Načelo cjelovitosti i povjerljivosti (sigurnosti) u Općoj uredbi o zaštiti podataka

Baban, Pia

Pravni fakultet Sveučilišta u Zagrebu

Katedra za pravo informacijskih tehnologija i informatiku

Pia Baban

Načelo cjelovitosti i povjerljivosti (sigurnosti) u Općoj uredbi o zaštiti podataka

Diplomski rad

Mentor: izv. prof. dr. sc. Tihomir Katulić

Zagreb, listopad 2022.

Izjava o izvornosti

Ja Pia Baban, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključiva autorica diplomskog rada te da u radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova te da se prilikom izrade rada nisam koristila drugim izvorima do onih navedenih u radu.

Pia Baban

Privacy is...“the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.“[1]

[1] Westin A.F., *Privacy and Freedom*, Atheneum, New York 1967., str 7.

Sadržaj

Abstract

This thesis aims to illuminate the role of Integrity and Confidentiality (Security) principle of the General Data Protection Regulation (GDPR). It illustrates the importance of data privacy through history and offers concise description of the other key principles of the Regulation. The thesis outlines the controller's responsibilities encased in the principle and examines the relationship between the controller and the regulator as well as the individual. It demonstrates the controller's and processor's obligation to implement appropriate technical and organizational measures in order to realise an appropriate level of security as well as the impact on the rights and freedoms of individuals. Furthermore, it addresses the importance of completing a risk assessment before carrying out a processing operation. Finally, this thesis offers an insight to recent rulings in regards to the violation of the principle.

Key words: General data protection regulation, GDPR, integrity and confidentiality principle, security principle, controller's responsibilities, data breach, risk assessment

Sažetak

Cilj ovog rada je prikazati ulogu načela cjelovitosti i povjerljivosti (sigurnosti) Opće uredbe o zaštiti podataka. Ilustrira važnost privatnosti podataka kroz povijest i nudi sažeti opis ključnih načela Uredbe. Diplomski rad ocrtava odgovornosti voditelja obrade sadržane u načelu i ispituje odnos između voditelja obrade i izvršitelja kao i odnos voditelja i ispitanika. Iskazuje obvezu poduzimanja odgovarajućih tehničkih i organizacijskih mjera voditelja i izvršitelja obrade radi ostvarivanja odgovarajuće razine sigurnosti kao i utjecaj obrade na prava i slobode pojedinaca. Rad govori o važnosti procjene učinka na zaštitu podataka prije izvođenja postupka obrade te konačno, nudi uvid u ulogu načela cjelovitosti i povjerljivosti kroz recentnu pravnu praksu.

Ključne riječi: Opća uredba o zaštiti podataka, načelo cjelovitosti i povjerljivosti, načelo sigurnosti, odgovornost voditelja obrade, povreda osobnih podataka, procjena učinka na zaštitu podataka

1. UVODNA RAZMATRANJA

Uredba „EU 2016/679 Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka“ od 27. travnja 2016. godine, stupila je na snagu 25. svibnja 2018. godine.[2] Skraćeni naziv ove Uredbe je „Opća uredba o zaštiti podatka“[3], poznata i pod engleskom skraćenicom – GDPR (General data protection regulation). Opća uredba je željno iščekivani autoritativni odgovor na ugrozu osobnih podataka pojedinca i u konačnici njegovu privatnost. Iako poneki autori razgraničavaju pojam zaštite podataka od pojma zaštite privatnosti[4], u pravnoj praksi i znanosti, ta dva pojma nužno su spojiva i isprepletena. Stoga ne možemo govoriti o zaštiti osobnih podataka pojedinca bez razumijevanja važnosti koja imaju prava čovjeka, a u sklopu njih i pravo čovjeka na privatnost, u kontinentalnom pravnom krugu, a i na međunarodnoj razini.

1.1. Povijesni pregled razvoja prava na zaštitu osobnih podataka

Povijesno gledajući pravo je uvijek kasnilo za razvojem i napretkom tehnologije i izazovima koje ona nužno nameće, posebno u sferi privatnosti i osobnih podataka pojedinca, no uvijek je bilo svjesno važnosti reguliranja i tih novonastalih (pravnih) područja. Tako je još 1890. godine Louis Brandeis definirao moderne pojmove prava pojedinca na privatnost u revolucionarnom članku koji je objavio zajedno sa Samuelom Warrenom, u Harvard Law Review-u 15. prosinca 1890.g., pod nazivom „Pravo na privatnost“.[5] U ovom značajnom djelu, Brandeis i Warren su se dotakli sve učestalijeg, nepoželjnog, utjecaja tadašnjih novinskih kuća koje su objavljivale fotografije pojedinaca bez njihove privole te time

[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.
[3] U daljnjem tekstu: Opća uredba ili Uredba.
[4] Gonzalez Fuster, Gloria, *The emergence of personal data protection as a fundamental right of the EU*, Springer International Publishing, Bruxelles, 2014., poglavlje VII.
[5] The right to privacy, originally published in 4 Harvard Law Review 193 (1890): https://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/the-right-to-privacy, 1. rujna 2022.

ugrožavali njihovu privatnost. Mnogi ovo djelo smatraju rođenjem prava na privatnost pojedinca jer su njime udarili temelje pravu na privatnost, ukazali na potrebnu pravnu zaštitu od zadiranja u to pravo te ga razgraničili od ostalih prava čovjeka.[6] Tako je i Vijeće Europe 1960-ih uvidjelo da je članak 8. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda koji propisuje da „*svatko ima pravo na poštovanje svoga privatnog i obiteljskog života, doma i dopisivanja*“[7] ugrožen tehnološkim napretkom. Vijeće je tada donijelo „Preporuku 509 o ljudskim pravima i suvremenom i znanstveno-tehnološkom razvoju“ i druge Rezolucije.[8] U ranim osamdesetima značajno je djelovanje OECD-a koje je svojim smjernicama[9] ustoličilo temeljne ideje vodilje koje uređuju prekogranični promet podataka i zaštitu osobnih podataka i privatnosti, a sve kako bi ujednačilo praksu država članica.[10] Istovremeno Vijeće Europe donijelo je „Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka“ (Konvencija 108), koja je bila otvorena za potpisivanje svim državama svijeta i time potakla međunarodno ujednačavanje zakonodavstva u području zaštite osobnih podataka.[11] Zanimljivo je napomenuti da je Protokol za izmjenu Konvencije 108+ otvoren za potpisivanje i danas.[12]

U hrvatskom zakonodavstvu prava pojedinca na zaštitu privatnosti osigurava Ustav Republike Hrvatske[13] i to člancima 34., 36. i 37. koji se odnose na prostornu, komunikacijsku i informacijsku privatnost. Na području zaštite osobnih podataka obvezujuća je Opća uredba

[6] Dragičević Dražen et al., *Pravna informatika i pravo informacijskih tehnologija*, Narodne novine, Zagreb, 2015, poglavlje V (2018), str. 4.
[7] Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda , stupila na snagu 3. rujna 1953. g., članak 8.
[8] Ustaran Eduardo, CIPP/E, Partner, Lovells, Hogan, *European Data Protection: Law and Practice,* IAPP Publication, Sjedinjene Američke Države, 2018., str.19.
[9] *Smjernice o zaštiti privatnosti i međunarodnom prijenosu osobnih podataka* , OECD 1981.g.
[10] Ustaran, op.cit. (bilj. 8), str 20.
[11] Ibid.
[12]U svibnju 2022. godine u Dubrovniku održana je trideseta međunarodna konferencija stručnjaka i nadzornih tijela u području zaštite podataka (*Spring conference)* gdje su stručnjaci urigirali na potpisivanje i ratificiranje Konvencije 108+ jer je samo 17 država članica ratificiralo Konvenciju u vrijeme pisanja ovog rada; https://azop.hr/wp-content/uploads/2022/05/RESOLUTION-108.pdf i https://azop.hr/spring-conference2022-dubrovnik-croatia/, 1. rujna 2022.g.
[13] Ustav Republike Hrvatske, Narodne Novine br. 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14

kao uredba Europske unije, za razliku od prijašnje Direktive ZOP koju je Opća uredba stavila izvan snage. Pored Uredbe donesen je i Zakon o provedbi Opće uredbe o zaštiti podataka. Ovaj rad fokusira se na značaj načela cjelovitosti i povjerljivosti, odnosno sigurnosti, osiguravanje pravilne primjene načela prema konsenzusu stručnjaka za zaštitu podataka, obveze i odgovornosti pri vršenju obrade podataka te njegovu primjenu kroz pravnu praksu i djelovanje lokalnih nadzornih tijela članica EU.

1.2. Ključni pojmovi

Prije doticanja važnosti Uredbe i njezinih načela potrebno je definirati ključne pojmove zaštite osobnih podataka koji su posredno važni za razumijevanje ovog rada;

Osobni podatak znači svaki podatak koji se odnosi na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik").[14]

Voditelj obrade znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka.[15]

Izvršitelj obrade znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.[16]

Pored ovih pojmova, važno je spomenuti i *nadzorna tijela* koje imenuje svaka država članica, a koja osiguravaju pravilnu primjenu Uredbe kako bi se zaštitila temeljna prava i slobode pojedinaca u pogledu obrade i kako bi se olakšao slobodan protok osobnih podataka unutar Unije.[17] U Republici Hrvatskoj službeno nadzorno tijelo je Agencija za zaštitu osobnih podataka (AZOP) čije je djelovanje uređeno Zakonom o provedbi Opće uredbe o zaštiti

[14] Opća Uredba, op.cit. (bilj. 2), čl. 4
[15] Ibid.
[16] Ibid.
[17] Ibid., čl. 51. st. 1.

podataka.[18] Na razini Europske unije djeluje Europski odbor za zaštitu podataka (EOZP) koji je neovisno tijelo Europske unije čija je svrha osigurati dosljednu primjenu Opće uredbe o zaštiti podataka i promicati suradnju među tijelima EU-a za zaštitu podataka.

2. SAŽETI PREGLED NAČELA OPĆE UREDBE

U suštini, načela su smjernice i misli vodilje koje služe kao kriterij za djelovanje i prosuđivanje. Opća uredba propisuje načela obrade osobnih podataka kroz koja je vidljiva intencija europskog zakonodavca da u srž načela sažme sve one situacije koje zakonodavac ne može predvidjeti. Osim načela cjelovitosti i povjerljivosti, odnosno sigurnosti koje je fokus ovog rada, Uredba propisuje i načela: zakonitosti, poštenosti i transparentnosti, ograničavanja svrhe obrade, smanjenje količine podataka, točnosti, ograničenja pohrane te pouzdanosti kao dodatnog načela koje se izravno odnosi na voditelja obrade.

