EVROPSKÁ
KOMISE

V Bruselu dne 24.6.2020
SWD(2020) 115 final

PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE

[…]

Průvodní dokument k

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ

Ochrana osobních údajů jakožto pilíř posílení postavení občanů a přístup EU k digitální transformaci – dva roky uplatňování obecného nařízení o ochraně údajů

{COM(2020) 264 final}

Obsah

1 SOUVISLOSTI

Obecné nařízení o ochraně osobních údajů[1] (dále jen „nařízení GDPR“) je výsledkem osm let trvajících příprav, návrhů a interinstitucionálních jednání a v účinnost vstoupilo dne 25. května 2018 po dvouletém přechodném období (květen 2016 – květen 2018). Článek 97 nařízení GDPR požaduje, aby Komise předložila zprávu o hodnocení a přezkumu tohoto nařízení, přičemž první zpráva má být předložena po dvou letech uplatňování a poté každé čtyři roky.

Hodnocení je rovněž součástí mnohostranného přístupu, který Komise uplatňovala již před vstupem nařízení GDPR v platnost a v jehož aktivním prosazování od té doby pokračuje. V rámci tohoto přístupu se Komise zapojila do probíhajících dvoustranných dialogů s členskými státy o souladu vnitrostátních právních předpisů s nařízením GDPR, aktivně přispěla k práci Evropského sboru pro ochranu osobních údajů (dále jen „sbor“) tím, že poskytovala své zkušenosti a odborné znalosti, podporovala úřady pro ochranu osobních údajů a udržovala úzké kontakty s širokou škálou zúčastněných stran ohledně uplatňování nařízení v praxi.

Hodnocení vychází z posouzení, které Komise provedla v prvním roce uplatňování nařízení GDPR a které bylo shrnuto ve sdělení vydaném v červenci 2019[2]. Navazuje rovněž na sdělení o uplatňování obecného nařízení o ochraně osobních údajů vydané v lednu 2018[3]. Komise rovněž přijala pokyny k používání osobních údajů ve volebním kontextu, které byly zveřejněny v září 2018, a pokyny k aplikacím na podporu boje proti pandemii COVID-19 vydané v dubnu 2020.

Navzdory svému důrazu na dvě otázky, na něž se upozorňuje v čl. 97 odst. 2 nařízení GDPR, konkrétně na otázku mezinárodního předávání údajů a otázku mechanismů spolupráce a jednotnosti, zaujímá toto hodnocení širší přístup, který se zabývá otázkami, které během posledních dvou let vznesli různí aktéři.

Při přípravě hodnocení vzala Komise v úvahu příspěvky:

- Rady[4],
- Evropského parlamentu (Výboru pro občanské svobody, spravedlnost a vnitřní věci)[5],
- sboru[6] a jednotlivých úřadů pro ochranu osobních údajů[7] na základě dotazníku zaslaného Komisí,

---

[1] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Úř. věst. L 119, 4.5.2016, s. 1).

[2] Sdělení Komise Evropskému parlamentu a Radě – Pravidla pro ochranu údajů zprostředkující důvěru v EU i za jejími hranicemi – vyhodnocení – COM (2019) 374 final, 24. 7. 2019.

[3] Sdělení komise Evropskému parlamentu a Radě s názvem „Posílená ochrana, nové příležitosti – pokyny Komise týkající se přímého uplatňování obecného nařízení o ochraně osobních údajů ke dni 25. května 2018“, COM(2018) 43 final.

[4] Postoj Rady a zjištění ohledně uplatňování obecného nařízení o ochraně osobních údajů – 14994/2/19 Rev2, 15. 1. 2020: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/cs/pdf.

[5] Dopis Výboru Evropského parlamentu pro občanské svobody, spravedlnost a vnitřní věci (LIBE) ze dne 21. února 2020 adresovaný komisaři Reyndersovi, č.j.: IPOL-COM-LIBE D (2020)6525.

- zpětnou vazbu od členů expertní skupiny více zúčastněných stran na podporu uplatňování nařízení GDPR[8], a to rovněž na základě dotazníku zaslaného Komisí,
- a příspěvky ad hoc obdržené od zúčastněných stran.

2 PROSAZOVÁNÍ NAŘÍZENÍ GDPR A FUNGOVÁNÍ MECHANISMŮ SPOLUPRÁCE A JEDNOTNOSTI

Nařízení GDPR zavedlo inovativní systém řízení a vytvořilo základy skutečně evropské kultury ochrany osobních údajů, jejímž cílem je zajistit nejen harmonizovaný výklad, ale také harmonizované uplatňování a prosazování pravidel ochrany osobních údajů. Jejími pilíři jsou nezávislé vnitrostátní úřady pro ochranu osobních údajů a nově zřízený sbor.

Jelikož úřady pro ochranu osobních údajů mají zásadní význam pro fungování celého systému EU pro ochranu osobních údajů, Komise pozorně sleduje jejich skutečnou nezávislost, a to i z hlediska vhodných finančních, lidských a technických zdrojů.

Vzhledem k dosavadním malým zkušenostem je ještě příliš brzy na plné posouzení fungování mechanismů spolupráce a jednotnosti[9]. Úřady pro ochranu osobních údajů navíc k dalšímu prohloubení své spolupráce dosud nevyužívají celou řadu nástrojů, které jsou stanoveny v nařízení GDPR.

2.1 Využití posílených pravomocí úřady pro ochranu osobních údajů

Nařízení GDPR zřizuje nezávislé úřady pro ochranu osobních údajů a dává jim harmonizované a posílené donucovací pravomoci. Vzhledem k tomu, že se uplatňuje nařízení GDPR, používají tyto úřady širokou škálu nápravných pravomocí stanovených v nařízení GDPR, jako jsou správní pokuty (22 úřadů v EU/EHP)[10], upozornění a napomenutí (23), nařízení k vyhovění žádostem subjektu údajů (26), nařízení k uvedení operací zpracování do souladu s nařízením GDPR (27) a nařízení opravy či výmazu osobních údajů nebo omezení zpracování (17). Přibližně polovina úřadů pro ochranu osobních údajů (13) již uložila dočasná či trvalá omezení zpracování, včetně zákazů. To prokazuje vědomé používání všech nápravných opatření stanovených v nařízení GDPR; úřady pro ochranu osobních údajů se

---

[6] Příspěvek sboru k hodnocení nařízení GDPR podle článku 97 přijatý dne 18. února 2020: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en.

[7] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en.

[8] Expertní skupina více zúčastněných stran pro nařízení GDPR zřízená Komisí zahrnuje zástupce občanské společnosti a komerční sféry, akademickou obec a odborníky z praxe: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537 Zpráva expertní skupiny více zúčastněných stran je k dispozici na adrese: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=21356.

[9] Tuto skutečnost rovněž zdůrazňuje zejména Rada ve svém postoji a zjištěních týkajících se uplatňování nařízení GDPR a sbor ve svém příspěvku k hodnocení.

[10] V závorkách se uvádí počet úřadů pro ochranu osobních údajů v EU/EHP, které uvedenou pravomoc uplatnily v období od května 2018 do konce listopadu 2019. Viz příspěvek sboru na stranách 32–33.

nezdráhají ukládat správní pokuty vedle nebo namísto jiných nápravných opatření v závislosti na okolnostech jednotlivých případů.

Správní pokuty:

V období od 25. května 2018 do 30. listopadu 2019 uložilo 22 úřadů pro ochranu osobních údajů v EU/EHP přibližně 785 pokut. Žádné správní pokuty dosud neuložilo pouze několik úřadů, ačkoli k uložení takových pokut by mohla vést řízení, která v současné době probíhají. Většina pokut se týkala porušení: zásady zákonnosti, platného souhlasu, ochrany citlivých údajů, povinnosti týkající se transparentnosti, práv subjektů údajů, a případů porušení zabezpečení údajů.

Příklady pokut uložených úřady pro ochranu osobních údajů zahrnují[11]:

– 200 000 EUR z důvodu nedodržení práva vznést námitku proti přímému marketingu v Řecku,
– 220 000 EUR pro společnost z Polska zprostředkující informace za neinformování osob o tom, že jejich údaje se zpracovávají,
– 250 000 EUR pro španělskou fotbalovou ligu LaLiga za nedostatečně transparentní design aplikace pro chytré telefony,
– 14,5 milionu EUR za porušení zásad ochrany osobních údajů, zejména za nezákonné uchovávání, německou realitní společností,
– 18 milionů EUR za nezákonné zpracování zvláštních kategorií údajů ve velkém měřítku rakouskými poštovními službami,
– 50 milionů EUR pro společnost Google ve Francii za podmínky pro získávání souhlasu uživatelů.

Úspěch nařízení GDPR by se neměl měřit počtem uložených pokut, neboť nařízení GDPR stanoví širší paletu nápravných pravomocí. V závislosti na okolnostech může být například mnohem silnější odrazující účinek zákazu zpracování nebo přerušení toků údajů.

Zvláštní záležitosti týkající se veřejného sektoru

Nařízení GDPR umožňuje členským státům určit, zda a v jakém rozsahu mohou být orgánům veřejné moci a veřejným subjektům ukládány správní pokuty. Pokud členské státy této možnosti využijí, nepřicházejí úřady pro ochranu osobních údajů o možnost využít všechny ostatní nápravné pravomoci ve vztahu k orgánům veřejné moci a veřejným subjektům[12].

Další zvláštní záležitostí je dozor nad soudy: ačkoli se nařízení GDPR vztahuje i na činnosti soudů, jsou soudy vyňaty z dozoru úřadů pro ochranu osobních údajů při výkonu soudních pravomocí. Listina a Smlouva o fungování EU (SFEU) však zavazují členské státy, aby v rámci svých justičních systémů pověřily dozorem nad takovými operacemi zpracování nezávislý subjekt[13].

---

[11] Stále probíhá soudní přezkum několika rozhodnutí o uložení pokut.
[12] Čl. 83 odst. 7 nařízení GDPR.
[13] Čl. 8 odst. 3 Listiny, čl. 16 odst. 2 SFEU, 20. bod odůvodnění nařízení GDPR.

Spolupráce s ostatními regulačními orgány

Jak bylo oznámeno ve sdělení z července 2019, Komise podporuje interakci s ostatními regulačními orgány a zároveň plně respektuje příslušné oblasti působnosti. Slibné oblasti spolupráce zahrnují ochranu spotřebitele a hospodářskou soutěž. Sbor projevil ochotu spolupracovat s ostatními regulačními orgány, zejména pokud jde o koncentraci na digitálních trzích[14]. Komise uznala význam ochrany soukromí a údajů jako kvalitativní parametr pro hospodářskou soutěž[15]. Členové sboru se zúčastnili společných seminářů se sítí pro spolupráci v oblasti ochrany spotřebitele, které se týkaly spolupráce při lepším prosazování právních předpisů EU v oblasti ochrany spotřebitele a ochrany osobních údajů. Tento přístup bude uplatňován s cílem podpořit společné porozumění a vypracovat praktické způsoby řešení konkrétních problémů, se kterými se spotřebitelé setkávají zejména v digitální ekonomice.

V zájmu zajištění jednotného přístupu k ochraně soukromí a údajů a do přijetí nařízení o soukromí a elektronických komunikacích je nezbytná úzká spolupráce s orgány příslušnými pro vymáhání směrnice o soukromí a elektronických komunikacích[16], tj. „lex specialis“ v oblasti elektronických komunikací. Užší spolupráce s příslušnými orgány podle směrnice o bezpečnosti sítí a informací[17] a skupinou pro spolupráci v oblasti bezpečnosti sítí a informací by byla k vzájemnému prospěchu těchto orgánů a úřadů pro ochranu osobních údajů.

2.2 Mechanismy spolupráce a jednotnosti

Nařízení GDPR vytvořilo mechanismus spolupráce (systém jednotného kontaktního místa pro provozovatele, společné operace a vzájemnou pomoc mezi úřady pro ochranu osobních údajů) a mechanismus jednotnosti s cílem podpořit jednotné uplatňování pravidel pro ochranu osobních údajů prostřednictvím jednotného výkladu a řešení případných neshod mezi úřady ze strany sboru.

Sbor, sdružující všechny úřady pro ochranu osobních údajů, byl zřízen jako subjekt EU s právní subjektivitou, je plně funkční a je podporován sekretariátem[18]. Je zásadní pro fungování obou výše uvedených mechanismů. Do konce roku 2019 přijal sbor 67 dokumentů včetně 10 nových pokynů[19] a 43 stanovisek[2021].

---

[14] Srov. prohlášení sboru o dopadech hospodářské koncentrace na ochranu údajů https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_cs.pdf.

[15] Viz věc COMP M. 8124 Microsoft/LinkedIn.

[16] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), (Úř. věst. L 201, 31.7.2002, s. 37).

[17] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

[18] Viz podrobnosti o činnostech sekretariátu v příspěvku sboru, s. 24–26.

[19] Navíc k deseti pokynům, které přijala pracovní skupina zřízená podle článku 29 před vstupem nařízení GDPR v platnost a které sbor schválil. Sbor kromě toho přijal v období od ledna do konce května 2020 čtyři další pokyny a aktualizoval stávající pokyny.

[20] Celkem 42 z těchto stanovisek bylo přijato podle článku 64 nařízení GDPR a jedno bylo přijato podle čl. 70 odst. 1 písm. s) nařízení GDPR a týkalo se rozhodnutí o odpovídající ochraně s ohledem na Japonsko.

[21] Úplný přehled činností sboru viz příspěvek sboru, s. 18–23.

Důležitá úloha sboru vyvstala v případech, kdy bylo třeba urychleně zajistit jednotný výklad nařízení GDPR a nalézt okamžitě použitelná řešení na úrovni EU. Například v souvislosti s rozšířením onemocnění COVID-19 přijal sbor v březnu 2020 prohlášení o zpracování osobních údajů, které se mimo jiné zabývá zákonností zpracování a používáním mobilních lokalizačních údajů v tomto kontextu[22], a v dubnu 2020 přijal pokyny ke zpracování údajů o zdravotním stavu pro účely vědeckého výzkumu v souvislosti s rozšířením onemocnění COVID-19[23] a pokyny k používání lokalizačních údajů a nástrojů k vysledování kontaktů v souvislosti s rozšířením onemocnění COVID-19[24]. Sbor rovněž významně přispěl k navržení přístupu EU k aplikacím pro sledování Komisí a členskými státy.

Bez ohledu na to, zda úřady pro ochranu osobních údajů jednají ze své vlastní funkce nebo jako členové sboru, je jejich každodenní vzájemná spolupráce založena na výměnách informací a oznámeních případů, které úřady zahájily. S cílem usnadnit jejich vzájemnou komunikaci podpořila Komise úřady významně tím, že jim poskytla systém výměny informací[25]. Většina úřadů jej pokládá za přizpůsobený potřebám mechanismů spolupráce a jednotnosti, i když by mohl být ještě vylepšen například tím, že se stane přívětivějším pro uživatele.

I když je stále ještě brzy, lze již rozpoznat řadu úspěchů a výzev, které jsou představeny níže. Ukazují, že úřady pro ochranu osobních údajů doposud účinně využívaly nástroje spolupráce, přičemž upřednostňovaly flexibilnější řešení.

Jednotné kontaktní místo

Obecně platí, že v přeshraničních případech může být úřad pro ochranu osobních údajů členského státu zapojen buď i) jako vedoucí úřad, jestliže se hlavní místo podnikání provozovatele nachází v tomto členském státě, nebo ii) jako dotčený úřad, pokud má provozovatel provozovnu na území tohoto členského státu, pokud jsou osoby v tomto členském státě podstatně dotčeny nebo pokud byla u tohoto úřadu podána stížnost.

Tato úzká spolupráce se stala každodenní praxí: od data použitelnosti nařízení GDPR byly úřady pro ochranu osobních údajů ve všech členských státech v přeshraničních případech někdy označeny buď za vedoucí úřady, nebo za dotčené úřady, i když v různé míře.

Od května 2018 do konce roku 2019 jednal úřad pro ochranu osobních údajů v Irsku jako vedoucí úřad v nejvyšším počtu přeshraničních případů (127), po něm následovalo Německo (92), Lucembursko (87), Francie (64) a Nizozemsko (45). Toto pořadí odráží zejména specifickou situaci Irska a Lucemburska, kde sídlí několik velkých nadnárodních technologických společností.

[22] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[23] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_cs.

[24] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

[25] Systém pro výměnu informací o vnitřním trhu (IMI).

Pořadí se liší, pokud jde o zapojení dotčených úřadů pro ochranu osobních údajů, přičemž úřady v Německu jsou zapojeny do nejvyššího počtu případů (435), následuje Španělsko (337), Dánsko (327), Francie (332) a Itálie (306)[26].

V období od 25. května 2018 do 31. prosince 2019 bylo prostřednictvím jednotného kontaktního místa předloženo 141 návrhů rozhodnutí, z nichž 79 vedlo ke konečným rozhodnutím. Ke dni zveřejnění této zprávy se očekává několik důležitých rozhodnutí s přeshraničním rozměrem, na něž se vztahuje mechanismus jediného kontaktního místa. Mezi tato rozhodnutí patří i rozhodnutí týkající se nadnárodních velkých technologických společností[27]. Očekává se, že přispějí k větší harmonizaci při výkladu nařízení GDPR a poskytnou vyjasnění.

Vzájemná pomoc

Úřady pro ochranu osobních údajů využívají v široké míře nástroj vzájemné pomoci.

Do konce roku 2019 proběhlo 115 řízení o vzájemné pomoci[28], zejména pro účely provádění šetření, přičemž většinu z nich provedly úřady pro ochranu osobních údajů ve Španělsku (26), Německu (20), Dánsku (13), Polsku (12) a České republice (10). Na druhou stranu nejvíce žádostí obdrželo Irsko (19), Francie (11), Rakousko (10), Německo (10) a Lucembursko (9)[29].

Valná většina úřadů považuje vzájemnou pomoc za velmi užitečný nástroj spolupráce a při využití řízení o vzájemné pomoci se nesetkala s žádnou konkrétní překážkou. Dobrovolná výměna vzájemné pomoci, která nemá zákonnou lhůtu ani striktní povinnost odpovědět, byla využita častěji, a to ve 2 427 řízeních. Úřad pro ochranu osobních údajů v Irsku zaslal a obdržel nejvyšší počet žádostí o vzájemnou pomoc (527 zasláno a 359 obdrženo), za ním následovaly německé úřady (260 zasláno / 356 obdrženo).

Na druhé straně společné operace[30], které by umožnily zapojení úřadů pro ochranu osobních údajů několika členských států již na úrovni vyšetřování přeshraničních případů, nebyly dosud provedeny. V rámci sboru probíhají úvahy o praktickém provádění tohoto nástroje a o tom, jak jeho používání podpořit.

Mechanismus jednotnosti

Doposud byla využita pouze první část mechanismu jednotnosti, a sice přijetí stanovisek sboru[31]. Na druhé straně nebylo dosud zahájeno žádné řešení sporů na úrovni sboru[32] ani žádný postup pro naléhavé případy[33].

---

[26] Viz příspěvek sboru, s. 8.

[27] Například dne 22. května 2020 irský úřad pro ochranu osobních údajů předložil v souladu s článkem 60 nařízení jiným dotčeným úřadům návrh rozhodnutí týkajícího se šetření společnosti Twitter International ohledně oznámení o porušení zabezpečení osobních údajů. Tentýž den irský úřad pro ochranu osobních údajů rovněž oznámil, že probíhají přípravy návrhu rozhodnutí týkajícího se společnosti WhatsApp Ireland Limited podle článku 60 ve věci transparentnosti, a to i v souvislosti s transparentností ohledně toho, jaké informace jsou sdíleny se společností Facebook.

[28] Článek 61 nařízení GDPR.

[29] Viz příspěvek sboru, s. 12–14.

[30] Článek 62 nařízení GDPR.

[31] Na základě článku 64 nařízení GDPR.

[32] Článek 65 nařízení GDPR.

V období od 25. května 2018 do 31. prosince 2019 vydal sbor 36 stanovisek v souvislosti s přijetím opatření jedním z jeho členů[34]. Většina z nich (31) se týkala přijetí vnitrostátních seznamů operací zpracování, které vyžadují posouzení dopadu na ochranu osobních údajů. Dvě stanoviska se dotýkala závazných podnikových pravidel, dvě další se týkala návrhů požadavků na akreditaci subjektu pro monitorování kodexů chování a jedna se týkala standardních smluvních doložek[35].

Sbor dále na žádost přijal šest stanovisek[36]. Tři z těchto stanovisek pojednávala o vnitrostátních seznamech určujících zpracování, které nevyžaduje posouzení dopadu na ochranu osobních údajů. Ostatní se týkala správního ujednání o předávání osobních údajů mezi orgány finančního dohledu v EHP a třetích zemích, vzájemného vztahu mezi směrnicí o ochraně soukromí a elektronických komunikacích a nařízením GDPR a působnosti dozorového úřadu v případě změny okolností týkajících se hlavní nebo jediné provozovny[37].

Problémy, které je třeba řešit

Přestože úřady pro ochranu osobních údajů ve sboru velmi aktivně spolupracují a již intenzivně využívají nástroj spolupráce pro vzájemnou pomoc, budování skutečné společné kultury v oblasti ochrany osobních údajů stále probíhá.

Zejména řešení přeshraničních případů vyžaduje účinnější a harmonizovanější přístup a účinné využívání všech nástrojů spolupráce stanovených v nařízení GDPR. V tomto ohledu existuje velmi široká shoda, neboť na tuto otázku různými způsoby upozornil Evropský parlament, Rada, evropský inspektor ochrany údajů, zúčastněné strany (v rámci skupiny více zúčastněných stran a mimo ni) a úřady pro ochranu osobních údajů.

