaložil neprimerané množstvo zdrojov, ak existujú alternatívne opatrenia, ktoré si nevyžadujú toľko zdrojov, pričom sú stále účinné. Náklady na vykonanie opatrení sú však faktorom, ktorý by sa mal zohľadniť s cieľom zaviesť špecificky navrhnutú ochranu údajov, a nie dôvodom na jej nezavedenie.

25. Zvolenými opatreniami sa teda zabezpečí, aby sa v rámci spracovateľskej činnosti, ktorú prevádzkovateľ plánuje, osobné údaje nespracúvali v rozpore so zásadami, a to bez ohľadu na náklady. Prevádzkovatelia by mali byť schopní riadiť celkové náklady s cieľom účinne vykonávať všetky zásady, a tak chrániť práva.

2.1.3.3 „povaha, rozsah, kontext a účel spracúvania“

26. Prevádzkovatelia musia pri určovaní potrebných opatrení zohľadniť povahu, rozsah, kontext a účel spracúvania.

27. Tieto faktory by sa mali vykladať vzhľadom na ich úlohu v iných ustanoveniach všeobecného nariadenia o ochrane údajov, ako sú články 24, 32 a 35, s cieľom zahrnúť zásady ochrany údajov do spracúvania.

28. V krátkosti možno pojem **povaha** chápať ako charakteristickú[11] vlastnosť spracúvania. **Rozsah** sa vzťahuje na veľkosť a objem spracúvania. **Kontext** sa vzťahuje na okolnosti spracúvania, ktoré môžu ovplyvniť očakávania dotknutej osoby, kým **účel** súvisí s cieľmi spracúvania.

2.1.3.4 „riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie predstavuje pre práva a slobody fyzických osôb“

29. Vo všeobecnom nariadení o ochrane údajov sa v mnohých jeho ustanoveniach, v článkoch 24, 25, 32 a 35, uplatňuje koherentný prístup založený na riziku s cieľom určiť primerané technické a organizačné opatrenia na ochranu jednotlivcov, ich osobných údajov a na splnenie požiadaviek všeobecného nariadenia o ochrane údajov. Chránené aktíva sú vždy rovnaké (jednotlivci, keďže sa chránia ich osobné údaje), chránia sa pred rovnakými rizikami (riziká pre práva jednotlivcov) a zohľadňujú sa rovnaké podmienky (povaha, rozsah, kontext a účel spracúvania).

30. Pri vykonávaní analýzy rizika na účely dodržiavania súladu s článkom 25 musí prevádzkovateľ identifikovať riziká pre práva dotknutých osôb, ktoré predstavujú porušenie zásad, a určiť ich pravdepodobnosť a závažnosť s cieľom vykonať opatrenia na účinné zmiernenie identifikovaných rizík.

[11] Príkladmi sú osobitné kategórie osobných údajov, automatické rozhodovanie, skreslené mocenské vzťahy, nepredvídateľné spracúvanie, ťažkosti dotknutých osôb pri vykonávaní práv atď.

Pri posudzovaní rizika je rozhodujúce systematické a dôkladné hodnotenie spracúvania. Prevádzkovateľ napríklad posudzuje konkrétne riziká spojené s absenciou slobodne udeleného súhlasu, ktorá predstavuje porušenie zásady zákonnosti, v priebehu spracúvania osobných údajov detí a mladých ľudí mladších ako 18 rokov ako zraniteľnej skupiny v prípade, že neexistuje žiadny iný právny základ, a vykonáva primerané opatrenia na riešenie a účinné zmiernenie zistených rizík spojených s touto skupinou dotknutých osôb.

31. Usmernenia EDPB týkajúce sa posúdenia vplyvu na ochranu údajov,[12] ktoré sa zameriavajú na určenie toho, či spracovateľská operácia pravdepodobne povedie k vysokému riziku pre dotknutú osobu alebo nie, poskytujú aj usmernenie k tomu, ako posudzovať riziká v oblasti ochrany údajov a ako vykonávať posúdenie rizika v oblasti ochrany údajov. Tieto usmernenia môžu byť užitočné aj pri posudzovaní rizika na základe všetkých uvedených článkov vrátane článku 25.

32. Pri prístupe založenom na riziku sa nevylučuje využívanie základných scenárov, najlepších postupov a noriem. Tie pre prevádzkovateľov môžu predstavovať užitočný súbor nástrojov na riešenie podobných rizík v podobných situáciách (povaha, rozsah, kontext a účel spracúvania). Napriek tomu sa naďalej uplatňuje povinnosť uvedená v článku 25 [ako aj v článkoch 24, 32 a článku 35 ods. 7 písm. c)] zohľadniť *„riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie predstavuje pre práva a slobody fyzických osôb*“. Preto prevádzkovatelia aj napriek tomu, že využívajú takéto nástroje, musia vždy v jednotlivých prípadoch vykonať posúdenie rizika pre ochranu údajov v súvislosti s konkrétnou spracovateľskou činnosťou a overiť účinnosť navrhovaných primeraných opatrení a záruk. V takomto prípade sa môže vyžadovať aj posúdenie vplyvu na ochranu údajov alebo aktualizácia existujúceho posúdenia.

2.1.4 Časové hľadisko

2.1.4.1 V čase určenia prostriedkov spracúvania

33. Špecificky navrhnutá ochrana údajov sa musí vykonať *„v čase určenia prostriedkov spracúvania“*.

34. Pri „*prostriedkoch spracúvania*“ môže ísť o všeobecné i podrobné prvky návrhu spracúvania vrátane architektúry, postupov, protokolov, usporiadania a vzhľadu.

35. „*Čas určenia prostriedkov spracúvania*“ znamená obdobie, kedy sa prevádzkovateľ rozhoduje o tom, ako sa spracúvanie vykoná a o spôsobe jeho vykonania a mechanizmoch, ktoré sa na vykonanie takéhoto spracúvania použijú. Pri prijímaní takýchto rozhodnutí musí prevádzkovateľ posúdiť primerané opatrenia a záruky pre účinné zavedenie zásad a práv dotknutých osôb do spracúvania a zohľadniť také prvky, ako sú najnovšie poznatky, náklady na vykonávanie, povaha, rozsah, kontext, účel a riziká. Zahŕňa to aj čas obstarania a zavedenia softvéru, hardvéru a služieb na spracúvanie údajov.

36. Včasné zohľadnenie ŠNaŠOÚ je kľúčové, pokiaľ ide o úspešné vykonávanie zásad a ochranu práv dotknutých osôb. Okrem toho z hľadiska nákladov a prínosov by bolo aj v záujme prevádzkovateľov, aby ŠNaŠOÚ zohľadnili radšej skôr ako neskôr, pretože by mohlo byť náročné a nákladné neskôr meniť plány, ktoré už boli vypracované, a spracovateľské operácie, ktoré už boli navrhnuté.

[12] Pracovná skupina zriadená podľa článku 29, Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“, WP 248 rev.01, 4. október 2017. ec.europa.eu/newsroom/document.cfm?doc_id=47711 – schválené EDPB.

2.1.4.2 V čase samotného spracúvania (zachovávanie a preskúmanie požiadaviek spracúvania osobných údajov)

37. Po začatí spracúvania má prevádzkovateľ nepretržitú povinnosť zachovávať ŠNaŠOÚ, t. j. nepretržité účinné vykonávanie zásad s cieľom chrániť práva, mať najnovšie poznatky, prehodnocovať úrovne rizika atď. Druh, rozsah a kontext spracovateľských operácií, ako aj riziko sa môže v priebehu spracúvania zmeniť, čo znamená, že prevádzkovateľ musí prehodnocovať svoje spracovateľské operácie na základe pravidelných preskúmaní a hodnotení účinnosti zvolených opatrení a záruk.

38. Povinnosť zachovávať, preskúmavať a podľa potreby aktualizovať spracovateľskú operáciu sa vzťahuje aj na už existujúce systémy. To znamená, že pôvodné systémy vytvorené pred nadobudnutím účinnosti všeobecného nariadenia o ochrane údajov sa musia podrobiť preskúmaniu a údržbe s cieľom zabezpečiť vykonávanie opatrení a záruk, ktorými sa účinne uplatňujú zásady a práva dotknutých osôb, ako sa uvádza v týchto usmerneniach.

39. Táto povinnosť sa vzťahuje aj na každé spracúvanie vykonávané prostredníctvom sprostredkovateľov. Operácie sprostredkovateľov by mali prevádzkovatelia pravidelne preskúmavať a posudzovať s cieľom zabezpečiť, že umožňujú neustále dodržiavanie zásad a prevádzkovateľovi umožňujú plniť si príslušné povinnosti.

2.2 Článok 25 ods. 2: Štandardná ochrana údajov

2.2.1 Štandardne sa spracúvajú len osobné údaje, ktoré sú nevyhnutné pre každý konkrétny účel spracúvania

40. „Štandard“ podľa bežného vymedzenia v počítačovej vede znamená už existujúcu alebo vopred zvolenú hodnotu konfigurovateľných nastavení, ktorá je priradená softvérovej aplikácii, počítačovému programu alebo zariadeniu. Takéto nastavenia sa nazývajú aj „pôvodné nastavenia“ [presets] alebo „výrobné nastavenia“ [factory presets], najmä v prípade elektronických zariadení.

41. V súvislosti so spracúvaním osobných údajov preto pojem „štandardný“ označuje rozhodovanie sa o konfiguračných hodnotách alebo možnostiach spracúvania, ktoré sú nastavené alebo predpísané v systéme spracúvania, napríklad v softvérovej aplikácii, v službe alebo zariadení, alebo v postupe ručného spracúvania, ktoré ovplyvňujú množstvo získaných osobných údajov, rozsah ich spracúvania, dobu ich uchovávania a ich dostupnosť.

42. Prevádzkovateľ by si mal vybrať štandardné nastavenia a možnosti spracúvania a byť zodpovedný za ich zavedenie tak, aby sa štandardne vykonávalo len spracúvanie, ktoré je nevyhnutne potrebné na dosiahnutie stanoveného zákonného účelu. V takom prípade by mali prevádzkovatelia vychádzať zo svojho posúdenia nevyhnutnosti spracúvania na základe právnych dôvodov podľa článku 6 ods. 1. To znamená, že prevádzkovateľ štandardne nezískava viac údajov, než je potrebné, nespracúva získané údaje viac, ako je potrebné na jeho účely, ani ich neuchováva dlhšie, ako je potrebné. Základnou požiadavkou je, aby bola ochrana údajov začlenená do štandardného spracúvania.

