EURÓPSKA
KOMISIA

V Bruseli 24. 6. 2020
COM(2020) 264 final

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU A RADE

Ochrana údajov ako pilier posilnenia postavenia občanov a prístupu EÚ k digitálnej transformácii – dva roky uplatňovania všeobecného nariadenia o ochrane údajov

{SWD(2020) 115 final}

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU A RADE

Ochrana údajov ako pilier posilnenia postavenia občanov a prístupu EÚ k digitálnej transformácii – dva roky uplatňovania všeobecného nariadenia o ochrane údajov

1 PRAVIDLÁ OCHRANY ÚDAJOV AKO PILIER POSILNENIA POSTAVENIA OBČANOV A PRÍSTUPU EÚ K DIGITÁLNEJ TRANSFORMÁCII

Táto správa je prvou správou o hodnotení a preskúmaní všeobecného nariadenia o ochrane údajov[1], najmä o uplatňovaní a fungovaní pravidiel o prenose osobných údajov do tretích krajín a medzinárodným organizáciám a pravidiel spolupráce a konzistentnosti, podľa článku 97 všeobecného nariadenia o ochrane údajov.

Všeobecné nariadenie o ochrane údajov, ktoré sa uplatňuje od 25. mája 2018, je jadrom rámca EÚ[2], ktorý zaručuje základné právo na ochranu údajov zakotvené v Charte základných práv Európskej únie (článok 8) a v zmluvách (článok 16 Zmluvy o fungovaní Európskej únie, ďalej len „ZFEÚ“). Všeobecné nariadenie o ochrane údajov prinieslo posilnenie záruk ochrany údajov, poskytlo jednotlivcom dodatočné a silnejšie práva, zvýšilo transparentnosť, a zabezpečilo, že všetci tí, ktorí zaobchádzajú s osobnými údajmi v rozsahu jeho pôsobnosti, sú zodpovednejší. Poskytuje nezávislým orgánom pre ochranu osobných údajov silnejšie a harmonizované právomoci v oblasti presadzovania práva a vytvára nový systém riadenia. Takisto vytvára rovnaké podmienky pre všetky spoločnosti pôsobiace na trhu EÚ bez ohľadu na to, kde sú usadené, a zabezpečuje voľný tok údajov v rámci EÚ, čím sa posilňuje vnútorný trh.

Všeobecné nariadenie o ochrane údajov je dôležitým prvkom antropocentrického prístupu k technológiám, a kompasom pri využívaní technológií v rámci dvojitej zelenej a digitálnej transformácie, ktorá charakterizuje tvorbu politiky EÚ. Táto skutočnosť bola nedávno zdôraznená v Bielej knihe o umelej inteligencii[3] a v oznámení o Európskej dátovej stratégii[4] z februára 2020.

V hospodárstve, ktoré je čoraz viac založené na spracúvaní údajov vrátane osobných údajov, je všeobecné nariadenie o ochrane údajov základným nástrojom na zabezpečenie toho, aby jednotlivci mali lepšiu kontrolu nad svojimi osobnými údajmi a aby sa tieto údaje spracúvali na legitímny účel zákonným, spravodlivým a transparentným spôsobom. Zároveň všeobecné nariadenie o ochrane údajov pomáha

---

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (Ú. v. EÚ L 119, 4.5.2016, s. 1 – 88).

[2] Po začlenení do dohody o Európskom hospodárskom priestore (EHP) sa nariadenie uplatňuje aj na Nórsko, Island a Lichtenštajnsko.

[3] https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_sk.

[4] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_sk.

podporovať dôveryhodné inovácie, najmä prostredníctvom prístupu založeného na riziku a zásad ako je špecificky navrhnutá a štandardná ochrana súkromia. Komisia navrhla doplniť legislatívny rámec ochrany údajov a súkromia[5] nariadením o súkromí a elektronických komunikáciách[6], ktoré má nahradiť súčasnú smernicu o súkromí a elektronických komunikáciách[7]. Tento návrh v súčasnosti skúmajú spoluzákonodarcovia a je veľmi dôležité zabezpečiť jeho rýchle prijatie.

Ako súčasť kľúčových priorít Komisie „Európa pripravená na digitálny vek“[8] a európska zelená dohoda[9], môžu byť pripravené nové iniciatívy s cieľom umožniť občanom zohrávať aktívnejšiu úlohu pri digitálnej transformácii a lepšie využívať digitálne nástroje s cieľom dosiahnuť klimaticky neutrálnu spoločnosť a udržateľnejší rozvoj. Vo všeobecnom nariadení o ochrane údajov sa stanovuje rámec pre tieto iniciatívy a zabezpečuje sa ním, že tieto iniciatívy sú navrhnuté tak, aby účinne posilňovali postavenie jednotlivcov.

Dátová stratégia[10] vyzýva na vytvorenie spoločného európskeho dátového priestoru, ako aj desiatich odvetvových spoločných európskych dátových priestorov, ktoré sú relevantné pre dvojitú zelenú a digitálnu transformáciu[11]. Pre všetky tieto priority má kľúčový význam jasný a uskutočniteľný rámec pre bezpečnú výmenu údajov a väčšiu dostupnosť dát. V dátovej stratégii bol takisto oznámený úmysel Komisie preskúmať v budúcej legislatíve možnosti používania dát uchovávaných vo verejných databázach na účely vedeckého výskumu spôsobom, ktorý je v súlade so všeobecným nariadením o ochrane údajov. Dátové priestory bude podporovať európska cloudová federácia, ktorá bude poskytovať služby spracovania dát a cloudových infraštruktúr v súlade so všeobecným nariadením o ochrane údajov. Všeobecné nariadenie o ochrane údajov zabezpečuje vysokú úroveň ochrany osobných údajov a ústrednú úlohu jednotlivcov vo všetkých týchto dátových priestoroch, pričom poskytuje potrebnú flexibilitu na prispôsobenie rôznym prístupom.

Potreba zabezpečiť dôveru a požiadavka na ochranu osobných údajov sa určite neobmedzuje na EÚ. Jednotlivci na celom svete čoraz viac oceňujú súkromie a bezpečnosť svojich údajov. Ako vyplýva z nedávneho globálneho prieskumu[12],

---

[5] Tento legislatívny rámec zahŕňa aj smernicu o presadzovaní práva v oblasti ochrany údajov (smernica 2016/680) a nariadenie o ochrane údajov v prípade inštitúcií a orgánov EÚ (nariadenie 2018/1725).

[6] Návrh nariadenia Európskeho parlamentu a Rady o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES (smernica o súkromí a elektronických komunikáciách) [COM(2017) 10 final – 2017/0003 (COD)].

[7] Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, str. 37 – 47).

[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_sk

[9] Oznámenie Komisie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Európsky ekologický dohovor [COM(2019) 640 final].

[10] Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov – Európska dátová stratégia, COM(2020) 66 final.

[11] Týchto desať odvetvových spoločných európskych dátových priestorov je určených pre: zdravotníctvo, priemyselnú výrobu, energetiku, mobilitu, poľnohospodárstvo, finančné údaje, verejnú správu, spoločný európsky dátový priestor pre zručnosti, dátový priestor pre európsku zelenú dohodu a európsky cloud pre otvorenú vedu.

[12] Pozri napríklad prieskum o súkromí spoločnosti Cisco z roku 2019 (Cisco Consumer Privacy Study 2019) (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf). Podľa tejto štúdie na vzorke 2 600 spotrebiteľov na celom svete, veľký počet spotrebiteľov už

považujú to za dôležitý faktor, ktorý ovplyvňuje ich nákupné rozhodnutia a ich správanie na internete. Rastúci počet spoločností reagoval na tento dopyt po ochrane súkromia, najmä tým, že dobrovoľne rozšírili niektoré práva a záruky stanovené vo všeobecnom nariadení o ochrane údajov na svojich zákazníkov so sídlom mimo EÚ. Veľa spoločností takisto uvádza rešpektovanie osobných údajov ako konkurenčnú výhodu a prvok, ktorý podporuje predaj na globálnom trhu tým, že ponúkajú inovatívne produkty a služby s novými riešeniami v oblasti ochrany súkromia alebo bezpečnosti údajov. Okrem toho zvýšená schopnosť aktérov súkromného a verejného sektora zhromažďovať a spracúvať údaje vo veľkom rozsahu vyvoláva dôležité a zložité otázky, ktoré čoraz viac stavajú ochranu súkromia do centra verejnej diskusie v rôznych častiach sveta.