2.1. Načelo zakonitosti

Uz načelo poštenosti i transparentnosti, ovo načelo jedno je od glavnih načela Uredbe. Prema Općoj uredbi da bi se obrada osobnih podataka smatrala zakonitom nužno je da postoji jedna od sljedećih okolnosti:

1. Ispitanik je dao privolu[19] za obradu svojih osobnih podataka;
2. Obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili u vezi sa zahtjevom ispitanika prije sklapanja ugovora;
3. Voditelj obrade podatke ispitanika obrađuje kako bi ispunio svoju pravnu obvezu;
4. Obrada je nužna za zaštitu ključnih interesa ispitanika ili druge fizičke osobe;

[18] Zakon o provedbi Opće uredbe o zaštiti podataka, Narodne Novine br. 42/18

[19] „Privola" ispitanika prema članku 4. t. 11. Uredbe, znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.

5. Obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službenih ovlasti voditelja obrade;
6. Obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane.[20]

2.2. Načelo transparentnosti

Načelo transparentnosti upućuje na to da svaka informacija i komunikacija upućena ispitaniku u vezi s obradom njegovih osobnih podataka mora biti lako dostupna i razumljiva uz upotrebu jasnog i jednostavnog jezika.[21] Transparentnost u postupku obrade osobnih podataka ukazuje na obveze voditelja obrade u svim fazama ciklusa obrade, kako prije samog započinjanja obrade, tako i tijekom obrade pa i u točno određenim trenutcima tijekom obrade.[22] Informacije koje voditelj obrade pruža ispitaniku moraju biti „sažete“, no valjalo bi taj izraz tumačiti kao „jasne“, „lako razumljive“, „važne“, „precizne“ i „bitne“, s obzirom da izvorni tekst Opće uredbe koristi englesku riječ „concise“. Ova riječ prevedena na hrvatski jezik znači „sažeto“, te tada ima predznak „kratkog“, odnosno „neopširnog“ čime gubi smisao i intenciju zakonodavca. Ovdje je smisao ovog načela u tome da prosječnom ispitaniku komunikacija i informacija budu jasne i nedvojbene, a ne da se opširnošću izgubi bit odnosno da se ispitanika zaslijepi.[23] Istovremeno načelo propisuje i prava ispitanika u vezi njegovih osobnih podataka koji se obrađuju.

2.3. Načelo poštene obrade osobnih podataka

Načelo poštene obrade usko je vezano za načelo zakonitosti i transparentnosti. Ono je slabije opipljivo načelo te ostavlja prostora ponajviše iskustvenom i moralnom sudu kao misli vodilji

[20] Opća Uredba, op. cit. (bilj. 2), članak 6.
[21] Ibid., čl. 12.
[22] Radna skupina za zaštitu pojedinaca u vezi s obradom osobnih podataka, *Smjernice o transparentnosti na temelju Uredbe 2016/679* od 11. travnja 2018., https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227, str. 6.
[23] EU Agency for Fundamental Rights, *Handbook on european data protection law*, 2020.: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf, str. 135., 13. rujna 2022.

o tome što se smatra poštenom obradom osobnih podataka. U akademskoj zajednici prevladava misao da je svrha ovog načela pružiti ravnotežu između interesa voditelja obrade i ispitanika.[24] Information Comissioner Office ili skraćeno ICO[25] kaže da obrada osobnih podataka uvijek mora biti poštena i zakonita. Ako je bilo koji aspekt obrade nepošten, on vrijeđa ovo načelo čak i ako postoji zakonska osnova za obradu.[26] ICO nadalje navodi *checklist* koji treba poslužiti voditeljima obrade pri ocjeni je li obrada poštena;

-Razmotrili smo kako obrada može utjecati na točno određenog ispitanika i možemo opravdati svaki negativan učinak

-S podacima ispitanika postupamo samo na način na koji bi oni razumno očekivali ili možemo objasniti zašto je svaka neočekivana obrada opravdana

-Ne zavaramo niti dovodimo u zabludu ispitanike kada prikupljamo njihove osobne podatke.[27]

2.4. Načelo obrade podataka za specifičnu svrhu

Voditelj obrade dužan je osobne podatke koje je dobio od ispitanika obrađivati samo u posebne, izričite i zakonite svrhe.[28] Ovim načelom obrada osobnih podataka ograničena je kvalitativno jer sprječava voditelja da izlazi iz okvira koji su uspostavljeni zakonskim temeljem obrade osobnih podataka ispitanika, odnosno neposredne svrhe prikupljanja tih podataka. Od samog početka obrade podataka ciljevi obrade moraju biti jasni i svrha obrade

[24] Malgieri, Gianclaudio, *The concept of fairness in the GDPR*; *A linguistic and contextual interpretation*, In Proceedings of FAT* on Fairness, Accountability, and Transparency, Barcelona, 2020., str. 10

[25] ICO je neovisno tijelo Ujedinjenog Kraljevstva ustanovljeno s ciljem osiguravanja zaštite i poštivanja informacijskih prava građana; Information Commissioner's Office, What we do,: https://ico.org.uk/about-the-ico/what-we-do/, 14. rujna 2022.

[26] ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/#fairness, 1. rujna 2022.

[27] Ibid.

[28] Opća Uredba, op.cit. (bilj. 2), članak 5. st. 1. t. b

mora biti zabilježena.[29] Ukoliko nastane potreba za obradom podataka van svrhe za koju su inicijalno prikupljeni, utoliko je ispitaniku potrebno pružiti informacije o takvoj obradi.[30]

2.5. Načelo minimiziranja količine osobnih podataka koji se obrađuju

Opća uredba propisuje da: „*osobni podaci moraju biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju*.“[31] „Primjerenost“ podrazumijeva da su dovoljni za ispravno ispunjavanje navedene svrhe, „relevantnost“ se odnosi na racionalnu vezu sa tom svrhom te konačno „ograničenost“ znači da su ograničeni na ono što je potrebno, odnosno, ne više od onog što je potrebno za tu svrhu.[32]

2.6. Načelo točnosti

Načelo točnosti obvezuje voditelja obrade da osigura točnost osobnih podataka nad kojima vrši obradu i da ih prema potrebi, dopunjuje i osvježava brzo i učinkovito.[33] Ispitanik ima mogućnost tražiti od voditelja obrade da u bazama podataka ispravi njegove netočne osobne podatke, a voditelju obrade Opća uredba propisuje obvezu da to učini bez nepotrebnog odgađanja.[34]

2.7. Načelo vremenski ograničene obrade

Opća uredba propisuje da osobni podaci trebaju biti pohranjeni samo onoliko dugo koliko je to potrebno za ostvarenje svrhe zbog koje se pristupilo obradi.[35] Načelo vremenski ograničene obrade usko je povezano s načelom obrade podataka u specifične svrhe. Svrha zbog koje voditelj obrade prikuplja od ispitanika osobne podatke ograničava opseg obrade osobnih

[29] ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/, 2. rujna 2022.
[30] Opća uredba, op.cit. (bilj. 2), recital 61
[31] Ibid., članak 5. st. 1. t. c
[32] ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/, 2. rujna 2022.
[33] Opća uredba, op.cit. (bilj. 2), čl. 5. st. 1. t. d.
[34] Ibid., čl. 16.
[35] Ibid., čl. 5. st. 1. t. e

podataka kvalitativno i kvantitativno te u odnosu na vremenski opravdano razdoblje u kojoj se vrši obrada osobnih podataka. Osobni podaci ne smiju se čuvati dulje nego što je potrebno. Voditelj obrade mora biti u mogućnosti opravdati razdoblje čuvanja osobnih podataka. To prvenstveno ovisi o svrsi čuvanja podataka.[36] Primjerice, banka čuva osobne podatke svojih klijenata koji najčešće uključuju podatke o adresi svakog kupca, datumu rođenja i djevojačkom prezimenu majke. Banka koristi ove informacije kao dio svojih sigurnosnih procedura i primjereno je da ih čuva sve dok klijent ima otvoren račun u banci pa čak i nakon što je račun zatvoren jer će možda trebati zadržati neke od ovih podataka iz pravnih ili operativnih razloga još određeno vrijeme. Naprotiv poslodavac koji primi više prijava za natječaj ne bi trebao voditi evidenciju o neuspješnim kandidatima nakon proteka zakonskog roka u kojem se može podnijeti zahtjev ili pritužba koji proizlaze iz postupka zapošljavanja.[37]

2.8. Načelo pouzdanosti

Načelo pouzdanosti isprepleteno je sa ostalim načelima, a pogotovo sa načelom cjelovitosti i povjerljivosti koje je fokus ovoga rada. Ono ukazuje na odgovornost voditelja obrade za usklađenost obrade podataka s ostalim načelima koju mora biti u mogućnosti dokazati.[38] Novina je upravo obveza voditelja obrade njegova mogućnost da usklađenost dokaže.[39] Voditelj obrade dužan je poduzeti mjere koje će osigurati pouzdanost. Prema ICO-u neke od mjera koje bi voditelj mogao, odnosno mora, poduzeti su: sklapanje pisanih ugovora s izvršiteljima obrade, održavanje dokumentacije o aktivnostima obrade, provođenje odgovarajućih sigurnosnih mjera, bilježenje i, prema potrebi, prijavljivanje povreda osobnih podataka, provođenje procjene učinka zaštite podataka za upotrebe osobnih podataka koje će

[36] ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/, 2. rujna 2022.
[37] Ibid.
[38] Opća uredba, op.cit. (bilj. 2), čl. 5. st. 2.
[39] Dragičević, op.cit. (bilj. 6), str. 34.

vjerojatno dovesti do visokog rizika za interese pojedinaca te imenovanje službenika za zaštitu podataka.[40] O ostalim tehničkim i sigurnosnim mjerama bit će više riječi kasnije.

3. NAČELO CJELOVITOSTI I POVJERLJIVOSTI

Načelo cjelovitosti i povjerljivosti koje je sadržano u članku 5. st. 1. t. f) nalaže da podaci moraju biti: „*obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera*.“[41]

U akademskoj zajednici i literaturi uobičajeno je ovo načelo nazivati i načelom sigurnosti. Ono se gotovo poistovjećuje sa člankom 32. Uredbe koji sadrži odredbe o sigurnosti. Tako i ICO kaže da je načelo cjelovitosti i povjerljivosti Uredbe poznato kao načelo sigurnosti.[42] Intencija zakonodavca bila je razraditi manifestaciju načela cjelovitosti i povjerljivosti kroz odredbe članka 32. o čemu će detaljnije biti riječ u nastavku rada, kao i o obvezama koje to stvara za voditelja i izvršitelja obrade. U nastavku rada bit će pojašnjene tehničke i organizacijske mjere koje voditelj i izvršitelj obrade trebaju poduzeti da bi obrada podataka bila u skladu sa načelima Uredbe. Konačno, rad će prikazati i manifestaciju načela kroz recentnu sudsku praksu.

[40] ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/, 2.rujna 2022.
[41] Opća uredba, op.cit. (bilj. 2), čl. 5., t., f
[42] ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/,5. rujna 2022.