43. Od prevádzkovateľa sa vyžaduje, aby vopred určil, na ktoré konkrétne určené, výslovne uvedené a legitímne účely sa osobné údaje získavajú a spracúvajú.[13] Opatrenia musia byť štandardne primerané na to, aby sa zabezpečilo, že sa spracúvajú iba osobné údaje, ktoré sú nevyhnutné pre každý konkrétny účel spracúvania. Usmernenia EDPS týkajúce sa posúdenia nevyhnutnosti a primeranosti opatrení,

[13] Článok 5 ods. 1 písm. b), c), d), e) všeobecného nariadenia o ochrane údajov.

ktoré obmedzujú právo na ochranu osobných údajov, môžu byť užitočné aj pri rozhodovaní o tom, ktoré údaje je potrebné spracúvať na dosiahnutie konkrétneho účelu.[14] [15] [16]

44. Ak prevádzkovateľ používa softvér tretej strany alebo štandardne dodávaný softvér [off-the shelf software], mal by vykonať posúdenie rizika daného produktu a zabezpečiť, aby sa funkcie, ktoré nemajú právny základ alebo ktoré nie sú zlučiteľné so zamýšľanými účelmi spracúvania, vypli.

45. Tieto isté úvahy sa vzťahujú na organizačné opatrenia, ktorými sa podporujú spracovateľské operácie. Mali by byť navrhnuté tak, aby sa už od začiatku spracúval len minimálny objem osobných údajov nevyhnutných na konkrétne operácie. Osobitne by sa to malo zohľadňovať pri udeľovaní prístupu k údajom zamestnancom s rôznymi úlohami a rôznymi potrebami prístupu.

46. Primerané „technické a organizačné opatrenia“ v kontexte štandardnej ochrany údajov sa teda chápu rovnako, ako sa uvádza v podkapitole 2.1.1, ale uplatňujú sa konkrétne na vykonávanie zásady minimalizácie údajov.

47. Uvedená povinnosť spracúvať len osobné údaje, ktoré sú potrebné pre každý konkrétny účel, sa vzťahuje na tieto prvky.

2.2.2 Aspekty povinnosti minimalizácie údajov

48. Článok 25 ods. 2 vymenováva aspekty povinnosti minimalizácie údajov pri štandardnom spracúvaní, pričom uvádza, že táto povinnosť sa vzťahuje na množstvo získaných osobných údajov, rozsah ich spracúvania, obdobie ich uchovávania a ich dostupnosť.

2.2.2.1 „množstvo získaných osobných údajov“

49. Prevádzkovatelia by mali zohľadniť objem osobných údajov, ako aj typy, kategórie a úroveň podrobnosti osobných údajov požadovaných na účely spracúvania. Ich rozhodnutia pri navrhovaní spracúvania by pri získavaní veľkých objemov podrobných osobných údajov mali zohľadniť vyššie riziko, pokiaľ ide o zásadu integrity a dôvernosti, minimalizáciu údajov a obmedzenie uchovávania, a porovnať ho s nižším rizikom vyplývajúcim zo získavania menších množstiev a/alebo menej podrobných informácií o dotknutých osobách. Štandardné nastavenie v každom prípade nesmie zahŕňať získavanie osobných údajov, ktoré nie sú nevyhnutné pre konkrétny účel spracúvania. Inými slovami, ak niektoré kategórie osobných údajov nie sú potrebné alebo ak nie sú potrebné podrobné údaje, pretože postačuje menej podrobností, potom akékoľvek prebytočné osobné údaje nemajú byť zbierané.

50. Rovnaké štandardné požiadavky sa vzťahujú na služby nezávisle od toho, ktorá platforma alebo zariadenie využívajú, pričom môžu získavať len nevyhnutné osobné údaje na daný účel.

[14] EDPS, Usmernenia týkajúce sa posúdenia nevyhnutnosti a primeranosti opatrení, ktoré obmedzujú právo na ochranu údajov, 25. február 2019, edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.

[15] Pozri tiež EDPS, Posúdenie nevyhnutnosti opatrení, ktoré obmedzujú základné právo na ochranu osobných údajov: Súbor nástrojov https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en.

[16] Viac informácií o nevyhnutnosti sa nachádza v stanovisku pracovnej skupiny zriadenej podľa článku 29 č. 06/2014 k pojmu legitímne záujmy prevádzkovateľa podľa článku 7 smernice 95/46/ES, WP 217, 9. apríl 2014. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_sk.pdf.

2.2.2.2 „rozsah ich spracúvania“

51. Spracovateľské operácie[17] vykonávané v súvislosti s osobnými údajmi sa obmedzujú na to, čo je nevyhnutné. K účelu spracúvania môžu prispievať mnohé spracovateľské operácie. Skutočnosť, že určité osobné údaje sú potrebné na splnenie nejakého účelu však ešte neznamená, že v súvislosti s týmito údajmi môžu byť vykonávané akékoľvek typy spracovateľských operácií s akoukoľvek frekvenciou. Prevádzkovatelia by mali dbať aj na to, aby nedochádzalo k rozširovaniu hraníc „zlučiteľných účelov“ stanovených v článku 6 ods. 4, a zohľadniť, aké spracúvanie budú dotknuté osoby primerane očakávať.

2.2.2.3 „doba ich uchovávania“

52. Získané osobné údaje sa neuchovávajú, ak nie sú potrebné na účel spracúvania a ak neexistuje iný zlučiteľný účel ani právny základ podľa článku 6 ods. 4. Každé uchovávanie by prevádzkovateľ mal objektívne odôvodniť ako nevyhnutné v súlade so zásadou zodpovednosti.

53. Prevádzkovateľ obmedzí obdobie uchovávania na obdobie potrebné na daný účel. Ak osobné údaje nie sú už na účely spracúvania potrebné, štandardne sa vymažú alebo anonymizujú. Dĺžka obdobia uchovávania bude preto závisieť od účelu konkrétneho spracúvania. Táto povinnosť priamo súvisí so zásadou minimalizácie uchovávania uvedenou v článku 5 ods. 1 písm. e) a uplatňuje sa štandardne, t. j. prevádzkovateľ by mal do spracúvania zaviesť systematické postupy na vymazanie údajov alebo ich anonymizáciu.

54. Anonymizácia[18] osobných údajov je alternatívou k vymazaniu za predpokladu, že sa zohľadnia všetky relevantné kontextové prvky a pravidelne sa posudzuje pravdepodobnosť a závažnosť rizika vrátane rizika opätovnej identifikácie.[19]

2.2.2.4 „ich dostupnosť“

55. Prevádzkovateľ by mal na základe posúdenia nevyhnutnosti obmedziť, kto má prístup k osobným údajom a aké druhy prístupu k nim má, a takisto zabezpečiť, aby boli osobné údaje skutočne dostupné tým, ktorí ich v prípade potreby potrebujú, napríklad v kritických situáciách. Kontrola prístupu by sa mala dodržiavať pre celý tok údajov počas spracúvania.

56. Článok 25 ods. 2 ďalej uvádza, že osobné údaje sa bez zásahu fyzickej osoby nesprístupňujú neobmedzenému počtu fyzických osôb. Prevádzkovateľ štandardne obmedzí prístupnosť a poskytne dotknutej osobe možnosť zasiahnuť pred uverejnením alebo iným sprístupnením osobných údajov o dotknutej osobe neobmedzenému počtu fyzických osôb.

---

[17] Podľa článku 4 ods. 2 všeobecného nariadenia o ochrane údajov to zahŕňa získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmenu, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidáciu.

[18] Pracovná skupina zriadená podľa článku 29, Stanovisko č. 05/2014 k technikám anonymizácie, WP 216, 10. apríla 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_sk.pdf.

[19] Pozri článok 4 ods. 1 všeobecného nariadenia o ochrane údajov, odôvodnenie 26 všeobecného nariadenia o ochrane údajov, Stanovisko pracovnej skupiny zriadenej podľa článku 29 č. 5/2014 k technikám anonymizácie. Pozri aj pododdiel „minimalizácia uchovávania“ v časti 3 tohto dokumentu, ktorý odkazuje na skutočnosť, že je potrebné, aby prevádzkovateľ zabezpečil účinnosť vykonávanej/vykonávaných techniky/techník anonymizácie.

57. Sprístupnenie osobných údajov neobmedzenému počtu osôb môže viesť k väčšiemu šíreniu údajov, ako sa pôvodne predpokladalo. To je osobitne dôležité v súvislosti s internetom a vyhľadávačmi. To znamená, že prevádzkovatelia by mali štandardne poskytnúť dotknutým osobám možnosť zasiahnuť pred sprístupnením osobných údajov na otvorenom internete. Toto je mimoriadne dôležité, pokiaľ ide o deti a zraniteľné skupiny.

58. V závislosti od právnych základov na spracúvanie by sa možnosť zasiahnuť mohla líšiť na základe kontextu spracúvania. Mohla by zahŕňať napr. požiadanie o súhlas s verejným sprístupnením osobných údajov alebo poskytnutie nastavení ochrany súkromia tak, aby mali samotné dotknuté osoby kontrolu nad verejným prístupom.

59. Aj v prípade, že osobné údaje sa sprístupňujú verejnosti s povolením a pochopením dotknutej osoby, neznamená to, že každý ďalší prevádzkovateľ s prístupom k osobným údajom ich môže voľne spracúvať na vlastné účely – musí mať svoj vlastný právny základ.[20]

3 VYKONÁVANIE ZÁSAD OCHRANY ÚDAJOV PRI SPRACÚVANÍ OSOBNÝCH ÚDAJOV POMOCOU ŠPECIFICKY NAVRHNUTEJ A ŠTANDARDNEJ OCHRANY ÚDAJOV

60. Prevádzkovateľ by mal vo všetkých fázach navrhovania spracovateľských činností vrátane obstarávania, súťaží, outsourcingu, vývoja, podpory, údržby, testovania, uchovávania, výmazu atď. zohľadňovať rôzne prvky ŠNaŠOÚ, ktorých príklady sa uvádzajú v tejto kapitole v kontexte uplatňovania týchto zásad.[21] [22] [23]

61. Prevádzkovatelia musia zaviesť príslušné zásady, aby dosiahli ŠNaŠOÚ. Tieto zásady zahŕňajú: transparentnosť, zákonnosť, spravodlivosť, obmedzenie účelu, minimalizáciu údajov, presnosť, obmedzenie uchovávania, integritu a dôvernosť a zodpovednosť. Tieto zásady sú uvedené v článku 5 a v odôvodnení 39 všeobecného nariadenia o ochrane údajov. Aby bolo možné úplne pochopiť spôsob vykonávania ŠNaŠOÚ, je nevyhnutné rozumieť významu jednotlivých zásad.

62. Pri jednotlivých príkladoch spôsobov zabezpečenia fungovania ŠNaŠOÚ uvádzame zoznamy **kľúčových prvkov ŠNaŠOÚ** pre každú zo zásad. Niektoré príklady, ktoré zvýrazňujú konkrétnu zásadu ochrany údajov, sa môžu prekrývať s inými úzko súvisiacimi zásadami. EDPB zdôrazňuje, že kľúčové prvky a ďalej uvedené príklady nie sú ani vyčerpávajúce, ani záväzné, ale predstavujú hlavné prvky jednotlivých zásad. Prevádzkovatelia musia posúdiť, ako zaručiť dodržiavanie zásad v súvislosti s konkrétnou spracovateľskou operáciou.

