NAČELO ODGOVORNOSTI I ODGOVARAJUĆE I UČINKOVITE MJERE PREMA OPĆOJ UREDBI O ZAŠTITI PODATAKA

*Izv. prof. dr. sc. Hrvoje Lisičar**

UDK: 342.738(4)EU
347.152:341.176(4)EU
342.738:347.51(4)EU
DOI: 10.3935/zpfz.74.2.03
Izvorni znanstveni rad
Primljeno: travanj 2024.

Donošenjem Opće uredbe o zaštiti podataka (EU) 2016/679 u zakonodavni okvir koji uređuje zaštitu osobnih podataka u Europskoj uniji zakonodavac je kao novost uveo načelo odgovornosti. Uvođenjem predmetnog načela želi se naglasiti odgovornost voditelja (i izvršitelja) obrade osobnih podataka kao odgovornih subjekata za ispravno i sa zakonom usklađeno postupanje u obradi osobnih podataka a koje je ujedno usklađeno i s razinom rizika za prava pojedinca. Kako bi načelo odgovornosti bilo ostvareno, odgovorni subjekti moraju tijekom cijelog trajanja obrade osobnih podataka aktivno implementirati odgovarajuće i učinkovite mjere kojima se jamči poštovanje propisanih pravila za zaštitu osobnih podataka, pri čemu je teret dokaza o ispunjenju zahtjeva koje nameće načelo odgovornosti na samim odgovornim subjektima. U radu se analiziraju razlozi koji su bili odlučni za uvođenje načela odgovornosti u zakonodavni okvir za zaštitu podataka te njegova povezanost s već prethodno utvrđenim i ustaljenim načelima koja se moraju primjenjivati pri obradi osobnih podataka. Nadalje, razmatraju se odredbe Opće uredbe o zaštiti podataka koje uređuju i nalažu implementaciju odgovarajućih i učinkovitih mjera za usklađivanje sa zahtjevima Uredbe, njihova povezanost s razinom rizika za prava pojedinca a u svrhu postizanje bolje zaštite osobnih podataka te ostvarenja načela odgovornosti. Konačno, u radu se analiziraju recentne

* Dr. sc. Hrvoje Lisičar, izvanredni profesor Pravnog fakulteta Sveučilišta u Zagrebu, Trg Republike Hrvatske 14, 10000 Zagreb; hrvoje.lisicar@pravo.unizg.hr; ORCID ID: orcid.org/0009-0003-7566-3538

odluke Suda EU-a, nacionalnih sudova država članica EU-a te odluke nadležnih nacionalnih regulatornih tijela koje su u vezi s primjenom načela odgovornosti u obradi osobnih podataka i implementacijom odgovarajućih i učinkovitih mjera za usklađivanje sa zahtjevima Uredbe.

Ključne riječi: Opća uredba o zaštiti podataka, GDPR, zaštita podataka, osobni podaci, načelo odgovornosti, tehničke i organizacijske mjere, sigurnost podataka

1. UVODNO O POJMU I NAČELU ODGOVORNOSTI U ZAŠTITI OSOBNIH PODATAKA

Pojam odgovornosti (engl. *accountability*) u području zaštite osobnih podataka spominje se prvi put još u *Smjernicama OECD-a o zaštiti privatnosti i prekograničnom protoku osobnih podataka*[1] iz 1980. godine, gdje se govori o odgovornosti voditelja obrade za poštovanje mjera kojima se implementiraju utvrđena načela pri obradi osobnih podataka. Unatoč tomu, kao jedno od temeljnih načela u obradi osobnih podataka, načelo odgovornosti je u zakonodavni okvir EU-a za zaštitu osobnih podataka uvršteno tek donošenjem Opće uredbe o zaštiti podataka (EU) 2016/679 (dalje u tekstu: Uredba).[2] Kao zasebno načelo, načelo odgovornosti se i prije uključivanja u europski zakonodavni okvir može pronaći u nekoliko zakona kojima se uređuje zaštita osobnih podataka, kao što su kanadski *Personal Information Protection and Electronic Documents Act* (PIPEDA)[3] iz 2000. godine ili *Commercial Privacy Bill of Rights Act* SAD-a iz 2011. godine.[4]

Donošenju Uredbe i uključivanju načela odgovornosti kao samostalnog načela u konačni tekst Uredbe prethodila je široka rasprava o nužnosti jačanja zakonom propisanih obveza u pogledu odgovornog ponašanja odgovornih su-

[1] Organizacija za ekonomsku suradnju i razvoj (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* https://www.oecd-ilibrary.org/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_5lmqcr2k94s8.pdf?itemId=%2Fcontent%2Fpublication%2F9789264196391-en&mimeType=pdf, (20. 10. 2023.).

[2] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (Tekst značajan za EGP), SL L 119, 4. 5. 2016., str. 1 – 88.

[3] Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) od 20. ožujka 2024, Glava 5. odjeljak 4.1., https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-7.html#h-417659 (20. 10. 2023.).

[4] Commercial Privacy Bill of Rights Act of 2011, S.799, https://www.congress.gov/bill/112th-congress/senate-bill/799.

bjekata pri obradi osobnih podataka.[5] Tako je Radna skupina osnovana prema čl. 29. Direktive 95/46/EC[6] (dalje u tekstu: WP29) o važnosti uvođenja načela odgovornosti raspravljala u *Mišljenju 3/2010 o načelu odgovornosti*[7] (dalje u tekstu: Mišljenje WP29) kojim se upućuje na nužnost promjene zakonodavnog okvira za zaštitu osobnih podataka te se predlaže uvođenje načela odgovornosti koje bi zahtijevalo od odgovornih subjekata koji obrađuju osobne podatke da implementiraju odgovarajuće i učinkovite mjere koje bi osigurale da se poštuju sva ostala načela i obveze utvrđeni zakonodavnim okvirom, te da su na zahtjev regulatornog tijela to u mogućnosti i dokazati. Kako se u spomenutom Mišljenju navodi, takva mjera ima za cilj "premještanje" zaštite osobnih podataka "iz teorije u praksu" te pomoći nadležnim tijelima u nadzoru i primjeni zakona.[8] Potreba za jačanjem obveza za odgovorne subjekte u obradi osobnih podataka te uvođenje načela odgovornosti prema Mišljenju WP29 uzrokovani su efektom "poplave podataka", pri čemu je količina osobnih podataka koja se obrađuje i prenosi u stalnom porastu. Uzrok tomu je razvoj informacijsko-komunikacijskih tehnologija te eksponencijalni rast broja korisnika. Time znatno raste i rizik za povrede osobnih podataka. Nadalje se kao razlozi navode i porast vrijednosti osobnih podataka u ekonomskom, društvenom i političkom kontekstu. Konačno, povrede osobnih podataka mogu imati znatan negativan utjecaj na reputaciju i povjerenje za same odgovorne subjekte, kako u javnom tako i u privatnom sektoru.[9]

Nastavno na prethodno spomenuto Mišljenje WP29, Europska komisija 2010. godine u *Komunikaciji br. COM(2010) 609 o sveobuhvatnom pristupu zaštiti osobnih podataka u Europskoj uniji*[10] također navodi da je potrebno razmotriti mogućnosti uvođenja načela odgovornosti u svrhu jačanja obveza implementacije učinkovitih mjera i mehanizama kako bi se osigurala usklađenost s pravilima za

---

5 Cerasaro, E.F., *Accountability principle under the GDPR: is data protection law moving from theory to practice?*, Luiss Law Review, br. 2, 2017., str. 214 – 226, str. 217.

6 Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, SL L 281, 23. 11. 1995., str. 31 – 50.

7 Radna skupina prema čl. 29. za zaštitu podataka (WP29), *Mišljenje 3/2010 o načelu odgovornosti, WP 173*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf (20. 10. 2023.).

8 *Ibid.*, str. 2.

9 *Cf. ibid.*, str. 4 – 5.

10 Europska komisija, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union'*, November 2010, Brussels, COM(2010) 609 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010DC0609 (20.10.2023.).

zaštitu osobnih podataka od strane odgovornih subjekata.[11] U skladu s time u konačni tekst Uredbe uvršteno je načelo odgovornosti kao jedno od temeljnih načela koje je potrebno poštovati u obradi osobnih podataka. Tako se čl. 5. st. 2. propisuje da je *"voditelj obrade odgovoran za usklađenost sa stavkom 1. te je mora biti u mogućnosti dokazati ("pouzdanost")."*[12] Usklađenost sa st. 1. istog članka odnosi se na poštovanje utvrđenih načela u obradi osobnih podataka, i to s načelom zakonitosti, poštenosti, transparentnosti, ograničavanja svrhe, smanjenja količine podataka, točnosti te načelima ograničenja pohrane, cjelovitosti i povjerljivosti. Usporedbom izvornog engleskog teksta Uredbe sa službenim hrvatskim prijevodom može se jasno zaključiti da je pojam "accountability" preveden kao "pouzdanost", što upućuje na to da je riječ o načelu pouzdanosti, a ne o načelu odgovornosti, što je krajnje pogrešno. Kako bismo bolje razumjeli namjeru zakonodavca te razjasnili pojmovnu razliku, potrebno je prethodno razumjeti značenje pojma "accountability". Naime, u gore spomenutim raspravama, posebice u Mišljenju WP29, koje su prethodile donošenju same Uredbe upućuje se na problem tumačenja pojma "accountability", pri čemu se jasno navodi da navedeni pojam u ostalim zemljama članicama nije lako prevesti[13], što može imati za posljedicu različito terminološko i pravno tumačenje te negativan utjecaj na harmoniziranu primjenu pravila na razini EU-a. Jednako tako mnogobrojni autori[14] govore o pojmu "accountability" kao pojmu koji je izrazito teško definirati te pojmu kojega značenje vrlo često ovisi o kontekstu u kojem se rabi.

Definicija pojma "accountability" prema Oxford English Dictionary kazuje da se pojam odnosi na kvalitetu odgovornosti; odgovornost za polaganje računa i odgovaranje za izvršavanje dužnosti ili ponašanja te na podložnost.[15] Iz toga se jasno može utvrditi da navedena definicija u sebi sadržava dva bitna elementa. Prvi se odnosi na obvezu subjekta da obrazloži na koji se način oslobodio

---

11 *Ibid.*, str. 11.

12 Čl. 5. st. 2. Uredbe.

13 Mišljenje WP29, *op. cit*. u bilj. 7, str. 8.

14 V. npr. Bennet, C., *International privacy standards: can accountability ever be adequate?*, Privacy Laws & Business International Report, 2010, str. 23, https://www.privacylaws.com/reports-gateway/reports/, (21. 12. 2023.) ili Bovens, M., *Analysing and assessing accountability: A conceptual framework*, European law journal, *vol*. 13, br. 4, 2007., str. 447 – 468.

15 *Cf*. Alhadeff, J.; Van Alsenoy, B.; Dumortier, J., *The accountability principle in data protection regulation: origin, development and future directions*, u: Guagnin, D.; Hempel, L.; Ilten, C. *et al.* (ur.), *Managing Privacy through Accountability*, Palgrave Macmillan, London, 2012., str. 49 – 82; Oxford English Dictionary, https://www.oed.com (21.10.2023.).

određene obveze ili objasni svoje ponašanje u pogledu nametnutih obveza, a drugi se odnosi na postojanje odnosa između odgovornog subjekta prema drugom tijelu kojemu je odgovoran. Iako je navedena definicija jasna, u praksi se taj pojam vrlo često rabi umjesto nekih drugih pojmova, poput primjerice pojma "responsibility". Iako se oba pojma na hrvatski jezik često prevode kao "odgovornost"[16] važno je naglasiti da između njih postoje bitne razlike. Pojam "responsibility" upućuje na područje dužnosti ili obveze dodijeljene subjektu prirodom položaja, funkcije ili posla tog subjekta[17], iz čega se jasno može zaključiti da su obveze u vezi sa statusom subjekta ili njegovim djelovanjem, za razliku od pojma "accountability" koji osim alociranja odgovornosti zahtijeva od odgovornog subjekta da je u mogućnosti i dokazati, razložiti i objasniti svoje postupke. Stoga je jasno da je pojam "accountability" širi pojam koji podrazumijeva jasno i transparentno ponašanje.

Na temelju prethodne analize samog značenja pojma odgovornosti možemo zaključiti da postoji nekoliko pretpostavki koje je potrebno ispuniti kako bi se moglo smatrati da odgovorni subjekti postupaju u skladu s načelom odgovornosti. Prva pretpostavka je postojanje zakonske norme u skladu s kojom odgovorni subjekti moraju djelovati te prema kojoj će se njihovo djelovanje ocjenjivati. Druga pretpostavka je postojanje odnosa između odgovornog subjekta te subjekta kojemu je odgovoran, bilo nadzornog tijela ili ispitanika čiji se osobni podaci obrađuju. Konačno, treći element je postojanje sankcija za ponašanje odgovornog subjekta koji ne obrađuje osobne podatke u skladu sa zakonom (obrada nije usklađena sa svim načelima) ili svoje usklađeno ponašanje nije u mogućnosti dokazati.[18] Upravo ovaj treći element upućuje na to koliko je pogrešan hrvatski prijevod riječi "accountability" iz izvornog engleskog teksta Uredbe kao "pouzdanost". Da je riječ o pogrešnom prijevodu te neosnovanom korištenju pojma "pouzdanost", jasno se može iščitati i iz samog teksta hrvatskog prijevoda Uredbe gdje se rabi pojam "načelo odgovornosti", a ne "načelo pouzdanosti", kao npr. u uvodnoj izjavi br. 85 Uredbe gdje se izrijekom upućuje na načelo odgovornosti.