Mezi hlavní otázky, které je třeba v této souvislosti řešit, patří rozdíly:

- ve vnitrostátních správních postupech týkajících se zejména: postupů vyřizování stížností, kritérií přípustnosti stížností, délky řízení z důvodu různých časových rámců nebo neexistence lhůt, okamžiku řízení, kdy je přiznáno právo být vyslechnut, nebo informací a zapojení stěžovatelů v průběhu řízení,
- ve výkladech pojmů souvisejících s mechanismem spolupráce, jako jsou relevantní informace, pojem „neprodleně“, „stížnost“, dokument, který je definován jako „návrh rozhodnutí“ vedoucího úřadu pro ochranu osobních údajů, smírné řešení (zejména postup vedoucí ke smírnému řešení a právní forma řešení), a
- v přístupu k tomu, kdy má být zahájen postup spolupráce, kdy zapojit dotčené úřady pro ochranu osobních údajů a kdy jim sdělit informace. Stěžovatelé také nemají jasno v tom, jak jsou jejich případy řešeny v přeshraničních situacích, jak zdůraznilo několik členů skupiny více zúčastněných stran. Podniky navíc uvádějí, že v některých případech vnitrostátní úřady pro ochranu osobních údajů

[33] Článek 66 nařízení GDPR.
[34] Podle čl. 64 odst. 1 nařízení GDPR.
[35] Čl. 28 odst. 8 nařízení GDPR.
[36] Podle čl. 64 odst. 2 nařízení GDPR.
[37] Viz příspěvek sboru, s. 15.

nepostoupily případy vedoucímu úřadu pro ochranu osobních údajů, ale řešily je jako místní případy.

Komise vítá oznámení sboru, že zahájil úvahy o tom, jak tyto obavy řešit. Sbor zejména uvedl, že objasní procesní kroky, které jsou součástí spolupráce mezi vedoucím úřadem pro ochranu osobních údajů a dotčenými úřady pro ochranu osobních údajů, že provede analýzu vnitrostátních správních procesních předpisů, bude usilovat o společný výklad klíčových pojmů a posílí komunikaci a spolupráci (včetně společných operací). Jeho úvahy a analýzy by měly vést k navržení efektivnějších pracovních ujednání v přeshraničních případech[38], mimo jiné využitím odborných znalostí jeho členů a posílením účasti jeho sekretariátu. Kromě toho je třeba poznamenat, že odpovědnost sboru při zajišťování jednotného výkladu nařízení GDPR nemůže být vyřízena pouhým nalezením nejnižšího společného jmenovatele.

A konečně, jako subjekt EU musí sbor rovněž uplatňovat unijní správní právo a zajistit transparentnost rozhodovacího procesu.

2.3 Poradenství a pokyny

Zvyšování povědomí a poradenství ze strany úřadů pro ochranu osobních údajů

Několik úřadů pro ochranu osobních údajů vytvořilo nové nástroje, jako jsou linky pomoci pro fyzické osoby a podniky a sady nástrojů pro podniky[39]. Mnozí provozovatelé vítají pragmatický přístup těchto úřadů, pokud jde o pomoc při uplatňování nařízení GDPR. Některé z nich zejména aktivně a úzce spolupracovaly a komunikovaly s pověřenci pro ochranu osobních údajů, a to i prostřednictvím sdružení pověřenců pro ochranu osobních údajů. Mnoho úřadů rovněž vydalo pokyny týkající se úlohy a povinností pověřenců pro ochranu osobních údajů na jejich podporu v průběhu jejich každodenních činností a uspořádalo semináře, které jim byly speciálně určeny. To však neplatí pro všechny úřady pro ochranu osobních údajů.

Zpětná vazba od zúčastněných stran rovněž poukazuje na řadu problémů, pokud jde o pokyny a poradenství:

- absence jednotného přístupu a pokynů mezi vnitrostátními úřady pro ochranu osobních údajů ohledně určitých otázek (např. ohledně souborů cookie[40], uplatňování oprávněného zájmu, oznámení o porušení zabezpečení osobních údajů nebo posouzení dopadu na ochranu osobních údajů), nebo dokonce mezi úřady pro ochranu osobních údajů v rámci týchž členských států (např. v Německu ohledně pojmů správce a zpracovatele),
- nejednotnost pokynů přijatých na vnitrostátní úrovni s pokyny, které přijal sbor,

---

[38] Jak bylo rovněž zdůrazněno v postoji a zjištěních Rady.

[39] Viz bod 7 níže.

[40] Až do přijetí nařízení o soukromí a elektronických komunikacích je nezbytná úzká spolupráce s příslušnými orgány odpovědnými za prosazování směrnice o soukromí a elektronických komunikacích v členských státech. V souladu s uvedenou směrnicí nejsou v některých členských státech orgány příslušné pro vymáhání čl. 5 odst. 3 směrnice o soukromí a elektronických komunikací (který stanoví podmínky, za nichž je možné nastavit soubory „cookie“ a používat je v koncovém zařízení uživatele) totožné s dozorovými úřady podle nařízení GDPR.

- absence veřejných konzultací o některých pokynech přijatých na vnitrostátní úrovni,
- různé úrovně spolupráce se zúčastněnými stranami mezi úřady pro ochranu osobních údajů,
- zpoždění při přijímání odpovědí na žádosti o informace,
- obtíže při získávání praktických a cenných rad od úřadů pro ochranu osobních údajů,
- potřeba zvýšit úroveň oborových odborných znalostí v některých úřadech pro ochranu osobních údajů (např. v oblasti zdraví a farmacie).

Několik z těchto otázek souvisí také s nedostatkem zdrojů v některých úřadech pro ochranu osobních údajů (viz níže).

Odlišné postupy, pokud jde o ohlašování případů porušení zabezpečení osobních údajů[41]

Ačkoli Rada zdůrazňuje zátěž způsobenou tímto ohlašováním, existují značné rozdíly v ohlašování mezi členskými státy: zatímco od května 2018 do konce listopadu 2019 byl ve většině členských států celkový počet ohlášení případů porušení zabezpečení osobních údajů nižší než 2 000 a v sedmi členských státech mezi 2 000 až 10 000, nizozemské a německé úřady pro ochranu osobních údajů uvedly 37 400, resp. 45 600 ohlášení[42].

To může ukazovat na nedostatek jednotného výkladu a provádění, a to i přesto, že existují pokyny na úrovni EU pro ohlašování případů porušení zabezpečení osobních údajů.

Pokyny Evropského sboru pro ochranu osobních údajů

Sbor dosud přijal více než dvacet pokynů týkajících se klíčových aspektů nařízení GDPR[43]. Pokyny jsou základním nástrojem pro jednotné uplatňování nařízení GDPR, a zúčastněné strany je proto do značné míry uvítaly. Zúčastněné strany ocenily systematickou veřejnou konzultaci (v délce šesti až osmi týdnů). Žádají však o další dialog se sborem. V této souvislosti by měla pokračovat a posílit se praxe organizování seminářů zaměřených na předmětná témata před vypracováním pokynů, aby byla zajištěna transparentnost, inkluzivnost a význam činnosti sboru. Zúčastněné strany rovněž požadují, aby byl výklad nejspornějších otázek řešen v pokynech, neboť ty jsou předmětem veřejné konzultace, a nikoli v rámci stanovisek podle čl. 64 odst. 2 nařízení GDPR. Některé zúčastněné strany rovněž požadují praktičtější pokyny, které upřesní používání pojmů a ustanovení nařízení GDPR[44]. Členové skupiny více zúčastněných stran zdůrazňují potřebu konkrétnějších příkladů s cílem co nejvíce omezit prostor pro rozcházející se výklady mezi úřady pro ochranu osobních údajů.

---

41 Článek 33 nařízení GDPR.

42 Viz příspěvek sboru, s. 35.

43 Práce na pokynech již byly zahájeny před vstupem nařízení GDPR v platnost dne 25. května 2018 v souvislosti s pracovní skupinou zřízenou podle článku 29. Úplný seznam pokynů je k dispozici na adrese https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_cs.

44 To zdůraznil i Evropský parlament a Rada.

Současně by žádosti o objasnění způsobu, jak uplatňovat nařízení GDPR, a o zajištění právní jistoty neměly vést k dalším požadavkům ani by neměly omezit výhody přístupu založeného na rizicích a zásadu odpovědnosti.

Témata, o nichž by zúčastněné strany chtěly od sboru další pokyny, zahrnují: rozsah práv subjektů údajů (mimo jiné v kontextu pracovního poměru), aktualizace stanoviska týkajícího se zpracování na základě oprávněného zájmu, pojmy správce, společného správce a zpracovatele a nezbytná ujednání mezi stranami[45], uplatňování nařízení GDPR na nové technologie (např. technologie blockchain a umělá inteligence), zpracování v souvislosti s vědeckým výzkumem (mimo jiné v souvislosti s mezinárodní spoluprací), zpracování údajů dětí, pseudonymizace a anonymizace a zpracování zdravotních údajů.

Sbor již uvedl, že vydá pokyny týkající se mnoha z těchto témat, a práce na několika z nich již začaly (např. na uplatňování oprávněného zájmu jako právního základu pro zpracování).

Zúčastněné strany žádají sbor, aby v případě potřeby aktualizoval a přepracoval stávající pokyny s přihlédnutím ke zkušenostem získaným od jejich zveřejnění a s využitím možnosti případného podrobnějšího rozvedení.

2.4 Zdroje úřadů pro ochranu osobních údajů

Nezbytným předpokladem pro účinné plnění úkolů a výkon pravomocí úřadů pro ochranu osobních údajů, a tedy základní podmínkou pro jejich nezávislost je vybavení každého z nich nezbytnými lidskými, technickými a finančními zdroji, prostorami a infrastrukturou[46].

Od vstupu nařízení GDPR v platnost v roce 2016 došlo ve většině úřadů pro ochranu osobních údajů ke zvýšení počtu zaměstnanců a zdrojů[47]. Mnohé z nich však stále uvádějí, že nemají dostatečné zdroje[48].

Počet zaměstnanců pracujících pro vnitrostátní úřady pro ochranu osobních údajů

Celkový počet zaměstnanců pracujících v úřadech pro ochranu osobních údajů v EHP se v letech 2016 až 2019 souhrnně zvýšil o 42 % (o 62 %, je-li brána v úvahu prognóza pro rok 2020).

Počet zaměstnanců se během tohoto období ve většině úřadů zvýšil, přičemž největší nárůst (vyjádřený v procentech) byl zaznamenán u úřadů v Irsku (+169 %), v Nizozemsku (+145 %), na Islandu (+143 %), v Lucembursku (+126 %) a ve Finsku (+114 %). Na druhé straně se v několika úřadech pro ochranu osobních údajů počet zaměstnanců snížil, přičemž k největšímu poklesu došlo v Řecku (–15 %), Bulharsku (–14 %), Estonsku (–11 %), Lotyšsku (–10 %) a Litvě (–8 %). V některých úřadech je pokles počtu zaměstnanců také důsledkem odchodu odborníků na ochranu osobních údajů do soukromého sektoru, který nabízí atraktivnější podmínky.

[45] V současné době se připravují pokyny sboru týkající se správců a zpracovatelů.
[46] Viz čl. 52 odst. 4 nařízení GDPR.
[47] Nařízení vstoupilo v platnost v květnu 2016 a v květnu 2018 se začalo po dvouletém přechodném období používat.
[48] Viz příspěvek sboru, s. 26-30.

Prognóza pro rok 2020 obecně stanoví zvýšení počtu zaměstnanců oproti roku 2019, s výjimkou úřadů v Rakousku, Bulharsku, Itálii, Švédsku a na Islandu (u nichž se očekává, že počet zaměstnanců zůstane stabilní), na Kypru a v Dánsku (kde se očekává pokles počtu zaměstnanců).

Německé úřady pro ochranu osobních údajů[49] mají dohromady nejvyšší počet zaměstnanců (888 v roce 2019 / 1002 v prognóze pro rok 2020), dále pak úřady pro ochranu osobních údajů v Polsku (238/260), ve Francii (215/225), ve Španělsku (170/220), v Nizozemsku (179/188), v Itálii (170/170) a v Irsku (140/176).

Úřady pro ochranu osobních údajů s nejnižším počtem zaměstnanců jsou úřady na Kypru (24/22), v Lotyšsku (19/31), na Islandu (17/17), v Estonsku (16/18) a na Maltě (13/15).

Rozpočet vnitrostátních úřadů pro ochranu osobních údajů

Celkový rozpočet úřadů pro ochranu osobních údajů v EHP se v letech 2016 až 2019 souhrnně zvýšil o 49 % (o 64 %, je-li brána v úvahu prognóza pro rok 2020).

Rozpočet většiny úřadů se během tohoto období zvýšil, přičemž největší nárůst (vyjádřený v procentech) byl zaznamenán u úřadů v Irsku (+223 %), na Islandu (+167 %), v Lucembursku (+165 %), v Nizozemsku (+130 %) a na Kypru (+114 %). Na druhé straně zaznamenaly některé úřady pouze malý nárůst rozpočtu s nejmenším nárůstem zaznamenaným u úřadů pro ochranu osobních údajů v Estonsku (7 %), Lotyšsku (4 %), Rumunsku (3 %) a Belgii (1 %), zatímco u úřadu ve Francii byl zaznamenán pokles (–2 %).

Prognóza pro rok 2020 obecně stanoví navýšení rozpočtu ve srovnání s rokem 2019, s výjimkou úřadů v Rakousku, Bulharsku, Estonsku a Nizozemsku (jejichž rozpočet by měl zůstat stabilní).

Úřady pro ochranu osobních údajů s nejvyšším rozpočtem jsou úřady v Německu (76,6 milionu EUR v roce 2019 / EUR 85,8 milionu v prognóze pro rok 2020), v Itálii (29,1/30,1), Nizozemsku (18,6/18,6), Francii (18,5/20,1) a Irsku (15,2/16,9).

Úřady s nejnižším rozpočtem jsou úřady v Chorvatsku (1,2 milionu EUR v roce 2019 / 1,4 milionu EUR v prognóze pro rok 2020), v Rumunsku (1,1/1,3), v Lotyšsku (0,6/1,2), na Kypru (0,5/0,5) a na Maltě (0,5/0,6).

Tabulka v příloze II poskytuje přehled lidských a rozpočtových zdrojů vnitrostátních úřadů pro ochranu osobních údajů.

Kromě toho, že má dopad na jejich schopnost prosazovat pravidla na vnitrostátní úrovni, omezuje nedostatek zdrojů i schopnost úřadů pro ochranu osobních údajů účastnit se mechanismů spolupráce a jednotnosti a přispívat k činnosti v rámci sboru. Jak sbor zdůraznil, úspěch mechanismu jednotného kontaktního místa závisí na čase a úsilí, které úřady pro ochranu osobních údajů mohou věnovat řešení jednotlivých přeshraničních případů a spolupráci na nich. Otázka zdrojů je znásobena větší úlohou

[49] V Německu je osmnáct úřadů, z nichž jeden je spolkový a sedmnáct jich je zemských (včetně dvou v Bavorsku).

úřadů při dohledu nad rozsáhlými informačními systémy, které jsou v současné době vyvíjeny. Úřady pro ochranu osobních údajů v Irsku a Lucembursku mají navíc specifické potřeby v oblasti zdrojů vzhledem k jejich úloze vedoucích úřadů pro prosazování nařízení GDPR ve vztahu k velkým technologickým společnostem, které většinou sídlí v těchto členských státech.

Zatímco Rada poukazuje na dopad mechanismu spolupráce a jeho lhůt na práci úřadů pro ochranu osobních údajů[50], nařízení GDPR ukládá členským státům povinnost zajistit pro své vnitrostátní úřady pro ochranu osobních údajů odpovídající lidské, finanční a technické zdroje[51].

Sekretariát sboru, jehož služby poskytuje evropský inspektor ochrany údajů[52], je v současné době složen z dvaceti osob, včetně odborníků na právo, informační technologie a komunikace. Je třeba posoudit, zda je zapotřebí toto číslo v budoucnu změnit s ohledem na účinné plnění jeho funkce analytické, administrativní a logistické podpory sboru a jeho podskupin, a to i prostřednictvím správy systému pro výměnu informací.

3 PRAVIDLA JSOU HARMONIZOVANÁ, STÁLE VŠAK EXISTUJE URČITÁ MÍRA ROZTŘÍŠTĚNOSTI A ROZDÍLNÝCH PŘÍSTUPŮ

Nařízení GDPR stanoví jednotný přístup k pravidlům pro ochranu osobních údajů v celé EU a nahrazuje odlišné vnitrostátní režimy, které existovaly podle směrnice o ochraně údajů z roku 1995.

3.1 Provádění nařízení GDPR členskými státy

Nařízení GDPR je přímo použitelné ve všech členských státech od 25. května 2018. Uložilo členským státům povinnost vydávat právní předpisy, zejména zřídit vnitrostátní úřady pro ochranu osobních údajů a stanovit obecné podmínky pro jejich členy, aby se zajistilo, že každý úřad bude při plnění svých úkolů a při výkonu svých pravomocí jednat zcela nezávisle v souladu s nařízením GDPR. Právní povinnosti a veřejné úkoly mohou představovat právní základ zpracování osobních údajů, pouze pokud jsou stanoveny v (unijních nebo) vnitrostátních právních předpisech. Kromě toho musí členské státy stanovit sankce zejména za protiprávní jednání, na která se nevztahují správní pokuty, a musí sladit právo na ochranu osobních údajů s právem na svobodu projevu a informací. Vnitrostátní právo může rovněž stanovit právní základ pro osvobození od obecného zákazu u zpracování zvláštních kategorií osobních údajů, například z důvodu významného veřejného zájmu v oblasti veřejného zdraví, včetně ochrany před vážnými přeshraničními zdravotními hrozbami. Členské státy musí navíc zajistit akreditaci subjektů pro vydávání osvědčení.

Komise sleduje provádění nařízení GDPR ve vnitrostátních právních předpisech. V době práce na této zprávě přijaly všechny členské státy s výjimkou Slovinska nové právní předpisy o ochraně osobních údajů nebo přizpůsobily své právní předpisy v

[50] Článek 60 nařízení GDPR.
[51] Čl. 52 odst. 4 nařízení GDPR.
[52] Článek 75 nařízení GDPR.

této oblasti. Komise proto požádala Slovinsko, aby upřesnilo dosavadní pokrok, a vyzvala jej, aby tento proces dokončilo[53].

Soulad vnitrostátních právních předpisů s pravidly pro ochranu osobních údajů, pokud jde o schengenské acquis, je rovněž posuzován v kontextu schengenského hodnotícího mechanismu koordinovaného Komisí. Komise a členské státy společně hodnotí, jak země provádějí a uplatňují schengenské acquis v řadě oblastí; pokud jde o ochranu osobních údajů, týká se to rozsáhlých informačních systémů, jako je Schengenský informační systém a Vízový informační systém, a součástí je i úloha úřadů pro ochranu osobních údajů při dozoru nad zpracováním osobních údajů v rámci těchto systémů.

Na vnitrostátní úrovni stále probíhají práce na přizpůsobení odvětvových právních předpisů. V návaznosti na začlenění nařízení GDPR do Dohody o Evropském hospodářském prostoru byla jeho použitelnost rozšířena na Norsko, Island a Lichtenštejnsko. Tyto země rovněž přijaly vnitrostátní právní předpisy o ochraně osobních údajů.

Komise využije všech nástrojů, které má k dispozici, včetně řízení o nesplnění povinnosti, aby zajistila, že členské státy budou dodržovat nařízení GDPR.

Hlavní otázky týkající se vnitrostátního provádění

K hlavním otázkám, které byly dosud zaznamenány v rámci probíhajícího posuzování vnitrostátních právních předpisů a dvoustranných výměn s členskými státy, patří:

- omezení použití nařízení GDPR: některé členské státy například zcela vylučují činnosti vnitrostátního parlamentu,
- rozdíly v použitelnosti vnitrostátních právních předpisů se specifikacemi. Některé členské státy spojují použitelnost svého vnitrostátního práva s místem, kde je nabízeno zboží nebo služby, jiné s místem provozovny správce nebo zpracovatele. To je v rozporu s cílem harmonizace, který sleduje nařízení GDPR,
- vnitrostátní právní předpisy, které vyvolávají otázky ohledně přiměřenosti zásahu do práva na ochranu osobních údajů. Komise například zahájila řízení o nesplnění povinnosti proti členskému státu, který přijal právní předpisy požadující, aby soudci zveřejňovali konkrétní informace o svých neprofesních činnostech, což je neslučitelné s právem na respektování soukromého života a právem na ochranu osobních údajů[54],
- absence nezávislého orgánu pro dozor nad zpracováváním údajů ze strany soudů, které jednají v rámci svých soudních pravomocí[55],
- právní předpisy v oblastech, které v plném rozsahu upravuje nařízení GDPR, mimo rámec specifikací nebo omezení. Jedná se zejména o případ, kdy

[53] Je třeba poznamenat, že vnitrostátní úřad pro ochranu osobních údajů ve Slovinsku je zřízen na základě současného vnitrostátního právního předpisu o ochraně osobních údajů a dohlíží na uplatňování nařízení GDPR v tomto členském státě.

[54] Toto řízení o nesplnění povinnosti se týká polského zákona o soudnictví ze dne 20. prosince 2019, který má dopad na nezávislost soudců a týká se mimo jiné zpřístupňování informací o zapojení soudců do neprofesních činností: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_772.

[55] Viz čl. 8 odst. 3 Listiny, článek 16 SFEU, 20. bod odůvodnění nařízení GDPR.

vnitrostátní předpisy určují podmínky pro zpracování založené na oprávněném zájmu, a to stanovením rovnováhy mezi příslušnými zájmy správce a dotčených osob, zatímco nařízení GDPR ukládá každému správci povinnost provádět toto vyvážení individuálně a využít tohoto právního základu,

- specifikace a další požadavky nad rámec zpracování pro splnění právní povinnosti nebo výkon veřejného úkolu (např. pro kamerový dohled v soukromém sektoru nebo pro přímý marketing) a pro pojmy používané v nařízení GDPR (např. „velký rozsah“ nebo „výmaz“).

Některé z těchto otázek může vyjasnit Soudní dvůr v dosud neuzavřených věcech[56].

Sladění práva na ochranu osobních údajů se svobodou projevu a informací

Konkrétní otázka se týká zavedení povinnosti členských států uvést zákonem do souladu právo na ochranu osobních údajů se svobodou projevu a informací[57]. Tato otázka je velmi složitá, neboť posouzení rovnováhy mezi těmito základními právy musí zohlednit i ustanovení a záruky v právních předpisech týkajících se tisku a sdělovacích prostředků.

