EVROPSKA
KOMISIJA

Bruselj, 24.7.2019
COM(2019) 374 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

Pravila o varstvu podatkov za utrjevanje zaupanja v EU in zunaj nje – ocena

Sporočilo Komisije Evropskemu parlamentu in Svetu

Pravila o varstvu podatkov za utrjevanje zaupanja v EU in zunaj nje – ocena

I. Uvod

Splošna uredba o varstvu podatkov[1] (v nadaljnjem besedilu: Uredba) se v Evropski uniji uporablja že več kot eno leto ter je središče usklajenega in moderniziranega področja varstva podatkov EU, ki vključuje tudi direktivo o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj[2] in uredbo o varstvu podatkov za institucije in organe EU[3]. Ta okvir naj bi dopolnila uredba o zasebnosti in elektronskih komunikacijah, ki je trenutno v zakonodajnem postopku.

Stroga pravila o varstvu podatkov so bistvena za zagotavljanje temeljne pravice do varstva osebnih podatkov. So osrednjega pomena za demokratično družbo[4] in pomemben sestavni del vse bolj podatkovno vodenega gospodarstva. EU si prizadeva izkoristiti številne priložnosti, ki jih ponuja digitalizacija v smislu storitev, delovnih mest in inovacij, hkrati pa obravnavati izzive, ki pri tem nastajajo. Kraja identitete, razkritje občutljivih podatkov, diskriminacija posameznikov, inherentna pristranskost, izmenjava nezakonitih vsebin in razvoj vsiljivih nadzornih orodij je le nekaj primerov vprašanj, ki so vedno bolj prisotna v javni razpravi, iz katere je razvidno, da ljudje pričakujejo, da bodo njihovi podatki zaščiteni.

Varstvo podatkov je postalo pravi globalni pojav, saj ljudje po celem svetu vse bolj cenijo varnost in varstvo svojih podatkov. Številne države so sprejele ali trenutno sprejemajo celovita pravila o varstvu podatkov na podlagi načel, podobnih tistim iz Uredbe, zaradi česar je prišlo do globalne konvergence pravil o varstvu podatkov. S tem so se pojavile nove priložnosti za olajšanje pretoka podatkov med komercialnimi operaterji ali javnimi organi, hkrati pa se izboljšuje raven varstva osebnih podatkov v EU in po vsem svetu.

---

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 (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1). https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

2 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, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016). https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:32016L0680&from=EN. Države članice so morale to direktivo prenesti do 6. maja 2018. Poročila o varnostni uniji navajajo stanje prenosa te direktive.

3 Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39). https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:32018R1725&from=EN. Uporabljati se je začela 11. decembra 2018.

4 Indijsko vrhovno sodišče je v prelomni sodbi z dne 24. avgusta 2017 priznalo zasebnost kot temeljno pravico, ki je „bistven element dostojanstva vsakega človeka“.

Varstvo podatkov se obravnava bolj resno kot kdaj koli prej in ima velik vpliv na različne deležnike in sektorje. Komisija je odločena poskrbeti, da bo EU uspešno izvajala novo ureditev varstva podatkov in bo podprla vse vidike te ureditve, da se bo ta začela v celoti izvajati. Komisija v tem sporočilu povzema dosežene rezultate v zvezi z doslednim izvajanjem pravil o varstvu podatkov v EU, delovanjem novega sistema upravljanja, vplivom na državljane in podjetja ter prizadevanji EU za spodbujanje konvergence ureditev varstva podatkov na svetovni ravni. To sporočilo je nadaljevanje sporočila Komisije o uporabi Uredbe iz januarja 2018[5] in temelji na delu večdeležniške skupine[6], zlasti o njenem prispevku k enoletnem pregledu stanja, pa tudi razpravah, ki so potekale ob pregledu stanja, ki ga je Komisija organizirala 13. junija 2019[7]. Hkrati je tudi prispevek k pregledu, ki ga Komisija namerava izvesti do maja 2020[8].

Zakonodajni okvir za varstvo podatkov v EU je temelj evropskega pristopa k inovacijam, osredotočenim na človeka. Postaja del regulativnega okvira za vse več politik, vključno z zdravstvom in raziskavami, umetno inteligenco, prometom, energijo, konkurenco ter preprečevanjem, odkrivanjem in preiskovanjem kaznivih dejanj. Komisija je dosledno poudarjala pomen ustreznega izvajanja in uveljavljanja novih pravil o varstvu podatkov, kot je poudarjeno v njenem sporočilu o uporabi Uredbe, izdanem januarja 2018, in njenih smernicah o uporabi osebnih podatkov v volilnem kontekstu, ki so bile objavljene septembra 2018[9]. Do tega sporočila je bil pri doseganju tega cilja dosežen velik napredek, zagotovo pa je potrebnega več dela, da bi se Uredba lahko začela v celoti izvajati.

II. Ena celina, en zakon: okvir varstva podatkov je v državah članicah vzpostavljen

Eden od ključnih ciljev Uredbe je bil odpraviti razdrobljenost zaradi 28 različnih nacionalnih zakonov, ki so obstajali na podlagi prejšnje direktive o varstvu podatkov[10], in zagotoviti pravno varnost za posameznike in podjetja po vsej EU. Ta cilj je bil večinoma dosežen.

---

5 Sporočilo komisije evropskemu parlamentu in svetu „Okrepljeno varstvo, nove priložnosti – navodila Komisije o neposredni uporabi splošne uredbe o varstvu podatkov od 25. maja 2018“ (COM(2018) 43 final). https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:52018DC0043&from=EN.

6 Večdeležniška skupina o Uredbi, 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&Lang=SL.

7 http://europa.eu/rapid/press-release_IP-19-2956_en.htm.

8 Člen 97 Uredbe.

9 Smernice Komisije o uporabi prava Unije o varstvu podatkov v volilnem kontekstu, (COM(2018) 638) https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:52018DC0638&from=SL

10 Direktiva 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:31995L0046&from=EN.

Harmonizacija pravnega okvira

Čeprav se Uredba neposredno uporablja v državah članicah, jih tudi zavezuje, da na nacionalni ravni sprejmejo številne pravne ukrepe, zlasti za vzpostavitev in dodelitev pristojnosti nacionalnim organom za varstvo podatkov[11], določijo pravila o posebnih vprašanjih, kot so usklajevanje varstva osebnih podatkov s svobodo izražanja in obveščanja, ter spreminjajo ali razveljavljajo sektorsko zakonodajo, ki se nanaša na varstvo podatkov. V času tega sporočila so vse države članice razen treh[12] posodobile svojo nacionalno zakonodajo o varstvu podatkov. Na nacionalni ravni še potekajo prizadevanja v zvezi s prilagajanjem sektorskih zakonov. Po vključitvi Uredbe v Sporazum o Evropskem gospodarskem prostoru je bila njena uporaba razširjena na Norveško, Islandijo in Lihtenštajn, ki so tudi sprejele svojo nacionalno zakonodajo o varstvu podatkov.

Vendar deležniki pozivajo k še višji stopnji harmonizacije na nekaterih področjih[13]. Uredba državam članicam omogoča, da podrobneje opredelijo njeno uporabo na nekaterih področjih, kot sta starostna meja privolitve s strani otrok za uporabo spletnih storitev[14] ali obdelava osebnih podatkov na področjih, kot sta medicina in javno zdravje. V tem primeru ukrepanje držav članic temelji na dveh elementih:

i) vsi zakoni, ki zadevajo nacionalno specifikacijo, morajo izpolnjevati zahteve iz Listine o temeljnih pravicah[15] (in ne smejo presegati omejitev iz Uredbe, ki temelji na Listini);
ii) ne sme posegati v prosti pretok osebnih podatkov v EU[16].