Konačno, razmatrajući i druga područja u kojima se na neki način spominje ili rabi načelo odgovornosti kao što su financije, javna administracija i druga pravna područja gdje se ono rabi kao alat kojim se želi nametnuti veća razina

---

16 Pojam "responsibility" se također prevodi i kao "dužnost".

17 Shaw, W.; Barry, V., *Moral Issues in Business*, 13th edition, Wadsworth Publishing Company, Cengage Learning, Boston, 2016., str. 48.

18 *Cf.* Converso, D., *The accountability of data controllers in relation to cloud providers*, Master Thesis Tilburg University, srpanj 2013., str. 10, http://arno.uvt.nl/show.cgi?-fid=131417 (14. 12. 2023.); Alhadeff, J. *et al.*, *op. cit.* u bilj. 15, str. 61.

odgovornosti za organizacije[19], načelo odgovornosti se najčešće definira kao: *preuzimanje odgovornosti od strane odgovornih subjekata za uspostavu odgovarajućih politika i postupka, promicanje dobrih praksi koje uključuju postupanje u skladu sa svim načelima, pravovremeno ispravljanje propusta, saniranje štete, pružanje informacija nadležnim tijelima te odgovornost za štetu. Ono također podrazumijeva i uspostavu infrastrukture koja omogućuje provedbu odgovarajućih i učinkovitih mjera u svrhu bolje zaštite i sigurnosti osobnih podataka.* Kako je implementacija načela odgovornosti ponajprije obveza odgovornih subjekata u obradi osobnih podataka, njih je potrebno ispravno identificirati, razumjeti njihovu ulogu i obveze u obradi osobnih podataka, što je predmet daljnjeg razmatranja.

2. ULOGA ODGOVORNIH SUBJEKATA U OBRADI OSOBNIH PODATAKA

Zakonodavni okvir za zaštitu osobnih podataka nameće pravnu odgovornost za ispunjavanje obveza koje su propisane Uredbom i Zakonom o provedbi opće uredbe o zaštiti podataka[20] (dalje u tekstu: ZPOUZP) za sve odgovorne subjekte u obradi osobnih podataka. Važno je da su svi odgovorni subjekti upoznati s obvezama i temeljnim načelima obrade podataka kako bi se smanjili rizici za prava i slobode ispitanika te kako bi obrada osobnih podataka bila zakonita. Stoga su odgovorni subjekti dužni provoditi obradu osobnih podataka ispitanika u skladu sa svim načelima koja su propisana Uredbom i ZPOUZP-om vodeći računa da su prava ispitanika zaštićena te da je svaka aktivnost obrade provedena na zakonit način.[21] Upravo se uvođenjem načela odgovornosti želi naglasiti potreba i obveza odgovornih subjekata da u obradi osobnih podataka provedu odgovarajuće i učinkovite mjere za usklađivanje sa zahtjevima Uredbe te da su to u mogućnosti i dokazati.[22]

Odgovorni subjekti koji vrše obradu osobnih podataka mogu biti *voditelj obrade, izvršitelj obrade* te u određenim slučajevima *zajednički voditelji obrade*. Kada je riječ o gospodarstvu, ulogu voditelja ili izvršitelja najčešće imaju pravne ili fizičke osobe, a u javnom sektoru određeno nadležno tijelo za obradu osobnih podataka koje je najčešće utvrđeno zakonom. Valja naglasiti da između

19 *Cf. ibid.*, str. 11.

20 Zakon o provedbi opće uredbe o zaštiti podataka, Narodne novine, br. 42/2018.

21 Radna skupina prema čl. 29. za zaštitu podataka (WP29), *Mišljenje 1/2010 o pojmovima "voditelj" i "izvršitelj"*, 16. veljače 2010, str. 7, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (18. 11. 2023.).

22 Uvodna izjava 74. Uredbe.

voditelja i izvršitelja postoje znatne razlike a najvažnija je da voditelj obrade donosi odluku o svrsi i načinu obrade, a izvršitelj obrade obrađuje podatke u ime voditelja obrade, pridržavajući se isključivo naloga i uputa voditelja. Uvijek kada neki odgovorni subjekt vrši obradu osobnih podataka, imat će ulogu voditelja i/ili izvršitelja[23] pa će zato u odnosu na svoju ulogu imati određene obveze koje će morati ispuniti prigodom aktivnosti obrade osobnih podataka. Iz toga razloga od ključne je važnosti ispravno identificirati ulogu pojedinog odgovornog subjekta – djeluje li u svojstvu voditelja i/ili izvršitelja te u skladu s time razumjeti i ispuniti obveze propisane Uredbom i ZPOUZP-om. Nakon utvrđivanja uloge i odgovornosti potrebno je uskladiti poslovanje u skladu sa zakonodavnim okvirom te implementirati odgovarajuće i učinkovite mjere u skladu s načelom odgovornosti kako je to utvrđeno čl. 24. Uredbe. Predmetne mjere i njihovu implementaciju potrebno je biti u mogućnosti i dokazati te kontinuirano preispitivati i ažurirati. Pritom je važno da se pojmovi voditelja i izvršitelja tumače dovoljno široko kako bi se osiguralo ispunjavanje načela odgovornosti, veća razina učinkovitost zaštite osobnih podataka te bolja zaštita ispitanika.[24] Time se umanjuje mogućnost nastajanja eventualnih pravnih praznina i sprečava eventualne zloporabe ili moguće zaobilaženje pravila za zaštitu osobnih podataka.

Valja naglasiti da su pojmovi voditelja i izvršitelja obrade funkcionalni pojmovi kojima je cilj dodijeliti odgovornost subjektima prema njihovoj stvarnoj ulozi u obradi osobnih podataka. To podrazumijeva da uloga pojedinog odgovornog subjekta u obradi kao voditelja ili izvršitelja obrade odgovara njihovoj pravoj funkciji u obradi osobnih podataka te nije ovisna o formalnom imenovanju. To također znači da je, čak i ako je pojedinom odgovornom subjektu formalno dodijeljena pogrešna uloga u obradi osobnih podataka, u kontekstu ispunjavanja načela odgovornosti potrebno promatrati njihovu stvarnu ulogu

---

[23] Osim u slučajevima kada se primjenjuje izuzeće od primjene Uredbe, a što je uređeno čl. 2. t. 2. te se odnosi na obrade tijekom djelatnosti koja nije obuhvaćena opsegom prava Unije; koju obavljaju države članice kada obavljaju aktivnosti koje su obuhvaćene područjem primjene glave V. poglavlja 2. UEU-a; koju provodi fizička osoba tijekom isključivo osobnih ili kućnih aktivnosti; koju obavljaju nadležna tijela u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihova sprečavanja.

[24] O potrebi širokog tumačenja pojma "voditelj obrade" u svojim presudama na jednak način govori i Sud Europske unije u predmetima: C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, presuda od 5. lipnja 2018., točka 28.; C-40/17, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*, presuda od 29. srpnja 2019., točka 66; C-25/17, Korkein hallinto-oikeus (Vrhovni upravni sud, Finska).

u obradi te činjenice koje upućuju na odgovornost za implementaciju odgovarajućih i učinkovitih mjera. Pojmovi voditelja i izvršitelja su također i pojmovi koji su neovisni o drugim pravnim izvorima. Utvrđivanje uloge odgovornih subjekata je isključivo određeno zakonodavnim okvirom za zaštitu osobnih podataka te ne ovisi o određivanju uloga na temelju drugih pravnih propisa.

2.1. Voditelj obrade

Pojam voditelja obrade definiran je čl. 4. st. 7. Uredbe kao *fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje, samo ili zajedno s drugima, određuje svrhe i sredstva obrade osobnih podataka. U slučajevima kada su svrhe i sredstva takve obrade utvrđenim pravom Unije ili pravom države članice, voditelj obrade ili posebni kriterij za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice.* Iz navedene definicije može se jasno zaključiti da ona u sebi sadržava pet bitnih elemenata za određivanje odgovornog subjekta kao voditelja obrade.[25] To su element vrste subjekta, element odlučivanja o svrsi i sredstvima obrade, element samostalnosti, element svrhe i sredstava te element obrade osobnih podataka.[26]

Prvi element odnosi se na vrstu subjekta na koji se definicija odnosi, a to je "fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo". To jasno upućuje na to da ne postoji ograničenje u pogledu vrste subjekta koji može u kontekstu obrade imati ulogu voditelja obrade. Pri tumačenju ovog elementa definicije voditelja obrade do najviše prijepora dolazi u odnosu na ulogu pojedinih fizičkih i pravnih osoba u obradi osobnih podataka. Naime, u praksi ulogu voditelja obrade prema Uredbi najčešće imaju pravne osobe koje određuju svrhu i sredstva obrade a pitanje koje se često nameće vezano je uz ulogu pojedinaca (fizičkih osoba) koji djeluju unutar ili u ime pravnih osoba. Ako je primjerice neka fizička osoba unutar pravne osobe zadužena da provodi obradu osobnih podataka i osigura usklađenost sa zakonodavnim okvirom za zaštitu osobnih podataka za pravnu osobu, ta osoba neće se smatrati voditeljem obrade, već ona djeluje u ime pravne osobe. Tako se može smatrati da za svaku obradu osobnih podataka koju provode zaposlenici unutar neke pravne osobe odgovornost snosi sama pravna osoba, tj. ona ima ulogu voditelja obrade te je dužna postupati u skladu s načelom odgovornosti i implementirati odgovara-

[25] O definiciji pojma voditelja obrade na jednak način raspravlja se i u: Europski odbor za zaštitu podataka (EDPB), *Smjernice 07/2020 o pojmovima voditelja i izvršitelja obrade u Općoj uredbi o zaštiti podataka*, Verzija 2.0 usvojeno 7. srpnja 2021., https://edpb.europa.eu/system/files/2023- 10/edpb_guidelines_202007_controllerprocessor_final_hr.pdf (7. 12. 2023.).

[26] *Cf. ibid.*, str. 9.

juće i učinkovite mjere za usklađivanje s Uredbom, uključujući i mjere koje se odnose na obuku, nadzor i odgovornost zaposlenika. Iznimno, postoje slučajevi kada bi se fizička osoba koja djeluje unutar neke pravne osobe mogla smatrati samostalnim voditeljem obrade. To su slučajevi kada zaposlenik odluči koristiti se osobnim podacima prikupljenima u vrijeme obavljanja svojih zadaća za pravnu osobu za vlastite svrhe, te će se u tom slučaju pored pravne osobe koja je izvorni voditelj obrade i sam zaposlenik – fizička osoba smatrati samostalnim voditeljem obrade.[27]

Drugi bitan element definicije za imenovanje voditelja obrade odnosi se na mogućnost donošenja odluka o ključnim elementima obrade, tj. na mogućnost "određivanja" svrhe i sredstva obrade osobnih podataka. To određivanje svrhe i sredstava obrade može proizlaziti iz zakona ili ugovora kojim je pojedini voditelj obrade definiran kao tijelo koje će odlučivati o ključnim elementima obrade osobnih podataka ili iz činjenice da je svojim poslovnim aktivnostima sam preuzeo takvu ulogu u postupku obrade osobnih podataka. Kada je nekim zakonom utvrđena svrha obrade osobnih podataka, voditelj obrade će najčešće biti onaj koji je zadužen za ispunjavanje te svrhe. Tako je i u slučaju kada se osobni podaci obrađuju u svrhu ispunjavanja ugovornih obveza. Najčešće će iz samog ugovora i njegove svrhe proizlaziti tko odlučuje o svrsi i sredstvima obrade, čak i ako sam ugovor ne navodi tko je voditelj obrade.

Ako pak ugovor izrijekom predviđa i izričito navodi tko je voditelj obrade, u slučaju sumnje o odlučnom utjecaju odredbe ugovora nisu od presudne važnosti, već se u skladu s funkcionalnim određenjem pojma voditelja obrade određuje prema stvarnim okolnostima koje upućuju na određenje uloga.[28] Također, kada zakonom nije utvrđena neka svrha ili odgovorni subjekt (voditelj obrade), potrebno je promatrati konkretne aktivnosti u određenom kontekstu obrade osobnih podataka, pri čemu određivanje uloge voditelja neće ovisiti o prirodi nekog subjekta, nego o odlučnom utjecaju na ključne elemente obrade osobnih podataka – svrhu i sredstva. Primjerice, ako neki subjekt obrađuje osobne podatke zaposlenika ili svojih klijenata u svrhu obavljanja svojih poslovnih aktivnosti, on će ujedno najčešće i određivati koja je svrha obrade osobnih podataka te na koji način i uz pomoć kojih sredstava će se obrada provoditi pa će stoga u kontekstu Uredbe i imati ulogu voditelja obrade. Iz svega navedenoga važno je istaknuti da je za ulogu voditelja obrade ključan element odlučni utjecaj koji je stvaran i realiziran prigodom određivanju svrhe i sredstava obrade osobnih podataka.[29]

---

[27] *Cf. ibid.*, str. 10.

[28] *Cf. ibid.*, str. 12.