Posouzení právních předpisů členských států ukazuje různé přístupy k sladění práva na ochranu osobních údajů se svobodou projevu a informací:

- Některé členské státy stanoví zásadu přednosti svobody projevu nebo v zásadě používají výjimky z uplatňování celých kapitol uvedených v čl. 85 odst. 2 nařízení GDPR, pokud jde o zpracování pro účely žurnalistiky a pro akademické, umělecké a literární účely. Právní předpisy týkající se sdělovacích prostředků stanoví do jisté míry určité záruky, pokud jde o práva subjektu údajů.
- Některé členské státy stanoví přednost ochrany osobních údajů a výjimky z uplatňování pravidel ochrany osobních údajů používají pouze ve specifických situacích, např. v případě, kdy se jedná o osobu s veřejným postavením.
- Jiné členské státy stanoví určité vyvážení ze strany zákonodárce a/nebo posouzení jednotlivých případů, pokud jde o výjimky z některých ustanovení nařízení GDPR.

Komise bude pokračovat v posuzování vnitrostátních právních předpisů na základě požadavků stanovených v Listině. Sladění musí být stanoveno zákonem, musí respektovat podstatu těchto základních práv a musí být přiměřené a nezbytné (čl. 52 odst. 1 Listiny). Pravidla ochrany osobních údajů by neměla ovlivnit uplatňování svobody projevu a informací zejména tím, že by měla odrazující účinek, nebo tím, že by byla vykládána jako způsob, jak vyvíjet tlak na novináře, aby zveřejňovali své zdroje.

[56] Například předmětem probíhajícího řízení o předběžné otázce je osvobození parlamentního výboru od uplatňování nařízení GDPR (C-272/19).

[57] Článek 85 nařízení GDPR.

3.2 Doložky o volitelných specifikacích a jejich omezení

Nařízení GDPR dává členským státům možnost dále upřesnit jeho uplatňování v omezeném počtu oblastí. Tento prostor pro vnitrostátní právní předpisy je třeba odlišit od povinnosti provést některá další ustanovení nařízení GDPR, jak je uvedeno výše. Doložky o volitelných specifikacích jsou vyjmenovány v příloze I.

Prostor pro právo členských států podléhají podmínkám a omezením stanoveným v nařízení GDPR a neumožňují paralelní vnitrostátní režim ochrany osobních údajů[58]. Členské státy jsou povinny změnit nebo zrušit vnitrostátní právní předpisy o ochraně osobních údajů, včetně odvětvových právních předpisů s aspekty ochrany osobních údajů.

Kromě toho nesmí související právní předpisy členských států obsahovat ustanovení, která by mohla vést k nejasnostem ohledně přímého použití nařízení GDPR. Pokud tedy nařízení GDPR stanoví specifikace nebo omezení svých pravidel právem členského státu, mohou členské státy začlenit do svého vnitrostátního práva prvky tohoto nařízení, pokud je to nezbytné pro účely soudržnosti a pro zajištění srozumitelnosti vnitrostátních předpisů pro osoby, na něž se vztahují[59].

Zúčastněné strany se domnívají, že by členské státy měly omezit používání doložek o volitelných specifikacích nebo se jejich používání zdržet, neboť nepřispívají k harmonizaci. Vnitrostátní rozdíly v provádění právních předpisů i v jejich výkladu ze strany úřadů pro ochranu osobních údajů značně zvyšují náklady na dodržování právních předpisů v celé EU.

Roztříštěnost spojená s používáním doložek o volitelných specifikacích

- Věková hranice pro souhlas dětí se službami informační společnosti

Řada členských států využila možnosti stanovit pro udělení souhlasu v souvislosti se službami informační společnosti nižší věk než 16 let (čl. 8 odst. 1 nařízení GDPR). Zatímco devět členských států uplatňuje věkovou hranici 16 let, osm členských států zvolilo 13 let, šest 14 let a tři 15 let[60].

V důsledku toho musí společnost poskytující služby informační společnosti nezletilým v celé EU rozlišovat věk potenciálních uživatelů v závislosti na tom, ve kterém členském státě pobývají. To je v rozporu s hlavním cílem nařízení GDPR, který spočívá v zajištění stejné úrovně ochrany fyzických osob a stejné úrovně obchodních příležitostí ve všech členských státech.

Tyto rozdíly vedou k situacím, kdy členský stát, v němž je správce usazen, stanoví jinou věkovou hranici než členský stát, v němž mají subjekty údajů bydliště.

---

[58] Široce používaný výraz „deregulační doložky“ ve smyslu doložek o specifikacích je zavádějící, neboť by mohl vyvolat dojem, že členské státy mají manévrovací prostor nad rámec ustanovení nařízení.

[59] 8. bod odůvodnění nařízení GDPR.

[60] Věková hranice 13 let v případě Belgie, Dánska, Estonska, Finska, Lotyšska, Malty, Portugalska a Švédska; 14 let v Rakousku, Bulharsku, na Kypru, ve Španělsku, Itálii a Litvě, 15 let v České republice, Řecku a Francii, 16 let v Německu, Maďarsku, Chorvatsku, Irsku, Lucembursku, Nizozemsku, Polsku, Rumunsku a na Slovensku.

- Zdraví a výzkum

Při uplatňování výjimek z obecného zákazu zpracování zvláštních kategorií osobních údajů[61] se právní předpisy členských států řídí různými přístupy, pokud jde o úroveň specifikace a záruk, včetně přístupů pro účely zdraví a výzkumu. Většina členských států zavedla nebo zachovala další podmínky pro zpracování genetických údajů, biometrických údajů nebo údajů týkajících se zdraví. Totéž platí pro výjimky týkající se práv subjektů údajů pro výzkumné účely[62], a to jak z hlediska rozsahu výjimek, tak i z hlediska souvisejících záruk.

Budoucí pokyny sboru k používání osobních údajů v oblasti vědeckého výzkumu přispějí k harmonizovanému přístupu v této oblasti. Komise poskytne sboru vstupní informace, zejména informace týkající se výzkumu v oblasti zdraví, a to i formou konkrétních otázek a analýz konkrétních scénářů, které obdržela od výzkumné obce. Bylo by užitečné, kdyby tyto pokyny mohly být přijaty před zahájením rámcového programu Horizont Evropa s cílem harmonizovat postupy v oblasti ochrany osobních údajů a usnadnit sdílení údajů pro pokrok v oblasti výzkumu. Užitečné by mohly být i pokyny Rady ke zpracování osobních údajů v oblasti zdraví.

Nařízení GDPR poskytuje robustní rámec pro vnitrostátní právní předpisy v oblasti veřejného zdraví a výslovně zahrnuje přeshraniční zdravotní hrozby a monitorování epidemií a jejich šíření[63], které byly relevantní v souvislosti s bojem proti pandemii COVID-19.

Na úrovni EU přijala Komise dne 8. dubna 2020 doporučení o sadě nástrojů pro využití technologií a dat v této souvislosti, včetně mobilních aplikací a využívání anonymizovaných dat o mobilitě[64], a dne 16. dubna 2020 pokyny k aplikacím podporujícím boj proti pandemii ve vztahu k ochraně údajů[65]. Dne 19. března 2020 zveřejnil sbor prohlášení o zpracování osobních údajů v této souvislosti[66], dne 21. dubna 2020 následovaly pokyny ke zpracování údajů o zdravotním stavu pro účely vědeckého výzkumu a k používání lokalizačních údajů a nástrojů v této souvislosti[67]. Tato doporučení a pokyny objasňují, jak se zásady a pravidla pro ochranu osobních údajů uplatňují v souvislosti s bojem proti pandemii.

- Rozsáhlá omezení práv subjektů údajů

Většina vnitrostátních právních předpisů o ochraně osobních údajů, které omezují práva subjektu údajů, neupřesňuje cíle obecného veřejného zájmu zaručené těmito omezeními a/nebo dostatečně nesplňuje podmínky a záruky požadované čl. 23 odst. 2 nařízení GDPR[68]. Několik členských států neponechává žádný prostor pro test přiměřenosti ani pro rozšíření omezení, a to i nad rámec čl. 23 odst. 1 nařízení GDPR.

---

[61] Článek 9 nařízení GDPR.
[62] Čl. 89 odst. 2 nařízení GDPR.
[63] Viz čl. 9 odst. 2 písm. i) nařízení GDPR a 46. bod odůvodnění.
[64] https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.
[65] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417 (08) & from = EN.
[66] https://edpb.europa.eu/our-work-tools/our-documents/outros/statement-processing-personal-data-context-covid-19-outbreak_cs.
[67] https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_cs.
[68] Například proto, že jednoduše opakují znění čl. 23 odst. 1 nařízení GDPR.

Některé vnitrostátní právní předpisy například odpírají právo na přístup z důvodu nepřiměřeného úsilí na straně správce, pokud jde o osobní údaje, které jsou uchovávány na základě povinnosti uchovávat údaje nebo souvisejí s plněním veřejných úkolů, aniž by toto omezení bylo omezeno na cíle obecného veřejného zájmu.

- Další požadavky na společnosti

Ačkoli se požadavek povinného pověřence pro ochranu osobních údajů opírá o přístup založený na rizicích[69], jeden členský stát[70] jej rozšířil o kvantitativní kritéria, přičemž stanovil, že společnosti, ve kterých je do automatizovaného zpracování osobních údajů trvale zapojeno dvacet nebo více zaměstnanců, musí jmenovat pověřence pro ochranu osobních údajů nezávisle na rizicích spojených s činnostmi zpracování[71]. To vedlo k další zátěži.

4 POSÍLENÍ POSTAVENÍ FYZICKÝCH OSOB, ABY MĚLY POD KONTROLOU SVÉ OSOBNÍ ÚDAJE

Nařízení GDPR zajišťuje účinnost základních práv, zejména práva na ochranu osobních údajů, ale také ostatních základních práv uznávaných Listinou, včetně respektování soukromého a rodinného života, svobody projevu a informací, nediskriminace, svobody myšlení, svědomí a náboženského vyznání, svobody podnikání a práva na účinnou právní ochranu. Tato práva musí být vzájemně vyvážena v souladu se zásadou proporcionality[72].

Nařízení GDPR poskytuje fyzickým osobám vymahatelná práva, jako je právo na přístup, opravu, výmaz, námitku, přenositelnost a zvýšenou transparentnost. Rovněž dává fyzickým osobám právo podat stížnost u úřadu pro ochranu osobních údajů, a to i prostřednictvím zástupných žalob, a právo na soudní ochranu.

Jak vyplývá z výsledků průzkumu Eurobarometru z července 2019[73] a z průzkumu provedeného Agenturou pro základní práva[74], jsou si fyzické osoby stále více vědomy svých práv.

Podle průzkumu základních práv, který provedla Agentura pro základní práva:

- 69 % obyvatel ve věku 16 a více let v EU slyšelo o nařízení GDPR,
- 71 % respondentů v EU slyšelo o svém vnitrostátním úřadu pro ochranu osobních údajů, tento údaj se pohybuje mezi 90 % v České republice a 44 % v Belgii,
- 60 % respondentů v EU si je vědomo zákona, který jim umožňuje přístup k jejich osobním údajům, které uchovávají orgány veřejné správy, tento procentní podíl se však snižuje na 51 % u soukromých společností,

[69] Čl. 37 odst. 1 nařízení GDPR.
[70] Německo.
[71] Použití doložky o specifikacích v čl. 37 odst. 4 nařízení GDPR.
[72] Srov. 4. bod odůvodnění nařízení GDPR.
[73] https://ec.europa.eu/commission/presscorner/detail/cs/IP_19_2956.
[74] Agentura Evropské unie pro základní práva (FRA) (2020): Průzkum základních práv 2019. Ochrana osobních údajů a technologie: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection.

- více než jeden z pěti respondentů (23 %) v EU nechce sdílet osobní údaje (např. adresu, občanství nebo datum narození) s orgány veřejné správy a 41 % nechce tyto údaje sdílet se soukromými společnostmi.

Fyzické osoby stále více využívají své právo podávat stížnosti k úřadům pro ochranu osobních údajů, a to buď samostatně, nebo prostřednictvím zástupných žalob[75]. Pouze několik členských států umožnilo nevládním organizacím podávat žaloby bez pověření v souladu s možností stanovenou v nařízení GDPR. Očekává se, že navrhovaná směrnice o zástupných žalobách na ochranu kolektivních zájmů spotřebitelů[76] posílí po svém přijetí rámec pro zástupné žaloby i v oblasti ochrany osobních údajů.

Stížnosti

Jak uvádí sbor, bylo v období od května 2018 do konce listopadu 2019 podáno celkem přibližně 275 000 stížností[77]. Tento údaj by však měl být brán v úvahu s velkou obezřetností vzhledem k tomu, že definice stížnosti není mezi úřady totožná. Absolutní počet stížností obdržených úřady pro ochranu osobních údajů[78] se mezi členskými státy velmi liší. Nejvyšší počet stížností byl zaznamenán v Německu (67 000), Nizozemsku (37 000), Španělsku a Francii (po 18 000), Itálii (14 000), Polsku a Irsku (po 12 000). Dvě třetiny úřadů oznámily počet stížností pohybující se od 8 000 do 600. Nejnižší počet stížností byl zaznamenán v Estonsku a Belgii (přibližně po 500), na Maltě a na Islandu (v každém státě méně než 200).

Počet stížností není nutně spojen s počtem obyvatel nebo HDP, například téměř dvojnásobek stížností v Německu v porovnání s Nizozemskem a čtyřnásobek ve srovnání se Španělskem a Francií.

Zpětná vazba skupiny více zúčastněných stran ukazuje, že organizace zavedly řadu opatření k usnadnění výkonu práv subjektů údajů, včetně prováděcích postupů, které zajišťují individuální přezkum žádostí a odpověď správce, využívání několika kanálů (pošta, vyhrazená e-mailová adresa, internetové stránky atd.), aktualizovaných vnitřních postupů a politik týkajících se včasného interního vyřizování žádostí a odborné přípravy zaměstnanců. Některé společnosti zavedly digitální portály přístupné na internetových stránkách společnosti (nebo na intranetu společnosti pro zaměstnance) s cílem usnadnit výkon práv subjektů údajů.

Je však třeba dosáhnout dalšího pokroku v těchto bodech:

- Ne všichni správci údajů plní svou povinnost usnadnit výkon práv subjektů údajů[79]. Musí zajistit, aby subjekty údajů měly účinné kontaktní místo, kterému mohou vysvětlit své problémy. Tím může být pověřenec pro ochranu osobních údajů, jehož kontaktní údaje musí být subjektu údajů proaktivně poskytnuty[80]. Možnosti kontaktu nesmí být omezeny na e-maily, ale musí subjektu údajů dávat též možnost obrátit se na správce jinými prostředky.

---

75 Článek 80 nařízení GDPR.
76 COM/2018/0184 final - 2018/089 (COD).
77 Podle článku 77 i článku 80 nařízení GDPR.
78 Viz příspěvek sboru, s. 31-32.
79 Čl. 12 odst. 2 nařízení GDPR.
80 Čl. 13 odst. 1 písm. b) a čl. 14 odst. 1 písm. b) nařízení GDPR.

- Fyzické osoby se i nadále potýkají s obtížemi při podávání žádostí o přístup ke svým údajům, například z platforem, od zprostředkovatelů údajů a společností působících v oblasti špičkových technologií.
- Právo na přenositelnost údajů není plně využíváno. Evropská strategie pro data (dále jen „datová strategie“)[81], kterou Komise přijala dne 19. února 2020, zdůraznila potřebu usnadnit veškerá možná využití tohoto práva (např. zavedením technických rozhraní a strojově čitelných formátů umožňujících přenositelnost dat v (téměř) reálném čase). Provozovatelé upozorňují, že někdy dochází k obtížím při poskytování údajů ve strukturovaném, běžně používaném strojově čitelném formátu (z důvodu neexistence standardu). To, že byla zavedena nezbytná rozhraní, uvádějí pouze organizace v určitých odvětvích, jako je bankovnictví, telekomunikace, vodoměry a měřiče vytápění[82]. Byly vyvinuty nové technologické nástroje, které fyzickým osobám usnadňují výkon jejich práv podle nařízení GDPR a které se neomezují pouze na přenositelnost údajů (např. prostory pro osobní údaje a služby správy osobních informací).
- Práva dětí: Několik členů skupiny více zúčastněných stran zdůrazňuje potřebu poskytovat informace dětem a skutečnost, že mnohé organizace ignorují, že jejich zpracování údajů se může týkat dětí. Rada zdůraznila, že při přípravě kodexů chování by mohla být zvláštní pozornost věnována ochraně dětí. Úřady pro ochranu osobních údajů se zaměřují i na ochranu dětí[83].
- Právo na informace: Některé společnosti mají velmi formalistický přístup, kdy jako právní nástroj používají oznámení o ochraně osobních údajů, přičemž informace jsou poměrně složité, obtížně srozumitelné či neúplné. Naopak nařízení GDPR vyžaduje, aby veškeré informace byly stručné a používaly se jasné a jednoduché jazykové prostředky[84]. Zdá se, že některé společnosti se doporučeními sboru neřídí, například pokud jde o uvádění názvů subjektů, s nimiž sdílejí údaje.
- Několik členských států široce omezuje práva subjektů údajů prostřednictvím vnitrostátních právních předpisů, a některé při tom dokonce i překračují mez článku 23 nařízení GDPR.
- Výkon práv fyzických osob je někdy ztěžován praktikami několika významných digitálních hráčů, které fyzickým osobám ztěžují volbu nastavení, která nejvíce chrání jejich soukromí (v rozporu s požadavkem na záměrnou a standardní ochranu osobních údajů[85])[86].

---

81 https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

82 Viz zpráva skupiny více zúčastněných stran.

83 Viz výsledky veřejné konzultace o právech dětí na ochranu osobních údajů, kterou provedl irský úřad pro ochranu osobních údajů: https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf. Veřejnou konzultaci zahájil v dubnu 2020 i francouzský úřad pro ochranu osobních údajů: https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-sur-les-droits-des-mineurs-dans-lenvironnement-numerique.

84 Čl. 12 odst. 1 nařízení GDPR.

85 Článek 25 nařízení GDPR.

86 Viz zpráva Norské rady pro spotřebitele, „Deceived by Design“, která poukázala na „temné vzorce“, standardní nastavení a další prvky a techniky, které společnosti používají k tomu, aby uživatele donutily k možnostem narušujícím soukromí: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/.

Zúčastněné strany netrpělivě očekávají pokyny sboru týkající se práv subjektů údajů.

5 PŘÍLEŽITOSTI A VÝZVY PRO ORGANIZACE, ZEJMÉNA PRO MALÉ A STŘEDNÍ PODNIKY

Příležitosti pro organizace

Nařízení GDPR podporuje hospodářskou soutěž a inovace. Společně s nařízením o volném toku neosobních údajů[87] zajišťuje volný tok údajů v rámci EU a vytváří rovné podmínky se společnostmi se sídlem mimo EU. Vytvořením harmonizovaného rámce pro ochranu osobních údajů zajišťuje nařízení GDPR, aby všechny subjekty na vnitřním trhu byly vázány stejnými pravidly a využívaly stejných příležitostí bez ohledu na to, kde mají sídlo a kde zpracování probíhá. Technologická neutralita nařízení GDPR poskytuje rámec ochrany osobních údajů pro nový technologický vývoj. Zásady záměrné a standardní ochrany osobních údajů motivují inovativní řešení, která od samého počátku zahrnují hlediska ochrany osobních údajů a mohou snížit náklady na dodržování pravidel ochrany osobních údajů.

Soukromí se navíc stává důležitým parametrem hospodářské soutěže, který fyzické osoby stále více zohledňují při výběru svých služeb. Ti, kdo jsou lépe informováni a citlivější na hlediska ochrany osobních údajů, hledají výrobky a služby, které zajišťují účinnou ochranu osobních údajů. Provádění práva na přenositelnost údajů má potenciál snížit překážky vstupu na trh pro podniky, které nabízejí inovativní služby respektující ochranu osobních údajů. Je třeba sledovat účinky potenciálně širšího využívání tohoto práva na trhu v různých odvětvích. Dodržování pravidel ochrany osobních údajů a jejich transparentní uplatňování zajistí důvěru v používání osobních údajů jednotlivců, a tím i nové příležitosti pro podniky.

Stejně jako všechny právní předpisy přinášejí pravidla ochrany osobních údajů vlastní náklady na dodržování předpisů pro společnosti. Nad těmito náklady však převažují příležitosti a výhody posílené důvěry v digitální inovace a společenský přínos vyplývající z dodržování základního práva. Zajištěním rovných podmínek a vybavením úřadů pro ochranu osobních údajů tím, co potřebují k účinnému vymáhání pravidel, zabraňuje nařízení GDPR společnostem, které nedodržují předpisy, v parazitování na důvěře budované těmi, kdo pravidla dodržují.

Zvláštní výzvy pro malé a střední podniky

Zúčastněné strany, ale také Evropský parlament, Rada a úřady pro ochranu osobních údajů obecně vnímají, že uplatňování nařízení GDPR je obzvláště náročné pro mikropodniky, malé a střední podniky a malé dobrovolnické a charitativní organizace.

Podle přístupu založeného na rizicích by nebylo vhodné stanovovat výjimky na základě velikosti provozovatelů, neboť jejich velikost není sama o sobě ukazatelem

---

Viz rovněž výzkum zveřejněný v prosinci 2019 Transatlantickým dialogem spotřebitelů a nadací Heinrich-Böll-Stiftung Brussels European Union, který analyzuje postupy tří velkých globálních platforem: https://eu.boell.org/en/2019/12/11/privacy-eu-and-us-consumer-experiences-across-three-global-platforms.