V nekaterih primerih so države članice poleg Uredbe uvedle nacionalne zahteve, zlasti s številnimi sektorskimi zakoni, kar povzroča razdrobljenost in nepotrebna bremena. Primer dodatne zahteve, ki so jo poleg Uredbe uvedle države članice, je obveznost iz nemške zakonodaje, da se imenuje pooblaščena oseba za varstvo podatkov v podjetjih z 20 ali več zaposlenimi, ki so stalno vključeni v avtomatizirano obdelavo osebnih podatkov.

Nadaljnja prizadevanja za večjo usklajenost

Komisija se udeležuje dvostranskih dialogov z nacionalnimi organi, v okviru katerih namenja posebno pozornost nacionalnim ukrepom v zvezi z:

- dejansko neodvisnostjo organov za varstvo podatkov, vključno z ustreznimi finančnimi, človeškimi in tehničnimi viri;

---

11 Kot je pristojnost za naložitev upravnih glob.
12 Grčija, Portugalska in Slovenija so od 23. julija 2019 še vedno v postopku sprejemanja svoje nacionalne zakonodaje.
13 Glej poročilo večdeležniške skupine o Uredbi z dne 13. junija 2019: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=SL.
14 13 let za Belgijo, Dansko, Estonijo, Finsko, Latvijo, Malto, Švedsko in Združeno kraljestvo; 14 let za Avstrijo, Bolgarijo, Ciper, Španijo, Italijo in Litvo; 15 let za Češko in Francijo; 16 let za Nemčijo, Madžarsko, Hrvaško, Irsko, Luksemburg, Nizozemsko, Poljsko, Romunijo in Slovaško.
15 Člen 8.
16 V skladu s členom 16(2) Pogodbe o delovanju Evropske unije.

- tem, kako zakoni na nacionalni ravni omejujejo pravice posameznikov, na katere se nanašajo osebni podatki;
- dejstvom, da nacionalna zakonodaja ne bi smela uvajati zahtev, ki presegajo Uredbo, kadar niso predvidene druge specifikacije, kot so dodatni pogoji za obdelavo;
- izpolnitvijo obveznosti uskladitve pravice do varstva osebnih podatkov s svobodo izražanja in obveščanja, pri čemer je treba upoštevati, da se ta obveznost ne sme zlorabiti za zastraševanje novinarjev.

Delo organov za varstvo podatkov, ki sodelujejo v okviru Evropskega odbora za varstvo podatkov (v nadaljnjem besedilu: odbor), je ključno gonilo za dosledno uporabo novih pravil, saj izvršilni ukrepi, ki vplivajo na več držav članic, potekajo v okviru mehanizma za sodelovanje in skladnost[17] znotraj odbora, smernice, ki jih sprejme odbor, pa prispevajo k harmoniziranemu razumevanju Uredbe. Kljub temu pa deležniki pričakujejo, da bodo organi za varstvo podatkov na tem področju posegli dlje.

Delo nacionalnih sodišč in Sodišča Evropske unije tudi prispeva k dosledni razlagi pravil o varstvu podatkov. Nacionalna sodišča so pred kratkim izdala sodbe, s katerimi se razveljavijo določbe v nacionalnih zakonih, ki odstopajo od Uredbe[18].

III. Novi sistem upravljanja postaja vedno bolj izoblikovan

Z Uredbo je bila vzpostavljena nova struktura upravljanja, ki je v središče postavila neodvisne nacionalne organe za varstvo podatkov, ki izvršujejo Uredbo in so prva kontaktna točka za deležnike. Čeprav je večina organov za varstvo podatkov v preteklem letu prejela več sredstev, so med državami članicami še vedno velike razlike[19].

Organi za varstvo podatkov uporabljajo svoja nova pooblastila

Uredba je organom za varstvo podatkov dodelila večja izvršilna pooblastila. Nacionalni organi za varstvo podatkov so kljub pomislekom nekaterih deležnikov pred majem 2018 sprejeli uravnotežen pristop v zvezi z izvršilnimi pooblastili. Osredotočili so se na dialog in ne na sankcije, zlasti z najmanjšimi subjekti, katerih osnovna dejavnost ni obdelava osebnih podatkov. Poleg tega so učinkovito uporabili svoje nove pristojnosti, ko je bilo to potrebno, vključno z uvedbo preiskav na področju družbenih medijev[20] in naložitvijo upravnih glob v razponu od nekaj tisoč evrov do več milijonov evrov, odvisno od resnosti kršitev pravil o varstvu podatkov.

---

17 Člen 60 Uredbe določa sodelovanje med organi za varstvo podatkov za uporabo ene razlage te uredbe v konkretnih primerih. Člen 64 določa, da odbor v nekaterih primerih izdaja mnenja, da se zagotovi dosledna uporaba Uredbe. Odbor ima tudi pooblastila, da v primeru nesoglasja med organi za varstvo podatkov sprejme na njih naslovljene zavezujoče odločitve.

18 To velja za Nemčijo in Španijo.

19 https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf.

20 Na primer, irska komisija za varstvo podatkov je začela 15 uradnih preiskav v zvezi s skladnostjo večnacionalnih tehnoloških podjetij z Uredbo. Glej stran 49 letnega poročila irske komisije za varstvo podatkov za leto 2018: https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018.

Primeri glob, ki so jih naložili organi za varstvo podatkov[21]:

- 5 000 EUR za kavarno s športnimi stavami v Avstriji, za nezakonit video nadzor;
- 220 000 EUR za podjetje za posredovanje podatkov na Poljskem, ker ni obvestilo posameznikov, da se njihovi podatki obdelujejo;
- 250 000 EUR je bilo naloženo španski nogometni ligi LaLiga zaradi pomanjkanja preglednosti pri načrtovanju aplikacije za pametne telefone;
- 50 milijonov EUR za Google v Franciji zaradi pogojev za pridobitev soglasja uporabnikov.

Pri preiskovanju je bistvenega pomena, da organi za varstvo podatkov zberejo ustrezne dokaze, spoštujejo vse postopkovne korake v skladu z nacionalno zakonodajo in zagotovijo ustrezen postopek v pogosto zapletenih zadevah. Za to sta potrebna čas in ogromno dela, kar pojasnjuje, zakaj je večina preiskav, začetih po začetku uporabe Uredbe, še vedno v teku.

Tako se uspešnost Uredbe ne bi smela meriti s številom naloženih glob, temveč s spremembami v kulturi in vedenju vseh udeležencev. V zvezi s tem imajo organi za varstvo podatkov na voljo druga orodja, kot je uvedba začasne ali dokončne omejitve obdelave, vključno s prepovedjo ali odreditvijo začasnega preklica pretoka podatkov prejemniku v tretji državi[22].

Nekateri organi za varstvo podatkov so vzpostavili nova orodja, kot so telefonske številke za pomoč in nabor orodij za podjetja, medtem ko so drugi razvili nove pristope, kot so regulativni peskovniki[23] za pomoč podjetjem pri njihovih prizadevanjih za skladnost. Vendar številni deležniki še vedno menijo, da zlasti mala in srednje velika podjetja[24] v nekaterih državah članicah niso prejela dovolj podpore in informacij. Komisija v pomoč pri reševanju tega položaja organom za varstvo podatkov omogoča, da stopijo v stik z deležniki, zlasti posamezniki ter malimi in srednjimi podjetji[25].