Prijatie všeobecného nariadenia o ochrane údajov podnietilo ďalšie krajiny v mnohých regiónoch sveta, aby zvážili nasledovanie tohto príkladu. Ide o skutočne celosvetový trend zaznamenaný v mnohých krajinách od Čile po Južnú Kóreu, od Brazílie po Japonsko, od Kene po Indiu a od Kalifornie po Indonéziu. Vedúce postavenie EÚ v oblasti ochrany údajov ukazuje, že môže určovať globálne normy pre reguláciu digitálneho hospodárstva a privítali ho významné hlasy medzinárodného spoločenstva, ako napr. generálny tajomník OSN António Guterres, ktorý uviedol, že všeobecné nariadenie o ochrane údajov „*ide príkladom* […], „*ktorý inšpiruje podobné opatrenia inde*“ a „*vyzval EÚ a jej členské štáty, aby naďalej viedli utváranie digitálneho veku a boli na čele technologických inovácií a regulácie*“[13].

Súčasná kríza spôsobená pandémiou ochorenia COVID-19 ponúka jasný príklad globalizácie tejto diskusie o ochrane súkromia počas krízy, ako aj v rámci celosvetového úsilia o jej ukončenie. Viaceré členské štáty v EÚ prijali núdzové opatrenia v snahe chrániť verejné zdravie. Vo všeobecnom nariadení o ochrane údajov sa jasne uvádza, že každé obmedzenie musí rešpektovať podstatu základných práv a slobôd a musí byť nevyhnutným a primeraným opatrením v demokratickej spoločnosti na ochranu verejného záujmu, ako je verejné zdravie. Ako sa opatrenia na zamedzenie šírenia postupne ukončujú, aktéri s rozhodovacími právomocami musia reagovať na očakávania občanov, že im budú ponúknuté digitálne riešenia, ktoré sú dôveryhodné a rešpektujú práva na súkromie a ochranu osobných údajov.

V mnohých krajinách sú integrované opatrenia na ochranu súkromia, ako napr. dobrovoľné prihlásenie sa používateľmi, minimalizácia údajov a ich bezpečnosť, ako aj vylúčenie geolokalizácie, považované za nevyhnutné na zaistenie spoľahlivosti a spoločenskej akceptácie riešení založených na údajoch zameraných na monitorovanie a obmedzenie šírenia vírusu, kalibrovanie protiopatrení verejnej politiky, pomoc pacientom alebo vykonávanie stratégií ukončenia opatrení. V EÚ sa legislatívny rámec[14] na ochranu údajov a súkromia osvedčil ako dostatočne pružný nástroj, ktorý umožňuje vyvíjať praktické riešenia (napr. aplikácie na sledovanie kontaktov), pri súčasnom zabezpečení vysokej úrovne ochrany osobných údajov.

---

prijal opatrenia na ochranu svojho súkromia, napríklad zmenou spoločností alebo poskytovateľov z dôvodu ich politík v oblasti údajov alebo postupov spoločného využívania údajov.

[13] Prejav generálneho tajomníka OSN v talianskom Senáte 18. decembra 2019 (k dispozícii na adrese: https://www.un.org/press/en/2019/sgsm19916.doc.htm).

[14] Tento rámec obsahuje okrem všeobecného nariadenia o ochrane údajov aj smernicu o súkromí a elektronických komunikáciách (smernica 2002/58/ES), ktorá stanovuje okrem iného pravidlá prístupu a uchovávania informácií o koncovom zariadení používateľa.

Komisia v tejto súvislosti 16. apríla 2020 uverejnila usmernenia týkajúce sa aplikácií podporujúcich boj proti pandémii v súvislosti s ochranou údajov[15].

Ochrana osobných údajov má tiež zásadný význam pri predchádzaní manipulácii výberu občanov, najmä prostredníctvom mikrozacielenia voličov na základe nezákonného spracovania osobných údajov, predchádzaní zasahovaniu do demokratických procesov a zachovaní otvorenej diskusie, spravodlivosti a transparentnosti, ktoré sú pre demokraciu kľúčové. Komisia preto v septembri 2018 uverejnila usmernenie o uplatňovaní práva Únie v oblasti ochrany údajov v kontexte volieb[16].

Komisia pri tomto hodnotení a preskúmaní zohľadnila príspevky od Rady[17], Európskeho parlamentu[18], Európskeho výboru pre ochranu údajov (ďalej len „výbor“)[19] a jednotlivých orgánov pre ochranu osobných údajov[20], expertnej skupiny viacerých zainteresovaných strán[21] a ostatných zainteresovaných strán, okrem iného prostredníctvom spätnej väzby poskytnutej k plánu[22].

Prevláda názor, že všeobecné nariadenie o ochrane údajov po dvoch rokoch od začiatku uplatňovania splnilo svoje ciele posilniť ochranu práva jednotlivca na ochranu osobných údajov a zaručiť voľný tok osobných údajov v rámci EÚ[23]. Určilo sa však aj niekoľko oblastí, v ktorých by bolo možné budúce zlepšenie. Komisia sa podobne ako väčšina zainteresovaných strán a orgánov pre ochranu osobných údajov domnieva, že v tejto fáze by bolo predčasné vyvodzovať konečné závery týkajúce sa uplatňovania všeobecného nariadenia o ochrane údajov. Je pravdepodobné, že väčšinu problémov zistených členskými štátmi a zainteresovanými stranami bude možné riešiť na základe skúseností pri uplatňovaní všeobecného nariadenia o ochrane údajov v nadchádzajúcich rokoch. Táto správa však poukazuje na problémy, ktoré sa doteraz

---

[15] Oznámenie Komisie – Usmernenie týkajúce sa aplikácií podporujúcich boj proti pandémii COVID-19 v súvislosti s ochranou údajov (2020/C 124 I/01) – C(2020) 2523 (Ú. v. EÚ C 124I, 17.4.2020, s. 1 – 9). Členské štáty EÚ v reakcii na pandémiu koronavírusu 16. apríla 2020 s podporou Komisie vypracovali súbor nástrojov EÚ na používanie mobilných aplikácií určených na sledovanie kontaktov a varovanie. Ide o súčasť spoločného koordinovaného prístupu k podpore postupného odstraňovania opatrení na obmedzenie pohybu. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[16] Usmernenie Komisie o uplatňovaní práva Únie v oblasti ochrany údajov v kontexte volieb – Príspevok Európskej komisie k zasadnutiu lídrov 19. – 20. septembra 2018 v Salzburgu, COM/2018/638 final.

[17] Pozícia Rady a zistenia o uplatňovaní všeobecného nariadenia o ochrane údajov: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/sk/pdf.

[18] List výboru LIBE Európskeho parlamentu z 21. februára 2020 adresovaný komisárovi Reyndersovi, ref. č.: IPOL-COM-LIBE D (2020)6525.

[19] Príspevok výboru k hodnoteniu všeobecného nariadenia o ochrane údajov podľa článku 97, prijatý 18. februára 2020: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en.

[20] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_sk.

[21] Do expertnej skupiny viacerých zainteresovaných strán, ktorú Komisia zriadila v súvislosti s nariadením, patria zástupcovia občianskej spoločnosti a podnikov, akademici i odborníci z praxe: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537.

[22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation/feedback?p_id=7669437.

[23] Pozri napríklad pozíciu a zistenia Rady, ako aj príspevok výboru.

vyskytli pri uplatňovaní všeobecného nariadenia o ochrane údajov, a vytyčujú sa v nej možné spôsoby ich riešenia.

Bez ohľadu na to, že sa zameriava na dve otázky zdôraznené v článku 97 ods. 2 všeobecného nariadenia o ochrane údajov, konkrétne na medzinárodné prenosy a mechanizmy spolupráce a konzistentnosti, toto hodnotenie a preskúmanie má širší prístup s cieľom riešiť aj otázky, na ktoré poukázali rôzni aktéri počas posledných dvoch rokov.

2 HLAVNÉ ZISTENIA

Presadzovanie všeobecného nariadenia o ochrane údajov a fungovanie mechanizmov spolupráce a konzistentnosti

Vo všeobecnom nariadení o ochrane údajov sa zaviedol inovatívny mechanizmus riadenia založený na nezávislých orgánoch pre ochranu osobných údajov v členských štátoch a ich spolupráci v cezhraničných prípadoch a v rámci Európskeho výboru pre ochranu údajov (ďalej len „výbor“). Všeobecným názorom je, že orgány pre ochranu údajov vyvážene využívali posilnené nápravné právomoci vrátane upozornení a napomenutí, uloženia pokút a dočasného alebo trvalého obmedzenia spracúvania[24]. Komisia zaznamenala, že tieto orgány uložili správne pokuty v rozsahu od niekoľko tisíc eur až po niekoľko miliónov eur, v závislosti od závažnosti porušení. Ostatné sankcie, napríklad zákaz spracovania, môžu mať rovnako odstrašujúci, prípadne vyšší účinok, ako pokuty. Konečným cieľom všeobecného nariadenia o ochrane údajov je zmeniť kultúru a správanie všetkých zúčastnených aktérov v prospech jednotlivcov. Podrobnejšie informácie o využívaní nápravných právomocí orgánmi pre ochranu osobných údajov sú uvedené v sprievodnom pracovnom dokumente útvarov Komisie.