87 Nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii (Úř. věst. L 303, 28.11.2018, s. 59).

rizik, jež může pro fyzické osoby představovat zpracování osobních údajů, které provádějí. Přístup založený na rizicích spojuje flexibilitu s účinnou ochranou. Bere v úvahu potřeby malých a středních podniků, které nemají zpracování osobních údajů jako svou hlavní činnost, a přesně měří jejich povinnosti zejména na základě pravděpodobnosti a závažnosti rizik souvisejících s konkrétním zpracováním, které provádějí[88].

Se zpracováním spojeným s malým a nízkým rizikem by se nemělo nakládat stejně jako se zpracováním s vysokým rizikem a častým zpracováním – nezávisle na velikosti společnosti, která je provádí. Sbor proto dospěl k závěru, že „v každém případě by měl být zachován přístup založený na rizicích prosazovaný zákonodárcem v textu, neboť rizika pro subjekty údajů nezávisí na velikosti správců“[89]. Úřady pro ochranu osobních údajů by měly tuto zásadu plně zohlednit při prosazování nařízení GDPR, nejlépe v rámci společného evropského přístupu, aby nevznikaly překážky pro jednotný trh.

Úřady pro ochranu osobních údajů vyvinuly několik nástrojů a zdůraznily, že mají v úmyslu je dále zlepšovat. Některé úřady zahájily osvětové kampaně, a budou pořádat dokonce i bezplatné „kurzy o nařízení GDPR“ pro malé a střední podniky.

Příklady pokynů a nástrojů, které úřady pro ochranu osobních údajů poskytují konkrétně malým a středním podnikům

- Zveřejňování informací určených malým a středním podnikům.
- Semináře pro pověřence pro ochranu osobních údajů a akce pro malé a střední podniky, které nemusí jmenovat pověřence pro ochranu osobních údajů.
- Interaktivní pokyny na pomoc malým a středním podnikům.
- Telefonní linky pro konzultace.
- Šablony pro zpracování smluv a záznamů o činnostech zpracování.

Popis činností vykonávaných úřady pro ochranu osobních údajů je uveden v příspěvku sboru[90].

Několik opatření, jež konkrétně podporují malé a střední podniky, obdrželo finanční prostředky EU. Komise poskytla finanční podporu prostřednictvím tří vln grantů v celkové hodnotě 5 milionů EUR, přičemž dvě poslední vlny byly konkrétně zaměřeny na podporu vnitrostátních úřadů pro ochranu osobních údajů v jejich úsilí oslovit fyzické osoby a malé a střední podniky. V důsledku toho byla v roce 2018 přidělena devíti úřadům pro ochranu osobních údajů na činnosti v období 2018–2019 částka v celkové výši 2 milionů EUR (Belgie, Bulharsko, Dánsko, Litva, Lotyšsko, Maďarsko, Nizozemsko, Slovinsko a Island)[91] a v roce 2019 byla čtyřem úřadům pro ochranu osobních údajů přidělena na činnosti v roce 2020 částka ve výši 1 milion EUR

[88] Čl. 24 odst. 1 nařízení GDPR.
[89] Viz příspěvek sboru, s. 35.
[90] Viz příspěvek sboru, s. 35-45.
[91] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai- ag-2017.

(Belgie, Malta, Slovinsko a Chorvatsko v partnerství s Irskem)92. Další 1 milion EUR bude přidělen v roce 2020.

Navzdory těmto iniciativám malé a střední podniky a začínající podniky často uvádějí, že mají potíže s uplatňováním zásady odpovědnosti stanovené v nařízení GDPR[93]. Zejména uvádějí, že ne vždy dostávají dostatek pokynů a praktického poradenství od vnitrostátních úřadů pro ochranu osobních údajů, nebo že trvá příliš dlouho, než pokyny a poradenství dostanou. Vyskytly se také případy, kdy se úřady zdráhaly zapojit se do právních otázek. V takových situacích se malé a střední podniky často obracejí na externí poradce a právníky, aby se vypořádaly s uplatňováním zásady odpovědnosti a přístupu založeného na rizicích (včetně požadavků na transparentnost, záznamů o zpracování a ohlašování případů porušení zabezpečení osobních údajů). V důsledku toho jim mohou vznikat další náklady.

Jedním z konkrétních problémů je zaznamenávání činností zpracování, které malé a střední podniky a malá sdružení považují za těžkopádnou administrativní zátěž. Výjimka z této povinnosti stanovená v čl. 30 odst. 5 nařízení GDPR je ve skutečnosti velmi úzká. Související úsilí o splnění této povinnosti by však nemělo být přeceňováno. Pokud hlavní činnost malých a středních podniků nezahrnuje zpracování osobních údajů, mohou být tyto záznamy jednoduché a nezatěžující. Totéž platí pro dobrovolnická a jiná sdružení. Tyto zjednodušené záznamy by byly usnadněny šablonami záznamů, jak je již praxí některých úřadů pro ochranu osobních údajů. V každém případě by každý, kdo zpracovává osobní údaje, měl mít přehled o svém zpracování osobních údajů jako základní požadavek zásady odpovědnosti.

Rozvoj praktických nástrojů sborem na úrovni EU, např. harmonizovaných formulářů pro případy porušení ochrany osobních údajů a zjednodušených záznamů o činnostech zpracování, může pomoci malým a středním podnikům a malým sdružením[94], jejichž hlavní činnosti se nezaměřují na zpracování osobních údajů za účelem splnění jejich povinností.

Různá odvětvová sdružení vyvinula úsilí ke zvýšení povědomí a informování svých členů, například prostřednictvím konferencí a seminářů, poskytování informací o dostupných pokynech podnikům nebo rozvoje asistenčních služeb pro ochranu soukromí pro členy. Rovněž uvádějí rostoucí počet seminářů, zasedání a akcí pořádaných think tanky a sdruženími malých a středních podniků v záležitostech souvisejících s nařízením GDPR.

S cílem posílit volný pohyb všech údajů v rámci EU a zavést ucelené uplatňování nařízení GDPR a nařízení o volném toku neosobních údajů vydala Komise rovněž praktické pokyny týkající se pravidel zpracování smíšených datových sad, které se skládají z osobních i neosobních údajů, a zaměřené zejména na malé a střední podniky[95].

Sada nástrojů pro podniky

---

92 https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en.

93 Viz zpráva skupiny více zúčastněných stran.

94 Viz příspěvek Rady.

95 Sdělení Komise Evropskému parlamentu a Radě – Pokyny k nařízení o rámci pro volný tok neosobních údajů v Evropské unii, COM/2019/250 final.

Nařízení GDPR stanoví nástroje, které pomáhají prokazovat dodržování předpisů, jako jsou kodexy chování, mechanismy vydávání osvědčení a standardní smluvní doložky.

- Kodexy chování

Sbor vypracoval pokyny[96] s cílem poskytnout podporu a pomoc „majitelům kodexů“ při navrhování, změně nebo rozšiřování kodexů a poskytnout praktické pokyny a pomoc při výkladu. Tyto pokyny rovněž vyjasňují postupy pro předkládání, schvalování a zveřejňování kodexů jak na vnitrostátní, tak na unijní úrovni stanovením minimálních požadovaných kritérií.

Zúčastněné strany považují kodexy chování za velmi užitečné nástroje. Ačkoli je mnoho kodexů prováděno na vnitrostátní úrovni, připravuje se v současné době řada celounijních kodexů chování (například v oblasti mobilních zdravotních aplikací, zdravotního výzkumu v oblasti genomiky, cloud computingu, přímého marketingu, pojištění, zpracování pomocí služeb v oblasti prevence a poradenství pro děti)[97]. Provozovatelé se domnívají, že celounijní kodexy chování by měly být více prosazovány, neboť podporují důsledné uplatňování nařízení GDPR ve všech členských státech.

Kodexy chování však rovněž vyžadují od provozovatelů čas a investice na jejich vývoj i na zřízení požadovaných nezávislých subjektů pro monitorování. Zástupci malých a středních podniků zdůrazňují význam a užitečnost kodexů chování, které jsou přizpůsobeny jejich situaci a nepředstavují neúměrné náklady.

Obchodní sdružení v řadě odvětví tudíž zavádějí jiné druhy samoregulačních nástrojů, např. kodexy osvědčených postupů nebo pokyny. I když tyto nástroje mohou poskytnout užitečné informace, nemají souhlas úřadů pro ochranu osobních údajů a nemohou sloužit jako nástroj, který pomůže prokázat soulad s nařízením GDPR.

Rada zdůrazňuje, že kodexy chování musí věnovat zvláštní pozornost zpracování osobních údajů dětí a zdravotních údajů. Komise podporuje kodex(y) chování, který (které) by harmonizoval(y) přístup v oblasti zdraví a výzkumu a usnadnil(y) by přeshraniční zpracování osobních údajů[98]. Sbor pracuje na schvalování návrhu požadavků na akreditaci subjektů pro monitorování kodexů chování, které předložila řada úřadů pro ochranu osobních údajů[99]. Jakmile budou nadnárodní nebo unijní kodexy chování připraveny k předložení úřadům pro ochranu osobních údajů ke schválení, projdou konzultací sboru. Rychlé zavedení nadnárodních kodexů chování je zvláště důležité pro oblasti, které zahrnují zpracování značného množství údajů (např. cloud computing) nebo citlivých údajů (např. zdraví/výzkum).

- Vydávání osvědčení

Vydávání osvědčení může být užitečným nástrojem k prokázání souladu s konkrétními požadavky nařízení GDPR. Může zvýšit právní jistotu pro podniky a celkově podpořit nařízení GDPR.

---

[96] https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_cs.

[97] Viz zpráva skupiny více zúčastněných stran.

[98] Viz opatření oznámená v Evropské strategii pro data, s. 30.

[99] Podle čl. 41 odst. 3 nařízení GDPR. Viz stanoviska Evropského sboru pro ochranu osobních údajů: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_cs

Jak upozorňuje studie o vydávání osvědčení zveřejněná v dubnu 2019[100], cílem by mělo být usnadnit osvojování příslušných systémů. Vývoj systémů vydávání osvědčení v EU bude podporován pokyny, které sbor vydá ke kritériím pro vydávání osvědčení[101] a k akreditaci subjektů pro vydávání osvědčení[102].

Záměrná bezpečnost a ochrana osobních údajů jsou klíčovými prvky, které je třeba zohlednit v systémech vydávání osvědčení podle nařízení GDPR, a těžily by ze společného a ambiciózního přístupu v celé EU. Komise bude i nadále podporovat stávající kontakty mezi Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA), úřady pro ochranu osobních údajů a sborem.

Pokud jde o kybernetickou bezpečnost, Komise po přijetí aktu o kybernetické bezpečnosti požádala agenturu ENISA, aby připravila dva systémy vydávání osvědčení, včetně jednoho systému pro cloudové služby[103]. Jsou zvažovány další systémy týkající se kybernetické bezpečnosti služeb a produktů pro spotřebitele. Ačkoli tyto systémy vydávání osvědčení zřízené podle aktu o kybernetické bezpečnosti výslovně neupravují ochranu osobních údajů a soukromí, přispívají ke zvýšení důvěry spotřebitelů v digitální služby a produkty. Tyto systémy mohou prokázat dodržování záměrných zásad bezpečnosti, jakož i provádění vhodných technických a organizačních opatření týkajících se bezpečnosti zpracování osobních údajů.

- Standardní smluvní doložky

Komise pracuje na standardních smluvních doložkách mezi správci a zpracovateli[104], a to i s ohledem na modernizaci standardních smluvních doložek pro mezinárodní předávání údajů (viz oddíl 7.2). Akt Unie přijatý Komisí bude mít závazný celounijní účinek, který zajistí plnou harmonizaci a právní jistotu.

6 POUŽITÍ NAŘÍZENÍ GDPR NA NOVÉ TECHNOLOGIE

Technologicky neutrální rámec otevřený novým technologiím

Nařízení GDPR je technologicky neutrální, umožňující budování důvěry a založené na zásadách[105]. Tyto zásady, včetně zákonného a transparentního zpracování, omezení účelu a minimalizace údajů, poskytují pevný základ pro ochranu osobních údajů bez ohledu na používané operace a techniky zpracování.

Členové skupiny více zúčastněných stran uvádějí, že nařízení GDPR má pozitivní dopad na vývoj nových technologií a poskytuje dobrý základ pro inovace. Nařízení GDPR je považováno za nezbytný a flexibilní nástroj k zajištění vývoje nových

100 https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en.

101 https://edpb.europa.eu/our-work-tools/our-documents/nasoki/guidelines-12018-certification-and-identifying-certification_cs.

102 https://edpb.europa.eu/our-work-tools/our-documents/pokyny/guidelines-42018-accreditation-certification-bodies-under_cs. Některé dozorové úřady již své požadavky na akreditaci sboru předložily, a to jak pro kontrolní orgány pro kodexy chování, tak pro subjekty pro vydávání osvědčení. Viz přehled na adrese: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_cs.

103 https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe.

104 Čl. 28 odst. 7 nařízení GDPR.

105 Jak připomněla Rada, Evropský parlament a sbor ve svých příspěvcích k hodnocení.

technologií v souladu se základními právy. Provádění jeho základních zásad je obzvláště zásadní pro intenzivní zpracování osobních údajů. Technologicky neutrální přístup nařízení GDPR založený na rizicích zajišťuje úroveň ochrany osobních údajů, která je přiměřená pro řešení rizika zpracování, a to i prostřednictvím vznikajících technologií.

Zúčastněné strany zejména uvádějí, že zásady nařízení GDPR týkající se omezení účelu a dalšího slučitelného zpracování, minimalizace údajů, omezení uložení, transparentnosti, odpovědnosti a podmínek, za nichž lze legálně použít automatizované rozhodovací procesy[106], řeší do značné míry obavy související s využíváním umělé inteligence.

V možném budoucím rámci pro umělou inteligenci a při provádění datové strategie bude rovněž uplatněn přístup založený na nařízení GDPR, který obstojí i v budoucnu a bude založen na rizicích. Cílem datové strategie je podpora dostupnosti údajů a vytvoření společných evropských datových prostor podporovaných službami federativní cloudové infrastruktury. Pokud jde o osobní údaje, nařízení GDPR poskytuje hlavní právní rámec, v němž lze v jednotlivých případech navrhnout účinná řešení v závislosti na povaze a obsahu každého datového prostoru.

Nařízení GDPR zvýšilo povědomí o ochraně osobních údajů jak v rámci EU, tak mimo ni, a přimělo společnosti k tomu, aby při inovacích své postupy přizpůsobily zásadám ochrany osobních údajů. Organizace občanské společnosti však poukazují na to, že ačkoli je dopad nařízení GDPR na vývoj nových technologií pozitivní, postupy velkých digitálních hráčů se zatím zásadně nezměnily směrem ke zpracování, které je příznivější pro ochranu soukromí. Významným prvkem ochrany fyzických osob je silné a účinné prosazování nařízení GDPR ve vztahu k velkým digitálním platformám a integrovaným společnostem, a to i v oblastech, jako je reklama na internetu a mikrocílení.

Komise analyzuje širší otázky související s chováním velkých digitálních hráčů na trhu v kontextu balíčku předpisů aktu o digitálních službách[107]. Pokud jde o výzkum v oblasti sociálních médií, Komise připomíná, že nařízení GDPR nelze používat jako omluvu ze strany platforem sociálních médií k omezení přístupu výzkumných pracovníků a ověřovatelů faktů k neosobním údajům, jako jsou statistiky o tom, které cílené inzeráty byly zaslány kterým kategoriím osob, kritéria pro vypracování tohoto zacílení, informace o falešných účtech atd.

Během pandemie COVID-19 byl technologicky neutrální přístup nařízení GDPR, který obstojí v budoucnosti, podroben testu a ukázal se jako úspěšný. Jeho pravidla založená na zásadách podporovala vývoj nástrojů pro boj proti šíření viru a sledování jeho šíření.

Problémy, které je třeba řešit

Vývoj a používání nových technologií tyto zásady nezpochybňují. Problémy leží ve vyjasnění, jak osvědčené zásady uplatnit na konkrétní technologie, jako je umělá inteligence, technologie blockchain, internet věcí, rozpoznávání obličeje nebo kvantová výpočetní technika.

---

[106] Zúčastněné strany však poznamenávají, že ne všechny automatizované rozhodovací procesy v kontextu umělé inteligence spadají do působnosti článku 22 nařízení GDPR.

[107] https://ec.europa.eu/commission/presscorner/detail/cs/ip_20_962.

V této souvislosti Evropský parlament a Rada zdůraznily potřebu průběžného sledování s cílem objasnit, jak se nařízení GDPR vztahuje na nové technologie a velké technologické společnosti. Zúčastněné strany navíc varují, že posouzení toho, zda je nařízení GDPR pro daný účel vhodné, vyžaduje neustálé sledování.

Zúčastněné strany z průmyslu zdůrazňují, že inovace vyžadují, aby bylo nařízení GDPR uplatňováno na základě zásad, a to v souladu s jeho návrhem, a nikoli rigidně a formálně. Jsou toho názoru, že pokyny sboru, jak uplatňovat zásady, koncepce a pravidla nařízení GDPR na nové technologie, jako je umělá inteligence, technologie blockchain nebo internet věcí, by s přihlédnutím k přístupu založenému na rizicích pomohly poskytnout vyjasnění a větší právní jistotu. Tyto nástroje „měkkého“ práva jsou vhodné k tomu, aby doprovázely uplatňování nařízení GDPR na nové technologie, neboť zajišťují větší právní jistotu a mohou být přezkoumány v souladu s technologickým vývojem. Některé zúčastněné strany rovněž naznačují, že užitečné by mohly být odvětvové pokyny, jak uplatňovat nařízení GDPR na nové technologie.

Sbor uvedl, že bude i nadále posuzovat dopad nově vznikajících technologií na ochranu osobních údajů.

Zúčastněné strany rovněž zdůrazňují, že pro regulační orgány je důležité důkladně porozumět tomu, jak je technologie využívána, a zapojit se do dialogu s průmyslem o vývoji nově vznikajících technologií. Domnívají se, že přístup založený na tzv. regulačním pískovišti – jako prostředek k získání pokynů k uplatňování pravidel – by mohl být zajímavou možností vyzkoušet nové technologie a pomoci podnikům uplatňovat v nových technologiích záměrnou a standardní ochranu osobních údajů.

Pokud jde o další politická opatření, zúčastněné strany doporučují, aby veškeré budoucí návrhy politik týkající se umělé inteligence vycházely ze stávajících právních rámců a byly sladěny s nařízením GDPR. Před navržením nových normativních pravidel je třeba pečlivě posoudit potenciální konkrétní otázky, a to na základě relevantních důkazů.

Bílá kniha Komise o umělé inteligenci předkládá řadu možností politiky, k nimž měly zúčastněné strany předložit do 14. června 2020 svá stanoviska. Pokud jde o rozpoznávání obličeje, což je technologie, která může mít významný dopad na práva fyzických osob, bílá kniha připomněla stávající právní rámec a zahájila veřejnou diskusi o případných zvláštních okolnostech, které by mohly odůvodnit využití umělé inteligence k rozpoznávání obličeje a k jiným účelům biometrické identifikace na dálku na veřejných místech, a o společných zárukách.

7 MEZINÁRODNÍ PŘEDÁVÁNÍ ÚDAJŮ A CELOSVĚTOVÁ SPOLUPRÁCE

7.1 Soukromí: celosvětová problematika

Poptávka po ochraně osobních údajů nezná hranic, neboť lidé na celém světě si stále více střeží a oceňují soukromí a bezpečnost svých osobních údajů.

Zároveň je důležité, aby toky údajů pro fyzické osoby, vlády, společnosti a obecněji i celou společnost představovaly nevyhnutelný fakt v našem propojeném světě. Tvoří nedílnou součást obchodu, spolupráce mezi orgány veřejné moci a sociálních interakcí. V tomto ohledu současná pandemie COVID-19 rovněž upozorňuje na to, jak kritické je předávání a výměna osobních údajů pro mnoho zásadních činností,

včetně zajištění kontinuity vládních a obchodních operací (tím, že se umožní práce na dálku a další řešení, která do značné míry závisejí na informačních a komunikačních technologiích), rozvoje spolupráce v oblasti vědeckého výzkumu diagnostiky, léčby a vakcín a boje proti novým formám kyberkriminality, jako jsou on-line systémy podvodů nabízející padělané léčivé přípravky, které prý předcházejí onemocnění COVID-19 nebo jej léčí.

V tomto kontextu a více než kdy předtím musí jít ochrana soukromí ruku v ruce s usnadňováním toků údajů. EU se svým režimem ochrany osobních údajů, který spojuje otevřenost vůči mezinárodnímu předávání údajů s vysokou úrovní ochrany fyzických osob, má velmi dobré předpoklady pro podporu bezpečných a důvěryhodných toků údajů. Nařízení GDPR se již objevilo jako referenční bod na mezinárodní úrovni a působilo jako katalyzátor pro mnoho zemí na celém světě, aby zvážily zavedení moderních pravidel na ochranu soukromí.

Jedná se o skutečně celosvětový trend vyskytující se od Chile po Jižní Koreu, od Brazílie po Japonsko, od Keni po Indii, od Tuniska po Indonésii a od Kalifornie po Tchaj-wan, abychom zmínili alespoň několik příkladů. Tento vývoj je pozoruhodný nejen z kvantitativního, ale i z kvalitativního hlediska: mnoho právních předpisů v oblasti ochrany soukromí přijatých nedávno nebo právě přijímaných vychází ze základního souboru společných záruk, práv a mechanismů pro vymáhání práva, které sdílí EU. Ve světě, který se příliš často vyznačuje rozdílnými, pokud ne zcela protichůdnými regulačními přístupy, je tento trend směrem k celosvětovému sbližování velmi pozitivním vývojem, který přináší nové příležitosti ke zvýšení ochrany fyzických osob v Evropě a zároveň usnadňuje toky údajů a snižuje transakční náklady pro hospodářské subjekty.

V zájmu využití těchto příležitostí a provádění strategie stanovené ve sdělení z roku 2017 nazvaném „Výměna a ochrana osobních údajů v globalizovaném světě“[108] Komise výrazně zintenzivnila svou práci na mezinárodním rozměru soukromí při plném využití dostupné sady nástrojů k předávání údajů, jak je vysvětleno níže. To zahrnovalo aktivní zapojení klíčových partnerů s cílem dojít ke „zjištění odpovídající ochrany“ a přineslo důležité výsledky, jako je vytvoření největší oblasti volných a bezpečných toků údajů na světě mezi EU a Japonskem.