---

21 Več odločitev o naložitvi glob je še vedno v sodni presoji.

22 Člen 58(2)(f) in (j).

23 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/.

24 Glej poročilo večdeležniške skupine o Splošni uredbi o varstvu podatkov: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670

25 Dva milijona EUR, dodeljenih devetim organom za varstvo podatkov v letu 2018 za dejavnosti v obdobju 2018–2019: Belgija, Bolgarija, Danska, Madžarska, Litva, Latvija, Nizozemska, Slovenija in Islandija: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017;
en milijon EUR, ki bo dodeljen leta 2019:
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019.

Evropski odbor za varstvo podatkov je operativen

Organi za varstvo podatkov so okrepili delo v Evropskem odboru za varstvo podatkov[26]. To intenzivno delo je odboru omogočilo sprejetje približno 20 smernic o ključnih vidikih Uredbe[27]. Prihodnja področja dela odbora so predstavljena v dvoletnem programu[28], kot zahteva Uredba.

V čezmejnih zadevah vsak organ za varstvo podatkov ni več zgolj nacionalni organ, temveč je del pravega vseevropskega postopka z vsemi fazami, od preiskave do odločitve. Takšno tesno sodelovanje je postalo vsakodnevna praksa: do konca junija 2019 je bilo s pomočjo mehanizma sodelovanja obravnavanih 516 čezmejnih zadev.

Komisija dejavno prispeva k delu odbora[29] ter spodbuja črko in duha Uredbe ter opozarja na splošna načela prava EU[30].

Oblikovanje kulture varstva podatkov v EU

Novi sistem upravljanja še vedno ni v celoti izkoristil svojega potenciala. Pomembno je, da odbor še poenostavi postopek odločanja in razvije skupno kulturo varstva podatkov EU med svojimi člani. Možnosti organov za varstvo podatkov, da združijo svoja prizadevanja[31] v zvezi z vprašanji, ki zadevajo več kot eno državo članico, na primer za izvajanje skupnih preiskav in izvršilnih ukrepov, lahko prispevajo k takemu cilju, hkrati pa blažijo učinek omejenih virov.

Številni deležniki želijo tesnejše sodelovanje z nacionalnimi organi za varstvo podatkov[32] in enoten pristop z njihove strani. Od organov za varstvo podatkov[33] zahtevajo tudi večjo doslednost pri svetovanju in popolno uskladitev nacionalnih smernic z navodili odbora. Nekateri deležniki pričakujejo tudi nadaljnje pojasnitve ključnih konceptov Uredbe, kot je pristop na podlagi tveganja, pri katerem je treba upoštevati pomisleke zlasti malih in srednjih podjetij.

V tem okviru je bistvenega pomena, da se lahko deležniki bolje vključijo v delo odbora. Zato Komisija podpira sistematično javno posvetovanje, ki ga je v zvezi s smernicami organiziral odbor. To prakso, skupaj z organizacijo delavnic z deležniki o ciljno usmerjenih temah v

---

[26] Odbor je pravna oseba, sestavljajo pa ga vodje nacionalnih nadzornih organov za varstvo podatkov in Evropski nadzornik za varstvo podatkov.

[27] https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

[28] https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_en.

[29] Kot udeleženec brez glasovalne pravice.

[30] Komisija je prav tako pomagala pri nemoteni vzpostavitvi odbora in njegovo delovanje podpira z zagotavljanjem komunikacijskega sistema.

[31] Člen 62 Uredbe.

[32] Glej poročilo večdeležniške skupine o Uredbi: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=SL.
Podjetja so na primer prepričana, da bi bili lahko nacionalni seznami, ki zajemajo tiste vrste postopkov obdelave, za katere se zahteva ocena učinka v zvezi z varstvom podatkov v skladu s členom 35 Uredbe, bolje usklajeni.

[33] Vključno med različnimi organi v zveznih državah.

zgodnji fazi razmisleka, bi bilo treba nadaljevati in dopolniti, da se zagotovi preglednost, vključenost in ustreznost dela odbora.

IV. Posamezniki uveljavljajo svoje pravice, vendar bi se moralo ozaveščanje nadaljevati

Še en ključni cilj uredbe je bil okrepiti pravice posameznikov. Združenja za civilne pravice in organizacije potrošnikov na splošno menijo, da pomeni Uredba pomemben prispevek k pravični digitalni družbi, ki temelji na medsebojnem zaupanju.

Večja ozaveščenost o pravicah glede varstva podatkov.

Posamezniki v EU se vedno bolj zavedajo pravil o varstvu podatkov in svojih pravic: 67 % vprašanih, ki so sodelovali v raziskavi Eurobarometer[34] iz maja 2019, je seznanjenih s to uredbo, 57 % pa jih je vedelo, da obstaja nacionalni organ za varstvo podatkov, na katerega se lahko obrnejo za informacije ali pri njem vložijo pritožbe. 73 % jih je slišalo za vsaj eno od pravic, ki jih podeljuje Uredba. Vendar pa zelo veliko posameznikov v EU še vedno ne ukrepa aktivno, da bi zaščitili svoje osebne podatke na spletu. 44 % posameznikov na primer ni spremenilo privzetih nastavitev zasebnosti na družbenih omrežjih.

Posamezniki vse pogosteje uveljavljajo svoje pravice

To povečanje ozaveščenosti o pravicah je posameznike spodbudilo, da intenzivneje uveljavljajo svoje pravice z uporabo vprašalnikov za potrošnike in s stikom z organi za varstvo podatkov z namenom zaprositi za informacije ali vložiti pritožbo[35]. Tudi podjetja poročajo, da se je število zahtev za dostop do osebnih podatkov povečalo v več sektorjih, na primer v bančništvu in telekomunikacijah. Posamezniki so tudi pogosteje umaknili svojo privolitev in uveljavljali svojo pravico do ugovora na komercialna sporočila[36].

Kljub temu so nekateri gospodarski subjekti poročali o napakah posameznikov glede razumevanja pravil o varstvu podatkov, kot je prepričanje, da bi morali posamezniki privoliti v vsako obdelavo ali da je pravica do izbrisa absolutna (subjekti morajo včasih hraniti osebne podatke zaradi pravnih obveznosti)[37]. Organizacije civilne družbe pa se pritožujejo zaradi velikih zamud nekaterih podjetij in organov za varstvo podatkov pri odgovarjanju na vprašanja.

Pomembno je, da so nevladne organizacije po pooblastilu posameznikov sprožile več zastopniških tožb in pri tem uporabile novo možnost iz Uredbe[38]. Uporaba zastopniških tožb

---

34 https://europa.eu/rapid/press-release_IP-19-2956_sl.htm.
35 https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf.
36 Glej poročilo večdeležniške skupine o Splošni uredbi o varstvu podatkov.
37 Glej poročilo večdeležniške skupine o Splošni uredbi o varstvu podatkov.
38 Člen 80(1) Uredbe.

bi bila lažja, če bi več držav članic uporabilo možnost iz Uredbe, da se nevladnim organizacijam omogoči izvajanje ukrepov brez pooblastila[39].

Potreba po nadaljevanju prizadevanj za ozaveščanje

Zato je treba prizadevanja za dialog in ozaveščanje, ki se osredotočajo na splošno javnost, nadaljevati na nacionalni ravni in na ravni EU. V ta namen je Komisija julija 2019[40] začela izvajati novo spletno kampanjo, da bi posameznike spodbudila k branju izjav o varstvu osebnih podatkov in izboljšanju njihovih nastavitev zasebnosti.