3.1. Odredbe Opće uredbe o zaštiti podataka koje predstavljaju primjenu načela cjelovitosti i povjerljivosti

Načelo cjelovitosti i povjerljivosti sadržano u članku 5. Uredbe, prošireno je člankom 32. koji govori o tome što sigurnost zapravo podrazumijeva te služi kao alat kojim se načelo cjelovitosti i povjerljivosti štiti i kojim se osigurava njegova pravilna primjena. Iako se u samoj Uredbi pojam „informacijska sigurnost“ spominje samo jednom, ipak je potpuno jasno da priznata praksa informacijske sigurnosti predstavlja okvir za osiguranje odgovornosti obrade osobnih podataka.[43] Uredba predviđa potencijalno kobne kazne u slučaju nepridržavanja mjera koje propisuje te uspostavlja okvir za kolektivnu akciju protiv voditelja obrade koji je odgovoran za povredu osobnih podataka, bez obzira na izvor i uzročnika incidenta. Ovaj oblik objektivne i stroge odgovornosti stvara značajno opterećenje za voditelje obrade te samim time ih potiče da poboljšaju sigurnost obrade.[44]

3.1.1. Odgovornost voditelja i izvršitelja obrade

Načelo sigurnosti traži da se poduzmu odgovarajuće tehničke i organizacijske mjere koje su proporcionalne mogućem riziku koji prijeti osobnim podacima ispitanika.[45] Voditelji i izvršitelji obrade moraju moći dokazati da primjenjuju adekvatnu razinu zaštite odnosno da su poduzeli primjerene tehničke i organizacijske mjere. U ovom smislu, načelo pouzdanosti zajedno sa člankom 24. Uredbe, koji propisuje odgovornosti voditelja obrade, stavlja teret upravo na voditelja obrade.[46] Članak 24. nalaže implementaciju odgovarajućih politika zaštite te redoviti pregled i ažurno poduzimanje tehničkih i organizacijskih mjera gdje je to potrebno.

[43] Katulić, Tihomir, Protrka, Nikola, *Information Security in Principles and Provisions of the EU Data Protection Law*, 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2019., str. 2., dostupno na: https://www.bib.irb.hr/1014209, 14.listopada, 2022.
[44] Ibid.
[45] Ustaran, op.cit. (bilj. 8), poglavlje 10.
[46] Ibid.

Ove odredbe popraćene su sa nekoliko uvodnih izjava Uredbe koje utvrđuju odgovornost voditelja obrade podataka za sigurnost obrade koju provodi on sam ili netko drugi za njega, obvezu provedbe odgovarajućih i učinkovitih mjera te sposobnost voditelja da dokaže da obradu obavlja u skladu s Uredbom.[47]

3.1.2. Procjena učinka na zašttu podataka

Zadaća voditelja i izvršitelja obrade sastoji se u procjeni učinka i osiguravanju obrade osobnih podataka od nepažnje i slučajnih povreda s jedne strane te namjernih i malicioznih s druge. To podrazumijeva zaštitu od kompleksnih tehnoloških prijetnji poput maleware programa, DOS[48] napada i drugih kriminalnih djela, kao i unutarnju zaštitu od grube nepažnje zaposlenika.[49] Uredba u članku 32. navodi primjerene odnosno odgovarajuće tehnološke i organizacijske mjere koje treba poduzeti s obzirom na prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, da bi se gore navedeno spriječilo.[50] Koristeći riječ „odgovarajuće“ mjere, zakonodavac jasno daje do znanja da ne očekuje apsolutnu zaštitu osobnih podataka u tehnološkom smislu da bi se načelo sigurnosti pa i ostale odredbe Uredbe smatrale zadovoljenima. Dovoljno je da one s obzirom na tehnološka dostignuća i, ostale uvjete gore navedene, budu primjerene odnosno odgovarajuće. Tako ukoliko do povrede i dođe to ne znači automatsku odgovornost voditelja i izvršitelja obrade već dovoljno je da oni mogu dokazati usklađenost obrade sa odredbama Uredbe u konkretnoj situaciji.[51] Oni moraju procjenom učinka na zaštitu podatka ustvrditi jesu li te mjere primjerene s obzirom na rizik i vrstu postupka obrade podatka. Rizike bi trebalo procjenjivati na temelju objektivne procjene, kojom se utvrđuje je su li postupci obrade

[47] Katulić, Tihomir, loc.cit.
[48] „Denial of service“; napad *uskraćivanja usluga ili servisa* kojim se korisnicima onemogući njihovo korištenje.
[49] Ustaran, Eduardo, loc.cit. (bilj. 43)
[50] Opća uredba, op.cit. (bilj. 2), članak 32., vidi *infra*
[51] Ustaran, Eduardo, loc.cit.

podataka izloženi riziku ili visokom riziku.[52] Procjena učinka na zaštitu podataka trebala bi uključivati *state-of-the*-art[53] testove kako bi voditelji i izvršitelji obrade bili sigurni da primjenjuju procese obrade koji odgovaraju najnovijim tehnološkim dostignućima u području informatičke sigurnosti, a ne da se oslanjanju na prosječna rješenja industrije.[54]

U tom smislu, članak 25. i 35. Uredbe osnažuju procjenu učinka na zaštitu podatka kao zadaću voditelja obrade[55]. Članak 35. Uredbe navodi situacije u kojima je procjena učinka na zaštitu podataka obvezna:

- „*sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila, i na temelju koje se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca ili na sličan način značajno utječu na pojedinca*
- *opsežne obrade posebnih kategorija osobnih podataka ili podataka u vezi s kaznenim osudama i kažnjivim djelima*
- *sustavno praćenje javno dostupnog područja u velikoj mjeri*.“[56]

Obrada osobnih podataka nije opsežna ako se odnosi na osobne podatke pacijenata ili klijenata pojedinih liječnika, zdravstvenih djelatnika ili odvjetnika te tada procjena učinka nije obvezna.[57]

Recital 75. Uredbe specificira upravljanje rizicima i sigurnosti obrade te uključuje sljedeće situacije kao iznimno bitne ako obrada može dovesti do:

- „*diskriminacije, krađe identiteta ili prijevare*

[52] Dragičević, op.cit. (bilj. 6), str. 47.
[53] Hrv.: „Test stanja tehnike“
[54] Ustaran, Eduardo, loc.cit.
[55] Ibid.
[56] Opća uredba, op.cit. (bilj. 2), članak 35. st. 3.
[57] Ibid., Recital 91

- *financijskog gubitka, štete za ugled, gubitka povjerljivosti osobnih podataka zaštićenih poslovnom tajnom*
- *neovlaštenog obrnutog postupka pseudonimizacije*
- *bilo koje druge znatne gospodarske ili društvene štete*
- *ako ispitanici mogu biti uskraćeni za svoja prava i slobode ili spriječeni u obavljanju nadzora nad svojim osobnim podacima*
- *ako se obrađuju osobni podaci koji odaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, članstvo u sindikatu i ako je riječ o obradi genetičkih podataka, podataka koji se odnose na zdravlje ili spolni život ili kaznene osude i kažnjiva djela ili povezane sigurnosne mjere*
- *ako se procjenjuju osobni aspekti, osobito analiza ili predviđanje aspekata u vezi s učinkom na poslu, ekonomskim stanjem, zdravljem, osobnim preferencijama ili interesima, pouzdanošću ili ponašanjem, lokacijom ili kretanjem kako bi se izradili ili upotrebljavali osobni profili*
- *ako se obrađuju osobni podaci osjetljivih pojedinaca, osobito djece*
- *ako obrada uključuje veliku količinu osobnih podataka i utječe na velik broj ispitanika.*“[58]

Ako procjena učinka pokaže da će obrada dovesti do visokog rizika za prava i slobode ispitanika, ukoliko voditelj obrade ne donese mjere za ublažavanje rizika, on se mora obratiti nadzornom tijelu za savjetovanje prije obrade, što se naziva Prethodnim savjetovanjem i detaljno je uređeno u članku 36. Uredbe.[59] Savjetovanje je nužno samo u slučajevima u

[58] Opća uredba, op .cit., (bilj. 2), recital 75
[59] Ibid., čl. 36.

kojima utvrđene rizike voditelj obrade podataka ne može ukloniti na odgovarajući način, odnosno preostali rizici su i dalje visoki.[60]

Agencija za zaštitu osobnih podataka kao domaće nadzorno tijelo ovlašteno je i utvrđivati vrste postupaka obrade koji podliježu obveznoj procjeni učinka, odnosno one za koje nije potrebna procjena učinka. Na temelju te ovlasti AZOP je objavio „Odluku o uspostavi i javnoj objavi popisa vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka“[61] koja je podložna promjenama[62], a zadnja promjena je od 21. prosinca 2018. godine. Osim toga AZOP je prema članku 18. Zakona o provedbi Opće uredbe ovlašten na svojim mrežnim stranicama objavljivati anonimizirana ili pseudonimizirana rješenja i mišljenja vezana za one vrste obrada koje mogu prouzročiti visoki rizik.[63]

3.1.3. Tehničke i organizacijske mjere zaštite

Uredba primjeričnom listom navodi kakve bi mjere trebalo poduzeti, shodno potrebi, u svrhu osiguranja zaštite podataka,:

- „*pseudonimizacija i enkripcija osobnih podataka;*
- *sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade;*
- *sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta;*

[60] AZOP: *Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik" u smislu Uredbe 2016/679*; https://azop.hr/wp-content/uploads/2020/12/wp248_rev.01_hr-1.pdf, 15. rujna 2022.
[61] AZOP:https://azop.hr/odluka-o-uspostavi-i-javnoj-objavi-popisa-vrsta-postupaka-obrade-koje-podlijezu-zahtjevu-za-procjenu-ucinka-na-zastitu-podataka/, 10. rujna 2022.
[62] Dragičević, op.cit. (bilj. 6), str. 54.
[63] Ibid., str. 55.