Kromě této práce na odpovídající ochraně Komise úzce spolupracovala s úřady pro ochranu osobních údajů ve sboru i s dalšími zúčastněnými stranami s cílem plně využít potenciálu pružných pravidel nařízení GDPR pro mezinárodní předávání údajů. Jedná se o modernizaci nástrojů, jako jsou standardní smluvní doložky, rozvoj systémů vydávání osvědčení, kodexy chování nebo správní ujednání pro výměnu údajů mezi orgány veřejné moci, jakož i vyjasnění klíčových pojmů týkajících se například územní působnosti unijních pravidel ochrany osobních údajů nebo používání tzv. „výjimek“ k předávání osobních údajů.

V neposlední řadě Komise zintenzivnila dialog v řadě dvoustranných, regionálních a mnohostranných fór s cílem podpořit celosvětovou kulturu respektování soukromí a rozvíjet prvky sbližování různých systémů ochrany soukromí. Komise se ve svém

[108] Sdělení Komise Evropskému parlamentu a Radě s názvem „Výměna a ochrana osobních údajů v globalizovaném světě“, 10. 1. 2017 (COM(2017) 7 final).

úsilí mohla opírat o aktivní podporu Evropské služby pro vnější činnost a sítě delegací EU ve třetích zemích a o diplomatické zastoupení v mezinárodních organizacích. To rovněž zajistilo soudržnost a větší doplňkovost mezi různými aspekty vnějšího rozměru politik EU – od obchodu po nové partnerství mezi EU a Afrikou.

7.2 Sada nástrojů GDPR pro předávání údajů

Jelikož se stále více soukromých a veřejných subjektů v rámci svých běžných operací spoléhá na mezinárodní toky údajů, je stále více zapotřebí flexibilních nástrojů, které lze přizpůsobit různým odvětvím, obchodním modelům a situacím, v nichž jsou předávány údaje. S ohledem na tyto potřeby nabízí nařízení GDPR modernizovanou sadu nástrojů, která usnadňuje předávání osobních údajů z EU do třetí země nebo mezinárodní organizaci, přičemž zajišťuje, aby údaje i nadále požívaly vysoké úrovně ochrany. Tato kontinuita ochrany je důležitá vzhledem k tomu, že v dnešním světě se údaje snadno pohybují přes hranice a ochrana zaručená nařízením GDPR by byla neúplná, pokud by byla omezena na zpracování uvnitř EU.

Pokud jde o kapitolu V nařízení GDPR, zákonodárce potvrdil architekturu pravidel pro předávání údajů, která již existovala podle směrnice 95/46: údaje mohou být předávány v případě, že Komise učinila zjištění odpovídající ochrany v souvislosti s třetí zemí nebo mezinárodní organizací, nebo v případě neexistence takového rozhodnutí tam, kde správce nebo zpracovatel v EU („vývozce údajů“) poskytli vhodné záruky, například prostřednictvím smlouvy s příjemcem („dovozcem údajů“). Kromě toho jsou nadále k dispozici zákonné důvody pro předávání údajů (tzv. výjimky) pro konkrétní situace, u nichž zákonodárce rozhodl, že vyvážení zájmů předání údajů za určitých podmínek umožňuje. Zároveň byla vyjasněna a zjednodušena stávající pravidla, například stanovením podrobných podmínek pro zjištění odpovídající ochrany nebo závazných podnikových pravidel, omezením požadavků na povolení na velmi málo konkrétních případů a úplným zrušením požadavků na ohlašování. Kromě toho byly zavedeny nové nástroje k předávání údajů, jako jsou kodexy chování nebo systémy vydávání osvědčení a byly rozšířeny možnosti využití stávajících nástrojů (např. standardní smluvní doložky).

Dnešní digitální ekonomika umožňuje zahraničním subjektům, aby se (na dálku, ale) přímo podílely na vnitřním trhu EU a soutěžily o evropské zákazníky a jejich osobní údaje. Pokud se zaměřují konkrétně na Evropany prostřednictvím nabídek zboží nebo služeb nebo sledování jejich chování, měly by dodržovat právo EU stejným způsobem jako provozovatelé v EU. To se odráží v článku 3 nařízení GDPR, který rozšiřuje přímou použitelnost unijních pravidel ochrany osobních údajů na určité operace zpracování správců a zpracovatelů mimo EU. Tím jsou zaručeny nezbytné záruky a navíc i rovné podmínky pro všechny společnosti působící na trhu EU.

Jeho široký dosah je jedním z důvodů, proč se účinky nařízení GDPR projevily i v jiných částech světa. Podrobné pokyny vydané sborem k územní působnosti nařízení GDPR jsou tudíž po komplexní veřejné konzultaci důležité, aby pomohly zahraničním

subjektům určit, zda a jaké činnosti zpracování přímo podléhají jeho zárukám, mimo jiné tím, že uvádějí konkrétní příklady[109].

Rozšíření oblasti působnosti práva EU v oblasti ochrany osobních údajů však samo o sobě nestačí k tomu, aby bylo zaručeno jeho dodržování v praxi. Jak zdůraznila i Rada[110], je zásadní zajistit dodržování předpisů zahraničními subjekty a účinné prosazování vůči nim. V tomto ohledu by mělo hrát klíčovou úlohu jmenování zástupce v EU (čl. 27 odst. 1 a 2 nařízení GDPR), na kterého se mohou obrátit fyzické osoby i dozorové úřady navíc k odpovědné společnosti působící v zahraničí[111] nebo namísto ní. Tento přístup, který je ve stále větší míře využíván i v jiných souvislostech[112], by se měl prosazovat důrazněji, aby byl vyslán jasný signál, že neexistence provozovny v EU nezbavuje zahraniční subjekty jejich odpovědnosti podle nařízení GDPR. Pokud tito provozovatelé nesplní svou povinnost jmenovat svého zástupce[113], měly by dozorové úřady využívat všech opatření k prosazování nařízení podle článku 58 nařízení GDPR (např. veřejná varování, dočasné nebo trvalé zákazy zpracování údajů v EU, vymáhání vůči společným správcům usazeným v EU).

A konečně je velmi důležité, aby sbor dokončil svou práci na dalším vyjasnění vztahu mezi článkem 3 o přímém použití nařízení GDPR a pravidly pro mezinárodní předávání údajů v kapitole V[114].

Rozhodnutí o odpovídající ochraně

Příspěvky obdržené od zúčastněných stran potvrzují, že rozhodnutí o odpovídající ochraně jsou i nadále základním nástrojem pro provozovatele v EU k bezpečnému předávání osobních údajů do třetích zemí[115]. Tato rozhodnutí poskytují nejkomplexnější, nejpřímočařejší a nákladově nejefektivnější řešení pro předávání údajů, neboť ta jsou považována za rovnocenná přenosům v rámci EU, a zajišťují tak bezpečný a volný tok osobních údajů bez dalších podmínek nebo potřeby povolení. Rozhodnutí o odpovídající ochraně tudíž pro provozovatele v EU otevírají obchodní kanály a usnadňují spolupráci mezi orgány veřejné moci a současně poskytují

---

[109] Evropský sbor pro ochranu osobních údajů (EDPB), Pokyny č. 2/2018 k místní působnosti nařízení GDPR, 12. 11. 2019. Pokyny se zabývají několika body vznesenými během veřejné konzultace, například výkladem kritérií pro zacílení a sledování.

[110] Viz postoj a zjištění Rady, body 34, 35 a 38.

[111] Viz čl. 27 odst. 4 a 80. bod odůvodnění nařízení GDPR („Vůči jmenovanému zástupci by se v případě neplnění povinností správcem nebo zpracovatelem mělo uplatnit vymáhací řízení.“).

[112] Návrh směrnice Evropského parlamentu a Rady, kterou se stanoví harmonizovaná pravidla pro jmenování právních zástupců za účelem shromažďování důkazů v trestním řízení, (COM/2018/226 final), článek 3, návrh nařízení Evropského parlamentu a Rady o prevenci šíření teroristického obsahu online (COM (2018) 640 final), čl. 16 odst. 2 a 3.

[113] Podle jednoho příspěvku k veřejné konzultaci je jedním z hlavních bodů, které je třeba uvést, „účinné prosazování a skutečné důsledky pro ty, kteří se rozhodli tento požadavek ignorovat, […] Je třeba zejména mít na paměti, že to rovněž staví podniky usazené v Unii do konkurenční nevýhody vůči podnikům, které nedodržují právní předpisy a jsou usazeny mimo Unii a s Unií obchodují.“ Viz obchodní partneři EU, podání ze dne 29. dubna 2020.

[114] Tohoto tématu se týkalo několik příspěvků k veřejné konzultaci, například pokud jde o předávání osobních údajů příjemcům mimo EU, ale zahrnuté do nařízení GDPR.

[115] Postoj a zjištění Rady, odstavec 17, příspěvek sboru, s. 5–6. Několik příspěvků k veřejné konzultaci, mimo jiné od řady podnikatelských sdružení (jako je Francouzské sdružení velkých společností, Digital Europe, Global Data Alliance/BSA, Computer & Communication Industry Association (CCIA) nebo Obchodní komora USA), vyzvalo k zintenzivnění práce na zjištěních odpovídající ochrany, zejména s důležitými obchodními partnery.

privilegovaný přístup na jednotný trh EU. Na základě praxe podle směrnice z roku 1995 nařízení GDPR výslovně umožňuje, aby bylo určení odpovídající ochrany provedeno ve vztahu k určitému území třetí země nebo ke konkrétnímu sektoru či odvětví v rámci třetí země (tzv. „částečná“ odpovídající ochrana).

Nařízení GDPR vychází ze zkušeností z minulých let a z vysvětlení poskytnutých Soudním dvorem tím, že stanoví podrobný katalog prvků, které Komise musí ve svém posouzení zohlednit. Standard odpovídající ochrany vyžaduje takovou úroveň ochrany, která je srovnatelná s úrovní ochrany zajištěnou v rámci EU (neboli „v zásadě rovnocenná“)[116]. Jedná se o komplexní posouzení systému třetí země jako celku, včetně podstaty ochrany soukromí, jejího účinného provádění a prosazování, jakož i pravidel přístupu orgánů veřejné moci k osobním údajům, zejména pro účely vymáhání práva a národní bezpečnosti[117].

To se rovněž odráží v pokynech přijatých bývalou pracovní skupinou zřízenou podle článku 29 (a potvrzených sborem), zejména v tzv. „referenčním rámci pro odpovídající ochranu“, který dále objasňuje prvky, jež Komise musí zohlednit při posuzování odpovídající ochrany, mimo jiné poskytnutím přehledu „základních záruk“ pro přístup orgánů veřejné moci k osobním údajům[118]. Referenční rámec vychází zejména z judikatury Evropského soudu pro lidská práva. I když standard „zásadní rovnocennosti“ neznamená doslovnou replikaci („fotokopii“) pravidel EU, vzhledem k tomu, že způsob zajištění srovnatelné úrovně ochrany se může lišit v závislosti na různých systémech ochrany soukromí, často odrážejících různé právní tradice, přesto vyžaduje silnou úroveň ochrany.

Tento standard je odůvodněn skutečností, že rozhodnutí o odpovídající ochraně v zásadě rozšiřuje na třetí zemi výhody jednotného trhu, pokud jde o volný tok údajů. To však též znamená, že mezi úrovní ochrany zajištěnou v dané třetí zemi budou někdy v porovnání s nařízením GDPR významné rozdíly, které bude třeba překlenout, například jednáním o dalších zárukách. Tyto záruky by měly být vnímány pozitivně, neboť ještě více posilují ochranu dostupnou fyzickým osobám v EU. Komise se zároveň shoduje se sborem na tom, že je důležité průběžně sledovat jejich uplatňování v praxi, včetně účinného prosazování úřadem pro ochranu osobních údajů ve třetí zemi[119].

Nařízení GDPR objasňuje, že rozhodnutí o odpovídající ochraně jsou „živé nástroje“, které by měly být průběžně sledovány a pravidelně přezkoumávány[120]. V souladu s těmito požadavky má Komise pravidelné výměny s příslušnými orgány s cílem

---

[116] Rozsudek Soudního dvora EU ze dne 6. října 2015 ve věci C-362/14, Maximillian Schrems v. Data Protection Commissioner (dále jen „*Schrems*“), body 73, 74 a 96. Viz rovněž 104. bod odůvodnění nařízení GDPR, který odkazuje na standard zásadní rovnocennosti.

[117] Čl. 45 odst. 2 a 104. bod odůvodnění nařízení GDPR. Viz rovněž věc *Schrems*, body 75 a 91.

[118] Referenční rámec pro odpovídající ochranu, WP 254 rev. 01, 6. února 2018 (k dispozici na adrese: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

[119] Příspěvek sboru, s. 5–6.

[120] Čl. 45 odst. 4 a 5 nařízení GDPR požadují, aby Komise průběžně sledovala vývoj ve třetích zemích a pravidelně – alespoň každé čtyři roky – provedla přezkum zjištění odpovídající ochrany. Rovněž dávají Komisi pravomoc zrušit, změnit nebo pozastavit rozhodnutí o odpovídající ochraně, pokud zjistí, že dotyčná země nebo mezinárodní organizace již nezajišťuje odpovídající úroveň ochrany. Čl. 97 odst. 2 písm. a) nařízení GDPR dále požaduje, aby Komise do roku 2020 předložila Evropskému parlamentu a Radě zprávu o hodnocení. Viz též rozsudek Soudního dvora EU ze dne 6. října 2015 ve věci C-362/14, *Maximillian Schrems* v. *Data Protection Commissioner*, bod 76.

proaktivně navazovat na nový vývoj. Například od přijetí rozhodnutí o štítu EU–USA na ochranu soukromí v roce 2016[121] provedla Komise spolu se zástupci sboru tři každoroční přezkumy s cílem posoudit všechny aspekty fungování rámce[122]. Tyto přezkumy vycházely z informací získaných prostřednictvím výměn s orgány USA, jakož i z informací od dalších zúčastněných stran, jako jsou úřady pro ochranu osobních údajů v EU, občanská společnost a obchodní sdružení. Umožnily zlepšit praktické fungování různých prvků rámce. Z širšího hlediska přispěly každoroční přezkumy k navázání širšího dialogu s administrativou USA o soukromí obecně a o omezeních a ochranných opatřeních, zejména pokud jde o národní bezpečnost.

V rámci prvního hodnocení nařízení GDPR musí Komise rovněž přezkoumat rozhodnutí o odpovídající ochraně přijatá podle směrnice z roku 1995[123]. Útvary Komise zahájily s každou z jedenácti dotčených zemí a území intenzivní dialog s cílem posoudit, jak se jejich systémy ochrany osobních údajů vyvinuly od přijetí rozhodnutí o odpovídající ochraně a zda splňují standard stanovený v nařízení GDPR. Potřeba zajistit kontinuitu takových rozhodnutí, která jsou klíčovým nástrojem obchodu a mezinárodní spolupráce, je jedním z faktorů, který podnítil několik těchto zemí a území k modernizaci a posílení jejich právních předpisů v oblasti ochrany soukromí. To je jistě vítaný vývoj. S některými z těchto zemí a území jsou projednávány další bezpečnostní záruky, které řeší příslušné rozdíly v ochraně.

Avšak vzhledem k tomu, že Soudní dvůr v rozsudku, který má být vynesen dne 16. července, možná poskytne vysvětlení, která by mohla být relevantní pro určité prvky standardu odpovídající ochrany, předloží Komise odděleně zprávu o hodnocení uvedených jedenácti rozhodnutí o odpovídající ochraně poté, co Soudní dvůr vynese rozsudek v dané věci[124].

Při provádění strategie stanovené ve sdělení z roku 2017 nazvaném „Výměna a

[121] Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí. Toto rozhodnutí o odpovídající ochraně je zvláštní případ, který se v případě neexistence obecných právních předpisů v oblasti ochrany osobních údajů v USA opírá o závazky přijaté zúčastněnými společnostmi (které jsou podle práva USA vynutitelné), že budou uplatňovat standardy ochrany osobních údajů stanovené v tomto ujednání. Štít na ochranu soukromí navíc vychází ze zvláštních prohlášení a ujištění vlády USA ohledně přístupu pro účely národní bezpečnosti, které tvoří základ zjištění odpovídající ochrany.

[122] Přezkumy proběhly v roce 2017 (zpráva Komise Evropskému parlamentu a Radě o prvním každoročním přezkumu fungování štítu EU–USA na ochranu soukromí, COM(2017) 611 final), v roce 2018 (zpráva Komise Evropskému parlamentu a Radě o druhém každoročním přezkumu fungování štítu EU–USA na ochranu soukromí, COM(2018) 860 final) a v roce 2019 (zpráva Komise Evropskému parlamentu a Radě o třetím každoročním přezkumu fungování štítu EU–USA na ochranu soukromí, COM(2019) 495 final).

[123] Tato stávající rozhodnutí o odpovídající ochraně se týkají zemí, které jsou úzce integrovány s Evropskou unií a jejími členskými státy (Švýcarsko, Andorra, Faerské ostrovy, Guernsey, Jersey, Ostrov Man), významných obchodních partnerů (např. Argentina, Kanada, Izrael) a zemí, které hrají průkopnickou roli v rozvoji právních předpisů o ochraně osobních údajů ve svém regionu (Nový Zéland, Uruguay).

[124] Věc C-311/18, Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems („Schrems II“), se týká žádosti o rozhodnutí o předběžné otázce týkající se tzv.standardních smluvních doložek. Některé prvky standardu odpovídající ochrany však může dále vyjasnit i Soudní dvůr. Slyšení v této věci se konalo dne 9. července 2019 a rozhodnutí bylo oznámeno na dne 16. července 2020.

ochrana osobních údajů v globalizovaném světě“ se Komise rovněž zapojila do nových dialogů o odpovídající ochraně[125]. Tyto práce již přinesly významné výsledky za účasti klíčových partnerů EU. V lednu 2019 přijala Komise rozhodnutí o odpovídající ochraně pro Japonsko, které je založeno na vysokém stupni sbližování, mimo jiné prostřednictvím konkrétních záruk, například v oblasti dalšího předávání, a prostřednictvím vytvoření mechanismu pro vyšetřování a vyřizování stížností fyzických osob na přístup vlády k osobním údajům pro účely vymáhání práva a národní bezpečnosti.

Jako první zjištění odpovídající ochrany přijaté v rámci nařízení GDPR poskytuje rámec sjednaný s Japonskem užitečný precedens pro budoucí rozhodnutí[126]. To zahrnuje i skutečnost, že na japonské straně bylo opětováno zjištěním o „odpovídající ochraně“ pro EU. Tato vzájemná zjištění odpovídající ochrany společně vytvářejí největší prostor bezpečných a volných toků osobních údajů na světě, čímž doplňují dohodu o hospodářském partnerství mezi EU a Japonskem. Tento mechanismus ve skutečnosti každý rok podporuje obchod se zbožím ve výši přibližně 124 miliard EUR a obchod se službami ve výši 42,5 miliardy EUR.

Řízení o odpovídající ochraně je v pokročilé fázi i s Jižní Koreou. Jedním z důležitých výsledků je nedávná legislativní reforma Jižní Korey, která vedla ke zřízení nezávislého úřadu pro ochranu osobních údajů, který má silné donucovací pravomoci. To ilustruje, jak může dialog o odpovídající ochraně přispět ke zvýšenému sbližování mezi unijními pravidly ochrany osobních údajů a takovými pravidly cizí země.

Komise plně souhlasí s výzvou zúčastněných stran zintenzivnit dialog s vybranými třetími zeměmi s ohledem na možná nová zjištění odpovídající ochrany[127]. Aktivně zkoumá tuto možnost s dalšími důležitými partnery v Asii, Latinské Americe a v sousedství, přičemž vychází ze současného trendu směrem k vzestupnému celkovému sbližování standardů v oblasti ochrany osobních údajů. Komplexní právní předpisy týkající se ochrany soukromí byly například přijaty nebo jsou v pokročilé fázi legislativního procesu v Latinské Americe (Brazílie, Chile) a slibný je vývoj v Asii (např. v Indii, Indonésii, Malajsii, na Šrí Lance, na Tchaj-wanu a v Thajsku), v Africe (např. v Etiopii a Keni), jakož i v zemích východního a jižního sousedství (např. v Gruzii a Tunisku). Bude-li to možné, Komise bude usilovat o dosažení komplexních

[125] Viz pozn. pod čarou 109. Komise vysvětlila, že při posuzování, se kterými třetími zeměmi by měl být veden dialog o odpovídající ochraně, budou brána v úvahu tato kritéria: i) rozsah (skutečných nebo potenciálních) obchodních vztahů EU s danou třetí zemí, včetně existence dohody o volném obchodu nebo probíhajících jednání; ii) rozsah toků osobních údajů z EU, který odráží zeměpisné a/nebo kulturní vazby; iii) průkopnická úloha země v oblasti ochrany soukromí a osobních údajů, která by mohla sloužit jako vzor pro další země v jejím regionu; a iv) celkové politické vztahy s touto zemí, zejména pokud jde o prosazování společných hodnot a sdílených cílů na mezinárodní úrovni.

[126] Usnesení Evropského parlamentu ze dne 13. prosince 2018 o odpovídající úrovni ochrany osobních údajů v Japonsku (2018/2979(RSP)), bod 27, příspěvek sboru, s. 5–6.

[127] Viz např. usnesení Evropského parlamentu ze dne 12. prosince 2017 nazvané „Směrem ke strategii v oblasti digitálního obchodu“ (2017/2065 (INI)), body 8 a 9, postoj Rady a zjištění ohledně uplatňování obecného nařízení o ochraně osobních údajů, 19. 12. 2019 (14994/1/19), bod 17, příspěvek sboru, s. 5.

rozhodnutí o odpovídající ochraně, která budou zahrnovat soukromý i veřejný sektor[128].