V. Podjetja prilagajajo svoje prakse

Namen Uredbe je podpreti podjetja v digitalnem gospodarstvu z rešitvami, ki bodo primerne tudi v prihodnosti. Podjetja so na splošno zadovoljna z načelom odgovornosti v Uredbi, ki odpravlja prejšnji obremenjujoči predhodni pristop (odprava zahtev glede obveščanja, nadgradljivost obveznosti in prožnost načela vgrajenega in privzetega varstva podatkov, ki omogoča konkurenco na podlagi rešitev, ki varujejo zasebnost). Hkrati nekatera podjetja od organov za varstvo podatkov zahtevajo večjo pravno varnost in dodatne ali jasnejše smernice[41].

Dobro upravljanje podatkov

Čeprav podjetja poročajo o številnih izzivih pri prilagajanju novim pravilom[42], pa mnoga druga poudarjajo, da je bila to tudi priložnost, da so na vprašanje varstva podatkov opozorila odbore podjetij, uredila svoje poslovanje v zvezi s podatki, s katerimi razpolagajo, izboljšala varnost, se bolje pripravila na incidente, zmanjšala izpostavljenost nepotrebnim tveganjem ter vzpostavila večje zaupanje s strankami in trgovinskimi partnerji. Kar zadeva preglednost, podjetja in organizacije civilne družbe omenjajo občutljivo ravnovesje, ki ga je treba doseči med zagotavljanjem vseh potrebnih informacij posameznikom v skladu z Uredbo ter uporabo jasnega in preprostega jezika, v obliki, ki je posameznikom razumljiva. Gospodarski subjekti razvijajo inovativne rešitve v tej smeri.

Na splošno so podjetja navedla, da so lahko uresničila nove pravice posameznikov, na katere se nanašajo osebni podatki, čeprav so včasih težko izpolnila roke zaradi povečanega števila zahtev in njihovega širšega značaja[43] ali zaradi preverjanja identitete osebe, ki je vložila zahtevo.

---

[39] Člen 80(2) Uredbe.

[40] Gre za nadaljevanje predhodne kampanje za razširjanje informativnega gradiva za posameznike in podjetja, ki je na voljo: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

[41] Glej poročilo večdeležniške skupine o Uredbi.

[42] Posodobitev informacijskega sistema je pogosto omenjena kot eden od glavnih izzivov, zlasti v zvezi z izvajanjem načel vgrajenega in privzetega varstva podatkov, pravico do izbrisa v varnostnih kopijah itd.

[43] Podjetja se zavzemajo tudi za smernice odbora v zvezi z neutemeljenimi in pretiranimi zahtevami.

Vpliv na inovacije

Uredba ne le dopušča, temveč spodbuja razvoj novih tehnologij, hkrati pa spoštuje temeljno pravico do varstva osebnih podatkov. To velja za področja, kot je na primer umetna inteligenca.

Podjetja so začela pripravljati svojo ponudbo novih storitev, ki bodo varovale zasebnost. Na primer iskalniki, ki ne sledijo uporabnikom ali ki ne uporabljajo vedenjskega oglaševanja, v nekaterih državah članicah postopoma pridobivajo tržne deleže. Druga podjetja razvijajo storitve, ki temeljijo na novih pravicah, podeljenih posameznikom, kot je na primer prenosljivost njihovih osebnih podatkov. Vedno večje število podjetij spodbuja spoštovanje osebnih podatkov kot konkurenčno prednost in prodajno točko. Ta razvoj ni omejen le na EU, temveč se nanaša tudi na zelo inovativna tuja gospodarstva[44].

Poseben položaj mikropodjetij in malih podjetij z „nizkim tveganjem“

Čeprav se razmere med državami članicami razlikujejo, imajo deležniki največ vprašanj o uporabi Uredbe v zvezi z mikropodjetji in malimi podjetji[45], pri katerih obdelava podatkov ni osnovna poslovna dejavnost. Čeprav se zdi, da so ta vprašanja delno posledica pomanjkanja ozaveščenosti o pravilih o varstvu podatkov, se njihovi pomisleki včasih še stopnjujejo s kampanjami svetovalnih podjetij, ki zagotavljajo plačljive nasvete, širjenjem napačnih informacij, na primer o potrebi po sistematičnem pridobivanju soglasja posameznikov[46], in dodatnimi zahtevami na nacionalni ravni.

V zvezi s tem mikropodjetja in mala podjetja zahtevajo smernice, ki bi bile prilagojene njihovim posebnim položajem in bi zagotavljale zelo praktične informacije. Nekateri organi za varstvo podatkov so to že storili na nacionalni ravni[47]. Da bi dopolnila nacionalne pobude, je Komisija izdala informativno gradivo, ki je s prikazom niza praktičnih korakov tem podjetjem v pomoč pri izpolnjevanju novih pravil[48].

Uporaba zbirke orodij v okviru Uredbe

Uredba določa orodja za dokazovanje skladnosti, kot so standardne pogodbene klavzule, kodeksi ravnanja in novi mehanizmi certificiranja.

Standardne pogodbene klavzule so vzorčne klavzule, ki jih je mogoče prostovoljno vključiti v pogodbo med na primer upravljavcem podatkov in obdelovalcem podatkov in ki določajo obveznosti pogodbenih strank v skladu z Uredbo. Uredba razširja možnosti uporabe

---

44 V skladu s poročilom, ki ga je objavilo izraelsko združenje industrije kibernetske varnosti, je bil na primer leta 2018 podsektor „varstvo podatkov in zasebnost“ na področju kibernetske varnosti najhitreje rastoč podsektor, kar je delno posledica začetka uporabe Splošne uredbe o varstvu podatkov.

45 Kot je opredeljeno v opredelitvi MSP, na voljo na: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_sl.

46 Uredba se dejansko ne sklicuje le na soglasje, temveč določa več pravnih podlag za obdelavo osebnih podatkov.

47 Na primer priročnik, ki ga je pripravil francoski organ za varstvo podatkov: https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement.

48 https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-en-n.pdf.

standardnih pogodbenih klavzul za mednarodne prenose in znotraj EU[49]. Na področju mednarodnih prenosov njihova široka uporaba izkazuje[50], da so zelo koristna za podjetja pri njihovih prizadevanjih za doseganje skladnosti in da koristijo zlasti podjetjem, ki nimajo sredstev, da bi se o posameznih pogodbah pogajala z vsakim izvajalcem obdelave podatkov.

Številni sektorji prav tako menijo, da je sprejetje standardnih pogodbenih klavzul koristen način za spodbujanje usklajevanja, zlasti kadar jih sprejme Komisija. Komisija bo sodelovala z deležniki, da bi izkoristila možnosti, ki jih ponuja Uredba, in posodobila obstoječe klavzule.

Spoštovanje kodeksov ravnanja je še eno operativno in praktično orodje, ki je industriji na voljo za lažje dokazovanje skladnosti z Uredbo[51] . Te kodekse bi morala oblikovati trgovinska združenja ali organi, ki zastopajo kategorije upravljavcev in obdelovalcev, opisovati pa bi morali, kako se lahko pravila o varstvu podatkov izvajajo v določenem sektorju. Ker obveznosti umerjajo s tveganji[52], so ti kodeksi lahko zelo koristni in stroškovno učinkoviti tudi za mala in srednje velika podjetja pri izpolnjevanju obveznosti.

