EVROPSKA
KOMISIJA

Bruselj, 24.6.2020
COM(2020) 264 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

Varstvo podatkov kot steber krepitve vloge državljanov in pristopa EU k digitalnemu prehodu – dve leti uporabe splošne uredbe o varstvu podatkov

{SWD(2020) 115 final}

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

Varstvo podatkov kot steber krepitve vloge državljanov in pristopa EU k digitalnemu prehodu – dve leti uporabe splošne uredbe o varstvu podatkov

1 PRAVILA O VARSTVU PODATKOV KOT STEBER KREPITVE VLOGE DRŽAVLJANOV IN PRISTOPA EU K DIGITALNEMU PREHODU

To je prvo poročilo o vrednotenju in pregledu splošne uredbe o varstvu podatkov[1] (v nadaljnjem besedilu: Uredba) ter zlasti o uporabi in delovanju pravil o prenosu osebnih podatkov v tretje države ali mednarodne organizacije ter pravil o sodelovanju in skladnosti v skladu s členom 97 Uredbe.

Uredba, ki se uporablja od 25. maja 2018, je v središču okvira EU[2], s katerim se zagotavlja temeljna pravica do varstva podatkov, kot je zapisana v Listini Evropske unije o temeljnih pravicah (člen 8) in Pogodbah (člen 16 Pogodbe o delovanju Evropske unije, v nadaljnjem besedilu: PDEU). Z Uredbo so se utrdili zaščitni ukrepi za varstvo podatkov, posameznikom so se zagotovile dodatne in močnejše pravice, povečala se je preglednost in zagotovila večja odgovornost vseh, ki ravnajo z osebnimi podatki v okviru področja uporabe Uredbe. Neodvisni organi za varstvo podatkov so prejeli močnejša in usklajena pooblastila za izvrševanje, poleg tega pa je bil vzpostavljen nov sistem upravljanja. Uredba prav tako ustvarja enake konkurenčne pogoje za vsa podjetja, ki poslujejo na trgu EU, ne glede na to, kje imajo sedež, ter zagotavlja prosti pretok podatkov v EU, s čimer krepi notranji trg.

Uredba je pomemben sestavni del pristopa k tehnologiji, ki je osredotočen na človeka, in kompas za uporabo tehnologije pri dvojnem zelenem in digitalnem prehodu, ki je značilen za oblikovanje politik EU. To je bilo nedavno poudarjeno v Beli knjigi o umetni inteligenci[3] in Sporočilu o evropski strategiji za podatke[4] (v nadaljnjem besedilu: strategija za podatke) iz februarja 2020.

V gospodarstvu, ki vse bolj sloni na obdelavi podatkov, tudi osebnih podatkov, je Uredba bistveno orodje za zagotavljanje, da lahko posamezniki bolje nadzorujejo svoje osebne podatke in da se ti podatki zakonito, pošteno in na pregleden način obdelujejo za zakonite namene. Obenem Uredba prispeva k spodbujanju zaupanja vrednih inovacij, zlasti prek pristopa na podlagi tveganja in načel, kot sta vgrajena in privzeta zasebnost. Komisija je predlagala dopolnitev zakonodajnega okvira za

---

[1] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (UL L 119, 4.5.2016, str. 1).

[2] Uredba se po vključitvi v Sporazum o Evropskem gospodarskem prostoru uporablja tudi za Norveško, Islandijo in Lihtenštajn.

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

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

varstvo podatkov in zasebnost[5] z uredbo o e-zasebnosti[6], ki naj bi nadomestila sedanjo direktivo o e-zasebnosti[7]. Ta predlog trenutno proučujeta sozakonodajalca in zelo je pomembno, da se zagotovi njegovo hitro sprejetje.

V okviru ključnih prioritet Komisije, kot sta „Evropa, pripravljena na digitalno dobo“[8] in „Evropski zeleni dogovor“[9], je mogoče razviti nove pobude za okrepitev aktivne vloge državljanov v digitalnem prehodu ter za čim večji izkoristek digitalnih orodij pri uresničevanju podnebno nevtralne družbe in bolj trajnostnega razvoja. Uredba določa okvir za te pobude in zagotavlja, da so zasnovane na način, ki učinkovito krepi vlogo posameznikov.

Strategija za podatke[10] poziva k oblikovanju „enotnega evropskega podatkovnega prostora“, pravega enotnega trga za podatke, ter desetih skupnih evropskih sektorskih podatkovnih prostorov, ki so relevantni za dvojni zeleni in digitalni prehod[11]. Pri vseh teh prioritetah sta bistvena jasen in izvedljiv okvir za varno izmenjavo podatkov ter večja razpoložljivost podatkov. V strategiji za podatke je bila napovedana tudi namera Komisije, da v prihodnji zakonodaji prouči, kako bi bilo mogoče podatke v javnih podatkovnih zbirkah uporabiti za namene znanstvenih raziskav na način, ki je skladen z Uredbo. Podatkovni prostori naj bi bili podprti z evropsko zvezo oblakov, ki bi zagotavljala storitve obdelave podatkov in infrastrukture v oblaku, skladne z zahtevami Uredbe. Uredba zagotavlja visoko raven varstva osebnih podatkov in osrednjo vlogo posameznikov v vseh teh podatkovnih prostorih, hkrati pa omogoča potrebno prožnost za upoštevanje različnih pristopov.

Gotovo pa potreba po zagotavljanju zaupanja in zahteve glede varstva osebnih podatkov niso omejene na EU. Posamezniki po svetu vse bolj cenijo zasebnost in varnost svojih podatkov. Kot kaže nedavna svetovna raziskava[12], vprašani menijo, da je to pomemben dejavnik, ki vpliva na njihove odločitve o nakupu in na njihovo ravnanje na spletu. Podjetja se vse pogosteje odzivajo na to zahtevo po zasebnosti,

---

[5] Ta zakonodajni okvir vključuje tudi direktivo o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj (Direktiva 2016/680) in uredbo o varstvu podatkov za institucije in organe EU (Uredba 2018/1725).

[6] Predlog uredbe Evropskega parlamenta in Sveta o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o zasebnosti in elektronskih komunikacijah) (COM(2017) 10 final – 2017/03 (COD)).

[7] Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

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

[9] Sporočilo Komisije Evropskemu parlamentu, Evropskemu svetu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij – Evropski zeleni dogovor (COM(2019) 640 final).

[10] Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij – Evropska strategija za podatke (COM(2020) 66 final).

[11] Teh deset skupnih evropskih sektorskih podatkovnih prostorov zajema naslednja področja: zdravstvo, industrijsko proizvodnjo, energijo, mobilnost, kmetijstvo, finančne podatke, javno upravo, skupni evropski podatkovni prostor za znanje in spretnosti, evropski podatkovni prostor za zeleni dogovor in evropski oblak za odprto znanost.

[12] Glej npr. Raziskavo o zasebnosti potrošnikov, ki jo je leta 2019 izvedlo podjetje Cisco (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf). Glede na to raziskavo, v kateri je sodelovalo 2 600 potrošnikov iz celega sveta, je precejšnje število potrošnikov že ukrepalo, da bi zaščitili svojo zasebnost, na primer z menjavo podjetij ali ponudnikov zaradi njihove politike glede podatkov ali prakse izmenjave podatkov.

med drugim s prostovoljnim ponujanjem nekaterih pravic in zaščitnih ukrepov iz Uredbe tudi svojim strankam iz tretjih držav. Prav tako številna podjetja spodbujajo spoštovanje osebnih podatkov kot konkurenčno in tržno prednost na svetovnem trgu, in sicer s ponujanjem inovativnih izdelkov in storitev, ki zagotavljajo nove rešitve v zvezi z zasebnostjo ali varnostjo podatkov. Zaradi povečane sposobnosti akterjev iz zasebnega in javnega sektorja, da podatke zbirajo in obdelujejo v velikem obsegu, se poleg tega porajajo pomembna in kompleksna vprašanja, ki zasebnost vse pogosteje umeščajo v središče javne razprave v različnih delih sveta.

