Usmernenia

Usmernenia č. 1/2018 týkajúce sa certifikácie a určovania kritérií certifikácie podľa článkov 42 a 43 nariadenia 2016/679

Verzia 3.0

4. júna 2019

Prijaté

Prehľad verzií

Verzia 3.0	4. júna 2019	Zahrnutie prílohy 2 (verzia 2.0 prílohy 2 prijatá 4. júna 2019 po verejnej konzultácii)
Verzia 2.1	9. apríla 2019	Prijatie korigenda k usmerneniam (odsek 45)
Verzia 2.0	23. januára 2019	Prijatie usmernení po verejnej konzultácii – k tomu istému dátumu bola prijatá príloha 2 (verzia 1.0) na účely verejnej konzultácie
Verzia 1.0	25. mája 2018	Prijatie usmernení na účely verejnej konzultácie

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

so zreteľom na články 12 a 22 svojho rokovacieho poriadku z 25. mája 2018,

po zohľadnení výsledkov verejnej konzultácie k usmerneniam, ktorá sa uskutočnila v období od 30. mája 2018 do 12. júla 2018, a k prílohe 2, ktorá sa uskutočnila od 15. februára do 29. marca 2019, podľa článku 70 ods. 4 všeobecného nariadenia o ochrane údajov

PRIJAL TOTO USMERNENIE

1 ÚVOD

1. Všeobecné nariadenie o ochrane údajov (nariadenie 2016/279, ďalej len „všeobecné nariadenie o ochrane údajov“ alebo „nariadenie“) poskytuje modernizovaný rámec pre právnu zodpovednosť a dodržiavanie základných práv v oblasti ochrany údajov v Európe. Ústredným prvkom tohto nového rámca je celý rad opatrení, ktoré uľahčujú dodržiavanie ustanovení všeobecného nariadenia o ochrane údajov. Patria k nim povinné požiadavky pre prípad určitých konkrétnych okolností (napr. prípad vymenovania zodpovedných osôb a vykonávania posúdení vplyvu na ochranu údajov) a dobrovoľné opatrenia, ako sú napr. kódexy správania a certifikačné mechanizmy.

2. Pred prijatím všeobecného nariadenia o ochrane údajov WP29 konštatovala, že certifikácia by mohla zohrávať dôležitú úlohu v rámci právnej zodpovednosti za ochranu údajov.[1] Aby mohla byť certifikácia spoľahlivým dôkazom dodržiavania predpisov o ochrane údajov, treba zaviesť jasné pravidlá stanovujúce požiadavky na poskytovanie certifikácie.[2] V článku 42 všeobecného nariadenia o ochrane údajov sa stanovuje právny základ pre vypracovanie takýchto pravidiel.

3. V článku 42 ods. 1 všeobecného nariadenia o ochrane údajov sa stanovuje, že:

> „Členské štáty, dozorné orgány, výbor [Európsky výbor pre ochranu údajov] a Európska komisia podporia, predovšetkým na úrovni Únie, zavedenie certifikačných mechanizmov ochrany údajov a pečatí a značiek ochrany údajov na účely preukázania súladu s týmto nariadením, pokiaľ ide o spracovateľské operácie vykonávané prevádzkovateľmi a sprostredkovateľmi. Zohľadnia sa osobitné potreby mikropodnikov a malých a stredných podnikov“.

[1] Stanovisko WP29 č. 3/2010 týkajúce sa zásady právnej zodpovednosti, WP173, 13. júla 2010, odseky 69 – 71.

[2] Stanovisko WP29 č. 3/2010 týkajúce sa zásady právnej zodpovednosti, (WP173), odsek 69.

4. Certifikačné mechanizmy[3] môžu zaistiť väčšiu transparentnosť pre dotknuté osoby, ale aj vo vzťahoch medzi podnikmi, napríklad medzi prevádzkovateľmi a sprostredkovateľmi. V odôvodnení 100 všeobecného nariadenia o ochrane údajov sa uvádza, že vytvorenie certifikačných mechanizmov môže viesť k zlepšeniu transparentnosti a posilneniu súladu s nariadením a môže dotknutým osobám umožniť posúdiť úroveň ochrany údajov v prípade relevantných produktov a služieb[4].

5. Všeobecným nariadením o ochrane údajov sa nestanovuje právo prevádzkovateľov a sprostredkovateľov na certifikáciu ani povinnosť certifikácie; podľa článku 42 ods. 3 je certifikácia dobrovoľným procesom, ktorý má pomôcť pri preukazovaní súladu so všeobecným nariadením o ochrane údajov. Členské štáty a dozorné orgány sa vyzývajú, aby podporovali zavedenie certifikačných mechanizmov, a určia zapojenie zainteresovaných strán do procesu a životného cyklu certifikácie.

6. Dodržiavanie schválených certifikačných mechanizmov je navyše jedným z faktorov, ktoré musia dozorné orgány zohľadniť ako priťažujúcu alebo poľahčujúcu okolnosť pri rozhodovaní o uložení správnej pokuty a jej výške [článok 83 ods. 2 písm. j)][5].

1.1 Rozsah pôsobnosti usmernení

7. Rozsah pôsobnosti týchto usmernení je obmedzený; nejde o príručku postupov pri certifikácii podľa všeobecného nariadenia o ochrane údajov. Hlavným cieľom týchto usmernení je určiť všeobecné požiadavky a kritériá, ktoré môžu byť relevantné pre všetky druhy certifikačných mechanizmov vytvorených podľa článkov 42 a 43 všeobecného nariadenia o ochrane údajov. V usmerneniach sa na tento účel:

    - skúmajú dôvody certifikácie ako nástroja právnej zodpovednosti,
    - vysvetľujú kľúčové pojmy ustanovení článkov 42 a 43 týkajúcich sa certifikácie a
    - objasňuje predmet toho, čo môže byť podľa článkov 42 a 43 predmetom certifikácie, ako aj účel certifikácie,
    - zabezpečuje, aby výsledky certifikácie mali výpovednú hodnotu a boli jednoznačné, čo možno najviac reprodukovateľné a porovnateľné bez ohľadu na subjekt vykonávajúci certifikáciu (porovnateľnosť).

8. Všeobecné nariadenie o ochrane údajov umožňuje členským štátom a dozorným orgánom vykonávať články 42 a 43 rôznymi spôsobmi. Usmernenia uvádzajú odporúčania týkajúce sa výkladu ustanovení článkov 42 a 43 a ich vykonávania a pomôžu členským štátom, dozorným orgánom a vnútroštátnym akreditačným orgánom zaviesť jednotnejší a harmonizovaný prístup k uplatňovaniu certifikačných mechanizmov podľa všeobecného nariadenia o ochrane údajov.

---

[3] Certifikačné mechanizmy a pečate a značky ochrany údajov sa v týchto usmerneniach spoločne označujú ako „certifikačné mechanizmy“, pozri oddiel 1.3.2.

[4] V odôvodnení 100 sa uvádza, že vytvorenie certifikačných mechanizmov by sa malo podporiť s cieľom „zlepšiť transparentnosť a posilniť súlad s týmto nariadením, aby sa dotknutým osobám umožnilo rýchlo posúdiť úroveň ochrany údajov v prípade relevantných produktov a služieb“.

[5] Pozri dokument WP29, Usmernenia týkajúce sa používania a stanovovania správnych pokút na účely nariadenia 2016/679 (WP 253).

9. Odporúčania uvedené v usmerneniach budú relevantné pre:

    - príslušné dozorné orgány a Európsky výbor pre ochranu údajov (ďalej len „EDPB“) pri schvaľovaní kritérií certifikácie podľa článku 42 ods. 5, článku 58 ods. 3 písm. f) a článku 70 ods. 1 písm. o),
    - certifikačné subjekty pri vypracúvaní a revidovaní kritérií certifikácie pred ich predložením príslušnému dozornému orgánu na schválenie podľa článku 42 ods. 5,
    - EDPB pri schvaľovaní európskej pečate ochrany údajov podľa článku 42 ods. 5 a článku 70 ods. 1 písm. o),
    - dozorné orgány pri vypracúvaní vlastných kritérií certifikácie,
    - Európsku komisiu, ktorá je podľa článku 43 ods. 8 splnomocnená prijímať delegované akty na účely bližšieho určenia požiadaviek, ktoré treba zohľadniť v certifikačných mechanizmoch,
    - EDPB pri poskytovaní stanoviska k požiadavkám na certifikáciu Európskej komisii v súlade s článkom 70 ods. 1 písm. q) a článkom 43 ods. 8,
    - národné akreditačné orgány, ktoré budú musieť zohľadňovať kritériá certifikácie v súvislosti s akreditáciou certifikačných subjektov podľa normy EN-ISO/IEC 17065/2012 a dodatočné požiadavky podľa článku 43 a
    - prevádzkovateľov a sprostredkovateľov pri stanovovaní vlastnej stratégie dodržiavania všeobecného nariadenia o ochrane údajov a zvažovaní certifikácie ako prostriedku na preukázanie dodržiavania.

10. EDPB uverejní v súlade s článkom 42 ods. 2 samostatné usmernenia týkajúce sa stanovovania kritérií schvaľovania certifikačných mechanizmov ako nástrojov na prenos do tretích krajín alebo medzinárodným organizáciám.

1.2 Účel certifikácie podľa všeobecného nariadenia o ochrane údajov

11. V článku 42 ods. 1 sa stanovuje, že certifikačné mechanizmy sa majú zaviesť „na účely preukázania súladu s týmto nariadením, pokiaľ ide o spracovateľské operácie vykonávané prevádzkovateľmi a sprostredkovateľmi“.

12. Všeobecné nariadenie o ochrane údajov uvádza príklady situácií, v ktorých sa môžu schválené certifikačné mechanizmy používať ako prvok na preukázanie dodržiavania povinností prevádzkovateľov a sprostredkovateľov týkajúcich sa:

    - vykonávania a preukázania vhodných technických a organizačných opatrení uvedených v článku 24 ods. 1 a ods. 3, článku 25 a článku 32 ods. 1 a 3,
    - dostatočných záruk (sprostredkovateľa voči prevádzkovateľovi) uvedených v článku 28 ods. 1 a (ďalšieho sprostredkovateľa voči sprostredkovateľovi) ods. 4.