[29] *Cf.* Ivanova, Y., *Data Controller, Processor, or Joint Controller: Towards Reaching GDPR*

Treći element definicije odnosi se na broj odgovornih subjekata koji su u mogućnosti određivati ključne elemente obrade osobnih podataka – svrhu i sredstva obrade. Prethodno je već spomenut pojam zajednički voditelji obrade. Tako i definicija pojma voditelja obrade prepoznaje mogućnost da jedan subjekt samostalno odlučuje o ključnim elementima obrade ili da se u toj ulozi istodobno nalazi više subjekata. To ujedno znači da se nekoliko odgovornih subjekata istodobno može naći i u ulozi voditelja pojedine obrade osobnih podataka, pri čemu svaki od njih solidarno odgovara ispitaniku za svoja postupanja u skladu s načelom odgovornosti i implementacije odgovarajućih i učinkovitih mjera.

Četvrti element definicije pojma voditelja obrade odnosi se na samu svrhu i sredstva o kojima odlučuje voditelj obrade. Uredba u skladu s načelom ograničenja svrhe, tj. čl. 5 st. 1(b) propisuje da se osobni podaci prikupljaju u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama. Navedeno upućuje na to da je svrha i sredstvo obrade ključni element koji neki subjekt određuje kako bi ga se moglo smatrati voditeljem obrade. Stoga je, kada se utvrđuje uloga pojedinog odgovornog subjekta u obradi osobnih podataka, nužno postaviti pitanje tko utvrđuje razloge, tj. zbog čega se obrada provodi te na koji način, tj. kako će se obrada osobnih podataka provoditi.[30] Odgovorni subjekt koji kumulativno odlučuje o oba pitanja ima odlučni utjecaj te se ima smatrati voditeljem obrade.

Konačno, peti element definicije i identificiranja voditelja obrade odnosi se na sam postupak obrade. Pojam obrade je definiran čl. 4. st. 2. Uredbe kao svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, stoga je važno da se svrha i sredstva koja utvrđuje voditelj obrade odnose na pojedinačnu ili skupnu obradu osobnih podataka. Ako su predmet obrade podaci koji ne pripadaju kategoriji osobnih podataka, odgovorni subjekt neće prema Uredbi biti voditelj obrade te se Uredba ne primjenjuje. Također, moguća je situacija da obrada koja uključuje više dionika bude podijeljena u zasebne obrade pa će svatko od dionika za pojedinačnu obradu biti voditelj obrade. S druge strane ako obrada uključuje više dionika a cilj je ostvarenje iste svrhe, svi odgovorni subjekti smatrat će se zajedničkim voditeljima. Važno je istaknuti da sam voditelj obrade ne mora nužno provoditi obradu u stvarnom smislu. Kada je od strane voditelja obrade angažiran drugi

Compliance in a Data- and Technology-Driven World, u: Tzanou, M. (ur.), *Personal Data Protection and Legal Developments in the European Union*, IGI Global, Hershey, PA, 2020., str. 61 – 84.

30 Na jednak način o svrsi i sredstvima obrade te njihovom utvrđivanju rasprava se i u predmetu Suda Europske unije u Mišljenju nezavisnog odvjetnika Bota u predmetu *Wirtschaftsakademie*, C-210/16, točka 46.

subjekt da vrši stvarnu obradu nad osobnim podacima, voditelj obrade je i dalje onaj subjekt koji je imao odlučni utjecaj na određivanje svrhe i načina (kako će se podaci obrađivati), tj. onaj koji je angažirao predmetni subjekt za obradu.

U postupku utvrđivanja voditelja obrade osobnih podataka potrebno je sve navedene elemente uzeti u obzir. Tek kada su svi elementi kumulativno ispunjeni, sa sigurnošću se može utvrditi tko je od razmatranih odgovornih subjekata koji sudjeluju u obradi voditelj obrade, tj. tko je odgovoran za potpunu implementaciju načela odgovornosti i odgovarajućih i učinkovitih mjera u svrhu zaštite osobnih podataka koji su predmet obrade.

2.2 Zajednički voditelji obrade

Kao što je već prethodno spomenuto kod trećeg elementa definicije pojma voditelja obrade, u obradi kao voditelj može sudjelovati i više od jednog subjekta. Ako pritom više subjekata zajednički određuje svrhu i način obrade, oni će se smatrati zajedničkim voditeljima obrade.[31] Zajedničko utvrđivanje svrhe podrazumijeva da svi uključeni subjekti provode obradu osobnih podataka u zajednički utvrđenu svrhu, dok zajedničko utvrđivanje sredstava zahtijeva da su zajednički voditelji utjecali na njihov odabir, pri čemu je važno istaknuti da to nužno ne podrazumijeva zajedničko korištenje istog načina obrade osobnih podataka. Pritom je potrebno ispuniti i sve ostale bitne elemente definicije pojma voditelja obrade od strane svih subjekata. Takvo sudjelovanje u obradi osobnih podataka može biti temeljeno na dogovoru kojim se uređuje međusoban odnos, prava i dužnosti, osim ako su pravom Unije ili pravom države članice unaprijed utvrđene odgovornosti u pogledu specifične obrade osobnih podataka.[32] Dogovor između zajedničkih voditelja obrade mora biti u skladu s načelom transparentnosti, tj. svi ključni elementi tog dogovora moraju biti dostupni na uvid ispitanicima, bez obzira na uvjete koji su u odnosu na odgovornosti, dužnosti i prava dogovorom utvrđeni, za ostvarivanje prava utvrđenih Uredbom te za implementaciju načela odgovornosti ispitaniku u građanskopravnom smislu odgovaraju svi zajednički voditelji obrade solidarno. Postojanje zajedničke odgovornosti prema ispitaniku u kontekstu zakonodavnog okvira za zaštitu osobnih podataka, prema tumačenju Suda Europske unije[33], potrebno je promatrati u svezi s obradom i relevantnim okolnostima, budući da pojedini subjekti mogu sudjelovati u obradi osobnih podataka u različitim fazama i različitom opsegu.

---

31 Čl. 26. Uredbe.

32 *Cf.* Colcelli, V., *Joint controller agreement under GDPR*, EU and Comparative Law Issues and Challenges Series, *vol.* 3, 2019, str. 1030 – 1047, str. 1032.

33 *V.* Sud Europske unije, C-40/17, *op. cit.* u bilj. 23, točka 80.

Pri utvrđivanju odgovornih subjekata kao zajedničkih voditelja obrade važno je uzeti u obzir stvarnu ulogu u obradi osobnih podataka. Čak i ako je na temelju dogovora utvrđeno da više subjekata određuje svrhu i sredstva obrade, a u stvarnosti jedan od njih nije imao takav odlučujući utjecaj, u tom slučaju voditelj obrade bit će samo onaj subjekt koji je samostalno odlučivao o ključnim elementima obrade. Jednako tako, u slučajevima kada jedan od subjekata odlučuje o svrsi a drugi o sredstvima obrade, neće se smatrati zajedničkim voditeljima obrade, već će svaki od njih biti samostalni voditelj obrade. Ključno je da svi subjekti istodobno imaju odlučan utjecaj na oba ključna elementa – svrhu i sredstva. Također, činjenica da jedan od voditelja koji sudjeluje u obradi nema pristup osobnim podacima nije dovoljna da bi se isključilo postojanje zajedničkih voditelja.[34]

Zajedničkim voditeljima obrade mogu se smatrati i oni odgovorni subjekti u obradi koji djeluju bez prethodnog formalnog dogovora, ali se svojim usklađenim postupanjem međusobno nadopunjuju a u nedostatku takvog djelovanja sama obrada ne bi bila moguća. U tom kontekstu usklađenog djelovanja odgovornih subjekata, važno je promatrati isključivo djelovanje koje se odnosi na određivanje svrhe i sredstava obrade osobnih podataka te da je ono neraskidivo povezana s njihovim određivanjem i samom obradom.

Uz ispravno utvrđivanje slučajeva gdje dva ili više odgovornih subjekata djeluju kao zajednički voditelji obrade, potrebno je izdvojiti i pojedine primjere gdje se njihovo djelovanje neće smatrati djelovanjem zajedničkih voditelja. Primjerice, kada je predmet suradnje između dva odgovorna subjekta razmjena istih osobnih podataka, pri čemu izostaje zajedničko utvrđivanje svrhe i sredstava, treba se smatrati da odgovorni subjekti djeluju kao zasebni voditelji obrade. Također, u slučaju kada se više odgovornih subjekata koristi istim sredstvima obrade i istim osobnim podacima ali je svaki od njih utvrdio svoju svrhu, smatrat će se da djeluju kao zasebni voditelji obrade.

2.3. Izvršitelj obrade

Uz prethodno spomenute uloge odgovornih subjekata u obradi osobnih podataka kao voditelja obrade ili zajedničkih voditelja obrade, jednu od ključnih uloga u obradi osobnih podataka imaju i izvršitelji obrade. Iako je primarna odgovornost za potpunu implementaciju načela odgovornosti i mjera za usklađivanje sa zahtjevima Uredbe na voditelju obrade to ne znači da su izvršitelji obrade izuzeti od tih obveza, štoviše, na temelju uputa voditelja obrade i s ob-

[34] *V.* Sud Europske unije, C-25/17, *op. cit.* u bilj. 23., točka 75.

zirom na njihovu ulogu u obradi osobnih podataka na njih se najčešće odnosi najviše obveza u pogledu implementacije tehničkih i organizacijskih mjera u svrhu postizanja veće sigurnosti obrade i osobnih podataka.

Uredba čl. 4. st. 8. definira izvršitelja obrade kao fizičku ili pravnu osobu, tijelo javne vlasti, agenciju ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade. Kao i u slučaju voditelja obrade, navedenu definiciju izvršitelja obrade potrebno je promatrati u kontekstu njezinih ključnih elemenata. Prvi element je sam subjekt koji može imati ulogu izvršitelja obrade. Kao i u slučaju voditelja obrade, nema ograničenja u pogledu vrste subjekta koji može imati takvu ulogu, ali pritom je važno istaknuti da u odnosu na voditelja obrade taj subjekt mora biti zaseban subjekt u pravnom smislu (neovisan o voditelju) na koji je voditelj obrade prenio neke ili sve aktivnosti obrade. U slučajevima kada voditelj obrade sam odluči provoditi sve aktivnosti obrade osobnih podataka unutar svoje organizacije, rabeći vlastita sredstva za obradu osobnih podataka, on u cijelosti preuzima i ulogu izvršitelja obrade, pa izvršitelj obrade kao zaseban subjekt u predmetnoj obradi ne postoji. Drugi bitan element definicije jest da je riječ o obradi osobnih podataka, što upućuje na to da se mora raditi o osobnim podacima na kojima se poduzimaju aktivnosti koje Uredba smatra obradom osobnih podataka kako je definirano čl. 4. st. 2.[35] Treći je bitan element definicije pojma izvršitelja obrade da se aktivnost obrade provodi na temelju naloga u ime voditelja obrade. To je ujedno i ključan element koji određuje ulogu izvršitelja. Takvo djelovanje podrazumijeva da je izvršitelj u pravnom smislu neovisan o voditelju obrade koji mu prenosi (delegira) određene ovlasti i na temelju uputa u njegovo ime vrši obradu, pri čemu upute mogu biti jasno utvrđene (ograničene) ili općenite, ali se isto tako može izvršitelju ostaviti mogućnost odabira odgovarajućih i učinkovitih mjera u obradi osobnih podataka. Također, prema čl. 28. st. 3. Uredbe delegiranje ovlasti, tj. angažman izvršitelja mora biti utemeljen i uređen ugovorom ili nekim drugim pravno obvezujućim aktom, a što se može smatrati odgovarajućom i učinkovitom mjerom te ispunjavanjem načela odgovornosti samog voditelja. Kao i pojam voditelja obrade, pojam izvršitelja obrade funkcionalan je pojam. Neovisno o dodijeljenim ulogama voditelja i izvršitelja obrade, promatra se stvarna uloga u obradi osobnih podataka. Tako u slučaju da se izvršitelj koristi osobnim podacima

[35] Sam pojam obrade osobnih podataka je Uredbom postavljen izrazito široko te obuhvaća gotovo bilo kakvu aktivnost koja je povezana s osobnim podacima: prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje.

voditelja obrade mimo svrhe koju je odredio voditelj obrade ili se koristi osobnim podacima za drugu svrhu koju je sam utvrdio, za tu obradu smatrat će se samostalnim voditeljem obrade. Takvo postupanje ujedno predstavlja i kršenje obveza utvrđenih ugovorom ili pravno obvezujućim aktom, ali i kršenje Uredbe što može imati za posljedicu izricanje kazne od strane neovisnog nadzornog tijela u skladu s Uredbom. Za pojedinu obradu osobnih podataka voditelj obrade može angažirati i više izvršitelja, dok s druge strane jedan izvršitelj može biti angažiran od strane više voditelja, pri čemu vrši obradu osobnih podataka za svaku svrhu i svakog voditelja pojedinačno u skladu s Uredbom i obvezujućim pravnim aktom.