Sprejetje Uredbe je spodbudilo tudi druge države v številnih regijah sveta k razmisleku o podobnem ravnanju. To je resnično globalen trend, ki sega od Čila do Južne Koreje, od Brazilije do Japonske, od Kenije do Indije in od Kalifornije do Indonezije. Vodilna vloga EU na področju varstva podatkov je pokazala, da lahko EU v svetovnem merilu postavlja standarde za urejanje digitalnega gospodarstva. To vlogo so ji priznali tudi vplivni posamezniki iz mednarodne skupnosti, kot na primer generalni sekretar ZN António Guterres, ki je dejal, da je Uredba „dala zgled [...] za podobne ukrepe drugod“ ter „poz[val] EU in njene države članice, naj bodo še naprej vodilne pri oblikovanju digitalne dobe ter naj ostanejo na čelu tehnoloških inovacij in predpisov“[13].

Sedanja kriza zaradi pandemije COVID-19 je nazorno prikazala globalizacijo razprave o zasebnosti tako v času krize kot tudi v času svetovnih prizadevanj za izhod iz nje. Več držav članic EU je sprejelo nujne ukrepe, da bi zavarovale javno zdravje. Uredba jasno določa, da morajo vsakršne omejitve spoštovati bistvo temeljnih pravic in svoboščin ter biti potreben in sorazmeren ukrep v demokratični družbi za zaščito javnega interesa, kot je javno zdravje. Zdaj, ko se ukrepi zapore postopno odpravljajo, morajo nosilci odločanja odgovoriti na pričakovanja državljanov in državljank glede tega, da bodo imeli na voljo zaupanja vredne digitalne rešitve, ki spoštujejo pravico do zasebnosti in zagotavljajo varstvo osebnih podatkov.

V mnogih državah se šteje, da so vgrajeno varstvo zasebnosti, kot je prostovoljna prijava s strani uporabnikov, zmanjšanje količine podatkov in njihova varnost ter izključitev geolociranja bistvenega pomena za zagotavljanje zanesljivosti in družbene sprejemljivosti rešitev na podlagi podatkov, ki so namenjene spremljanju in omejevanju širjenja virusa, določanju javnozdravstvenih protiukrepov, pomoči bolnikom ali izvajanju izhodnih strategij. V EU se je zakonodajni okvir za varstvo podatkov in zasebnost[14] izkazal za dovolj prožno orodje, da omogoča razvoj praktičnih rešitev (npr. aplikacij za sledenje) ob hkratnem zagotavljanju visoke ravni varstva osebnih podatkov. Komisija je v tem kontekstu 16. aprila 2020 objavila usmeritve v zvezi z varstvom podatkov za aplikacije, ki podpirajo boj proti pandemiji[15].

---

[13] Nagovor generalnega sekretarja ZN v italijanskem senatu dne 18. decembra 2019 (na voljo na strani: https://www.un.org/press/en/2019/sgsm19916.doc.htm).

[14] Ta okvir poleg Uredbe sestavlja direktiva o e-zasebnosti (Direktiva 2002/58/ES), ki med drugim določa pravila za dostop do informacij na terminalski opremi uporabnika in njihovo shranjevanje.

[15] Sporočilo Komisije z naslovom „Usmeritve v zvezi z varstvom podatkov za aplikacije, ki podpirajo boj proti pandemiji COVID-19“ (2020/C 124 I/01 – C/2020/2523 – UL C 124I, 17.4.2020, str. 1). Države članice EU so 16. aprila 2020 ob podpori Komisije razvile nabor orodij EU za uporabo mobilnih aplikacij za sledenje stikom in opozarjanje kot odziv na pandemijo koronavirusa. To je del

Varstvo osebnih podatkov je ključno tudi pri preprečevanju manipuliranja državljank in državljanov – zlasti z mikrociljanjem volivcev in volivk na podlagi nezakonite obdelave osebnih podatkov –, izogibanju vmešavanjem v demokratične procese in ohranjanju odprte razprave, poštenosti in preglednosti, brez katerih ni demokracije. Zato je Komisija septembra 2018 objavila Smernice o uporabi prava Unije o varstvu podatkov v volilnem kontekstu[16].

Komisija je pri tem vrednotenju in pregledu Uredbe upoštevala prispevke Sveta[17], Evropskega parlamenta[18], Evropskega odbora za varstvo podatkov (v nadaljnjem besedilu: odbor)[19] ter posameznih organov za varstvo podatkov[20], večdeležniške strokovne skupine[21] in drugih deležnikov, vključno prek povratnih informacij v zvezi z načrtom[22].

Na splošno so bili cilji Uredbe, tj. krepitev varstva pravice posameznikov do varstva osebnih podatkov in jamčenje prostega pretoka osebnih podatkov v EU[23], v dveh letih od začetka njene uporabe uspešno izpolnjeni. Vendar je bilo poleg tega opredeljenih kar nekaj področij, na katerih so v prihodnje potrebne izboljšave. Komisija se strinja z večino deležnikov in organov za varstvo podatkov, da bi bili na tej stopnji dokončni zaključki v zvezi z uporabo Uredbe prenagljeni. Verjetno je, da se bo večina vprašanj, ki so jih izpostavili države članice in deležniki, razjasnila v prihodnjih letih, ko bodo pridobljene nadaljnje izkušnje z uporabo Uredbe. Kljub temu so v poročilu poudarjeni dosedanji izzivi pri uporabi Uredbe in zarisani možni načini za njihovo reševanje.

To vrednotenje in pregled se osredotočata na vprašanji iz člena 97(2) Uredbe, tj. na mednarodne prenose osebnih podatkov ter na mehanizma za sodelovanje in skladnost, vendar je uporabljeni pristop širši in zajema tudi vprašanja, ki so jih v zadnjih dveh letih zastavili različni akterji.

2 GLAVNE UGOTOVITVE

Izvajanje Uredbe in delovanje mehanizmov za sodelovanje in skladnost

---

skupnega usklajenega pristopa v podporo postopnemu odpravljanju ukrepov zapore. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[16] Smernice Komisije o uporabi prava Unije o varstvu podatkov v volilnem kontekstu – Prispevek Evropske komisije k srečanju voditeljev v Salzburgu 19. in 20. septembra 2018 (COM(2018) 638 final).

[17] Stališče in ugotovitve Sveta o uporabi splošne uredbe o varstvu podatkov: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/sl/pdf.

[18] Pismo Odbora LIBE Evropskega parlamenta z dne 21. februarja 2020 komisarju Reyndersu, sklic: IPOL-COM-LIBE D (2020)6525.

[19] Prispevek odbora k vrednotenju Uredbe na podlagi člena 97, sprejet 18. februarja 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_en.

[21] Večdeležniška strokovna skupina za Uredbo, ki jo je ustanovila Komisija, vključuje predstavnike civilne družbe in podjetij, akademike in strokovnjake: 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] Glej na primer stališče in ugotovitve Sveta ter prispevek odbora.

Z Uredbo je bil vzpostavljen inovativen sistem upravljanja, ki je zasnovan na delovanju neodvisnih organov za varstvo podatkov v državah članicah in njihovem sodelovanju v čezmejnih primerih ter v Evropskem odboru za varstvo podatkov (v nadaljnjem besedilu: odbor). Prevladuje mnenje, da so organi za varstvo podatkov uravnoteženo uporabljali svoja okrepljena popravljalna pooblastila, vključno z opozorili in opomini, globami in začasnimi ali dokončnimi omejitvami obdelave[24]. Komisija ugotavlja, da so organi naložili upravne globe v višini od nekaj tisoč evrov do več milijonov evrov, odvisno od teže kršitev. Druge kazni, kot je prepoved obdelave, imajo lahko enako odvračilen ali še bolj odvračilen učinek kot globe. Končni cilj Uredbe je spremeniti kulturo in ravnanje vseh akterjev v korist posameznikov. Podrobnejše informacije o uporabi popravljalnih pooblastil organov za varstvo podatkov so predstavljene v spremnem delovnem dokumentu služb Komisije.