13. Keďže certifikácia nie je sama osebe dôkazom súladu, ale skôr prvkom, ktorý možno použiť na preukázanie súladu, mala by sa uskutočňovať transparentným spôsobom. Na preukázanie súladu sú potrebné podkladové dokumenty, konkrétne písomné správy, v ktorých sa nielen opakujú kritériá, ale sa aj opisuje, ako sú kritériá splnené, a ak kritériá nie sú na počiatku

splnené, opisujú sa opravy a nápravné opatrenia a ich vhodnosť, ktorými sa poskytujú dôvody na udelenie a zachovanie certifikácie. To zahŕňa aj návrh konkrétneho rozhodnutia o udelení, obnovení alebo odňatí certifikátu. Rozhodnutie by malo uvádzať dôvody, argumenty a dôkazy vyplývajúce z uplatnenia kritérií a závery, úsudky alebo dedukcie, ku ktorým sa dospelo na základe faktov alebo premís zhromaždených počas certifikácie.

1.3 Kľúčové pojmy

14. V nasledujúcom oddiele sa rozoberajú kľúčové pojmy uvedené v článkoch 42 a 43. V tejto analýze sa rozvíja chápanie základných pojmov a predmet certifikácie *[scope of certification]* podľa všeobecného nariadenia o ochrane údajov.

1.3.1 Výklad pojmu „certifikácia“

15. Vo všeobecnom nariadení o ochrane údajov sa pojem „certifikácia“ nevymedzuje. Medzinárodná organizácia pre normalizáciu (ISO) vypracovala univerzálnu definíciu certifikácie, podľa ktorej ide o „poskytnutie písomného uistenia (certifikátu) nezávislým orgánom o tom, že príslušný výrobok, služba alebo systém spĺňa osobitné požiadavky.“ Certifikácia sa chápe aj ako „posudzovanie zhody treťou stranou“ a certifikačné subjekty sa môžu označovať aj ako „orgány posudzovania zhody“. V norme EN-ISO/IEC 17000: 2004 – Posudzovanie zhody – Slovník a všeobecné zásady (na ktorú sa odkazuje v norme ISO 17065) je certifikácia je definovaná takto: „atestácia ... treťou stranou týkajúca sa produktov, procesov a služieb“.

16. Atestácia je „vydanie osvedčenia založeného na rozhodnutí po preskúmaní, že sa preukázalo splnenie určených požiadaviek“ (oddiel 5.2 normy ISO 17000: 2004).

17. V kontexte certifikácie podľa článkov 42 a 43 všeobecného nariadenia o ochrane údajov je certifikácia atestácia treťou stranou týkajúca sa spracovateľských operácií prevádzkovateľov a sprostredkovateľov.

1.3.2 Certifikačné mechanizmy, pečate a značky

18. Vo všeobecnom nariadení o ochrane údajov sa pojmy „certifikačné mechanizmy, pečate alebo značky“ nevymedzujú a používajú sa spolu. Certifikát je vyhlásením zhody. Pečať alebo značka sa môžu použiť na potvrdenie úspešného dokončenia postupu certifikácie. Pečaťou alebo značkou je zvyčajne logo alebo symbol, ktorého prítomnosť poukazuje (popri certifikáte) na to, že predmet certifikácie bol nezávisle posúdený v rámci postupu certifikácie a spĺňa stanovené požiadavky uvedené v normatívnych dokumentoch, ako sú nariadenia, normy alebo technické špecifikácie. V súvislosti s certifikáciou podľa všeobecného nariadenia o ochrane údajov sú tieto požiadavky stanovené v dodatočných požiadavkách, ktoré dopĺňajú pravidlá akreditácie certifikačných subjektov stanovené v norme EN-ISO/IEC 17065/2012 a kritériá certifikácie schválené príslušným dozorným orgánom alebo Výborom. Podľa všeobecného nariadenia o ochrane údajov možno certifikát, pečať alebo značku vydať len na základe nezávislého posúdenia dôkazov akreditovaným certifikačným subjektom alebo príslušným dozorným orgánom, v ktorom sa uvádza, že kritériá certifikácie boli splnené.

19. V tabuľke je uvedený všeobecný príklad procesu certifikácie.

Predloženie žiadosti prevádzkovateľom alebo sprostredkovateľom	Formálna kontrola certifikačným subjektom	Posúdenie Predbežné vyhodnotenie	Posúdenie Vyhodnotenie cieľa hodnotenia (ToE)	Posúdenie Potvrdenie výsledkov	Informácia pre dotknutý dozorný orgán	Certifikácia	Monitorovanie	Obnovenie certifikácie
Je opis cieľa hodnotenia (ToE) jednoznačný a úplný a zahŕňa aj rozhrania?	Je opis cieľa hodnotenia (ToE) možné akceptovať?	Aké kritéria treba uplatniť?	Zodpovedá cieľ hodnotenia (ToE) kritériám?	Sú všetky relevantné kritériá vymedzené a odrážajú cieľ hodnotenia (ToE)?	Sú uvedené dôvody udelenia, resp. odňatia certifikácie?	Možno udeliť certifikát?	Spĺňa cieľ hodnotenia (ToE) aj naďalej kritériá?	Spĺňa spracúvanie aj naďalej kritéria certifikácie?
Možno poskytnúť prístup k spracovateľským činnostiam cieľa hodnotenia (ToE) ?	Sú všetky dokumenty úplné a aktuálne?	Aké metódy hodnotenia treba uplatniť?	Je cieľ hodnotenia (ToE) zdokumentovaný správne?	Je vyhodnotenie dostatočne zdokumentované?		Sú správy pripravené na uverejnenie?	Používa sa certifikát/pečať/značka správne?	Sú oblasti vývoja riešené uspokojivo?
Článok 42 ods. 6	Článok 43 ods. 4	Článok 43 ods. 4	Článok 42 ods. 5, článok 43 ods. 4	Článok 43 ods. 4	Článok 43 ods. 1 a ods. 5	Článok 43 ods. 1 Článok 42 ods. 7	Článok 42 ods. 7	Článok 42 ods. 7

2 ÚLOHA DOZORNÝCH ORGÁNOV

20. V článku 42 ods. 5 sa stanovuje, že certifikáciu vydáva akreditovaný certifikačný subjekt alebo príslušný dozorný orgán. Dozorné orgány nie sú podľa všeobecného nariadenia o ochrane údajov povinné vydávať certifikácie. Všeobecné nariadenie o ochrane údajov namiesto toho umožňuje niekoľko rôznych modelov. Dozorný orgán si môže napríklad vybrať jednu alebo viaceré z týchto možností:

    - vydávať certifikácie sám, v súvislosti s vlastnou certifikačnou schémou;
    - vydávať certifikácie sám, v súvislosti s vlastnou certifikačnou schémou, ale delegovať celý proces posudzovania alebo jeho časť na tretie strany;
    - vytvoriť vlastnú certifikačnú schému a poveriť postupom certifikácie a vydávaním certifikácie certifikačné subjekty; a
    - podnecovať trh na vytvorenie certifikačných mechanizmov.

21. Dozorný orgán bude zároveň musieť zvážiť svoju úlohu vo vzťahu k rozhodnutiam o mechanizmoch akreditácie prijímaným na vnútroštátnej úrovni, najmä ak je samotný dozorný orgán podľa článku 43 ods. 1 všeobecného nariadenia o ochrane údajov oprávnený akreditovať certifikačné subjekty. Každý dozorný orgán teda určí, ktorý prístup sa v záujme naplnenia široko vymedzeného zámeru certifikácie podľa všeobecného nariadenia o ochrane údajov uplatní. Uvedené sa určí nielen v súvislosti s úlohami a právomocami podľa článkov 57 a 58, ale aj vo vzťahu k zohľadneniu certifikácie ako faktora, ktorý treba vziať do úvahy pri určovaní správnych pokút, a vo všeobecnosti ako prostriedku na preukázanie zhody.

2.1 Dozorný orgán ako certifikačný subjekt

22. Ak sa dozorný orgán rozhodne vykonávať certifikáciu, bude musieť starostlivo posúdiť svoje poslanie, pokiaľ ide o úlohy, ktoré mu vyplývajú zo všeobecného nariadenia o ochrane údajov. Jeho poslanie pri výkone funkcií by malo byť transparentné. V záujme predídenia prípadným konfliktom záujmov bude musieť osobitne prihliadať na oddelenie právomocí súvisiacich s vyšetrovaním a presadzovaním.

23. Pri výkone funkcie certifikačného subjektu bude musieť dozorný orgán zabezpečiť riadne vytvorenie certifikačného mechanizmu a vypracovať alebo prijať vlastné kritériá certifikácie. Každý dozorný orgán, ktorý vydáva certifikácie, má okrem toho úlohu pravidelne ich preskúmavať [článok 57 ods. 1 písm. o)] a právomoc ich odňať, ak požiadavky na certifikáciu nie sú, resp. už nie sú splnené [článok 58 ods. 2 písm. h)]. V záujme splnenia týchto požiadaviek je vhodné stanoviť postup certifikácie a procesné požiadavky, a ak nie je stanovené inak, napr. vo vnútroštátnych právnych predpisoch, uzavrieť právne vymáhateľnú dohodu o poskytovaní certifikačných činností s konkrétnou žiadateľskou organizáciou. Malo by sa zabezpečiť, že na základe tejto certifikačnej dohody je žiadateľ povinný dodržiavať aspoň kritéria certifikácie, ktoré zahŕňajú nevyhnutné opatrenia na výkon vyhodnotenia, monitorovanie dodržiavania kritérií a pravidelné preskúmavanie vrátane prístupu k informáciám a/alebo do priestorov, dokumentovania a zverejňovania správ a výsledkov, a vyšetrovania sťažností. Okrem toho sa predpokladá, že dozorný orgán bude popri požiadavkách podľa článku 43 ods. 2 dodržiavať aj požiadavky stanovené v usmerneniach o akreditácii certifikačných subjektov.