Hoci je ešte skoro na úplné posúdenie fungovania nových mechanizmov spolupráce a konzistentnosti, orgány pre ochranu osobných údajov rozvinuli svoju spoluprácu prostredníctvom mechanizmu jednotného kontaktného miesta[25] a rozsiahlym využívaním vzájomnej pomoci[26]. Mechanizmus jednotného kontaktného miesta, ktorý je kľúčovým prvkom vnútorného trhu, sa používa na rozhodovanie o mnohých cezhraničných prípadoch[27]. V súčasnosti sa pripravujú dôležité rozhodnutia s cezhraničným rozmerom, na ktoré sa bude vzťahovať mechanizmus jednotného kontaktného miesta. Tieto rozhodnutia, ktoré sa často týkajú veľkých nadnárodných technologických spoločností, budú mať značný vplyv na práva jednotlivcov v mnohých členských štátoch.

Rozvoj skutočnej spoločnej európskej kultúry ochrany údajov medzi orgánmi pre ochranu osobných údajov je však stále pokračujúcim procesom. Orgány pre ochranu osobných údajov zatiaľ v plnej miere nevyužívajú nástroje, ktoré poskytuje všeobecné nariadenie o ochrane údajov, ako sú spoločné operácie, ktoré by mohli viesť k spoločným vyšetrovaniam. Niekedy snaha o spoločný prístup znamená prechod na

[24] Pozri bod 2.1 pracovného dokumentu útvarov Komisie.
[25] Ak spoločnosť vykonáva cezhraničné spracúvanie, príslušným orgánom pre ochranu osobných údajov je orgán v členskom štáte, v ktorom má spoločnosť hlavné miesto podnikateľskej činnosti.
[26] Pozri bod 2.2 pracovného dokumentu útvarov Komisie.
[27] Od 25. mája 2018 do 31. decembra 2019 bolo prostredníctvom mechanizmu jednotného kontaktného miesta predložených 141 návrhov rozhodnutí, z ktorých 79 vyústilo do konečných rozhodnutí.

najnižší spoločný menovateľ a v dôsledku toho sa nevyužili príležitosti na podporu väčšej harmonizácie[28].

Ďalší pokrok je potrebný na zefektívnenie a harmonizáciu riešenia cezhraničných prípadov v celej EÚ, a to aj z procesného hľadiska, napríklad v otázkach, ako sú postupy vybavovania sťažností, kritériá prípustnosti pre sťažnosti, trvanie konaní z dôvodu rôznych časových rámcov alebo absencia lehôt vo vnútroštátnom správnom procesnom práve, moment v konaní, v ktorom sa udeľuje právo na vypočutie, alebo informácie a zapojenie sťažovateľov počas konania. Víta sa proces reflexie, ktorý v tejto súvislosti začal výbor, a Komisia sa na týchto diskusiách zúčastňuje[29].

Aktivity a usmernenia výboru majú kľúčový význam pre ďalší konzistentný rozvoj výmen medzi výborom a zainteresovanými stranami[30]. Ku koncu roka 2019 výbor prijal 67 dokumentov vrátane 10 nových usmernení[31] a 43 stanovísk[32]. Zainteresované strany vo všeobecnosti vítajú usmernenia výboru a požadujú dodatočné usmernenia týkajúce sa kľúčových pojmov všeobecného nariadenia o ochrane údajov, ale poukazujú aj na nezrovnalosti medzi vnútroštátnymi usmerneniami a usmerneniami výboru. Zdôrazňujú potrebu praktickejšieho poradenstva, najmä konkrétnejších príkladov a potrebu, aby orgány pre ochranu osobných údajov boli vybavené potrebnými ľudskými, technickými a finančnými zdrojmi na účinné vykonávanie svojich úloh.

Komisia neustále zdôrazňovala povinnosť členských štátov vyčleniť dostatočné ľudské, finančné a technické zdroje pre vnútroštátne orgány pre ochranu osobných údajov[33]. Väčšina orgánov zaznamenala nárast počtu zamestnancov a rozpočtu od roku 2016 do roku 2019[34], pričom írsky, holandský, islandský, luxemburský a fínsky orgán mali najväčší relatívny nárast počtu zamestnancov. Keďže najväčšie nadnárodné podniky v oblasti technológií majú sídlo v Írsku a Luxembursku, orgány pre ochranu osobných údajov v týchto krajinách majú vedúcu úlohu v mnohých dôležitých cezhraničných prípadoch a môžu potrebovať väčšie zdroje, než by naznačoval počet ich obyvateľov. Situácia v jednotlivých členských štátoch je však stále nevyrovnaná a celkovo ešte nie je uspokojivá. Orgány pre ochranu osobných údajov zohrávajú kľúčovú úlohu pri zabezpečovaní presadzovania všeobecného nariadenia o ochrane autorských práv na vnútroštátnej úrovni a zaistenia účinného fungovania mechanizmov spolupráce a konzistentnosti v rámci výboru, predovšetkým mechanizmu jednotného kontaktného miesta pre cezhraničné prípady. Členské štáty

---

[28] Napríklad vnútroštátne zoznamy druhov spracovateľských operácií, ktoré si vyžadujú posúdenie vplyvu na ochranu údajov podľa článku 35 všeobecného nariadenia o ochrane údajov, by sa mohli lepšie zosúladiť.

[29] Pozri bod 2.2 pracovného dokumentu útvarov Komisie.

[30] Najmä zástupcovia spoločností a občianskej spoločnosti. Pozri bod 2.3 pracovného dokumentu útvarov Komisie.

[31] Dopĺňajú celkovo 10 usmernení, ktoré prijala pracovná skupina zriadená podľa článku 29 pred začatím uplatňovania nariadenia a ktoré schválil výbor. Výbor od januára do konca mája 2020 prijal aj 4 dodatočné usmernenia a aktualizoval jedno už existujúce.

[32] 42 z týchto stanovísk bolo prijatých podľa článku 64 všeobecného nariadenia o ochrane údajov a jedno bolo prijaté podľa článku 70 ods. 1 písm. s) všeobecného nariadenia o ochrane údajov a týkalo sa rozhodnutia o primeranosti vo vzťahu k Japonsku.

[33] Oznámenie Komisie Európskemu parlamentu a Rade – Pravidlá ochrany údajov ako nástroj budovania dôvery v EÚ a mimo nej – celkové hodnotenie, COM(2019) 374 final, 24.7.2019

[34] Celkovo došlo v EHP od roku 2016 do roku 2019 pri vnútroštátnych orgánoch pre ochranu osobných údajov k zvýšeniu počtu zamestnancov o 42 % a rozpočtu o 49 %.

sa preto vyzývajú, aby im poskytli primerané zdroje, ako sa vyžaduje vo všeobecnom nariadení o ochrane údajov[35].

Harmonizované pravidlá, ale pretrváva miera fragmentácie a odlišné prístupy

Komisia monitoruje vykonávanie všeobecného nariadenia o ochrane údajov vo vnútroštátnych právnych predpisoch. S výnimkou Slovinska všetky členské štáty v čase prípravy tejto správy prijali nové právne predpisy alebo upravili svoje vnútroštátne právne predpisy o ochrane údajov. Slovinsko[36] bolo požiadané, aby Komisii poskytlo vysvetlenia k dokončeniu tohto procesu[37].

Vo všeobecnom nariadení o ochrane údajov sa stanovuje konzistentný prístup k pravidlám ochrany údajov v celej EÚ. Od členských štátov však vyžaduje, aby v niektorých oblastiach[38] prijímali právne predpisy a poskytuje im možnosť podrobnejšie rozviesť všeobecné nariadenie o ochrane údajov v iných oblastiach[39]. V dôsledku toho stále existuje určitá miera fragmentácie, ktorá je spôsobená najmä rozsiahlym používaním voliteľných delegačných ustanovení. Napríklad rozdiel medzi členskými štátmi vo veku, v ktorom deti poskytujú súhlas vo vzťahu k službám informačnej spoločnosti, spôsobuje neistotu pre deti a ich rodičov, pokiaľ ide o uplatňovanie ich práv na ochranu údajov na jednotnom trhu. Táto fragmentácia takisto spôsobuje problémy pre cezhraničné podnikanie, inovácie, najmä pokiaľ ide o nový technologický vývoj a riešenia v oblasti kybernetickej bezpečnosti. V záujme účinného fungovania vnútorného trhu a s cieľom vyhnúť sa zbytočnému zaťaženiu spoločností je takisto nevyhnutné, aby vnútroštátne právne predpisy neprekračovali právne rámce stanovené vo všeobecnom nariadení o ochrane údajov, resp. aby nestanovovali nové požiadavky, ak takéto rámce neexistujú.