- *proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.“*[64]

Nastavno na prethodno spomenute state-of-the-art testove, voditelji i izvršitelji obrade trebaju u suštini pratiti konsenzus stručnjaka na području informatičke sigurnosti da bi uskladili svoje procese obrade sa najboljim rješenjima koje industrija u tom trenutku nudi. Iz zakonske perspektive, Uredba ostavlja prostor samim voditeljima obrade i konsenzusu stručne zajednice da odredi koje su to primjerene mjere, no izrijekom spominje enkripciju i pseudonimizaciju te stavlja fokus upravo na njih. Zanimljiv je utjecaj znanosti i tehnološkog napretka na zakonodavca koji ovdje prepoznaje važnost stručnjaka određene industrije. Tako je prijašnja Direktiva ZOP ostala suzdržana o specifičnim tehnološkim mjerama, a stručni konsenzus je bio taj koji je tada enkripciju[65] postavio kao standard u svijetu zaštite podataka.[66]

Pseudonimizacija je također izrijekom spomenuta u članku 32. Uredbe i tako je uvedena u opći pravni okvir Europe, čime je potaknuta njena primjena u procesima obrade podataka. Iako pseudonimizacijom podataka i dalje raspolažemo osobnim podacima, njenom primjenom smanjujemo rizik za ispitanike i osiguravamo ispunjenje zadaća voditelja i izvršitelja obrade.[67] Prema Uredbi pseudonimizacija je: „*obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi*“[68]

[64] Opća uredba, op.cit. (bilj. 2), članak 32.
[65] Enkripcija je proces kojim se vrši izmjena podataka tako da se poruka, odnosno informacije, učine nečitljivim za osobe koje ne posjeduju ključ; vidi: https://bs.wikipedia.org/wiki/Enkripcija
[66] Ustaran, op.cit. (bilj. 8), poglavlje 10.2.1.
[67] Dragičević, op.cit. (bilj. 6), str. 26.
[68] Opća uredba, op.cit. (bilj. 2), čl. 4. t. 5

Osim enkripcije i pseudonimizacije važnost konsenzusa stručnjaka manifestirala se i u stavku prvom točkama b, c i d članka 32. Uredbe gdje su „cjelovitost“, „povjerljivost“, „dostupnost“ i „otpornost“ stupovi tehničkog i organizacijskog uspjeha voditelja i izvršitelja obrade.[69] Takozvana „CIA trijada“[70] , poznata je kao esencija informacijske sigurnosti te ako je bilo koji od ovih elementa ugrožen, tada mogu nastupiti ozbiljne posljedice, kako za voditelja obrade, tako i za pojedince čiji se podaci obrađuju. Mjere sigurnosti koje se provode trebale bi jamčiti sva tri elementa i za sustave obrade i za sve podatke koji se obrađuju.[71] Dužnost je i izvršitelja da pomaže voditelju obrade putem odgovarajućih tehničkih i organizacijskih mjera da ispuni obvezu voditelja obrade u pogledu odgovaranja na zahtjeve za ostvarivanje prava ispitanika.[72] Novost u odnosu na prijašnje zakonodavstvo je u tome da se traži jamstvo poštivanja svih odredaba Uredbe, a ne samo odredaba o sigurnosti prilikom sklapanja ugovora i određivanja obveza između voditelja i izvršitelja obrade.[73] Novina je i dužnost izvršitelja da pomaže voditelju obrade u osiguravanju usklađenosti s obvezama koje se tiču odredbi o sigurnosti, procjenu učinka i obavještavanju ispitanika i nadzornog tijela o povredi osobnih podataka.[74]

I hrvatsko nadzorno tijelo AZOP objavilo je preporuke za voditelje obrade kojima osiguravaju primjenu načela sigurnosti:

- „*dokumentaciju u papirnatom obliku koja sadrži osobne podatke voditelj obrade dužan je istu pohraniti, primjerice u ormare ili ladice pod ključem koja će biti pod nadzorom ovlaštenih osoba voditelja obrade*

[69] Ustaran, Eduardo, loc.cit.
[70] Eng.: CIA: Confidentiality (povjerljivost), integrity (cjelovitost), availability (dostupnost)
[71] ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/, 8.rujna 2022.
[72] Opća uredba, op.cit. (bilj. 2), članak 28. st. 3. f
[73] ICO: https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf , 7. rujna 2022.
[74] Ustaran, op.cit. (bilj. 8), Poglavlje 10.2.3.

- *pristup osobnim podacima pohranjenim u elektroničkom obliku trebao bi biti omogućen uporabom korisničkog imena i lozinke*
- *izrada sigurnosnih kopija od strane ovlaštenih osoba*
- *potpisivanje izjava o povjerljivosti osoba koje su u obradi osobnih podataka*
- *pseudonimizacija ili enkripcija osobnih podataka, osobito ako se radi o posebnim kategorijama (primjerice: podataka o zdravlju)*
- *bilježenje pristupa podacima*".[75]

3.1.4. Tehnička i integrirana zaštita podataka

Tehnička zaštita podataka bazira se na konceptu *privatnosti po dizajnu* (privacy by design), koji označava filozofiju i pristup ugrađivanja zaštite prava na privatnost već u specifikacije dizajna različitih tehnologija.[76] Privatnost po dizajnu obuhvaća primjenu na: IT sustave, odgovorno poslovanje prakse i fizički dizajn i umreženu infrastrukturu.[77] Ovo načelo poslovanja traži da se uz korištenje naprednih tehnologija za zaštitu privatnosti u samoj fazi planiranja i oblikovanja sustava za obradu osobnih podataka ugrade i predvide sve potrebne mjere zaštite podataka.[78] Zakonodavac je prepoznao važnost ovog koncepta pa ga je implementirao u Uredbu kao zaštitu podataka po dizajnu[79] odnosno *tehničku zaštitu podataka* u članku 25.: „*Uzimajući u obzir najnovija dostignuća, trošak provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade podataka, voditelj obrade, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, provodi odgovarajuće tehničke i*

[75] AZOP: https://azop.hr/osnovne-informacije-za-organizacije/, 5. rujna 2022.
[76] Cavoukian, Ann, *Privacy by design...take the challenge*, Information and Privacy Commissioner of Ontario, Kanada, 2009., str. 3.; https://www.ipc.on.ca/wp-content/uploads/Resources/PrivacybyDesignBook.pdf, 15.rujna 2022.
[77] Cavoukian, Ann, *Privacy by design*, *The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, Kanada, 2011., str. 1.; https://www.sfu.ca/~palys/Cavoukian-2011-PrivacyByDesign-7FoundationalPrinciples.pdf, 15. rujna 2022.
[78] Ustaran, op. cit. (bilj. 8), str. 49.
[79] Eng. : Data protection by design

organizacijske mjere, poput pseudonimizacije, za omogućavanje učinkovite primjene načela zaštite podataka, kao što je smanjenje količine podataka, te uključenje zaštitnih mjera u obradu kako bi se ispunili zahtjevi iz ove Uredbe i zaštitila prava ispitanika."[80] Ovaj koncept dakle nije nov, no ključna promjena je to što je sada pravno obvezujuć. Tehnička zaštita podataka odnosi se na razmatranje pitanja zaštite podataka i privatnosti unaprijed. Može pomoći voditeljima obrade da djeluju u skladu s temeljnim načelima i zahtjevima Uredbe i stavlja fokus na odgovornost.[81] Recital 78 dodatno pojašnjava da bi radi dokazivanja sukladnosti s Uredbom voditelj obrade trebao uvesti interne politike i provesti mjere koje ispunjavaju načela tehničke zaštite podataka i integrirane zaštite podataka. Osim pseudonimizacije kao primjer navodi se i transparentnost u vezi s funkcijama i obradom osobnih podataka, što omogućava voditelju obrade da stvara i poboljšava sigurnosne značajke.[82] Nadalje, voditelji obrade bi trebali provoditi redovite preglede mjera informacijske sigurnosti koje štite osobne podatke te postupak postupanja s povredama podataka.

Načelo integrirane zaštite podataka[83] obvezuje voditelja obrade da kao početnu, zadanu, vrijednost obrađuje samo nužne podatke za svaku vrstu obrade, koristeći se tehničkim i organizacijskim mjerama. Ta obveza podrazumijeva i opseg obrade, količinu prikupljenih podataka, razdoblje vremenske pohrane i njihovu dostupnost trećima.[84] Od iznimne su važnosti proizvođači usluga i aplikacija koji bi trebali implementirati mjere koje štite osobne podatke jer će se mnogi voditelji obrade koristiti njihovim uslugama.

ICO je objavio *checklist* namijenjen voditeljima obrade kako bi provjerili pridržavaju li se

[80] Opća uredba, op. cit. (bilj. 2), članak 25. st. 1.
[81] ICO:https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/, 16. rujna 2022.
[82] Opća uredba, op.cit. (bilj. 2), Recital 78
[83] Eng.: Data protection by default
[84] Dragičević, op.cit. (bilj. 6), str 49.

načela tehničke i integrirane zaštite podataka, neke od konstatacija koje bi trebale biti zadovoljene su:

- Zaštita podataka bitna je komponenta temeljne funkcionalnosti sustava obrade i usluga.
- Rizici i događaji koji ugrožavaju privatnost predviđeni su prije nego što se dogode uz poduzimanje koraka da se spriječi šteta pojedincima
- Osobni podaci automatski su zaštićeni u bilo kojem IT sustavu, usluzi, proizvodu i/ili poslovnoj praksi, tako da pojedinci ne bi trebali poduzimati nikakve posebne radnje za zaštitu svoje privatnosti
- Usvojena je politika 'jednostavnog jezika' za sve javne dokumente
- Obrada je povjerena samo izvršiteljima obrade koji daju dostatna jamstva za svoje tehničke i organizacijske mjere zaštite podataka po dizajnu[85]

Europski odbor za zaštitu podataka objavio je Smjernice o tumačenju članka 25. Uredbe[86] kojima između ostalog, detaljno pojašnjava načelo cjelovitosti i povjerljivosti u svjetlu načela tehničke i integrirane zaštite te navodi slijedeće ključne operativne elemente kao preporuku voditeljima obrade:

- *Sustav upravljanja sigurnošću informacija* (ISMS - Information security management system) – Imati operativna sredstva upravljanja politika i procedura informacijske sigurnosti.
- *Analiza rizika* – procijeniti rizike za sigurnost osobnih podataka uzimajući u obzir učinak na zaštitu podataka i prava pojedinaca te odgovoriti na identificirane rizike.

[85] ICO, loc.cit., (bilj. 78)
[86] EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, Version 2.0, Adopted on 20 October 2020: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, 15.rujna 2022.

- *Sigurnost prema dizajnu* – Razmotriti sigurnosne zahtjeve što je ranije moguće u dizajnu sustava i njegovu razvoju te kontinuirano integrirati i provoditi potrebne testove.
- *Održavanje* – Redovita analiza i evaluacija te testiranje softvera, hardvera, sustava i ostalih usluga, da bi otkrili ranjivosti sustava koji podržavaju obradu.
- *Upravljanje kontrolom pristupa* – Samo ovlašteno osoblje koje treba imati pristup može imati pristup osobnim podatcima, a voditelj obrade bi trebao moći diferencirati između povlastica pristupa ovlaštenog osoblja pa razlikujemo ograničenje s obzirom na osobe i sadržaj. S obzirom na osobe, obradu podataka treba oblikovati da što manji broj osoba ima pristup podacima da bi vršili svoju zadaću te treba segregirati pristup na način da nitko, pojedinačno, nema pristup svim podacima ispitanika. S obzirom na sadržaj, u kontekstu svake obrade treba procesirati minimalan sadržaj potreban za tu radnju.
- *Sigurni prijenosi* – Prijenosi trebaju biti osigurani od neovlaštenog i slučajnog pristupa i promjena.
- *Sigurna pohrana* – pohrana podataka mora biti zaštićena od neovlaštenog pristupa i promjena. Trebaju postojati postupci za procjenu rizika centralizirane ili decentralizirane pohrane i kategorija osobnih podataka na koje se ovo odnosi. Neki podaci mogu zahtijevati dodatne sigurnosne mjere ili bi trebali biti izolirani od drugih podataka.
- *Pseudonimizacija* – Osobni podaci i sigurnosne kopije trebaju biti pseudonimizirani kao sigurnosna mjera za smanjenje rizika potencijalnih povreda podataka, primjerice uporabom enkripcije.
- *Sigurnosne kopije/ dnevnici logiranja* - Potrebno je čuvati sigurnosne kopije i dnevnike logiranja u onoj mjeri koja je potrebna za sigurnost informacija. Oni moraju

biti zaštićeni od neovlaštenog i slučajnog pristupa i promjene te redovito pregledavani,a na povrede treba reagirati odmah.