2.2 Ďalšie úlohy dozorného orgánu v súvislosti s certifikáciou

24. V členských štátoch, v ktorých začnú pôsobiť certifikačné subjekty, má dozorný orgán, bez ohľadu na vlastné činnosti, tieto právomoci a úlohy:

    - posúdiť kritériá certifikačnej schémy a vypracovať návrh rozhodnutia (článok 42 ods. 5),
    - oznámiť Výboru návrh rozhodnutia, keď má v úmysle schváliť kritériá certifikácie [článok 64 ods. 1 písm. c), článok 64 ods. 7] a zohľadniť stanovisko Výboru [článok 64 ods. 1 písm. c) a článok 70 ods. 1 písm. t)],
    - schváliť kritériá certifikácie [článok 58 ods. 3 písm. f)] ešte pred akreditáciou a certifikáciou [článok 42 ods. 5 a článok 43 ods. 2 písm. b)],
    - zverejniť kritériá certifikácie [článok 43 ods. 6],
    - fungovať ako príslušný orgán pre celoúnijné certifikačné schémy, ktoré môžu viesť k schváleniu európskych pečatí ochrany údajov EDPB [článok 42 ods. 5 a článok 70 ods. 1 písm. o)] a
    - nariadiť certifikačnému subjektu, aby a) nevydal certifikáciu alebo b) odňal certifikáciu, ak nie sú splnené, resp. už nie sú splnené, požiadavky na certifikáciu (certifikačné postupy alebo kritériá certifikácie) [článok 58 ods. 2 písm. h)].

25. Všeobecné nariadenie o ochrane údajov ukladá dozornému orgánu úlohu schvaľovať kritériá certifikácie, ale nie ich vypracúvať. V záujme schválenia kritérií certifikácie podľa článku 42 ods. 5 by mal mať dozorný orgán jasnú predstavu o tom, čo možno očakávať, najmä pokiaľ ide

o rozsah a obsah preukázania súladu so všeobecným nariadením o ochrane údajov a so zreteľom na svoju úlohu monitorovať a presadzovať uplatňovanie nariadenia. V prílohe sa uvádza usmernenie na zabezpečenie harmonizovaného prístupu pri posudzovaní kritérií na účely schválenia.

26. V článku 43 ods. 1 sa vyžaduje, aby certifikačné subjekty pred vydaním alebo obnovením certifikácie informovali svoj dozorný orgán a umožnili mu tak výkon jeho nápravných právomocí podľa článku 58 ods. 2 písm. h). V článku 43 ods. 5 sa okrem toho vyžaduje, aby certifikačné subjekty informovali príslušný dozorný orgán o dôvodoch udelenia alebo odňatia požadovanej certifikácie. Hoci dozorné orgány môžu podľa všeobecného nariadenia o ochrane údajov určiť, ako tieto informácie operatívne získať, potvrdiť, preskúmať a ako s nimi nakladať (to by napríklad mohlo zahŕňať technologické riešenia, ktoré by umožňovali podávanie správ certifikačnými subjektmi), možno zaviesť postup a kritériá spracúvania informácií a správ o každom úspešnom projekte certifikácie realizovanom certifikačným subjektom podľa článku 43 ods. 1. Dozorný orgán môže na základe týchto informácií uplatniť svoju právomoc nariadiť certifikačnému subjektu, aby certifikáciu odňal alebo nevydal [článok 58 ods. 2 písm. h)] a aby monitoroval a presadzoval uplatňovanie požiadaviek na certifikáciu a kritérií certifikácie podľa všeobecného nariadenia o ochrane údajov [článok 57 ods. 1 písm. a) a článok 58 ods. 2 písm. h)]. Tým sa podporí harmonizovaný prístup a porovnateľnosť pri certifikácii rôznymi certifikačnými subjektmi a zaistí sa, aby dozorné orgány mali informácie o stave certifikácie danej organizácie.

3 ÚLOHA CERTIFIKAČNÉHO SUBJEKTU

27. Úlohou certifikačného subjektu je vydávať, preskúmavať, obnovovať a odnímať certifikácie (článok 42 ods. 5 a ods. 7) na základe certifikačného mechanizmu a schválených kritérií (článok 43 ods. 1). Na to je potrebné, aby certifikačný subjekt alebo vlastník certifikačnej schémy stanovil kritériá a postupy certifikácie vrátane postupov monitorovania dodržiavania, preskúmavania, vybavovania sťažností a odnímania. Kritériá certifikácie sa preskúmavajú v rámci procesu akreditácie, pri ktorom sa berú do úvahy pravidlá a postupy, na základe ktorých sa vydávajú certifikácie, pečate alebo značky [článok 43 ods. 2 písm. c)].

28. Na to, aby certifikačný subjekt získal akreditáciu podľa článku 43, je potrebný certifikačný mechanizmus a kritériá certifikácie. Na činnosť certifikačného subjektu má významný vplyv rozsah kritérií certifikácie a ich druh, ktoré zasa majú vplyv na postupy certifikácie a naopak. Špecifické kritériá si môžu napríklad vyžadovať osobitné metódy vyhodnotenia, ako sú kontroly na mieste a preskúmanie kódexu. Tieto postupy sú na účely akreditácie povinné a podrobnejšie sa vysvetľujú v usmerneniach k akreditácii.

29. Certifikačný subjekt je podľa všeobecného nariadenia o ochrane údajov povinný poskytovať dozorným orgánom informácie, a to najmä informácie o jednotlivých certifikáciách, ktoré sú potrebné na monitorovanie uplatňovania certifikačného mechanizmu [článok 42 ods. 7, článok 43 ods. 5, článok 58 ods. 2 písm. h)].

4 SCHVAĽOVANIE KRITÉRIÍ CERTIFIKÁCIE

30. Neoddeliteľnou súčasťou každého certifikačného mechanizmu sú kritériá certifikácie. Vo všeobecnom nariadení o ochrane údajov sa preto vyžaduje, aby kritériá certifikácie certifikačného mechanizmu schválil príslušný dozorný orgán [článok 42 ods. 5 a článok 43 ods. 2 písm. b)]. V prípade európskej pečate ochrany údajov schvaľuje kritériá certifikácie EDPB [článok 42 ods. 5 a článok 70 ods. 1 písm. o)]. Oba postupy schvaľovania kritérií certifikácie sú vysvetlené ďalej.

31. Podľa EDPB možno kritériá certifikácie schváliť na tieto účely:

    - náležite zohľadniť požiadavky a zásady týkajúce sa ochrany fyzických osôb so zreteľom na spracúvanie osobných údajov stanovené v nariadení (EÚ) 2016/679 a
    - prispievať k jednotnému uplatňovaniu všeobecného nariadenia o ochrane údajov.

32. Schválenie sa udeľuje na základe toho, že v kritériách certifikácie sa plne odráža požiadavka stanovená vo všeobecnom nariadení o ochrane údajov, podľa ktorej musí certifikačný mechanizmus umožňovať prevádzkovateľom a sprostredkovateľom, aby preukázali súlad so všeobecným nariadením o ochrane údajov.

4.1 Schválenie kritérií príslušným dozorným orgánom

33. Príslušný dozorný orgán musí kritériá certifikácie schváliť pred procesom akreditácie certifikačného subjektu alebo počas neho. Schválenie sa vyžaduje aj v prípade predloženia aktualizovaných alebo dodatočných schém alebo súborov kritérií podľa normy ISO 17065 tým istým certifikačným subjektom, pričom k nemu musí dôjsť pred použitím zmenených certifikačných mechanizmov [článok 42 ods. 5 a článok 43 ods. 2 písm. b)]. Dozorné orgány nakladajú so všetkými žiadosťami o schválenie kritérií certifikácie spravodlivým a nediskriminačným spôsobom, v súlade s verejne dostupným postupom špecifikujúcim všeobecné podmienky, ktoré treba splniť, a opis procesu schvaľovania.

34. Certifikačný subjekt môže vydávať certifikácie len v konkrétnom členskom štáte, a to v súlade s kritériami, ktoré schválil dozorný orgán v danom členskom štáte. Inými slovami, kritériá certifikácie musí schváliť dozorný orgán príslušný pre štát, v ktorom chce certifikačný subjekt ponúkať certifikáciu a v ktorom získa akreditáciu. Pre celoeurópske schémy certifikácie pozri nasledujúci oddiel.

4.2 Schválenie kritérií pre európsku pečať ochrany údajov EDPB

35. Certifikačný subjekt môže vydávať certifikácie aj v súlade s kritériami, ktoré v súvislosti s európskou pečaťou ochrany údajov schválil EDPB. Kritériá certifikácie schválené EDPB podľa článku 63 môžu viesť k európskej pečati ochrany údajov (článok 42 ods. 5). Vzhľadom na existujúce dohovory týkajúce sa certifikácie a akreditácie sa EDPB domnieva, že je žiaduce vyhnúť sa fragmentácii trhu v oblasti certifikácie ochrany údajov. Poukazuje na to, že podľa článku 42 ods. 1 majú členské štáty, dozorné orgány, Výbor a Komisia podporiť zavedenie certifikačných mechanizmov, a to predovšetkým na úrovni Únie.

4.2.1 Žiadosť o schválenie

36. Žiadosť o schválenie kritérií podľa článku 42 ods. 5 a článku 70 ods. 1 písm. o) EDPB sa musí predložiť prostredníctvom príslušného dozorného orgánu, pričom by sa v nej mal uvádzať zámer vlastníka schémy, záujemcu alebo akreditovaného certifikačného subjektu ponúkať kritériá v rámci certifikačného mechanizmu určeného prevádzkovateľom a sprostredkovateľom vo všetkých členských štátoch. Ak sa príslušný dozorný orgán domnieva, že EDPB by mohol kritériá schváliť, predloží mu návrh kritérií.

37. Výber miesta, kde sa predloží žiadosť o schválenie kritérií, bude závisieť od hlavného sídla vlastníkov certifikačnej schémy alebo certifikačných subjektov.

