Procjena učinka na zaštitu podataka u pravnom okviru i praksi u Europskoj uniji

Ivelja, Tamara

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Tamara Ivelja

PROCJENA UČINKA NA ZAŠTITU PODATAKA U PRAVNOM OKVIRU I PRAKSI U EUROPSKOJ UNIJI

SPECIJALISTIČKI RAD

Zagreb, 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Tamara Ivelja

PROCJENA UČINKA NA ZAŠTITU PODATAKA U PRAVNOM OKVIRU I PRAKSI U EUROPSKOJ UNIJI

SPECIJALISTIČKI RAD

Zagreb, 2024.

UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING
SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Tamara Ivelja

DATA PROTECTION IMPACT ASSESSMENT IN THE LEGAL FRAMEWORK AND PRACTICE OF THE EUROPEAN UNION

SPECIALIST THESIS
SPECIJALISTIČKI RAD

Zagreb, 2024

Specijalistički rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva u sklopu poslijediplomskog specijalističkog studija Informacijska sigurnost
Mentor: izv. prof. dr. sc. Tihomir Katulić

Specijalistički rad ima: 82 stranice
Specijalistički rad br.:_____.

Povjerenstvo za ocjenu u sastavu:

1. prof. dr. sc. Boris Vrdoljak – predsjednik
2. izv. prof. dr. sc. Tihomir Katulić, Sveučilište u Zagrebu Pravni fakultet - mentor
3. prof. dr. sc. Krešimir Fertalj - član

Povjerenstvo za obranu u sastavu:

1. prof. dr. sc. Boris Vrdoljak – predsjednik
2. izv. prof. dr. sc. Tihomir Katulić, Sveučilište u Zagrebu Pravni fakultet - mentor
3. prof. dr. sc. Krešimir Fertalj - član

Datum obrane: 12. srpnja 2024.

Za najbolju baku na svijetu.

Sažetak

Opća uredba o zaštiti podataka (OUZP) sadrži niz odredbi koje služe osiguravanju pouzdane, sigurne i povjerljive obrade osobnih podataka od strane voditelja obrade i izvršitelja obrade. Aktivnosti obrade osobnih podataka trebaju osigurati sustavnu zaštitu osobnih podataka i stvarnu mogućnost ostvarenja prava koja ispitanici prema OUZP imaju. Ti se zadaci ostvaruju odredbama Uredbe koje uređuju obveze voditelja i izvršitelja obrade. Među takvim odredbama ističe se uloga procjene učinka na zaštitu podataka kao instituta čija je zadaća sustavna analiza karaktera obrade osobnih podataka iz perspektive rizika za sigurnost i povjerljivost obrade.
Smisao procjene učinka je dokumentirati rizike za sigurnost obrade osobnih podataka te aktivnosti voditelja odnosno izvršitelja obrade kako bi se ti rizici uklonili ili sveli na prihvatljivu razinu. Provedba procjene učinka na zaštitu podataka je zakonom definirana obveza za voditelje obrade u slučaju novih, posebno rizičnih obrada ili u slučaju kad se mijenja karakter rizika za postojeće obrade. U praksi, voditelji obrade vode se smjernicama za provedbu procjene učinka koje pripremaju nadležna europska i nacionalna nadzorna tijela. Također, na raspolaganju su i specijalizirana digitalna rješenja kako bi se postigla ujednačena i kvalitetnija provedba ovih postupaka. Rad daje pregled praktičnih pitanja i izazova provedbe postupka procjene učinka na zaštitu podataka uz osvrt na neke od dostupnih digitalnih alata i njihovu primjenjivost. Također, dane su preporuke za unapređenja za bolju usklađenost s Općom uredbom po pitanju procjene učinka na zaštitu podataka.

Ključne riječi

Opća uredba za zaštitu podataka, temeljna prava ispitanika, načelo cjelovitosti i povjerljivosti, procjena učinka na zaštitu podataka, smjernice nacionalnih nadzornih tijela, digitalni alati procjenu učinka na zaštitu podataka.

Summary

The General Data Protection Regulation (GDPR) contains a number of provisions that are there to ensure a reliable, secure and confidential processing of personal data by the data controller and processor. Personal data processing activities should ensure the systematic protection of personal data and the real possibility of exercising the rights that data subjects have according to the GDPR. These tasks are carried out in accordance with the provisions of the Regulation, which regulate the obligations of the controller and processors. Among such provisions, the role of data protection impact assessment stands out as an institute. Its task is a systematic analysis of the nature of personal data processing from the perspective of security and confidentiality risks of processing data. The purpose of the impact assessment is to document the risks for the security of personal data processing, and the activities of the controller and processor, in order to eliminate or reduce these risks to an acceptable level. The implementation of an impact assessment on data protection is a legally defined obligation for controllers in the case of new, particularly risky processing, or in the case when the nature of the risk for existing processing changes. In practice, data controllers are guided by the impact assessment guidelines prepared by the competent European and national supervisory authorities. Also, specialized digital solutions are available in order to achieve uniform, high-quality implementation of these procedures.The paper provides an overview of the practical issues and challenges of implementing the data protection impact assessment procedure, with a review of some of the available digital tools and their applicability. Also, recommendations are given for improvements for better compliance with the General Regulation in terms of data protection impact assessment requirements.

Keywords

General Data Protection Regulation, fundamental rights of data subjects, principle of integrity and confidentiality, data protection impact assessment, guidelines of national supervisory authorities, data protection impact assessment digital tools.

SADRŽAJ

POPIS SLIKA

1 UVOD

Sveprisutna upotreba interneta te intenzivni razvoj i upotreba različitih digitalnih alata i usluga omogućili su velike društvene i ekonomske koristi[1], ali su također stvorili i potencijalne izazove na području zaštite privatnosti i osobnih podataka[2]. Razmatrajući kontekst suvremenog gospodarstva koji se sve više temelji na podacima, osobni podaci postali su izuzetno važan resurs koji se često koristi u poslovnim aktivnostima, osobito u analitičkim i marketinškim aktivnostima. Međutim, elementi intenzivne digitalizacije, kao i ekonomija temeljena na podacima, stvaraju okruženje s povećanim rizicima za privatnost i osobne podatke pojedinaca, proširujući mogućnosti za neovlašteno stjecanje i manipulaciju osobnim podacima, što između ostalog kompromitira njihovu povjerljivost i cjelovitost.