Čeprav je še prezgodaj za celovito oceno delovanja novih mehanizmov za sodelovanje in skladnost, so organi za varstvo podatkov razvili svoje sodelovanje prek mehanizma „vse na enem mestu“[25] in s široko uporabo medsebojne pomoči[26]. Mehanizem „vse na enem mestu“, ki je eden ključnih adutov notranjega trga, se uporablja za odločanje v mnogih čezmejnih primerih[27]. Pričakuje se, da se bodo v okviru tega mehanizma v kratkem obravnavale pomembne odločitve s čezmejno razsežnostjo. Te odločitve, ki pogosto vključujejo velike tehnološke večnacionalne družbe, bodo imele precejšen vpliv na pravice posameznikov v številnih državah članicah.

Vendar razvoj resnično skupne evropske kulture varstva podatkov med organi za varstvo podatkov še ni končan. Organi za varstvo podatkov še ne uporabljajo vseh orodij, ki jih ponuja Uredba, kot je skupno ukrepanje, ki bi lahko privedlo do skupnih preiskav. Včasih se je bilo treba pri iskanju skupnega pristopa zateči k najmanjšemu skupnemu imenovalcu in posledično niso bile izkoriščene priložnosti za večje usklajevanje[28].

Potreben je še dodaten napredek, da bi bila obravnava čezmejnih zadev učinkovitejša in bolj usklajena po vsej EU, med drugim tudi z vidika postopka samega, na primer v zvezi z vprašanji, kot so postopki za obravnavanje pritožb, merila dopustnosti pritožb, trajanje postopka zaradi različnih časovnih okvirov ali odsotnosti rokov v nacionalnem upravnem procesnem pravu, trenutek v postopku, ko je mogoče uveljavljati načelo kontradiktornosti, ali pa obveščanje in vključenost pritožnikov med postopkom. Postopek razmisleka, ki ga je v zvezi s tem začel odbor, je dobrodošel in Komisija se teh razprav udeležuje[29].

---

[24] Glej točko 2.1 delovnega dokumenta služb Komisije.

[25] Kadar podjetje obdeluje osebne podatke, ki izvirajo iz druge države, je pristojni organ za varstvo podatkov organ države članice, v kateri ima podjetje svoj glavni sedež.

[26] Glej točko 2.2 delovnega dokumenta služb Komisije.

[27] Med 25. majem 2018 in 31. decembrom 2019 je bilo v okviru postopka „vse na enem mestu“ predloženih 141 osnutkov odločitev, od tega je bila v 79 primerih sprejeta končna odločitev.

[28] Na primer bolje bi lahko bili usklajeni nacionalni seznami, ki zajemajo tiste vrste postopkov obdelave, za katere se v skladu s členom 35 Uredbe zahteva ocena učinka v zvezi z varstvom podatkov.

[29] Glej točko 2.2 delovnega dokumenta služb Komisije.

Dejavnosti in smernice odbora so ključnega pomena za dosledni nadaljnji razvoj izmenjav med odborom in deležniki[30]. Od konca leta 2019 je odbor sprejel 67 dokumentov, vključno z 10 novimi smernicami[31] in 43 mnenji[32]. Deležniki so na splošno z zadovoljstvom sprejeli smernice odbora in zahtevali dodatne smernice glede ključnih pojmov iz Uredbe, vendar so opozorili tudi na nedoslednosti med nacionalnimi navodili in smernicami odbora. Poudarili so potrebo po bolj praktičnih nasvetih, zlasti več konkretnih primerih, in potrebo, da se organom za varstvo podatkov zagotovijo potrebni človeški, tehnični in finančni viri, da bi lahko učinkovito opravljali svoje naloge.

Komisija je vseskozi poudarjala, da so države članice dolžne nacionalnim organom za varstvo podatkov dodeliti zadostne človeške, finančne in tehnične vire[33]. Večini organov je bilo med letoma 2016 in 2019 odobreno povečanje osebja in proračuna[34], pri čemer so irski, nizozemski, islandski, luksemburški in finski organi zabeležili sorazmerno največje povečanje osebja. Glede na to, da imajo največje tehnološke večnacionalne družbe sedež na Irskem in v Luksemburgu, so organi za varstvo podatkov teh dveh držav vodilni organi v številnih pomembnih čezmejnih primerih in bodo morda potrebovali obsežnejše vire, kot je mogoče sklepati glede na velikost njunega prebivalstva. Vendar je stanje v državah članicah še vedno neenakomerno in na splošno še ni zadovoljivo. Organi za varstvo podatkov imajo ključno vlogo pri zagotavljanju izvajanja Uredbe na nacionalni ravni in učinkovitega delovanja mehanizmov za sodelovanje in skladnost v okviru odbora, vključno zlasti z mehanizmom „vse na enem mestu“ za čezmejne primere. Države članice so zato pozvane, naj jim zagotovijo ustrezne vire, kot to zahteva Uredba[35].

Kljub harmoniziranim pravilom ostajajo določena razdrobljenost in različni pristopi

Komisija spremlja izvajanje Uredbe v nacionalnih zakonodajah. V času priprave tega poročila so razen Slovenije vse države članice sprejele novo zakonodajo o varstvu podatkov ali pa prilagodile obstoječo nacionalno zakonodajo. Slovenija[36] je bila pozvana, naj Komisiji zagotovi pojasnila o dokončanju tega postopka[37].

Uredba zagotavlja usklajen pristop k pravilom o varstvu podatkov po vsej EU, vendar pa od držav članic zahteva, da zakonsko uredijo nekatera področja[38], na drugih področjih pa jim daje možnost, da natančneje opredelijo, kako se bodo uporabljale

[30] Predvsem podjetja in predstavniki civilne družbe. Glej točko 2.3 delovnega dokumenta služb Komisije.
[31] Poleg 10 smernic, ki jih je sprejela Delovna skupina iz člena 29 v pripravah na začetek uporabe Uredbe in jih je potrdil odbor. Odbor je med januarjem in koncem maja 2020 sprejel tudi 4 dodatne smernice in posodobil obstoječe smernice.
[32] Od tega je bilo 42 mnenj sprejetih na podlagi člena 64 Uredbe in eno na podlagi člena 70(1)(s) Uredbe (nanašalo se je na sklep o ustreznosti za Japonsko).
[33] Sporočilo Komisije Evropskemu parlamentu in Svetu – Pravila o varstvu podatkov za utrjevanje zaupanja v EU in zunaj nje – ocena (COM(2019) 374 final z dne 27. julija 2019).
[34] Na splošno se je število osebja povečalo za 42 %, obseg proračuna pa za 49 %, gledano skupaj za vse nacionalne organe za varstvo podatkov v EGP med letoma 2016 in 2019.
[35] Glej točko 2.4 delovnega dokumenta služb Komisije.
[36] Nazadnje z dopisom evropskega komisarja Reyndersa marca 2020.
[37] Opozoriti je treba, da je nacionalni organ za varstvo podatkov v Sloveniji ustanovljen na podlagi veljavne nacionalne zakonodaje o varstvu podatkov in nadzira uporabo Uredbe v tej državi članici.
[38] Glej točko 3.1 delovnega dokumenta služb Komisije.

nekatere določbe Uredbe[39]. Zato ostaja določena razdrobljenost, ki je zlasti posledica obsežne uporabe določil o neobvezni natančnejši ureditvi. Na primer, razlikovanje med državami članicami glede starosti za privolitev otroka v zvezi s storitvami informacijske družbe ustvarja negotovost za otroke in njihove starše glede uporabe njihovih pravic do varstva podatkov na enotnem trgu. Takšna razdrobljenost prav tako ustvarja izzive za čezmejno poslovanje in inovacije, zlasti kar zadeva nov tehnološki razvoj in rešitve na področju kibernetske varnosti. Za dejansko delovanje notranjega trga in preprečitev nepotrebnih bremen za podjetja je bistveno tudi, da nacionalna zakonodaja ne presega mej, določenih v Uredbi, ali da uvaja dodatne zahteve, kadar meje niso določene.