38. Pri predložení žiadosti by certifikačný subjekt mal obvykle byť v procese žiadania o akreditáciu alebo by mal byť už akreditovaný príslušným dozorným orgánom alebo národným akreditačným orgánom svojho členského štátu. K zjednodušeniu procesu schvaľovania môže prispieť, ak je už certifikačný subjekt akreditovaný v rámci certifikačného mechanizmu podľa všeobecného nariadenia o ochrane údajov.

4.2.2 Kritériá pre európsku pečať ochrany údajov

39. EDPB bude koordinovať proces posudzovania a prípadne schváli kritériá pre európsku pečať ochrany údajov. Posudzovanie bude zamerané napríklad na: rozsah pôsobnosti kritérií a ich vhodnosť na účely spoločnej certifikácie. Po schválení kritérií EDPB by mal sťažnosti na samotný mechanizmus vybavovať dozorný orgán príslušný pre hlavné sídlo certifikačného subjektu v EÚ, ktorý by mal informovať ostatné dozorné orgány. Daný dozorný orgán má zároveň právomoc prijímať opatrenia proti certifikačnému subjektu. Príslušný dozorný orgán bude v relevantných prípadoch informovať ostatné dozorné orgány a EDPB.

40. Na kritériá certifikácie na účely spoločnej certifikácie sa vzťahujú požiadavky z celej EÚ a na riešenie týchto požiadaviek by mali ponúkať osobitný mechanizmus. Európske certifikačné mechanizmy musia byť určené na použitie vo všetkých členských štátoch. Na základe článku 42 ods. 5 by sa mal dať mechanizmus pre európsku pečať ochrany údajov, ako aj jeho kritériá prispôsobiť tak, aby bolo v príslušných prípadoch možné zohľadniť vnútroštátne odvetvové predpisy, napríklad o spracúvaní údajov v školách, a malo by sa pri ňom predpokladať uplatňovanie v celej EÚ.

41. Príklad: Medzinárodná škola, ktorá ponúka vzdelávanie dotknutým osobám v Únii, má sídlo v členskom štáte „A“. Škola by chcela certifikovať svoj proces podávania online prihlášok na základe celoúnijnej certifikačnej schémy, aby získala európsku pečať ochrany údajov. Má v úmysle požiadať o certifikáciu spracovateľských operácií, ktorú na základe európskej pečate ochrany údajov ponúka certifikačný subjekt v členskom štáte „B“. V rámci kritérií pečate, navrhnutých a zdokumentovaných v príslušnom mechanizme, musí byť možné zohľadniť predpisy pre školy platné v členskom štáte „A“. V kritériách by sa zároveň malo požadovať, aby sa v procese podávania online prihlášok danej školy uvádzali informácie o požiadavkách na ochranu údajov platných v danom členskom štáte, ktoré sa môžu v iných členských štátoch líšiť, a aby sa tieto požiadavky zohľadňovali. Ako príklad možno uviesť súbory osobných údajov, ktoré treba predložiť na účely žiadosti, napr. hodnotenie alebo výsledky testov z materskej

školy, rôzne obdobia uchovávania, zber alebo spracúvanie finančných či biometrických údajov, ďalšie obmedzenia spracúvania.

- Medzi kritériá vysokej úrovne pre schválenie mechanizmu európskej pečate ochrany údajov patria:
  - kritériá schválené Výborom,
  - uplatňovanie kritérií v rôznych jurisdikciách, v rámci čoho sa v prípade potreby zohľadňujú vnútroštátne právne požiadavky a odvetvové predpisy,
- harmonizované kritériá, ktoré sa dajú prispôsobiť tak, aby odrážali vnútroštátne požiadavky,
  - opis špecifikácie certifikačného mechanizmu,
  - dohody o vydávaní certifikácie, v ktorých sa uznávajú celoeurópske požiadavky,
  - postupy na zabezpečenie a poskytovanie riešení v prípade rozdielov medzi požiadavkami v jednotlivých členských štátoch a na zabezpečenie toho, aby pečať prispela k preukázaniu súladu s ustanoveniami všeobecného nariadenia o ochrane údajov a
  - jazyk správ určených všetkým dotknutým dozorným orgánom.

42. Odporúčania v súvislosti s kritériami pre európsku pečať ochrany údajov sú uvedené aj v prílohe.

4.2.3 Úloha akreditácie

43. Ako sa uvádza v bode 4.2.1, keď sú kritériá označené ako vhodné na účely spoločnej certifikácie a boli ako také schválené Výborom podľa článku 42 ods. 5, potom môžu byť certifikačné subjekty akreditované na vykonávanie certifikácie na základe týchto kritérií na úrovni Únie.

44. Schémy, ktoré sa majú ponúkať len v jednotlivých členských štátoch, sa nemôžu uchádzať o udelenie pečatí EÚ. Pre akreditáciu v rozsahu predmetu európskej pečate ochrany údajov bude potrebná akreditácia v členskom štáte, v ktorom má hlavné sídlo certifikačný subjekt zamýšľajúci schému prevádzkovať, t. j. subjekt zodpovedný za vydávanie certifikácií a riadenie certifikačných činností svojich subjektov a dcérskych spoločností v ostatných členských štátoch. Ak iné pobočky alebo zložky zabezpečujú a vykonávajú certifikácie samostatne, každá z nich bude musieť byť samostatne akreditovaná v členskom štáte, v ktorom má sídlo. Inými slovami, ak certifikáty vydáva iba hlavné sídlo certifikačného subjektu, akreditácia je potrebná iba v členskom štáte, v ktorom sa toto hlavné sídlo nachádza. Naopak, ak certifikáty vydávajú aj iné pobočky certifikačného subjektu, musia byť akreditované aj tieto pobočky.

45. Teda, ak certifikačný subjekt nebol akreditovaný na účely vydávania certifikátov na základe európskej pečate ochrany údajov, nie je možné používať kritériá schválené EDPB a ponúkať pečať.

5 VYPRACOVANIE KRITÉRIÍ CERTIFIKÁCIE

46. Všeobecným nariadením o ochrane údajov sa zaviedol rámec pre vypracovanie kritérií certifikácie. Keďže základné požiadavky týkajúce sa postupu certifikácie sa uvádzajú v článkoch 42 a 43, ktoré zároveň stanovujú základné kritériá certifikačných postupov, základ pre kritériá certifikácie musí vychádzať zo zásad a pravidiel všeobecného nariadenia o ochrane údajov a musí pomôcť zabezpečiť, že sú tieto zásady a pravidlá splnené.

47. Pri vypracovávaní kritérií certifikácie sa treba zamerať na overiteľnosť, význam a vhodnosť kritérií certifikácie vzhľadom na preukázanie súladu s nariadením. Kritériá certifikácie by mali byť formulované tak, aby boli jasné a zrozumiteľné a aby umožňovali uplatňovanie v praxi.

48. Pri navrhovaní kritérií certifikácie sa na podporu posúdenia spracovateľskej operácie prípadne zohľadnia aj tieto aspekty súladu:

    - zákonnosť spracúvania podľa článku 6,
    - zásady spracúvania údajov podľa článku 5,
    - práva dotknutých osôb podľa článkov 12 až 23,
    - povinnosť oznamovať porušenia ochrany údajov podľa článku 33,
    - povinnosť špecificky navrhnutej a štandardnej ochrany údajov podľa článku 25,
    - skutočnosť, či sa vykonalo posúdenie vplyvu na ochranu údajov podľa článku 35 ods. 7 písm. d), ak je to relevantné a
    - technické a organizačné opatrenia zavedené podľa článku 32.

49. Rozsah, v akom sa tieto aspekty odrážajú v kritériách, sa môže líšiť v závislosti od predmetu certifikácie, ktorý môže zahŕňať druh spracovateľskej operácie, resp. spracovateľských operácií a oblasť certifikácie (napr. sektor zdravotníctva).

5.1 Čo možno certifikovať podľa všeobecného nariadenia o ochrane údajov?

50. EDPB sa domnieva, že vo všeobecnom nariadení o ochrane údajov sa stanovuje široký predmet toho, čo možno podľa neho certifikovať, pokiaľ sa dôraz kladie na to, že to pomáha preukazovať súlad spracovateľských operácií prevádzkovateľov a sprostredkovateľov s týmto nariadením (článok 42 ods. 1).

51. Pri posudzovaní spracovateľskej operácie sa v príslušných prípadoch musia zohľadniť tieto tri hlavné zložky:

    1. osobné údaje (vecná pôsobnosť všeobecného nariadenia o ochrane údajov),
    2. technické systémy – infraštruktúra, ako napríklad hardvér a softvér – používaná na spracúvanie osobných údajov a

3. procesy a postupy týkajúce sa spracovateľskej operácie, resp. spracovateľských operácií.

52. Každá zložka použitá pri spracovateľských operáciách sa musí posúdiť na základe stanovených kritérií. Vplyv na to môžu mať najmenej štyri rôzne významné faktory: 1. organizácia a právna štruktúra prevádzkovateľa alebo sprostredkovateľa; 2. útvar, prostredie a osoby zapojené do spracovateľskej operácie, resp. spracovateľských operácií; 3. technický opis prvkov, ktoré sa majú posúdiť a napokon 4. IT infraštruktúra na podporu spracovateľskej operácie vrátane operačných systémov, virtuálnych systémov, databáz, autentifikačných a autorizačných systémov, routerov a firewallov, systémov uchovávania, komunikačnej infraštruktúry alebo prístupu na internet a súvisiace technické opatrenia.

53. Pre koncipovanie certifikačných postupov a kritérií certifikácie sú relevantné všetky tri hlavné zložky. Rozsah, v akom sa zohľadňujú, sa môže líšiť v závislosti od predmetu certifikácie. V niektorých prípadoch sa napríklad nemusí na niektoré zložky prihliadať, ak sa nepovažujú za relevantné vzhľadom na predmet certifikácie.