Osobitnou výzvou pre vnútroštátne právne predpisy je zosúladenie práva na ochranu osobných údajov so slobodou prejavu a právom na informácie a riadne vyváženie týchto práv. Niektoré vnútroštátne právne predpisy zakotvujú zásadu prednosti slobody prejavu, kým iné stanovujú prednosť ochrany osobných údajov a výnimky z uplatňovania pravidiel ochrany údajov uvádzajú len v špecifických situáciách, ako napríklad v prípade osoby s verejným postavením. Iné členské štáty stanovili určité vyvažovanie zákonodarcom a/alebo hodnotenie jednotlivých prípadov, pokiaľ ide o výnimky z určitých ustanovení všeobecného nariadenia o ochrane údajov.

Komisia bude pokračovať vo svojom hodnotení vnútroštátnych právnych predpisov. Zosúladenie musí byť stanovené zákonom, rešpektovať podstatu uvedených základných práv a musí byť primerané a nevyhnutné[40]. Pravidlá ochrany údajov (ako aj ich výklad a uplatňovanie) by nemali mať vplyv na uplatňovanie slobody prejavu a práva na informácie, napríklad vytvorením odrádzajúceho účinku alebo vyvíjaním tlaku na novinárov, aby zverejnili svoje zdroje. Vyváženie týchto dvoch

[35] Pozri bod 2.4 pracovného dokumentu útvarov Komisie.
[36] Najnovšie prostredníctvom listu komisára Reyndersa v marci 2020.
[37] Treba poznamenať, že vnútroštátny orgán pre ochranu osobných údajov v Slovinsku je zriadený na základe súčasných vnútroštátnych právnych predpisov o ochrane údajov a dohliada na uplatňovanie všeobecného nariadenia o ochrane údajov v tomto členskom štáte.
[38] Pozri bod 3.1 pracovného dokumentu útvarov Komisie.
[39] Pozri bod 3.2 pracovného dokumentu útvarov Komisie.
[40] Článok 52 ods. 1 Charty.

práv vnútroštátnymi právnymi predpismi by malo byť v súlade s judikatúrou Súdneho dvora a Európskeho súdu pre ľudské práva[41].

V právnych predpisoch členských štátov sa uplatňujú rôzne prístupy pri uplatňovaní výnimiek zo všeobecného zákazu spracúvania osobitných kategórií osobných údajov, pokiaľ ide o úroveň špecifikácie a záruk, a to aj na účely zdravotníctva a výskumu. S cieľom riešiť tento problém Komisia ako prvý krok mapuje rôzne prístupy členských štátov[42] a ako nasledujúci krok podporí vytvorenie kódexu či kódexov správania, ktoré by prispeli k dôslednejšiemu prístupu v tejto oblasti a uľahčili cezhraničné spracúvanie osobných údajov[43]. Okrem toho k harmonizovanému prístupu prispejú aj budúce usmernenia výboru o používaní osobných údajov v oblasti vedeckého výskumu. Komisia poskytne výboru informácie, najmä pokiaľ ide o výskum v oblasti zdravotníctva, a to aj vo forme konkrétnych otázok a analýz konkrétnych scenárov, ktoré získala od výskumnej obce.

[41] Pozri v bode 3.1 pracovného dokumentu útvarov Komisie. Zosúladenie práva na ochranu osobných údajov a slobody prejavu a práva na informácie.

[42] Komisia spustila štúdiu o „posúdení pravidiel členských štátov v oblasti údajov týkajúcich sa zdravia z hľadiska všeobecného nariadenia o ochrane údajov“ Chafea/2018/Health/03, špecifická zmluva č. 2019 70 01.

[43] Pozri opatrenia oznámené v Európskej dátovej stratégii, strana 30.

Posilnenie postavenia jednotlivcov pri kontrole ich údajov

Podľa prieskumu o základných právach[44] 69 % obyvateľov EÚ starších ako 16 rokov počulo o všeobecnom nariadení o ochrane údajov a 71 % ľudí v EÚ vie o svojom vnútroštátnom orgáne pre ochranu údajov.

Jednotlivci si čoraz viac uvedomujú svoje práva: práva na prístup, opravu, vymazanie a prenosnosť ich osobných údajov, právo namietať proti spracovaniu, ako aj posilnenú transparentnosť. Posilnené procesné práva vo všeobecnom nariadení o ochrane údajov zahŕňajú právo podať sťažnosť orgánu pre ochranu osobných údajov, a to aj prostredníctvom žalôb v zastúpení, a právo na súdny prostriedok nápravy. Jednotlivci čoraz častejšie využívajú tieto práva, ale je potrebné uľahčiť ich uplatňovanie a ich plné presadzovanie. Úvahy, ktoré vedie výbor, vyjasnia a ďalej uľahčia uplatňovanie individuálnych práv, kým prijatie navrhovanej smernice o žalobách v zastúpení[45] by malo umožniť jednotlivcom podať kolektívnu žalobu vo všetkých členských štátoch a znížiť náklady na cezhraničné konania.

Právo na prenosnosť údajov má jasný potenciál, ale stále nie je plne využitý na to, aby sa jednotlivci stali stredobodom dátového hospodárstva tým, že sa im umožní meniť rôznych poskytovateľov služieb, kombinovať rôzne služby, využívať iné inovatívne služby a vybrať si služby, ktoré sú najpriaznivejšie pre ochranu údajov. Tým sa nepriamo podporí hospodárska súťaž a inovácie. Využitie tohto potenciálu je jednou z priorít Komisie, najmä preto, že pri čoraz širšom využití zariadení „internetu vecí“ spotrebitelia generujú stále viac údajov, a existuje pre nich riziko, že budú čeliť nekalým praktikám a odkázanosti na určitého dodávateľa. Prenosnosť by mohla priniesť významné výhody v súvislosti so zdravím a blahobytom, zníženú environmentálnu stopu, ako aj prístup k verejným a súkromným službám, vyššiu produktivitu vo výrobe a zvýšenie kvality a bezpečnosti výrobkov.

V dátovej stratégii sa zdôraznila potreba riešiť problémy, ako je nedostatok noriem umožňujúcich poskytovanie údajov v strojovo čitateľnom formáte, zvýšenie účinného využívania práva na prenosnosť údajov, ktoré je v súčasnosti obmedzené na niekoľko sektorov (napr. bankovníctvo a telekomunikácie). Mohlo by sa to dosiahnuť najmä prostredníctvom návrhu vhodných nástrojov, normalizovaného formátu a rozhraní[46]. Toto zvýšené využívanie by sa mohlo dosiahnuť najmä povinným zavedením technických rozhraní a strojovo čitateľných formátov umožňujúcich prenosnosť údajov v reálnom čase. Zvýšené využívanie práva na prenosnosť by mohlo okrem iného uľahčiť jednotlivcom povoľovanie využívania ich údajov vo verejnom záujme (napríklad na podporu výskumu v oblasti zdravotníctva), ak si to želajú („dátový altruizmus“). Komisia pri príprave balíka predpisov o digitálnych službách[47] komplexnejšie preskúma úlohu údajov a postupov s nimi súvisiacich v rámci ekosystému platforiem.

---

[44] Agentúra Európskej únie pre základné práva (FRA) (2020): Prieskum základných práv za rok 2019. Ochrana údajov a technológie: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection

[45] Očakáva sa, že navrhovaná smernica o žalobách v zastúpení na ochranu kolektívnych záujmov spotrebiteľov [COM/2018/0184 final – 2018/089 (COD)] po prijatí posilní rámec pre žaloby v zastúpení aj v oblasti ochrany údajov.

[46] Tieto nástroje môžu zahŕňať nástroje na riadenie súhlasu a aplikácie na riadenie osobných informácií.

[47] https://ec.europa.eu/commission/presscorner/detail/sk/ip_20_962.