Ovaj razvoj događaja rezultirao je potrebom za stvaranje suvremenog i kompetentnog okvira za zaštitu osobnih podataka uz jačanje regulatornih mjera osmišljenih izričito za jačanje pozicije pojedinca čiji se podaci obrađuju. Ovu potrebu prepoznala je i Europska unija i odgovorila na takve zahtjeve donošenjem Opće uredbe o zaštiti podataka, koja je stupila na snagu u svibnju 2016. godine, a u primjenu krenula nakon dvogodišnjeg vakacijskog roka 25. svibnja 2018. godine.[3] Glavna zadaća Uredbe je osigurati temeljno pravo pojedinca na zaštitu osobnih podataka kroz pružanje sveobuhvatnog okvira zaštite uspostavom sustavnih provjera i kontrola koje garantiraju zaštitu pojedinaca prilikom obrade njihovih podataka.

Jedan od ključnih alata za osiguravanje usklađenosti te cjelovitosti i povjerljivosti osobnih podataka koje Opća uredba uvodi kao obavezu je i provođenje postupka

[1] Brynjolfsson E., Kahin B., editors. Understanding the Digital Economy: Data, Tools, and Research. MIT Press; Cambridge, MA: 2002.
[2] Wang, C., Zhang, N., Wang, C, „*Managing privacy in the digital economy*“, Fundamental Research, 1(5), str. 543-551, 2021.
[3] Opća uredba o zaštiti podataka, Europski parlament i Vijeće Europske unije, “ 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,” 2016, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679, (09.02.2024.).

procjene utjecaja na zaštitu podataka (*engl. Data Protection Impact Assessment - DPIA*). Povođenje DPIA-e nužno je za postupke obrade koji vrlo vjerojatno mogu dovesti do visokog rizika za prava i slobode ispitanika[4], a utvrđivanjem rizika te povezane vjerojatnosti i potencijalnih utjecaja prije nego što se pojave, pomaže organizacijama ne samo da se pridržavaju zakonskih zahtjeva, već i da pokažu predanost zaštiti osobnih podataka kao temeljnom pravu uz osiguranje cjelovitosti i povjerljivosti.

Uz Opću uredbu koja osigurava pravni okvir te DPIA-u kao jedan od alata za osiguravanje sukladnosti, informacijska sigurnost jedan je od temeljnih principa zaštite osobnih podataka, vidljivo i iz odredbi čl. 5 OUZP, a osobito načela cjelovitosti i povjerljivosti. Ona pruža tehničke i operativne mjere koje osiguravaju cjelovitost, povjerljivost i dostupnost osobnih podataka. U tom kontekstu, protokoli informacijske sigurnosti nisu samo „*tehnička*“ potreba, već i temeljni element koji podupire mandat Opće uredbe za zaštitu podataka.

Konvergencija usklađenosti s GDPR-om, učinkovitih DPIA-a i robustnih mjera sigurnosti obrade osobnih podataka predstavlja sveobuhvatan pristup očuvanju privatnosti ispitanika. Naglašava važnost integriranja pravnih, proceduralnih i tehničkih zaštitnih mjera za postizanje otpornog ekosustava privatnosti i osiguranju sigurne obrade osobnih podataka. Ovaj holistički pristup zaštiti osobnih podataka naglašava kako zaštita osobnih podataka nije samo puko osiguravanje zakonske usklađenosti, već predanost osiguravanju privatnosti pojedinaca kao njihovog temeljnog prava u digitalnom dobu.

Nadalje, čvrsta primjena i pridržavanje načela koja podupiru odgovorno i transparentno rukovanjem osobnim podatcima nadilaze smanjenje rizika ili imperative zakonske usklađenosti te služi kako katalizator za uspostavu povjerenja između voditelja obrade i ispitanika čime se između ostalog omogućava stabilnost ekonomije temeljene na podacima.

[4] *Ibid*. Opća uredba o zaštiti podataka, članak 35.

U nastavku rada obradit će se ključni elementi za osiguravanje sigurne obrade osobnih podataka. U poglavlju 2. prikazat će se ključni sadržaji vezani za zaštitu osobnih podataka u Europskoj uniji s posebnim fokusom na Opću uredbu za zaštitu podataka. Poglavlje 3. detaljno će prikazati što podrazumijeva procjena učinka na zaštitu podataka uključujući i njenu pravnu regulativu. Fokus četvrtog poglavlja uključivat će prikaz praktičnih pitanja i izazova prilikom provođenja procjene učinka na zaštitu podataka, što uključuje različite metodologije provođenja postupka procjene učinka na zaštitu podataka uz posebni osvrt na procjenu rizika. Također, dat će se prikaz nekih od dostupnih digitalnih DPIA alata, kao i uloge službenika za zaštitu podataka uz osvrt na prakse nadzornih tijela u pogledu povreda odredbi o procjeni učinka na zaštitu podataka. Nadalje, bit će prikazana zaključna razmatranja u pogledu prakse o procjeni učinka na zaštitu podataka s prijedlozima za poboljšanje usklađenosti i kvalitete. U petom poglavlju dat će se kritički osvrt na glavne teme rada uz definiranje smjera nastavka rada.