63. Zatiaľ čo sa táto časť zameriava na zavádzanie zásad, prevádzkovateľ by mal takisto zaviesť *primerané* a *účinné* spôsoby ochrany práv dotknutých osôb, a to aj podľa kapitoly III všeobecného nariadenia o ochrane údajov, ak to nie je povinné už na základe samotných zásad.

[20] Pozri vec Satakunnan Markkinapörssi Oy a Satamedia Oy/Fínsko č. 931/13.
[21] Viac príkladov možno nájsť v dokumente nórskeho orgánu pre ochranu údajov. *Software Development with Data Protection by Design and by Default* (Vývoj softvéru so špecificky navrhnutou a štandardnou ochranou osobných údajov),28. novembra 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.

64. Zásada zodpovednosti je ústredná: vyžaduje sa ňou, aby prevádzkovateľ bol zodpovedný za výber potrebných technických a organizačných opatrení.

3.1 Transparentnosť[24]

65. Prevádzkovateľ musí s dotknutou osobou jasne a otvorene komunikovať o tom, ako bude získavať, využívať a poskytovať osobné údaje. Cieľom transparentnosti je umožniť dotknutým osobám pochopiť a v prípade potreby uplatniť ich práva podľa článkov 15 až 22. Táto zásada je zakotvená v článkoch 12, 13, 14 a 34. Opatrenia a záruky zavedené na podporu zásady transparentnosti by mali podporovať aj vykonávanie týchto článkov.

66. Pokiaľ ide o zásadu transparentnosti, ku kľúčovým prvkom špecificky navrhnutej a štandardnej ochrany údajov môže patriť:

- jasnosť – informácie sú formulované jasne a jednoducho, sú stručné a zrozumiteľné;
- sémantika – komunikácia by mala mať pre príslušné publikum jednoznačný význam;
- prístupnosť – informácie sú pre dotknutú osobu ľahko prístupné;
- kontext – informácie by sa mali poskytovať v relevantnom čase a v primeranej forme;
- relevantnosť – informácie by mali byť relevantné a vzťahovať sa na konkrétnu dotknutú osobu;
- dizajn pre všetkých – informácie musia byť prístupné pre všetky dotknuté osoby, zahŕňať používanie strojovo čitateľných jazykov na uľahčenie a automatizáciu čitateľnosti a jasnosti;
- zrozumiteľnosť – dotknuté osoby by mali dostatočne dobre chápať, čo môžu očakávať v súvislosti so spracúvaním svojich osobných údajov, najmä ak pri dotknutých osobách ide o deti alebo iné zraniteľné skupiny;
- viackanálovosť – informácie by sa mali okrem textovej formy poskytovať prostredníctvom rôznych kanálov a médií, aby sa zvýšila pravdepodobnosť, že informácie účinne oslovia dotknuté osoby;
- vrstvenosť – informácie by mali byť vrstvené tak, aby sa odstránilo napätie medzi úplnosťou a porozumením, pričom by sa mali zohľadniť primerané očakávania dotknutých osôb.

Príklad[25]

Prevádzkovateľ na svojom webovom sídle uvádza politiku ochrany súkromia s cieľom splniť požiadavky transparentnosti. Politika ochrany súkromia by nemala obsahovať rozsiahle množstvo informácií, ktoré je pre priemernú dotknutú osobu ťažké porozumieť a pochopiť. Musí byť napísaná jasne a stručne, aby používateľ webového sídla ľahko pochopil, ako sa jeho osobné údaje spracúvajú. Prevádzkovateľ preto poskytuje informácie vo vrstvách a zdôrazňuje najdôležitejšie body. Podrobnejšie informácie sú ľahko dostupné. Na vysvetlenie rôznych prvkov a koncepcií obsiahnutých v tejto politike sú k dispozícii rozbaľovacie ponuky a odkazy na iné stránky. Prevádzkovateľ sa okrem toho uistí, že informácie sa poskytujú prostredníctvom viacerých kanálov, pričom poskytuje videá s cieľom vysvetliť najdôležitejšie aspekty poskytnutých písomných informácií. Synergia medzi jednotlivými stránkami je nevyhnutná na to, aby sa zabezpečilo, že vrstvený prístup nezvýši nejasnosti, ale ich naopak minimalizuje.

Prístup k politike ochrany osobných údajov by nemal byť pre dotknuté osoby ťažký. Politika ochrany osobných údajov sa preto sprístupňuje a zviditeľňuje na všetkých webových stránkach daného

[24] Vysvetlenie toho, ako je potrebné chápať pojem transparentnosti, sa nachádza v „usmerneniach pracovnej skupiny zriadenej podľa článku 29 k transparentnosti podľa nariadenia 2016/679“, WP 260 rev.01,11. apríla 2018. ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 – schválené EDPB.
[25] Francúzsky orgán pre ochranu údajov uverejnil niekoľko príkladov vykresľujúcich najlepšie postupy pre informovanie používateľov, ako aj ďalšie zásady transparentnosti: https://design.cnil.fr/en/.

webového sídla, takže dotknutej osobe vždy stačí len jedno kliknutie na to, aby mala prístup k týmto informáciám. Poskytnuté informácie sú navrhnuté v súlade s najlepšími postupmi a normami univerzálneho dizajnu pre všetkých tak, aby boli prístupné pre všetkých.

Okrem toho by sa potrebné informácie mali poskytovať v správnom kontexte a v správnom čase. Keďže prevádzkovateľ vykonáva množstvo spracovateľských operácií s použitím údajov získaných na webovom sídle, samotná všeobecná politika ochrany súkromia na webovom sídle nepostačuje na to, aby prevádzkovateľ splnil požiadavky transparentnosti. Prevádzkovateľ preto navrhne taký tok informácií, v rámci ktorého sa dotknutej osobe prezentujú príslušné informácie vo vhodnom kontexte, napr. pomocou informačných úryvkov alebo kontextových okien. Napríklad ak prevádzkovateľ žiada dotknutú osobu o zadanie osobných údajov, informuje ju o spôsobe spracúvania osobných údajov a prečo sú tieto osobné údaje potrebné na spracúvanie.

3.2 Zákonnosť

67. Prevádzkovateľ určí platný právny základ pre spracúvanie osobných údajov. Opatrenia a záruky by mali podporovať túto požiadavku, aby sa zabezpečilo, že celý životný cyklus spracúvania je v súlade s príslušnými právnymi dôvodmi spracúvania.

68. Pokiaľ ide o zákonnosť, ku kľúčovým prvkom špecificky navrhnutej a štandardnej ochrany údajov môže patriť:
    - relevantnosť – pri spracúvaní sa uplatní správny právny základ;
    - rozlišovanie[26] – rozlíši sa právny základ používaný pre každú spracovateľskú činnosť ;
    - konkrétny účel – vhodný právny základ musí jednoznačne súvisieť s konkrétnym účelom spracúvania;[27]
    - nevyhnutnosť – spracúvanie musí byť nevyhnutné a bezpodmienečné pre daný účel, aby bolo zákonné;
    - autonómia – dotknutá osoba by mala mať pri kontrole nad osobnými údajmi čo najvyššiu mieru autonómnosti v rámci príslušného právneho základu;
    - získanie súhlasu – súhlas musí byť udelený dobrovoľne, musí byť konkrétny, informovaný a jednoznačný.[28] Osobitná pozornosť by sa mala venovať schopnosti detí a mladých ľudí poskytnúť informovaný súhlas;
    - odvolanie súhlasu – ak je právnym základom súhlas, v rámci spracúvania by malo byť umožnené súhlas odvolať. Odvolanie súhlasu musí byť rovnako jednoduché ako jeho udelenie. Ak nie je, potom mechanizmus udeľovania súhlasu prevádzkovateľa nie je v súlade so všeobecným nariadením o ochrane údajov;[29]
    - vyváženie záujmov – ak je právnym základom oprávnený záujem, prevádzkovateľ musí vykonať vážené vyváženie záujmov, pričom osobitne zohľadní nerovnováhu síl, konkrétne v prípade detí mladších ako 18 rokov a iných zraniteľných skupín. Musia existovať opatrenia a záruky na zmiernenie nepriaznivého vplyvu na dotknuté osoby;

[26] EDPB, Usmernenia 2/2019 o spracúvaní osobných údajov podľa článku 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov v súvislosti s poskytovaním on-line služieb dotknutým osobám, verzia 2.0, 8. október 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_sk.pdf.
[27] Pozri časť o obmedzení účelu nižšie.
[28] Pozri Usmernenia 05/2020 o súhlase podľa nariadenia 2016/679. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_sk.pdf.
[29] Pozri Usmernenia 05/2020 o súhlase podľa nariadenia 2016/679, s. 24. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_sk.pdf.

- určenie vopred – právny základ sa stanoví pred vykonaním spracúvania;
- ukončenie – ak sa právny základ už neuplatňuje, spracúvanie sa zodpovedajúcim spôsobom ukončí;
- úprava – ak dôjde k platnej zmene právneho základu na spracúvanie, skutočné spracúvanie sa musí upraviť v súlade s novým právnym základom;[30]
- pridelenie zodpovednosti – pri plánovaní využívania spoločného prevádzkovateľstva musia strany jednoznačne a transparentne rozdeliť svoje príslušné zodpovednosti voči dotknutej osobe a navrhnúť opatrenia v rámci spracúvania v súlade s týmto pridelením.

Príklad

Banka plánuje ponúkať službu na zlepšenie efektívnosti pri správe žiadostí o úver. Základnou myšlienkou tejto služby je, že banka na základe vyžiadania súhlasu od klienta môže získať informácie o klientovi priamo od verejných daňových orgánov. V tomto príklade sa nezohľadňuje spracúvanie osobných údajov z iných zdrojov.

Získanie osobných údajov o finančnej situácii dotknutej osoby je potrebné na to, aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením úverovej zmluvy.[31] Získanie osobných údajov priamo od daňovej správy sa však nepovažuje za potrebné, pretože zákazník môže uzatvoriť zmluvu na základe toho, že sám poskytne informácie od daňovej správy. Hoci banka môže mať oprávnený záujem získať dokumentáciu priamo od daňových orgánov, napríklad s cieľom zabezpečiť efektívnosť spracovania úveru, poskytnutie takéhoto priameho prístupu bankám k osobným údajom žiadateľov predstavuje riziko spojené s využívaním alebo možným zneužitím prístupových oprávnení.

Pri vykonávaní zásady zákonnosti prevádzkovateľ zistí, že v tomto kontexte nemôže použiť právny základ „nevyhnutnosti na plnenie zmluvy“ v tejto časti spracúvania, ktoré zahŕňa získavanie osobných údajov priamo od daňových orgánov. Relevantným faktorom pri posudzovaní zákonnosti samotného spracúvania je aj skutočnosť, že toto konkrétne spracúvanie predstavuje riziko, že dotknutá osoba bude menej zapojená do spracúvania vlastných údajov. Banka dospeje k záveru, že táto časť spracúvania sa musí opierať o iný právny základ spracúvania. V konkrétnom členskom štáte, v ktorom sa prevádzkovateľ nachádza, existujú vnútroštátne právne predpisy, ktoré umožňujú banke získavať informácie priamo od verejných daňových orgánov, ak s tým dotknutá osoba vopred súhlasí.