- *Oporavak od nepogode/ kontinuitet poslovanja* – Na potencijalnu nepogodu odnosno povredu potrebno je reagirati adresiranjem informacijskog sustava za slučaj nepogode i zahtjeva za kontinuitetom poslovanja kako bi se ponovno uspostavila dostupnost osobnih podataka.
- *Zaštita prema riziku* – Sve kategorije osobnih podataka trebaju biti zaštićene mjerama primjerenima riziku od povrede sigurnosti. Podaci kojima prijeti poseban rizik trebaju, kada je to moguće, biti odvojeni od ostalih osobnih podataka.
- *Upravljanje odgovorom na sigurnosne incidente* – Potrebno je uspostaviti rutine, procedure i resurse za otkrivanje, obuzdavanje, rukovanje, prijavljivanje i učenje u slučaju povreda podataka.
- *Upravljanje incidentima* – Voditelj obrade bi trebao imati uspostavljene procese za rješavanje povreda i incidenata. Ovo uključuje procedure o obavještavanja nadzornog tijela i ispitanika.

Voditelj obrade bi uspostavljanjem ovih sigurnosnih mjera osigurao poštivanje načela cjelovitosti i povjerljivosti i spriječio daljnje povrede izazvane kibernetičkim napadima te takvim sofisticiranim i izdržljivim sustavom minimizirao učinak eventualno nastalih povreda, a istovremeno stekao povjerenje ispitanika i osigurao zaštitu podataka.

3.1.5. Sudjelovanje drugih pojedinaca u obradi podataka

Preporuke AZOP-a ne odnose se samo na voditelje i izvršitelje obrade već i na ostale osobe koje imaju pristup osobnim podacima odnosno koje djeluju prema uputama voditelja i izvršitelja. U tom smislu i stavak 4. članka 32. kaže: „*Voditelj obrade i izvršitelj obrade poduzimaju mjere kako bi osigurali da svaki pojedinac koji djeluje pod odgovornošću*

voditelja obrade ili izvršitelja obrade, a koji ima pristup osobnim podacima, ne obrađuje te podatke ako to nije prema uputama voditelja obrade, osim ako je to obvezan učiniti prema pravu Unije ili pravu države članice.“[87] Ovaj članak treba čitati i tumačiti zajedno sa člankom 28. Uredbe koji specificira odgovornosti izvršitelja obrade i konkretno u stavku trećem točki b kaže da izvršitelj obrade: „*..osigurava da su se osobe ovlaštene za obradu osobnih podataka obvezale na poštovanje povjerljivosti ili da podliježu zakonskim obvezama o povjerljivosti*.“ U tom smislu, kriterij i obveza povjerljivosti odnosi se i na sve ostale koji tokom svoga rada dođu u doticaj sa osobnim podacima te je ona jednaka onoj voditelja i izvršitelja. Treći koji vrše obradu za voditelja ili izvršitelja ne bi smjeli ni na koji način osujetiti njihovu poziciju.[88] Članak 28. odnosi se na odnos izvršitelja i voditelja obrade kroz poštivanje svih načela no prvenstveno načela sigurnosti jer želi osigurati njegovu primjenu kod izbora izvršitelja i njegova djelovanja sve do nižih razina pod-izvršitelja obrade.[89] Tako ono kontrolira izbor voditelja obrade pri angažiranju izvršitelja da bi se osigurala obrada podataka od strane kompetentnih izvršitelja koji mogu jamčiti zadovoljavajuću stručnost pri obradi podataka, odnosno koji mogu jamčiti obradu koja je u potpunosti u skladu sa zahtjevima Opće uredbe; „*Ako se obrada provodi u ime voditelja obrade, voditelj obrade koristi se jedino izvršiteljima obrade koji u dovoljnoj mjeri jamče provedbu odgovarajućih tehničkih i organizacijskih mjera na način da je obrada u skladu sa zahtjevima iz ove Uredbe i da se njome osigurava zaštita prava ispitanika*.“[90] Kako bi ispunili svoju obvezu iz stavka četvrtog članka 32., voditelji obrade i izvršitelji obrade trebali bi uspostaviti jasna pravila ponašanja, interne upute i postupke sankcioniranja. U određenim slučajevima bitne su i tehničke mjere koje

[87] Opća uredba, op. cit. (bilj. 2), čl. 32. t. 4
[88] Ustaran, op. cit. (bilj. 8), Poglavlje 10.2.2.
[89] Ibid., Poglavlje 10.2.3.
[90] Opća uredba, op. cit. (bilj. 2), članak 28. st. 1.

sprječavaju neovlašteni pristup.[91]

3.1.6. Povreda osobnih podataka

Povreda osobnih podataka je: „*kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani*.“[92] Zanimljivo je istaknuti kako usporedbom članka petog Uredbe, koji definira načelo cjelovitosti i povjerljivosti, i definicije povrede iz članka četvrtog ne nalazimo potpuno preklapanje. Naime, članak 5. Uredbe ne spominje „izmjenu“ podataka, a normativnim tumačenjem članka 4. da se zaključiti da se povredom smatra samo ona povreda koja dovodi do negativnog ishoda, izostavljajući potencijalni rizik za čijim sprječavanjem ide načelo cjelovitosti i povjerljivosti.[93] Stoga iako ne dolazi do potpunog preklapanja ideja ovih dvaju članaka treba ih tumačiti zajedno kako bi se cjelovito pristupilo zaštiti podataka i spriječilo povredu. Vrste povreda možemo klasificirati kao: „povrede povjerljivosti”, „cjelovitosti“ i „dostupnosti“. O povredi povjerljivosti radilo bi se u slučaju neovlaštenog ili slučajnog otkrivanja osobnih podataka ili pristupa tim podacima, o povredi cjelovitosti u slučaju neovlaštene ili slučajne izmjene osobnih podataka, a o povredi dostupnosti u slučaju slučajnog ili neovlaštenog gubitka pristupa osobnim podacima ili uništenja tih podataka.[94]

3.1.7. Izvješćivanje nadzornog tijela o povredi osobnih podataka

Ukoliko dođe do povrede osobnih podataka Opća uredba propisuje obvezu voditelja obrade o izvješćivanju nadzornog tijela o toj povredi osim ako nije vjerojatno da će povreda prouzročiti

[91] Vidi izvor: https://gdprhub.eu/index.php?title=Article_32_GDPR#.284.29_Natural_Persons_Acting_under_the_Authority_of_the_Controller_or_the_Processor, 15. rujna 2022.
[92] Opća uredba, op. cit. (bilj. 2), čl. 4. st.1. t. 12
[93] Ustaran, op. cit. (bilj. 8), Poglavlje 10.3.1
[94] AZOP; https://azop.hr/rjesavanje-povreda-osobnih-podataka/, 17.rujna 2022.

rizik za prava i slobode pojedinaca.[95] Osim obveze voditelja obrade, Uredba propisuje i obvezu izvršitelja da obavijesti voditelja o povredi bez nepotrebnog odgađanja.[96] Transparentnost u slučaju povrede podataka od pozitivnog je utjecaja na djelovanje voditelja i izvršitelja obrade jer im omogućava veći stupanj pažnje i poticaj ka poboljšanju svojih organizacijskih i tehnoloških mjera kojima štite podatke. Također im omogućuje bolji uvid u eventualne propuste na koje će, u slučaju buduće opasnosti povrede, imati spremne sustave zaštite podataka i k tome spriječiti nove povrede. U tom smislu, transparentnost olakšava i zadaću nadzornih tijela koja dobivaju informacije na temelju kojih mogu djelovati, a i potiče javnost na budnost i pažnju kada su u pitanju osobna prava i njihova zaštita.[97]

Neki autori smatraju kako postoji opasnost izbjegavanja obveze izvješćivanja nadzornog tijela od strane voditelja obrade, s obzirom da Uredba propisuje tu obvezu u trenutku kada je do povrede već došlo, dakle nakon što se povreda dogodila, a čak ni tada ukoliko voditelj obrade procijeni da prava i slobode pojedinaca nisu ugrožene. Dapače, situacija da voditelji obrade ni ne poduzmu mjere kojima će detektirati povredu, moguća je ukoliko žele izbjeći obavještavanje nadzornog tijela i moguće sankcije.[98] Dakako, u tom slučaju izložili bi se i većem riziku jer bi time direktno kršili načelo cjelovitosti i povjerljivosti. AZOP navodi primjer povrede u kojoj obveza izvješćivanja ne bi postojala jer nije izgledno da bi takva povreda uzrokovala ugrozu prava i sloboda pojedinaca:“ *Povreda povodom koje se ne bi zahtijevalo obavješćivanje nadzornog tijela bila bi gubitak šifriranog mobilnog uređaja kojim se koristi voditelj obrade i članovi njegova osoblja. Pod uvjetom da ključ za šifriranje ostane u sigurnom posjedu voditelja obrade i da se ne radi o jedinoj kopiji tih osobnih podataka, osobni podaci bili bi nedostupni napadaču. To znači da nije vjerojatno da će povreda prouzročiti rizik za prava i slobode predmetnih ispitanika. Ako kasnije postane očito da je*

[95] Ibid.
[96] Opća uredba, op. cit. (bilj. 2), članak 33. st. 2.
[97] Ustaran, op.cit. (bilj. 8), Poglavlje 10.3
[98] Ibid., Poglavlje 10.3.2

ključ za šifriranje ugrožen ili da računalni program ili algoritam za šifriranje ima slabih točaka, promijenit će se rizik za prava i slobode pojedinaca pa će se stoga možda zahtijevati obavješćivanje.“[99] Nakon što dođe do povrede, voditelj obrade mora brzo djelovati i u roku od 72 sata obavijestiti nadzorno tijelo, ako je istovremeno došle do moguće ugroze na prava ispitanika. Upravo zbog vrlo kratkog roka u kojem voditelj obrade mora reagirati iznimno je važno da ima ustanovljene strategije odgovora na povredu. Primjeri strategije uključuju: ustanovljen plan djelovanja u slučaju povrede, priručnik za djelovanje u slučaju povrede, ustanovljivanje timova i centra za operacijsku sigurnost.[100] Razumno je očekivati da s obzirom na težinu povrede neće svaki voditelj obrade moći obavijestiti nadležno tijelo u roku od 72 sata pa Uredba daje prostora i postupnom pružanju informacija.[101] Izvršitelj obrade prema članku 33. stavku 2., ima obvezu izvještavanja voditelja obrade o nastaloj povredi jer iako voditelj zadržava opću odgovornost za zaštitu osobnih podataka, izvršitelj obrade ima važnu ulogu u omogućivanju voditelju obrade da pravilno izvrši svoju zadaću.[102] Konačno, stavak peti članka 33. Uredbe konstatira obvezu voditelja obrade da dokumentira svaku povredu osobnih podataka, okolnosti povrede i mjere koje su bile poduzete kao reakcija na povredu. Dokumentacija koju je voditelj dužan uredno voditi suštinski će imati ulogu obavijesti prema nadzornom tijelu koja će ukazati na poštivanje odnosno nepoštivanje ovih odredaba. Za očekivati je da će prilikom provođenja nadzora rada voditelja obrade u slučaju povrede, nadzorno tijelo tražiti uvid i u dokumentaciju o prijašnjim povredama, stoga ju treba pohraniti na neodređeno vrijeme i učiniti dostupnom.[103]

[99] AZOP; https://azop.hr/rjesavanje-povreda-osobnih-podataka/, 17. rujna 2022.
[100] Ustaran, op.cit. (bilj. 8), 10.3.2.
[101] Opća uredba, op.cit. (bilj. 2), članak 33. st. 4.
[102] AZOP, loc.cit.
[103] Ustaran, Eduardo, loc.cit.