Kromě toho zavedlo nařízení GDPR i možnost, aby Komise přijala zjištění odpovídající ochrany pro mezinárodní organizace. V době, kdy některé mezinárodní organizace modernizují své systémy ochrany osobních údajů zavedením komplexních pravidel, jakož i mechanismů, které zajišťují nezávislý dohled a nápravu, by tato možnost mohla být prozkoumána poprvé.

Odpovídající ochrana hraje rovněž důležitou úlohu v souvislosti se vztahy se Spojeným královstvím po brexitu za předpokladu, že budou splněny příslušné podmínky. Představuje podpůrný faktor pro obchod, včetně digitálního obchodu, a zásadní předpoklad pro úzkou a ambiciózní spolupráci v oblasti vymáhání práva a bezpečnosti[129]. Vzhledem k významu toků údajů se Spojeným královstvím a jeho blízkosti k trhu EU je navíc vysoká míra sbližování mezi pravidly ochrany osobních údajů na obou stranách Lamanšského průlivu důležitým prvkem pro zajištění rovných podmínek. V souladu s politickým prohlášením o budoucím vztahu mezi EU a Spojeným královstvím provádí Komise v současné době posouzení odpovídající ochrany jak podle nařízení GDPR, tak podle směrnice o prosazování práva[130]. S ohledem na autonomní a jednostrannou povahu posouzení odpovídající ochrany probíhají tyto rozhovory odděleně od jednání o dohodě o budoucích vztazích mezi EU a Spojeným královstvím.

Komise rovněž vítá skutečnost, že mechanismy předávání údajů podobné zjištění odpovídající ochrany zavádějí další země. Často tak uznávají EU a země, pro něž Komise přijala rozhodnutí o odpovídající ochraně, jakožto bezpečné cílové země pro předávání údajů[131]. Na jedné straně roste počet zemí, které využívají rozhodnutí EU o odpovídající ochraně, a na druhé straně má tato forma uznání ze strany jiných zemí potenciál vytvořit síť zemí, kde údaje mohou proudit volně a bezpečně. Komise to pokládá za vítaný vývoj, který dále zvýší přínosy rozhodnutí o odpovídající ochraně pro třetí země a přispěje k celosvětovému sbližování. Tento druh synergií může rovněž užitečným způsobem přispět k rozvoji rámců pro bezpečný a volný tok údajů, například v souvislosti s iniciativou „Data Free Flow with Trust („volný tok údajů s důvěrou“) (viz níže).

Vhodné záruky

Nařízení GDPR stanoví řadu dalších nástrojů k předávání údajů, které přesahují komplexní řešení zjištění odpovídající ochrany. Flexibilita této „sady nástrojů“ je

[128] Jak rovněž požadovala Rada, viz postoj Rady a zjištění ohledně uplatňování obecného nařízení o ochraně osobních údajů, 19. 12. 2019 (14994/1/19), body 17 a 40. To však vyžaduje, aby byly splněny podmínky pro zjištění odpovídající ochrany týkající se předávání údajů orgánům veřejné moci, a to i pokud jde o nezávislý dohled.

[129] Viz pokyny pro jednání připojené k rozhodnutí Rady o zmocnění k zahájení jednání se Spojeným královstvím Velké Británie a Severního Irska o nové dohodě o partnerství (ST 5870/20 ADD 1 REV 3), body 13 a 118.

[130] Viz revidované znění politického prohlášení, které stanoví rámec budoucích vztahů mezi Evropskou unií a Spojeným královstvím, jak bylo dohodnuto na úrovni vyjednavačů dne 17. října 2019, body 8–10 (k dispozici na adrese https://ec.europa.eu/commission/sites/beta-political/files/revised_political_declaration.pdf).

[131] Například Argentina, Kolumbie, Izrael, Švýcarsko nebo Uruguay.

prokázána článkem 46 nařízení GDPR, který upravuje předávání údajů na základě „vhodných záruk“, včetně vymahatelných práv subjektu údajů a účinné právní ochrany. Aby byly zaručeny vhodné záruky, jsou k dispozici různé nástroje, které uspokojují jak potřeby komerčních provozovatelů, tak i potřeby veřejných subjektů v oblasti předávání údajů.

- Standardní smluvní doložky

První skupina těchto nástrojů se týká smluvních nástrojů, kterými mohou být buď individuálně přizpůsobené ad hoc doložky o ochraně osobních údajů sjednané mezi vývozcem údajů z EU a dovozcem údajů mimo EU, povolené příslušným úřadem pro ochranu osobních údajů (čl. 46 odst. 3 písm. a) nařízení GDPR), nebo vzorová ustanovení předem schválená Komisí (čl. 46 odst. 2 písm. c) a d) nařízení GDPR[132]). Nejdůležitější z těchto nástrojů jsou tzv. standardní smluvní doložky, tj. vzorové doložky o ochraně osobních údajů, které vývozce údajů a dovozce údajů mohou začlenit do svých smluvních ujednání (např. do smlouvy o poskytování služeb vyžadující předávání osobních údajů) na dobrovolném základě a které stanoví požadavky související s vhodnými zárukami.

Standardní smluvní doložky představují zdaleka nejčastěji používaný mechanismus předávání údajů[133]. Opírají se o ně tisíce společností v EU, aby poskytovaly širokou škálu služeb svým klientům, dodavatelům, partnerům a zaměstnancům, včetně služeb nezbytných pro fungování hospodářství. Jejich široké využití naznačuje, že jsou velmi užitečné pro podniky v jejich úsilí o dodržování předpisů, a zejména pro společnosti, které nemají zdroje k vyjednávání jednotlivých smluv s každým ze svých obchodních partnerů. Prostřednictvím standardizace a předběžného schválení poskytují standardní smluvní doložky společnostem snadno proveditelný nástroj ke splnění požadavků na ochranu osobních údajů v souvislosti s jejich předáváním.

Stávající sady standardních smluvních doložek[134] byly přijaty a schváleny na základě směrnice z roku 1995. Tyto standardní smluvní doložky zůstávají v platnosti tak dlouho, dokud nebudou v případě potřeby změněny, nahrazeny nebo zrušeny rozhodnutím Komise (čl. 46 odst. 5 nařízení GDPR). Nařízení GDPR rozšiřuje možnosti používat standardní smluvní doložky v rámci EU i pro mezinárodní předávání údajů. Komise spolupracuje se zúčastněnými stranami s cílem využít těchto

---

[132] Standardní smluvní doložky pro mezinárodní předávání údajů vyžadují vždy schválení ze strany Komise, ale může je vypracovat sama Komise nebo vnitrostátní úřad pro ochranu osobních údajů. Všechny stávající standardní smluvní doložky spadají do první kategorie.

[133] Podle výroční zprávy o řízení ochrany soukromí za rok 2019, kterou vypracovaly organizace IAPP a EY, „jsou nejoblíbenějšími z těchto nástrojů [k předávání údajů] – rok co rok – převážně standardní smluvní doložky: 88 % respondentů v průzkumu v tomto roce uvedlo standardní smluvní doložky jako svou nejlepší metodu pro předávání údajů mimo jejich území, po ní následovala dodržování štítu EU–USA na ochranu soukromí (60 %). V případě respondentů předávajících údaje z EU do Spojeného království (52 %) 91 % uvádí, že mají v úmyslu používat standardní smluvní doložky k plnění předpisů o předávání údajů po brexitu“.

[134] V současnosti existují tři sady standardních smluvních doložek přijatých Komisí pro předávání osobních údajů do třetích zemí: dvě pro předávání údajů správcem v EHP správci se sídlem mimo EHP a jedna pro předávání údajů správcem v EHP zpracovateli se sídlem mimo EHP. V roce 2016 byly pozměněny v návaznosti na rozsudek Soudního dvora ve věci *Schrems I* (C-362/14), aby byla odstraněna veškerá omezení týkající příslušných dozorových úřadů při výkonu jejich pravomocí dohlížet na předávání údajů. Viz https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

možností a aktualizovat stávající doložky[135]. S cílem zajistit, aby budoucí podoba standardních smluvních doložek byla vhodná pro daný účel, shromažďovala Komise zpětnou vazbu ohledně zkušeností zúčastněných stran s těmito doložkami prostřednictvím skupiny více zúčastněných stran pro nařízení GDPR a specializovaného pracovního setkání konaného v září 2019, ale také prostřednictvím četných kontaktů se společnostmi, které standardní smluvní doložky používají, jakož i s organizacemi občanské společnosti. Sbor rovněž aktualizuje řadu pokynů, které by mohly být relevantní pro přezkum standardních smluvních doložek, například pokyny k pojmům správce a zpracovatele.

Na základě získané zpětné vazby pracují útvary Komise v současné době na revizi standardních smluvních doložek. V této souvislosti bylo určeno několik oblastí ke zlepšení, zejména pokud jde o tyto aspekty:

1. Aktualizace standardních smluvních doložek s ohledem na nové požadavky zavedené nařízením GDPR, například požadavky týkající se vztahu mezi správcem a zpracovatelem podle článku 28 nařízení GDPR (zejména povinnosti zpracovatele), povinnosti dovozce údajů týkající se transparentnosti (pokud jde o nezbytné informace, které mají být subjektu údajů poskytnuty) atd.
2. Řešení řady scénářů předávání údajů, na které se nevztahují současné standardní smluvní doložky, např. předávání údajů zpracovatelem v EU (pod)zpracovateli z třetí země, ale také například situace, kdy se správce nachází mimo EU[136].
3. Lepší vyjádření reality operací zpracování v moderní digitální ekonomice, kde tyto operace často zahrnují více dovozců a vývozců údajů, dlouhé a často složité řetězce zpracování, vyvíjející se obchodní vztahy atd. V zájmu zohlednění takových situací patří ke zkoumaným řešením například možnost povolit v průběhu platnosti smlouvy podpis standardních smluvních doložek několika stranami nebo přistoupení nových stran.

Při řešení těchto bodů Komise rovněž zvažuje způsoby, jak učinit stávající „architekturu“ standardních smluvních doložek přívětivější pro uživatele, například nahrazením velkého počtu sad těchto doložek jediným komplexním dokumentem. Úkolem je dosáhnout dobré rovnováhy mezi potřebou jasnosti a určitým stupněm standardizace na jedné straně a na straně druhé nezbytnou flexibilitou, která umožní, aby doložky byly využívány řadou provozovatelů s různými požadavky, v různých kontextech a pro různé druhy předávání údajů.

Dalším důležitým aspektem, který je třeba vzít v úvahu, je s ohledem na stávající soudní spor před Soudním dvorem[137] případná potřeba dále vyjasnit záruky, pokud jde o přístup zahraničních orgánů veřejné moci k údajům předávaným na základě

[135] Viz rovněž příspěvek sboru, s. 6–7. Rada podobně vyzvala Komisi, aby „v blízké budoucnosti přezkoumala a zrevidovala [standardní smluvní doložky] za účelem zohlednění potřeb správců a zpracovatelů“. Viz postoj a zjištění Rady.

[136] K tomuto poslednímu scénáři se vyjádřilo několik příspěvků k veřejné konzultaci, v nichž byly často vyjádřeny obavy, že pokud by zpracovatelé v EU museli v rámci svých vztahů se správci z třetích zemí zajistit vhodné záruky, konkurenčně by je to znevýhodnilo vůči zahraničním zpracovatelům, kteří nabízejí podobné služby.

[137] Viz věc Schrems II.

standardních smluvních doložek, zejména pro účely národní bezpečnosti. To může zahrnovat požadavek, aby dovozce údajů nebo vývozce údajů nebo oba přijali opatření a aby byla v této souvislosti vyjasněna úloha úřadů pro ochranu osobních údajů. I když revize standardních smluvních doložek značně pokročila, bude nutné se zohledněním jakéhokoli případného dalšího požadavku v revidovaných doložkách vyčkat na rozsudek Soudního dvora a teprve poté bude možné předložit návrh rozhodnutí o nové sadě standardních smluvních doložek sboru k vyjádření a poté jej navrhnout k přijetí prostřednictvím „postupu projednávání ve výborech“[138].

Komise je zároveň v kontaktu s mezinárodními partnery, kteří vyvíjejí podobné nástroje[139]. Tento dialog, který umožňuje výměnu zkušeností a osvědčených postupů, by mohl významně přispět k dalšímu vývoji sbližování „v praxi“, a tím usnadnit dodržování pravidel přeshraničního předávání údajů pro společnosti působící v různých regionech světa.

- Závazná podniková pravidla

Dalším důležitým nástrojem jsou tzv. závazná podniková pravidla. Jedná se o právně závazné politiky a ujednání vztahující se na členy skupiny podniků, včetně jejich zaměstnanců (čl. 46 odst. 2 písm. b) a článek 47 nařízení GDPR). Používání závazných podnikových pravidel umožňuje volný pohyb osobních údajů mezi jednotlivými členy skupiny po celém světě, aniž by bylo nutné uzavírat smluvní ujednání mezi jednotlivými podniky, a zároveň zajišťuje, aby byla v celé skupině dodržována stejně vysoká úroveň ochrany osobních údajů. Nabízejí obzvláště kvalitní řešení pro složité a velké skupiny společností a pro úzkou spolupráci podniků, které si vyměňují údaje v několika jurisdikcích. Na rozdíl od směrnice z roku 1995 mohou být závazná podniková pravidla podle nařízení GDPR využívána skupinou podniků, které vykonávají společnou hospodářskou činnost, ale netvoří součást téže skupiny společností.

Z procesního hlediska musí být závazná podniková pravidla schválena příslušnými úřady pro ochranu osobních údajů na základě nezávazného stanoviska sboru[140]. Za účelem řízení tohoto procesu přezkoumal sbor s ohledem na nařízení GDPR „referenční rámce“ (stanovující podstatné standardy) závazných podnikových pravidel pro správce[141] a zpracovatele[142] a tyto dokumenty i nadále aktualizuje na základě praktických zkušeností, které dozorové úřady získaly. Rovněž přijal různé dokumenty s pokyny, které mají pomoci žadatelům a zefektivnit proces podávání

[138] V souladu s čl. 46 odst. 2 písm. c) nařízení GDPR musí být standardní smluvní doložky přijímány přezkumným postupem stanoveným v článku 5 nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13). Jedná se zejména o kladné rozhodnutí výboru složeného ze zástupců členských států.

[139] To zahrnuje například práci, kterou v současné době vykonávají členské státy sdružení ASEAN na tvorbě „vzorových smluvních doložek“. Viz ASEAN, Key Approaches for ASEAN Cross Border Data Flows Mechanism (Klíčové přístupy pro mechanismus sdružení ASEAN pro přeshraniční toky údajů (k dispozici na adrese: https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf).

[140] Přehled dosavadních stanovisek Evropského sboru pro ochranu osobních údajů, viz https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_cs.

[141] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109.

[142] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110.

žádostí a schvalování v případě závazných podnikových pravidel[143]. Podle sboru je v současnosti ke schválení připraveno více než 40 závazných podnikových pravidel, z nichž polovina má být schválena do konce roku 2020[144]. Je důležité, aby úřady pro ochranu osobních údajů pokračovaly v práci na dalším zjednodušení procesu schvalování, neboť délku těchto postupů zúčastněné strany často zmiňují jako praktickou překážku širšího využívání závazných podnikových pravidel.

A konečně, pokud jde konkrétně o závazná podniková pravidla schválená úřadem pro ochranu osobních údajů ve Spojeném království, Úřadem komisaře pro informace (Information Commissioner Office), budou je společnosti moci nadále používat jako platný mechanismus předávání údajů podle nařízení GDPR po skončení přechodného období podle dohody o vystoupení Spojeného království z EU, avšak pouze v případě, že budou pozměněna tak, aby jakékoli spojení s právním řádem Spojeného království bylo nahrazeno vhodnými odkazy na právnické osoby a příslušné úřady v rámci EU. Schválení jakýchkoli nových závazných podnikových pravidel by mělo být požadováno od jednoho z dozorových úřadů v EU.

- Mechanismy vydávání osvědčení a kodexy chování

Kromě modernizace a rozšíření používání již existujících nástrojů k předávání údajů zavedlo nařízení GDPR i nové nástroje, čímž rozšířilo možnosti pro mezinárodní předávání údajů. Patří sem používání (za určitých podmínek) schválených kodexů chování a mechanismů vydávání osvědčení (např. pečetí a známek dokládajících ochranu údajů) pro zajištění vhodných záruk. Jedná se o nástroje vycházející zdola nahoru, které umožňují řešení na míru, jako mechanismus obecné odpovědnosti (viz články 40 až 42 nařízení GDPR) a konkrétně pro mezinárodní předávání údajů, odrážející například specifické rysy a potřeby daného sektoru nebo odvětví, nebo konkrétních toků údajů. Tím, že budou povinnosti nastaveny podle rizik, mohou být kodexy chování též velmi užitečným a nákladově efektivním způsobem, jak malé a střední podniky mohou splnit své povinnosti vyplývající z nařízení GDPR.

Pokud jde o mechanismy vydávání osvědčení, sbor sice přijal pokyny na podporu jejich používání v rámci EU, avšak jeho práce na tvorbě kritérií pro schvalování mechanismů vydávání osvědčení jako nástrojů pro mezinárodní předávání údajů stále probíhají. Totéž platí pro kodexy chování, u nichž sbor v současné době pracuje na pokynech k jejich používání jako nástroje k předávání údajů.

Vzhledem k tomu, že je důležité poskytovat provozovatelům širokou škálu nástrojů pro předávání údajů, které jsou přizpůsobeny jejich potřebám, a vzhledem k potenciálu, který mají zejména mechanismy vydávání osvědčení pro usnadnění předávání údajů při současném zajištění vysoké úrovně ochrany osobních údajů, vyzývá Komise naléhavě sbor, aby co nejdříve dokončil své pokyny v tomto ohledu. To se týká jak hmotněprávních (kritérií), tak procesních aspektů (schválení, sledování atd.). Zúčastněné strany vyjádřily velký zájem o tyto mechanismy předávání údajů a měly by být schopny plně využívat sadu podle nařízení GDPR. Pokyny sboru by

[143] Tyto dokumenty byly přijaty (bývalou pracovní skupinou zřízenou podle článku 29) po vstupu nařízení GDPR v platnost, ale před koncem přechodného období. Viz WP263 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056), WP264 (https://edpb.europa.eu/sites/edpb/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf), WP265 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848).

[144] Příspěvek sboru, s. 7.

rovněž přispěly k prosazování modelu EU pro ochranu osobních údajů v celosvětovém měřítku a podpořily by sbližování, neboť jiné systémy ochrany soukromí používají podobné nástroje.

Ze stávajícího úsilí v oblasti normalizace v oblasti ochrany soukromí lze vyvodit cenné ponaučení, a to jak na evropské, tak mezinárodní úrovni. Zajímavým příkladem je nedávno zveřejněná mezinárodní norma ISO 27701[145], jejímž cílem je pomoci podnikům splnit požadavky na ochranu soukromí a řídit rizika spojená se zpracováním osobních údajů prostřednictvím „systémů řízení informací o soukromí". Ačkoli vydávání osvědčení podle této normy jako takové nesplňuje požadavky článků 42 a 43 nařízení GDPR, může uplatňování systémů řízení informací o soukromí přispět k odpovědnosti, a to i v souvislosti s mezinárodním předáváním údajů.

- Mezinárodní dohody a správní ujednání

Nařízení GDPR rovněž umožňuje zajistit vhodné záruky pro předávání údajů mezi orgány veřejné moci nebo veřejnými subjekty na základě mezinárodních dohod (čl. 46 odst. 2 písm. a)) nebo správních ujednání (čl. 46 odst. 3 písm. b)). Oba nástroje musí zaručit stejný výsledek, pokud jde o záruky, včetně vymahatelných práv subjektu údajů a účinných právních prostředků, avšak liší se svou právní povahou a postupem přijímání.

Na rozdíl od mezinárodních dohod, které vytvářejí závazné povinnosti podle mezinárodního práva, jsou správní ujednání (např. ve formě memoranda o porozumění) obvykle nezávazná, a vyžadují proto předchozí schválení příslušným úřadem pro ochranu osobních údajů (viz také 108. bod odůvodnění nařízení GDPR). Jeden z prvních příkladů se týká správního ujednání o předávání osobních údajů mezi orgány pro finanční dohled v EHP a třetích zemích spolupracujícími pod záštitou Mezinárodní organizace komisí pro cenné papíry (IOSCO), k němuž sbor vydal své stanovisko[146] počátkem roku 2019. Sbor od té doby dále rozvíjel svůj výklad „minimálních záruk", které mezinárodní dohody (o spolupráci) a správní ujednání mezi orgány veřejné moci nebo veřejnými subjekty (včetně mezinárodních organizací) musí zajistit, aby vyhověly požadavkům článku 46 nařízení GDPR. Dne 18. ledna 2020 přijal návrh pokynů[147], v němž se zabýval žádostí členských států o další objasnění a pokyny ohledně toho, co lze považovat za vhodné záruky pro předávání údajů mezi orgány veřejné moci[148]. Sbor důrazně doporučuje, aby orgány

---

[145] Seznam konkrétních požadavků tvořících tuto normu ISO je k dispozici na adrese: https://www.iso.org/standard/71670.html.

[146] Evropský sbor pro ochranu osobních údajů, stanovisko č. 4/2019 k návrhu správního ujednání pro předávání osobních údajů mezi úřady pro finanční dohled v Evropském hospodářském prostoru (dále „EHP") a úřady pro finanční dohled mimo Evropský hospodářský prostor, 12. 2. 2019.

[147] Evropský sbor pro ochranu osobních údajů, pokyny 2/2020 k čl. 46 odst. 2 písm. a) a čl. 46 odst. 3 písm. b) nařízení 2016/679 pro předávání osobních údajů mezi orgány veřejné správy a veřejnými subjekty EHP a mimo Evropský hospodářský prostor (návrh k dispozici na adrese: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en). Podle Evropského sboru pro ochranu osobních údajů „[příslušný dozorový úřad] založí své přezkoumání na obecných doporučeních uvedených v těchto pokynech, ale může rovněž požádat o více záruk v závislosti na konkrétním případu." Evropský sbor pro ochranu osobních údajů tento návrh pokynů předložil k veřejné konzultaci, která skončila dne 18. května 2020.