Banka preto predloží informácie o spracúvaní na online platforme pre podávanie žiadostí takým spôsobom, ktorý dotknutým osobám umožní ľahšie pochopiť, ktoré spracúvanie je povinné a ktoré je nepovinné. Možnosti spracúvania štandardne neumožňujú vyhľadávanie údajov priamo z iných zdrojov než od samotnej dotknutej osoby a možnosť priameho vyhľadávania informácií sa prezentuje spôsobom, ktorý neodradí dotknutú osobu od odmietnutia. Akýkoľvek súhlas so získavaním údajov priamo od iných prevádzkovateľov je dočasným právom na prístup ku konkrétnemu súboru informácií.

Každý udelený súhlas sa spracúva elektronicky spôsobom, ktorý umožňuje zdokumentovanie, a dotknutým osobám sa poskytuje jednoduchá možnosť kontroly toho, s čím súhlasili a možnosť odvolania súhlasu.

Prevádzkovateľ vopred posúdil tieto požiadavky na ŠNaŠOÚ a zahrnul všetky tieto kritériá do svojich špecifikácií požiadaviek na verejné obstarávanie na účely zaistenia uvedenej platformy. Prevádzkovateľ si je vedomý toho, že ak verejné obstarávanie nebude obsahovať požiadavky na ŠNaŠOÚ, neskôr už

[30] Ak je pôvodným právnym základom súhlas, pozri Usmernenia 05/2020 o súhlase podľa nariadenia 2016/679. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_sk.pdf.
[31] Pozri článok 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov.

môže byť buď priveľmi neskoro, alebo môže ísť o veľmi nákladný postup následného uplatňovania ochrany údajov.

3.3 Spravodlivosť

69. Spravodlivosť je všeobecná zásada, ktorá vyžaduje, aby sa osobné údaje nespracúvali spôsobom, ktorý je pre dotknutú osobu neodôvodnene škodlivý, nezákonne diskriminačný, neočakávaný alebo zavádzajúci. Opatrenia a záruky, ktorými sa vykonáva zásada spravodlivosti, podporujú aj práva a slobody dotknutých osôb, konkrétne právo na informácie (transparentnosť), právo na zásah (prístup, vymazanie, prenosnosť údajov, oprava) a právo na obmedzenie spracúvania (právo nepodliehať automatizovanému individuálnemu rozhodovaniu a nediskriminácia dotknutých osôb v takýchto procesoch).

70. Ku kľúčovým prvkom špecificky navrhnutej a štandardnej ochrany údajov, pokiaľ ide o spravodlivosť, môže patriť:
    - autonómia – dotknuté osoby by mali mať čo najvyššiu mieru autonómie pri určovaní použitia ich osobných údajov, ako aj rozsahu a podmienok tohto použitia alebo spracúvania;
    - interakcia – dotknuté osoby musia byť schopné komunikovať a uplatňovať svoje práva v súvislosti s osobnými údajmi spracúvanými prevádzkovateľom;
    - očakávanie – spracúvanie by malo zodpovedať primeraným očakávaniam dotknutých osôb;
    - nediskriminácia – prevádzkovateľ by nemal nespravodlivo diskriminovať dotknuté osoby;
    - nezneužívanie – prevádzkovateľ by nemal zneužívať potreby alebo zraniteľnosť dotknutých osôb;
    - voľba na spotrebiteľovi – prevádzkovateľ by nemal nespravodlivým spôsobom „zviazať používateľov“. Ak je služba spracúvania osobných údajov proprietárna, môže to viesť k viazanosti k tejto službe, čo nemusí byť spravodlivé, ak to negatívne ovplyvňuje možnosť dotknutých osôb uplatňovať si právo na prenosnosť údajov v súlade s článkom 20;
    - rovnováha síl – rovnováha síl by mala byť kľúčovým cieľom vzťahu medzi prevádzkovateľom a dotknutou osobou. Treba sa vyhýbať nerovnováhe síl. Ak to nie je možné, treba ju uznať a vyriešiť prostredníctvom vhodných protiopatrení;
    - neprenášanie rizika – prevádzkovatelia by nemali prenášať podnikateľské riziká na dotknuté osoby;
    - nezavádzanie – informácie o spracúvaní údajov a možnosti spracúvania údajov by sa mali poskytovať objektívnym a neutrálnym spôsobom, pričom sa treba vyhýbať zavádzajúcemu alebo manipulatívnemu vyjadrovaniu či dizajnu;
    - dodržiavanie práv – prevádzkovateľ musí rešpektovať základné práva dotknutých osôb a vykonávať primerané opatrenia a záruky a neporušovať tieto práva, pokiaľ to nie je výslovne právne odôvodnené;
    - etika – prevádzkovateľ by mal sledovať širší vplyv spracúvania na práva a dôstojnosť jednotlivcov;
    - pravdivosť – prevádzkovateľ musí sprístupniť informácie o tom, ako spracúva osobné údaje, mal by konať v súlade s vlastnými vyjadreniami a nezavádzať dotknuté osoby;

- zásah človeka – prevádzkovateľ musí zahrnúť *kvalifikovaný* zásah človeka, schopný odhaliť chyby, ktoré vznikajú pri strojovom spracúvaní, v súlade s právom, aby sa na dotknutú osobu nevzťahovalo automatizované individuálne rozhodovanie podľa článku 22;[32]
- spravodlivé algoritmy – pravidelne posudzovať, či algoritmy fungujú v súlade so svojimi účelmi a prispôsobovať ich s cieľom zmierniť odhalené chyby a zaistiť spravodlivosť v rámci spracúvania. Dotknuté osoby by mali byť informované o fungovaní spracúvania osobných údajov na základe algoritmov, ktoré ich analyzujú alebo vytvárajú súvisiace predpovede, napríklad pokiaľ ide o výkonnosť v práci, majetkové pomery, zdravie, osobné preferencie, spoľahlivosť alebo správanie, polohu alebo pohyby.[33]

Príklad 1

Prevádzkovateľ poskytuje vyhľadávač, ktorý spracúva väčšinou osobné údaje vytvorené používateľmi. Prevádzkovateľ má úžitok z toho, že vlastní veľké množstvo osobných údajov a môže tieto osobné údaje použiť na cielenú reklamu. Prevádzkovateľ chce preto ovplyvniť dotknuté osoby, aby mu povolili rozsiahlejšie získavanie a používanie ich osobných údajov. Súhlas je potrebné získať tak, že sa dotknutej osobe predložia možností spracúvania.

Pri uplatnení zásady spravodlivosti a zohľadnení povahy, rozsahu, kontextu a účelu spracúvania si prevádzkovateľ uvedomí, že nemôže možnosti prezentovať tak, aby dotknutú osobu navádzal k tomu, aby prevádzkovateľovi povolila získavanie väčšieho množstva osobných údajov, než keby boli možnosti prezentované rovnako a neutrálne. Znamená to, že nemôže prezentovať možnosti spracúvania spôsobom, ktorý dotknutým osobám sťažuje odmietnutie zdieľania ich údajov alebo im sťažuje úpravu nastavení ochrany súkromia a takto obmedziť spracúvanie. Toto sú príklady tzv. tmavých vzorov [dark patterns], ktoré sú v rozpore s duchom článku 25. Štandardné možnosti spracúvania by nemali porušovať súkromie a voľba ďalšieho spracúvania by mala byť prezentovaná spôsobom, ktorý nenúti dotknutú osobu udeliť súhlas. Prevádzkovateľ preto prezentuje možnosti udeliť alebo neudeliť súhlas ako dve rovnako viditeľné voľby, pričom presne uvádza dôsledky každej možnosti pre dotknutú osobu.

Príklad 2

Iný prevádzkovateľ spracúva osobné údaje na účely poskytovania strímingových služieb, pri ktorých si používatelia môžu vybrať medzi bežným predplatným štandardnej kvality a bonusovým predplatným vyššej kvality. Pri bonusovom predplatnom sa predplatiteľom prednostne poskytujú zákaznícke služby.

Z hľadiska zásady spravodlivosti prednostné poskytovanie zákazníckych služieb pre predplatiteľov bonusových služieb nemôže byť diskriminačné, pokiaľ ide o prístup bežných predplatiteľov k uplatňovaniu ich práv podľa článku 12 všeobecného nariadenia o ochrane údajov. Znamená to, že aj keď bonusoví predplatitelia získavajú prednostné služby, takéto uprednostnenie nemôže viesť k nedostatku primeraných opatrení umožňujúcich odpovedať na žiadosti bežných predplatiteľov bez zbytočného odkladu a v každom prípade do jedného mesiaca od prijatia žiadostí.

Uprednostňovaní zákazníci si môžu zaplatiť lepšie služby, ale všetky dotknuté osoby majú mať rovnaký a neobmedzený prístup k presadzovaniu svojich práv a slobôd, ako vyžaduje článok 12.

[32] Pozri Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679. https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826.
[33] Pozri odôvodnenie 71 všeobecného nariadenia o ochrane údajov.

3.4 Obmedzenie účelu[34]

71. Prevádzkovateľ musí získavať údaje na konkrétne určené, výslovne uvedené a legitímne účely a nesmie ich ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s účelmi, na ktoré boli získané.[35] Návrh spracúvania by sa preto mal utvárať tým, čo je nevyhnutné na dosiahnutie týchto účelov. Ak sa má uskutočniť akékoľvek ďalšie spracúvanie, prevádzkovateľ musí najprv zabezpečiť, aby bolo toto spracúvanie zlučiteľné s pôvodnými účelmi a v súlade s tým ho navrhnúť. To, či je nový účel zlučiteľný alebo nie, sa posúdi podľa kritérií uvedených v článku 6 ods. 4.

72. Pokiaľ ide o obmedzenie účelu, ku kľúčovým prvkom špecificky navrhnutej a štandardnej ochrany údajov môže patriť:
    - určenie vopred – legitímne účely sa musia určiť pred navrhnutím spracúvania;
    - konkrétnosť – účely sú konkrétne a zrejmé, pokiaľ ide o dôvody prečo sú údaje spracúvané;
    - orientácia na účel – návrh spracúvania a stanovovanie hraníc spracúvania by sa mali riadiť účelom spracúvania;
    - nevyhnutnosť – na základe účelu sa určuje, ktoré osobné údaje sú nevyhnutné na dané spracúvanie;
    - zlučiteľnosť – každý nový účel musí byť zlučiteľný s pôvodným účelom, na ktorý boli údaje získané, a príslušné zmeny návrhu sa ním musia riadiť;
    - obmedzenie ďalšieho spracúvania – prevádzkovateľ by nemal spájať súbory údajov alebo vykonávať ďalšie spracúvanie pre nové, nezlučiteľné účely;
    - obmedzenia opätovného použitia – prevádzkovateľ by mal používať technické opatrenia vrátane hašovania [hashing] a šifrovania s cieľom obmedziť možnosť použitia osobných údajov na iný účel. Prevádzkovateľ by mal takisto mať aj organizačné opatrenia, ako sú politiky a zmluvné záväzky, ktoré obmedzujú opakované použitie osobných údajov;
    - preskúmanie – prevádzkovateľ by mal pravidelne preskúmať, či je spracúvanie nevyhnutné na účely, na ktoré boli údaje získané, a vykonať test, či návrh stále zodpovedá zásade obmedzenia účelu.