54. V záujme ďalšieho spresnenia toho, čo môže byť certifikované podľa všeobecného nariadenia o ochrane údajov, sa v ňom uvádzajú ďalšie usmernenia. Z článku 42 ods. 7 vyplýva, že certifikácie podľa všeobecného nariadenia o ochrane údajov sa vydávajú len prevádzkovateľom a sprostredkovateľom, čo vylučuje napríklad certifikáciu zodpovedných osôb. Článok 43 ods. 1 písm. b) odkazuje na normu ISO 17065, v ktorej sa stanovuje akreditácia certifikačných subjektov posudzujúcich zhodu výrobkov, služieb a procesov. Spracovateľská operácia alebo súbor operácií môže viesť v terminológii normy ISO 17065 k produktu alebo službe a ako taká môže byť predmetom certifikácie. Napríklad spracúvanie údajov zamestnancov na účely vyplácania mzdy alebo spravovania dovoleniek predstavuje v zmysle všeobecného nariadenia o ochrane údajov súbor operácií a v terminológii ISO môže viesť k produktu, procesu alebo službe.

55. Na základe týchto skutočností sa EDPB domnieva, že predmet certifikácie podľa všeobecného nariadenia o ochrane údajov je zameraný na spracovateľské operácie alebo súbory operácií. Tie môžu zahŕňať procesy riadenia v zmysle organizačných opatrení, teda ako neoddeliteľné súčasti spracovateľskej operácie (napr. riadiaci proces vytvorený na vybavovanie sťažností v rámci spracúvania údajov o zamestnancoch na účely vyplácania mzdy).

56. V záujme posúdenia súladu spracovateľskej operácie s kritériami certifikácie sa musí uviesť, v akom prípade sa bude používať. Napríklad súlad používania technickej infraštruktúry využívanej pri spracovateľskej operácii závisí od kategórií údajov, ktoré sa s jej pomocou majú spracúvať. Organizačné opatrenia závisia od kategórií údajov a ich objemu, ako aj od technickej infraštruktúry používanej na spracúvanie, pričom sa zohľadňuje povaha, rozsah, obsah a účely spracúvania, ako aj riziká z hľadiska práv a slobôd dotknutých osôb.

57. Okrem toho treba mať na pamäti, že medzi aplikáciami informačných technológií môžu byť veľké rozdiely, aj keď slúžia na rovnaké účely spracúvania. Túto skutočnosť je preto potrebné zohľadniť pri vymedzovaní rozsahu predmetu certifikačných mechanizmov *[scope of the certification mechanisms]* a navrhovaní kritérií certifikácie, t. j. predmetu certifikácie a kritériá by nemali byť natoľko úzke, aby z nich boli vylúčené aplikácie IT, ktoré sú poňaté inak.

5.2 Určenie predmetu certifikácie

58. Treba rozlišovať medzi rozsahom predmetu certifikačného mechanizmu a predmetom jednotlivých projektov certifikácie v rámci certifikačného mechanizmu, ktorý sa označuje aj ako cieľ hodnotenia (ToE) *[target of evaluation].* Rozsah predmetu certifikačného mechanizmu môže byť vymedzený všeobecne alebo vo vzťahu k osobitnému druhu či oblasti spracovateľských operácií, a teda môže už naznačovať, aké predmety certifikácie spadajú do rozsahu predmetu certifikačného mechanizmu (napr. bezpečné uchovávanie a ochrana osobných údajov obsiahnutých v digitálnom trezore). Spoľahlivé posúdenie zhody, ktoré má určitú výpovednú hodnotu, je v každom prípade možné uskutočniť len vtedy, keď sa presne vymedzí konkrétny predmet projektu certifikácie. Musí sa jasne opísať, ktoré spracovateľské operácie sú zahrnuté do predmetu certifikácie, ako aj ktoré hlavné zložky, t. j. ktoré údaje, procesy a technická infraštruktúra sa budú posudzovať a ktoré sa posudzovať nebudú. Pritom treba vždy brať do úvahy a opísať rozhrania s ďalšími procesmi. Samozrejme, čo nie je známe, nemôže byť súčasťou posúdenia, a teda nemôže byť certifikované. Konkrétny predmet certifikácie musí mať v každom prípade výpovednú hodnotu, pokiaľ ide o posolstvo alebo tvrdenie vyplývajúce z certifikácie, a nemal by používateľa, zákazníka alebo spotrebiteľa uvádzať do omylu.

59. (Príklad 1)

Banka ponúka svojim zákazníkom webové sídlo na účely internetového bankovníctva. V rámci tejto služby je možné uskutočňovať prevody, nakupovať akcie, vytvárať trvalé príkazy a spravovať účet. Banka chce na základe certifikačného mechanizmu v oblasti ochrany osobných údajov so všeobecným rozsahom predmetu, založenom na všeobecných kritériách certifikovať nasledovné:

a) Zabezpečené prihlásenie

Zabezpečené prihlásenie je spracovateľská operácia, ktorá je pre koncového používateľa zrozumiteľná a ktorá je relevantná z hľadiska ochrany údajov, keďže zohráva dôležitú úlohu pri zaistení bezpečnosti súvisiacich osobných údajov. Táto spracovateľská operácia je preto potrebná na zabezpečené prihlásenie, a teda môže predstavovať cieľ hodnotenia (ToE) s určitou výpovednou hodnotou, ak sa v certifikáte jasne uvádza, že je certifikovaná len spracovateľská operácia prihlásenia.

b) Web front-end

„Web front-end“ môže byť síce relevantný z hľadiska ochrany údajov, ale pre koncového používateľa nie je zrozumiteľný, a preto nemá ako cieľ hodnotenia (ToE) výpovednú hodnotu. Používateľovi navyše nie je jasné, na ktoré služby na webovom sídle, a teda na ktoré spracovateľské operácie sa certifikácia vzťahuje.

c) Internetbanking

„Web front-end“ a „back-end“ sú spracovateľské operácie zabezpečované v rámci služby internetbankingu, čo môže mať pre používateľa určitú výpovednú hodnotu. V tejto súvislosti musia byť obe zahrnuté do cieľa hodnotenia (ToE). Na druhej strane, spracovateľské operácie, ktoré nie sú priamo spojené s poskytovaním služby

internetbankingu, ako sú spracovateľské operácie na účely predchádzania praniu špinavých peňazí, netreba v rámci cieľa hodnotenia (ToE) uvádzať.

Služby internetbankingu, ktoré banka ponúka na svojom webovom sídle, však môžu zahŕňať aj ďalšie služby, ktoré si vyžadujú vlastné spracovateľské operácie. Medzi ďalšie služby môže v tejto súvislosti patriť napríklad ponúkanie poistného produktu. Keďže táto doplnková služba priamo nesúvisí s účelom poskytovania služieb internetbankingu, nemusí byť uvedená v rámci cieľa hodnotenia (ToE). Ak táto doplnková služba (poistenie) nie je v rámci cieľa hodnotenia (ToE) uvedená, rozhrania na túto službu, integrované vo webovom sídle, sú súčasťou cieľa hodnotenia (ToE), a preto ich v záujme rozlíšenia jednotlivých služieb treba opísať. Takýto opis je potrebný na identifikáciu a hodnotenie prípadných tokov údajov medzi týmito dvoma službami.

60. (Príklad 2)

Banka svojim zákazníkom ponúka službu, ktorá im umožňuje zlúčiť informácie týkajúce sa rôznych účtov a kreditných kariet od niekoľkých bánk (agregovanie účtov). Banka chce mať túto službu certifikovanú podľa všeobecného nariadenia o ochrane údajov. Príslušný dozorný orgán schválil osobitný súbor kritérií certifikácie zameraných na tento druh činnosti. Do rozsahu predmetu certifikačného mechanizmu patria iba tieto aspekty súladu:

- autentifikácia používateľa a
- prijateľné spôsoby získavania údajov, ktoré sa majú agregovať, od iných bánk/služieb.

Keďže cieľ hodnotenia (ToE) je v tomto prípade vymedzený samotným rozsahom predmetu tohto certifikačného mechanizmu, nie je ho možné v rámci navrhovaného rozsahu predmetu zmysluplne zúžiť a certifikovať len osobitné funkcie alebo len jednu spracovateľskú činnosť. V tomto scenári musí cieľ hodnotenia (ToE) zodpovedať konkrétnemu rozsahu predmetu.

5.3 Metódy vyhodnotenia a metodika posudzovania

61. V záujme posúdenia zhody, ktoré pomôže preukázať súlad spracovateľských operácií, treba určiť a stanoviť metódy vyhodnotenia a metodiku posudzovania. Pritom je dôležité, či sa informácie na účely posúdenia zhromažďujú iba z dokumentácie (čo samo osebe nepostačuje) alebo či sa informácie aktívne zhromažďujú na mieste, na základe priameho alebo nepriameho prístupu. Spôsob, akým sa informácie zhromažďujú, má vplyv na váhu certifikácie, a preto by sa mal vymedziť a opísať.

Postupy vydávania a pravidelného preskúmavania certifikácií by mali zahŕňať špecifikácie, na základe ktorých bude možné určiť úroveň vyhodnotenia (hĺbku a podrobnosť) vhodnú v záujme splnenia kritérií certifikácie, a mali by zahŕňať tieto položky:

- informácie o použitých metódach posudzovania a špecifikácie týchto metód, ako aj zistenia, ku ktorým sa dospelo, napr. počas auditov na mieste alebo na základe dokumentácie,

- metódy vyhodnotenia zamerané na spracovateľské operácie (údaje, systémy, procesy) a účel spracúvania,
- stanovenie kategórií údajov, potrieb, pokiaľ ide o ochranu, a informácie o tom, či sú zapojení sprostredkovatelia alebo tretie strany,
- určenie úloh a existenciu mechanizmu na kontrolu prístupu vymedzeného vo vzťahu k úlohám a povinnostiam.

62. Význam a hodnotu certifikácie ovplyvňuje aj hĺbka vyhodnotenia. Ak sa hĺbka vyhodnotenia z pragmatických dôvodov alebo v záujme ušetrenia nákladov zníži, váha certifikácie ochrany údajov klesne. Pri rozhodnutiach o miere podrobnosti vyhodnotenia môže na druhej strane dôjsť k presiahnutiu finančných možností žiadateľa a často aj schopností hodnotiteľov a audítorov. Na účely preukázania súladu nemusí byť vždy rozhodujúce vykonať analýzu používaných IT systémov detailne, aby si analýza zachovala svoj význam.