2 REGULACIJA ZAŠTITE OSOBNIH PODATAKA I POSEBNO NAČELO CJELOVITOSTI I POVJERLJIVOSTI OBRADE

2.1 Definicija zaštite podataka

Zaštita osobnih podataka je temeljno pravo sadržano i regulirano u nizu međunarodnih i nacionalnih pravnih dokumenata. Ustavi brojnih država jamče sigurnost i tajnost osobnih podataka, te utvrđuju pravo svakog pojedinca na zaštitu osobnih podataka.[5]

U Europskoj uniji, zaštita osobnih podataka kao izdvojeno temeljno pravo odvojeno od zaštite privatnosti kao usporednog prava[6], potvrđeno je člankom 8. Povelje o temeljnim pravima Europske unije[7] te člankom 16. Ugovora o funkcioniranju Europske Unije.[8]

Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Zaštita osobnih podataka smatra se suvremenim i aktivnim pravom kojim se uspostavlja sustav provjera i kontrole kako bi se pojedinci zaštitili prilikom svake obrade njihovih podataka.[9]

---

[5] Bevanda, M., Čolaković, M., "*Pravni okvir za zaštitu osobnih podataka (u vezi sa zdravljem) u pravu Europske unije*", Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 37, no. 1, 2016, str. 125–154, doi: 10.30925/zpfsr.37.1.5.

[6] Fuster, G.G,:"*The Emergence of Personal Data Protection as a Fundamental Right of the EU*", Springer, 2014.

[7] Povelja Europske unije o temeljnim pravima, 2007/C 303/01, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:12016P/TXT&from=RO (09.02.2024.)

[8] Ugovor o funkcioniranju Europske unije, članak 16, dostupno na: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0011.01/DOC_3&format=PDF (09.02.2024.)

[9] *Priručnik o europskom zakonodavstvu o zaštiti podataka*, Agencija Europske unije za temeljna prava, Europski nadzornik za zaštitu podataka, Europski sud za ljudska prava, Vijeće Europe, . Izdanje iz 2018.," 2018, doi: 10.2811/266278.

Valja naglasiti da temeljno pravo na zaštitu osobnih podataka ipak nije apsolutno pravo, nego pravo koje je podložno određenim ograničenjima.[10] To je pravo uvjetovano svojim općim društvenim značenjem, odnosno općim interesima i zaštitom prava i sloboda drugih osoba[11], odnosno može se ograničiti radi ostvarenja određenog cilja od općeg interesa ili radi zaštite prava i sloboda drugih osoba.

Dakle, iako je važno osigurati zaštitu osobnih podataka, postoje situacije u kojima se to pravo može ograničiti. U nastavku su navedeni određeni primjeri kada može biti opravdano ograničiti pravo na zaštitu osobnih podataka:

- Javni interes informiranja odnosno prava na pristup podacima i osiguranja slobode izražavanja može biti suprotstavljen pravu na zaštitu osobnih podataka. Na primjer, u novinarstvu ili istraživačkom radu može biti potrebno objaviti osobne podatke radi razotkrivanja korupcije ili drugih nezakonitih aktivnosti.
- U kaznenim postupcima ili sudskim sporovima, prikupljanje i obrada osobnih podataka može biti neophodna za pravično suđenje, uključujući identifikaciju svjedoka ili dokaza.
- U nekim slučajevima, državne agencije mogu prikupljati osobne podatke radi zaštite nacionalne sigurnosti, sprječavanja terorizma ili drugih teških zločina.
- U izvanrednim situacijama poput epidemija ili pandemija, može biti potrebno prikupljati i obrađivati osobne podatke radi zaštite javnog zdravlja i sprječavanja širenja bolesti.
- Prikupljanje i obrada osobnih podataka može biti potrebna radi sprječavanja kriminalnih aktivnosti, poput borbe protiv terorizma ili organiziranog kriminala.

U svim ovim slučajevima, ograničenja prava na zaštitu osobnih podataka trebala bi biti proporcionalna i nužna za postizanje legitimnog cilja te bi trebala biti u skladu s relevantnim zakonima i propisima.

[10] Uvjeti za ograničenje prava za poštovanje privatnog života i zaštitu osobnih podataka navedeni su u članku 8. Europske konvencije o ljudskim pravima i članku 52. stavku 1. Povelje o temeljnim pravima Europske unije

[11] *Ibid.* Bevanda, M., Čolaković, M., str. 125–154

2.2 Kakvu zaštitu podataka uživa EU?

Europska unija već desetljećima prednjači u osiguranju zaštite temeljnih prava i sloboda pojedinaca u pogledu obrade njihovih osobnih podataka. Posljednji i aktualni iskorak u tom smjeru postignut je uvođenjem Opće uredbe o zaštiti podataka (*engl. General Data Protection Regulation - GDPR*), koja je zamijenila Direktivu o zaštiti podataka 95/46/EC, prvi opći propis kojim je Unija regulirala zaštitu podataka kao obvezu država članica sredinom devedesetih godina 20. stoljeća. Opća uredba o zaštiti podataka stupila je na snagu u svibnju 2016. godine, a izravno se i obvezujuće primjenjuje u svim državama članicama Europske unije od 25. svibnja 2018. godine.

Cilj Opće uredbe o zaštiti podataka je zaštititi osobne podatke građana i pružiti im kontrolu nad njihovim osobnim podacima te stvoriti visoku i ujednačenu razinu zaštite podataka u Europskoj uniji, odnosno osigurati zajednički okvir minimalnih standarda zaštite prava ispitanika u svim državama članicama. To nije bilo moguće putem ranijeg okvira, odnosno Direktive o zaštiti i podataka i na njoj temeljenih nacionalnih transpozicijskih mjera kao što je u zakonodavstvu Republike Hrvatske bio Zakon o zaštiti osobnih podataka.[12]

2.3 Povijesni razvoj zaštite osobnih podataka

Povijesni je razvoj zaštite osobnih podataka u Europi bio dug i kompleksan. Sa zaštitom osobnih podataka započelo se 1970-ih godina kada su pojedine EU države članice donijele vlastite propise vezane za regulaciju obrade osobnih podataka od strane javne vlasti, državnih i javnih organizacija i velikih trgovačkih društava.[13]

Na tom primjeru počeli su se razvijati i uspostavljati instrumenti za zaštitu podataka na razini Europe. To se primarno odnosi na Konvenciju Vijeća Europe o zaštiti

[12] Zakon o zaštiti osobnih podataka, NN 103/03, 118/06, 41/08, 130/11, 106/12, prestao važiti 25.05.2018.
[13] Njemačka savezna država Hessen – 1970. godine, Švedska – 1973. godine

pojedinaca pri automatskoj obradi osobnih podataka (Konvencija br. 108) koja je donesena 1981. godine i još uvijek je na snazi. Konvencija br. 108 imala je za cilj regulirati svaku obradu podataka u javnom i privatnom sektoru, uključujući sudstvo i tijela zadužena za izvršavanje zakonodavstva[14] te zaštititi pojedince od zlouporabe prilikom obrade osobnih podataka. Konvenciji mogu pristupiti države i izvan EU, a po ratificiranju ona postaje obvezujuća te je kao takva prvi i trenutno jedini međunarodni pravno obvezujući instrument koji se bavi zaštitom podataka.