Príklad

Prevádzkovateľ spracúva osobné údaje o svojich zákazníkoch. Účelom spracúvania je splniť zmluvu, t. j. byť schopný dodať tovar na správnu adresu a prijať platbu. Uložené osobné údaje zahŕňajú históriu nákupov, meno, adresu, e-mailovú adresu a telefónne číslo.

Prevádzkovateľ uvažuje o kúpe produktu na riadenie vzťahov so zákazníkmi, ktorý zhromažďuje všetky údaje o zákazníkoch týkajúce sa predaja, marketingu a služieb zákazníkom na jednom mieste. Tento produkt ponúka možnosť ukladať všetky telefonické hovory, aktivity, dokumenty, e-maily a marketingové kampane, s cieľom získať komplexný obraz o zákazníkovi. Okrem toho sa v rámci riadenia vzťahov so zákazníkmi môže automaticky analyzovať kúpna sila zákazníkov na základe verejných informácií. Cieľom analýzy je zlepšiť zacielenie reklamných činností. Tieto činnosti nie sú súčasťou pôvodného zákonného účelu spracúvania.

[34] Pracovná skupina zriadená podľa článku 29 poskytla usmernenia týkajúce sa pochopenia zásady obmedzenia účelu podľa smernice 95/46/ES. Hoci EDPB toto stanovisko neprijal, môže byť relevantné, keďže znenie tejto zásady je podľa všeobecného nariadenia o ochrane údajov rovnaké. Pracovná skupina zriadená podľa článku 29, Stanovisko č. 03/2013 k obmedzeniu účelu, WP 203,2. apríla 2013. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[35] Článok 5 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov.

Aby prevádzkovateľ konal v súlade so zásadou obmedzenia účelu, od poskytovateľa produktu vyžaduje, aby zmapoval jednotlivé spracovateľské činnosti, ktoré využívajú osobné údaje na účely, ktoré sú relevantné pre daného prevádzkovateľa.

Na základe poskytnutých výsledkov mapovania prevádzkovateľ posúdi, či nový marketingový účel a účel cielenej reklamy sú zlučiteľné s pôvodnými účelmi vymedzenými v čase získania údajov a či existuje dostatočný právny základ pre príslušné spracúvanie. Ak na základe tohto posúdenia prevádzkovateľ nedospeje ku kladnej odpovedi, nesmie používať príslušné funkcie. Prevádzkovateľ by sa prípadne mohol rozhodnúť, že posudzovanie nevykoná a jednoducho nevyužije opísané funkcie produktu.

3.5 Minimalizácia údajov

73. Spracúvajú sa len osobné údaje, ktoré sú primerané, relevantné a obmedzené na to, čo je **nevyhnutné** na daný účel.[36] Preto musí prevádzkovateľ vopred určiť, ktoré prvky a parametre systémov spracúvania a ich podporných funkcií sú prípustné. Minimalizácia údajov potvrdzuje zásadu nevyhnutnosti a zavádza ju do praxe. Pri ďalšom spracúvaní by mal prevádzkovateľ pravidelne zvažovať, či sú spracúvané osobné údaje stále primerané, relevantné a nevyhnutné, alebo či by sa údaje mali vymazať alebo anonymizovať.

74. Prevádzkovatelia by mali v prvom rade určiť, či vôbec musia spracúvať osobné údaje na svoje príslušné účely. Prevádzkovateľ by si mal overiť, či sa dajú príslušné účely dosiahnuť spracúvaním menšieho počtu osobných údajov alebo získavaním menej podrobných či súhrnných osobných údajov alebo úplne bez nutnosti spracúvať osobné údaje.[37] Takéto overenie by sa malo uskutočniť pred každým spracúvaním údajov, ale možno ho vykonať aj kedykoľvek počas životného cyklu spracúvania. Je to v súlade aj s článkom 11.

75. Minimalizácia sa môže vzťahovať aj na mieru identifikácie. Ak si účel spracúvania nevyžaduje, aby sa v konečnom súbore údajov odkazovalo na identifikovaného alebo identifikovateľného jednotlivca (napríklad v štatistike), ale pôvodné spracúvanie údajov takéto odkazy obsahuje (napr. pred agregáciou údajov), potom prevádzkovateľ vymaže alebo anonymizuje osobné údaje hneď, ako už identifikácia nie je potrebná. V opačnom prípade, pokiaľ je identifikácia potrebná pre ďalšie spracovateľské činnosti, osobné údaje by mali byť pseudonymizované, aby sa zmiernili riziká pre práva dotknutých osôb.

76. Pokiaľ ide o minimalizáciu údajov, ku kľúčovým prvkom špecificky navrhnutej a štandardnej ochrany údajov môže patriť:
    - vyhýbanie sa spracúvaniu údajov – úplne sa vyhýbať spracúvaniu osobných údajov, ak je to na príslušný účel možné;
    - obmedzenie – obmedzenie množstva získavaných osobných údajov na množstvo nevyhnutné na tento účel;
    - obmedzenie prístupu – upraviť spracúvanie údajov tak, aby na vykonávanie svojich úloh potreboval prístup k osobným údajom minimálny počet osôb, a zodpovedajúcim spôsobom obmedziť prístup;
    - relevantnosť – osobné údaje by mali byť relevantné pre konkrétne spracúvanie a prevádzkovateľ by mal byť schopný túto relevantnosť preukázať;

[36] Článok 5 ods. 1 písm. c) všeobecného nariadenia o ochrane údajov.
[37] Odôvodnenie 39 všeobecného nariadenia o ochrane údajov uvádza: „…Osobné údaje by sa mali spracúvať len vtedy, ak účel spracúvania nebolo možné za primeraných podmienok dosiahnuť inými prostriedkami.“

- nevyhnutnosť – každá kategória osobných údajov je nevyhnutná na dané účely a mala by sa spracúvať len vtedy, ak nie je účel možné splniť inými prostriedkami;
- agregácia – ak je to možné, treba používať súhrnné údaje [aggregated data];
- pseudonymizácia – pseudonymizovať osobné údaje hneď, ako už nie sú potrebné priamo identifikovateľné osobné údaje a oddelene uchovávať identifikačné kľúče;
- anonymizácia a vymazanie – ak osobné údaje na daný účel nie sú alebo už nie sú nevyhnutné, osobné údaje sa anonymizujú alebo vymažú;
- tok údajov – tok údajov by mal byť dostatočne efektívny na to, aby sa nevytváralo viac kópií, než je nevyhnutné;
- „najnovšie poznatky“ – prevádzkovateľ by mal využívať najnovšie a primerané technológie, aby sa vyhol spracúvaniu údajov a údaje minimalizoval.

Príklad 1

Kníhkupectvo chce zvýšiť svoje príjmy predajom kníh online. Majiteľ kníhkupectva chce vytvoriť štandardizovaný formulár pre proces objednávania. Majiteľ kníhkupectva stanoví všetky polia štandardného kontaktného formulára ako povinné (ak nebudú všetky polia vyplnené, zákazník nemôže odoslať objednávku), aby zabezpečil, že zákazníci vyplnia všetky požadované informácie. Majiteľ internetového obchodu najprv používa štandardný kontaktný formulár, v ktorom je potrebné zadať informácie, ako je dátum narodenia, telefónne číslo a bydlisko zákazníka. Nie všetky polia formulára sú však potrebné na účel nákupu a dodania kníh. Ak v tomto konkrétnom prípade dotknutá osoba zaplatí za výrobok dopredu, nie sú dátum narodenia ani telefónne číslo dotknutej osoby na nákup výrobku potrebné. To znamená, že na objednanie výrobku tieto polia nemožno vo webovom formulári vyžadovať, pokiaľ prevádzkovateľ jasne nepreukáže, že je to skutočne potrebné, ako aj prečo sú tieto polia potrebné. Okrem toho existujú situácie, v ktorých adresa nebude potrebná. Napríklad v prípade objednávky elektronickej knihy si ju zákazník môže stiahnuť priamo do svojho zariadenia.

Majiteľ internetového obchodu sa preto rozhodne vytvoriť dva internetové formuláre: jeden na objednávanie kníh s poľom pre adresu zákazníka a jeden na objednávanie elektronických kníh bez poľa pre adresu zákazníka.

Príklad 2

Spoločnosť poskytujúca verejnú dopravu chce zhromažďovať štatistické informácie na základe trás cestujúcich. Chce ich využiť na správne rozhodovanie o zmenách v cestovných poriadkoch verejnej dopravy a na správne trasy vlakov. Cestujúci musia prejsť lístkom cez čítačku pri každom nástupe do dopravného prostriedku a výstupe z dopravného prostriedku. Prevádzkovateľ na základe posúdenia rizika pre práva a slobody cestujúcich pri získavaní údajov o ich cestovných trasách dospeje k názoru, že cestujúcich možno identifikovať, pokiaľ žijú alebo pracujú v riedko osídlených oblastiach, a to na základe identifikácie jednej trasy prostredníctvom identifikátora cestovného lístka. Keďže identifikátor lístka nie je nevyhnutný na účely optimalizácie cestovných poriadkov verejnej dopravy a trás vlakov, prevádzkovateľ identifikátor lístka neuchováva. Po skončení cesty prevádzkovateľ uloží len jednotlivé cestovné trasy tak, aby nebol schopný identifikovať cesty spojené s jedným cestovným lístkom, ale uchová len informácie o samostatných cestovných trasách.

Ak stále existuje riziko, že sa určitá osoba identifikuje výlučne na základe jej cestovnej trasy verejnou dopravou, prevádzkovateľ zavedie štatistické opatrenia na zmiernenie tohto rizika, ako je napríklad odstránenie začiatku a konca trasy.