5.4 Dokumentovanie posudzovania

63. Certifikačná dokumentácia by mala byť podrobná a komplexná. Bez dokumentácie sa nedá uskutočniť náležité posúdenie. Základnou funkciou certifikačnej dokumentácie je, že zaisťuje transparentnosť procesu vyhodnotenia v rámci certifikačného mechanizmu. Dokumentácia poskytuje odpovede na otázky týkajúce sa požiadaviek stanovených právnymi predpismi. V rámci certifikačných mechanizmov by mala byť stanovená štandardizovaná metodika vypracovávania dokumentácie. Pri vyhodnotení tak následne bude možné porovnať certifikačnú dokumentáciu so skutočným stavom na mieste a s kritériami certifikácie.

64. Komplexná dokumentácia toho, čo sa certifikovalo a použitej metodiky, prispieva k transparentnosti. Podľa článku 43 ods. 2 písm. c) by sa mali v rámci certifikačných mechanizmov stanoviť postupy, ktoré umožnia preskúmanie certifikácií. Zrejme najvhodnejším prostriedkom komunikácie, ktorý umožní dozornému orgánu posúdiť, či možno certifikáciu pri formálnych vyšetrovaniach uznať a do akej miery, je podrobná dokumentácia. Dokumentácia vypracovaná počas vyhodnotenia by preto mala byť zameraná na tri hlavné aspekty:
    - konzistentnosť a súdržnosť uplatnených metód vyhodnotenia,
    - metódy vyhodnotenia slúžiace na preukázanie súladu predmetu certifikácie s kritériami certifikácie, a teda s nariadením a
    - že výsledky vyhodnotenia potvrdil nezávislý a nestranný certifikačný subjekt.

5.5 Dokumentovanie výsledkov

65. V odôvodnení 100 sa uvádzajú informácie o cieľoch sledovaných zavedením certifikácie.

„S cieľom zlepšiť transparentnosť a posilniť súlad s týmto nariadením by sa malo podporiť vytvorenie mechanizmov certifikácie a pečatí a značiek ochrany údajov, aby sa dotknutým osobám umožnilo rýchlo posúdiť úroveň ochrany údajov v prípade relevantných produktov a služieb.“

66. Pri zlepšovaní transparentnosti zohráva dôležitú úlohu dokumentácia a komunikácia výsledkov. Certifikačné subjekty, ktoré používajú certifikačné mechanizmy, pečate alebo značky určené dotknutým osobám (v role spotrebiteľov alebo zákazníkov), by mali poskytovať ľahko dostupné, zrozumiteľné a zmysluplné informácie o certifikovanej spracovateľskej operácii, resp. operáciách. Tieto verejné informácie by mali zahŕňať aspoň

    - opis cieľa hodnotenia (ToE),
    - odkaz na schválené kritériá, ktoré sa uplatnili pri danom cieli hodnotenia (ToE);
    - metodiku vyhodnotenia kritérií (vyhodnotenie na mieste, dokumentácia atď.) a
    - dobu platnosti certifikátu a
    - mali by dozorným orgánom a verejnosti umožňovať porovnanie výsledkov.

6 USMERNENIE K VYMEDZOVANIU KRITÉRIÍ CERTIFIKÁCIE

67. Kritériá certifikácie sú neoddeliteľnou súčasťou certifikačného mechanizmu. Certifikačný postup stanovuje požiadavky na to, ako sa má v jednotlivých projektoch certifikácie týkajúcich sa konkrétneho predmetu alebo cieľa hodnotenia (ToE) vykonávať posúdenie, kto ho má vykonávať, v akom rozsahu a na akej úrovni podrobnosti. Základnými požiadavkami, na základe ktorých sa posudzuje konkrétna spracovateľská operácia vymedzená v cieli hodnotenia (ToE), sú kritériá certifikácie. V týchto usmerneniach týkajúcich sa vymedzovania kritérií certifikácie sa uvádzajú všeobecné odporúčania, ktoré uľahčia posudzovanie kritérií certifikácie na účely schválenia.

    - Pri schvaľovaní alebo vymedzovaní kritérií certifikácie by sa mali zohľadniť ďalej uvedené všeobecné aspekty. Kritériá certifikácie by:
    - mali byť jednotné a overiteľné,
    - by mali byť preskúmateľné v rámci auditu v záujme umožnenia vyhodnotenia spracovateľských operácií podľa všeobecného nariadenia o ochrane údajov, a to najmä na základe stanovenia cieľov a plnenia usmernení na dosiahnutie týchto cieľov,
    - mali byť relevantné vzhľadom na cieľové publikum [napr. podniky (B2B) a koncových zákazníkov (B2C)],

- mali zohľadňovať ďalšie normy (napríklad normy ISO, vnútroštátne normy) a podľa potreby by s týmito normami mali byť interoperabilné a
- mali byť flexibilné a prispôsobiteľné, tak aby sa v súlade s článkom 42 ods. 1 a prístupom založeným na riziku podľa odôvodnenia 77 sa dali uplatniť na organizácie rôzneho druhu a veľkosti vrátane mikropodnikov, malých a stredných podnikov.

68. Malá miestna spoločnosť, napríklad maloobchodný predajca, bude spravidla vykonávať menej zložité spracovateľské operácie ako veľký nadnárodný prevádzkovateľ maloobchodných predajní. Hoci požiadavky na zákonnosť spracovateľských operácií zostávajú rovnaké, musí sa zohľadniť rozsah spracúvania údajov a jeho zložitosť; z toho vyplýva, že certifikačné mechanizmy a ich kritériá musí byť možné prispôsobiť v závislosti od príslušnej spracovateľskej činnosti.

6.1 Platné normy

69. Certifikačné subjekty budú musieť vziať do úvahy, ako sú v konkrétnych kritériách zohľadnené existujúce relevantné nástroje, ako sú kódexy správania, technické normy alebo vnútroštátne regulačné a právne iniciatívy. Kritériá budú v ideálnom prípade interoperabilné s existujúcimi normami, ktoré môžu prevádzkovateľovi alebo sprostredkovateľovi pomôcť pri plnení ich povinností podľa všeobecného nariadenia o ochrane údajov. Priemyselné normy sa však často zameriavajú na ochranu a bezpečnosť organizácie pred hrozbami, zatiaľ čo všeobecné nariadenie o ochrane údajov je zamerané na ochranu základných práv fyzických osôb. Toto odlišné hľadisko treba vziať do úvahy pri navrhovaní kritérií alebo schvaľovaní kritérií alebo certifikačných mechanizmov na základe priemyselných noriem.

6.2 Vymedzenie kritérií

70. Kritériá certifikácie musia zodpovedať certifikačnému vyhláseniu (správe alebo tvrdeniu) certifikačného mechanizmu alebo schémy, ako aj očakávaniam, ktoré z neho vyplývajú. Už samotný názov certifikačného mechanizmu môže určovať rozsah uplatňovania a bude mať dôsledky pre určenie kritérií.

71. (Príklad 3)

    Rozsah pôsobnosti mechanizmu s názvom „HealthPrivacyMark“ (značka potvrdzujúca ochranu súkromia v oblasti zdravotníctva) by mal byť obmedzený na sektor zdravotníctva. Na základe názvu pečate vzniká očakávanie, že boli preskúmané požiadavky na ochranu údajov vzťahujúce sa na údaje o zdravotnom stave. Kritériá tohto mechanizmu preto musia byť vhodné na posúdenie požiadaviek na ochranu údajov v tomto sektore.

72. (Príklad 4)

    V rámci mechanizmu, ktorý sa týka certifikácie spracovateľských operácií zahŕňajúcich systémy riadenia v oblasti spracúvania údajov, by mali byť určené kritériá, ktoré umožnia rozpoznanie a posudzovanie procesov riadenia a ich podporných technických a organizačných opatrení.

73. (Príklad 5)

    Kritériá pre mechanizmus, ktorý sa týka cloud computingu, musia zohľadňovať osobitné technické požiadavky potrebné na používanie služieb založených na cloude. Napríklad, ak sa používajú servery mimo EÚ, kritériá musia zohľadňovať podmienky stanovené v kapitole V *[prenosy osobných údajov do tretích krajín alebo medzinárodným organizáciám]* všeobecného nariadenia o ochrane údajov týkajúce sa prenosu údajov do tretích krajín.

74. Kritériá by mali byť koncipované tak, aby sa dali použiť pre rôzne ciele hodnotenia (ToE) v rôznych sektoroch a/alebo členských štátoch: umožňovať uplatnenie pri rôznych scenároch, umožňovať určenie vhodných opatrení pre spracovateľské operácie malého, stredného alebo veľkého rozsahu a zohľadňovať riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré ohrozujú práva a slobody fyzických osôb, v súlade so všeobecným nariadením o ochrane údajov. Certifikačné postupy (týkajúce sa napr. dokumentácie, testovania alebo metódy a hĺbky vyhodnotenia), ktoré tieto kritériá dopĺňajú, musia preto zodpovedať uvedeným potrebám a musia umožňovať a mať zavedené pravidlá, napríklad pre uplatňovanie príslušných kritérií v jednotlivých projektoch certifikácie. Kritériá musia uľahčovať posúdenie toho, či boli poskytnuté dostatočné záruky týkajúce sa vykonávania primeraných technických a organizačných opatrení.

6.3 Platnosť kritérií certifikácie

75. Aj keď sa na kritériá certifikácie musí dať určitý čas spoľahnúť, nemali by byť „vytesané do kameňa“. K ich revízii dôjde napríklad v prípadoch, keď:

    - došlo k zmene právneho rámca,
    - sa v rozsudkoch Európskeho súdneho dvora poskytne výklad príslušných podmienok a ustanovení, alebo
    - sa zmenil aktuálny stav vývoja techniky.