2.4 Podizvršitelj obrade

Osim izvršitelja, ovdje se je važno osvrnuti se i na ulogu podizvršitelja. Naime, u praksi je obrada osobnih podataka vrlo često kompleksan zadatak te za izvršavanje određenih segmenata obrade osobnih podataka izvršitelji mogu pod određenim uvjetima uključiti i podizvršitelje. Kako bi to bilo moguće, u skladu s čl. 28. st. 2. Uredbe izvršitelj obrade od voditelja obrade mora prethodno pribaviti opće ili posebno odobrenje koje mora biti u pisanom obliku (bilo na papiru ili elektronički). Kada izvršitelj obrade želi uključiti podizvršitelja u obradu osobnih podataka na temelju općeg odobrenja voditelja obrade, o tome prethodno mora obavijestiti voditelja obrade te zatražiti njegovu suglasnost. Opće odobrenje trebalo bi uključivati smjernice o načinu odabira podizvršitelja te zahtjeve u pogledu implementiranih tehničkih i organizacijskih mjera od strane podizvršitelja. U slučaju da voditelj obrade ne istakne prigovor ili uopće ne odgovori na zahtjev za uključivanjem podizvršitelja u dogovorenom roku, može se smatrati da je suglasan. Odobrenje voditelja obrade za uključivanje podizvršitelja može biti i posebno, tj. traženo za i odnositi se na specifičnog podizvršitelja kojeg izvršitelj obrade želi uključiti u obradu. U tom slučaju, ako voditelj obrade u dogovorenom roku ne odgovori na zahtjev izvršitelja, smatrat će se da nije suglasan s uključivanjem tog podizvršitelja u obradu osobnih podataka. Način uključivanja podizvršitelja u obradu osobnih podataka, putem općeg ili posebnog odobrenja, voditelj i izvršitelj uređuju istim ugovorom ili pravno obvezujućim aktom kojim uređuju i ostale obveze u pogledu obrade osobnih podataka.

Neovisno o načinu davanja odobrenja za uključivanje podizvršitelja u obradu osobnih podataka, prema čl. 28. st. 4. Uredbe izvršitelj koji je angažirao podizvršitelja u cijelosti je odgovoran voditelju obrade za postupanje u skladu s obvezujućim pravnim aktom i izvršavanje svih preuzetih obveza, uključujući

i one obveze koje je prenio na podizvršitelja. Pravila koja propisuju obvezu uređivanja odnosa voditelj – izvršitelj putem ugovora ili pravno obvezujućeg akta, primjenjuju se *mutatis mutandis* i na uređivanje odnosa izvršitelj – podizvršitelj. Tako izvršitelj mora od podizvršitelja zahtijevati ispunjenje svih onih obveza koje su njemu nametnute od strane voditelja obrade.

2.5. Primatelj i treća strana

Pojmovi primatelj i treća strana definirani su Uredbom kako bi se utvrdili odnosi voditelja obrade s ostalim subjektima koji eventualno imaju ovlaštenje za pristup osobnim podacima u nadležnosti voditelja. Za primatelja i treću stranu Uredba ne propisuje posebne obveze te se oni ne smatraju odgovornim subjektima, ali nakon prijenosa osobnih podataka to mogu postati.

Primatelj je čl. 4. st. 9. Uredbe definiran kao fizička ili pravna osoba, tijelo javne vlasti, agencija ili bilo koje drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana ili nije, te se time obuhvaćaju svi oni koji primaju podatke. Tako se u postupku obrade osobnih podataka svaki izvršitelj koji od voditelja prima osobne podatke ima smatrati primateljem. Također, svaka treća strana koja od voditelja ili izvršitelja (koji ima ovlaštenje) prima podatke smatrat će se primateljem podataka te se u pogledu tih podataka, nakon što ih zaprimi, ima smatrati voditeljem obrade osobnih podataka.[36]

Trećom stranom u obradi osobnih podataka se prema čl. 4. st. 10. ima smatrati ona osoba koja nije ispitanik, voditelj obrade, izvršitelj obrade ili pravna ili fizička osoba koja je ovlaštena za obradu osobnih podataka koja je pod izravnom nadležnošću voditelja ili izvršitelja obrade. U skladu s time, sve osobe koje nisu zaposlenici voditelja ili izvršitelja obrade ili osobe izjednačene po ulozi sa zaposlenicima koji imaju ovlaštenja za obradu osobnih podataka smatrat će se trećom stranom. To uključuje i one zaposlenike voditelja obrade koji nemaju ovlaštenja za obradu osobnih podataka. Također, kada se prenose podaci unutar grupe poduzeća, svaka članica grupe koja nema ulogu voditelja ili izvršitelja obrade a prenose joj se osobni podaci članova grupe ima se smatrati trećom stranom.

Razumijevanje razlike navedenih pojmova važno je kako bi se u slučaju otkrivanja osobnih podataka moglo utvrditi radi li se o odgovornom postupanju. Naime, kada zaposlenici voditelja ili izvršitelja sudjeluju u obradi osobnih po-

[36] *Cf.* Aridor, G.; Che, Y.-K.; Salz, T., *The effect of privacy regulation on the data industry: empirical evidence from GDPR*, The RAND Journal of Economics, *vol*. 54, 2023., str. 695 – 730.

dataka, oni mogu biti primatelji bez potrebe za dodatnim pravnim zahtjevima. S druge strane, treća strana je subjekt koji nije povezan s voditeljem ili izvršiteljem obrade, te samim time nije ovlašten za korištenje osobnih podataka voditelja obrade ako za to u konkretnom slučaju nema valjanu pravnu osnovu.

2.6. Predstavnici voditelja ili izvršitelja obrade

S obzirom na eksteritorijalnu primjenu Uredbe, koja odgovornim subjektima smatra i sve one voditelje ili izvršitelje obrade koji nemaju poslovni nastan na teritoriju EU-a a vrše obradu osobnih podataka ispitanika koji se nalaze u EU-u povezanih s nuđenjem robe ili usluga ispitanicima u Uniji, neovisno o tome treba li ispitanik izvršiti plaćanje ili praćenje njihova ponašanja dokle god se njihovo ponašanje odvija unutar Unije (čl. 3. st. 2. Uredbe), takvim se odgovornim subjektima nameće obveza imenovanja predstavnika u EU-u. Imenovanje mora biti u pisanom obliku te predstavnik koji se imenuje mora imati poslovni nastan u nekoj od država članica EU-a gdje se nalaze ispitanici čiji se osobni podaci obrađuju.[37] Imenovanje ovlašćuje predstavnika da u ime odgovornog subjekta zaprima sva pitanja vezana uz obradu osobnih podataka bilo od ispitanika ili od neovisnih nadzornih tijela. Time odgovorni subjekti koji nemaju poslovni nastan u EU-u ispunjavaju načela zakonitosti, transparentnosti te odgovornosti iako samo imenovanje ne otklanja mogućnost postavljanja pravnih zahtjeva usmjerenih protiv samih odgovornih subjekata.

3. IMPLEMENTACIJA ODGOVARAJUĆIH I UČINKOVITIH MJERA KAO ISPUNJAVANJE NAČELA ODGOVORNOSTI

Implementacija odgovarajućih i učinkovitih mjera u obradi osobnih podataka osnova je za ispunjavanje svih obveza i postizanje usklađenosti sa zahtjevima koje nameće Uredba. One su također u izravnoj vezi s načelom odgovornosti, gdje će ispunjavanje zahtjeva koje nameće načelo odgovornosti biti zadovoljeno tek nakon implementacije odgovarajućih i učinkovitih mjera. Pritom pojam "odgovarajuće" upućuje na primjenu onih mjera primjenom kojih se postiže određena svrha te ujedno osigurava zadovoljavajuća razina zaštite osobnih podataka u odnosu na samu vrstu obrade, kategoriju osobnih podataka te razinu

[37] Vojković, G.; Milenković, M.; Katulić, T., *IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law*, Business Systems Research : International journal of the Society for Advancing Innovation and Research in Economy, *vol*. 11, br. 3, 2020., https://hrcak.srce.hr/ojs/index.php/bsr/article/view/12916 [17. 4. 2024].

rizika koju ta obrada predstavlja za prava ispitanika, dok se pojam "učinkovito" odnosi na djelotvornost tih mjera, tj. postizanje najveće razine zaštite osobnih podataka, prava ispitanika zajamčenih Uredbom i pretpostavljenih načela uz proporcionalni utrošak vremena i resursa.[38] Oba pojma se također izravno povezuju s vjerojatnošću i ozbiljnosti rizika za prava i slobode ispitanika. Naime, koje mjere će se za pojedinu obradu osobnih podataka moći smatrati odgovarajućima i učinkovitima ovisi i o vjerojatnosti da dođe do povrede osobnih podataka tijekom njihove obrade te, u slučaju povrede, koliki rizik to predstavlja za prava i slobode ispitanika. Uvodna izjava (74) Uredbe tako govori da bi se vjerojatnost i ozbiljnost rizika za prava i slobode ispitanika trebale procjenjivati prema prirodi, opsegu, kontekstu i svrsi obrade. U praktičnom smislu to znači da primjena odgovarajućih i učinkovitih mjera za usklađivanje sa zahtjevima Uredbe ne ovisi o veličini i načinu organizacije odgovornog subjekta, broju zaposlenih, ostvarenom prihodu ili nekom drugom objektivnom kriteriju, već isključivo o samoj obradi osobnih podataka, tj. svrsi obrade, količini i kategoriji osobnih podataka te načinu na koji se ona provodi.

U skladu s pojmovima odgovarajuće i učinkovito Uredba izrijekom ne navodi koje je sve specifične mjere potrebno poduzeti kako bi se pojedina obrada osobnih podataka mogla smatrati usklađenom sa zahtjevima Uredbe. Neke se od mjera, kojih implementacija predstavlja minimum u ostvarivanju načela odgovornosti, izrijekom nameću pojedinim odgovornim subjektima s obzirom na njihovu ulogu u obradi osobnih podataka, dok je obveza primjene ostalih mjera vezana uz vjerojatnost i ozbiljnost rizika za prava i slobode ispitanika. U tom kontekstu potrebno je razmotriti sve mjere s kojima valja uskladiti obradu osobnih podataka, kako bi se moglo smatrati da odgovorni subjekti postupaju u skladu s načelom odgovornosti prema čl. 5. st. 2. Uredbe te da su to u mogućnosti i dokazati.

3.1. Tehničke i organizacijske mjere i sigurnost obrade

Temelj i polazna točka za ostvarenje zahtjeva koje postavlja načelo odgovornosti reflektira se u čl. 24. Uredbe koji izrijekom nameće obveze voditelju obrade kao odgovornom subjektu implementaciju odgovarajućih tehničkih i organizacijskih mjera. Tako čl. 24. st. 1. Uredbe nalaže da, uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obra-

[38] *Cf.* Foulsham, M.; Hitchen, B.; Denley, A., *GDPR: How To Achieve and Maintain Compliance*, 1st edition, Routledge, Abingdon, 2019., str. 63.

da provodi u skladu s Uredbom. Time se želi naglasiti primarna odgovornost voditelja obrade za implementaciju tih mjera. Isti stavak također ističe obvezu preispitivanja i ažuriranja tehničkih i organizacijskih mjera, čime se naglašava kontinuiranost obveza te nužnosti njihova prilagođavanja promijenjenim uvjetima u postupku obrade osobnih podataka. To se postiže implementacijom odgovarajućih politika zaštite podataka od strane voditelja obrade u skladu s čl. 24. st. 2. a koje imaju za cilj na cjelovit način urediti implementaciju svih odgovarajućih i učinkovitih mjera za usklađivanje koje Uredba nalaže. Iako Uredba ne navodi jasno što su odgovarajuće politike, riječ je o zahtjevu koji implicira sustavni pristup u zaštiti osobnih podataka a koji na sveobuhvatan način uređuje implementaciju svih odgovarajućih i učinkovitih mjera za usklađivanje koje Uredba nameće u svrhu postizanja usklađenosti. U praksi odgovarajuće politike najčešće podrazumijevaju: imenovanje službenika za zaštitu osobnih podataka, uspostavu organizacijske strukture koja jamči provedbu načela odgovornosti, nadgledanje i odobravanje internih politika, mapiranje i poznavanje osobnih podataka, procjenu svrha obrade osobnih podataka, procjenu rizika za prava i slobode ispitanika, usvajanje internih politika i postupaka koje su obvezujuće za sve osobe unutar organizacije koje sudjeluju u obradi osobnih podataka, dodjeljivanje odgovornosti za pojedine postupke obradu na različitim razinama organizacije, uspostavu sustava za trajno praćenje usklađenosti, nadzor te vanjsko vrednovanje, uspostavu sustava koji osiguravaju transparentnost u postupanju za sve uključene strane i uspostavu mehanizama za djelovanje u slučaju povrede osobnih podataka.[39]

Iako je za ispunjavanje načela odgovornosti ponajprije odgovoran voditelj obrade, kada je riječ o zaštiti osobnih podataka i njihovoj sigurnosti, obveza implementacije odgovarajućih tehničkih i organizacijskih mjera u svrhu umanjenja rizika te povećanja razine sigurnosti odnosi se i na izvršitelje obrade. Tako čl. 32. st. 1. nalaže da u svrhu sigurnosti obrade voditelj i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere pritom uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca.