Príklad 3

Kuriérska služba má záujem o posúdenie účinnosti jej dodávok, pokiaľ ide o čas dodania, rozvrhnutie pracovného zaťaženia a spotrebu paliva. Na dosiahnutie tohto cieľa musí kuriérska služba spracúvať viaceré osobné údaje týkajúce sa zamestnancov (vodičov) a zákazníkov (adresy, položky, ktoré sa majú dodať atď.). Táto spracovateľská operácia zahŕňa riziko sledovania zamestnancov, čo si vyžaduje osobitné právne záruky, ako aj riziko sledovania zvykov klientov prostredníctvom informácií o dodaných položkách v dlhšom období. Tieto riziká sa môžu výrazne znížiť prostredníctvom primeranej pseudonymizácie zamestnancov a zákazníkov. V prípade, že sa často menia pseudonymizované kľúče a namiesto podrobných adries sa používajú väčšie oblasti, dochádza k účinnej minimalizácii údajov a prevádzkovateľ sa môže zamerať výlučne na proces dodávania a na účel optimalizácie zdrojov bez toho, aby dochádzalo k sledovaniu správania (zákazníkov alebo zamestnancov).

Príklad 4

Nemocnica získava údaje o svojich pacientoch v nemocničnom informačnom systéme (elektronické zdravotné záznamy). Nemocničný personál musí mať prístup k dokumentácii pacientov, na základe ktorej prijíma rozhodnutia týkajúce sa starostlivosti o pacientov a ich liečby a na zdokumentovanie všetkých činností vykonaných v oblasti diagnostiky, starostlivosti a liečby. Štandardne sa prístup poskytuje len tým zdravotníckym pracovníkom, ktorí sa zaoberajú liečbou príslušného pacienta v rámci špecializovaného oddelenia, na ktoré je pridelený. Skupina ľudí, ktorí majú prístup k pacientovej dokumentácii, sa zväčší, ak sa do liečby zapoja ďalšie oddelenia alebo diagnostické jednotky. Po prepustení pacienta a po dokončení vyúčtovania sa prístup obmedzí na malú skupinu zamestnancov z každého špecializovaného oddelenia, ktorí vybavujú žiadosti o lekárske informácie alebo konzultácie predložené alebo požadované inými poskytovateľmi zdravotníckych služieb, a to na základe povolenia príslušného pacienta.

3.6 Správnosť

77. Osobné údaje musia byť správne a aktualizované; musia sa vykonať všetky rozumné kroky, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na aké sa spracúvajú, bezodkladne vymažú alebo opravia.[38]

78. Tieto požiadavky by mali byť vnímané vo vzťahu k rizikám a dôsledkom konkrétneho použitia údajov. Nesprávne osobné údaje by mohli predstavovať riziko pre práva a slobody dotknutých osôb, napríklad vtedy, keď vedú k chybnej diagnóze alebo nesprávnemu zaobchádzaniu so zdravotným záznamom, alebo keď nesprávna fotografia osoby môže viesť k prijímaniu rozhodnutí na nesprávnom základe buď manuálne, pomocou automatizovaného rozhodovania, alebo prostredníctvom umelej inteligencie.

[38] Článok 5 ods. 1 písm. d) všeobecného nariadenia o ochrane údajov.

79. Pokiaľ ide o správnosť, ku kľúčovým prvkom špecificky navrhnutej a štandardnej ochrany údajov môže patriť:
    - zdroj údajov – zdroje osobných údajov by mali byť spoľahlivé z hľadiska správnosti údajov;
    - miera správnosti – každý prvok osobných údajov by mal byť pre potreby konkrétneho účelu čo možno najsprávnejší;
    - merateľná správnosť – obmedzenie počtu falošne pozitívnych/negatívnych výsledkov, napríklad chýb v automatizovaných rozhodnutiach a umelej inteligencii;
    - overovanie – v závislosti od povahy údajov, v súvislosti s tým, ako často sa môžu meniť, by mal prevádzkovateľ pred spracúvaním a v rôznych fázach spracúvania overovať správnosť osobných údajov u dotknutej osoby (napr. v súvislosti s požiadavkami týkajúcimi sa veku);
    - vymazanie/oprava – prevádzkovateľ musí bezodkladne vymazať alebo opraviť nesprávne údaje. Prevádzkovateľ to musí uľahčiť najmä vtedy, keď dotknutými osobami sú alebo boli deti a chcú takéto osobné údaje odstrániť;[39]
    - vyhýbanie sa šíreniu chýb – prevádzkovatelia by mali zmierňovať účinok kumulovanej chyby v reťazci spracovateľských operácií;
    - prístup – dotknutým osobám by sa mali poskytnúť informácie o osobných údajoch a účinný prístup k nim v súlade s článkami 12 až 15 všeobecného nariadenia o ochrane údajov, aby mohli kontrolovať ich správnosť a podľa potreby ich opraviť;
    - trvalá správnosť – osobné údaje by mali byť správne vo všetkých fázach spracúvania, v kritických krokoch by sa mal vykonať test správnosti;
    - aktuálnosť – osobné údaje sa musia aktualizovať, ak je to na daný účel nevyhnutné;
    - formát údajov – používanie technologických a organizačných formátových prvkov na obmedzenie nepresností, ako je uvedenie stručných vopred určených možností namiesto voľných textových polí.

Príklad 1

Poisťovňa chce využívať umelú inteligenciu na profilovanie zákazníkov, ktorí si od nej kupujú poistenie, ako základ rozhodovania pri počítaní poistného rizika. Pri rozhodovaní o tom, ako vyvinúť tieto riešenia v oblasti umelej inteligencie, určuje prostriedky spracúvania a musí pri výbere aplikácie umelej inteligencie od dodávateľa a pri rozhodovaní o spôsobe vyškolenia umelej inteligencie zvážiť špecificky navrhnutú ochranu údajov.

Pri určovaní spôsobu vyškolenia umelej inteligencie by mal mať prevádzkovateľ správne údaje, aby dosiahol presné výsledky. Preto by mal prevádzkovateľ zabezpečiť, aby boli na vyškolenie umelej inteligencie použité správne údaje.

Vzhľadom na to, že existuje platný právny základ pre učenie umelej inteligencie použitím osobných údajov od veľkej podmnožiny existujúcich zákazníkov, prevádzkovateľ si zvolí skupinu zákazníkov, ktorá je reprezentatívna pre celú skupinu, aby nedošlo k skresleniu údajov.

Údaje o zákazníkoch sa potom získavajú z príslušného systému spracúvania údajov vrátane údajov o druhu poistenia, napríklad zdravotného poistenia, poistenia domácnosti, cestovného poistenia atď., ako aj údajov z verejných registrov, ku ktorým má zákonný prístup. Všetky údaje sa pred prenosom do systému určeného na učenie modelu umelej inteligencie pseudonymizujú.

S cieľom zabezpečiť, aby údaje používané na vyškolenie umelej inteligencie boli čo najsprávnejšie, prevádzkovateľ získava len údaje zo zdrojov, ktoré obsahujú správne a aktuálne informácie.

[39] Porovnaj odôvodnenie 65.

Poisťovňa testuje, či je umelá inteligencia spoľahlivá a či poskytuje nediskriminačné výsledky tak počas jej vývoja, ako aj pred uvedením produktu do používania. Keď je umelá inteligencia plne naučená a funkčná, poisťovňa využíva výsledky na podporu posúdenia poistných rizík, ale pri rozhodovaní o tom, či poskytne poistenie, sa neopiera výlučne o umelú inteligenciu, pokiaľ sa rozhodnutie neprijme v súlade s výnimkami uvedenými v článku 22 ods. 2 všeobecného nariadenia o ochrane údajov.

Poisťovňa bude takisto v záujme zachovania spoľahlivosti pravidelne preskúmavať výsledky, ktoré umelá inteligencia poskytuje, a v prípade potreby algoritmus upraví.

Príklad 2

Prevádzkovateľ je zdravotnícke zariadenie, ktoré hľadá spôsoby na zabezpečenie integrity a správnosti osobných údajov vo svojich registroch klientov.

V situáciách, keď dve osoby prídu do zariadenia v rovnakom čase a poskytne sa im rovnaké ošetrenie, existuje riziko ich zámeny, ak jediným parametrom, v ktorom sa líšia, je ich meno. Prevádzkovateľ preto na zabezpečenie správnosti potrebuje jedinečný identifikátor pre každú osobu, a preto potrebuje viac informácií ako len meno klienta.

Zariadenie používa niekoľko systémov obsahujúcich osobné informácie klientov a musí zabezpečiť, aby informácie týkajúce sa klienta boli v každom okamihu správne, presné a konzistentné vo všetkých systémoch. Zariadenie identifikovalo niekoľko rizík, ktoré môžu vzniknúť, ak sa informácie zmenia v jednom systéme, ale nie v ostatných.

Prevádzkovateľ sa rozhodne zmierniť riziko použitím techniky hašovania, ktorá sa môže použiť na zabezpečenie integrity údajov v denníku poskytnutých ošetrení. Pre záznamy o ošetrení a príslušných klientoch sa vytvoria nemenné kryptografické časové pečiatky, ktoré umožňujú prípadné zmeny rozpoznať, priradiť do vzájomného vzťahu a v prípade potreby vysledovať.

3.7 Minimalizácia uchovávania

80. Prevádzkovateľ musí zabezpečiť, aby sa osobné údaje uchovávali vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú.[40]
Je nevyhnutné, aby prevádzkovateľ presne vedel, aké osobné údaje spoločnosť spracúva a prečo.
Účel spracúvania je hlavným kritériom pri rozhodovaní o tom, ako dlho sa osobné údaje uchovávajú.

81. Opatrenia a záruky, ktorými sa vykonáva zásada minimalizácie uchovávania, dopĺňajú práva a slobody dotknutých osôb, konkrétne právo na vymazanie a právo vzniesť námietku.

82. Pokiaľ ide o minimalizáciu uchovávania, ku kľúčovým prvkom špecificky navrhnutej a štandardnej ochrany údajov môže patriť:
    - vymazanie a anonymizácia – prevádzkovateľ by mal mať jasné vnútorné postupy a funkcie na vymazávanie a/alebo anonymizáciu;
    - účinnosť anonymizácie/vymazania – prevádzkovateľ zabezpečí, aby nebolo možné opätovne identifikovať anonymizované údaje alebo obnoviť vymazané údaje, a vykoná testy, či je to možné;

[40] Článok 5 ods. 1 písm. c) všeobecného nariadenia o ochrane údajov.

- automatizácia – vymazanie niektorých osobných údajov by malo byť automatizované;
- kritériá uchovávania – prevádzkovateľ musí určiť, ktoré údaje a aká dĺžka uchovávania sú potrebné na daný účel;
- odôvodnenie – prevádzkovateľ musí byť schopný odôvodniť, prečo je príslušné obdobie uchovávania nevyhnutné na daný účel a pre príslušné osobné údaje, a musí byť schopný zverejniť dôvody a právny dôvod obdobia uchovávania;
- presadzovanie politík v oblasti uchovávania – prevádzkovateľ by mal presadzovať interné politiky v oblasti uchovávania údajov a vykonať testy, či organizácia tieto politiky uplatňuje;
- zálohovanie/logy – prevádzkovatelia určujú, ktoré osobné údaje a aká dĺžka uchovávania sú potrebné pre zálohovanie a vedenie logov;
- tok údajov – prevádzkovatelia by si mali byť vedomí toku osobných údajov a uchovávania ich kópií a mali by sa snažiť obmedziť ich „dočasné“ uchovávanie.