3.1.8. Obavještavanje ispitanika o povredi osobnih podataka

Osim obveze izvješćivanja nadzornog tijela, Uredba propisuje i obvezu obavještavanja ispitanika o povredi osobnih podataka, ukoliko je izgledno da će takva povreda uzrokovati *visoki* rizik za prava i slobode pojedinaca.[104] Uredba je postavila viši prag naspram članka 33. st.1. gdje se traži samo činjenica da postoji „rizik za prava i slobode pojedinaca." Recital 75 Uredbe kaže da se ozbiljnost rizika za prava i slobode ispitanika treba određivati s obzirom na prirodu, opseg, kontekst i svrhe obrade te da bi rizik bi trebalo procjenjivati na temelju objektivne procjene.[105] Primjenjujući Recitale 75 i 76 Uredbe prag rizika se može determinirati kvalitativno, s obzirom na povredu prema određenoj vrsti podataka ili kvantitativno, prema zahvaćenom broju ispitanika u svakom pojedinom slučaju. Ako se uzme primjer da povreda prouzroči curenje informacija o e-mail adresama velikog broja ispitanika to ne predstavlja visoki rizik za prava i slobode pojedinaca, s obzirom da je uobičajeno da pojedinci često dijele svoje e-mail adrese te bi ovakva povreda uzrokovala samo obvezu obavijesti nadzornom tijelu[106], no ako bi se radilo o manjem broju ispitanika i povredi s obzirom na posebnu kategoriju podataka, takva povreda bi iziskivala obavijest ispitanicima. Prilikom obavještavanja pojedinaca potrebna je uporaba jasnog i jednostavnog jezika te barem sljedeće informacije:

- opis prirode povrede;
- ime i kontaktne podatke službenika za zaštitu podataka ili drugu kontaktnu osobu;
- opis vjerojatnih posljedica povrede;

[104] Opća uredba, op. cit. (bilj. 2), članak 34.st.1.
[105] Ibid., Recital 75
[106] Ustaran, op. cit. (bilj. 8), Poglavlje 10.3.3

- opis poduzetih mjera ili predloženih mjera koje treba poduzeti voditelj obrade kako bi riješio povredu, uključujući, kada je to prikladno, mjere za ublažavanje njenih mogućih negativnih učinaka.[107]

Stavak 3. članka 34. navodi tri slučaja kada obavijest ispitaniku nije potrebna. Ova odredba upućuje na mogućnost izbjegavanja obveze da se ispitanik obavijesti o povredi ako su poduzete mjere kojima je spriječena ili umanjena mogućnost štetnih posljedica. Također ukazuje na institut „*encryption safe harbor*“ odnosno institut „sigurne luke enkripcije“, koji je poznat u svijetu kibernetičke sigurnosti.[108] Naime s obzirom da se enkripcijom osobni podaci ne mogu povezati sa ispitanikom jer su nerazumljivi, ovo omogućuje voditelju obrade da izbjegne obvezu odaslanja obavijesti o povredi ispitaniku te da prikaže sigurnosni događaj kao "incident" umjesto da proglasi da je došlo do povrede te tako oslobađa voditelja obrade od troškova i poniženja.[109] U slučaju povrede kojom je zahvaćen veliki broj ispitanika gdje bi bilo nerazumno očekivati da će voditelj obrade moći identificirati i obavijestiti sve ispitanike, može se izdati javna obavijest u tisku ili na web stranicama.[110] Stavak 4. članka 34. omogućuje nadzornim tijelima intervenciju i u slučaju da je voditelj obrade propustio izvijestiti o povredi sukladno odredbama članka 33. Intencija zakonodavca bila je u tome da se ispitanicima pruže informacije o koracima koje oni trebaju poduzeti kako bi zaštitili sami sebe, a istovremeno spriječiti zamor ispitanika nepotrebnim obavijestima.

3.1.9. Certifikati i kodeksi ponašanja

Opća Uredba potiče uspostavu mehanizama certificiranja zaštite podataka u svrhu dokazivanja da su postupci obrade koje provode voditelj obrade i izvršitelj obrade u skladu s

[107] Opća uredba, op. cit. (bilj. 2), 34. St. 2
[108] Ustaran, loc. cit.
[109] Porch, Alice M., *Safe Harbor From Data Breach Notification*, Cyber Law Blog, https://www.amp.legal/blog/safe-harbor-from-data-breach-notification/, 17.rujna 2022.
[110] Ustaran, loc.cit.

Uredbom.[111] Certifikate izdaju nadležna nadzorna tijela za zaštitu osobnih podataka kao i akreditirana certifikacijska tijela. U Hrvatskom zakonodavstvu Zakon o provedbi Opće uredbe uspostavio je Hrvatsku akreditacijsku agenciju kao nadležno tijelo.[112] EZOP je tijelo koje izdaje kriterije za certifikaciju. Osim certifikata Uredba potiče i izradu Kodeksa ponašanja koji mogu poslužiti pri dokazivanju usklađenosti sa Uredbom, odnosno osigurati njenu precizniju primjenu, između ostalog i u pogledu izvješćivanja nadzornih tijela o povredama osobnih podataka i obavješćivanja ispitanika o takvim povredama kao i o pseudonimizaciji.[113]

3.1.10. Položaj i kompetencije službenika za zaštitu osobnih podataka

Dok Direktiva o zaštiti podataka iz 1995. nije izričito regulirala ulogu službenika za zaštitu podataka, ona nije nepoznata u zakonima o zaštiti podataka u državama članicama EU. Nacionalni zakoni o zaštiti podataka, primjerice u Njemačkoj, usvojili su odredbe o službeniku za zaštitu podataka početkom već kasnih 1970-ih. Odatle su se ove odredbe proširile na pravne sustave mnogih članica EU, posebno u prvom desetljeću 21. stoljeća.[114] Pravni okviri nacionalnih zakonodavstava varirali su, tako primjerice hrvatski Zakon o zaštiti podataka pri propisivanju odredbi o službeniku za zaštitu podataka (dalje u tekstu: Službenik) nije uzeo u obzir prirodu, opseg i obujam osobnih podataka koje voditelj obrade obrađuje, već se orijentirao na broj zaposlenih voditelja obrade kao kriterij o tome je li potrebno imenovati i službenika za zaštitu podataka.[115] S obzirom da je ovakav pristup neminovno dovodio do situacija gdje se vršila obrada posebnih kategorija podataka bez sudjelovanja Službenika, Opća uredba detaljno propisuje imenovanje, položaj, skup vještina i zadaće službenika za

[111] Opća uredba, op.cit. (bilj. 2), članak 42.st.1.
[112] Zakon o provedbi Opće uredbe o zaštiti podataka, op. cit., (bilj. 18), članak 5.
[113] Ibid., članak 40.
[114] Katulić, Tihomir, Katulić Anita, *Competences, Position and Role of Data Protection Officers in Ensuring Library Data Protection Compliance*, FLA CPDWL Satellite Meeting 2019. Zagreb, 2019., str.5.: https://repozitorij.nsk.hr/islandora/object/nsk:246, 14. listopada, 2022.
[115] Ibid.

zaštitu podataka u člancima od 37. do 39.[116] Umjesto kvantitativnih kriterija, voditelj obrade sada mora odrediti službenika za zaštitu podataka ako obrada koju vrši zadovoljava kvalitativne kriterije koji se odnose na prirodu, opseg i obujam obrade.[117] Iako Uredba ne definira potrebnu razinu stručnosti, to je vidljivo iz Smjernica[118] koje upućuju na to da razina stručnosti mora biti proporcionalna složenosti i količini osobnih podataka koji se obrađuju. Primjenjuju se i dodatni čimbenici, primjerice ako se osobni podaci sustavno ili povremeno prenose izvan Europske unije, odnosno ako osobni podaci spadaju u posebnu kategoriju podataka.[119] Uloga Službenika u osiguravanju poštivanja načela zaštite podataka i prava i sloboda ispitanika od vitalnog su značaja pa bi on trebao posjedovati visoku razinu osobnog integriteta i profesionalne etike. Za razliku od prethodnog pravnog okvira koji nije predviđao imenovanje vanjskog Službenika, Uredba sada izričito dopušta imenovanje službenika koji nije zaposlen kod voditelja obrade te se njegova usluga može ugovoriti.[120] Unutar organizacije, službenici za zaštitu podataka trebali bi moći obavljati svoje dužnosti s dovoljnim stupnjem neovisnosti, a voditelji i izvršitelji ne smiju kazniti Službenika zbog vršenja njegovih dužnosti.[121] Smjernice Radne skupine 29 preporučuju da bi svaka organizacija koja ima obvezu imenovanja službenika za zaštitu podataka, trebala identificirati položaje zaposlenika koji nisu kompatibilni sa funkcijom Službenika. Također bi trebala stvoriti pravila za izbjegavanje sukoba interesa, a ako zaposlenik sudjeluje u donošenju odluka u vezi s prirodom i svrhom obrade, takve pozicije treba smatrati pozicijama sa sukobom interesa te takvi zaposlenici ne mogu djelovati kao neovisni i objektivni službenici za zaštitu podataka.[122]

[116] Ibid.
[117] Ibid.
[118] WP29 *Guidelines on Data Protection Officers*, WP243 16/EN, objavljene 13. prosinca, 2016.
[119] Katulić, op.cit., (bilj. 114), str.7.
[120] Ibid.
[121] Ibid.
[122] Ibid., str. 8.