U periodu otkad je na snazi, Konvencija je bila povrgnuta modernizaciji s ciljem povećanja zaštite privatnosti u digitalnom okruženju i jačanje mehanizama praćenja provedbe Konvencije donošenjem Protokola o izmjeni CETS br. 223.[15]

Kada govorimo o tzv. „*sekundarnom pravu*“ i razvoju glavnih pravnih instrumenta za zaštitu osobnih podataka EU, za prvo razdoblje zaštite ključna je bila Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom protoku takvih podataka (Direktiva o zaštiti podataka). Direktiva o zaštiti podataka donesena je s ciljem usklađivanja već donesenih nacionalnih zakona o zaštiti podataka članica EU te osiguravanja visoke razine zaštite i slobodnog protoka.

2.4 Razlozi razvoja OUZP

Uvođenje Direktive omogućilo je uspostavu detaljnog i sveobuhvatnog sustava zaštite podataka u EU, no problem se javio prilikom transponiranja odredbi u nacionalna zakonodavstva tj. različitih definicija i interpretacija - tumačenja nacionalnih propisa. Također, pojavile su se i neusklađenosti prilikom definiranja težina sankcija i razina provedbe među članicama EU. Dodatno, od izrade nacrta Direktive tijekom 1990-tih godina došlo je znatnog napretka informacijskih tehnologija, pojave internetskih tražilica, društvenih mreža, *broadband* pristupa Internetu odnosno općenito strelovitog

[14] *Ibid*. Priručnik o europskom zakonodavstvu o zaštiti podataka
[15] Dodatni protokol uz Konvenciju o zaštiti pojedinaca pri automatskoj obradi osobnih podataka, koji se tiče nadzornih tijela i prekograničnih prijenosa podataka, Vijeće Europe, CET br. 223

rasta broja korisnika Interneta i novog i inovativnog načina komercijalizacije osobnih podataka što je sve stvorilo potrebu za reformom zakonodavstva o zaštiti podataka EU.

Kao odgovor na ove potrebe, razvijena je te 2018. godine stavljena u primjenu Opća uredba o zaštiti podataka.[16] Kako su uredbe izravno primjenjive, Opća uredba o zaštiti podataka omogućava jedinstveni skup dosljednih pravila o zaštiti podataka za cijeli prostor EU. Opća uredba o zaštiti podataka naslanja se na tekovine Direktive o zaštiti podataka što podrazumijeva čuvanje temeljnih načela i prava ispitanika uz uvođenje novih obaveza organizacija koje uključuju: implementaciju tehničke i integralne zaštite podataka, imenovanje službenika za zaštitu podataka u određenim okolnostima, pridržavanje odgovornosti i prenosivosti podataka.[17]

2.5 Opća uredba kao okvir zaštite osobnih podataka u EU

Opća uredba o zaštiti podataka strukturirana je tako da su na početku navedene uvodne izjave, pružajući kontekst i vodeća načela, nakon čega slijede članci koji navode posebne odredbe i zahtjeve za zaštitu podataka.[18] Opća uredba o zaštiti podataka sadrži brojne i široke odredbe o pravima ispitanika te načela zaštite podataka koja odražavaju temeljne vrijednosti i ciljeve Uredbe.

Načela služe kao temelj za rukovanje osobnim podacima i sastavni su dio osiguravanja poštivanja prava i sloboda pojedinaca, a podrazumijevaju niz načela uređenih čl. 5. OUZP. Pregled načela započinje s načelom **zakonitosti, poštenosti i transparentnosti** (Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (a)). Ovo načelo naglašava važnost obrade osobnih podataka na zakonit i transparentan način, s fokusom na poštenost prema ispitanicima. Zahtijeva od voditelja obrade da ima pravnu osnovu za obradu osobnih podataka i da informira pojedince o načinima obrade.

[16] *Ibid.* Opća uredba o zaštiti podataka
[17] *Ibid.* Opća uredba o zaštiti podataka
[18] Voigt, P., Bussche, A., "*The EU General Data Protection Regulation (GDPR): A Practical Guide*", 2017., doi: 10.1007/978-3-319-57959-7.

Načelo **ograničavanja svrhe** (Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (b)) naglašava koncept prikupljanja podataka za određene, eksplicitne i legitimne svrhe. Od voditelja obrade se očekuje da jasno definiraju svrhe za koje se osobni podaci obrađuju i osiguraju da je daljnja obrada u skladu s tim početnim svrhama.

Načelo smanjenja količine podataka (Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (c)) je načelo kojim se naglašava važnost ograničavanja prikupljanja osobnih podataka na ono što je potrebno za navedene svrhe. Ovo načelo potiče organizacije da ograniče količinu prikupljenih podataka samo na ono što je relevantno i neophodno za namjeravanu upotrebu.

Načelo **točnosti podataka** (Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (d)) se odnosi na zahtjev za organizacije da osiguraju točnost i ažurnost osobnih podataka. To zahtijeva implementaciju procesa za ispravljanje ili brisanje netočnih podataka bez odgode.

Ograničenje pohrane (Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (e)) ističe nužnost pohrane osobnih podataka ne dulje nego što je potrebno za svrhe za koje su prikupljeni. Ovo načelo potiče organizacije da uspostave rasporede čuvanja i redovito preispituju nužnost čuvanja određenih podataka.

Cjelovitost i povjerljivost (Opća uredba o zaštiti podataka, članak 5. stavak 1. točka (f)) stavljaju značajan naglasak na sigurnost i zaštitu osobnih podataka. Organizacije imaju mandat za provedbu odgovarajućih tehničkih i organizacijskih mjera za zaštitu osobnih podataka od neovlaštene ili nezakonite obrade, slučajnog gubitka, uništenja ili oštećenja.