Príklad

Prevádzkovateľ získava osobné údaje, pričom účelom spracúvania je správa členstva dotknutej osoby. Osobné údaje sa vymažú po skončení členstva a neexistuje právny základ pre ďalšie uchovávanie údajov.

Prevádzkovateľ v prvom rade vypracuje vnútorný postup na uchovávanie a vymazávanie údajov. Podľa tohto postupu musia zamestnanci po skončení obdobia uchovávania manuálne vymazať osobné údaje. Zamestnanec dodržiava tento postup, v rámci ktorého pravidelne vymazáva a opravuje údaje zo všetkých zariadení, záložných súborov, denníkov, e-mailov a iných relevantných pamäťových médií.

Aby bolo vymazávanie účinnejšie a znížil sa výskyt chýb, prevádzkovateľ namiesto toho zavedie automatický systém na automatické, spoľahlivé a pravidelnejšie vymazávanie údajov. Systém je nastavený tak, aby vykonával daný postup vymazania údajov vo vopred stanovenom pravidelnom intervale s cieľom odstrániť osobné údaje zo všetkých pamäťových médií danej spoločnosti. Prevádzkovateľ pravidelne preskúmava a testuje postup uchovávania a zabezpečuje, aby bol v súlade s aktuálnou politikou uchovávania údajov.

3.8 Integrita a dôvernosť

83. Zásada integrity a dôvernosti zahŕňa ochranu pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení. Bezpečnosť osobných údajov si vyžaduje primerané opatrenia určené na predchádzanie incidentom porušenia ochrany údajov a ich riadenie, zaručenie riadneho vykonávania úloh spracúvania údajov a dodržiavanie ďalších zásad, ako aj na umožnenie účinného uplatňovania práv jednotlivcov.

84. Odôvodnenie 78 uvádza, že jedným z opatrení ŠNaŠOÚ by mohlo byť umožniť prevádzkovateľovi „*vypracovať a zlepšiť bezpečnostné prvky*“. Spolu s ďalšími opatreniami ŠNaŠOÚ odôvodnenie 78 navrhuje, aby prevádzkovatelia priebežne posudzovali, či vždy využívajú primerané prostriedky spracúvania, a aby posúdili, či zvolené opatrenia skutočne riešia existujúce zraniteľnosti. Okrem toho by prevádzkovatelia mali vykonávať pravidelné preskúmania opatrení v oblasti informačnej bezpečnosti, ktoré súvisia s osobnými údajmi a ich ochranou, ako aj postupu riešenia prípadov porušenia ochrany údajov.

85. Pokiaľ ide o integritu a dôvernosť, ku kľúčovým prvkom špecificky navrhnutej a štandardnej ochrany údajov môže patriť:

- systém riadenia informačnej bezpečnosti – mať zavedené operatívne riadenie politík a postupov v oblasti informačnej bezpečnosti;
- analýza rizika – posúdenie rizík v súvislosti s bezpečnosťou osobných údajov zohľadnením vplyvu na práva jednotlivcov a prijatie opatrení proti zisteným rizikám. Na účely využívania pri hodnotení rizika – vypracovanie a udržiavanie komplexného, systematického a realistického „modelovania hrozieb" a analýzy plochy útoku [attack surface] navrhnutého softvéru s cieľom obmedziť vektory útokov a príležitosti na využitie slabých a zraniteľných miest;
- štandardná bezpečnosť – zohľadnenie bezpečnostných požiadaviek čo najskôr pri navrhovaní a vývoji systému a nepretržité začleňovanie a vykonávanie príslušných testov;
- údržba – pravidelné kontroly a testovanie softvéru, hardvéru, systémov a služieb atď. s cieľom odhaliť slabé miesta systémov podporujúcich spracúvanie;
- riadenie kontroly prístupu – len oprávnení zamestnanci, ktorí potrebujú mať prístup k osobným údajom nevyhnutným na plnenie svojich spracovateľských úloh, by mali mať prístup k týmto údajom, pričom prevádzkovateľ by mal rozlišovať medzi prístupovými oprávneniami oprávnených zamestnancov;
    - obmedzenie prístupu (agenti) – upraviť spracúvanie údajov tak, aby na vykonávanie svojich úloh potreboval prístup k osobným údajom minimálny počet osôb, a zodpovedajúcim spôsobom obmedziť prístup;
    - obmedzenie prístupu (obsah) – v súvislosti s každou spracovateľskou operáciou sa prístup obmedzuje len na tie atribúty na jeden súbor údajov, ktoré sú potrebné na vykonanie príslušnej operácie. Okrem toho je prístup obmedzený na údaje týkajúce sa tých dotknutých osôb, ktoré patria do kompetencií príslušného zamestnanca;
    - oddelenie prístupu – taká úprava spracúvania údajov, aby žiadna osoba nepotrebovala komplexný prístup ku všetkým získaným údajom o dotknutej osobe, a už vôbec nie ku všetkým osobným údajom konkrétnej kategórie dotknutých osôb;
- bezpečné prenosy – prenosy sú zabezpečené proti neoprávnenému a náhodnému prístupu a zmenám;
- bezpečné uchovávanie – uchovávanie údajov musí byť zabezpečené pred neoprávneným prístupom a zmenami. Mali by existovať postupy na posúdenie rizika centralizovaného alebo decentralizovaného uchovávania, ako aj na ktoré kategórie osobných údajov sa to vzťahuje. Niektoré údaje si môžu vyžadovať dodatočné bezpečnostné opatrenia v porovnaní s inými údajmi alebo izoláciu od iných údajov;
- pseudonymizácia – osobné údaje a zálohovanie/logy by mali byť pseudonymizované ako bezpečnostné opatrenie s cieľom minimalizovať riziká možného porušenia ochrany údajov, napríklad použitím hašovania alebo šifrovania;
- zálohovanie/logy – uchovávanie záloh a logov v rozsahu potrebnom pre bezpečnosť informácií, využívanie revíznych záznamov [audit trails] a monitorovanie incidentov v rámci bežnej bezpečnostnej kontroly. Musia byť chránené pred neoprávneným a náhodným prístupom a zmenou a pravidelne sa preskúmavať, pričom incidenty by sa mali bezodkladne riešiť;
- havárijný plán [Disaster recovery]/kontinuita prevádzky [Business continuity] – riešenie požiadaviek obnovy informačného systému po havárii a požiadaviek na obnovenie dostupnosti osobných údajov po vážnych incidentoch;
- ochrana na základe rizika – všetky kategórie osobných údajov by mali byť chránené primeranými opatreniami vzhľadom na riziko narušenia bezpečnosti. Ak je to možné, údaje predstavujúce osobitné riziká by sa mali uchovávať oddelene od ostatných osobných údajov;

- riadenie reakcie na bezpečnostné incidenty – zavedenie rutinných procesov, postupov a zdrojov na odhalenie, riešenie, nahlasovanie porušení ochrany údajov a poučenie sa z týchto incidentov;
- riadenie incidentov – prevádzkovateľ by mal mať zavedené postupy na riešenie porušení a incidentov, aby bol systém spracúvania odolnejší. To zahŕňa postupy oznamovania, ako je spravovanie oznamovania (dozornému orgánu) a poskytovanie informácií (dotknutým osobám).

Príklad

Prevádzkovateľ chce extrahovať veľké množstvo osobných údajov zo zdravotníckej databázy obsahujúcej elektronické zdravotné záznamy (pacientov) na špecializovaný databázový server v spoločnosti s cieľom spracúvať získané údaje na účely zabezpečenia kvality. Spoločnosť posúdila riziko presmerovania získaných údajov na server, ktorý je dostupný pre všetkých zamestnancov spoločnosti, a dospela k záveru, že riziko pre práva a slobody dotknutých osôb bude pravdepodobne vysoké. Keďže v spoločnosti je len jedno oddelenie, ktoré potrebuje spracúvať získané údaje o pacientoch, prevádzkovateľ sa rozhodne obmedziť prístup k vyhradenému serveru zamestnancom tohto oddelenia. Okrem toho na účely ďalšieho zníženia rizika budú údaje pred prenosom pseudonymizované.

Spoločnosť sa rozhodla sieť oddeliť a zaviesť kontroly prístupu na server s cieľom regulovať prístup a zmierniť potenciálne škody spôsobené škodlivým softvérom. Okrem toho zavedie bezpečnostné monitorovanie a systém detekcie a prevencie narušenia a oddelí ho od bežného používania. Zavedie sa automatický systém auditovania s cieľom monitorovať prístup a zmeny. Pri konfigurácii určitých udalostí súvisiacich s používaním sa generujú hlásenia a automatické upozornenia. Prevádzkovateľ zabezpečí, aby používatelia mali prístup len k údajom, ktoré potrebujú poznať, a v súlade s vhodnou úrovňou prístupu. Nevhodné používanie možno rýchlo a ľahko zistiť.

Niektoré získané údaje sa musia porovnať s novými získanými údajmi, a preto sa musia uchovávať tri mesiace. Prevádzkovateľ sa rozhodne umiestniť ich do samostatných databáz na rovnakom serveri a použiť transparentné šifrovanie aj šifrovanie na úrovni stĺpcov na ich ukladanie. Kľúče na dešifrovanie údajov na úrovni stĺpcov sú uložené vo vyhradených bezpečnostných moduloch, ktoré môžu používať len oprávnení zamestnanci, ale nemožno ich extrahovať.

Riešením nasledujúcich incidentov sa systém stáva odolnejším a spoľahlivejším. Prevádzkovateľ si je vedomý toho, že preventívne a účinné opatrenia a záruky by sa mali začleniť do všetkých činností spracúvania osobných údajov, tak súčasných, ako aj budúcich, a že to môže pomôcť pri predchádzaní takýmto incidentom v budúcnosti.

Prevádzkovateľ zavádza tieto bezpečnostné opatrenia na zabezpečenie správnosti, integrity a dôvernosti, ako aj na zabránenie šírenia škodlivého softvéru prostredníctvom kybernetických útokov a posilňuje tak spoľahlivosť tohto riešenia. Spoľahlivé bezpečnostné opatrenia prispievajú k budovaniu dôvery dotknutých osôb.

3.9 Zodpovednosť[41]

86. Zásada zodpovednosti uvádza, že prevádzkovateľ je zodpovedný za súlad so všetkými uvedenými zásadami a musí vedieť tento súlad preukázať.

[41] Pozri odôvodnenie 74, podľa ktorého musia prevádzkovatelia preukázať účinnosť svojich opatrení.

87. Prevádzkovateľ musí vedieť preukázať súlad so zásadami. Prevádzkovateľ tak môže preukázať účinky opatrení prijatých na ochranu práv dotknutých osôb a prečo sa dané opatrenia považujú za primerané a účinné. Napríklad, preukázaním prečo je opatrenie primerané na účinné zabezpečenie zásady minimalizácie uchovávania.