Poseben izziv za nacionalno zakonodajo je uskladitev pravice do varstva osebnih podatkov s svobodo izražanja in obveščanja ter ustrezno uravnoteženje teh pravic. Nekatere nacionalne zakonodaje določajo načelo, da ima prednost svoboda izražanja, medtem ko druge določajo prednost varstvu osebnih podatkov in uporabo pravil o varstvu podatkov izvzemajo le v posebnih primerih, kot na primer za osebe z javnim statusom. Spet v drugih državah članicah za določeno uravnoteženje poskrbi zakonodajalec in/ali se odstopanja od nekaterih določb Uredbe ocenijo za vsak primer posebej.

Komisija bo nadaljevala ocenjevanje nacionalne zakonodaje. Omejevanje uresničevanja pravic in svoboščin mora biti predpisano z zakoni, upoštevati mora bistveno vsebino navedenih temeljnih pravic ter biti sorazmerno in potrebno[40]. Pravila o varstvu podatkov (pa tudi njihova razlaga in uporaba) ne bi smela vplivati na uveljavljanje svobode izražanja in obveščanja, na primer z ustvarjanjem zastraševalnega učinka ali izvajanjem pritiska na novinarje, da razkrijejo svoje vire. Uravnoteženje teh dveh pravic v nacionalnih zakonodajah bi moralo izhajati iz sodne prakse Sodišča in Evropskega sodišča za človekove pravice[41].

Zakonodaje držav članic različno pristopajo k izvajanju odstopanj od splošne prepovedi obdelave posebnih vrst osebnih podatkov, kar zadeva raven natančnejše ureditve in zaščitnih ukrepov, vključno za namene zdravja in raziskav. Komisija pri reševanju te težave kot prvi korak izvaja kartiranje različnih pristopov držav članic[42] in bo v nadaljevanju podprla pripravo kodeksov ravnanja, ki bi pripomogli k doslednejšemu pristopu na tem področju in olajšali čezmejno obdelavo osebnih podatkov[43]. Poleg tega bodo k usklajenemu pristopu prispevale prihodnje smernice odbora glede uporabe osebnih podatkov v znanstvenih raziskavah. Komisija bo odboru zagotovila informacije zlasti v zvezi z zdravstvenimi raziskavami, med drugim v obliki konkretnih vprašanj in analize posameznih scenarijev, ki jih je prejela od raziskovalne skupnosti.

---

[39] Glej točko 3.2 delovnega dokumenta služb Komisije.
[40] Člen 52(1) Listine.
[41] Glej točko 3.1 delovnega dokumenta služb Komisije. Uskladitev pravice do varstva osebnih podatkov s svobodo izražanja in obveščanja.
[42] Komisija je začela študijo z naslovom „Assessment of the Member States' rules on health data in the light of GDPR" (Ocena pravil držav članic na področju zdravstvenih podatkov glede na splošno uredbo o varstvu podatkov), Chafea/2018/Health/03, posebna pogodba št. 2019 70 01.
[43] Glej ukrepe, napovedane v Evropski strategiji za podatke, stran 30.

Omogočanje posameznikom, da bodo imeli nadzor nad lastnimi podatki

Po ugotovitvah raziskave o temeljnih pravicah[44] je 69 % prebivalcev in prebivalk EU, starejših od 16 let, že slišalo za Uredbo, 71 % ljudi v EU pa ve za nacionalni organ za varstvo podatkov v njihovi državi.

Posamezniki se vse bolj zavedajo svojih pravic: pravic do dostopa, popravka, izbrisa in prenosljivosti svojih osebnih podatkov, pravice do ugovora posamezni obdelavi in do večje preglednosti. Uredba je okrepila procesne pravice, ki zajemajo pravico do vložitve pritožbe pri organu za varstvo podatkov, vključno prek zastopniških tožb, in pravico do pravnega sredstva. Posamezniki te pravice vedno pogosteje uveljavljajo, vendar je treba olajšati njihovo uveljavljanje in polno izvrševanje. Razmislek o tem, ki ga vodi odbor, bo pojasnil in dodatno olajšal uveljavljanje pravic posameznikov, medtem ko naj bi predlagana direktiva z zastopniških tožbah[45], ko bo sprejeta, posameznikom omogočila vložitev skupinskih tožb v vseh državah članicah ter znižala stroške čezmejnih tožb.

Pravica do prenosljivosti podatkov ima jasen, a še ne v celoti izkoriščen potencial, da bi posameznike umestila v središče podatkovnega gospodarstva s tem, ko bi jim omogočila menjavo ponudnikov storitev, kombiniranje različnih storitev, uporabo drugih inovativnih storitev in izbiro storitev, ki v največji meri spoštujejo varstvo podatkov. To bo posredno spodbudilo konkurenco in podprlo inovacije. Sprostitev tega potenciala je ena od prioritet Komisije, še zlasti ker zaradi vse večjega obsega uporabe naprav v internetu stvari vedno večje količine podatkov ustvarjajo tudi potrošniki, ki tvegajo soočanje z nepoštenimi praksami in učinki „tehnološke vezanosti“. Prenosljivost bi lahko prinesla znatne koristi, povezane z zdravjem in dobrim počutjem, zmanjšanim okoljskim odtisom ter dostopom do javnih in zasebnih storitev, večjo produktivnostjo v proizvodnji ter večjo kakovostjo in varnostjo izdelkov.

V strategiji za podatke je bila poudarjena potreba po reševanju težav, kot so pomanjkanje standardov zagotavljanja podatkov v strojno berljivi obliki, da bi se povečala dejanska uporaba pravice do prenosljivosti podatkov, ki je trenutno omejena na nekaj sektorjev (npr. bančništvo in telekomunikacije). To bi bilo mogoče doseči zlasti z zasnovo primernih orodij, standardiziranih oblik in vmesnikov[46]. Tako povečanje uporabe bi bilo mogoče doseči tudi s pooblastitvijo tehničnih vmesnikov in strojno berljivih oblik, ki bi omogočali prenosljivost podatkov v realnem času. Povečana uporaba pravice do prenosljivosti bi lahko med drugim posameznikom, ki to želijo, olajšala soglašanje z uporabo njihovih podatkov za javno dobro (na primer za spodbujanje raziskav v zdravstvenem sektorju), t. i. „podatkovni altruizem“. Pri pripravi svežnja akta o digitalnih storitvah[47] bo Komisija širše proučila vlogo podatkov in s podatki povezanih praks v ekosistemu platform.

---

[44] Agencija Evropske unije za temeljne pravice (FRA) (2020): raziskava o temeljnih pravicah iz leta 2019. Varstvo podatkov in tehnologija: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection.

[45] Predlagana direktiva o zastopniških tožbah za varstvo kolektivnih interesov potrošnikov (COM(2018) 184 final – 2018/089 (COD)) naj bi, ko bo sprejeta, okrepila okvir za zastopniške tožbe tudi na področju varstva podatkov.

[46] Ta orodja lahko vključujejo orodja za upravljanje soglasij in aplikacije za upravljanje osebnih informacij.