Konačno, načelo odgovornosti (Opća uredba o zaštiti podataka, članak 5. stavak 2) uspostavlja obvezu organizacija da pokažu odnosno dokumentiraju usklađenost s Općom uredbom o zaštiti podataka i definiranim načelima zaštite podataka. Ovo načelo potiče transparentnost i odgovornost u postupanju s osobnim podacima.

Uz ova temeljna načela, Uredba također izričito uređuje određena prava ispitanicima, što između ostalog uključuje pravo na pristup i ispravak svojih osobnih podataka, pravo na zaborav i pravo na prenosivost podataka. Prava ispitanika su temeljna za sveobuhvatne ciljeve Uredbe i imaju za cilj osnažiti pojedince u kontroli nad svojim osobnim podacima.

U nastavku će biti prikazan osvrt na sva prava ispitanika prema Općoj uredbi o zaštiti podataka: [19,20]

I. **Pravo na informiranje o obradi osobnih podataka** predstavlja praktičnu primjenu jednog od temeljnih načela obrade osobnih podataka prema Općoj uredbi – načela zakonitosti, poštenosti i transparentnosti.[21] Ovo pravo nalaže da voditelj mora transparentno i jasno informirati ispitanika o korištenju njihovih podataka. To podrazumijeva informaciju o svrsi obrade podataka, pravni temelj obrade, razdoblje pohrane podataka, primatelje s kojima će se podaci dijeliti, osnovna prava ispitanika u vezi sa zaštitom podataka, eventualni prijenos podataka izvan EU-a, pravo na podnošenje pritužbe, postupak povlačenja danih privola, te kontakt podatke organizacije ili društva odgovornog za obradu podataka.[22]

II. **Pravo pristupa osobnim podacima** ima za cilj omogućiti ispitanicima uvid u podatke koje neki voditelj obrade posjeduje, a koji se odnose na njih. Putem prava na pristup podacima, ispitanici mogu zatražiti detaljne informacije, posebno u vezi s namjenom obrade, vrstom/kategorijama osobnih podataka koji se obrađuju (uključujući uvid u vlastite podatke), primateljima ili kategorijama primatelja te planiranim razdobljem pohrane osobnih podataka.[23] Nadalje, pristup osobnim podacima može biti ograničen samo u slučajevima propisanim pravom Europske unije ili

[19] *Ibid*. Opća uredba o zaštiti podataka
[20] Katulić, T., Mladinić, A., "*Prava ispitanika prema Općoj uredbi o zaštiti podataka i Zakonu o provedbi Opće uredbe o zaštiti podataka*", Zagreb, 2021.
[21] *Ibid.* Katulić, T., Mladinić, A.
[22] *Ibid*. članci 13. i 14. i uvodne izjave 60, 61, 62.
[23] *Ibid*. članak 15. i uvodne izjave 63 i 64.

nacionalnim zakonodavstvom, odnosno kada takva ograničenja služe zaštiti bitnih temeljnih prava i sloboda drugih.[24]

III. **Pravo ispitanika na ispravak podataka** naslanja se na temeljno načelo obrade osobnih podatka – načelo točnosti. Pravom na ispravak ispitanik ima pravo bez nepotrebnog odgađanja ishoditi od voditelja obrade ispravak netočnih osobnih podataka koji se na njega odnose. Uzimajući u obzir svrhe obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave.[25]

IV. **Pravo ispitanika na brisanje osobnih podataka („pravo na zaborav“)** definira uvjete kada ispitanik može bez nepotrebnog odgađanja tražiti brisanje svojih osobnih podataka. Uvjeti su sljedeći: osobni podaci više nisu nužni za svrhe za koje su obrađivani; osobni podaci su se obrađivali na temelju ispitanikove privole koju je on povukao, a više nema neke druge primjenjive pravne osnove za njihovu daljnju obradu; obrada se vrši temeljem legitimnog interesa, a ispitanik je uložio prigovor protiv kojeg voditelj obrade ne može argumentirati da bi prevladao njegov legitimni interes; osobni podaci se obrađuju nezakonito; brisanje osobnih podataka voditelju obrade nalaže obveza propisana pravom Europske unije ili nacionalnim zakonodavstvom; osobni podaci su obrađivani u okviru ponude usluge informacijskog društva koja je upućena djetetu.[26,27]

V. **Pravo na ograničenje obrade osobnih podataka**, može biti primjenjivo u sljedećim situacijama: kada postoji osporavanje točnosti podataka, kada je obrada nezakonita, a ispitanik se protivi brisanju, te kada su podaci potrebni radi ostvarivanja ili obrane pravnih zahtjeva. Također, ograničenje obrade može biti zatraženo ukoliko je podnesen prigovor na obradu osobnih podataka. Ova prava omogućavaju zaštitu interesa ispitanika, čuvajući istovremeno zakonitost i transparentnost u postupku obrade osobnih podataka.[28]

[24] *Ibid.* Katulić, T., Mladinić, A.
[25] *Ibid*. članak 16. i uvodna izjava 65.
[26] *Ibid*. članak 17. i uvodne izjave 65 i 66.
[27] *Ibid.* Opća uredba o zaštiti osobnih podataka
[28] *Ibid*. članak 18, i uvodna izjava 67

VI. **Pravo na prenosivost osobnih podataka** odnosi se na pravo ispitanika da prenese svoje osobne podatke s jednog voditelja obrade na drugog kada su podatci prikupljeni temeljem privole ili ugovora. Dodatno, potrebno je zadovoljiti uvjet da se radi o automatskoj obradi podataka. U slučaju ispunjavanja oba uvjeta ispitanik ima pravo prijenosa, a inicijalni voditelj obrade dužan je dostaviti osobne podatke ispitanika u strukturiranom, često korištenom i strojno čitljivom formatu.[29]