[148] Postoj a zjištění Rady, bod 20.

veřejné moci používaly tyto pokyny jako referenční bod pro svá jednání se třetími stranami[149].

Pokyny prokazují flexibilitu při navrhování takových nástrojů, včetně důležitých aspektů, jako je dohled[150] a náprava[151]. To by mělo orgánům veřejné moci umožnit, aby překonaly potíže například tím, že zajistí vymahatelná práva subjektů údajů prostřednictvím nezávazných ujednání. Důležitým prvkem takových ujednání je jejich průběžné sledování příslušným úřadem pro ochranu osobních údajů – podporovaným požadavky na informace a vedení záznamů – a pozastavení toků údajů v případě, že v praxi již nelze zajistit vhodné záruky.

Výjimky

A konečně, nařízení GDPR objasňuje použití tzv. „výjimek“. Jedná se o konkrétní důvody pro předávání údajů (např. výslovný souhlas[152], plnění smlouvy nebo důležité důvody veřejného zájmu) uznané zákonem, o které se subjekty při neexistenci jiných nástrojů k předávání údajů a za určitých podmínek mohou opřít.

Za účelem objasnění použití těchto zákonných důvodů vydal sbor zvláštní pokyny[153] a vyložil článek 49 v řadě případů s ohledem na konkrétní scénáře předávání údajů[154]. Vzhledem k jejich výjimečnému charakteru se sbor domnívá, že výjimky je třeba v jednotlivých případech vykládat restriktivně. I přes jejich striktní výklad se tyto důvody týkají široké škály scénářů předávání údajů. To zahrnuje zejména předávání

---

[149] Současně Evropský sbor pro ochranu osobních údajů vyjasňuje, že orgány veřejné moci „se mohou i nadále opírat o další relevantní nástroje, které poskytují vhodné záruky v souladu s článkem 46 nařízení GDPR“. Pokud jde o volbu nástroje, Evropský sbor pro ochranu osobních údajů zdůrazňuje, že „[j]e třeba pečlivě posoudit, zda využít právně nezávazných správních ujednání k zajištění záruk ve veřejném sektoru, či nikoli, s ohledem na účel zpracování a povahu údajů, které jsou k dispozici. Pokud nejsou práva na ochranu osobních údajů a nápravu pro fyzické osoby v EHP stanovena ve vnitrostátním právu třetí země, měla by být dána přednost uzavření právně závazné dohody. Bez ohledu na typ přijatého nástroje musí být zavedená opatření účinná, aby mohlo být zajištěno řádné provádění, prosazování a dozor“ (bod 67).

[150] To může zahrnovat například kombinování vnitřních kontrol (se závazkem informovat druhou stranu o nesouladu) s nezávislým dohledem prostřednictvím externích nebo alespoň funkčně nezávislých mechanismů, jakož i s možností, aby předávající veřejný subjekt předávání údajů pozastavil nebo ukončil.

[151] To může zahrnovat například kvazisoudní, závazné mechanismy (např. rozhodčí řízení) nebo alternativní mechanismy řešení sporů spolu s možností, aby předávající orgán veřejné moci předávání osobních údajů pozastavil nebo ukončil, pokud se stranám nepodaří vyřešit spor smírně, a se závazkem přijímajícího veřejného subjektu vrátit nebo vymazat osobní údaje. Když zvolí alternativní mechanismy nápravy v závazných a vymahatelných nástrojích, protože neexistuje možnost zajistit účinnou soudní nápravu, doporučuje Evropský sbor pro ochranu osobních údajů před uzavřením těchto nástrojů požádat o radu příslušný dozorový úřad.

[152] Jedná se o změnu oproti směrnici 95/46, která pouze vyžadovala „nezpochybnitelný“ souhlas. Kromě toho se použijí obecné požadavky na souhlas podle čl. 4 odst. 11 nařízení GDPR.

[153] Evropský sbor pro ochranu osobních údajů, pokyny 2/2018 k výjimkám podle článku 49 nařízení (EU) 2016/679, 25. 5. 2018 (k dispozici na adrese: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_cs.pdf).

[154] To zahrnuje například mezinárodní předávání zdravotních údajů pro výzkumné účely v souvislosti s rozšířením onemocnění COVID-19. Viz Evropský sbor pro ochranu osobních údajů, pokyny 03/2020 ke zpracování údajů o zdravotním stavu pro účely vědeckého výzkumu v souvislosti s rozšířením onemocnění COVID-19, 21. 4. 2020 (k dispozici na adrese: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_cs.pdf).

údajů orgány veřejné moci i soukromými subjekty nutné z „důležitých důvodů veřejného zájmu“, například mezi orgány pro hospodářskou soutěž, finančními, daňovými či celními správami, útvary příslušnými v oblasti sociálního zabezpečení nebo veřejného zdraví, (například v případě vysledování kontaktů v souvislosti s nakažlivými chorobami nebo za účelem odstranění dopingu ve sportu)[155]. Další oblastí je oblast přeshraniční spolupráce pro účely vymáhání trestního práva, zejména pokud jde o závažnou trestnou činnost[156].

Sbor objasnil, že ačkoli relevantní veřejný zájem musí být uznán v právu EU nebo členských států, ukazatelem při posuzování existence veřejného zájmu podle čl. 49 odst. 1 písm. d) může být i „existence mezinárodní dohody nebo úmluvy, která uznává určitý cíl a stanovuje mezinárodní spolupráci pro dosažení takového cíle, jsou-li EU nebo členské státy smluvní stranou takové dohody nebo úmluvy“[157].

Rozhodnutí zahraničních soudů nebo úřadů: není důvodem pro předávání údajů

Kromě toho, že kapitola V nařízení GDPR pozitivně stanoví důvody pro předávání údajů, rovněž v článku 48 vyjasňuje, že příkazy soudů a rozhodnutí správních orgánů mimo EU *samy o sobě* takové důvody neposkytují, ledaže jsou uznány či učiněny vykonatelnými na základě mezinárodní dohody (např. smlouva o vzájemné právní pomoci). Jakékoli poskytnutí informací dožádaným subjektem v EU zahraničnímu soudu nebo úřadu v reakci na takový příkaz nebo rozhodnutí představuje mezinárodní předání údajů, které se musí opírat o jeden z uvedených nástrojů k předávání údajů[158].

Nařízení GDPR nepředstavuje „blokovací právní předpis“ a za určitých podmínek povoluje předání údajů v reakci na příslušnou žádost o vymáhání práva ze třetí země. Důležité je, že je to právo EU, co by mělo určit, zda tomu tak je a na základě kterých záruk se tato předání mohou uskutečnit.

Komise vysvětlila fungování článku 48 nařízení GDPR, včetně možného využití

---

155 Viz 112. bod odůvodnění.

156 Viz poznámka Evropské komise jménem Evropské unie jako *Amicus Curiae* nepodporující žádnou stranu ve věci US v. Microsoft, s. 15: „Právo Unie a členských států obecně uznává význam boje proti závažné trestné činnosti, a tím i prosazování trestního práva a mezinárodní spolupráce v tomto ohledu, jako cíl obecného zájmu. […] Článek 83 SFEU vymezuje několik oblastí trestné činnosti, které jsou obzvláště závažné a mají přeshraniční rozměr, např. nedovolený obchod s drogami.“ (k dispozici na adrese: https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf).

157 Evropský sbor pro ochranu osobních údajů, pokyny k výjimkám (pozn. pod čarou 153), s. 10. Evropský sbor pro ochranu osobních údajů dále objasnil, že ačkoli k předání údajů vycházejícímu z výjimky na základě veřejného zájmu nemůže docházet „ve velkém rozsahu“ nebo „systematicky“, ale musí se „omezit na konkrétní situace a […] [splnilo] přísné kritérium nezbytnosti“, není požadováno, aby bylo „příležitostné“.

158 To jasně vyplývá ze znění článku 48 nařízení GDPR („aniž jsou dotčeny jiné důvody pro převod podle této kapitoly“) a průvodního 115. bodu odůvodnění („[p]ředání údajů by mělo být povoleno jen tehdy, jsou-li splněny podmínky předání údajů do třetích zemí stanovené v tomto nařízení. Tak tomu může být mimo jiné v případě, kdy je sdělení údajů nezbytné z důležitého důvodu veřejného zájmu, jenž je uznán v právu Unie nebo členského státu, které se na správce vztahuje.“). Uznává to též Evropský sbor pro ochranu osobních údajů, viz pokyny k výjimkám (pozn. pod čarou 153), s. 5. Stejně jako v případě všech operací zpracování musí být splněny i další záruky podle nařízení (např. že se údaje předávají pro konkrétní účel, jsou relevantní, jsou omezené na nezbytný rozsah ve vztahu k účelu atd.).

výjimky ve veřejném zájmu v souvislosti s předávacím příkazem, který vydal zahraniční donucovací orgán ve věci *Microsoft* u Nejvyššího soudu USA[159] Komise ve svém podání zdůraznila, že EU má zájem na tom, aby spolupráce v oblasti vymáhání práva probíhala „v právním rámci, který zabrání kolizím norem, a aby byla založena na […] respektování základních zájmů všech stran při prosazování ochrany soukromí i práva“[160]. Konkrétně „z hlediska mezinárodního práva veřejného vyžaduje, aby byly uplatňovány zásady teritoriality a zdvořilosti podle mezinárodního práva veřejného, pokud orgán veřejné moci požaduje, aby společnost usazená v jeho jurisdikci předložila elektronické údaje uložené na serveru v cizí jurisdikci“[161].

To se rovněž odráží v návrhu nařízení o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech[162], který předložila Komise a který obsahuje zvláštní „ustanovení o zdvořilosti“, které umožňuje vznést námitku proti předávacímu příkazu, pokud by v případě jeho splnění došlo k rozporu s právními předpisy třetí země zakazujícími sdělení dotčených údajů z toho důvodu, že je to nezbytné pro ochranu základních práv dotčených fyzických osob[163].

Zajištění zdvořilosti je důležité vzhledem k tomu, že prosazování práva – v oblasti trestné činnosti, a zejména kyberkriminality – má stále více přeshraniční charakter, a proto často vyvolává otázky soudní příslušnosti a vytváří možné kolize norem[164]. Není žádným překvapením, že nejlepším způsobem řešení těchto otázek jsou mezinárodní dohody, které stanoví nezbytná omezení a záruky pro přeshraniční přístup k osobním údajům, včetně zajištění vysoké úrovně ochrany osobních údajů na straně žádajícího orgánu.

---

[159] Podání ve věci Microsoft (viz poznámka pod čarou 156). Jak vysvětlila Komise, nařízení GDPR tak činí smlouvy o vzájemné právní pomoci „upřednostňovanou možností“ pro předávání údajů, neboť tyto smlouvy „stanoví shromažďování důkazů na základě souhlasu a obsahují pečlivě sjednanou rovnováhu mezi zájmy různých států, které mají zmírnit kompetenční spory, jež mohou jinak nastat“. Viz rovněž Evropský sbor pro ochranu osobních údajů (pozn. pod čarou 153), s. 5. („V situacích, kdy existuje mezinárodní dohoda, jako je smlouva o vzájemné právní pomoci, by podniky z EU měly obecně odmítat přímé žádosti a odkazovat žádající orgán třetí země na existující smlouvu o vzájemné právní pomoci nebo dohodu.“).

[160] Podání ve věci Microsoft (viz poznámka pod čarou 156), s. 4.

[161] Podání ve věci Microsoft (viz poznámka pod čarou 156), s. 6.

[162] Evropská komise, návrh nařízení Evropského parlamentu a Rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech, 17. 4. 2018 (COM (2018) 225 final). Rada přijala obecný přístup k navrhovanému nařízení dne 7. 12. 2018 (k dispozici na adrese: https://www.consilium.europa.eu/cs/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-eevidence-council-agrees-its-position/#). Viz rovněž stanovisko evropského inspektora ochrany údajů 7/19 k návrhům týkajícím se evropských předávacích a uchovávacích příkazů pro elektronické důkazy v trestních věcech (k dispozici na adrese: https://edps.europa.eu/data-protection/ourwork/publications/opinions/electronic-evidence-criminal-matters_en).

[163] Důvodová zpráva, s. 21, upřesňuje, že kromě zajištění zdvořilosti ve vztahu ke svrchovaným zájmům třetích zemí, ochrany dotyčné osoby a zabránění kolizím norem pro poskytovatele služeb je jedním z důležitých motivů doložky zdvořilosti reciprocita, tj. zajistit dodržování pravidel EU, včetně pravidel týkajících se ochrany osobních údajů (článek 48 nařízení GDPR). Viz rovněž prohlášení pracovní skupiny zřízené podle článku 29 ze dne 29. listopadu 2017 o aspektech ochrany údajů a soukromí při přeshraničním přístupu k elektronickým důkazům (prohlášení pracovní skupiny zřízené podle článku 29) (k dispozici na adrese: file:///C:/Users/ralfs/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20171207_e-Evidence_Statement_FINALpdf%20(1).pdf), s. 9.

[164] Viz prohlášení pracovní skupiny zřízené podle článku 29 (viz poznámka pod čarou 163), s. 6.

Komise, která jedná jménem EU, se v současné době účastní mnohostranných jednání o druhém dodatkovém protokolu k Úmluvě Rady Evropy o kyberkriminalitě (dále jen „Budapešťská úmluva“), jehož cílem je posílit stávající pravidla k získání přeshraničního přístupu k elektronickým důkazům při vyšetřování trestných činů a současně zajistit odpovídající záruky ochrany osobních údajů v rámci protokolu[165]. Podobně byla zahájena dvoustranná jednání o dohodě mezi EU a Spojenými státy o přeshraničním přístupu k elektronickým důkazům pro justiční spolupráci v trestních věcech[166]. Komise počítá v průběhu těchto jednání s podporou Evropského parlamentu a Rady a s pokyny Evropského sboru pro ochranu osobních údajů.

V obecnější rovině je důležité zajistit, aby společnosti, které působí na evropském trhu, sdílely údaje pro účely vymáhání práva, když k tomu budou vyzvány na základě oprávněné žádosti ke sdílení, aniž by čelily kolizi norem, a při plném respektování základních práv EU. V zájmu zlepšení těchto předání je Komise odhodlána vytvořit se svými mezinárodními partnery vhodné právní rámce s cílem zabránit kolizím norem a podpořit účinné formy spolupráce, zejména zajištěním nezbytných záruk ochrany osobních údajů, a tím přispět k účinnějšímu boji proti trestné činnosti.

7.3 Mezinárodní spolupráce v oblasti ochrany osobních údajů

Podpora sbližování mezi různými systémy ochrany soukromí rovněž znamená vzájemné učení prostřednictvím výměny znalostí, zkušeností a osvědčených postupů. Tyto výměny mají zásadní význam pro řešení nových problémů, které jsou svou povahou a rozsahem stále globálnější. Proto Komise zintenzivnila svůj dialog o ochraně osobních údajů a tocích údajů s širokou škálou aktérů a na různých fórech na dvoustranné, regionální a mnohostranné úrovni.

Dvoustranný rozměr

Po přijetí nařízení GDPR roste zájem o zkušenosti EU s navrhováním, vyjednáváním a prováděním moderních pravidel ochrany soukromí. Dialog se zeměmi, které procházejí podobnými procesy, má několik forem.

Útvary Komise předložily příspěvky k řadě veřejných konzultací uspořádaných zahraničními vládami s ohledem na právní předpisy v oblasti ochrany soukromí,

---

[165] Viz doporučení pro rozhodnutí Rady o zmocnění k účasti na jednání o druhém dodatkovém protokolu k Úmluvě Rady Evropy o kyberkriminalitě (CETS č. 185), 5. 2. 2019 (COM(2019) 71 final). Viz také stanovisko Evropského inspektora ochrany údajů, 3/2019 k účasti na jednáních s ohledem na druhý dodatkový protokol k Budapešťské úmluvě o kyberkriminalitě, 2. 4. 2019 (k dispozici na adrese: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_budapest_convention_en.pdf); Evropský sbor pro ochranu osobních údajů, příspěvek ke konzultaci o návrhu druhého dodatkového protokolu k Úmluvě Rady Evropy o kyberkriminalitě (Budapešťská úmluva), 13. 11. 2019 (k dispozici na adrese: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf).

[166] Viz doporučení pro rozhodnutí Rady o zmocnění k zahájení jednání za účelem dosažení dohody mezi Evropskou unií a Spojenými státy americkými o přeshraničním přístupu k elektronickým důkazům pro justiční spolupráci v trestních věcech, 5. 2. 2019 (COM(2019) 70 final). Viz také stanovisko evropského inspektora ochrany údajů 2/2019 k mandátu pro jednání o dohodě mezi EU a USA o přeshraničním přístupu k elektronickým důkazům (k dispozici na adrese: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf).

například v USA[167], Indii[168], Malajsii a Etiopii. V některých třetích zemích měly útvary Komise výsadu vypovídat u příslušných parlamentních orgánů, například v Brazílii[169], Chile[170], Ekvádoru a Tunisku[171].

Kromě toho se v kontextu probíhajících reforem právních předpisů na ochranu osobních údajů konala setkání se zástupci vlád nebo s parlamentními delegacemi z mnoha regionů světa (např. z Gruzie, Keni, Tchaj-wanu, Thajska a Maroka). Součástí toho bylo pořádání seminářů a studijních návštěv, například za účasti zástupců indonéské vlády a delegace stálých pracovníků Kongresu USA. To poskytlo příležitost objasnit důležité pojmy z nařízení GDPR, zlepšit vzájemné porozumění problematice ochrany soukromí a ilustrovat přínosy sbližování pro zajištění vysoké úrovně ochrany práv fyzických osob, obchodu a spolupráce. V některých případech bylo možné též upozornit na některé mylné představy o ochraně osobních údajů, které mohou vést k zavedení ochranářských opatření, jako jsou požadavky na nucenou lokalizaci.

Od přijetí nařízení GDPR Komise rovněž spolupracuje s několika mezinárodními organizacemi, a to i v souvislosti s významem výměny údajů s těmito organizacemi v řadě oblastí politiky. Zejména byl navázán konkrétní dialog s Organizací spojených národů s cílem usnadnit diskuse se všemi zúčastněnými stranami, aby bylo zajištěno hladké předávání údajů a aby se dále rozvíjelo sbližování příslušných režimů ochrany osobních údajů. V rámci tohoto dialogu bude Komise úzce spolupracovat s Evropským sborem pro ochranu osobních údajů s cílem dále vyjasnit, jak mohou veřejní a soukromí provozovatelé v EU při výměně údajů s mezinárodní organizací, jako je OSN, dodržovat své povinnosti vyplývající z nařízení GDPR.

---

[167] Viz příspěvek GŘ pro spravedlnost a spotřebitele ze dne 9. listopadu 2018 v reakci na žádost o veřejné připomínky k navrhovanému přístupu k ochraně soukromí spotřebitele [Docket č. 180821780–8780–01] ze strany Národní telekomunikační a informační správy USA (k dispozici na adrese: https://ec.europa.eu/info/sites/info/files/european_commission_submission_on_a_proposed_approach_to_consumer_privacy.pdf).

[168] Viz příspěvek GŘ pro spravedlnost a spotřebitele ze dne 19. listopadu 2018 k návrhu indického zákona o ochraně osobních údajů z roku 2018 pro Ministerstvo elektroniky a informačních technologií (k dispozici na adrese: https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en).

[169] Viz plenární zasedání brazilského Senátu dne 17. dubna 2018 (https://www25.senado.leg.br/web/atividade/sessao-plenaria/-/pauta/23384), schůze smíšeného výboru brazilského Kongresu dne 10. dubna 2019 ve věci MP 869/2018 (https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=15392) a zasedání zvláštního výboru brazilské Poslanecké sněmovny ze dne 26. listopadu 2019 (https://www.camara.leg.br/noticias/616579-comissao-discutira-protecao-de-dados-no-ambito-das-constituicoes-de-outros-paises/).

[170] Viz zasedání Výboru pro ústavní a legislativní záležitosti chilského senátu ze dne 29. května 2018 (https://senado.cl/appsenado/index.php?mo=comisiones&ac=asistencia_sesion&idcomision=186&idsesion=12513&idpunto=15909&sesion=29/05/2018&listado=1) a 24. dubna 2019 (https://www.senado.cl/appsenado/index.php?mo=comisiones&ac=sesiones_celebradas&idcomision=186&tipo=3&legi=485&ano=2019&desde=0&hasta=0&idsesion=13603&idpunto=17283&listado=2).

[171] Viz zasedání Výboru pro práva, svobody a vnější vztahy tuniského Shromáždění zástupců lidu (https://www.facebook.com/1515094915436499/posts/2264094487203201/) konané dne 2. listopadu 2018.

Komise je připravena i nadále sdílet poznatky získané z procesu reforem se zúčastněnými zeměmi a mezinárodními organizacemi, a to stejným způsobem, jakým se poučila z jiných systémů při vypracovávání svého návrhu nových pravidel EU pro ochranu osobních údajů. Tento druh dialogu je pro EU a její partnery vzájemně prospěšný, neboť umožňuje lépe porozumět rychle se vyvíjející situaci v oblasti ochrany soukromí a vyměňovat si názory na vznikající právní a technologická řešení.

V tomto duchu Komise zřizuje „Akademii ochrany osobních údajů“ s cílem podpořit výměny mezi evropskými regulačními orgány a regulačními orgány třetích zemí a zlepšit tak spolupráci „na místě“.

Kromě toho je třeba vytvořit vhodné právní nástroje pro užší formy spolupráce a vzájemné pomoci, včetně umožnění nezbytné výměny informací v souvislosti s vyšetřováním. Komise proto využije pravomocí, které jí v této oblasti uděluje článek 50 nařízení GDPR, a zejména požádá o povolení zahájit jednání o uzavření dohod o spolupráci v oblasti vymáhání práva s příslušnými třetími zeměmi. V této souvislosti vezme rovněž v úvahu názory sboru týkající se toho, které země by měly být upřednostněny s ohledem na objem předávání údajů, úlohu a pravomoci donucovacích orgánů ve třetí zemi a potřebu spolupráce v oblasti vymáhání práva pro účely řešení případů společného zájmu.