88. Aby mohol prevádzkovateľ spracúvať osobné údaje zodpovedným spôsobom, mal by mať vedomosti o vykonávaní ochrany údajov a schopnosť ju vykonávať. Znamená to, že prevádzkovateľ by mal rozumieť svojim povinnostiam ochrany údajov stanoveným vo všeobecnom nariadení o ochrane údajov a mal by byť schopný ich dodržiavať.

4 ČLÁNOK 25 ODS. 3 CERTIFIKÁCIA

89. Podľa článku 25 ods. 3 sa certifikácia podľa článku 42 môže použiť ako prvok na preukázanie súladu so ŠNaŠOÚ. Dokumenty preukazujúce súlad so ŠNaŠOÚ môžu byť zas užitočné v certifikačnom procese. To znamená, že ak bola spracovateľská operácia vykonaná prevádzkovateľom alebo sprostredkovateľom certifikovaná podľa článku 42, orgány dohľadu to zohľadnia pri posudzovaní súladu so všeobecným nariadením o ochrane údajov, najmä pokiaľ ide o ŠNaŠOÚ.

90. Ak je spracovateľská operácia, ktorú vykonáva prevádzkovateľ alebo sprostredkovateľ, certifikovaná podľa článku 42, prvky, ktoré prispievajú k preukázaniu súladu s článkom 25 ods. 1 a 2, sú procesy navrhovania, t. j. proces určovania prostriedkov spracúvania, riadenie a technické a organizačné opatrenia na vykonávanie zásad ochrany údajov. Kritériá certifikácie ochrany údajov určujú certifikačné orgány alebo majitelia certifikačnej schémy a následne ich schvaľuje príslušný dozorný orgán alebo EDPB. Viac informácií o mechanizmoch certifikácie nájde čitateľ v usmerneniach EDPB k certifikácii[42] a iných relevantných usmerneniach zverejnených na webovom sídle EDPB.

91. Aj v prípadoch, keď spracovateľská operácia získala certifikáciu v súlade s článkom 42, prevádzkovateľ je stále zodpovedný za nepretržité monitorovanie a zlepšovanie dodržiavania kritérií ŠNaŠOÚ uvedených v článku 25.

5 PRESADZOVANIE ČLÁNKU 25 A DÔSLEDKY

92. Dozorné orgány môžu posudzovať súlad s článkom 25 podľa postupov uvedených v článku 58. Nápravné právomoci sú uvedené v článku 58 ods. 2 a zahŕňajú upozorňovanie, napomínanie, nariadenie dodržiavania práv dotknutých osôb, obmedzenia alebo zákaz spracúvania, správne pokuty atď.

93. ŠNaŠOÚ okrem toho predstavuje faktor pri určovaní výšky peňažných sankcií za porušenie všeobecného nariadenia o ochrane údajov, pozri článok 83 ods. 4.[43] [44]

[42] EDPB, Usmernenia č. 1/2018 týkajúce sa certifikácie a určovania kritérií certifikácie podľa článkov 42 a 43 nariadenia, verzia 3.0, 4. jún 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_sk_0.pdf.

[43] Článok 83 ods. 2 písm. d) všeobecného nariadenia o ochrane údajov stanovuje, že pri určovaní ukladania pokút za porušenie všeobecného nariadenia o ochrane údajov „*sa náležite zohľadní miera zodpovednosti prevádzkovateľa alebo sprostredkovateľa so zreteľom na technické a organizačné opatrenia, ktoré prijali podľa článkov 25 a 32*“.

[44] Viac informácií o pokutách sa nachádza v usmerneniach pracovnej skupiny zriadenej podľa článku 29 k uplatňovaniu a stanovovaniu správnych pokút na účely nariadenia 2016/679, WP 253, utorok 3. októbra 2017. ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 – schválené EDPB.

6 ODPORÚČANIA

94. Hoci sa na sprostredkovateľov a výrobcov článok 25 priamo nevzťahuje, takisto sa považujú za kľúčových aktérov ŠNaŠOÚ a mali by mať na zreteli, že od prevádzkovateľov sa vyžaduje, aby spracúvali osobné údaje len pomocou systémov a technológií, ktoré majú zabudovanú ochranu údajov.

95. Pri spracúvaní v mene prevádzkovateľov alebo poskytovaní riešení prevádzkovateľom by sprostredkovatelia a výrobcovia mali využívať svoje odborné znalosti na budovanie dôvery a usmerňovanie svojich zákazníkov vrátane MSP pri navrhovaní/obstarávaní riešení, ktoré zahŕňajú do procesu ochrany údajov. To naopak znamená, že návrhy produktov a služieb by mali zohľadňovať potreby prevádzkovateľov.

96. Pri vykonávaní článku 25 by sa malo zohľadňovať, že hlavným cieľom návrhu je *účinné zavedenie* zásad a *ochrany* práv dotknutých osôb do primeraných opatrení spracúvania. S cieľom uľahčiť a posilniť prijatie ŠNaŠOÚ predkladáme prevádzkovateľom, ako aj výrobcom a sprostredkovateľom tieto odporúčania:
    - Prevádzkovatelia by mali ochranu údajov zohľadňovať už v *počiatočných fázach* plánovania spracovateľskej operácie, a to ešte pred určením prostriedkov spracúvania.
    - Ak má prevádzkovateľ zodpovednú osobu, EDPB nabáda k aktívnemu zapojeniu zodpovednej osoby s cieľom začleniť ŠNaŠOÚ do postupov obstarávania a vývoja, ako aj do celého životného cyklu spracúvania.
    - Spracovateľská operácia môže byť *certifikovaná*. Možnosť získať certifikát pre spracovateľskú operáciu poskytuje prevádzkovateľovi pridanú hodnotu pri výbere medzi rôznymi spracovateľskými softvérmi, hardvérom, službami a/alebo systémami od výrobcov alebo sprostredkovateľov. Výrobcovia by sa preto mali snažiť preukázať ŠNaŠOÚ v životnom cykle ich vývoja spracovateľského riešenia. Certifikačná pečať môže takisto usmerniť dotknuté osoby pri výbere medzi rôznymi tovarmi a službami. Možnosť získať certifikát pre spracúvanie môže slúžiť ako konkurenčná výhoda pre výrobcov, prevádzkovateľov a sprostredkovateľov a môže dokonca zvýšiť dôveru dotknutých osôb, pokiaľ ide o spracúvanie ich osobných údajov. Ak certifikácia nie je ponúknutá, mali by sa prevádzkovatelia snažiť získať iné *záruky*, že výrobcovia alebo sprostredkovatelia spĺňajú požiadavky ŠNaŠOÚ.
    - Prevádzkovatelia, sprostredkovatelia a výrobcovia by mali mať na zreteli svoje povinnosti poskytovať osobám mladším ako 18 rokov a iným zraniteľným skupinám osobitnú ochranu pri dodržiavaní ŠNaŠOÚ.
    - Výrobcovia a sprostredkovatelia by sa mali snažiť uľahčiť vykonávanie ŠNaŠOÚ s cieľom podporiť schopnosť prevádzkovateľa plniť povinnosti podľa článku 25. Prevádzkovatelia by si naopak nemali vyberať výrobcov ani sprostredkovateľov, ktorí neponúkajú systémy umožňujúce alebo pomáhajúce prevádzkovateľovi dodržiavať článok 25, pretože prevádzkovatelia nesú zodpovednosť za nedodržiavanie tohto článku.
    - Výrobcovia a sprostredkovatelia by mali zohrávať aktívnu úlohu pri zabezpečovaní toho, aby bolo splnené kritérium stavu podľa „najnovších poznatkov“, a informovať prevádzkovateľov o všetkých zmenách „najnovších poznatkov“, ktoré môžu ovplyvniť účinnosť zavedených opatrení. Prevádzkovatelia by mali túto požiadavku zahrnúť ako zmluvné ustanovenie, aby tým zabezpečili, že budú mať aktuálne informácie.
    - EDPB odporúča prevádzkovateľom, aby od výrobcov a sprostredkovateľov vyžadovali preukázanie, ako ich hardvér, softvér, služby alebo systémy umožňujú prevádzkovateľovi

dodržiavať požiadavky zodpovednosti v súlade so ŠNaŠOÚ, napr. pomocou kľúčových ukazovateľov výkonnosti na preukázanie účinnosti opatrení a záruk pri vykonávaní zásad a práv.

- EDPB zdôrazňuje potrebu harmonizovaného prístupu k účinnému uplatňovaniu zásad a práv a nabáda združenia alebo orgány, ktoré pripravujú kódexy správania v súlade s článkom 40, aby do nich zahrnuli aj usmernenia pre jednotlivé sektory k ŠNaŠOÚ.
- Prevádzkovatelia by mali byť korektní voči dotknutým osobám a transparentní, pokiaľ ide o spôsob posudzovania a preukazovanie účinného vykonávania ŠNaŠOÚ, a postupovať rovnako, ako keď prevádzkovatelia preukazujú súlad so všeobecným nariadením o ochrane údajov podľa zásady zodpovednosti.
- Technológie na zvyšovanie súkromia, ktoré dosahujú kritériá stavu najnovších poznatkov, sa môžu použiť ako opatrenie v súlade s požiadavkami ŠNaŠOÚ, ak je to primerané v rámci prístupu založenom na riziku. Technológie na zvyšovanie súkromia samy osebe nemusia zahŕňať povinnosti obsiahnuté v článku 25. Prevádzkovatelia posúdia, či je opatrenie primerané a účinné, pokiaľ ide o vykonávanie zásad ochrany údajov a práv dotknutých osôb.
- Na existujúce pôvodné systémy sa vzťahujú rovnaké povinnosti v oblasti ŠNaŠOÚ ako na nové systémy. Pokiaľ pôvodné systémy už nie sú v súlade so ŠNaŠOÚ a nemožno vykonať zmeny na splnenie týchto povinností, pôvodný systém jednoducho nespĺňa povinnosti všeobecného nariadenia o ochrane údajov a nemôže sa používať na spracúvanie osobných údajov.
- Článok 25 neznižuje úroveň požiadaviek pre MSP. MSP môžu dodržiavanie súladu s článkom 25 uľahčiť tieto kroky:
    - vykonať posúdenia rizika v skorom štádiu,
    - začať spracúvanie v malom a neskôr zvýšiť jeho rozsah a zložitosť,
    - vyhľadávať záruky ŠNaŠOÚ poskytované výrobcom a sprostredkovateľom, ako je certifikácia a dodržiavanie kódexu správania,
    - využívať partnerov, ktorí dosahujú dobré výsledky,
    - komunikovať s orgánmi pre ochranu údajov,
    - prečítať si usmernenia orgánov pre ochranu údajov a EDPB,
    - dodržiavať kódexy správania, ak sú k dispozícii,
    - získať odbornú pomoc a poradenstvo.

Za Európsky výbor pre ochranu údajov

predsedníčka

(Andrea Jelinek)