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

Priložnosti in izzivi za organizacije, zlasti za mala in srednja podjetja

Uredba prinaša skupaj z uredbo o prostem pretoku neosebnih podatkov[48] priložnosti za podjetja, saj spodbuja konkurenco in inovacije, zagotavlja prosti pretok podatkov znotraj EU in ustvarja enake konkurenčne pogoje v primerjavi s podjetji s sedežem zunaj EU[49]. Glede na to, da vse več posameznikov išče rešitve, ki varujejo zasebnost, bi lahko pravica do prenosljivosti podatkov zmanjšala vstopne ovire za podjetja in prinesla možnosti za rast, ki temelji na zaupanju in inovacijah. Nekateri deležniki poročajo, da uporaba Uredbe povzroča težave zlasti malim in srednjim podjetjem (v nadaljnjem besedilu: MSP). V skladu s pristopom na podlagi tveganja ne bi bilo primerno, da se določijo odstopanja glede na velikost gospodarskih subjektov, saj njihova velikost sama po sebi ne odraža tveganj, ki bi jih za posameznike pomenila obdelava osebnih podatkov, ki jo ti subjekti izvajajo. Več organov za varstvo podatkov je zagotovilo praktična orodja, ki naj bi MSP z nizko tveganimi dejavnostmi obdelave omogočila lažje izvajanje Uredbe. Ta prizadevanja bi bilo treba okrepiti in razširiti, po možnosti v okviru skupnega evropskega pristopa, da ne bi ustvarili ovir za enotni trg.

Organi za varstvo podatkov so razvili vrsto dejavnosti, da bi MSP pomagali izpolnjevati obveznosti iz Uredbe. Izdelali so na primer predloge pogodb o obdelavi podatkov in evidence za dejavnosti obdelave, organizirali so seminarje in vzpostavili telefonske številke za posvetovanje. Več teh pobud je prejelo sredstva EU[50]. Razmisliti bi bilo treba o dodatnih dejavnostih, s katerimi bi MSP olajšali uporabo Uredbe.

Uredba daje vsem vrstam podjetij in organizacij na voljo nabor orodij za lažje dokazovanje skladnosti, kot so kodeksi ravnanja, mehanizmi certificiranja in standardna pogodbena določila. Ta nabor orodij bi bilo treba v celoti izkoristiti. MSP zlasti poudarjajo pomen in koristnost kodeksov ravnanja, ki so prilagojeni njihovim razmeram in ne povzročajo nesorazmernih stroškov. Kar zadeva certifikacijske sheme, sta varnost (vključno s kibernetsko varnostjo) in vgrajeno varstvo podatkov ključna elementa, ki ju je treba upoštevati v okviru Uredbe, in koristno bi bilo zanju pripraviti skupen in ambiciozen pristop po vsej EU. Komisija trenutno pripravlja standardna pogodbena določila med upravljavci in obdelovalci[51], pri čemer se opira na tekoče delo v zvezi s posodobitvijo standardnih pogodbenih določil za mednarodne prenose osebnih podatkov[52].

Uporaba Uredbe za nove tehnologije

---

[48] Uredba (EU) 2018/1807 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o okviru za prosti pretok neosebnih podatkov v Evropski uniji (UL L 303, 28.11.2018, str. 59).

[49] Glej točko 5 delovnega dokumenta služb Komisije. Glej tudi Smernice k uredbi o okviru za prosti pretok neosebnih podatkov v Evropski uniji (dokument COM(2019) 250 final), ki so praktične za podjetja, vključno z MSP, saj pojasnjujejo pravila, ki urejajo obdelavo mešanih podatkovnih nizov, sestavljenih iz osebnih in neosebnih podatkov.

[50] Komisija je zagotovila finančno podporo prek treh krogov nepovratnih sredstev v skupni vrednosti 5 milijonov EUR, pri čemer sta bila zadnja dva kroga namenjena prav podpori za nacionalne organe za varstvo podatkov pri njihovih prizadevanjih, da pomagajo posameznikom ter malim in srednjim podjetjem: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en. Dodatni milijon EUR bo dodeljen leta 2020.

[51] V skladu s členom 28 Uredbe.

[52] V skladu s členom 46 Uredbe.

Uredba, ki je bila zasnovana na tehnološko nevtralen način, temelji na načelih in je zato oblikovana tako, da zajema nove tehnologije, ki se razvijajo.

Velja za bistveno in prožno orodje, ki zagotavlja, da je razvoj novih tehnologij v skladu s temeljnimi pravicami. Zakonodajni okvir za varstvo podatkov in zasebnost se je med krizo zaradi izbruha COVID-19 izkazal kot pomemben in prožen, zlasti z vidika zasnove aplikacij za sledenje in drugih tehnoloških rešitev za boj proti pandemiji. V prihodnosti bo izziv pojasniti, kako naj bi se dokazana načela uporabljala za specifične tehnologije, kot so umetna inteligenca, blokovna veriga, internet stvari ali prepoznavanje obraza, ki zahtevajo stalno spremljanje. Komisijina Bela knjiga o umetni inteligenci[53] je na primer spodbudila javno razpravo o morebitnih posebnih okoliščinah, ki bi lahko upravičile uporabo umetne inteligence za namene biometrične identifikacije na daljavo (kot je prepoznavanje obraza) na javnih mestih, in o skupnih zaščitnih ukrepih. V tem pogledu bi morali biti organi za varstvo podatkov pripravljeni na to, da že v zgodnji fazi spremljajo postopke tehničnega načrtovanja.

Nenazadnje je močno in učinkovito uveljavljanje Uredbe v razmerju do velikih digitalnih platform in integriranih podjetij, tudi na področjih, kot sta spletno oglaševanje in mikrociljanje, bistven element za zaščito posameznikov.

Razvoj sodobnega nabora orodij za mednarodni prenos podatkov

Uredba ponuja posodobljen nabor orodij za olajšanje prenosa osebnih podatkov iz EU v tretjo državo ali mednarodno organizacijo, pri čemer zagotavlja, da so podatki še naprej deležni visoke ravni varstva. Komisija je v zadnjih dveh letih okrepila svoje delo, da bi izkoristila ves potencial orodij, ki so na voljo v okviru Uredbe.

V ta namen je med drugim dejavno sodelovala s ključnimi partnerji, da bi lahko sprejela „sklep o ustreznosti“. Tak sklep učinkuje tako, da omogoči varen in prosti pretok osebnih podatkov v zadevno tretjo državo, ne da bi moral izvoznik podatkov zagotoviti dodatne zaščitne ukrepe ali pridobiti kakršno koli dovoljenje. Vzajemna sklepa EU in Japonske o ustreznosti, ki sta začela veljati februarja 2019, sta ustvarila največje območje prostih in varnih tokov podatkov na svetu. Poleg tega je postopek za sprejetje sklepa o ustreznosti z Republiko Korejo v napredni fazi, potekajo pa tudi predhodni pogovori z drugimi pomembnimi partnerji v Aziji in Latinski Ameriki.

Ustreznost je pomembna tudi v kontekstu prihodnjih odnosov z Združenim kraljestvom, če bodo izpolnjeni veljavni pogoji. Je dejavnik, ki omogoča trgovino, vključno z digitalno trgovino, ter bistven predpogoj za tesno in ambiciozno sodelovanje na področju kazenskega pregona in varnosti. Poleg tega je visoka stopnja konvergence na področju varstva podatkov pomemben element za zagotavljanje enakih konkurenčnih pogojev med dvema tako tesno povezanima gospodarstvoma. V skladu s politično izjavo o prihodnjih odnosih med EU in Združenim kraljestvom Komisija trenutno izvaja oceno ustreznosti na podlagi Uredbe in direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj[54].

[53] Bela knjiga o umetni inteligenci – evropski pristop k odličnosti in zaupanju (COM(2020) 65 final).