Príležitosti a výzvy pre organizácie, najmä pre malé a stredné podniky

Všeobecné nariadenie o ochrane údajov spolu s nariadením o voľnom toku iných ako osobných údajov[48] ponúka spoločnostiam príležitosti, ktoré plynú z podpory hospodárskej súťaže a inovácií, zabezpečenia voľného toku údajov v rámci EÚ a vytvárania rovnakých podmienok so spoločnosťami usadenými mimo EÚ[49]. Je možné, že právo na prenosnosť a čoraz vyšší počet jednotlivcov, ktorí hľadajú riešenia priaznivejšie z hľadiska ochrany osobných údajov, znížia prekážky brániace vstupu pre podniky a otvoria možnosti rastu na základe dôvery a inovácie. Niektoré zainteresované strany uvádzajú, že uplatňovanie všeobecného nariadenia o ochrane údajov je náročné najmä pre malé a stredné podniky (MPS). V zmysle prístupu založeného na riziku by nebolo vhodné stanoviť výnimky na základe veľkosti hospodárskeho subjektu, pretože jeho veľkosť nie je sama osebe ukazovateľom rizík, ktoré vyplývajú pre jednotlivcov zo spracúvania osobných údajov, ktoré vykonáva daný hospodársky subjekt. Niekoľko orgánov pre ochranu osobných údajov poskytlo praktické nástroje na uľahčenie uplatňovania všeobecného nariadenia o ochrane údajov pre MSP, ktoré vykonávajú spracovateľské činnosti s nízkym rizikom. Toto úsilie by sa malo zintenzívniť a rozšíriť, najlepšie formou jednotného európskeho prístupu, aby sa nevytvárali prekážky jednotnému trhu.

Orgány pre ochranu osobných údajov vypracovali celý rad činností, ktoré majú pomôcť MSP spĺňať požiadavky všeobecného nariadenia o ochrane údajov, napríklad poskytli vzory zmlúv o spracúvaní údajov a záznamov o spracovateľských činnostiach alebo zabezpečili semináre a telefonické linky na konzultácie. Mnohé z týchto iniciatív boli financované z prostriedkov EÚ[50]. S cieľom uľahčiť malým a stredným podnikom uplatňovanie všeobecného nariadenia o ochrane údajov by sa mali zvážiť aj ďalšie aktivity.

Vo všeobecnom nariadení o ochrane údajov sa poskytuje súbor nástrojov pre všetky typy spoločností a organizácií, ktorý im má pomôcť preukázať súlad, napríklad kódexy správania, certifikačné mechanizmy a štandardné zmluvné doložky. Tento súbor nástrojov by sa mal využívať v plnom rozsahu. MSP zdôrazňujú najmä význam a užitočnosť kódexov správania, ktoré sú prispôsobené ich situácii a nepredstavujú neprimerané náklady. Pokiaľ ide o certifikačné schémy, kľúčovými prvkami, ktoré sa majú zvážiť podľa všeobecného nariadenia o ochrane údajov a pri ktorých by sa zišiel spoločný a ambiciózny prístup v rámci celej EÚ, sú bezpečnosť (vrátane kybernetickej bezpečnosti) a špecificky navrhnutá ochrana údajov. Komisia v súčasnosti pracuje na štandardných zmluvných doložkách medzi prevádzkovateľmi

[48] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1807 zo 14. novembra 2018 o rámci pre voľný tok iných ako osobných údajov v Európskej únii, Ú. v. EÚ L 303, 28.11.2018, s. 59 – 68.

[49] Pozri bod 5 pracovného dokumentu útvarov Komisie. Pozri aj COM(2019) 250 final – Usmernenie k nariadeniu o rámci pre voľný tok iných ako osobných údajov v Európskej únii, v ktorom sú vysvetlené pravidlá spracúvania zmiešaných súborov údajov pozostávajúcich z osobných údajov aj iných ako osobných údajov, čo je praktické pre podniky vrátane MSP.

[50] Komisia poskytla finančnú podporu v troch vlnách grantov v celkovej výške 5 miliónov EUR, pričom posledné dve vlny boli osobitne zamerané na podporu vnútroštátnych orgánov pre ochranu osobných údajov v ich úsilí o spoluprácu s jednotlivcami a malými a strednými podnikmi: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en. V roku 2020 sa pridelí ďalší 1 milión EUR.

a sprostredkovateľmi[51], pričom vychádza z prác prebiehajúcich na modernizácii štandardných zmluvných doložiek pre medzinárodné prenosy[52].

Uplatňovanie všeobecného nariadenia o ochrane údajov na nové technológie

Všeobecné nariadenie o ochrane údajov, koncipované ako technologicky neutrálne, je založené na zásadách, a teda je navrhnuté tak, aby sa vzťahovalo aj na nové technológie, ktoré budú vznikať.

Považuje sa za základný a flexibilný nástroj, ktorý zabezpečí, aby vývoj nových technológií bol v súlade so základnými právami. Legislatívny rámec ochrany údajov a súkromia preukázal svoj význam a pružnosť práve počas krízy spôsobenej ochorením COVID-19, najmä v súvislosti s vývojom aplikácií na sledovanie kontaktov a iných technologických riešení na boj proti pandémii. Výzvou do budúcnosti je objasniť, akým spôsobom sa osvedčené zásady budú uplatňovať na špecifické technológie, napríklad na umelú inteligenciu, blockchain, internet vecí alebo rozpoznávanie tváre, ktoré si vyžadujú nepretržité monitorovanie. V Bielej knihe Komisie o umelej inteligencii[53] sa napríklad otvorila verejná diskusia o osobitných okolnostiach, za ktorých – ak vôbec – by mohlo byť opodstatnené použiť umelú inteligenciu na účely biometrickej identifikácie na diaľku (napríklad rozpoznávanie tváre) na verejných miestach, a o spoločných zárukách. V tejto súvislosti by orgány pre ochranu osobných údajov mali byť pripravené zapojiť sa do procesov technického návrhu od samého začiatku.

Pevné a účinné presadzovanie všeobecného nariadenia o ochrane údajov vo vzťahu k veľkým digitálnym platformám a integrovaným spoločnostiam, a to aj v oblastiach, ako sú online reklama a mikrozacielenie, je zároveň zásadným prvkom ochrany jednotlivcov.

Vypracovanie moderného súboru nástrojov pre medzinárodné prenosy údajov

Všeobecné nariadenie o ochrane údajov ponúka modernizovaný súbor nástrojov na uľahčenie prenosu osobných údajov z EÚ do tretej krajiny alebo medzinárodnej organizácie, pričom zabezpečuje, aby tieto údaje naďalej využívali vysokú úroveň ochrany. V posledných dvoch rokoch Komisia zintenzívnila prácu na plnom využití potenciálu nástrojov dostupných podľa všeobecného nariadenia o ochrane údajov.

Zahŕňa to aktívnu spoluprácu s kľúčovými partnermi s cieľom dosiahnuť „rozhodnutie o primeranosti“. Účinkom takéhoto rozhodnutia je umožniť bezpečný a voľný tok osobných údajov do dotknutej tretej krajiny bez potreby toho, aby vývozca údajov musel poskytnúť ďalšie záruky alebo získať akékoľvek povolenie. Konkrétne rozhodnutia o vzájomnej primeranosti medzi EÚ a Japonskom, ktoré nadobudli účinnosť v februári 2019, vytvorili najväčšiu oblasť voľného a bezpečného toku údajov na svete. V pokročilom štádiu je tiež proces posudzovania primeranosti s Kórejskou republikou a prebiehajú prieskumné rokovania s ďalšími dôležitými partnermi v Ázii a Latinskej Amerike.

[51] Podľa článku 28 všeobecného nariadenia o ochrane údajov.
[52] Podľa článku 46 všeobecného nariadenia o ochrane údajov.
[53] Biela kniha o umelej inteligencii – európsky prístup k excelentnosti a dôvere, COM(2020) 65 final.

Primeranosť zohráva dôležitú úlohu aj v súvislosti s budúcim vzťahom so Spojeným kráľovstvom za predpokladu, že sú splnené príslušné podmienky. Predstavuje kľúčový faktor pre obchod vrátane digitálneho obchodu a základný predpoklad úzkej a ambicióznej spolupráce v oblasti presadzovania práva a bezpečnosti. Dôležitým prvkom pre zabezpečenie rovnakých podmienok medzi týmito dvoma úzko integrovanými ekonomikami je aj vysoká miera konvergencie v oblasti ochrany údajov. V súlade s politickým vyhlásením o budúcom vzťahu medzi EÚ a Spojeným kráľovstvom Komisia v súčasnosti vykonáva posúdenie primeranosti podľa všeobecného nariadenia o ochrane údajov, ako aj podľa smernice o presadzovaní práva v oblasti ochrany údajov[54].

V rámci prvého hodnotenia všeobecného nariadenia o ochrane údajov sa od Komisie takisto vyžaduje, aby preskúmala rozhodnutia o primeranosti, ktoré boli prijaté podľa predchádzajúcich pravidiel[55]. Útvary Komisie nadviazali intenzívny dialóg so všetkými 11 dotknutými tretími krajinami a územiami[56] s cieľom posúdiť, ako sa vyvinuli ich systémy ochrany údajov od prijatia rozhodnutia o primeranosti a či spĺňajú štandard stanovený vo všeobecnom nariadení o ochrane údajov. Potreba zabezpečiť kontinuitu takýchto rozhodnutí ako kľúčového nástroja pre obchod a medzinárodnú spoluprácu je jedným z faktorov, ktoré viedli viaceré z týchto krajín a území k modernizácii a posilneniu ich predpisov o ochrane súkromia. S niektorými z týchto krajín a území sa rokuje o dodatočných zárukách, ktoré majú riešiť príslušné rozdiely v ochrane. Vzhľadom na to, že rozsudok, ktorý má Súdny dvor vydať 16. júla, môže poskytnúť objasnenia, ktoré by mohli byť relevantné pre určité prvky štandardu primeranosti, Komisia predloží samostatnú správu týkajúcu sa hodnotenia existujúcich rozhodnutí o primeranosti po tom, ako Súdny dvor vynesie rozsudok v tejto veci[57].