Iz navedenoga se jasno može zaključiti da je upravo implementacija tehničkih i organizacijskih mjera jedan od temeljnih zahtjeva Uredbe i središnja točka za postizanje sigurnosti podataka te postupanje u skladu s načelom odgovornosti. Pojam tehničkih i organizacijskih mjera potrebno je tumačiti u širem smi-

[39] Kuner, C.; Bygrave, L. A.; Docksey, C.; Drechsler, L. (ur.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford Academic, New York, 2020., str. 564.

slu kao bilo koju odgovarajuću metodu ili sredstvo koje voditelj obrade primjenjuje prigodom ručne ili automatizirane obrade osobnih podataka kako bi na učinkovit način ostvario zadani cilj u svrhu postizanja veće sigurnosti osobnih podataka.[40] Iako se Uredba često poziva na primjenu tehničkih i organizacijskih mjera njome nije jasno definirano na što se one točno odnose. Članak 32. st. 1. Uredbe kao primjer navodi neke od odgovarajućih tehničkih i organizacijskih mjera koje se prema potrebi primjenjuju u svrhu osiguravanja odgovarajuće razine sigurnosti s obzirom na rizik. To su pseudonimizacija i enkripcija podataka (čl. 32. st. 1. (a)); sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade (čl. 32. st. 1. (b)); sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta (čl. 32. st. 1. (c)); proces za redovito testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade (čl. 32. st. 1. (d)). Navedene mjere ne predstavljaju izričitu obvezu za svakog voditelja i izvršitelja obrade, ali njihova primjena svakako može pridonijeti većoj sigurnosti podataka i ispunjavanju načela odgovornosti.

Kako je pojam tehničkih i organizacijskih mjera usko vezan uz koncept informacijske sigurnosti, razmatrajući različite izvore[41] koji se bave tim pitanjem te govore o primjeni tehničkih i organizacijskih mjera, a kao daljnju razradu mjera koje se navode u čl. 32. st. 1. Uredbe, te mjere možemo detaljnije klasificirati u nekoliko skupina. U prvu skupinu tehničkih i organizacijskih mjera spadaju mjere kojima se osigurava kontrola fizičkog pristupa koje je cilj fizička zaštita informacijskih sustava koji sadržavaju osobne podatke. Mjere koje se primjenjuju u svrhu postizanja tog cilja su primjena mehanizama za zaštitu pristupa građevinama, prostorijama i sustavima gdje su podaci pohranjeni, što uključuje kontinuirani nadzor, poštovanje sigurnosnih protokola, osiguravanje

---

40 *Cf.* Europski odbor za zaštitu podataka, *Smjernice br. 4/2019 o članku 25 o tehničkoj i integriranoj zaštiti podataka* 2.0, od 20.10.2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (19. 12. 2023.).

41 *Cf.* Huth, D.; Matthes, F., *"Appropriate Technical and Organizational Measures": Identifying Privacy Engineering Approaches to Meet GDPR Requirements*, Technical University Munich, 25th Americas Conference on Information Systems, Cancun, 2019., https://wwwmatthes.in.tum.de/file/14qun4klf0r0d/Sebis-Public-Website/-/Appropriate-Technical-and-Organizational-Measures-Identifying-Privacy-Engineering-Approaches-to-Meet-GDPR-Requirements/Huth%20AMCIS2019.pdf (17. 1. 2024.); Selzer, A., *The Appropriateness of Technical and Organisational Measures under Article 32 GDPR*, European Data Protection Law Review, *vol*. 7, br. 1, 2021., https://edpl.lexxion.eu/article/EDPL/2021/1/16 (18. 1. 2024.).

pristupa isključivo autoriziranim osobama, zaštitu od prirodnih katastrofa i slučajnih događaja te ispravno održavanje. Druga skupina tehničkih i organizacijskih mjera ima za cilj osigurati kontrolu pristupa sustavima. To podrazumijeva implementaciju onih mjera kojima se pristup informacijskim sustavima ograničava na autorizirane osobe (ili izvršitelje) te je dozvoljen isključivo u svrhu izvršavanja dodijeljene funkcije u obradi osobnih podataka. Pritom je nužno osigurati da svi autorizirani korisnici pristupaju sustavu s pomoću jedinstvenog identifikatora i lozinkama kojih su kompleksnost i promjena unaprijed određene. Također, nužno je uspostaviti mjere koje strogo ograničavaju potpuni administratorski pristup, te koje omogućavaju bilježenje svakog pristupa sustavu od strane korisnika kao i mogućnost deaktiviranja korisničkih računa. Treća skupina tehničkih i organizacijskih mjera ima za cilj osigurati da pristup određenoj kategoriji podataka imaju samo autorizirani korisnici kojima je pristup potreban za izvršavanje njihove funkcije u obradi osobnih podataka. Mjere kojima se navedeni cilj postiže mogu uključivati ograničavanje pristupa podacima na temelju "need to know" osnove, tj. omogućavanje pristupa samo onim podacima koji su potrebni za izvršavanje funkcije, što se postiže upravljanjem pravima pristupa, bilježenjem pristupa te rješavanjem dozvola i sigurnosti u slučajevima udaljenog pristupa sustavima. Četvrta skupina tehničkih i organizacijskih mjera odnosi se na prijenos, pohranu i uništavanje podataka. Cilj je njihove primjene osigurati da osobni podaci ispitanika nisu otkriveni, izmijenjeni ili obrisani od neautorizirane strane tijekom prijenosa ili pohrane. Mjere koje se u tu svrhu implementiraju mogu uključivati uporabu sigurnosnih protokola za pristup i prijenos podataka, korištenje enkripcije u prijenosu podataka i pravodobno brisanje podataka. Peta skupina tehničkih i organizacijskih mjera odnosi se na povjerljivost i cjelovitost osobnih podataka cilj implementacije koje je osigurati da podaci ostanu povjerljivi, neizmijenjeni i cjeloviti tijekom njihove obrade. Mjere koje se pritom primjenjuju mogu uključivati prethodnu provjeru zaposlenika i osoba koje sudjeluju u obradi osobnih podataka i imaju pristup podacima, primjenu integrirane zaštite osobnih podataka, osiguranje pristupa izvornom kodu sustava koji se rabi za obradu osobnih podataka isključivo autoriziranim osobama, testiranje sigurnosti sustava koje uključuje reviziju izvornog koda, provođenje redovitih testova mogućnosti proboja sustava te korištenje propisanih standarda prigodom uporabe kriptografije i kriptografskih funkcionalnosti. Šesta skupina tehničkih i organizacijskih mjera ima za cilj osigurati dostupnost podataka, tj. osigurati da su podaci zaštićeni od slučajnog uništavanja ili gubitka te da postoje procedure vraćanja podataka u slučaju incidenta. Mjere koje je u tu svrhu moguće implementirati mogu biti pravodobna izrada sigurnosnih kopija, zaštita informacijskih sustava od slučajnih događaja ili nepogoda, osiguravanje višestrukog pristupa te pohrana podataka na fizič-

ki odvojenim lokacijama. Konačno, sedma skupna tehničkih i organizacijskih mjera podrazumijeva upravljanje incidentima. Glavni je cilj njihove primjene osigurati da se u slučaju povrede osobnih podataka minimiziraju efekti povrede te se pravodobno informira nadležno tijelo i prema potrebi ispitanike. Mjere koje se u tu svrhu implementiraju mogu uključivati uspostavu ažurnog plana za postupanje u slučaju incidenata koji podrazumijeva određivanje odgovornosti za postupanje u slučaju incidenta, kontinuiranu procjenu informacijske sigurnosti, klasifikaciju incidenata s obzirom na utjecaj na prava i slobode ispitanika, utvrđivanje jasnog plana za postupanje i provođenje potrebnih procedura te konačno periodično testiranje uspostavljenog plana za postupanje u slučaju incidenta.

Navedena klasifikacija tehničkih i organizacijskih mjera ne predstavlja konačan popis mogućih mjera te je, s obzirom na način i sredstva pojedine obrade osobnih podataka ali i s obzirom na budući razvoj tehnologije, moguće uključivanje i provedba i drugih mjera kojima se može postići odgovarajuća i učinkovita zaštita osobnih podataka.[42]

3.2. Tehnička i integrirana zaštita podataka

Za razliku od čl. 24. Uredbe koji nameće voditelju obrade općenitu obvezu implementacije odgovarajućih tehničkih i organizacijskih mjera u svrhu ispunjenja i dokazivosti načela odgovornosti, te čl. 32. koji voditelju i izvršitelju propisuje implementaciju odgovarajućih tehničkih i organizacijskih mjera u svrhu postizanja odgovarajuće razine sigurnosti podataka u odnosu na rizik, tehnička i integrirana zaštita podataka podrazumijeva implementaciju odgovarajućih tehničkih i organizacijskih mjera u svrhu učinkovitog ispunjenja svih načela obrade osobnih podataka predviđenih Uredbom te obradu samo onih podataka koji su nužni za ispunjenje svake posebne svrhe obrade.

U pogledu tehničke zaštite čl. 25. st. 1. Uredbe nalaže voditelju obrade da u vrijeme kada određuje sredstva obrade i tijekom trajanja same obrade osobnih podataka provodi odgovarajuće tehničke i organizacijske mjere kako bi primjena predviđenih načela zaštite podataka bila učinkovita te kako bi se zaštitila prava ispitanika zajamčena Uredbom. U primjeni odgovarajućih tehničkih i organizacijskih mjera mora se voditi računa o najnovijim dostignućima u tehničkom i organizacijskom smislu, trošku implementacije, prirodi, opsegu, kontekstu i svrsi obrade te rizicima za prava i slobode ispitanika. Primjena

[42] Commission Nationale Informatique Libertes (CNIL), *Security of personal data, CNIL's Guide 2018*, https://www.cnil.fr/sites/cnil/files/atoms/files/guide_security-personal-data_en.pdf (19. 1. 2024.).

najnovijih tehničkih dostignuća ovdje podrazumijeva kontinuirano praćenje napretka tehnologije te njezine primjene u obradi osobnih podataka kako bi se na odgovarajući i učinkovit način osigurala provedba načela obrade i zaštitila zajamčena prava ispitanika u obradi. Pritom je svakako potrebno voditi računa i o trošku implementacije, koji uključuje utrošena financijska sredstva, utrošeno vrijeme i ljudske resurse a koji treba biti proporcionalan s obzirom na rizike za prava i slobode ispitanika. Priroda obrade odnosi se na specifične značajke obrade, tj. na to obrađuju li se primjerice posebne kategorije osobnih podataka, podrazumijeva li obrada profiliranje ili automatsko odlučivanje i slično. Opseg obrade ovdje uzima u obzir količinu podataka i broj ispitanika koje obrada obuhvaća, dok kontekst obrade uzima u obzir sve specifične okolnosti obrade. Konačno, svrha uzima u obzir koji se cilj želi ostvariti samom obradom osobnih podataka.

Integrirana zaštita podataka odnosi se na ograničavanje obrade na one osobne podatke koji su nužni za postizanje svrhe obrade. Članak 25. st. 2. nalaže da voditelj obrade implementira odgovarajuće tehničke i organizacijske mjere kojima se omogućava da na integrirani način budu obrađeni samo oni podaci koji su nužni za svaku posebnu svrhu. Ta se obveza primjenjuje na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost. Točnije, takvim se mjerama osigurava da osobni podaci nisu automatski, bez intervencije pojedinca, dostupni neograničenom broju pojedinaca. Ovdje se pojam "integriran" rabi kao prijevod pojma "by default" koji se koristi u engleskom tekstu Uredbe, te djelomično može upućivati na pogrešan zaključak oko implementacije odgovarajućih tehničkih i organizacijskih mjera. Naime, definicija pojam "integriranog" na hrvatskom jeziku upućuje na spajanje više elemenata skupa u jedan skup ili proces kojim se dopunjuje ili stvara neka cjelina[43] dok engleski pojam "by default" podrazumijeva postojeće ili unaprijed zadane vrijednosti koje se mogu mijenjati.[44] Budući da implementacija odgovarajućih tehničkih i organizacijskih mjera podrazumijeva implementaciju različitih mjera u obradi osobnih podataka (v. više *infra* o sedam skupina tehničkih i organizacijskih mjera), jasno je da one u konačnici moraju biti komplementarne te djelovati kao cjelina, ali ujedno moraju biti unaprijed zadane. Tako se u kontekstu obrade osobnih podataka pojam "integrirano" treba tumačiti u širem smislu, tj. kao pojam koji se odnosi i na zadanu obvezu odabira onih tehničkih i organizacijskih mjera koje će u obradi osobnih podataka unaprijed

[43] Hrvatska enciklopedija, definicija pojma "integracija", https://www.enciklopedija.hr/clanak/integracija (20. 1. 2024.).

[44] Cambridge dictionary, definicija pojma "by default", https://dictionary.cambridge.org/dictionary/english/default (21. 1. 2024.).

jamčiti da se provodi samo obrada koja je izričito nužna za ispunjenje svrhe, a da će se pritom prikupljati samo oni podaci koji su nužno potrebni za obradu i ispunjenje svrhe, te da će se pohranjivati onoliko dugo koliko je to nužno za potrebe obrade.[45] Pritom je također bitno voditi računa o dostupnosti osobnih podataka, te implementirati odgovarajuće i učinkovite tehničke i organizacijske mjere kojima će se pristup podacima ograničiti samo na one osobe kojima je to potrebno za ispunjavanje funkcije.

Budući da je načelo odgovornosti sveobuhvatno te podrazumijeva da voditelj obrade prigodom odabira odgovarajućih i učinkovitih mjera bude odgovoran, to svakako podrazumijeva i implementaciju svih mjera koje se odnose na tehničku i integriranu zaštitu podataka. Tako je potrebno u svim fazama obrade osobnih podataka, uključujući i pripremnu fazu kao što je osmišljavanje postupka obrade, utvrđivanje svrhe i sredstva obrade te daljnji razvoj obrade, održavanje sustava, pohrana podataka, angažiranje izvršitelja i brisanja podataka, voditi računa o različitim tehničkim i organizacijskim mjerama koje će na odgovarajući i učinkovit način osigurati da su ispunjena sva načela obrade osobnih podataka te da je obrada ograničena na nužne podatke, tj. da su ispunjeni zahtjevi tehničke i integrirane zaštite podataka prema čl. 25. Uredbe.