Tudi certificiranje je lahko uporaben instrument za dokazovanje skladnosti s posebnimi zahtevami iz Uredbe. To lahko poveča pravno varnost za podjetja in Uredbo promovira na svetovni ravni. Smernice za certificiranje in akreditacijo[53], ki jih je nedavno sprejel Evropski odbor za varstvo podatkov, bodo omogočile razvoj sistemov certificiranja v EU. Komisija bo spremljala ta razvoj in po potrebi uporabila pooblastilo iz Uredbe za opredelitev zahtev za certificiranje. Komisija lahko organom EU za standardizacijo izda tudi zahtevo za standardizacijo v zvezi z elementi, ki so pomembni za Uredbo.

VI. Navzgor usmerjena konvergenca napreduje na mednarodni ravni

Zahteva po varstvu osebnih podatkov ni omejena na EU. Kot kaže nedavna svetovna raziskava o varnosti na internetu, se po svetu širi pomanjkanje zaupanja, zaradi česar ljudje spreminjajo način vedenja na spletu[54]. Vse več podjetij te pomisleke obravnava tako, da pravice, ki jih podeljuje Uredba, prostovoljno razširja na svoje stranke zunaj EU.

---

[49] Glej člen 28 Uredbe. Standardne pogodbene klavzule, ki jih je sprejela Komisija, veljajo za celotno EU. Nasprotno pa tiste, ki jih na podlagi člena 28(8) sprejme organ za varstvo podatkov, zavezujejo le organ, ki jih je sprejel, in se tako lahko v skladu s členoma 55 in 56 uporabijo kot standardne pogodbene klavzule za postopke obdelave, ki spadajo pod pristojnost tega organa.

[50] Dejansko so glavno orodje, na katerega se podjetja zanašajo za svoj izvoz podatkov.

[51] Evropski odbor za varstvo podatkov je 4. junija 2019 sprejel smernice o kodeksih ravnanja. Pojasnjujejo postopke in pravila za predložitev, odobritev in objavo kodeksov tako na nacionalni ravni kot na ravni EU.

[52] Uvodna izjava 98 Uredbe.

[53] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_sl; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_sl.

[54] Glej globalno spletno anketo „CIGI-Ipsos Global Survey on Internet Security and Trust“ iz leta 2019. V skladu s to raziskavo je bilo 78 % vprašanih zaskrbljenih zaradi svoje spletne zasebnosti, pri čemer jih je 49 % navedlo, da zaradi nezaupanja na spletu razkrijejo manj osebnih podatkov, 43 % vprašanih je poročalo, da skrbneje zavarujejo svoje naprave, 39 % vprašanih pa je odgovorilo, da med drugimi previdnostnimi ukrepi internet uporabljajo bolj selektivno. Raziskava je bila izvedena v 25 gospodarstvih: Avstralija, Brazilija, Egipt, Francija, Hongkong, Indija, Indonezija, Italija, Japonska, Južna Afrika, Kanada,

Ker se države po svetu vse bolj spopadajo s podobnimi izzivi, sprejemajo nova pravila o varstvu podatkov ali posodabljajo že obstoječa. Ti zakoni imajo pogosto veliko značilnosti, ki so skupne z ureditvijo EU za varstvo podatkov, npr. krovna zakonodaja namesto sektorskih pravil, izvršljive individualne pravice in neodvisen nadzorni organ. Ta trend je resnično globalen in sega od Južne Koreje do Brazilije, od Čila do Tajske ter od Indije do Indonezije. Vse bolj splošno sodelovanje v „Konvenciji št. 108“ Sveta Evrope[55] – nedavno posodobljeni[56] z znatnim prispevkom Komisije – je še en jasen znak tega trenda navzgor usmerjene konvergence.

Spodbujanje varnega in prostega pretoka podatkov s sklepi o ustreznosti in drugače

Ta razvoj konvergence ponuja nove priložnosti za olajšanje pretoka podatkov in s tem trgovine ter sodelovanja med javnimi organi, hkrati pa izboljšuje raven varstva podatkov posameznikov v EU, ko se ti prenašajo v tujino.

Komisija je v okviru izvajanja strategije iz sporočila o izmenjavi in varovanju osebnih podatkov v globaliziranem svetu iz leta 2017[57] okrepila sodelovanje s tretjimi državami in drugimi mednarodnimi partnerji pri nadgrajevanju in nadaljnjem razvoju elementov konvergence med sistemi varstva zasebnosti. To je vključevalo preučitev možnosti sprejetja ugotovitev o ustreznosti z izbranimi tretjimi državami[58]. Ta prizadevanja so prinesla pomembne rezultate, zlasti z začetkom veljavnosti sporazuma o vzajemni ustreznosti EU-Japonska, ki je začel veljati februarja 2019 in ki je ustvaril največje območje prostega in varnega pretoka podatkov na svetu. Pogajanja o ustreznosti z Južno Korejo so v napredni fazi, trenutno pa poteka raziskovalno delo, da bi se začela pogajanja o ustreznosti z več latinskoameriškimi državami, kot sta Čile in Brazilija, odvisno zaključka tekočih zakonodajnih postopkov. Razvoj dogodkov je obetaven tudi v nekaterih delih Azije, kot so Indija, Indonezija in Tajvan, pa tudi v evropskem vzhodnem in južnem sosedstvu, kar bi lahko odprlo vrata prihodnjim sklepom o ustreznosti.

Hkrati se Komisija veseli dejstva, da so druge države, ki so vzpostavile instrumente prenosa, podobne ustreznosti iz Uredbe, priznale, da EU in države, ki jih EU priznava kot „ustrezne“,

---

Kenija, Kitajska, Mehika, Nemčija, Nigerija, Pakistan, Republika Koreja, Poljska, Rusija, Švedska, Tunizija, Turčija, Velika Britanija in Združene države.

55 Konvencija Sveta Evrope z dne 28. januarja 1981 o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (ETS št. 108) in Dodatni protokol h Konvenciji o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, ki se nanaša na nadzorne organe in čezmejni prenos podatkov, (ETS št. 181) iz leta 2001. To je edini zavezujoči večstranski instrument na področju varstva podatkov. Zadnje države, ki so ratificirale konvencijo, so Argentina, Mehika, Zelenortski otoki in Maroko.

56 Protokol o spremembi Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (ETS št. 108), kot je bil dogovorjen na 128. zasedanju Odbora ministrov v Elsinoruju na Danskem od 17. do 18. maja 2018. Prečiščeno besedilo posodobljene Konvencije št. 108 je na voljo na: https://rm.coe.int/16808ade9d.

57 Sporočilo Komisije Evropskemu parlamentu in Svetu z naslovom Izmenjava in varstvo osebnih podatkov v globaliziranem svetu, COM(2017) 17 final.

58 Uredba je prav tako ustvarila možnost za ugotovitve o ustreznosti tudi v zvezi z mednarodnimi organizacijami, kar je del prizadevanj EU za olajšanje izmenjave podatkov s takimi subjekti.

zagotavljajo zahtevano raven zaščite[59]. S tem bi lahko ustvarili mrežo držav, v katerih bi se podatki lahko prosto pretakali.

Poleg tega poteka intenzivno delo z drugimi tretjimi državami, kot so Kanada, Nova Zelandija, Argentina in Izrael, da se v okviru Uredbe zagotovi kontinuiteta o sklepih o ustreznosti, sprejetih na podlagi direktive o varstvu podatkov iz leta 1995. Izkazalo se je tudi, da je zasebnostni ščit EU-ZDA koristno orodje za zagotavljanje čezatlantskega pretoka podatkov na podlagi visoke ravni zaščite podatkov ob sodelovanju več kot 4 700 podjetij[60]. Njegov letni pregled zagotavlja redno preverjanje pravilnega delovanja okvira in pravočasno reševanje novih vprašanj.