[54] Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij,

Komisija mora v okviru prvega vrednotenja Uredbe pregledati tudi sklepe o ustreznosti, ki so bili sprejeti na podlagi prejšnjih pravil[55]. Službe Komisije so z vsako od 11 zadevnih tretjih držav in ozemelj[56] začele intenziven dialog, da bi ocenile, kako so se od sprejetja sklepa o ustreznosti razvili njihovi sistemi za varstvo podatkov in ali so v skladu s standardi iz Uredbe. Potreba po zagotovitvi kontinuitete takšnih sklepov, ki so ključno orodje za trgovino in mednarodno sodelovanje, je eden od dejavnikov, zaradi katerih je več teh držav in ozemelj moderniziralo in okrepilo svojo zakonodajo o zasebnosti. Z nekaterimi od teh držav in ozemelj trenutno potekajo razprave o dodatnih zaščitnih ukrepih za obravnavanje relevantnih razlik v varstvu. Ker pa bo Sodišče v sodbi, ki bo izdana 16. julija, morda zagotovilo pojasnila, ki bi lahko bila pomembna za nekatere elemente standarda ustreznosti, bo Komisija ločeno poročala o vrednotenju obstoječih sklepov o ustreznosti, po tem ko bo Sodišče izdalo sodbo v navedeni zadevi[57].

Komisija si poleg svojega dela v zvezi z ustreznostjo prizadeva za celovito posodobitev standardnih pogodbenih določil, da bi bila usklajena z novimi zahtevami, ki jih je uvedla Uredba. Cilj je, da bi ta določila bolje odražala realnost dejanj obdelave v sodobnem digitalnem gospodarstvu in da bi se upoštevala morebitna potreba, tudi glede na pričakovano sodno prakso Sodišča[58], da se dodatno pojasnijo nekateri zaščitni ukrepi. Ta določila so daleč najpogosteje uporabljeni mehanizem za prenos podatkov in na tisoče podjetij v EU na njihovi podlagi zagotavlja najrazličnejše storitve za svoje stranke, dobavitelje, partnerje in zaposlene.

Tudi odbor je dejavno sodeloval pri oblikovanju mednarodnih vidikov Uredbe. To vključuje posodobitev smernic o obstoječih mehanizmih za prenos podatkov, kot so zavezujoča poslovna pravila in tako imenovana „odstopanja“, ter razvoj pravne infrastrukture za uporabo novih orodij, uvedenih z Uredbo, tj. kodeksov ravnanja in certificiranja.

Da bi deležnikom omogočili celovito uporabo nabora orodij za prenos podatkov, ki ga zagotavlja Uredba, je pomembno, da odbor okrepi svoje tekoče delo v zvezi z različnimi mehanizmi za prenos, vključno z nadaljnjo racionalizacijo postopka odobritve za zavezujoča poslovna pravila, dokončanjem smernic glede kodeksov ravnanja in certificiranja kot orodij za prenose ter pojasnitvijo medsebojnega vpliva pravil o mednarodnih prenosih podatkov (poglavje V) in ozemeljske veljavnosti Uredbe (člen 3).

Drug pomemben vidik mednarodne razsežnosti pravil EU o varstvu podatkov je razširjena ozemeljska veljavnost Uredbe, ki zajema tudi dejavnosti obdelave s strani tujih gospodarskih subjektov, ki so dejavni na trgu EU. Da bi zagotovili učinkovito

---

in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89).

[55] Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31).

[56] Te države in ozemlja so: Andora, Argentina, Ferski otoki, Guernsey, Izrael, Jersey, Kanada, Nova Zelandija, Otok Man, Švica in Urugvaj.

[57] Glej zadevo C-311/18, Data Protection Commissioner/Facebook Ireland Limited, Maximillian Schrems (v nadaljevanju: Schrems II), ki se navezuje na predlog za sprejetje predhodne odločbe glede t. i. standardnih pogodbenih določil. Vendar bo morda Sodišče dodatno pojasnilo tudi nekatere elemente standarda ustreznosti.

[58] Glej zadevo Schrems II.

skladnost z Uredbo in resnično enake konkurenčne pogoje, je bistveno, da organi za varstvo podatkov to razširitev ustrezno upoštevajo v izvršilnih ukrepih. Ti bi zlasti morali po potrebi vključevati predstavnika upravljavca ali obdelovalca v EU, ki ga je mogoče nasloviti poleg podjetja s sedežem zunaj EU ali namesto njega. Ta pristop bi bilo treba odločneje izvajati, saj bi tako poslali jasno sporočilo, da neobstoj poslovne enote v EU tujih gospodarskih subjektov ne odvezuje odgovornosti, ki jih imajo v skladu z Uredbo.

Spodbujanje konvergence in mednarodnega sodelovanja na področju varstva podatkov

Uredba je že postala ključna referenčna točka na mednarodni ravni in je številne države po svetu spodbudila k razmisleku o uvedbi sodobnih pravil o zasebnosti. Ta trend v smeri globalne konvergence je zelo pozitiven in prinaša nove priložnosti za boljšo zaščito posameznikov v EU, kadar se njihovi podatki prenašajo v tujino, hkrati pa olajšuje tokove podatkov.

Na podlagi tega trenda je Komisija okrepila dialog v številnih dvostranskih, regionalnih in večstranskih forumih, da bi spodbudila globalno kulturo spoštovanja zasebnosti in razvila elemente konvergence med različnimi sistemi zasebnosti. V svojih prizadevanjih se je in se bo tudi v prihodnje opirala na aktivno podporo Evropske službe za zunanje delovanje ter mreže delegacij EU v tretjih državah in misij v mednarodnih organizacijah. To je omogočilo tudi večjo skladnost in dopolnjevanje med različnimi vidiki zunanje razsežnosti politik EU, od trgovine do novega partnerstva med EU in Afriko. Tudi skupini G20 in G7 sta nedavno priznali prispevek varstva podatkov k zaupanju v digitalno gospodarstvo in tokove podatkov, zlasti prek koncepta „prostega pretoka podatkov na podlagi zaupanja“, ki ga je prvotno predlagalo japonsko predsedovanje skupini G20[59]. V strategiji za podatke je poudarjen namen Komisije, da še naprej spodbuja izmenjavo podatkov z zaupanja vrednimi partnerji, hkrati pa se bori proti zlorabam, kot je nesorazmeren dostop (tujih) javnih organov do osebnih podatkov.

Poleg spodbujanja konvergence standardov za varstvo podatkov na mednarodni ravni kot načina za olajšanje tokov podatkov in s tem trgovine je Komisija prav tako odločena, da bo obravnavala digitalni protekcionizem, kot je nedavno poudarila v strategiji za podatke[60]. V ta namen je pripravila posebne določbe o tokovih podatkov in varstvu podatkov v trgovinskih sporazumih[61], ki jih sistematično predlaga v dvostranskih pogajanjih, kot je nedavno storila v pogajanjih z Avstralijo, Novo Zelandijo in Združenim kraljestvom, ter v večstranskih pogajanjih, kot so sedanje razprave v STO o e-trgovanju[62]. Te horizontalne določbe izključujejo neutemeljene

[59] Glej npr. besedilo izjave voditeljev skupine G20 v Osaki: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[60] Strategija za podatke, str. 23.

[61] Glej besedilo horizontalnih določb za čezmejne tokove podatkov in varstvo osebnih podatkov (v trgovinskih in naložbenih sporazumih EU): https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

[62] 84 članic STO je zdaj vključenih v večstranska pogajanja o e-trgovanju, in sicer v okviru pobude, ki se je začela na podlagi skupne izjave, ki so jo ministri sprejeli 25. januarja 2019 v Davosu. V okviru tega procesa je EU 3. maja 2019 predložila predlog za prihodnja pravila in obveznosti v zvezi z e-trgovanjem. Predlog vključuje horizontalne določbe o tokovih podatkov in varstvu osebnih podatkov: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

omejitve, kot so zahteve za prisilno lokalizacijo podatkov, hkrati pa ohranjajo regulativno avtonomijo pogodbenic pri zaščiti temeljne pravice do varstva podatkov.