Ako tehničku i integriranu zaštitu osobnih podataka razmatramo na razini pojedinog načela, možemo kao primjer navesti neke od odgovarajućih i učinkovitih tehničkih i organizacijskih mjera, a koje se spominju u Smjernicama Europskog odbora za zaštitu podataka br. 04/2019, kako bi pojedino načelo bilo zadovoljeno. Tako se načelo transparentnosti koje nalaže da se ispitanika jasno mora obavijestit o tome kako se prikupljaju, obrađuju i prenose podaci te koja je svrha obrade može ispuniti implementacijom onih mjera koje omogućuju da su informacije lako dostupne, relevantne i razumljive te da se dostavljaju različitim komunikacijskim kanalima.[46] U pogledu ispunjavanja zahtjeva koje nameće načelo zakonitosti koje se odnosi na utvrđivanje valjane pravne osnove za obradu osobnih podataka, neke od odgovarajućih i učinkovitih mjera mogu biti: jasno utvrđivanje određene svrhe i pravnog temelja koji se razlikuju za svaku pojedinu aktivnost obrade koju provodi voditelj; uspostavljanje mjera koje omogućavaju dobivanje i povlačenje privole u skladu s Uredbom; prigodom uporabe legitimnog interesa kao pravnog temelja za obradu osobnih podataka utvrđivanje mjera za provođenje i dostupnost testa legitimnog interesa.[47] Za ispunjavanje načela poštenosti koje zahtijeva da se osobni podaci ne obrađuju na način koji je štetan, neočekivan ili obmanjujući za ispitanike potrebno je na

[45] EDPB smjernice 4/2019, *op. cit.* bilj. 40, str. 12.
[46] *Cf. ibid.*, str. 15.
[47] *Cf. ibid*., str. 16.

primjer implementirati odgovarajuće i učinkovite mjere koje će omogućiti ispitanicima da imaju mogućnost odlučivati o uporabi njihovih osobnih podataka, uspostaviti mjere koje će omogućiti da ispitanici mogu komunicirati s voditeljem obrade, da se obrada provodi u skladu s očekivanjima ispitanika, da se uspostavi mogućnost prigovora automatiziranoj obradi osobnih podataka ili da se rabe algoritmi u obradi osobnih podataka koji su pod ljudskim nadzorom.[48] Odgovarajuće i učinkovite mjere koje pridonose ispunjavanju načela ograničenja svrhe mogu podrazumijevati utvrđivanje posebne i izričite svrhe prije početka same obrade, utvrđivanje nužnih podataka koji su potrebni za ispunjenje svrhe, ograničenje daljnje obrade podataka u svrhe koje nisu usklađene s prvotnom svrhom te ograničenje ponovne uporabe podataka.[49] Implementacija mjera koje imaju za cilj ispunjavanje načela smanjenja količine podataka koje nalaže da se obrađuju samo oni podaci koji su primjereni, relevantni i ograničeni na ono što je nužno za ostvarenje svrhe obrade mogu biti: ograničavanje količine podataka koji se prikupljaju i obrađuju, ograničavanje pristupa podacima, prikupljanje nužnih i relevantnih podataka za ispunjenje svrhe, pseudonimizacija, anonimizacija i brisanje podataka.[50] Načelo točnosti podataka može se ispuniti implementacijom odgovarajućih mjera koje jamče da su podaci ažurni, pouzdanošću izvora podataka, periodičnom provjerom podataka, ispravljanjem podataka, omogućavanjem pristupa ispitanicima i slično.[51] Za ispunjavanje načela ograničenja pohrane voditelji obrade moraju implementirati odgovarajuće i učinkovite mjere koje jamče da se podaci čuvaju u obliku koji omogućuje identifikaciju ispitanika onoliko dugo koliko je potrebno za ispunjenje svrhe, a to mogu biti mjere poput pravodobnog i učinkovitog brisanja ili anonimizacije podataka, utvrđivanja jasnih kriterija pohrane i zadržavanja podataka, sigurnosti podataka, izrade sigurnosnih kopija i slično.[52] Konačno, za ispunjavanje načela cjelovitosti i povjerljivosti koje predviđa zaštitu od neovlaštene ili nezakonite obrade, gubitka, uništenja ili oštećenja podataka te ostvarenje sigurnosti podataka mjere koje se mogu implementirati mogu uključivati: upravljanje informacijskom sigurnošću na učinkovit način, procjenu rizika za sustave i sigurnost podataka, redovito održavanje sustava, upravljanje kontrolom pristupa podacima, sigurnosne pohrane i prijenosi podataka, pseudonimizacija podataka te odgovarajuće mjere koje predviđaju upravljanje i odgovornosti u slučaju povrede tajnosti i cjelovitosti podataka.[53]

48 *Cf. ibid*., str. 17.
49 *Cf. ibid*., str. 19.
50 *Cf. ibid*., str. 20.
51 *Cf. ibid*., str. 23.
52 *Cf. ibid.*, str. 25.
53 *Cf. ibid*., str. 26.

Neovisno o načinu i vrsti mjera koje se implementiraju u samu obradu osobnih podataka u skladu s načelom odgovornosti, njihovu adekvatnost te osobito učinkovitost voditelj obrade mora biti u mogućnosti i dokazati, u protivnom može snositi odgovornost za neispunjavanje zahtjeva Uredbe, ali i građanskopravnu odgovornost prema čl. 82. Uredbe u slučaju povrede prava ispitanika i nastale štete za ispitanika, što razmatramo u sljedećem poglavlju.

3.3. Implementacija tehničkih i organizacijskih mjera i odgovornost za štetu

Načelo odgovornosti pretpostavlja implementaciju odgovarajućih tehničkih i organizacijskih mjera. Kao što je prethodno navedeno čl. 24. Uredbe u pogledu usklađenosti ponašanja voditelja obrade sa zahtjevima Uredbe, čl. 25. Uredbe u pogledu ispunjavanja svih načela Uredbe i ograničenja obrade nužnih podataka za ispunjenje svrhe te čl. 32. Uredbe u pogledu sigurnosti podataka nalažu odabir i implementaciju odgovarajućih i učinkovitih tehničkih i organizacijskih mjera odgovornim subjektima bez jasnog navođenja koje mjere su prikladne za pojedini postupak u obradi osobnih podataka. Tako je odgovornim subjektima ostavljeno da s obzirom na prirodu, opseg, kontekst i svrhu obrade samostalno odaberu odgovarajuće tehničke i organizacijske mjere. Stoga se nameće pitanje: treba li, kada dođe do povrede osobnih podataka od treće strane, presumirati odgovornost odgovornog subjekta zbog odabira neodgovarajućih tehničkih i organizacijskih mjera?

Navedeno pitanje razmatrano je i pred Sudom Europske unije (dalje u tekstu: SEU) u predmetu br. 340/21[54] u kojem se razmatraju prethodna pitanja koja se odnose na tumačenje čl. 5. st. 2., čl. 24., čl. 32. i čl. 82. Uredbe, a u vezi s implementacijom načela odgovornosti, odgovarajućih tehničkih i organizacijskih mjera i naknadom nematerijalne štete pretrpljene zbog nepoštovanja zakonskih obveza voditelja obrade osobnih podataka. U navedenom predmetu došlo je do povrede osobnih podataka šest milijuna ispitanika kao posljedica neovlaštenog pristupa (kibernetičkog napada) na informacijski sustav Nacionalne agencije za javne prihode u Bugarskoj, nakon čega su slijedile tužbe za naknadu nematerijalne štete koja je navodno nastala zbog otkrivanja osobnih podataka. Upravni sud u Bugarskoj odbio je tužbene zahtjeve dok je Vrhovni upravni sud u Bugarskoj na temelju žalbe odlučio prekinuti postupak te SEU-u uputiti nekoliko prethodnih pitanja za razmatranje i odlučivanje. Prvo, temeljno prethodno pitanje koje se u navedenom predmetu postavlja jest treba li

[54] Sud Europske unije, predmet br. 340/21, VB v. Nacionalna agencija za javne prihode, Bugarska, presuda 19. 1. 2024.

čl. 24. i 32. Uredbe tumačiti na način da su same činjenice da je treća strana neovlašteno otkrila osobne podatke ili im je neovlašteno pristupila dostatne za zaključak da tehničke i organizacijske mjere koje je proveo voditelj obrade o kojem je riječ nisu bile "odgovarajuće" u smislu čl. 24. i 32. Uredbe. SEU je zauzeo stajalište da čl. 24. i 32. Uredbe treba tumačiti na način da same činjenice da je treća strana u smislu čl. 4. t. 10. Uredbe neovlašteno otkrila osobne podatke ili im je neovlašteno pristupila nisu dostatne za zaključak da tehničke i organizacijske mjere koje je proveo voditelj obrade o kojem je riječ nisu bile "odgovarajuće" u smislu čl. 24. i 32. Naime, u svom obrazloženju SEU navodi da je, razmatrajući kontekstualne i teleološke elemente[55] navedenih odredbi Uredbe jasno da iz njih proizlazi da same odredbe nameću voditelju obrade obvezu donošenja tehničkih i organizacijskih mjera kojih je cilj izbjegavanje u najvećoj mogućoj mjeri bilo kakve povrede osobnih podataka. Jesu li takve mjere odgovarajuće, treba procijeniti konkretno, ispitivanjem je li voditelj proveo te mjere, uzimajući u obzir različite kriterije sadržane u navedenim člancima i potrebe zaštite podataka koje su posebno svojstvene obradi o kojoj je riječ te njome prouzročene rizike.[56] Stoga se odredbe ne mogu tumačiti na način da su činjenice da je treća strana neovlašteno otkrila osobne podatke ili im je neovlašteno pristupila dostatne za zaključak da mjere koje je proveo voditelj obrade o kojem je riječ nisu bile odgovarajuće u smislu tih odredaba, a da mu se pritom ni ne dopusti podnošenje dokaza o suprotnome.[57] Štoviše, SEU jasno naglašava i obvezu dokazivanja voditelja obrade o implementaciji načela odgovornosti, a što proizlazi iz razmatranih odredbi, tj. čl. 5. st. 2., čl. 24. i 32. Uredbe, te navodi da takva obveza dokazivanja da su te mjere odgovarajuće ne bi imala smisla kada bi voditelj obrade imao obvezu spriječiti svaku povredu navedenih podataka.[58] Budući da je na prvo pitanje odgovor SEU-a negativan, tj. da neovlašteni pristup podacima trećih strana ne presumira odgovornost voditelja obrade za primjenu neodgovarajućih mjera, sud je razmatrao daljnja pitanja. Drugo postavljeno pitanje vezano je uz čl. 32. Uredbe i sigurnosti podataka te se njime traži tumačenje na koji način sudovi moraju konkretno ocijeniti jesu li tehničke i organizacijske mjere koje provodi voditelj obrade na temelju tog članka odgovarajuće, osobito uzimajući u obzir rizike u vezi s obradom o kojoj je riječ. SEU tako navodi da je primjenu čl. 32. st. 1 i st. 2., tj. jesu li tehničke i organizacijske mjere odgovarajuće, potrebno ocijeniti u dva koraka. S jedne strane, valja identificirati rizike od povrede osobnih podataka koje podrazumi-

[55] *Ibid.*, t. 33.
[56] *Ibid.*, t. 30.
[57] *Ibid*., t. 31.
[58] *Ibid*., t. 34.

jeva obrada o kojoj je riječ i njezine eventualne posljedice za prava i slobode pojedinaca. Tu ocjenu treba provesti konkretno, uzimajući u obzir razinu vjerojatnosti identificiranih rizika i njihovu razinu ozbiljnosti. S druge strane, valja provjeriti jesu li mjere koje je proveo voditelj obrade prilagođene tim rizicima, uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade o kojoj je riječ.[59] Pritom iako voditelj obrade raspolaže određenim diskrecijskim pravom u određivanju odgovarajućih mjera kako bi se osigurala zadovoljavajuća razina sigurnosti s obzirom na rizik, nacionalni sudovi moraju konkretno ocijeniti jesu li tehničke i organizacijske mjere koje provodi voditelj obrade na temelju tog članka odgovarajuće, uzimajući u obzir rizike u vezi s obradom o kojoj je riječ i ocjenom toga jesu li priroda, sadržaj i provedba tih mjera prilagođeni tim rizicima.[60]