Za Európsky výbor pre ochranu údajov

predsedníčka

(Andrea Jelinek)

PRÍLOHA 1: ÚLOHY A PRÁVOMOCI DOZORNÝCH ORGÁNOV V SÚVISLOSTI S CERTIFIKÁCIOU PODĽA VŠEOBECNÉHO NARIADENIA O OCHRANE ÚDAJOV

	Ustanovenia	Požiadavky
Úlohy	Článok 43 ods. 6	Stanovuje, že dozorný orgán je povinný zverejniť kritériá uvedené v článku 42 ods. 5 v ľahko dostupnej forme a zaslať ich Výboru.
	Článok 57 ods. 1 písm. n)	Stanovuje, že dozorný orgán musí schváliť kritériá certifikácie podľa článku 42 ods. 5.
	Článok 57 ods. 1 písm. o)	Stanovuje, že dozorný orgán v relevantných prípadoch (t. j. ak vydáva certifikácie) uskutočňuje pravidelné preskúmanie certifikácií vydaných v súlade s článkom 42 ods. 7.
	Článok 64 ods. 1 písm. c)	Stanovuje, že dozorný orgán je povinný oznámiť Výboru návrh rozhodnutia, ak je zamerané na schválenie kritérií certifikácie uvedených v článku 42 ods. 5.
Právomoci	Článok 58 ods. 1 písm. c)	Stanovuje, že dozorný orgán má právomoc vykonávať preskúmania certifikácií vydaných podľa článku 42 ods. 7.
	Článok 58 ods. 2 písm. h)	Stanovuje, že dozorný orgán má právomoc odňať certifikáciu alebo nariadiť certifikačnému subjektu, aby odňal certifikáciu, alebo nariadiť certifikačnému subjektu, aby nevydal certifikáciu.
	Článok 58 ods. 3 písm. e).	Stanovuje, že dozorný orgán má právomoc akreditovať certifikačné subjekty.
	Článok 58 ods. 3 písm. f)	Stanovuje, že dozorný orgán má právomoc vydávať certifikácie a schvaľovať kritériá certifikácie.

PRÍLOHA 2

1 ÚVOD

V prílohe 2 sa uvádza usmernenie týkajúce sa preskúmania a posúdenia kritérií certifikácie podľa článku 42 ods. 5. Táto príloha stanovuje témy, ktoré dozorný orgán pre ochranu údajov a EDPB zvážia a uplatnia na účely schvaľovania kritérií certifikácie v rámci certifikačného mechanizmu. Certifikačné subjekty a vlastníci schém, ktorí chcú vypracovať kritériá a predložiť ich na schválenie, by mali vziať uvedené otázky do úvahy. Ich zoznam nie je úplný, zahŕňa však minimálne okruhy, ktoré treba zvážiť. Nie všetky otázky sa budú dať uplatniť; pri vypracúvaní kritérií by sa však mali zvážiť, pričom môže byť potrebné zdôvodniť, prečo sa kritériá nevzťahujú na konkrétne aspekty. Niektoré otázky sa opakujú, keďže sa týkajú rôznych hľadísk. Tieto usmernenia by sa mali zohľadniť v súlade s právnymi požiadavkami stanovenými vo všeobecnom nariadení o ochrane údajov a prípadne s požiadavkami vo vnútroštátnych právnych predpisoch.

2 PREDMET CERTIFIKAČNÉHO MECHANIZMU A CIEĽ HODNOTENIA (ToE)

a) Je rozsah predmetu certifikačného mechanizmu (pre ktorý sa majú dané kritériá ochrany údajov použiť) jasne opísaný?

b) Má rozsah predmetu certifikačného mechanizmu výpovednú hodnotu pre príslušnú cieľovú skupinu a nie je zavádzajúci?

- *Príklad: Pečať dôveryhodnej spoločnosti (Trusted Company Seal) naznačuje, že spracovateľské činnosti celej spoločnosti boli podrobené auditu, hoci predmetom certifikácie sú v skutočnosti len určené spracovateľské operácie, napr. online platobný proces. Rozsah predmetu je preto zavádzajúci.*

c) Odráža rozsah predmetu certifikačného mechanizmu všetky relevantné aspekty spracovateľských operácií?

- *Príklad: Aby značka ochrany súkromia v oblasti zdravotníctva (Privacy Health Mark) spĺňala požiadavky podľa článku 9, musí zahŕňať všetky hodnotené údaje týkajúce sa zdravia.*

d) Umožňuje rozsah predmetu certifikačného mechanizmu zmysluplnú certifikáciu ochrany údajov s prihliadnutím na povahu a obsah súvisiacich spracovateľských operácií, ako aj s nimi spojené riziko?

- *Príklad: Ak je rozsah predmetu certifikačného mechanizmu zameraný len na konkrétne aspekty spracovateľských operácií, ako je zber údajov, ale nie na ďalšie spracovateľské operácie, ako je spracúvanie v záujme vytvárania profilov na účely reklamy alebo správy práv dotknutých osôb, nebude pre dotknuté osoby zmysluplný.*

e) Vzťahuje sa rozsah predmetu certifikačného mechanizmu na spracúvanie osobných údajov v príslušnej krajine, kde sa žiadosť podáva, alebo sa týka cezhraničného spracúvania a/alebo prenosov?

f) Opisuje sa v kritériách certifikácie dostatočne, ako by mal byť vymedzený cieľ hodnotenia (ToE)?

- *Príklad: Pečať ochrany súkromia (Privacy Seal) so všeobecným rozsahom predmetu vyžadujúcim iba „špecifikáciu spracúvania, na ktoré sa vzťahuje certifikácia“ by neposkytovala dostatočne jasné usmernenie, ako stanoviť a opísať cieľ hodnotenia (ToE).*
- *Príklad: (Konkrétny) rozsah predmetu pečate potvrdzujúcej bezpečné uloženie osobných údajov v digitálnom trezore (The Privacy Vault Seal) by mal vo svojich kritériách podrobne opisovať požiadavky na splnenie tohto predmetu, napr. vymedzenie pojmu „trezor“, systémové požiadavky, povinné technické a organizačné opatrenia. V takom prípade sa dá cieľ* hodnotenia *(ToE) jednoznačne vymedziť v rámci rozsahu predmetu.*

    1. Vyžaduje sa v kritériách, aby cieľ hodnotenia (ToE) zahŕňal určenie všetkých relevantných spracovateľských operácií, znázornenie tokov údajov a určenie oblasti použitia cieľa hodnotenia (ToE)?
        - *Príklad: Certifikačný mechanizmus ponúka certifikáciu spracovateľských operácií prevádzkovateľov podľa všeobecného nariadenia o ochrane údajov bez bližšieho určenia oblasti použitia (všeobecný rozsah pôsobnosti). V kritériách používaných v rámci mechanizmu sa vyžaduje, aby žiadajúci prevádzkovateľ určil cieľovú spracovateľskú operáciu (cieľ hodnotenia (ToE)) z hľadiska typov údajov, použitých systémov a procesov.*
    2. Vyžaduje sa v kritériách, aby žiadateľ objasnil, kde spracúvanie, ktoré je predmetom vyhodnotenia, začína a kde končí? Vyžaduje sa v kritériách, aby cieľ hodnotenia (ToE) zahŕňal rozhrania, v prípade ktorých nie sú vzájomne závislé spracovateľské operácie zahrnuté do cieľa hodnotenia (ToE)? A je to dostatočne zdôvodnené?
        - *Príklad: Cieľ hodnotenia (ToE), v rámci ktorého sa dostatočne podrobne opisuje spracovateľská operácia webovej služby zahŕňa napríklad registrácia používateľov, poskytovanie služby, fakturácia, protokolovanie IP adries, rozhrania v smere k používateľom a tretím stranám, ale nie je v ňom zahrnutý hosting serverov (ale zahrnuté sú dohody o spracúvaní a dohody o technických a organizačných opatreniach).*

g) Zaručujú kritériá zrozumiteľnosť (jednotlivých) cieľov hodnotenia (ToEs) pre príslušnú cieľovú skupinu a prípadne aj pre dotknuté osoby?

3 VŠEOBECNÉ POŽIADAVKY

a) Sú všetky relevantné pojmy používané v katalógu kritérií (t. j. úplnom súbore kritérií certifikácie) určené, vysvetlené a opísané?

b) Sú uvedené všetky odkazy na normy?

c) Zahŕňajú kritériá vymedzenie zodpovedností, postupov a spracovateľských operácií v oblasti ochrany údajov, na ktoré sa vzťahuje rozsah predmetu certifikačného mechanizmu?

4 SPRACOVATEĽSKÁ OPERÁCIA, ČLÁNOK 42 ODS. 1

Pokiaľ ide o rozsah predmetu certifikačného mechanizmu (všeobecný alebo konkrétny), zohľadňujú kritériá všetky relevantné zložky spracovateľských operácií (údaje, systémy a procesy)?

a) Vyžaduje sa v kritériách, aby boli v súvislosti s cieľom hodnotenia (ToE) určené platné právne základy spracúvania?

b) Uznávajú sa v kritériách v súvislosti s cieľom hodnotenia (ToE) príslušné fázy spracúvania a celý životný cyklus údajov vrátane vymazania a/alebo anonymizácie?

c) Vyžaduje sa v kritériách v súvislosti s cieľom hodnotenia (ToE) prenosnosť údajov?

d) Umožňujú kritériá v súvislosti s cieľom hodnotenia (ToE), aby sa určili a zohľadnili osobitné druhy spracovateľských operácií, napr. automatizované rozhodovanie, profilovanie?

e) Umožňujú kritériá v súvislosti s cieľom hodnotenia (ToE), aby sa určili osobitné kategórie údajov?

f) Umožňujú kritériá posúdenie rizika spojeného s jednotlivými spracovateľskými operáciami a potrieb ochrany vo vzťahu k právam a slobodám dotknutých osôb a vyžaduje sa v nich toto posúdenie?

g) Umožňujú kritériá primerané zohľadnenie rizík pre práva a slobody fyzických osôb a vyžaduje sa v nich toto posúdenie?