Okrem činnosti v oblasti primeranosti Komisia pracuje aj na komplexnej modernizácii štandardných zmluvných doložiek, aby ich aktualizovala vzhľadom na nové požiadavky zavedené vo všeobecnom nariadení o ochrane údajov. Cieľom je lepšie zohľadniť realitu spracovateľských operácií v modernom digitálnom hospodárstve a zvážiť prípadnú potrebu ďalšieho objasnenia určitých záruk, a to aj vzhľadom na očakávanú judikatúru Súdneho dvora[58]. Tieto doložky sú zďaleka najpoužívanejším mechanizmom prenosu údajov. Spoliehajú sa na ne tisíce spoločností z EÚ pri poskytovaní širokej škály služieb svojim klientom, dodávateľom, partnerom a zamestnancom.

---

[54] Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV, Ú. v. EÚ L 119, 4.5.2016, s. 89 – 131.

[55] Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov, Ú. v. ES L 281 23.11.1995, s. 31 – 50.

[56] Ide o tieto krajiny a územia: Andorra, Argentína, Faerské ostrovy, Guernsey, Izrael, Jersey, Kanada, Nový Zéland, Ostrov Man, Švajčiarsko a Uruguaj.

[57] Pozri vec C-311/18, Data Protection Commissioner/Facebook Ireland Limited, Maximillian Schrems (ďalej len „Schrems II“), ktorá sa týka návrhu na začatie prejudiciálneho konania týkajúceho sa takzvaných štandardných zmluvných doložiek. Súdny dvor však môže podrobnejšie objasniť aj určité prvky štandardu primeranosti.

[58] Pozri vec Schrems II.

Výbor zohral aktívnu úlohu aj pri rozvíjaní medzinárodných aspektov všeobecného nariadenia o ochrane údajov. Patrí k nim aktualizácia usmernenia o existujúcich mechanizmoch prenosu, napríklad pokiaľ ide o záväzné vnútropodnikové pravidlá a tzv. výnimky, ako aj vytvorenie právnej infraštruktúry na používanie nových nástrojov zavedených všeobecným nariadením o ochrane údajov, t. j. kódexov správania a certifikácie.

Aby zainteresované strany mohli plnohodnotne využívať súbor nástrojov zo všeobecného nariadenia o ochrane údajov týkajúci sa prenosu, je dôležité, aby výbor zintenzívnil prebiehajúce práce na rôznych mechanizmoch prenosu, napríklad aj ďalším zefektívnením postupu schvaľovania záväzných vnútropodnikových pravidiel, dokončením usmernenia pre kódexy správania a certifikáciu ako nástrojov pre prenos a objasnením vzájomnej interakcie pravidiel týkajúcich sa medzinárodných prenosov údajov (kapitola V) a územnej pôsobnosti uplatňovania všeobecného nariadenia o ochrane údajov (článok 3).

Ďalším dôležitým aspektom medzinárodného rozmeru pravidiel EÚ v oblasti ochrany údajov je rozšírená územná pôsobnosť všeobecného nariadenia o ochrane údajov, ktoré sa vzťahuje aj na spracovateľské činnosti zahraničných hospodárskych subjektov, ktoré pôsobia na trhu EÚ. Pre zabezpečenie účinného dodržiavania všeobecného nariadenia o ochrane údajov a skutočne rovnakých podmienok je nevyhnutné, aby sa toto rozšírenie náležite zohľadňovalo aj pri kontrolných akciách orgánov pre ochranu osobných údajov. Predovšetkým by mali v prípade potreby zahŕňať aj zástupcu prevádzkovateľa alebo sprostredkovateľa v EÚ, ktorého možno kontaktovať namiesto spoločnosti so sídlom mimo EÚ alebo spolu s ňou. Energickejšie by sa mal uplatňovať práve takýto prístup, aby sa vyslal jasný signál, že nezriadenie prevádzkarne v EÚ nezbavuje zahraničné hospodárske subjekty povinností podľa všeobecného nariadenia o ochrane údajov.

Podpora konvergencie a medzinárodnej spolupráce v oblasti ochrany údajov

Zo všeobecného nariadenia o ochrane údajov sa už stal kľúčový referenčný bod na medzinárodnej úrovni a pôsobí ako katalyzátor pre mnohé krajiny sveta, aby zvážili zavedenie moderných pravidiel ochrany súkromia. Tento trend smerom ku globálnemu zbližovaniu je veľmi pozitívny vývoj, ktorý prináša nové príležitosti, ako lepšie ochrániť jednotlivcov v EÚ pri prenose ich údajov do zahraničia, pričom zároveň uľahčuje toky údajov.

Stavajúc na tomto trende Komisia posilnila dialóg na viacerých bilaterálnych, regionálnych a multilaterálnych fórach s cieľom podporiť globálnu kultúru rešpektovania súkromia a rozvíjať prvky konvergencie medzi rôznymi systémami ochrany osobných údajov. Vo svojom úsilí sa Komisia spolieha na aktívnu podporu Európskej služby pre vonkajšiu činnosť, siete delegácií EÚ v tretích krajinách a misií v medzinárodných organizáciách, s ktorých podporou naďalej počíta. Umožnilo to aj väčšiu konzistentnosť a komplementárnosť medzi rôznymi aspektmi vonkajšieho rozmeru politík EÚ, počínajúc obchodom až po nové partnerstvo EÚ – Afrika. Aj skupiny G20 a G7 nedávno uznali príspevok ochrany údajov k dôvere k digitálnemu hospodárstvu a tokom údajov, a to najmä prostredníctvom koncepcie „spoľahlivého voľného toku údajov“ (*Data Free Flow with Trust*), ktorú pôvodne navrhlo japonské

predsedníctvo G20[59]. V dátovej stratégii sa zdôrazňuje zámer Komisie naďalej podporovať výmenu údajov s dôveryhodnými partnermi a zároveň bojovať proti zneužívaniu, ako je napríklad neprimeraný prístup (zahraničných) verejných orgánov k osobným údajom.

Popri podpore konvergencie v oblasti štandardov ochrany údajov na medzinárodnej úrovni ako prostriedku uľahčenia tokov údajov, a teda aj obchodu, je Komisia odhodlaná riešiť aj otázku digitálneho protekcionizmu, ako nedávno zdôraznila v dátovej stratégii[60]. Na tento účel vypracovala osobitné ustanovenia o tokoch údajov a ochrane údajov v obchodných dohodách[61], ktoré systematicky predkladá pri bilaterálnych rokovaniach – najnovšie s Austráliou, Novým Zélandom a Spojeným kráľovstvom – a multilaterálnych rokovaniach, napríklad na súčasných rokovaniach o elektronickom obchode v rámci WTO[62]. Týmito horizontálnymi ustanoveniami sa zabraňuje bezdôvodným obmedzeniam, napríklad požiadavkám na vynútenú lokalizáciu údajov, a zároveň sa zachováva regulačná autonómia strán pri ochrane základného práva na ochranu údajov.

Mali by sa preto ďalej skúmať synergie medzi nástrojmi na ochranu obchodu a nástrojmi na ochranu údajov, aby sa zabezpečili voľné a bezpečné medzinárodné toky údajov, ktoré sú nevyhnutné pre obchodné operácie, konkurencieschopnosť a rast európskych spoločností vrátane MSP v čoraz viac digitalizovanom hospodárstve.

Rovnako je dôležité zabezpečiť, aby spoločnosti pôsobiace na európskom trhu mohli v prípade vyzvania na výmenu údajov na základe oprávnenej žiadosti na účely presadzovania práva poskytnúť tieto údaje pri plnom rešpektovaní základných práv EÚ a bez toho, aby čelili kolízii právnych poriadkov. V záujme zlepšenia takýchto prenosov sa Komisia zaviazala vypracovať príslušné právne rámce spolu s medzinárodnými partnermi s cieľom predchádzať kolízii právnych poriadkov a podporiť účinné formy spolupráce, a to najmä zabezpečením potrebných záruk ochrany údajov, a tým prispieť k účinnejšiemu boju proti trestnej činnosti.