Ker ni enotne rešitve za prenos podatkov, Komisija sodeluje tudi z deležniki in odborom, da se izkoristi celoten potencial nabora orodij Uredbe za mednarodni prenos podatkov. To zadeva instrumente, kot so standardne pogodbene klavzule, razvoj sistemov certificiranja, kodeksi ravnanja ali upravni dogovori za javne organe. V zvezi s tem se Komisija zanima za izmenjavo izkušenj in dobrih praks z drugimi sistemi, ki so pridobili posebno strokovno znanje o nekaterih od teh orodij. Komisija bo razmislila o uporabi pooblastil, dodeljenih na podlagi Uredbe, v zvezi z navedenimi orodji za prenos, zlasti v zvezi s standardnimi pogodbenimi klavzulami.

Poleg zgolj dvostranskih orodij bi bilo smiselno preučiti tudi, ali bi lahko podobno misleče države v času, ko postajajo podatkovni tokovi vse pomembnejši sestavni del trgovine, komunikacij in družbenih interakcij, vzpostavile večnacionalni okvir na tem področju. Tak instrument bi omogočil prosti pretok podatkov med pogodbenicami, hkrati pa bi zagotavljal zahtevano raven varstva na podlagi skupnih vrednot in konvergenčnih sistemov. Razvijal bi se lahko na primer na podlagi posodobljene Konvencije št. 108 ali na podlagi pobude „prosti pretok podatkov z zaupanjem“, ki jo je na začetku tega leta sprožila Japonska.

Razvoj novih sinergij med trgovinskimi instrumenti in instrumenti za varstvo podatkov

Komisija je za spodbujanje konvergence standardov za varstvo podatkov na mednarodni ravni tudi odločena, da se bo spopadla z digitalnim protekcionizmom. V ta namen je pripravila posebne določbe o pretoku podatkov in varstvu podatkov v trgovinskih sporazumih, ki jih sistematično predlaga v dvostranskih in večstranskih pogajanjih, kot so sedanje razprave STO o e-trgovanju. Te horizontalne določbe prepovedujejo izključno protekcionistične ukrepe, kot so zahteve za prisilno lokalizacijo podatkov, hkrati pa ohranjajo regulativno avtonomijo pogodbenic, da zaščitijo temeljne pravice do varstva podatkov.

Čeprav morajo dialogi o varstvu podatkov in trgovinskih pogajanjih potekati ločeno, se lahko medsebojno dopolnjujejo: sporazum o vzajemni ustreznosti med EU in Japonsko je najboljši primer takih sinergij, ki dodatno olajšujejo komercialne izmenjave in tako povečujejo koristi Sporazuma o gospodarskem partnerstvu z Japonsko. Dejansko ta vrsta konvergence, ki temelji na skupnih vrednotah in visokih standardih, podpira pa jo učinkovito izvrševanje, zagotavlja

---

[59] Tak pristop so na primer sprejele Argentina, Kolumbija, Izrael in Švica.

[60] To pomeni, da ima po prvih treh letih obstoja zasebnostni ščit več udeleženih podjetij, kot jih je njegov predhodnik varni pristan imel po 13 letih delovanja.

najmočnejše temelje za izmenjavo osebnih podatkov, kar vedno bolj priznavajo naši mednarodni partnerji[61]. Glede na to, da podjetja vse pogosteje delujejo čezmejno in dajejo prednost podobnim pravilom pri vseh svojih poslovnih dejavnostih po vsem svetu, taka konvergenca prispeva k ustvarjanju okolja, ki spodbuja neposredne naložbe, olajšuje trgovino in izboljšuje zaupanje med trgovinskimi partnerji.

Olajševanje izmenjave informacij za boj proti kriminalu in terorizmu na podlagi ustreznih zaščitnih ukrepov

Večja združljivost med ureditvami za varstvo podatkov lahko tudi bistveno olajša nujno potrebne izmenjave informacij med organi EU ter tujimi regulativnimi, policijskimi in pravosodnimi organi ter na ta način prispeva k učinkovitejšemu in hitremu sodelovanju na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj[62]. Zato namerava Komisija za poglobitev sodelovanja s ključnimi partnerji v boju proti kriminalu in terorizmu uporabiti možnost sprejetja sklepov o ustreznosti v skladu z direktivo o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj. Poleg tega se lahko krovni sporazum med EU in ZDA[63], ki je začel veljati februarja 2017, uporabi kot model za podobne sporazume z drugimi pomembnimi partnerji na področju varnosti.

Druga primera, ki kažeta na pomen visokih standardov varstva podatkov kot podlage za stabilno sodelovanje s tretjimi državami na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, sta prenos evidenc podatkov o potnikih (PNR)[64] in izmenjava operativnih informacij med Europolom in pomembnimi mednarodnimi partnerji. V zvezi s tem so trenutno v teku ali tik pred začetkom pogajanja o mednarodnih sporazumih z več državami južnega sosedstva[65].

Trdni zaščitni ukrepi za varstvo podatkov bodo prav tako bistven element vsakega prihodnjega sporazuma o čezmejnem dostopu do elektronskih dokazov v kazenskih preiskavah, tako na dvostranski ravni (Sporazum EU-ZDA) kot na večstranski ravni (Drugi

---

61 Kot je razvidno na primer pri sklicevanju na pojem „prosti pretok podatkov z zaupanjem“ v izjavi voditeljev skupine G20 iz Osake: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

62 Glej Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij – Evropska agenda za varnost (COM(2015) 185 final).

63 Sporazum med EU in ZDA o varstvu osebnih podatkov ob njihovem prenosu ali obdelavi za potrebe preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj, vključno s terorizmom, v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah: https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=celex%3A22016A1210%2801%29 (v nadaljnjem besedilu: krovni sporazum). Krovni sporazum je prvi dvostranski mednarodni sporazum na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ki zagotavlja celovit seznam pravic in obveznosti v zvezi z varstvom podatkov v skladu s pravnim redom EU. To je uspešen primer, kako je s pogajanji o močnem naboru zaščitnih ukrepov za varstvo podatkov mogoče okrepiti sodelovanje s pomembnim mednarodnim partnerjem na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

64 Resolucija Varnostnega sveta Združenih narodov 2396 z dne 21. decembra 2017 poziva vse države članice ZN, naj razvijejo zmogljivosti za zbiranje, obdelavo in analizo podatkov PNR ob polnem spoštovanju človekovih pravic in temeljnih svoboščin. Glej tudi Sporočilo Komisije „Evropska agenda za varnost“, COM(2015) 185 final: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:52015DC0185&qid=1567608053959&from=EN.

65 https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en

dodatni protokol h Konvenciji Sveta Evrope o kibernetski kriminaliteti (Budimpeški konvenciji))[66].

Spodbujanje sodelovanja med nadzornimi organi, pristojnimi za varstvo podatkov

V času, ko lahko vprašanja v zvezi s spoštovanjem zasebnosti ali incidenti v zvezi z varnostjo vplivajo hkrati na veliko število posameznikov v več jurisdikcijah, lahko tesnejše sodelovanje med nadzornimi organi na mednarodni ravni prispeva k učinkovitejšemu varstvu pravic posameznikov in stabilnejšemu okolju za nosilce dejavnosti. Komisija si bo v tem okviru in v tesnem stiku z odborom prizadevala za lajšanje sodelovanja pri izvrševanju in medsebojne pomoči med EU in tujimi nadzornimi organi, vključno z uporabo novih pristojnosti, ki jih na tem področju zagotavlja Uredba[67]. To bi lahko zajemalo različne oblike sodelovanja pri oblikovanju skupnih razlagalnih ali praktičnih orodij[68] za izmenjavo informacij o tekočih preiskavah.