VII. **Pravo na prigovor obradi osobnih podataka** omogućuje ispitaniku da uloži prigovor na obradu osobnih podataka koja se temelji na javnom ili legitimnom interesu kao pravnoj osnovi obrade. Ovo pravo obuhvaća situacije u kojima se osobni podaci obrađuju radi izvršavanja zadaća od javnog interesa ili u sklopu službenih ovlasti, te kada se koriste u svrhe direktnog marketinga. U takvim slučajevima, ispitanik može prigovoriti takvoj obradi. Važno je naglasiti da se u svakom pojedinačnom slučaju trebaju uzeti u obzir interesi ispitanika, kao što su zaštita njegovih prava i sloboda, te ekonomski interesi voditelja obrade koji se oslanja na legitimni interes za obradu osobnih podataka.[30]

VIII. **Pravo na prigovor automatiziranom pojedinačnom donošenju odluka, uključujući izradu profila** odnosi se na osporavanje tako ostvarenih rezultata obrade osobnih podataka ispitanika. Ispitanik ima za pravo izraziti svoje mišljenje, osporiti odluku i tražiti uključivanje osobe u proces radi pojašnjenja odluke koju je donesen automatiziranim putem, odnosno putem profiliranja. Također, ispitanici imaju pravo odbiti podvrgnuti se automatiziranom pojedinačnom donošenju odluka ili profiliranju.[31,32]

S obzirom na to da je načelo Uredbe o povjerljivosti i cjelovitosti, uz načelo pouzdanosti odnosno odgovornosti, ključno u smislu povezivanja zaštite podataka i informacijske sigurnosti, dodatno ćemo se osvrnuti na ovaj segment i njegovu ugrađenost u Opću uredbu o zaštiti podataka.

[29] *Ibid*. članak 20. i uvodna izjava 68.
[30] *Ibid*. članak 21. i uvodne izjave 69 i 70.
[31] *Ibid.* Katulić, T., Mladinić, A.
[32] *Ibid*. članak 22. i uvodne izjave 71 i 72.

Načelo povjerljivosti osigurava privatnost osobnih podataka i dostupnost samo ovlaštenim osobama – djelatnicima voditelja i izvršitelja obrade te samim ispitanicima, dok načelo cjelovitosti osigurava cjelovitost osobnih podataka u kontekstu obrada koje se provode na sustavima voditelja ili izvršitelja obrade. Te su odredbe navedene u članku 5. stavak 1, točka (f), koji navodi da će se osobni podaci obrađivati na način koji osigurava načelo cjelovitosti i povjerljivosti uključivanjem odgovarajućih tehničkih i organizacijskih mjera za zaštitu osobnih podataka.[33] Uredba također uključuje odredbe koje naglašavaju važnost informacijske sigurnosti i načela povjerljivosti, integriteta i dostupnosti (*engl. Confidentiality, Integrity, Availability – CIA*).[34]

Primjena načela povjerljivosti, cjelovitosti i dostupnosti u Uredbi je vidljiva u mnogim odredbama koje se tiču obveza voditelja obrade – primjerice, očituje se u zahtjevu prema voditeljima obrade podataka da osiguraju povjerljivost, integritet i dostupnost osobnih podataka (članak 24. Uredbe), u obvezama procjene rizika (primjerice kod procjene učinka na zaštitu podataka i općenito u kontekstu odabira tehničkih i organizacijskih mjera) itd. To uključuje provedbu mjera za sprječavanje neovlaštenog pristupa (povjerljivost), održavanje točnosti i pouzdanosti osobnih podataka (cjelovitost) te osiguranje dostupnosti osobnih podataka kada je to potrebno (dostupnost). Dodatno, u uvodnoj izjavi 39 ističe se važnost održavanja povjerljivosti, cjelovitosti i dostupnosti osobnih podataka, naglašavajući potrebu za odgovarajućim tehničkim i organizacijskim mjerama za postizanje tih ciljeva. Nadalje, članci 24., 25. i 32. Uredbe usko su povezani s načelima povjerljivosti, cjelovitosti i dostupnosti u zaštiti podataka. Ovi članci daju posebne zahtjeve i mjere za osiguranje zaštite osobnih podataka tijekom njihova životnog ciklusa. Članak 24. fokusira se na odgovornost voditelja obrade podataka za provedbu odgovarajućih tehničkih i organizacijskih mjera za osiguranje sigurnosti osobnih podataka.

Članak 25. uvodi koncept "*Tehnička i integrirana zaštita podataka*" (*engl. Data protection by design and by default*). Ovo načelo zahtijeva od voditelja obrade

[33] *Ibid.* Opća uredba o zaštiti osobnih podataka
[34] Death, D., "*Information security handbook: develop a threat model and incident response strategy to build a strong information security framework*", Packt Publishing Ltd, 2017.

podataka provođenje adekvatnih tehničkih i organizacijskih mjera koje će omogućiti zaštitu podataka od dizajniranja do implementacije sustava i procesa. Ove mjere trebale bi osigurati da se obrađuju samo potrebni osobni podaci i da se obrada vrši s najvišim mogućim razinama sigurnosti.

Konačno, članak 32. GDPR-a navodi sigurnosne zahtjeve za obradu osobnih podataka. Određuje da voditelji i izvršitelji obrade moraju primijeniti odgovarajuće tehničke i organizacijske mjere kako bi osigurali razinu sigurnosti primjerenu riziku. Ove mjere trebale bi uključivati pseudonimizaciju i enkripciju osobnih podataka, mogućnost osiguranja stalne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade, mogućnost pravodobnog ponovnog uspostavljanja dostupnosti i pristupa osobnim podacima u slučaju fizičkog ili tehničkog incidenta, te redovito testiranje, procjena i evaluacija učinkovitosti tih mjera.

Usklađujući se s načelom cjelovitosti i povjerljivosti, Uredba naglašava važnost sveobuhvatnog pristupa informacijskoj sigurnosti i zaštiti podataka. Naglasak Uredbe na informacijskoj sigurnosti i integraciji načela cjelovitosti i povjerljivosti odražava njegovu predanost osiguravanju sigurne i odgovorne obrade osobnih podataka.