…

5 ZÁKONNOSŤ SPRACÚVANIA

a) Vyžaduje sa v kritériách, aby sa v prípade jednotlivých spracovateľských operácií overila zákonnosť spracúvania, pokiaľ ide o jeho účel a nevyhnutnosť?

b) Vyžaduje sa v kritériách overenie všetkých požiadaviek stanovených v právnom základe pre jednotlivé spracovateľské operácie?

6 ZÁSADY, ČLÁNOK 5

a) Sú v rámci kritérií náležite zohľadnené všetky zásady ochrany údajov podľa článku 5?

b) Vyžaduje sa v kritériách preukázanie minimalizácie údajov pre jednotlivé ciele hodnotenia (ToE)?

…

7 VŠEOBECNÉ POVINNOSTI PREVÁDZKOVATEĽOV A SPROSTREDKOVATEĽOV

a) Vyžaduje sa v kritériách dôkaz o zmluvných dohodách medzi sprostredkovateľmi a prevádzkovateľmi?

b) Sú dohody medzi prevádzkovateľmi a sprostredkovateľmi predmetom vyhodnotenia?

c) Odrážajú kritériá povinnosti prevádzkovateľa podľa kapitoly IV?

d) Vyžaduje sa v kritériách dôkaz o preskúmaní a aktualizovaní technických a organizačných opatrení prijatých prevádzkovateľom podľa článku 24 ods. 1?

e) Overuje sa v rámci kritérií, či organizácia posúdila, či má byť určená zodpovedná osoba, ako sa to vyžaduje v článku 37? Ak je to relevantné, spĺňa zodpovedná osoba požiadavky podľa článkov 37 až 39?

f) Overuje sa v rámci kritérií, či sa požadujú záznamy o spracovateľských činnostiach v súlade s článkom 30 ods. 5 a či sú primerane splnené požiadavky stanovené v článku 30?

8 PRÁVA DOTKNUTÝCH OSÔB

a) Je v rámci kritérií náležite zohľadnené právo dotknutej osoby na informácie a vyžaduje sa zavedenie príslušných opatrení?

b) Vyžaduje sa v kritériách, aby bol dotknutým osobám poskytnutý primeraný alebo dokonca ešte väčší prístup k ich údajom a kontrola nad nimi vrátane prenosnosti údajov?

c) Vyžaduje sa v kritériách, aby sa zaviedli opatrenia zaisťujúce možnosť zasiahnuť do spracovateľskej operácie s cieľom zaručiť práva dotknutých osôb a umožniť opravu, vymazanie alebo obmedzenie?

…

9 RIZIKÁ PRE PRÁVA A SLOBODY FYZICKÝCH OSÔB

a) Umožňujú kritériá posúdenie rizika pre práva a slobody fyzických osôb a vyžaduje sa v nich toto posúdenie?

b) Stanovuje alebo vyžaduje sa v kritériách používanie uznávanej metodiky hodnotenia rizík? Ak áno, je primeraná?

c) Umožňujú kritériá posúdenie vplyvu plánovaných spracovateľských operácií na práva a slobody fyzických osôb a vyžaduje sa v nich toto posúdenie?

d) Vyžaduje sa v kritériách predchádzajúca konzultácia v súvislosti so zvyšnými rizikami, ktoré nebolo možné zmierniť, na základe výsledkov posúdenia vplyvu na ochranu údajov?

10 TECHNICKÉ A ORGANIZAČNÉ OPATRENIA ZARUČUJÚCE OCHRANU

a) Vyžaduje sa v kritériách uplatňovanie technických a organizačných opatrení, ktorými sa zaistí dôvernosť spracovateľských operácií?

b) Vyžaduje sa v kritériách uplatňovanie technických a organizačných opatrení, ktorými sa zaistí integrita spracovateľských operácií?

c) Vyžaduje sa v kritériách uplatňovanie technických a organizačných opatrení, ktorými sa zaistí dostupnosť spracovateľských operácií?

d) Vyžaduje sa v kritériách uplatňovanie opatrení, ktorými sa zaistí transparentnosť spracovateľských operácií, pokiaľ ide o

e) právnu zodpovednosť?

f) práva dotknutých osôb?

g) posúdenie jednotlivých spracovateľských operácií, napr. z hľadiska algoritmickej transparentnosti?

h) Vyžaduje sa v kritériách uplatňovanie technických a organizačných opatrení, ktorými sa zaručia práva dotknutých osôb, napr. schopnosť poskytovať informácie alebo prenosnosť údajov?

i) Vyžaduje sa v kritériách uplatňovanie technických a organizačných opatrení, ktorými sa zaistí možnosť zasiahnuť do spracovateľskej operácie s cieľom zaručiť právo dotknutých osôb a umožniť opravu, vymazanie alebo obmedzenie?

j) Vyžaduje sa v kritériách uplatňovanie opatrení, ktorými sa zaistí možnosť zasiahnuť do spracovateľskej operácie s cieľom opraviť alebo skontrolovať systém či proces?

k) Vyžaduje sa v kritériách uplatňovanie technických a organizačných opatrení, ktorými sa zaistí minimalizácia údajov, napríklad zrušenie prepojenia údajov s dotknutou osobou alebo oddelenie údajov od dotknutej osoby, anonymizácia alebo pseudonymizácia alebo izolácia dátových systémov?

l) Vyžadujú sa v kritériách technické opatrenia, ktorými sa zavedie štandardná ochrana údajov?

m) Vyžadujú sa v kritériách technické a organizačné opatrenia, ktorými sa zavedie špecificky navrhnutá ochrana údajov, napr. systém riadenia ochrany údajov na preukazovanie, oznamovanie, kontrolovanie a presadzovanie požiadaviek na ochranu údajov?

n) Vyžadujú sa v kritériách technické a organizačné opatrenia, ktorými sa zavedie primeraná pravidelná odborná príprava a vzdelávanie pracovníkov, ktorí majú stály alebo pravidelný prístup k osobným údajom?

o) Vyžaduje sa v kritériách preskúmanie opatrení?

p) Vyžaduje sa v kritériách vlastné hodnotenie/vnútorný audit?

q) Vyžaduje sa v kritériách opatrenie, ktorým sa zaistí, že povinnosti oznamovania prípadov porušenia ochrany osobných údajov sa budú plniť v primeranom čase a rozsahu?

r) Vyžaduje sa v kritériách, aby boli zavedené a overené postupy riadenia incidentov?

s) Vyžaduje sa v kritériách monitorovanie vývoja v oblasti ochrany súkromia a technológií a aktualizácia schémy v súlade s požiadavkami?

…

11 ĎALŠIE OSOBITNÉ PRVKY ZAISŤUJÚCE OCHRANU ÚDAJOV

a) Vyžaduje sa v kritériách zavedenie techník na zvýšenie ochrany údajov? To by mohlo zahŕňať kritériá, ktoré vyžadujú zvýšenú ochranu údajov odstránením alebo obmedzením osobných údajov a/alebo rizika spojeného s ochranou údajov.

- *Príklad: Techniku na zvýšenie ochrany údajov by napríklad predstavovali kritériá, v ktorých sa vyžaduje väčšia neprepojiteľnosť prostredníctvom využitia riadenia totožnosti zameraného na používateľa [user-centric identity management], ako sú napríklad prihlasovacie údaje založené na atribútoch (attribute-based credentials, ABC), namiesto riadenia totožnosti zameraného na organizáciu [organisation-centric identity management].*

b) Je na základe kritérií potrebné zaviesť rozšírené nástroje pre dotknuté osoby, ktoré im uľahčia slobodné rozhodovanie *[self-determination]* a výber?

…

12 KRITÉRIÁ NA ÚČELY PREUKÁZANIA EXISTENCIE PRIMERANÝCH ZÁRUK V PRÍPADE PRENOSU OSOBNÝCH ÚDAJOV

Kritériá sa budú riešiť v nadchádzajúcich usmerneniach k článku 42 ods. 2.

13 ĎALŠIE KRITÉRIÁ V SÚVISLOSTI S EURÓPSKOU PEČAŤOU OCHRANY ÚDAJOV

a) Predpokladá sa v kritériách pokrytie všetkých členských štátov?

b) Je možné v kritériách zohľadniť právne predpisy alebo scenáre jednotlivých členských štátov v oblasti ochrany údajov?

c) Vyžaduje sa v kritériách vyhodnotenie jednotlivých cieľov hodnotenia (ToE), pokiaľ ide o odvetvové právne predpisy členských štátov týkajúce sa ochrany údajov?

d) Vyžaduje sa v kritériách, aby prevádzkovateľ alebo sprostredkovateľ poskytovali dotknutým osobám a zainteresovaným stranám v jazykoch členských štátov

e) informácie o spracúvaní/cieli hodnotenia (ToE)?

f) dokumentáciu spracúvania/cieľa hodnotenia (ToE)?

g) výsledky vyhodnotenia?

…

14 CELKOVÉ VYHODNOTENIE KRITÉRIÍ

a) Pokrývajú kritériá celý rozsah predmetu certifikačného mechanizmu (t. j. ide o komplexné kritériá) a poskytujú tak dostatočné záruky, že je certifikácia dôveryhodná?

- *Príklad: Ak je rozsah predmetu certifikačného mechanizmu zameraný na operácie spracúvania údajov v oblasti zdravia, vysoká úroveň ochrany údajov by sa mala zaručiť stanovením kritérií, ktoré napríklad zabezpečia dôkladné posúdenie a uplatňovanie zásady ochrany súkromia už v štádiu návrhu [privacy-by-design] a zásady štandardnej ochrany súkromia [privacy-by-default].*

b) Sú kritériá primerané vzhľadom na rozsah spracovateľskej operácie, na ktorú sa vzťahuje rozsah predmetu certifikačného mechanizmu, citlivosť informácií a riziko spracúvania?

c) Je pravdepodobné, že kritériá zlepšia dodržiavanie predpisov v oblasti ochrany údajov zo strany prevádzkovateľov a sprostredkovateľov?

d) Bude to pre dotknuté osoby znamenať prínos, pokiaľ ide o ich práva na informácie vrátane vysvetlenia požadovaných výsledkov dotknutým osobám?