Komisija namerava okrepiti tudi dialog z regionalnimi organizacijami in mrežami, kot so Združenje držav jugovzhodne Azije (ASEAN), Afriška unija, forum organov Azijsko-pacifiške skupine za varstvo zasebnosti (APPA) ali Iberoameriška mreža za varstvo podatkov, ki imajo vse pomembnejšo vlogo pri oblikovanju skupnih standardov varstva podatkov, spodbujanju izmenjave dobrih praks in spodbujanju sodelovanja med nadzornimi organi. Sodelovala bo tudi z Organizacijo za gospodarsko sodelovanje in razvoj ter Organizacijo za gospodarsko sodelovanje v Azijsko-pacifiški regiji, da bi se dosegla konvergenca in s tem visoka raven varstva podatkov.

VII. Zakonodaja o varstvu podatkov je sestavni del številnih politik

Varstvo osebnih podatkov je zagotovljeno in vključeno v več politik Unije.

Telekomunikacijske in elektronske komunikacijske storitve

Komisija je januarja 2017 sprejela predlog uredbe o zasebnosti in elektronskih komunikacijah[69]. Namen predloga je zaščititi zaupnost komunikacij, kot je določeno v Listini o temeljnih pravicah, pa tudi varovati osebne podatke, ki so lahko del komunikacijske in terminalske opreme končnih uporabnikov.

Predlagana uredba o zasebnosti in elektronskih komunikacijah podrobno opredeljuje in dopolnjuje Uredbo, saj določa posebna pravila za navedene namene. Posodablja sedanja pravila EU o zasebnosti in elektronskih komunikacijah[70], ki odražajo tehnološki in pravni

---

66 http://europa.eu/rapid/press-release_IP-19-2891_en.htm

67 Glej člen 50 uredbe o mednarodnem sodelovanju na področju varstva podatkov. Ta določba zajema številne oblike sodelovanja, od informacij o zakonodaji o varstvu podatkov do posredovanja pritožb in pomoči pri preiskavah.

68 Kot so skupne predloge za obvestila o kršitvah.

69 https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A52017PC0010.

70 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).

razvoj. Povečuje zasebnost posameznikov z razširitvijo področja uporabe novih pravil tudi na ponudnike povrhnjih komunikacijskih storitev (OTT) in tako ustvarja enake pogoje za vse elektronske komunikacijske storitve. Čeprav je Evropski parlament oktobra 2017 sprejel mandat za začetek trialogov, Svet še ni sprejel splošnega pristopa. Komisija ostaja v celoti zavezana uredbi o zasebnosti in elektronskih komunikacijah in bo sozakonodajalca podprla pri njunih prizadevanjih za hitro sprejetje predlagane uredbe.

Zdravstvo in raziskave

Lajšanje izmenjave zdravstvenih podatkov, ki so na podlagi Uredbe občutljivi podatki, med državami članicami postaja vse pomembnejše na področju javnega zdravja iz razlogov splošnega interesa. Ti razlogi vključujejo zagotavljanje zdravstvenega varstva ali zdravljenje, zaščito pred resno čezmejno ogroženostjo zdravja ter zagotavljanje visokih standardov kakovosti in varnosti zdravstvenega varstva ter zdravil ali medicinskih pripomočkov. Uredba določa pravila, ki zagotavljajo zakonito in zanesljivo obdelavo ter izmenjavo zdravstvenih podatkov po EU. Ta pravila se uporabljajo tudi za dostop tretjih oseb do zdravstvenih podatkov bolnikov, vključno do podatkov v povzetkih o bolnikih, e-receptov, dolgoročno pa tudi obsežnih elektronskih zdravstvenih kartotek, ter za njihovo uporabo za namene znanstvenih raziskav. Za posebno področje kliničnih preskušanj je Komisija pripravila tudi posebna vprašanja in odgovore v zvezi z medsebojnim vplivanjem med uredbo o kliničnem preskušanju[71] in Splošno uredbo o varstvu podatkov[72].

Umetna inteligenca

Ker umetna inteligenca pridobiva strateški pomen, je bistveno oblikovati globalna pravila za njen razvoj in uporabo. Komisija se je pri spodbujanju razvoja in uporabe umetne inteligence odločila za pristop, osredotočen na človeka, kar pomeni, da morajo biti aplikacije umetne inteligence v skladu s temeljnimi pravicami[73]. V zvezi s tem pravila, določena v Uredbi, zagotavljajo splošen okvir in vsebujejo posebne obveznosti in pravice, ki so še posebej pomembne za obdelavo osebnih podatkov na področju umetne inteligence. Uredba na primer vključuje pravico ne biti izpostavljen zgolj avtomatiziranemu odločanju, razen v nekaterih primerih[74]. Vključuje tudi posebne zahteve glede preglednosti pri uporabi avtomatiziranega odločanja, in sicer obveznost obveščanja o obstoju takih odločitev ter zagotavljanje smiselnih informacij in pojasnitev njihovega pomena ter predvidenih posledic obdelave za

---

71 https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=celex%3A32014R0536.

72 https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf.

73 Sporočilo Komisije z dne 8. aprila 2019 o krepitvi zaupanja umetno inteligenco, osredotočeno na človeka: https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence.
Etične smernice za zaupanja vredno umetno inteligenco, ki jih je 8. aprila 2019 predstavila strokovna skupina na visoki ravni: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
Glej tudi Priporočilo Sveta OECD o umetni inteligenci: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, načela skupine G20 v zvezi z umetno inteligenco, odobrena kot del izjave voditeljev z vrha G20 v Osaki: https://www.g20.org/pdf/documents/en/annex_08.pdf in Ministrska izjava skupine G20 o trgovini in digitalnem gospodarstvu: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

74 Člen 22 Uredbe.

posameznika[75]. Ta temeljna načela Uredbe so kot posebej pomembna za obravnavanje izzivov in priložnosti, ki jih prinaša umetna inteligenca, priznali strokovna skupina na visoki ravni za umetno inteligenco[76], Organizacija za gospodarsko sodelovanje in razvoj[77] ter skupina G20[78]. Evropski odbor za varstvo podatkov je umetno inteligenco opredelil kot eno od možnih tem v delovnem programu za obdobje 2019–2020[79].

Promet

Razvoj povezanih avtomobilov in pametnih mest je vedno bolj odvisen od obdelave in izmenjave velikih količin osebnih podatkov med več stranmi, vključno z avtomobili, proizvajalci avtomobilov, ponudniki telematskih storitev in javnimi organi, zadolženimi za cestno infrastrukturo. To večstransko okolje pomeni določeno kompleksnost pri dodeljevanju vlog in odgovornosti različnih udeležencev, ki sodelujejo pri obdelavi osebnih podatkov, ter pri tem, kako zagotoviti zakonitost obdelave s strani vseh udeležencev. Skladnost z Uredbo o zasebnosti in elektronskih komunikacijah ter zadevno zakonodajo je bistvenega pomena za uspešno uvajanje inteligentnih prometnih sistemov v vseh načinih prevoza in širjenje digitalnih orodij in storitev, ki omogočajo večjo mobilnost posameznikov in blaga[80].