Nadalje, promjena pristupa koja je očita u Uredbi jest i pomak prema odgovornosti voditelja obrade, s ciljem postizanja učinkovite informacijske sigurnosti u praksi. Kao što smo ranije spomenuli, ovaj pristup se očituje se kroz obvezu voditelja obrade da implementiraju odgovarajuće tehničke i organizacijske mjere (članak 24., članak 25., članak 32.) kako bi osigurali i dokazali da se obrada provodi u skladu s ovom Uredbom.

Također, za voditelje obrade uvode se obaveze imenovanja službenika za zaštitu podataka (više u Poglavlju 4.4), te provođenja procjene utjecaja na zaštitu podataka. Uključivanjem ovih načela i pravnih obaveza, Uredba ima za cilj pružiti robustan okvir za zaštitu podataka uz usku povezanost sa informacijskom sigurnošću.

3 POJAM I REGULACIJA PROCJENE UČINKA NA ZAŠTITU PODATAKA

3.1 Što je to DPIA?

Opća uredba o zaštiti podataka u široku upotrebu kao obvezu voditelja obrade uvodi provođenje postupka procjene učinka na zaštitu podataka (*engl. Data Protection Impact Asseesment – DPIA*) za obrade za koje je izvjesno da će predstavljati visok rizik za prava i slobode ispitanika.

DPIA-u možemo definirati kao pravni, organizacijski i tehnički proces uspostavljen kako bi pomogao voditeljima obrade da identificiraju, procjene (vjerojatnost i ozbiljnost) te umanje rizike na prava i slobode ispitanika u postupcima obrade podataka.

Nadalje, ona služi kao alat za uspostavu i dokazivanje usklađenosti sa zahtjevima Opće uredbe o zaštiti podataka kojima voditelji obrade dokazuju da su poduzeli sve potrebne mjere, što je propisano temeljnim načelom Uredbe (Članak 5. stavak 2).

3.2 Kako je nastala i gdje je prvo regulirana?

Prije usvajanja Opće uredbe nije postojala jedinstvena regulativa na razini Europske unije po pitanju obveze provođenja postupka procjene učinka na zaštitu podataka i njenog sadržaja - identificiranja rizika po prava i slobode ispitanika. Postojale su određene inicijative koje nisu uvijek bile potpuno usklađene, što je rezultiralo različitim standardima i praksama. Kao primjer takvih inicijativa možemo izdvojiti praksu provođenja procjene utjecaja na privatnost (*engl. Privacy Impact Assessment –*

PIA) poznatu iz komparativnog okvira, osobito francuskog i britanskog zakonodavstva odnosno prakse nadzornih tijela.[35,36]

Uvođenje procjene učinka na zaštitu podataka donijelo je značajne promjene u odnosu na prijašnju najbolju praksu. Procjena učinka na zaštitu podataka, kako nalaže Opća uredba o zaštiti podataka, ima sveobuhvatniji i sustavniji pristup procjeni i ublažavanju rizika uz definiranje kriterija za obavezu provođenja postupka procjene.

Nadalje, više nije dovoljno samo identificirati kontekst i rizike, već je potrebno provesti procjenu nužnosti i proporcionalnosti obrade podataka, te predložiti adekvatne mjere za rješavanje identificiranih rizika (članak 35. stavak 7, uvodna izjava 90.).[37]

Procjena učinka na zaštitu podataka primarno je regulirana člankom 35. Opće uredbe o zaštiti podataka no na nju se također odnose i članak 36. te uvodne izjave 75., 84., 89., 90., 91., 92., 93., 94., 95. i 96., što će biti prikazano u nastavku.

3.3 Primjenjive odredbe Opće uredbe o zaštiti podataka na procjenu učinka

Obaveza provođenja DPIA-e regulirana je Člankom 35., stavak 1., dok su uloga i značenje DPIA-e pojašnjeni u uvodnoj izjavi 84. i 90.. Člankom 35., stavkom 1, uspostavlja se pristup temeljen na procjeni rizika te definira obaveza provođenja procjene u slučaju da neka vrsta obrade vrlo vjerojatno može rezultirati visokim rizikom za prava i slobode pojedinaca. Dakle, u slučaju niskog rizika i u slučaju kada se obrada nalazi na javno objavljenom popisu Nadzornog tijela kojim su definirane vrste postupaka obrade za koje nije potrebna procjena učinka (Članak 35, stavak 5.),

[35] Conducting privacy impact assessments code of practice, ICO (Information Commissioner's Office), UK Information Commissioner's Office, 2014., str. 1–55.
[36] European Commission, "*Privacy and Data Protection Impact Assessment Framework for RFID Applications*" Brussels, str. 1–24, 2011.
[37] *Ibid* OUZP čl. 35.

voditelji obrade nisu obavezni provoditi DPIA-u. Valja napomenuti kako odredbe iz stavka 1. ne oslobađaju voditelje obrade od generalne obaveze da kontinuirano procjenjuju rizike po pitanju prava i sloboda ispitanika.

Kriteriji koji uspostavljaju obavezu provođenja DPIA-e, odnosno definiraju vrste obrade koje će imati visok rizik za ispitanike, navedeni su u stavku 3., točka (a) do (c) članka 35, a dopunjeni su stavkom 4. i uvodnim izjavama 71, 75 i 91.

Prema stavku 3. procjena učinka na zaštitu podataka obvezna je *osobito* u slučaju:

- obrade osobnih podataka radi donošenja odluka o ispitanicima na temelju sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima, a koja se temelji na automatiziranoj obradi, uključujući izradu profila (uvodna izjava 71., 91.);
- obrade osjetljivih (posebnih kategorija) osobnih podataka ili podataka u vezi s kaznenim osudama i kažnjivim djelima (Uvodna izjava 75, 91);
- obrade koja uključuje opsežno i sustavno praćenje javno dostupnih područja (Uvodna izjava 75).