Praktická spolupráca medzi európskymi a medzinárodnými regulátormi by sa mala posilňovať predovšetkým v časoch, keď problémy pri dodržiavaní ochrany súkromia alebo incidenty spojené s bezpečnosťou údajov môžu ovplyvniť veľký počet jednotlivcov súbežne vo viacerých jurisdikciách. To si vyžaduje najmä vytvorenie vhodných právnych nástrojov pre užšie formy spolupráce a vzájomnej pomoci, napríklad umožnením potrebnej výmeny informácií v súvislosti s vyšetrovaniami. Práve v tomto duchu Komisia zriaďuje Akadémiu ochrany údajov – platformu, kde by si orgány pre ochranu osobných údajov z EÚ a zahraničia vymieňali poznatky,

---

[59] Pozri napríklad vyhlásenie vedúcich predstaviteľov skupiny G20 v Osake: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[60] Dátová stratégia, s. 23.

[61] Pozri znenie horizontálnych ustanovení pre cezhraničné toky údajov a pre ochranu osobných údajov (v obchodných a investičných dohodách EÚ): https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

[62] Do viacstranných rokovaní o elektronickom obchode v nadväznosti na iniciatívu pre spoločné vyhlásenie, ktorú prijali ministri 25. januára 2019 v Davose, sa v súčasnosti zapája 84 členov WTO. V rámci tohto procesu predložila EÚ 3. mája 2019 svoj návrh budúcich pravidiel a povinností v elektronickom obchode. Návrh obsahuje horizontálne ustanovenia o tokoch údajov a ochrane osobných údajov: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

skúsenosti a najlepšie postupy s cieľom sprostredkovať a podporovať spoluprácu medzi orgánmi presadzovania práva v oblasti ochrany súkromia.

3 ĎALŠÍ POSTUP

V záujme plného využitia potenciálu všeobecného nariadenia o ochrane údajov je dôležité vytvoriť harmonizovaný prístup a spoločnú európsku kultúru ochrany údajov a presadzovať účinnejšie a harmonizovanejšie riešenie cezhraničných prípadov. Očakávajú to ľudia aj podniky a predstavuje to základný cieľ reformy pravidiel EÚ v oblasti ochrany údajov. Rovnako dôležité je zabezpečiť plnohodnotné využívanie všetkých nástrojov dostupných podľa všeobecného nariadenia o ochrane údajov, aby sa zaručilo jeho efektívne uplatňovanie pre jednotlivcov a podniky.

Komisia bude pokračovať v bilaterálnych výmenách s členskými štátmi v súvislosti s vykonávaním všeobecného nariadenia o ochrane údajov a v prípade potreby bude naďalej využívať všetky nástroje, ktoré má k dispozícii, s cieľom podnietiť členské štáty k plneniu ich povinností podľa tohto nariadenia.

Vzhľadom na prebiehajúce posudzovanie vnútroštátnych právnych predpisov, krátke obdobie praktických skúseností od nadobudnutia účinnosti všeobecného nariadenia o ochrane údajov a vzhľadom na skutočnosť, že právne predpisy pre jednotlivé odvetvia sa v mnohých členských štátoch ešte stále len revidujú, je zatiaľ príliš skoro na vyvodenie konečných záverov o existujúcej miere roztrieštenosti. Pokiaľ ide o možnú kolíziu právnych poriadkov z dôvodu implementácie delegačných ustanovení v členských štátoch, je v prvom rade potrebné lepšie pochopiť dôsledky vyplývajúce pre prevádzkovateľov a sprostredkovateľov[63].

V nadväznosti na túto problematiku je prínosná príslušná judikatúra vnútroštátnych súdov a Súdneho dvora, ktorá pomáha vytvoriť jednotný výklad pravidiel ochrany údajov. Vnútroštátne súdy nedávno vydali rozsudky zrušujúce ustanovenia vnútroštátnych právnych predpisov, ktoré sa odchyľujú od všeobecného nariadenia o ochrane údajov[64].

Pokiaľ ide o medzinárodný rozmer, Komisia sa bude naďalej zameriavať na podporu zbližovania pravidiel ochrany údajov, ktoré vníma ako prostriedok na zabezpečenie bezpečných tokov údajov. To zahŕňa rôzne formy práce „smerom nahor“, napríklad v kontexte prebiehajúcich reforiem nových alebo aktualizovaných právnych predpisov o ochrane údajov, alebo presadzovanie koncepcie „spoľahlivého voľného toku údajov“ na multilaterálnych fórach. Patria sem aj rôzne dialógy o primeranosti, ako aj modernizácia a rozšírenie nášho súboru nástrojov na prenos údajov prostredníctvom aktualizácie štandardných zmluvných doložiek a položenie základov pre certifikačné mechanizmy. Táto práca zahŕňa aj medzinárodné rokovania, napríklad v oblasti cezhraničného prístupu k elektronickým dôkazom, s cieľom zabezpečiť, aby sa prenosy údajov uskutočňovali s vhodnými zárukami ochrany údajov. Účasťou na rokovaniach o medzinárodnej spolupráci a vzájomnej pomoci medzi orgánmi

[63] Pozri stanovisko Rady a zistenia týkajúce sa uplatňovania všeobecného nariadenia o ochrane údajov.
[64] Stalo sa tak v Nemecku a Španielsku, resp. v Rakúsku, čím sa odstránili rozdiely vo vnútroštátnych právnych predpisoch.

presadzovania ochrany údajov sa Komisia bude napokon usilovať o zbližovanie „teórie s praxou“.

Na základe tohto hodnotenia uplatňovania všeobecného nariadenia o ochrane údajov od mája 2018 sa určili nasledujúce činnosti, ktoré sú potrebné na podporu uplatňovania nariadenia. Komisia bude monitorovať ich vykonávanie aj vzhľadom na nadchádzajúcu hodnotiacu správu v roku 2024.

Vykonávanie a doplňanie právneho rámca

Členské štáty by mali

- dokončiť zosúlaďovanie svojich odvetvových právnych predpisov so všeobecným nariadením o ochrane údajov,
- zvážiť obmedzenie využívania delegačných ustanovení, ktoré by mohli vytvárať roztrieštenosť a ohrozovať voľný tok údajov v rámci EÚ,
- posúdiť, či vnútroštátne právne predpisy, ktorými sa vykonáva všeobecné nariadenie o ochrane údajov, sú za každých okolností v rámci hraníc stanovených právom členského štátu.

Komisia bude

- uskutočňovať bilaterálne výmeny s členskými štátmi na tému súladu vnútroštátnych právnych predpisov so všeobecným nariadením o ochrane údajov vrátane nezávislosti a zdrojov vnútroštátnych orgánov pre ochranu osobných údajov, využívať všetky nástroje, ktoré má k dispozícii, vrátane postupov v prípade nesplnenia povinnosti, s cieľom zabezpečiť, aby členské štáty dodržiavali všeobecné nariadenie o ochrane údajov,
- podporovať ďalšie výmeny názorov a vnútroštátnych postupov medzi členskými štátmi v oblastiach, ktoré sú predmetom bližšej špecifikácie na vnútroštátnej úrovni, s cieľom znížiť mieru roztrieštenosti jednotného trhu, napríklad v oblasti spracúvania osobných údajov týkajúcich sa zdravia a výskumu alebo v oblastiach, ktoré sú predmetom vyvažovania s inými právami, ako je napríklad sloboda prejavu,
- podporovať jednotné uplatňovanie rámca ochrany údajov v súvislosti s novými technológiami s cieľom podporovať inovácie a technologický vývoj,
- využívať expertnú skupinu členských štátov pre všeobecné nariadenie o ochrane údajov (zriadenú počas prechodnej fázy, kým sa nezačalo uplatňovať všeobecné nariadenie o ochrane údajov) na sprostredkovanie diskusie a výmeny skúseností medzi členskými štátmi a Komisiou,
- skúmať, či by vzhľadom na ďalšie skúsenosti a príslušnú judikatúru bolo vhodné navrhnúť prípadné budúce adresné zmeny určitých ustanovení všeobecného nariadenia o ochrane údajov, najmä pokiaľ ide o záznamy o spracovaní zo strany MSP, ktoré nemajú spracúvanie osobných údajov ako svoju hlavnú podnikateľskú činnosť (nízke riziko)[65], a o možnú harmonizáciu

[65] Článok 30 ods. 5 všeobecného nariadenia o ochrane údajov.

veku detí pre udelenie súhlasu v súvislosti so službami informačnej spoločnosti.