3.2. Načelo cjelovitosti i povjerljivosti kroz praksu

Imajući na umu važnost načela cjelovitosti i povjerljivosti te s obzirom je da ono akcent ovog rada potrebno je prikazati primjenu istog u praksi. Europska nadzorna tijela ovlaštena su provoditi nadzor i izricati upravne novčane kazne voditeljima obrade u slučaju povrede osobnih podataka. S obzirom na okolnosti, kazne mogu iznositi 10 000 000 EUR ili do 2% od ukupnog godišnjeg prometa, što god je veće ili 20 000 000 EUR ili do 4% ukupnog godišnjeg prometa, što god je veće.[123]

3.2.1. Slučaj CNIL-SAN-2019-005[124]

U ovom slučaju iz 2018.godine francusko nadzorno tijelo „CNIL“[125] izreklo je novčanu kaznu voditelju obrade u iznosu od 400.000 EUR zbog povreda prava i sloboda ispitanika uzrokovanih kršenjem načela cjelovitosti i povjerljivosti odnosno, članka 32. Uredbe o sigurnosti. Povreda je bila izuzetno ozbiljna pa je ovaj slučaj CNIL odlučio javno objaviti kako bi ukazao na važnost pridržavanja odredaba o sigurnosti, s obzirom da se radilo o iznimno osjetljivim i preciznim podacima ispitanika koji su pretrpjeli povredu. Naime, korisnik usluga Agencije za nekretnine „SERGIC“, (nadalje Agencija), uočio je da je online usluga kojom je Agencija prikupljala zahtjeve zainteresiranih kupaca nezaštićena na način da se promjenom jednog ili više znakova URL adrese može pristupiti podacima ostalih klijenata Agencije. Korisnik je nakon tog saznanja u ožujku 2018. godine obavijestio Agenciju o propustu te podnio zahtjev CNIL-u u kolovozu iste godine koji je idući mjesec započeo nadzor. Pitanja koja su se postavila tijekom nadzora su:

[123] Opća uredba, op. cit. (bilj. 2), članak 83.
[124] Vidi izvor: https://gdprhub.eu/CNIL_-_SAN-2019-005, 18.rujna 2022.g.
[125] Franc.: „Commission nationale informatique et des libertés“

a. Je li došlo do povrede načela povjerljivosti ukoliko su osobni podaci javno dostupni na web-u kroz nezaštićenu URL adresu? te
b. je li došlo do povrede načela ograničenja pohrane zbog zadržavanja osobnih podataka nakon što je sklopljen ugovor o najmu?

Tijekom istrage, ovlaštene osobe prikupile su 9, 446 (devet tisuća četiristo četrdeset i šest) dokumenata na način na koji je ukazao korisnik koji je otkrio ovaj propust. Dokumenti su između ostalog bili: osobne iskaznice, vjenčani i smrtni listovi, porezni dokumenti, izvodi iz banaka, podaci o policama zdravstvenog osiguranja, presude o razvodu braka itd. Isto tako, utvrđeno je da se može pristupiti cjelokupnoj bazi podataka Agencije jer nikakve tehničke i organizacijske mjere nisu primijenjene kako bi se osobni podaci uklonili. CNIL je obavijestio Agenciju o propustu 7.rujna 2018.godine, a obavio inspekcijski nadzor u prostorijama Agencije šest dana kasnije. Nadzorno tijelo ustvrdilo je da Agencija i dalje nije ispravila ukazani propust te je do povrede došlo zbog manjkavog dizajna web stranice koja nije imala integriranu opciju o autentifikaciji prilikom pristupanja određenim podacima što je direktna povreda članka 32. Uredbe. Nadzorno tijelo ustvrdilo je da Agencija nije ispravila propust nakon što je bila obaviještena već u ožujku 2018.godine jer više od šest mjeseci nije poduzela tehničke i organizacijske mjere kojima bi spriječila povredu podataka. Time je prekršila načelo cjelovitosti i povjerljivosti i dopustila da treći imaju pristup izuzetno privatnim i intimnim osobnim podacima ispitanika uslijed čega su prava i slobode pojedinaca pretrpjele ugrozu. Nadzorno tijelo ukazalo je na važnost implementacije primjerenih mjera pogotovo zbog već spomenute osjetljivosti podatka kojima je Agencija raspolagala. CNIL je uzeo u obzir vrstu, ozbiljnost i trajanje povrede, mjere koje je poduzeo voditelj obrade da bi smanjio posljedice povrede, okolnosti povrede i ostale važne faktore te prvotno predložio kaznu u visini od 900.000 EUR, no nakon prigovora Agencije i uzimajući u obzir njene prihode, kazna

je smanjena u skladu za zahtjevom proporcionalnosti te se smatra ujedno i odvračujućom i učinkovitom prema zahtjevima Uredbe.

3.2.2. Slučaj CNIL – SAN-2020-014[126]

Krajem rujna 2019. godine CNIL je izrekao novčanu kaznu od 3000 EUR doktoru koji je propustio poduzeti tehničke i organizacijske mjere zaštite osobnih podataka svojih pacijenata. CNIL je shodno zahtjevu koji je zaprimio poduzeo online provjeru te ustvrdio da se putem interneta može pristupiti tisućama fotografija medicinske naravi koje su pohranjene na serveru doktora u pitanju. Pitanja koja su se postavila tokom nadzora bila su:

1. Je li korištenje „otvaranja portova“ (eng. Port forwarding)[127], u svrhu daljinskog pristupa zdravstvenim podacima, povreda odredaba članka 32. Uredbe?
2. Je li činjenica da nije korištena enkripcija u svrhu zaštite podataka povreda članka 32. Uredbe? te
3. Oslobađa li okolnost, da je CNIL bio taj koji je doktora obavijestio o povredi, od obveze izvješćivanja nadzornog tijela propisane člankom 33. Uredbe?

Prilikom saslušanja, doktor je pojasnio da bi se mogao služiti zdravstvenim podacima pohranjenima na svom kućnom tvrdom disku trebao je otvoriti portove kako bi omogućio rad VPC-u.[128] CNIL je ustvrdio kako doktor nije koristio enkripciju kao mjeru zaštite osobnih podataka pacijenata koji spadaju u posebnu kategoriju podataka u smislu članka 9. Opće uredbe[129] te se nije držao ni smjernica koje je CNIL propisao u „Praktičnom priručniku za liječnike“. Podaci su bili nezaštićeni tijekom razdoblja od četiri mjeseca te su osim fotografija

[126] Vidi izvor: https://gdprhub.eu/index.php?title=CNIL_-_SAN-2020-014, 18. rujna 2022.g.
[127] Port forwarding omogućuje računalima ili uslugama u privatnim mrežama da se preko interneta povežu s drugim javnim ili privatnim računalima ili uslugama; https://learn.g2.com/port-forwarding, 19.rujna 2022.g.
[128] Virtualni privatni oblak, (eng. Virtual private cloud)
[129] Opća uredba, op.cit. (bilj. 2), članak 9.

uključivali i imena i prezimena pacijenata, njihov datum rođenja, datum i mjesto obavljenih pregleda te imena zaposlenika koji su obavili preglede. Ne koristeći se tehničkim i organizacijskim mjerama propisanima člankom 32., doktor je počinio povredu načela sigurnosti. Nadzorno tijelo nalazi i da je doktor počinio povredu članka 33. stavka 1. Uredbe jer nije izvijestio o povredi. Osim novčane kazne, CNIL je odlučio i javno objaviti ovaj slučaj s obzirom na osjetljivost podataka te učestalost povrede osobnih podataka u sferi privatnih liječnika. Ovaj slučaj povezan je sa slučajem SAN-2020-015 gdje je još jednom privatnom liječniku izrečena kazna i to u iznosu od 6000 EUR.[130]

3.2.3. Slučaj AEPD (Spain) - PS-00246-2022[131]

Ovaj recentni slučaj iz 2021.godine odnosi se na Proizvođača edukativnih časopisa za djecu (voditelj obrade) kojeg je španjolsko nadzorno tijelo AEPD kaznilo u iznosu od 31.200 EUR zbog povrede osobnih podataka koja se dogodila uslijed manjkavosti web stranice. U listopadu 2021. godine voditelj obrade zaprimio je e-mail od osobe nadležne za održavanje web stranice voditelja, u kojem je voditelj obrade obaviješten o sigurnosnom propustu gdje je treća osoba uspjela pristupiti podacima voditelja. Voditelj obrade je nakon toga izvršio internu provjeru te utvrdio da se radi o tzv. etičkom hakiranju bez maliciozne nakane. Povredom je zahvaćeno više od 470 000 osoba, a osobni podaci koji su bili u pitanju su kontaktni podaci i podaci o lokaciji. Povodom ovog saznanja, voditelj obrade je obavijestio zahvaćene osobe o povredi putem e-maila. Jedan od ispitanika podnio je zahtjev AEPD-u. Nadzorno tijelo utvrdilo je da su osobni podaci ispitanika bili neovlašteno obrađivani te je stoga nastupila povreda načela cjelovitosti odnosno članka 5.st.1.t.f Uredbe.[132] Osim toga, zbog propuštanja implementiranja tehničkih i organizacijskih mjera došlo je i do povrede članka 32. Uredbe.[133]

[130] Vidi: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042676787
[131] Vidi izvor: https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS-00246-2022, 19.rujna 2022.g.
[132] Opća uredba, op. cit. (bilj. 2), članak 5.st.1.t.f.
[133] Ibid., članak 32.

Voditelj obrade ukazao je na sredstvo kojim se poslužio pri procjeni učinka na zaštitu podataka, no AEPD je utvrdio da ne postoji korelacija između mjera koje je voditelj poduzeo i provedene procjene učinka, a poglavito zbog činjenice da je povreda zahvatila i osobne podatke maloljetne djece. U tom smislu, ne može se konstatirati da je voditelj obrade ispunio svoju dužnost iz članka 32. Konačno, AEPD je ustvrdio i povredu članka 33. Uredbe koji se odnosi na izvješćivanje nadzornog tijela od stane voditelja obrade, zbog činjenice da je voditelj obrade obavijestio o povredi dva tjedna nakon što se ona dogodila, točnije tek sredinom studenog 2021.godine. Nadzorno tijelo izreklo je kaznu u iznosu od 52.000 EUR, no kasnije preinačilo odluku, s obzirom da je voditelj obrade sam dobrovoljno uplatio dio novčane kazne, i reduciralo ju na 31.200 EUR. Zanimljivo je u odnosu na prethodne slučajeve da španjolsko nadzorno tijelo radi djelomičnu distinkciju između načela cjelovitosti i povjerljivosti i članka 32. koji sadrži odredbe o sigurnosti. Iako to izrijekom ne spominje, samim time što navodi dva različita razloga odnosno povrede od kojih se jedna odnosi na članak. 5. st. 1. točku f, a druga na članak 32. možemo uvidjeti da je dilema oko tumačenja tih odredaba Uredbe i dalje pendentna. Naime, iako su te odredbe nesumnjivo spojive i sinergične, u pravno-znanstvenoj literaturi i praksi ne postoji izričit i suglasan odgovor na pitanje istovjetnosti načela cjelovitosti i povjerljivosti i načela sigurnosti.

3.2.4. Praksa hrvatske Agencije za zaštitu osobnih podataka[134]

Hrvatsko nazdzorno tijelo AZOP izreklo je iznimno visoku novčanu kaznu od 675.000 HRK trgovačkom društvu koje je povrijedilo članak 32. st. 1. točke b) i d) kao i stavke 2. i 4. istog članka Uredbe. Ova povreda predstavlja povredu načela sigurnosti jer su osobni podaci ispitanika bili javno objavljeni na društvenim mrežama i u medijima. Društvo je dostavilo izvješće AZOP-u u kojem je objasnilo okolnosti povrede, odnosno pojasnilo kako su

[134] AZOP: https://azop.hr/izrecene-upravne-novcane-kazne-u-ukupnom-iznosu-od-1-6-milijuna-kuna/, 20. listopada, 2022.

zaposlenici Društva prekršili interne upute i akte te mobilnim uređajem snimili snimku videonadzora koja je nakon toga procurila u javnost i ostala dostupna u medijima i na društvenim mrežama. Agencija je ustvrdila kako društvo nije poduzelo odgovarajuće tehničke i organizacijske mjere ni prije ni nakon incidenta,a da bi njihovom primjenom bilo moguće svesti povredu i rizike za prava ispitanika na minimalnu razinu. Propust Društva kao voditelja obrade je i u tome da nije obavljao redoviti nadzor nad provedbom tehničkih i organizacijskih mjera kao što nije ni provodio testove učinkovitosti predviđenih mjera. Agencija je izricanjem visoke upravne novčane kazne ostvarila proporcionalan, odvraćujuć i učinkovit učinak u smislu odredaba Opće uredbe te ostvarila prevenciju budućih povreda.