Ostala pitanja koja se postavljaju u navedenom predmetu odnose se na teret dokazivanja, dokazna sredstva te moguću odgovornost za nematerijalnu štetu prema čl. 82. Uredbe, a koja je nastupila ili može nastupiti kao posljedica primjene tehničkih i organizacijskih mjera od strane voditelja obrade. Tako se trećim pitanjem traži tumačenje na kome je teret dokazivanja da su implementirane sigurnosne mjere na temelju čl. 32. Uredbe bile odgovarajuće. SEU je zauzeo stajalište da je u okviru tužbe za naknadu štete koja se temelji na čl. 82. Uredbe teret dokazivanja toga da su implementirane odgovarajuće sigurnosne mjere na voditelju obrade.[61] Nadalje, u pogledu dokaznih sredstava SEU je zauzeo stajalište da nalaz i mišljenje sudskog vještaka ne predstavljaju sustavno nužno i dostatno dokazno sredstvo jer bi takvo tumačenje moglo značiti povredu načela djelotvornosti sudova i ograničiti nacionalne sudove u njihovu odlučivanju te utjecati na objektivnu ocjenu suda i pravo na učinkovit sudski pravni lijek.[62] Također, zauzeto je stajalište da sama činjenica da je treća strana neovlašteno pristupila i otkrila osobne podatke ne oslobađa voditelja obrade od obveze naknade štete prema čl. 82. Uredbe, nego u tom slučaju voditelj obrade mora dokazati da ni na koji način nije odgovoran za događaj koji je prouzročio štetu o kojoj je riječ[63], tj. da je implementirao sve odgovarajuće tehničke i organizacijske mjere u obradi osobnih podataka uzevši u obzir prirodu, kontekst, opseg, rizik i svrhu obrade. Konačno, zadnje pitanje koje je SEU u navedenom predmetu razmatrao jest može li bojazan ispitanika da će njegovi osobni podaci biti zlorabljeni od treće strane, kao posljedica povrede Uredbe, sama po sebi

[59] *Ibid*., t. 42.
[60] *Ibid*., t. 47.
[61] *Ibid*., t. 57.
[62] *Ibid*., t. 64.
[63] *Ibid*., t. 74.

predstavljati nematerijalnu štetu, na što SEU odgovara potvrdno[64], pri čemu nacionalni sudovi pred kojima se vodi postupak moraju provjeriti može li se ta bojazan smatrati osnovanom u posebnim okolnostima i s obzirom na ispitanika te pojam "nematerijalne štete" u smislu čl. 82. st. 1. Uredbe trebaju tumačiti u širem smislu, što uključuje i bojazan da će osobni podaci biti zlorabljeni u budućnosti.[65]

Iako je u navedenom predmetu SEU zauzeo stajališta koja se odnose na postupanje nacionalnih sudova kada je u pitanju implementacija odgovarajućih tehničkih i organizacijskih mjera, dokazivanje njihove adekvatnosti i učinkovitosti te odgovornosti za štetu, navedena će odluka svakako znatno utjecati i na postupanje neovisnih nadzornih tijela.[66] Naime, prigodom utvrđivanja o povredama odredaba Uredbe te izricanja upravnih novčanih kazni, neovisna nadzorna tijela svakako moraju uzeti u obzir zauzeta stajališta SEU-a, posebice ona koja se odnose na potpunu implementaciju načela odgovornosti, tj. implementaciju odgovarajućih tehničkih i organizacijskih mjera, teret dokazivanja adekvatnosti i učinkovitosti mjera te mogućnosti ekskulpacije od odgovornosti na temelju činjenice da je šteta nastupila zbog djelovanja treće strane.

3.4. Izričiti organizacijski zahtjevi i izuzeće od primjene

Kako bi odgovorni subjekti ispunili zahtjeve koje nameće načelo odgovornosti, osim gore spomenutih odgovarajućih i učinkovitih tehničkih i organizacijskih mjera i odgovarajućih politika, obrada osobnih podataka mora biti usklađena i sa svim zahtjevima koje Uredba izrijekom navodi.[67] Za razliku od tehničkih i organizacijskih mjera koje nisu izrijekom navedene te njihov odabir i primjena ovisi o prirodi, opsegu, kontekstu, riziku za prava pojedinca i svrsi obrade, implementacija izričitih organizacijskih zahtjeva je jasno utvrđena Uredbom te je njihova implementacija obvezna kako bi obrada bila u cijelosti usklađena sa zahtjevima Uredbe. Izričite organizacijske zahtjeve možemo klasificirati kao učinkovite organizacijske mjere a u njih ubrajamo mjere poduzete za učinkovito pružanje informacija o obradi (čl. 13. i 14. Uredbe), uspostava i vođenje evidencije aktivnosti obrade (čl. 30. Uredbe), provođenje postupka

64 *Ibid*., t. 86.

65 *Ibid*., t. 81.

66 *Cf.* Kosta, E., *Security of Processing and Data Breach Notification*, European Data Protection Board, 2023., str. 7, https://www.edpb.europa.eu/system/files/2024-01/one_stop_shop_case_digest_security_data_breach_en.pdf (22. 1. 2024.).

67 Voigt, P.; Von dem Bussche, A., *The EU General Data Protection Regulation (GDPR) - A Practical Guide*, Springer International Publishing AG, Cham, 2017., str. 31.

procjene učinka na zaštitu podataka (čl. 35. Uredbe), imenovanje službenika za zaštitu osobnih podataka (čl. 37. Uredbe), obvezu izvješćivanja nadzornog tijela i ispitanika o povredi osobnih podataka (čl. 33. i 34. Uredbe), mjere koje omogućavaju poštovanje odobrenih kodeksa ponašanja (čl. 40. Uredbe) te uređivanje odnosa između voditelja i izvršitelja obrade pravno obvezujućim aktom (čl. 28. Uredbe). Za svaki od navedenih zahtjeva jasno je propisan način njegove implementacije, dok se za pojedine zahtjeve previđa izuzeće od primjene za pojedine voditelje obrade i vrste obrada osobnih podatka. Tako je u pogledu zahtjeva kojim se nameće obveza vođenja evidencije aktivnosti obrade predviđeno izuzeće u slučaju ako je riječ o poduzeću ili organizaciji u kojoj je zaposleno manje od 250 osoba, osim ako će obrada koju provodi vjerojatno prouzročiti visok rizik za prava i slobode ispitanika, ako obrada nije povremena ili obrada uključuje posebne kategorije podataka iz čl. 9. st. 1. ili je riječ o osobnim podacima u vezi s kaznenim osudama i kažnjivim djelima iz čl. 10.[68] Iako je navedeno izuzeće od obveze vođenja evidencije aktivnosti obrade postavljeno vrlo široko, rijetka je situacija da se prema tumačenju WP29 obrada osobnih podataka provodi povremeno (jednom ili dva puta na godinu bez trajne pohrane),[69] tako da je navedeni zahtjev vođenja evidencije aktivnosti obrade, unatoč navedenom izuzeću, obveza gotovo svih koji vrše obradu osobnih podataka. Nadalje, provođenje postupka procjene učinka na zaštitu podataka nije obvezno za svaku vrstu obrade osobnih podataka, nego samo u slučajevima ako je vjerojatno da će neka vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca,[70] te u slučajevima kada je neovisno nadzorno tijelo za pojedine vrste obrade utvrdilo da je provedba postupka procjene učinka na zaštitu podataka obvezna.[71] U pogledu zahtjeva za imenovanje službenika za zaštitu osobnih podataka obveza postoji samo ako obradu provodi tijelo javne vlasti ili javno tijelo (izuzev sudova), ako se osnovne djelatnosti voditelja obra-

68 Čl. 30. st. 5. Uredbe.

69 Radna skupina prema čl. 29. za zaštitu podataka (WP29), *Tumačenje WP29 o izuzeću od primjene obveze vođenja evidencije aktivnosti obrade prema čl. 30(5) Opće uredbe o zaštiti podataka* od 19. 4. 2018, https://ec.europa.eu/newsroom/article29/items/624045 (27. 1. 2024.).

70 Čl. 35. st. 1. Uredbe.

71 Hrvatsko neovisno nadzorno tijelo – Agencija za zaštitu osobnih podataka Odlukom o uspostavi i javnoj objavi popisa vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka od 21. prosinca 2018. utvrdilo je popis obrada za koje je uvijek obvezno provesti postupak procjene učinka na zaštitu osobnih podataka, https://azop.hr/odluka-o-uspostavi-i-javnoj-objavi-popisa-vrsta-postupaka-obrade-koje-podlijezu-zahtjevu-za-procjenu-ucinka-na-zastitu-podataka/ (28. 1. 2024.).

de ili izvršitelja obrade sastoje se od postupaka obrade koji zbog svoje prirode, opsega i/ili svrha iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri, ili ako se osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od opsežne obrade posebnih kategorija podataka na temelju čl. 9. Uredbe i osobnih podataka u vezi s kaznenim osudama i kažnjivim djelima iz čl. 10. Uredbe.[72] Kada je riječ o zahtjevu koji nameće obvezu izvješćivanja nadzornog tijela ili ispitanika o povredi osobnih podataka, u slučaju kada dođe do povrede osobnih podataka koja može prouzročiti rizik za prava i slobode pojedinca, voditelj mora obavijestiti nadzorno tijelo o povredi u roku od 72 sata od saznanja o povredi[73], dok ako postoji vjerojatnost da će povreda prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade bez nepotrebnog odgađanja mora obavijestiti i ispitanika o povredi osobnih podataka.[74] Konačno, sve mjere koje nameću poštovanje dodatnih obveza utvrđenih Odobrenim kodeksima ponašanja pretpostavljaju da su za potrebe pojedinih sektora, udruženja ili mikro, malih i srednjih poduzeća kodeksi ponašanja koji su namijenjeni pružanju doprinosa ispravnoj primjeni Uredbe i usvojeni.

4. ZAKLJUČAK

Načelo odgovornosti, ili "accountability", ključno je u zaštiti osobnih podataka jer zahtijeva od voditelja obrade ne samo da poštuju zakonske obveze već i da mogu dokazati usklađenost s načelima obrade podataka. Uvođenje ovog načela u zakonodavstvo EU-a putem Opće uredbe o zaštiti podataka (GDPR) odraz je šireg trenda prema jačanju pravnih obveza i odgovornosti subjekata koji obrađuju osobne podatke.[75] Ovo je posebice važno u kontekstu "poplave podataka" uzrokovane brzim razvojem tehnologija i povećanjem količine obrađenih osobnih podataka, što povećava rizik od povreda podataka. Načelo odgovornosti stoga pomaže u premošćivanju jaza između teorijskih pravila i njihove praktične primjene, pružajući regulatornim tijelima snažniji okvir za nadzor i osiguravajući da odgovorni subjekti aktivno provode mjere zaštite podataka. Ovom promjenom EU nastoji ojačati povjerenje i reputaciju u javnom i privatnom sektoru, ističući važnost transparentnosti i odgovornosti u obradi osobnih podataka. Engleski pojam "accountability" koji se rabi u izvornom tekstu Uredbe obuhvaća odgovornost subjekta za svoje postupke i obvezu do-

72 Čl. 37. st. 1. Uredbe.
73 Čl. 33. st. 1. Uredbe.
74 Čl. 34. st. 1. Uredbe.
75 Boros, A., *The Accountability Principle in Personal Data Processing*, Jurnalul Baroului Cluj, *vol*. 39, br. 2, 2021, str. 39 – 54.

kazivanja usklađenosti s nametnutim obvezama. Razlikuje se od pojma "responsibility", koji se odnosi na dužnosti proizašle iz položaja ili funkcije subjekta. U kontekstu obrade osobnih podataka, načelo odgovornosti zahtijeva od subjekata da uspostave mjere koje osiguravaju poštovanje zakonskih načela, transparentno postupanje i spremnost na ispravljanje propusta. Pogrešan prijevod pojma "accountability" kao "pouzdanost" u hrvatskom prijevodu Uredbe upućuje na važnost preciznosti u pravnom jeziku kako bi se osigurala pravilna primjena i razumijevanje zakonskih obveza. Načelo odgovornosti stoga predstavlja ključni element u zaštiti osobnih podataka, potičući odgovorne subjekte na aktivno provođenje i dokazivanje usklađenosti s pravilima zaštite podataka.

Primarna odgovornost postupanja u skladu s načelom odgovornosti jest na odgovornim subjektima. Oni pak, bilo da su voditelji ili izvršitelji obrade, moraju biti upoznati s obvezama i načelima obrade podataka kako bi osigurali zakonitost obrade i zaštitu prava ispitanika. Načelo odgovornosti također zahtijeva od subjekata da implementiraju odgovarajuće mjere za usklađivanje s Uredbom i da mogu dokazati usklađenost s njezinim zahtjevima. Razlikovanje uloga voditelja i izvršitelja obrade ključno je za ispunjavanje ovih obveza, a njihova stvarna funkcija u obradi podataka određuje njihovu odgovornost, neovisno o formalnom imenovanju. Implementacija i dokazivanje učinkovitih mjera zaštite osobnih podataka temelj su zaštite prava ispitanika i sprečavanja zlouporaba, čime se osigurava integritet zakonodavnog okvira za zaštitu osobnih podataka. Također, implementacija odgovarajućih i učinkovitih mjera ključna je za usklađivanje obrade osobnih podataka s Uredbom i načelom odgovornosti. Adekvatnost mjera odnosi se na njihovu sposobnost da postignu ciljeve zaštite podataka, dok učinkovitost mjera znači njihovu učinkovitost u zaštiti prava ispitanika. Ove mjere moraju biti proporcionalne vrsti obrade, kategoriji podataka i razini rizika. Usklađenost s Uredbom ne ovisi o veličini ili organizaciji odgovornog subjekta, već o prirodi obrade podataka. Odgovorni subjekti moraju biti spremni dokazati primjenu ovih mjera kako bi se osigurala zaštita prava ispitanika i izbjegle povrede osobnih podataka.