Zato bi bilo treba nadalje raziskati sinergije med trgovinskimi instrumenti in instrumenti za varstvo podatkov, da se zagotovijo prosti in varni mednarodni tokovi podatkov, ki so v vse bolj digitaliziranem gospodarstvu bistvenega pomena za poslovanje, konkurenčnost in rast evropskih podjetij, vključno z MSP.

Prav tako je pomembno zagotoviti, da lahko podjetja, ki so dejavna na evropskem trgu, na podlagi utemeljene zahteve za izmenjavo podatkov za namene kazenskega pregona takšne podatke izmenjajo brez tveganja kolizije zakonov in ob polnem spoštovanju temeljnih pravic EU. Za izboljšanje takih prenosov se je Komisija zavezala, da bo z mednarodnimi partnerji razvila ustrezne pravne okvire za preprečevanje kolizije zakonov in podpirala učinkovite oblike sodelovanja, zlasti z določitvijo potrebnih zaščitnih ukrepov za varstvo podatkov, s tem pa prispevala k učinkovitejšemu boju proti kriminalu.

V času, ko lahko vprašanja v zvezi s spoštovanjem zasebnosti ali incidenti v zvezi z varnostjo podatkov hkrati prizadenejo večje število posameznikov v različnih jurisdikcijah, pa bi bilo treba dodatno okrepiti sodelovanje „na terenu“ med evropskimi in mednarodnimi regulatorji. V ta namen je treba razviti ustrezne pravne instrumente za oblike tesnejšega sodelovanja in medsebojno pomoč, vključno z omogočanjem potrebne izmenjave informacij v okviru preiskav. Komisija v tem duhu ustanavlja tudi „Akademijo za varstvo podatkov“, tj. platformo, na kateri bodo organi EU in tuji organi za varstvo podatkov izmenjevali znanje, izkušnje in najboljše prakse ter tako olajšali in podprli sodelovanje med organi, ki skrbijo za izvrševanje zakonodaje o zasebnosti.

3 NADALJNJI KORAKI

Da bi se v celoti izkoristil potencial Uredbe, je treba oblikovati usklajen pristop in skupno evropsko kulturo varstva podatkov ter spodbujati učinkovitejše in bolj usklajeno obravnavanje čezmejnih primerov. To pričakujejo ljudje in podjetja; to je tudi glavni cilj reforme pravil EU o varstvu podatkov. Prav tako je pomembno zagotoviti, da se vsa orodja, ki jih ponuja Uredba, uporabljajo v celoti, da se zagotovi učinkovita uporaba za posameznike in podjetja.

Komisija bo nadaljevala dvostranske izmenjave z državami članicami o izvajanju Uredbe in po potrebi še naprej uporabljala vsa orodja, ki jih ima na voljo za spodbujanje skladnosti držav članic z njihovimi obveznostmi iz Uredbe.

Glede na potekajočo oceno nacionalnih zakonodaj, kratko obdobje praktičnih izkušenj od začetka uporabe Uredbe in dejstvo, da se sektorska zakonodaja v številnih državah članicah še vedno revidira, je še prezgodaj, da bi prišli do dokončnih ugotovitev o obstoječi ravni razdrobljenosti. Kar zadeva morebitno kolizijo zakonov zaradi izvajanja določil o natančnejši ureditvi v državah članicah, je treba najprej bolje razumeti posledice za upravljavce in obdelovalce[63].

[63] Primerjaj s stališčem in ugotovitvami Sveta glede uporabe Uredbe.

V zvezi s temi vprašanji sodna praksa nacionalnih sodišč in Sodišča Evropske unije pomaga oblikovati dosledno razlago pravil o varstvu podatkov. Nacionalna sodišča so pred kratkim izdala sodbe, s katerimi so razveljavila določbe v nacionalnih zakonih, ki odstopajo od Uredbe[64].

Kar zadeva mednarodno razsežnost, se bo Komisija še naprej osredotočala na spodbujanje konvergence pravil o varstvu podatkov kot načina za zagotavljanje varnih tokov podatkov. To vključuje različne oblike „pripravljalnega“ dela, na primer v okviru tekočih reform za nove ali posodobljene zakone o varstvu podatkov, ali spodbujanje koncepta „prostega pretoka podatkov na podlagi zaupanja“ v večstranskih forumih. Zajema tudi različne dialoge o ustreznosti ter posodobitev in razširitev našega nabora orodij za prenos s posodobitvijo standardnih pogodbenih določil in oblikovanjem temeljev za mehanizme certificiranja. To delo vključuje tudi mednarodna pogajanja, na primer na področju čezmejnega dostopa do elektronskih dokazov, da se zagotovi, da bodo prenosi podatkov potekali ob ustreznih zaščitnih ukrepih za varstvo podatkov. Komisija si bo s pogajanji o mednarodnem sodelovanju in medsebojni pomoči med nadzornimi organi, pristojnimi za varstvo podatkov, prizadevala za konvergenco „iz teorije v prakso“.

Na podlagi tega vrednotenja uporabe Uredbe od maja 2018 so v nadaljevanju našteti ukrepi opredeljeni kot potrebni za podporo njeni uporabi. Komisija bo spremljala njihovo izvajanje tudi z vidika prihodnjega poročila o vrednotenju leta 2024.

Izvajanje in dopolnitev pravnega okvira

Države članice bi morale:

- dokončati usklajevanje svojih sektorskih zakonov z Uredbo;
- razmisliti o omejitvi uporabe določil o natančnejši ureditvi, ki bi lahko povzročile razdrobljenost in ogrozile prosti pretok podatkov v EU;
- oceniti, ali je nacionalna zakonodaja, s katero se izvaja Uredba, v vseh okoliščinah v mejah, določenih za zakonodajo držav članic.

Komisija bo:

- dvostransko izmenjavala informacije z državami članicami o skladnosti nacionalne zakonodaje z Uredbo, vključno z informacijami o neodvisnosti in virih nacionalnih organov za varstvo podatkov; uporabljala vsa orodja, ki jih ima na voljo, vključno s postopki za ugotavljanje kršitev, da zagotovi skladnost držav članic z Uredbo;
- podpirala nadaljnje izmenjave mnenj in nacionalnih praks med državami članicami v zvezi z vprašanji, ki so podrobneje opredeljena na nacionalni ravni, kot je obdelava osebnih podatkov v zvezi z zdravjem in raziskavami, da se zmanjša raven razdrobljenosti enotnega trga, ali v zvezi z vprašanji, pri katerih je treba iskati ravnovesje z drugimi pravicami, kot je svoboda izražanja;

[64] Na primer v Nemčiji in Španiji, ali pa v Avstriji, s čimer se je zmanjšala vrzel v nacionalni zakonodaji.

– podpirala dosledno uporabo okvira za varstvo podatkov v zvezi z novimi tehnologijami za podporo inovacijam in tehnološkemu razvoju;

– uporabljala skupino strokovnjakov držav članic za Uredbo (ki je bila ustanovljena v prehodni fazi, preden se je Uredba začela uporabljati), da bi olajšala razprave in izmenjavo izkušenj med državami članicami ter s Komisijo;

- glede na nadaljnje izkušnje in relevantno sodno prakso preučila, ali bi bilo morda primerno predlagati prihodnje ciljno usmerjene spremembe nekaterih določb Uredbe, zlasti v zvezi z obveznostjo vodenja evidenc obdelave za MSP, katerih osnovna dejavnost ni obdelovanje osebnih podatkov (majhno tveganje)[65], in o morebitni uskladitvi zakonske starosti za privolitev otroka v zvezi s storitvami informacijske družbe.