4. ZAKLJUČAK

Danas živimo u svijetu u kojem je tehnologija neizbježan faktor koji utječe na svaki aspekt čovjekova života. Ne možemo zamisliti život bez naših džepnih suputnika koji nam u par klikova mogu reći gdje se nalazi najbliži restoran ili benzinska postaja, koje je radno vrijeme banke i koliko će nam vremena trebati do odredišta. Za vrijeme pandemije koja je zahvatila čitavu zemaljsku kuglu značaj tehnologije uspeo se na najvišu razinu u ljudskoj povijesti i omogućio koliku toliku „normalu“ za vrijeme svakakve, ali ne i baš normalne situacije. Iako je koncept rada na daljinu postojao i ranije, sada je sasvim česta i svakodnevna pojava. Nastava i rad na daljinu nadomjestili su tradicionalne modalitete rada. Cjelokupni život preselio se online, tako smo mogli iz udobnosti doma obaviti razgovor i dobiti savjet od liječnika, podnijeti zahtjev za kredit ili pak sudjelovati na sudskom ročištu. U vrijeme kada je odlazak u prodavaonicu predstavljao strah, kurirske usluge su doskočile i tome. Svijet je bio na tren stao, a tehnologija ga je ponovno pokrenula. U ovakvom svijetu nezamislivo je funkcionirati *off-grid* pa je stoga neizbježno da smo svi „izloženiji“ nego što smo bili prije. Današnji pametni telefoni trebaju otisak prsta i *face scan* da bi ispravno radili, lokacija

uređaja potrebna je za rad gotovo svih aplikacija, a telefoni znaju i kakvog smo zdravstvenog stanja i jesmo li pak previše „sjedilački tip“. Društvene mreže su sastavni dio života i svakodnevnica za mnoge, dapače neaktivnost na društvenim mrežama ponukati će bližnje da provjere je li sve u redu. Kako se onda u ovakvim okolnostima zaštititi od invazivnog zadiranja u privatnost po *default-u*? Vjerujemo li odgovornim osobama koje stoje iza aplikacija i usluga koje koristimo da su pažljivi s našim podacima, odnosno da će ih zaštititi ukoliko postanu ugroženi? Jesmo li uopće svjesni opasnosti koja vreba u tom neopipljivom svijetu interneta? Mnogi ni ne preispituju važnost zaštite podataka, ili pak pretpostavljaju da se ona podrazumijeva jer što je najgore što se može dogoditi? Djeca kao posebno osjetljiva skupina, prije su naučila kako otključati pametni telefon i naći „igricu“ nego što su naučila pisati. Uvjete korištenja aplikacija većina ni ne čita već svi spremno klikaju „prihvaćam“ samo kako bi mogli uživati u uslugama koje aplikacija nudi. Kako i kriviti ikoga kada smo de facto dovedeni u pat-poziciju. Ne možemo funkcionalno živjeti bez da svoje osobne podatke damo nekom drugom u ruke, doslovno. Neke države poput Saudijske Arabije imaju aplikacije koje su zakonom obavezne i koje prate lokaciju stanovnika u svakom trenutku. Pandemija je otvorila mnoga vrata još većem zadiranju u ljudsku privatnost i nema povrata. Iz primjera iz prakse navedenih *supra* vidimo da su i liječnici obavljali svoj rad na daljinu što je uzrokovalo povredu osobnih podataka tisuća ispitanika. Jesu li pacijenti mogli pretpostaviti da će njihovi osobni i privatni podaci plutati u bespućima interneta nezaštićeni? Sve do sada izloženo ukazuje koliku važnost načelo cjelovitosti i povjerljivosti ima, kao i cjelokupna Uredba. Opća uredba najinvazivniji je pravni korak ka zaštiti prava pojedinaca na privatnost, a posredno i na ljudsko dostojanstvo i integritet. Načelo sigurnosti osigurava da voditelji obrade poduzmu sve mjere kako bi zaštitili osobne podatke pojedinaca i spriječili i umanjili štetu koja može imati velike razmjere. Odgovornost osiguravaju i nadzorna tijela koja se ne libe izricati i iznimno visoke upravne kazne kako bi ukazali na važnost zaštite podataka koju propisuje Opća uredba

kroz svoje odredbe. Voditelji obrade svoju dužnost, koja živi kroz načelo cjelovitosti i povjerljivosti, moraju shvatiti ozbiljno. Nehaj ne ispričava. Uredba je svojim odredbama uistinu stavila teret na voditelje i izvršitelje obrade koji može izazvati financijska i druga opterećenja. Voditelji obrade moraju integrirati ne samo tehničke i organizacijske mjere nego ih uistinu oživjeti i to kroz rad svoga osoblja, kodeksima i pravilnicima na mjestu rada, obukama svih zaposlenika i strogim kontroliranjem provođenja istih. Također, pri izboru tehnologija ne mogu se voditi najdostupnijim i najlakšim izborom jer će posljedice biti puno skuplje ukoliko te tehnologije ne mogu ispuniti zadaću koje nalaže načelo sigurnosti. Gospodarski subjekti morat će prihvatiti multisidciplinarni i holistički pristup[135] i ne kritizirati pristup koji nalaže pravni okvir Uredbe. U striktno pravnom smislu ne bi bilo poželjno rangirati načela Uredbe po važnosti, no načelo cjelovitosti i povjerljivosti, odnosno njegova pertinencija što je načelo sigurnosti, nedvojbeno je jedno od važnijih načela Uredbe jer njegova težina leži u nepobitnoj činjenici da je naše temeljno ljudsko pravo na privatnost, u tuđim rukama.

[135] Ustaran, op.cit., (bilj. 8), Poglavlje 10.4

5. LITERATURA

1. Knjige:

1. Dragičević Dražen et al., Pravna informatika i pravo informacijskih tehnologija, Narodne novine, Zagreb, 2015, poglavlje V, 2018**.**

2. Gonzalez Fuster, Gloria, The emergence of personal data protection as a fundamental right of the EU, Springer International Publishing, Bruxelles, 2014.

3. Ustaran Eduardo, CIPP/E, Partner, Lovells, Hogan, European Data Protection: Law and Practice, IAPP Publication, Sjedinjene Američke Države, 2018.

2. Pravni izvori:

1. 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

2. (Europska) Konvencija za zaštitu ljudskih prava i temeljnih sloboda, MU 18/97, 6/99, 14/02, 13/03, 9/05, 1/06, 2/10, 13/17

3. Ustav Republike Hrvatske, Narodne Novine br. 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14

4. Zakon o provedbi Opće uredbe o zaštiti podataka, Narodne Novine br. 42/18

3. Članci:

1. Westin, Alan, Furman., Privacy and Freedom, Atheneum, New York, 1967.

2. Brandeis, Louis, The right to privacy, originally published in 4 Harvard Law Review 193, 1890. :https://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/the-right-to-privacy

4. Publikacije:

1. Malgieri, Gianclaudio, The concept of fairness in the GDPR; A linguistic and contextual interpretation, In Proceedings of FAT* on Fairness, Accountability, and Transparency, Barcelona, 2020.

2. Cavoukian, Ann, Privacy by design...take the challenge, Information and Privacy Commissioner of Ontario, Kanada, 2009.

3. Cavoukian, Ann, Privacy by design, The 7 Foundational Principles, Information and Privacy Commissioner of Ontario, Kanada, 2011.

4. Katulić, Tihomir, Protrka, Nikola, Information Security in Principles and Provisions of the EU Data Protection Law, 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2019.: https://www.bib.irb.hr/1014209

5. Katulić, Anita, Katulić Tihomir, Competences, Position and Role of Data Protection Officers in Ensuring Library Data Protection Compliance, FLA CPDWL Satellite Meeting Zagreb, 2019.: https://repozitorij.nsk.hr/islandora/object/nsk:246

6. EU Agency for Fundamental Rights, Handbook on european data protection law, 2018.: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

7. Radna skupina za zaštitu pojedinaca u vezi s obradom osobnih podataka, Smjernice o transparentnosti na temelju Uredbe 2016/679 od 11. travnja 2018.: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

8. Smjernice o zaštiti privatnosti i međunarodnom prijenosu osobnih podataka ,OECD, 1981.

9. EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020., 2020.: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

5. Internetski izvori:

1. Porch, Alice M., Safe Harbor From Data Breach Notification, Cyber Law Blog: https://www.amp.legal/blog/safe-harbor-from-data-breach-notification/

2. Agencija za zaštitu osobnih podataka: https://azop.hr/wp-content/uploads/2020/12/wp248_rev.01_hr-1.pdf

3. Agencija za zaštitu osobnih podatka: https://azop.hr/odluka-o-uspostavi-i-javnoj-objavi-popisa-vrsta-postupaka-obrade-koje-podlijezu-zahtjevu-za-procjenu-ucinka-na-zastitu-podataka/

4. Agencija za zaštitu osobnih podataka: https://azop.hr/osnovne-informacije-za-organizacije/

5. Agencija za zaštitu osobnih podataka: https://azop.hr/rjesavanje-povreda-osobnih-podataka/

6. Agencija za zaštitu osobnih podataka: https://azop.hr/wp-content/uploads/2022/05/RESOLUTION-108.pdf i https://azop.hr/spring-conference2022-dubrovnik-croatia/

7. Agencija za zaštitu osobnih podataka: https://azop.hr/izrecene-upravne-novcane-kazne-u-ukupnom-iznosu-od-1-6-milijuna-kuna/

8. GDPR hub, Odgovornost voditelja i izvršitelja obrade: https://gdprhub.eu/index.php?title=Article_32_GDPR#.284.29_Natural_Persons_Acting_under_the_Authority_of_the_Controller_or_the_Processor

9. GDPRhub, , CNIL: https://gdprhub.eu/index.php?title=CNIL_-_SAN-2020-014

10. GDPRhub, CNIL: https://gdprhub.eu/index.php?title=AEPD_(Spain)_-_PS-00246-2022

11. GDPRhub, CNIL: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042676787

12. GDPRhub, CNIL: https://gdprhub.eu/CNIL_-_SAN-2019-005

13. Information Commissioner's Office, What we do: https://ico.org.uk/about-the-ico/what-we-do/

14. Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/#fairness

15. Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/

16. Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/

17. Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/

18. Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

19. Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security

20. Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

21. Information Commissioner's Office: https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

22. Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

23. Enkripcija: https://bs.wikipedia.org/wiki/Enkripcija

24. Port forwarding: https://learn.g2.com/port-forwarding