Mnohostranný rozměr

Kromě dvoustranných výměn se Komise rovněž aktivně účastní řady mnohostranných fór, jejichž cílem je prosazovat sdílené hodnoty a rozvíjet sbližování na regionální a celosvětové úrovni.

Jasným signálem tohoto trendu směrem k (vzestupnému) sbližování je stále univerzálnější členství v „úmluvě č. 108“ Rady Evropy, která je jediným právně závazným mnohostranným nástrojem v oblasti ochrany osobních údajů[172]. Úmluva, která je otevřena i nečlenům Rady Evropy, již byla ratifikována v 55 zemích, včetně řady afrických a latinskoamerických států[173]. Komise významně přispěla k úspěšnému výsledku jednání o modernizaci úmluvy[174] a zajistila, aby odrážela stejné zásady, jaké jsou zakotveny v pravidlech EU pro ochranu osobních údajů. Většina členských států EU nyní podepsala pozměňovací protokol, ačkoli ještě chybí podpisy Dánska, Malty a Rumunska. Pozměňovací protokol dosud ratifikovaly pouze čtyři členské státy (Bulharsko, Chorvatsko, Litva a Polsko). Komise naléhavě vyzývá tři zbývající členské státy, aby modernizovanou úmluvu podepsaly, a všechny členské státy, aby

[172] Důležité je, že modernizovaná úmluva není pouze smlouvou, která stanoví silné záruky ochrany osobních údajů, ale také vytváří síť dozorových úřadů s nástroji pro spolupráci v oblasti vymáhání práva a prostřednictvím Výboru pro úmluvu fórum pro diskuse, výměnu osvědčených postupů a rozvoj mezinárodních norem.

[173] Úplný seznam členů: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures. Mezi země z Afriky patří Kapverdy, Mauricius, Maroko, Senegal a Tunisko, z Latinské Ameriky to je Argentina, Mexiko a Uruguay. K přistoupení k úmluvě byla pozvána Burkina Faso.

[174] Viz znění modernizované úmluvy: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

urychleně přistoupily k ratifikaci s cílem umožnit vstup úmluvy v platnost v blízké budoucnosti[175]. Kromě toho bude nadále proaktivně podporovat přistoupení třetích zemí.

V rámci skupin G20 a G7 byly rovněž nedávno řešeny otázky toků a ochrany osobních údajů. V roce 2019 vedoucí představitelé EU poprvé potvrdili myšlenku, že ochrana osobních údajů přispívá k důvěře v digitální ekonomiku a usnadňuje toky údajů. S aktivní podporou Komise[176] schválili vedoucí představitelé koncepci „volný tok údajů s důvěrou“, původně navržený Japonskem v Ósacké deklaraci G20[177], jakož i na summitu G7 v Biarritzu[178]. Tento přístup se odráží také ve sdělení Komise „Evropská strategie pro data“ z roku 2020[179], které zdůrazňuje její záměr nadále podporovat sdílení údajů s důvěryhodnými partnery a zároveň bojovat proti zneužívání, jako je nepřiměřený přístup (zahraničních) orgánů veřejné moci k údajům.

EU se při tom bude moci spolehnout na řadu nástrojů v různých oblastech politiky, které stále více zohledňují dopad na soukromí: například vůbec první unijní rámec pro prověřování zahraničních investic, který začne být plně použitelný v říjnu 2020, dává EU a jejím členským státům možnost prověřovat investiční transakce, které mají vliv na „přístup k citlivým informacím včetně osobních údajů nebo na schopnost kontrolovat tyto informace“, pokud mají vliv na bezpečnost nebo veřejný pořádek[180].

Komise spolupracuje s podobně smýšlejícími zeměmi na několika dalších mnohostranných fórech, aby aktivně prosazovala své hodnoty a normy. Důležitým fórem je nedávno vytvořená pracovní skupina OECD pro správu a ochranu osobních údajů (DGP), která provádí řadu důležitých iniciativ týkajících se ochrany, sdílení a předávání údajů. Součástí je i hodnocení Směrnice OECD o ochraně soukromí a přeshraničních tocích osobních údajů z roku 2013. Komise navíc aktivně přispěla k

---

[175] Podle svého rozhodnutí o pozměňovacím protokolu ze dne 18. května 2018 Výbor ministrů „naléhavě vyzval členské státy a další strany úmluvy, aby neprodleně přijaly nezbytná opatření, která umožní vstup protokolu v platnost do tří let od jeho otevření k podpisu, a aby neprodleně zahájily, v každém případě však nejpozději jeden rok po dni, kdy byl protokol otevřen k podpisu, postup podle svých vnitrostátních právních předpisů vedoucí k ratifikaci...“ Rovněž „pověřil své zástupce, aby dvakrát ročně a poprvé jeden rok po datu otevření k podpisu protokolu posoudili celkový pokrok, jehož bylo dosaženo na cestě k ratifikaci, na základě informací, které každý z členských států a jiných stran úmluvy předložil generálnímu tajemníkovi, a to nejpozději měsíc před takovým přezkumem.“ Viz https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016808a3c9f.

[176] V rámci summitu EU–Japonsko, který se konal v dubnu 2019, vyjádřil předseda Juncker podporu iniciativě „volný tok údajů s důvěrou“ a zahájení procesu „Osaka Track“ a přijal za Komisi závazek, že „bude v obou iniciativách hrát aktivní úlohu“.

[177] Viz znění Ósackého prohlášení vedoucích představitelů skupiny G20: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[178] Viz znění strategie G7 z Biarritzu pro otevřenou, svobodnou a bezpečnou digitální transformaci: https://www.elysee.fr/admin/upload/default/0001/05/62a9221e66987d4e0d6ffcb058f3d2c649fc6d9d.pdf

[179] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů, Evropská strategie pro data, 19. 2. 2020, COM(2020) 66 final (https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf), s. 23–24.

[180] Čl. 4 odst. 1 písm. d) nařízení Evropského parlamentu a Rady (EU) 2019/452 ze dne 19. března 2019, kterým se stanoví rámec pro prověřování přímých zahraničních investic směřujících do Unie (Úř. věst. L 79I, 21.3.2019).

doporučení Rady OECD v oblasti umělé inteligence[181] a zajistila, aby se přístup EU zaměřený na člověka, který znamená, že aplikace umělé inteligence musí být v souladu se základními právy, a zejména s ochranou osobních údajů, odrazil v konečném znění. Důležité je, že doporučení v oblasti umělé inteligence, které bylo následně zapracováno do zásad skupiny G20 v oblasti umělé inteligence připojených k Ósackému prohlášení vedoucích představitelů skupiny G20[182], stanoví zásady transparentnosti a srozumitelnosti, aby „osobám nepříznivě ovlivněným systémem umělé inteligence umožnily napadnout jeho výsledek na základě jednoduchých a snadno srozumitelných informací o faktorech a logice, která sloužila jako základ pro předpověď, doporučení nebo rozhodnutí“, čímž úzce odráží zásady nařízení GDPR, pokud jde o automatizované rozhodování[183].

Komise rovněž posiluje svůj dialog s regionálními organizacemi a sítěmi, jež hrají ve formování společných norem v oblasti ochrany osobních údajů[184] čím dál důležitější úlohu, podporují výměnu osvědčených postupů i spolupráci mezi donucovacími orgány. To se týká zejména Sdružení národů jihovýchodní Asie (ASEAN), a to i v souvislosti s probíhající prací na nástrojích k předávání údajů, Africké unie, fóra asijsko-tichomořských orgánů pro ochranu soukromí (APPA) nebo Iberoamerické sítě pro ochranu údajů, které zahájily důležité iniciativy v této oblasti a poskytují fóra pro plodný dialog mezi regulačními orgány v oblasti ochrany soukromí a dalšími zúčastněnými stranami.

Afrika je výmluvným příkladem doplňkovosti mezi národním, regionálním a celosvětovým rozměrem ochrany soukromí. Digitální technologie rychle a hluboce transformují africký kontinent. To má potenciál urychlit dosažení cílů udržitelného rozvoje tím, že se podpoří hospodářský růst, zmírní chudoba a zlepší se život lidí. Klíčovým prvkem této transformace je zavedení moderního rámce pro ochranu osobních údajů, který přiláká investice a podpoří rozvoj konkurenceschopných podniků a současně přispěje k dodržování lidských práv, demokracie a právního státu. Harmonizace pravidel ochrany osobních údajů v Africe by umožnila integraci digitálního trhu, zatímco sbližování s celosvětovými standardy by usnadnilo výměnu údajů s EU. Tyto různé aspekty ochrany osobních údajů jsou vzájemně propojené a vzájemně se posilují.

V současné době roste zájem o ochranu osobních údajů v mnoha afrických zemích a nadále roste[185] počet afrických zemí, které přijaly moderní pravidla ochrany osobních údajů nebo jsou v procesu jejich přijímání, ratifikovaly úmluvu č. 108[186] nebo úmluvu z Malaba[187]. Regulační rámec je na celém africkém kontinentu

[181] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[182] Ministerské prohlášení skupiny G20 o obchodu a digitální ekonomice: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

[183] Viz čl. 13 odst. 2 písm. f), čl. 14 odst. 2 písm. g) a článek 22 nařízení GDPR.

[184] Viz například *Úmluva Africké unie o kybernetické bezpečnosti a ochraně osobních údajů* (dále jen „Úmluva z Malaba“) a *normy pro ochranu osobních údajů pro iberoamerické státy* vyvinuté Iberoamerickou sítí pro ochranu údajů.

[186] Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=DW5jevqD.

[187] Úmluva Africké unie o kybernetické bezpečnosti a ochraně osobních údajů https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. Několik

zároveň stále velmi nerovnoměrný a roztříštěný. Mnoho zemí stále nabízí jen málo záruk ochrany osobních údajů nebo nenabízí záruky žádné. Opatření omezující toky údajů jsou stále velmi rozšířená a brání rozvoji regionální digitální ekonomiky.

S cílem využít vzájemných výhod plynoucích z harmonizovaných pravidel ochrany osobních údajů bude Komise spolupracovat se svými africkými partnery jak na dvoustranné úrovni, tak v regionálních fórech[188]. Vychází z práce pracovní skupiny EU a Africké unie pro digitální ekonomiku v kontextu nového partnerství mezi Afrikou a Evropou pro digitální ekonomiku[189]. Podporuje též takové cíle, aby oblast působnosti nástroje partnerství Komise „Prohloubená ochrana osobních údajů a toky údajů“ byla rozšířena i na Afriku. Projekt bude mobilizován, aby podpořil africké země, které mají v úmyslu vytvořit moderní rámce ochrany osobních údajů nebo které chtějí posílit kapacitu svých regulačních orgánů prostřednictvím odborné přípravy, sdílení znalostí a výměny osvědčených postupů.

V neposlední řadě je Komise při podpoře sbližování standardů v oblasti ochrany osobních údajů na mezinárodní úrovni jako způsobu, jak usnadnit toky údajů, a tím i obchod, rovněž odhodlána řešit digitální protekcionismus, jak bylo nedávno zdůrazněno v datové strategii[190]. Za tímto účelem vypracovala zvláštní ustanovení o tocích údajů a ochraně osobních údajů v obchodních dohodách, které systematicky předkládá ve svých dvoustranných obchodních dohodách (naposledy s Austrálií, Novým Zélandem a Spojeným královstvím) a vícestranných jednáních, jako jsou stávající rozhovory o elektronickém obchodování v rámci WTO. Tato horizontální ustanovení vylučují neodůvodněná omezení, jako jsou požadavky na nucenou lokalizaci, při zachování regulační autonomie stran v zájmu ochrany základního práva na ochranu osobních údajů.

Třebaže dialogy o ochraně osobních údajů a obchodních jednáních musí probíhat odděleně, mohou se vzájemně doplňovat. Sbližování, založené na vysokých standardech a podpořené účinným vymáháním, skutečně poskytuje nejsilnější základ pro výměnu osobních údajů, což naši mezinárodní partneři stále více uznávají. Vzhledem k tomu, že podniky stále více působí přes hranice a upřednostňují uplatňování obdobných souborů pravidel ve všech svých obchodních operacích po celém světě, pomáhá toto sbližování vytvářet prostředí příznivé pro přímé investice,

---

regionálních hospodářských společenství kromě toho vytvořilo pravidla ochrany osobních údajů, například Hospodářské společenství států západní Afriky (ECOWAS) a Jihoafrické společenství pro rozvoj (SADC). Viz http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf a http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf.

[188]Mimo jiné prostřednictvím iniciativy v oblasti politiky a regulace pro digitální Afriku (PRIDA), viz informace na adrese: https://www.africa-eu-partnership.org/en/projects/policy-and-regulation-initiative-digital-africa-prida.

[189]Viz společné sdělení Evropské komise a vysokého představitele Unie pro zahraniční věci a bezpečnostní politiku „Na cestě ke komplexní strategii pro Afriku“ (k dispozici na adrese: https://ec.europa.eu/international-partnerships/system/files/communication-eu-africa-strategy-join-2020-4-final_en.pdf), pracovní skupina pro digitální ekonomiku, Nové partnerství mezi Afrikou a Evropou pro digitální ekonomiku: Urychlení dosažení cílů udržitelného rozvoje (k dispozici na adrese: https://www.africa-eu-partnership.org/sites/default/files/documents/finaldetfreportpdf.pdf).

[190]https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf, s. 23.

usnadňování obchodu a zlepšování důvěry mezi obchodními partnery. Je proto třeba dále prozkoumat synergie mezi nástroji na ochranu obchodu a údajů, aby byly zajištěny volné a bezpečné mezinárodní toky údajů, které jsou zásadní pro obchodní činnosti, konkurenceschopnost a růst evropských společností, včetně malých a středních podniků, v našem stále digitalizovanějším hospodářství.

PŘÍLOHA I – Doložky o volitelných specifikacích ve vnitrostátních právních předpisech

Předmět	Oblast působnosti	Články nařízení GDPR
Specifikace pro právní povinnosti a veřejné úkoly	Přizpůsobení uplatňování ustanovení týkajících se zpracování za účelem splnění právní povinnosti nebo veřejného úkolu, mimo jiné pro zvláštní situace zpracování podle kapitoly IX	Čl. 6 odst. 2 a 3
Věková hranice pro souhlas v souvislosti se službami informační společnosti	Určení minimálního věku mezi 13 až 16 lety	Čl. 8 odst. 1
Zpracování zvláštních kategorií údajů	Zachování nebo zavedení dalších podmínek, včetně omezení, pro zpracování genetických údajů, biometrických údajů nebo údajů týkajících se zdraví	Čl. 9 odst. 4
Výjimka z požadavků na informace	Získání nebo zpřístupnění výslovně stanovené právními předpisy nebo pro profesní tajemství, které je upraveno zákonem	Čl. 14 odst. 5 písm. c) a d)
Automatizované individuální rozhodování	Povolení automatizovaného rozhodování odchylně od obecného zákazu	Čl. 22 odst. 2 písm. b)
Omezení práv subjektů údajů	Omezení z článků 12 až 22, článku 34 a odpovídajících ustanovení v článku 5, je-li to nezbytné a přiměřené pro zajištění taxativně uvedených důležitých cílů	Čl. 23 odst. 1
Požadavek na konzultaci a povolení	Povinnost správců konzultovat nebo získat povolení úřadu pro ochranu osobních údajů ke zpracování pro účely úkolu ve veřejném zájmu	Čl. 36 odst. 5
Jmenování pověřence pro ochranu osobních údajů v dalších případech	Jmenování pověřence pro ochranu osobních údajů v jiných případech, než jsou případy uvedené v čl. 37 odst. 1	Čl. 37 odst. 4
Omezení předávání údajů	Omezení předávání konkrétních kategorií osobních údajů	Čl. 49 odst. 5
Stížnosti a soudní žaloby organizací z vlastního rozhodnutí	Oprávnění organizací na ochranu soukromí podávat stížnosti a soudní žaloby nezávisle na pověření subjekty údajů	Čl. 80 odst. 2

Přístup k úředním dokumentům	Zajištění souladu přístupu veřejnosti k úředním dokumentům s právem na ochranu osobních údajů	Článek 86
Zpracování národních identifikačních čísel	Zvláštní podmínky pro zpracování národního identifikačního čísla	Článek 87
Zpracování v souvislosti se zaměstnáním	Konkrétnější pravidla pro zpracování osobních údajů zaměstnanců	Článek 88
Výjimky pro zpracování pro účely archivace ve veřejném zájmu, pro výzkum nebo statistické účely	Výjimky ze specifikovaných práv subjektů údajů, pokud je pravděpodobné, že by tato práva znemožnila nebo vážně ohrozila splnění zvláštních účelů.	Čl. 89 odst. 2 a 3
Zajištění souladu ochrany osobních údajů s povinností zachovávat mlčenlivost	Zvláštní pravidla pro vyšetřovací pravomoci úřadů pro ochranu osobních údajů ve vztahu ke správcům nebo zpracovatelům, na něž se vztahuje povinnost zachovávat profesní tajemství.	Článek 90

PŘÍLOHA II – Přehled zdrojů úřadů pro ochranu osobních údajů

Níže uvedená tabulka obsahuje přehled zdrojů (zaměstnanců a rozpočtu) úřadů pro ochranu osobních údajů podle členských států EU/EHP[191].

Při porovnávání údajů mezi členskými státy je důležité mít na paměti, že úřady mohou plnit úkoly, které jim byly svěřeny nad rámec nařízení GDPR, a že se tyto úkoly mohou v jednotlivých členských státech lišit. Poměr zaměstnanců, které úřady zaměstnávají, na jeden milion obyvatel, a poměr rozpočtu úřadů na jeden milion EUR HDP jsou zahrnuty pouze za účelem poskytnutí dalších prvků srovnání mezi členskými státy podobné velikosti a neměly by být posuzovány izolovaně. Při posuzování zdrojů daného orgánu by měly být brány v úvahu absolutní hodnoty, poměry a vývoj za poslední roky.

	ZAMĚSTNANCI (v přepočtu na plný pracovní úvazek)					ROZPOČET (EUR)				
Členské státy EU/EHP	**2019**	**Prognóza pro rok 2020**	**% růst, 2016–2019**	**% růst, 2016–2020 (prognóza)**	**Počet zaměstnanců na milion obyvatel (2019)**	**2019**	**Prognóza pro rok 2020**	**% růst, 2016–2019**	**% růst, 2016–2020 (prognóza)**	**Rozpočet na milion EUR HDP (2019)**
Rakousko	34	34	48 %	48 %	3,8	2 282 000	2 282 000	29 %	29 %	5,7
Belgie	59	65	9 %	20 %	5,2	8 197 400	8 962 200	1 %	10 %	17,3
Bulharsko	60	60	-14 %	-14 %	8,6	1 446 956	1 446 956	24 %	24 %	23,8
Chorvatsko	39	60	39 %	114 %	9,6	1 157 300	1 405 000	57 %	91 %	21,5
Kypr	24	22	NENÍ K DISPOZICI	NENÍ K DISPOZICI	27,4	503 855	NENÍ K DISPOZICI	114 %	NENÍ K DISPOZICI	23,0
Česká republika	101	109	0 %	8 %	9,5	6 541 288	6 720 533	10 %	13 %	29,7
Dánsko	66	63	106 %	97 %	11,4	5 610 128	5 623 114	101 %	101 %	18,0
Estonsko	16	18	-11 %	0 %	12,1	750 331	750 331	7 %	7 %	26,8
Finsko	45	55	114 %	162 %	8,2	3 500 000	4 500 000	94 %	150 %	14,6
Francie	215	225	9 %	14 %	3,2	18 506 734	20 143 889	-2 %	7 %	7,7
Německo	888	1002	52 %	72 %	10,7	76 599 800	85 837 500	48 %	66 %	22,3
Řecko	33	46	-15 %	18 %	3,1	2 849 000	3 101 000	38 %	50 %	15,2
Maďarsko	104	117	42 %	60 %	10,6	3 505 152	4 437 576	102 %	155 %	24,4
Island	17	17	143 %	143 %	47,6	2 272 490	2 294 104	167 %	170 %	105,2
Irsko	140	176	169 %	238 %	28,5	15 200 000	16 900 000	223 %	260 %	43,8
Itálie	170	170	40 %	40 %	2,8	29 127 273	30 127 273	46 %	51 %	16,3
Lotyšsko	19	31	-10 %	48 %	9,9	640 998	1 218 978	4 %	98 %	21,0
Litva	46	52	-8 %	4 %	16,5	1 482 000	1 581 000	40 %	49 %	30,6
Lucembursko	43	48	126 %	153 %	70,0	5 442 416	6 691 563	165 %	226 %	85,7
Malta	13	15	30 %	50 %	26,3	480 000	550 000	41 %	62 %	36,3
Nizozemsko	179	188	145 %	158 %	10,4	18 600 000	18 600 000	130 %	130 %	22,9
Norsko	49	58	2 %	21 %	9,2	5 708 950	6 580 660	27 %	46 %	15,9
Polsko	238	260	54 %	68 %	6,3	7 506 345	9 413 381	66 %	108 %	14,2
Portugalsko	25	27	-4 %	4 %	2,4	2 152 000	2 385 000	67 %	86 %	10,1
Rumunsko	39	47	-3 %	18 %	2,0	1 103 388	1 304 813	3 %	22 %	4,9
Slovensko	49	51	20 %	24 %	9,0	1 731 419	1 859 514	47 %	58 %	18,4
Slovinsko	47	49	42 %	48 %	22,6	2 242 236	2 266 485	68 %	70 %	46,7
Španělsko	170	220	13 %	47 %	3,6	15 187 680	16 500 000	8 %	17 %	12,2
Švédsko	87	87	81 %	81 %	8,5	8 800 000	10 300 000	96 %	129 %	18,5

[191] S výjimkou Lichtenštejnska.

CELKEM	**2 966**	**3 372**	**42 %**	**62 %**	**6,6**	**249 127 139**	**273 782 870**	**49 %**	**64 %**	**17,4**

Zdroj nezpracovaných údajů: příspěvek sboru. Výpočty Komise.