Članak 24. Opće uredbe o zaštiti podataka (GDPR) postavlja temelje za načelo odgovornosti, zahtijevajući od voditelja obrade da implementira odgovarajuće tehničke i organizacijske mjere kako bi osigurao usklađenost obrade osobnih podataka s Uredbom.[76] Ove mjere moraju se redovito preispitivati i ažurirati kako bi se prilagodile promjenama u obradi podataka. Ured-

[76] Cortina, S.; Picard, M.; Renault, S.; Valoggia, P., *Towards a Process-Based Approach to Compliance with GDPR*, u: Yilmaz, M.; Clarke, P.; Messnarz, R.; Reiner, M. (ur.), *Systems, Software and Services Process Improvement, EuroSPI 2021, Communications in Computer and Information Science*, Springer, Cham, 2021.

ba također predviđa sustavne politike zaštite podataka koje obuhvaćaju širok spektar aktivnosti, od imenovanja službenika za zaštitu podataka do uspostave transparentnosti i mehanizama za djelovanje u slučaju povrede podataka. Iako je primarna odgovornost na voditelju obrade, izvršitelji obrade također su dužni provoditi mjere za osiguranje sigurnosti obrade. Implementacija tehničkih i organizacijskih mjera, kao što su pseudonimizacija i enkripcija, ključna je za zaštitu podataka i usklađenost s načelom odgovornosti prema GDPR-u. Nadalje, osim implementacije tehničkih i organizacijskih mjera radi ispunjavanja načela odgovornosti i sigurnosti podataka, čl. 25. Uredbe dalje razrađuje ovu obvezu, naglašavajući potrebu za primjenom najnovijih tehničkih dostignuća i proporcionalnost troškova implementacije. Integrirana zaštita podataka, kako je navedeno u čl. 25. st. 2., odnosi se na obradu samo onih podataka koji su nužni za svrhu obrade, ograničavajući pristup podacima na ono što je neophodno. Ovaj pristup "po defaultu" osigurava da se mjere zaštite podataka automatski primjenjuju u svim fazama obrade, čime se štite prava ispitanika i osigurava usklađenost s GDPR-om. Konačno, za cjelovitu usklađenost s GDPR-om, voditelji obrade moraju implementirati ne samo odgovarajuće tehničke i organizacijske mjere već i osigurati da obrada osobnih podataka bude u skladu sa svim specifičnim zahtjevima Uredbe. To uključuje učinkovito pružanje informacija, vođenje evidencije aktivnosti obrade, procjenu učinka na zaštitu podataka, imenovanje službenika za zaštitu podataka, izvještavanje o povredama podataka, poštovanje kodeksa ponašanja te uređivanje odnosa između voditelja i izvršitelja obrade. Implementacija ovih mjera ključna je za zaštitu prava ispitanika i promicanje transparentnosti i odgovornosti u obradi osobnih podataka. Na to upućuje i zaključak predmeta br. 340/21 pred Sudom Europske unije (SEU) koji jasno upućuje na važnost kontekstualne i teleološke analize prigodom tumačenja odredbi Uredbe o zaštiti osobnih podataka. SEU je potvrdio da samo neovlašteno otkrivanje ili pristup osobnim podacima treće strane nije dovoljno za zaključak da voditelj obrade nije primijenio odgovarajuće tehničke i organizacijske mjere. Umjesto toga potrebno je detaljno ispitati provedene mjere, uzimajući u obzir različite kriterije i rizike povezane s konkretnom obradom podataka. Ova odluka naglašava obvezu voditelja obrade da dokaže primjenu odgovarajućih mjera, što implicira da odgovornost za zaštitu podataka nije presumirana, već ovisi o kontekstu i razumnoj procjeni rizika i mjerama koje je sam voditelj implementirao. SEU time potvrđuje da je zaštita osobnih podataka dinamičan proces koji zahtijeva kontinuiranu evaluaciju i prilagodbu odgovarajućih i učinkovitih mjera zaštite.

BIBLIOGRAFIJA

Alhadeff, J.; Van Alsenoy, B.; Dumortier, J., *The accountability principle in data protection regulation: origin, development and future directions*, u: Guagnin, D.; Hempel, L.; Ilten, C. *et al.* (ur.), *Managing Privacy through Accountability*, Palgrave Macmillan, London, 2012., str. 49 – 82, DOI: 10.1057/9781137032225_4

Aridor, G.; Che, Y.-K.; Salz, T., *The effect of privacy regulation on the data industry: empirical evidence from GDPR,* The RAND Journal of Economics, *vol*. 54, 2023., str. 695 – 730, DOI: 10.1111/1756-2171.12455

Boros, A., *The Accountability Principle in Personal Data Processing*, Jurnalul Baroului Cluj, *vol*. 39, br. 2, 2021., str. 39 – 54.

Bovens, M., *Analysing and assessing accountability: A conceptual framework*, European law journal, *vol*. 13, br. 4, 2007., str. 447 – 468, DOI: 10.1111/j.1468-0386.2007.00378.x

Cerasaro, E. F., *Accountability principle under the GDPR: is data protection law moving from theory to practice?*, Luiss Law Review, br. 02, 2017., str. 214 – 226.

Colcelli, V., *Joint controller agreement under GDPR*, EU and Comparative Law Issues and Challenges Series, *vol*. 3, 2019., str. 1030 – 1047, DOI: 10.25234/eclic/9043

Cortina, S.; Picard, M.; Renault, S.; Valoggia, P., *Towards a Process-Based Approach to Compliance with GDPR*, u: Yilmaz, M.; Clarke, P.; Messnarz, R.; Reiner, M. (ur.), *Systems, Software and Services Process Improvement. EuroSPI 2021*, Springer, Cham, 2021., DOI: 10.1007/978-3-030-85521-5_8

Foulsham, M.; Hitchen, B.; Denley, A., *GDPR: How To Achieve and Maintain Compliance* (1st edition), Routledge, Abingdon, 2019.

Ivanova, Y., *Data Controller, Processor, or Joint Controller: Towards Reaching GDPR Compliance in a Data- and Technology-Driven World*, u: Tzanou, M. (ur.), *Personal Data Protection and Legal Developments in the European Union*, IGI Global, Hershey, PA, 2020., str. 61 – 84, DOI: 10.4018/978-1-5225-9489-5.ch004

Kuner, C.; Bygrave, L.A.; Docksey, C.; Drechsler, L. (ur.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford Academic, New York, 2020., DOI: 10.2139/ssrn.3839645

Selzer, A., *The Appropriateness of Technical and Organisational Measures under Article 32 GDPR*, European Data Protection Law Review, *vol*. 7, br. 1, 2021., DOI: 10.21552/edpl/2021/1/16

Shaw, W.; Barry, V., *Moral Issues in Business*, 13th edition, Wadsworth Publishing Company, Cengage Learning, Boston, 2016.

Voigt, P.; Von dem Bussche, A., *The EU General Data Protection Regulation (GDPR) - A Practical Guide*, Springer International Publishing AG, Cham, 2017., DOI: 10.1007/978-3-319-57959-7

Vojković, G.; Milenković, M.; Katulić, T., *IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law*, Business Systems Research: International journal of the Society for Advancing Innovation and Research in Economy, *vol*. 11, br. 3, 2020., str. 167 – 185.

IZVORI

Pravni akti

Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), SL L 119, 4. 5. 2016., str. 1 – 88.

Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, SL L 281, 23. 11. 1995., str. 31 – 50.

Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) od 20. ožujka 2024., https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-7.html#h-417659 (20. 10. 2023.).

Zakon o provedbi opće uredbe o zaštiti podataka, Narodne novine, br. 42/2018.

Sudska praksa

Sud Europske unije, C-210/16, Wirtschaftsakademie Schleswig-Holstein, presuda od 5. lipnja 2018.

Sud Europske unije, C-40/17, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, presuda od 29. srpnja 2019.

Sud Europske Unije, predmet br. C-340/21, VB v. Nacionalna agencija za javne prihode, Bugarska, presuda 19. 1. 2024.

Mrežni izvori

Agencija za zaštitu osobnih podataka, *Odluka o uspostavi i javnoj objavi popisa vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka od 21. prosinca 2018.*, https://azop.hr/odluka-o-uspostavi-i-javnoj-objavi-popisa-vrsta-postupaka-obrade-koje-podlijezu-zahtjevu-za-procjenu-ucinka-na-zastitu-podataka/ (28. 1. 2024.).

Bennet, C., *International privacy standards: can accountability ever be adequate?*, Privacy Laws & Business International Report, 2010., https://www.privacylaws.com/reports-gateway/reports/ (21. 12. 2023.).

Commission Nationale Informatique Libertes (CNIL), *Security of personal data*, CNIL's Guide 2018, https://www.cnil.fr/sites/cnil/files/atoms/files/guide_security-personal-data_en.pdf (19. 1. 2024.).

Cambridge dictionary, definicija pojma "by default", dostupna na: https://dictionary.cambridge.org/dictionary/english/default (21. 1. 2024.).

Converso, D., *The accountability of data controllers in relation to cloud providers*, Master Thesis Tilburg University, Srpanj 2013, http://arno.uvt.nl/show.cgi?fid=131417 (14. 12. 2023.).

Europska komisija, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, '*A comprehensive approach on personal data protection in the European Union*', November 2010, Brussels, COM(2010) 609 final, 12, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=-CELEX%3A52010DC0609 (20. 10. 2023.).

Europski odbor za zaštitu podataka, *Smjernice br. 4/2019 o članku 25 o tehničkoj i integriranoj zaštiti podataka 2.0,* od 20. 10. 2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (19. 12. 2023.).

Europski odbor za zaštitu podataka (EDPB), *Smjernice 07/2020 o pojmovima voditelja i izvršitelja obrade u Općoj uredbi o zaštiti podataka*, Verzija 2.0 usvojeno 7. srpnja 2021., https://edpb.europa.eu/system/files/2023- 10/edpb_guidelines_202007_controllerprocessor_final_hr.pdf (7. 12. 2023.).

Huth, D.; Matthes, F., *"Appropriate Technical and Organizational Measures": Identifying Privacy Engineering Approaches to Meet GDPR Requirements*, Technical University Munich, 25th Americas Conference on Information Systems, Cancun, 2019, https://wwwmatthes.in.tum.de/file/14qun4klf0r0d/Sebis-Public-Website/-/Appropriate-Technical-and-Organizational-Measu-

res-Identifying-Privacy-Engineering-Approaches-to-Meet-GDPR-Requirements/Huth%20AMCIS2019.pdf (17. 1. 2024.).

Hrvatska enciklopedija, definicija pojma "integracija", https://www.enciklopedija.hr/clanak/integracija (20. 1. 2024.).

Kosta, E., *Security of Processing and Data Breach Notification*, European Data Protection Board, 2023, https://www.edpb.europa.eu/system/files/2024-01/one_stop_shop_case_digest_security_data_breach_en.pdf (22. 1. 2024.).

Organizacija za ekonomsku suradnju i razvoj (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, https://www.oecd-ilibrary.org/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_5lmqcr2k94s8.pdf?itemId=%2Fcontent%2Fpublication%2F9789264196391-en&mimeType=pdf, (20. 10. 2023.).

Radna skupina prema čl. 29. za zaštitu podataka (WP29), *Mišljenje 3/2010 o načelu odgovornosti*, WP 173, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf (20. 10. 2023.).

Radna skupina prema čl. 29. za zaštitu podataka (WP29), *Mišljenje 1/2010 o pojmovima "voditelj" i "izvršitelj"*, 16. veljače 2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (18. 11. 2023.).

Radna skupina prema čl. 29. za zaštitu podataka (WP29), *Tumačenje WP29 o izuzeću od primjene obveze vođenja evidencije aktivnosti obrade prema prema čl. 30(5) Opeće uredbe o zaštiti podataka od 19. 4. 2018*, https://ec.europa.eu/newsroom/article29/items/624045 (27. 1. 2024.).

Summary

Hrvoje Lisičar*

ACCOUNTABILITY PRINCIPLE AND APPROPRIATE AND EFFECTIVE MEASURES ACCORDING TO THE GENERAL DATA PROTECTION REGULATION

With the adoption of the General Data Protection Regulation (EU) 2016/679 in the legislative framework governing the protection of personal data in the European Union, the legislator introduced as a novelty the principle of accountability. By introducing this principle, the legislator wanted to emphasize the accountability of the controller (and processor) of personal data as the responsible entities for correct and law-compliant handling of personal data processing, which is also aligned with the level of risk for the individual. For the principle of accountability to be realized, the responsible entities must actively implement appropriate and effective measures during the entire period of personal data processing to guarantee compliance with the prescribed rules for the protection of personal data, whereby the burden of proof of the fulfilment of the requirements imposed by the principle of accountability rests with the accountable entities themselves. The paper analyses the reasons that were decisive for the introduction of the principle of accountability in the legislative framework for data protection and its connection with previously established principles that must be applied when processing personal data. Furthermore, the provisions which regulate the implementation of appropriate and effective measures to comply with the requirements of the General Data Protection Regulation are considered. Also, we consider their connection with the level of risk for individual rights, better protection of personal data and the realization of the principle of accountability. Finally, the paper analyses recent decisions of the EU Court, national courts of EU member states, and decisions of competent national regulatory authorities which are related to the application of the principle of accountability in the processing of personal data and the implementation of appropriate and effective measures to comply with the requirements of the Regulation.

Key words: General Data Protection Regulation; GDPR; data protection; personal data; principle of accountability; technical and organizational measures; data security

* Hrvoje Lisičar, Ph. D., Associate Professor, Faculty of Law, University of Zagreb, Trg Republike Hrvatske 14, 10000 Zagreb; hrvoje.lisicar@pravo.unizg.hr; ORCID ID: orcid.org/0009-0003-7566-3538