Energija

Razvoj digitalnih rešitev v energetskem sektorju se vedno bolj zanaša na obdelavo osebnih podatkov. Zakonodaja, sprejeta kot del svežnja Čista energija za vse Evropejce[81], vsebuje nove določbe, ki omogočajo digitalizacijo sektorja električne energije, ter pravila o dostopu do podatkov, upravljanju podatkov in interoperabilnosti, ki omogočajo obdelavo podatkov potrošnikov v realnem času, da se doseže gospodarnost ter spodbudi lastna proizvodnja in udeležba na trgu energije. Zato je spoštovanje pravil o varstvu podatkov zelo pomembno za uspešno izvajanje teh določb.

Konkurenca

Obdelava osebnih podatkov je element, ki ga je treba vedno bolj upoštevati v politiki konkurence[82]. Glede na to, da so organi za varstvo podatkov edini pristojni organi, ki ocenjujejo kršitev pravil o varstvu podatkov, organi za varstvo konkurence, potrošnikov in varstvo podatkov sodelujejo in bodo po potrebi še naprej sodelovali na področjih, na katerih se njihove pristojnosti prekrivajo. Komisija bo spodbujala tako sodelovanje in pozorno spremljala razvoj dogodkov.

---

75 Člen 13(2)(f) Uredbe.

76 https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

77 Priporočilo Sveta o umetni inteligenci: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

78 Ministrska izjava skupine G20 o trgovini in digitalnem gospodarstvu: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

79 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf

80 Na primer z olajšanjem njihovega načrtovanja in uporabe različnih prevoznih sredstev med celotnim potovanjem.

81 Zlasti direktiva o električni energiji: https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=CELEX%3A32009L0072.

82 Na primer zadevo M.8788 – Apple/Shazam in zadevo M. M.8124 – Microsoft/LinkedIn.

Volilni kontekst

V svojih smernicah o uporabi osebnih podatkov v volilnem kontekstu[83], ki so bile izdane septembra 2018 kot del volilnega svežnja[84], je Komisija opozorila na pravila, ki so posebej pomembna za udeležence volitev, vključno z vprašanji, povezanimi z izjemno natančnim ciljnim usmerjanjem na volivce. Te smernice so bile povzete v izjavi Evropskega odbora za varstvo podatkov[85], številni organi za varstvo podatkov pa so izdali smernice na nacionalni ravni. V okviru volilnega svežnja je bila vsaka država članica tudi pozvana, naj vzpostavi nacionalno volilno mrežo, ki bo vključevala nacionalne organe, pristojne za volilne zadeve, in organe, pristojne za spremljanje in uveljavljanje pravil (npr. varstvo podatkov) v zvezi s spletnimi dejavnostmi, povezanimi z volitvami. Sprejeti so bili tudi novi ukrepi za uvedbo sankcij za kršitve pravil o varstvu podatkov s strani evropskih političnih strank in fundacij. Komisija je priporočila, naj države članice uporabijo enak pristop na nacionalni ravni. Ocena volitev v Evropski parlament leta 2019, ki naj bi bila izdana oktobra 2019, bo upoštevala tudi vidike varstva podatkov.

Preprečevanje, odkrivanje in preiskovanje kaznivih dejanj

Učinkovita in prava varnostna unija lahko temelji le na popolnem spoštovanju temeljnih pravic iz Listine EU in sekundarne zakonodaje EU, vključno z ustreznimi zaščitnimi ukrepi za varstvo podatkov, ki omogočajo varno izmenjavo osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Za vse omejitve temeljne pravice do zasebnosti in varstva podatkov veljata strog preizkus nujnosti in sorazmernosti.

VIII. Zaključek

Komisija na podlagi trenutnih razpoložljivih informacij in dialoga z deležniki predhodno ocenjuje, da je bilo prvo leto uporabe uredbe na splošno pozitivno. Kot je razvidno iz tega sporočila, je na številnih področjih potreben nadaljnji napredek.

Izvajanje in dopolnitev pravnega okvira:

- Tri države članice, ki še niso posodobile svoje nacionalne zakonodaje o varstvu podatkov, morajo to nujno storiti. Vse države članice bi morale dokončati uskladitev svoje sektorske zakonodaje z zahtevami iz Uredbe.

- Komisija bo uporabila vsa orodja, ki jih ima na voljo, vključno s postopki za ugotavljanje kršitev, da bi zagotovila, da države članice spoštujejo obveznosti iz Uredbe, in omejila kakršno koli razdrobljenost okvira za varstvo podatkov.

Izkoriščanje celotnega potenciala novega sistema upravljanja:

---

83 https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:52018DC0638&from=SL.
84 https://europa.eu/rapid/press-release_IP-18-5681_sl.htm.
85 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.

- Države članice morajo nacionalnim organom za varstvo podatkov dodeliti zadostne človeške, finančne in tehnične vire.

- Organi za varstvo podatkov bi morali okrepiti sodelovanje, na primer s skupnimi preiskavami. Države članice bi morale olajšati izvajanje takih preiskav.

- Odbor bi moral še naprej razvijati kulturo varstva podatkov v EU in v celoti izkoristiti orodja iz Uredbe, da se zagotovi usklajena uporaba pravil. Še naprej bi moral delati na smernicah, zlasti za mala in srednje velika podjetja.

- Strokovno znanje sekretariata odbora bi bilo treba okrepiti, da bi učinkoviteje podpiral in vodil delo odbora.

- Komisija bo še naprej podpirala organe za varstvo podatkov in odbor, zlasti tako, da bo dejavno sodelovala pri delu odbora in opozarjala na zahteve zakonodaje EU med izvajanjem Uredbe.

- Komisija bo podpirala sodelovanje med organi za varstvo podatkov in drugimi organi, zlasti s področja konkurence, ob polnem spoštovanju njihovih pristojnosti.

Podpiranje in vključevanje deležnikov:

- Odbor bi moral okrepiti način vključevanja deležnikov v svoje delo. Komisija bo še naprej finančno podpirala organe za varstvo podatkov, da bodo lahko prišli v stik deležniki.

- Komisija bo nadaljevala dejavnosti ozaveščanja in sodelovala z deležniki.

Spodbujanje mednarodne konvergence

- Komisija bo še dodatno okrepila dialog o ustreznosti s pripravljenimi ključnimi partnerji, tudi na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Zlasti si prizadeva, da bi v prihodnjih mesecih zaključila pogajanja, ki potekajo z Južno Korejo. Leta 2020 bo poročala o pregledu enajstih sklepov o ustreznosti, sprejetih na podlagi direktive o varstvu podatkov.
- Komisija bo nadaljevala svoje delo, tudi prek tehnične pomoči, z izmenjavo informacij in dobrih praks z državami, ki želijo sprejeti sodobne zakone o zasebnosti, ter spodbujala sodelovanje z nadzornimi organi tretjih držav in regionalnimi organizacijami.
- Komisija bo z večstranskimi in regionalnimi organizacijami sodelovala pri spodbujanju visokih standardov varstva podatkov kot spodbujevalca trgovine in sodelovanja (npr. v okviru pobude „prosti pretok podatkov z zaupanjem“, ki jo je začela Japonska v okviru G20).

Uredba[86] določa, da mora Komisija poročati o njenem izvajanju v letu 2020. To bo priložnost, da se oceni doseženi napredek in to, ali so po dveh letih uporabe različni elementi nove ureditve za varstvo podatkov v celoti operativni. V ta namen bo Komisija sodelovala z Evropskim parlamentom, Svetom, državami članicami, Evropskim odborom za varstvo podatkov, ustreznimi deležniki in državljani.

[86] Člen 97 Uredbe.