Dosiahnutie plného potenciálu nového systému riadenia

Výbor a orgány pre ochranu osobných údajov sa vyzývajú, aby

- medzi orgánmi pre ochranu osobných údajov vypracovali účinné opatrenia, pokiaľ ide o fungovanie mechanizmov spolupráce a konzistentnosti vrátane procedurálnych aspektov, pričom budú vychádzať z odborných znalostí svojich členov a posilnia aj zapojenie sekretariátu výboru,
- podporovali harmonizáciu pri uplatňovaní a presadzovaní všeobecného nariadenia o ochrane údajov s využitím všetkých prostriedkov, ktoré majú k dispozícii, vrátane ďalšieho objasnenia kľúčových prvkov všeobecného nariadenia o ochrane údajov, a zabezpečili, aby vnútroštátne usmernenia boli plne v súlade s usmerneniami prijatými výborom,
- podnecovali na využívanie všetkých nástrojov stanovených vo všeobecnom nariadení o ochrane údajov, aby sa zabezpečilo jednotné uplatňovanie nariadenia,
- zintenzívnili spoluprácu medzi orgánmi pre ochranu osobných údajov, napríklad vedením spoločných vyšetrovaní.

Komisia bude

- naďalej pozorne monitorovať účinnú a úplnú nezávislosť vnútroštátnych orgánov pre ochranu osobných údajov,
- podnecovať spoluprácu medzi regulátormi (najmä v oblastiach, ako je hospodárska súťaž, elektronická komunikácia, bezpečnosť sietí a informačných systémov a spotrebiteľská politika),
- podporovať úvahy v rámci výboru o postupoch uplatňovaných vnútroštátnymi orgánmi pre ochranu osobných údajov s cieľom zlepšiť spoluprácu v cezhraničných prípadoch.

Členské štáty

- pridelia zdroje orgánom pre ochranu osobných údajov, ktoré sú dostatočné na to, aby mohli plniť svoje úlohy.

Podpora zainteresovaných strán

Výbor a orgány pre ochranu osobných údajov sa vyzývajú, aby

- prijali ďalšie praktické, ľahko pochopiteľné usmernenia, v ktorých poskytnú jasné odpovede a zabránia nejasnostiam v otázkach týkajúcich sa uplatňovania všeobecného nariadenia o ochrane údajov, napríklad v otázkach spracúvania údajov detí a práv dotknutých osôb vrátane uplatňovania práva na prístup a práva na vymazanie, pričom tento postup budú konzultovať so zainteresovanými stranami,

– preskúmali usmernenia, ak sú potrebné ďalšie objasnenia vzhľadom na skúsenosti a vývoj, napríklad aj v judikatúre Súdneho dvora,

– vyvinuli praktické nástroje, ako napríklad harmonizované formuláre pre prípady porušenia ochrany údajov a zjednodušené záznamy o spracovateľských činnostiach, s cieľom pomôcť nízkorizikovým MSP splniť si svoje povinnosti.

Komisia

– poskytne štandardné zmluvné doložky pre medzinárodné prenosy, ako aj pre vzťah prevádzkovateľa a sprostredkovateľa,

– zabezpečí nástroje, ktoré objasnia/podporia uplatňovanie pravidiel ochrany údajov v prípade detí[66],

– v súlade s dátovou stratégiou preskúma praktické prostriedky, ako uľahčiť častejšie využívanie práva na prenosnosť zo strany jednotlivcov, napríklad tým, že sa im poskytne väčšia kontrola nad tým, kto môže získať prístup k strojovo generovaným údajom a používať ich,

– bude podporovať štandardizáciu/certifikáciu, a to predovšetkým aspektov kybernetickej bezpečnosti, prostredníctvom spolupráce medzi Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA), orgánmi pre ochranu osobných údajov a výborom,

– v prípade potreby využije svoje právo požiadať výbor o vypracovanie usmernení a stanovísk ku konkrétnym otázkam, ktoré sú dôležité pre zainteresované strany,

– v prípade potreby poskytne usmernenie, a to pri úplnom rešpektovaní úlohy výboru,

– bude podporovať také činnosti orgánov pre ochranu osobných údajov, ktoré uľahčujú vykonávanie povinností vyplývajúcich zo všeobecného nariadenia o ochrane údajov zo strany MSP, a to prostredníctvom finančnej podpory určenej najmä na praktické usmernenia a digitálne nástroje, ktoré možno uplatniť aj v iných členských štátoch.

Povzbudzovanie inovácií

Komisia bude

– monitorovať uplatňovanie všeobecného nariadenia o ochrane údajov na nové technológie, pričom zohľadní aj možné budúce iniciatívy v oblasti umelej inteligencie a v rámci dátovej stratégie,

– podporovať, a to aj prostredníctvom finančnej podpory, vypracovanie kódexov správania EÚ v oblasti zdravia a výskumu,

[66] Projekt Komisie týkajúci sa nástrojov na určovanie veku – pilotný projekt na predvedenie interoperabilnej technickej infraštruktúry na ochranu detí vrátane overovania veku a súhlasu rodičov. Očakáva sa, že sa tým podporí zavedenie mechanizmov ochrany detí založených na existujúcich právnych predpisoch EÚ týkajúcich sa ochrany detí online.

– pozorne sledovať vývoj a používanie aplikácií v súvislosti s pandémiou COVID-19.

Výbor sa vyzýva, aby

– vydal usmernenia o uplatňovaní všeobecného nariadenia o ochrane údajov v oblasti vedeckého výskumu, umelej inteligencie, technológie blockchain a ďalších možných technologických výdobytkov,

– preskúmal usmernenia, ak sú potrebné ďalšie objasnenia vzhľadom na technologický rozvoj.

Ďalší vývoj súboru nástrojov na prenosy údajov

Komisia

– bude viesť dialógy o primeranosti so zainteresovanými tretími krajinami v súlade so stratégiou stanovenou v jej oznámení z roku 2017 s názvom Výmena a ochrana osobných údajov v globalizovanom svete, ak je to možné aj zahrnutím prenosov údajov do pôsobnosti orgánov presadzovania trestného práva (podľa smernice o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov) a iných verejných orgánov; to zahŕňa aj čo najrýchlejšie dokončenie procesu posudzovania primeranosti s Kórejskou republikou,

– dokončí prebiehajúce hodnotenie existujúcich rozhodnutí o primeranosti a podá o tom správu Európskemu parlamentu a Rade,

– dokončí prácu na modernizácii štandardných zmluvných doložiek s cieľom aktualizovať ich so zreteľom na všeobecné nariadenie o ochrane údajov tak, aby zahŕňali všetky relevantné scenáre prenosu a lepšie odrážali moderné obchodné praktiky.

Výbor sa vyzýva, aby

– bližšie objasnil vzájomnú interakciu pravidiel týkajúcich sa medzinárodných prenosov údajov (kapitola V) a územnej pôsobnosti uplatňovania všeobecného nariadenia o ochrane údajov (článok 3),

– zabezpečil účinné vykonávanie voči hospodárskym subjektom so sídlom v tretích krajinách, na ktoré sa vzťahuje územná pôsobnosť uplatňovania všeobecného nariadenia o ochrane údajov, a to v príslušných prípadoch aj pokiaľ ide o vymenovanie zástupcu (článok 27),

– zefektívnil posudzovanie a následné schválenie záväzných vnútropodnikových pravidiel s cieľom urýchliť tento proces,

– dokončil prácu na architektúre, postupoch a kritériách posudzovania kódexov správania a certifikačných mechanizmov ako nástrojov na prenos údajov.

Podpora konvergencie a rozvoj medzinárodnej spolupráce

Komisia

– podporí prebiehajúce procesy reforiem v tretích krajinách týkajúce sa nových alebo modernizovaných pravidiel ochrany údajov, a to výmenou skúseností a najlepších postupov,

– zaangažuje afrických partnerov s cieľom presadzovať zbližovanie právnych predpisov a podporovať budovanie kapacít dozorných orgánov v rámci digitálnej kapitoly nového partnerstva EÚ – Afrika,

– posúdi, ako by bolo možné uľahčiť spoluprácu medzi súkromnými hospodárskymi subjektmi a orgánmi presadzovania práva, a to aj prostredníctvom rokovaní o bilaterálnych a multilaterálnych rámcoch prenosov údajov v súvislosti s prístupom zahraničných orgánov presadzovania trestného práva k elektronickým dôkazom, s cieľom zamedziť kolíziám právnych poriadkov pri súčasnom zabezpečení primeraných záruk ochrany údajov,

– bude spolupracovať s medzinárodnými a regionálnymi organizáciami, ako sú OECD, ASEAN alebo G20, s cieľom podporiť spoľahlivé toky údajov založené na vysokých štandardoch ochrany údajov, a to aj v súvislosti s iniciatívou spoľahlivého voľného toku údajov,

– zriadi Akadémiu ochrany údajov s cieľom uľahčiť a podporiť výmeny medzi európskymi a medzinárodnými regulátormi,

– bude podporovať medzinárodnú spoluprácu dozorných orgánov v oblasti presadzovania práva, a to aj formou rokovaní o dohodách o spolupráci a vzájomnej pomoci.