Izkoriščanje celotnega potenciala novega sistema upravljanja

Odbor in organi za varstvo podatkov so pozvani, da:

– razvijejo učinkovite ureditve med organi za varstvo podatkov glede delovanja mehanizmov za sodelovanje in skladnost, tudi glede postopkovnih vidikov, pri čemer naj se oprejo na strokovno znanje članov odbora in krepijo sodelovanje njegovega sekretariata;

– podpirajo usklajevanje pri uporabi in izvrševanju Uredbe ter pri tem uporabljajo vsa sredstva, ki jih ima odbor na voljo, vključno z nadaljnjo pojasnitvijo ključnih pojmov Uredbe in zagotavljanjem, da so nacionalne smernice v celoti skladne s smernicami, ki jih je sprejel odbor;

– spodbujajo uporabo vseh orodij iz Uredbe, da zagotovijo njeno dosledno uporabo;

– okrepijo sodelovanje med organi za varstvo podatkov, na primer s skupnimi preiskavami.

Komisija bo:

– še naprej pozorno spremljala učinkovito in popolno neodvisnost nacionalnih organov za varstvo podatkov;

– spodbujala sodelovanje med regulatorji (zlasti na področjih, kot so konkurenca, elektronske komunikacije, varnost omrežij in informacijskih sistemov ter potrošniška politika);

– podpirala razmisleke v odboru o postopkih, ki jih uporabljajo nacionalni organi za varstvo podatkov, da bi se izboljšalo sodelovanje v čezmejnih primerih.

Države članice bodo:

– dodelile zadostne vire organom za varstvo podatkov, da bodo ti lahko izvajali svoje naloge.

[65] Člen 30(5) Uredbe.

Podpora deležnikom

Odbor in organi za varstvo podatkov so pozvani, da:

- v posvetovanju z deležniki sprejmejo nadaljnje praktične, lahko razumljive smernice, ki bodo ponujale jasne odgovore in ne bodo povzročale nejasnosti glede vprašanj, povezanih z uporabo Uredbe, na primer glede obdelave podatkov otrok in glede pravic posameznikov, na katere se nanašajo osebni podatki, vključno z uveljavljanjem pravice do dostopa in pravice do izbrisa;
- pregledajo smernice, da bi ugotovili, ali so glede na izkušnje in razvoj dogodkov, vključno s sodno prakso Sodišča, potrebna dodatna pojasnila;
- razvijejo praktična orodja, kot so usklajeni obrazci za kršitve podatkov in poenostavljene evidence dejavnosti obdelave, da bi MSP z nizko stopnjo tveganja pomagali pri izpolnjevanju njihovih obveznosti.

Komisija bo:

- zagotovila standardna pogodbena določila za mednarodne prenose ter za razmerje med upravljavcem in obdelovalcem;
- zagotovila orodja, ki bodo pojasnjevala/podpirala uporabo pravil o varstvu podatkov za otroke[66];
- v skladu s strategijo za podatke raziskala praktične načine, da bi posameznikom omogočila večjo uporabo pravice do prenosljivosti, tako da bi jim na primer dala večji nadzor nad tem, kdo lahko dostopa do strojno tvorjenih podatkov in te podatke uporablja;
- s sodelovanjem med Agencijo Evropske unije za kibernetsko varnost (ENISA), organi za varstvo podatkov in odborom podpirala standardizacijo/certificiranje, zlasti glede vidikov kibernetske varnosti;
- po potrebi izkoristila svojo pravico, da odbor zaprosi za pripravo smernic in mnenj o specifičnih vprašanjih, ki so pomembna za deležnike;
- po potrebi zagotavljala smernice, pri tem pa v celoti upoštevala vlogo odbora;
- dejavnosti organov za varstvo podatkov, ki MSP olajšujejo izvajanje obveznosti iz Uredbe, podpirala s finančno podporo, zlasti za praktične smernice in digitalna orodja, ki jih je mogoče uporabiti v drugih državah članicah.

Spodbujanje inovacij

Komisija bo:

[66] Projekt Komisije o orodjih za ugotavljanje starosti – pilotni projekt za prikaz interoperabilne tehnične infrastrukture za zaščito otrok, vključno s preverjanjem starosti in soglasjem staršev. Pričakuje se, da se bo s tem podprlo izvajanje mehanizmov za zaščito otrok na podlagi obstoječe zakonodaje EU, ki se uporablja za zaščito otrok na spletu.

– spremljala uporabo Uredbe pri novih tehnologijah, tudi ob upoštevanju morebitnih prihodnjih pobud na področju umetne inteligence in v okviru strategije za podatke;

– spodbujala, tudi s finančno podporo, pripravo osnutka kodeksa ravnanja EU na področju zdravja in raziskav;

– pozorno spremljala razvoj in uporabo aplikacij v kontekstu pandemije COVID-19.

Odbor je pozvan, da:

– izdaja smernice o uporabi Uredbe na področju znanstvenih raziskav, umetne inteligence, blokovne verige in morebitnih drugih tehnoloških dosežkov;

– pregleda smernice, kadar so glede na tehnološki razvoj potrebna dodatna pojasnila.

Nadaljnji razvoj nabora orodij za prenose podatkov

Komisija bo:

– izvajala dialoge o ustreznosti z zainteresiranimi tretjimi državami v skladu s strategijo iz svojega sporočila iz leta 2017 z naslovom „Izmenjava in varstvo osebnih podatkov v globaliziranem svetu“, pri čemer bo po možnosti vključila tudi prenose podatkov organom kazenskega pregona (na podlagi direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj) in drugim javnim organom; to vključuje čim prejšnji možni zaključek procesa za sprejetje sklepa o ustreznosti z Republiko Korejo;

– zaključila tekoče vrednotenje obstoječih sklepov o ustreznosti ter o tem poročala Evropskemu parlamentu in Svetu;

– dokončala delo v zvezi s posodobitvijo standardnih pogodbenih določil, da bi bile usklajene z Uredbo in da bi zajemale vse ustrezne scenarije prenosa in bolje upoštevale sodobne poslovne prakse.

Odbor je pozvan, da:

– dodatno pojasni medsebojni vpliv pravil o mednarodnih prenosih podatkov (poglavje V) in ozemeljske veljavnosti Uredbe (člen 3);

– zagotavlja učinkovito izvrševanje v razmerju do gospodarskih subjektov s sedežem v tretjih državah, ki spadajo v ozemeljsko veljavnost Uredbe, vključno v zvezi z imenovanjem predstavnika, kadar je to ustrezno (člen 27);

– racionalizira oceno in morebitno odobritev zavezujočih poslovnih pravil, da se pospeši proces;

– dokonča delo v zvezi z arhitekturo, postopki in ocenjevalnimi merili za kodekse ravnanja in mehanizme certificiranja kot orodij za prenose podatkov.

Spodbujanje konvergence in razvoj mednarodnega sodelovanja

Komisija bo:

- z izmenjavo izkušenj in najboljših praks podpirala tekoče procese reform v tretjih državah glede novih ali posodobljenih pravil o varstvu podatkov;
- sodelovala z afriškimi partnerji pri spodbujanju regulativne konvergence in podpiranju izgradnje zmogljivosti nadzornih organov v okviru digitalnega poglavja novega partnerstva med EU in Afriko;
- ocenila, kako bi bilo mogoče olajšati sodelovanje med zasebnimi gospodarskimi subjekti in organi kazenskega pregona, tudi s pogajanji o dvostranskih in večstranskih okvirih za prenose podatkov v kontekstu dostopa tujih organov kazenskega pregona do elektronskih dokazov, da bi se izognili koliziji zakonov in zagotovili ustrezne zaščitne ukrepe za varstvo podatkov;
- sodelovala z mednarodnimi in regionalnimi organizacijami, kot so OECD, ASEAN ali skupina G20, pri spodbujanju zanesljivih tokov podatkov, ki temeljijo na visokih standardih varstva podatkov, tudi v kontekstu pobude „prostega pretoka podatkov na podlagi zaupanja“;
- ustanovila „Akademijo za varstvo podatkov“, ki bo olajševala in podpirala izmenjave med evropskimi in mednarodnimi regulatorji;
- spodbujala mednarodno sodelovanje na področju izvrševanja med nadzornimi organi, tudi s pogajanji o sporazumih o sodelovanju in medsebojni pomoči.