Stavak 3. Opće uredbe dodatno je obrazložen s danim pojašnjenjima pojmova „*sustavno praćenje i „opsežna obrada*“ u Smjernicama o službenicima za zaštitu podataka[38] što je referencirano u Smjernicama o procjeni učinka na zaštitu podataka.[39]

Prema definiciji Radne skupine za zaštitu podataka iz članka 29 (WP 29) pojam „*sustavno praćenje*“ može imati jedno ili više sljedećih značenja: (i) odvija se u sladu sa sustavom, (ii) planirano, organizirano ili metodično, (iii) odvija se kao dio općeg plana za prikupljanje podataka, (iv) provedeno kao dio strategije. Nadalje, WP29 predlaže da se prilikom utvrđivanja „*opsežne obrade podataka*“ razmotre sljedeći čimbenici: (i) broj uključenih ispitanika, bilo kao određeni broj ili dio relevantnog

[38] Smjernice o službenicima za zaštitu podataka, Radna skupina za zaštitu podataka iz članka 29., Donesene 13. prosinca 2016. Posljednji put revidirane i donesene 5. travnja 2017.
[39] Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik” u smislu Uredbe 2016/679, Radna skupina za zaštitu podataka iz članka 29., Donesene 4. travnja 2017. Posljednji put revidirane i donesene 4. listopada 2017.

stanovništva, (ii) količina podataka i/ili niz različitih podataka koji se obrađuju, (iii) trajanje ili stalnost postupka obrade podataka, (iv) zemljopisni opseg aktivnosti obrade.

Osim navedenog u stavku 3., stavak 1. definira nužnost procjene prilikom uvođenja novih tehnologija za obradu podataka. Nakon što je utvrđena nužnost provođenja procedure procjene učinka na zaštitu podataka, člankom 35, stavak 7 definira kao minimalni sadržaj: (a) sustavan opis predviđenih postupaka obrade i svrha obrade, uključujući, ako je primjenjivo, legitimni interes voditelja obrade; (b) procjenu nužnosti i proporcionalnosti postupaka obrade povezanih s njihovim svrhama; (c) procjenu rizika za prava i slobode ispitanika.

Nadalje, osim obaveze provedbe, povezanih kriterija te minimalnog sadržaja DPIA-e, stavkom 8. članka 35. definirana je važnost usklađenosti s odobrenim kodeksima ponašanja prilikom procjene učinka postupaka obrade podataka.[40] Ovi kodeksi ponašanja, navedeni u članku 40., daju važne smjernice o pravilnoj provedbi Uredbe i trebaju se uzeti u obzir pri procjeni utjecaja postupaka obrade na zaštitu podataka. Prema stavku 9., također treba razmotriti traženje mišljenja ispitanika ili njihovih predstavnika u vezi s namjeravanom obradom, pri čemu treba voditi računa o balansiranju komercijalnih ili javnih interesa i sigurnosti postupka. Konzultiranje s ispitanicima se ne uvodi kao obaveza, no može biti od koristi za voditelja obrade kako bi stekao dodatnu perspektivu tijekom izrade DPIA-e te također može poslužiti kao dodatni dokaz da je procedura adekvatno provedena.

Nadalje, stavak 10. pruža smjernice za slučajeve u kojima obrada ima pravnu osnovu prema pravu Unije ili državi članici, a procjena učinka na zaštitu podataka već je provedena kao dio opće procjene učinka. U takvim slučajevima odredbe članka 35. u stavcima od 1. do 7. ne moraju se primjenjivati osim ako države članice smatraju drugačije. U stavku 11. navodi se da voditelj obrade treba pregledati obradu kako bi procijenio usklađenost s procjenom učinka na zaštitu podataka, posebno ako postoji promjena u razini rizika koju predstavljaju postupci obrade. Ovo implicira da se na

[40] Čl. 35. OUZP;

DPIA-u treba gledati kao na „*živi dokument*“ koji se razvija tijekom životnog ciklusa obrade.[41] Voditelj obrade trebao bi uspostaviti sustav kontinuiranog praćenja za DPIA-u kako bi identificirao potencijalne promjene u rizicima i procijenio učinkovitost mjera za ublažavanje kroz čitav život odnosno trajanje potrebe za obradom koja je predmet DPIA.

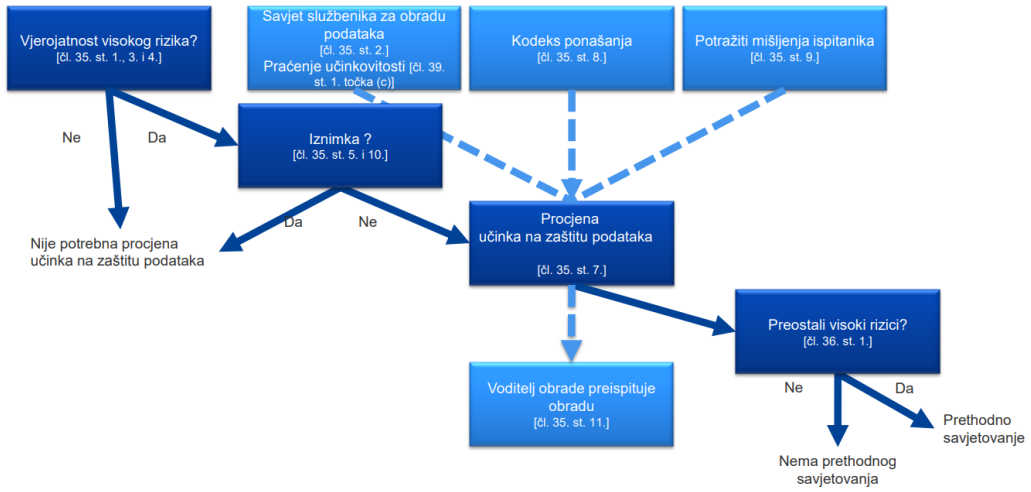
Dodatnu obavezu uvodi stavak 2. članka 35.. Njime je definirana obaveza savjetovanja sa službenikom pri provođenju procjene učinka za zaštitu podataka, ako je službenik imenovan, što je usklađeno sa zadaćama službenika za zaštitu podataka navedenima u članku 39., stavku 1, točki (c).

Odredbe koje se odnose na procjenu utjecaja na zaštitu podataka uključuju i odredbe unutar članka 36 što se odnosi na obvezu provođenja prethodnog savjetovanja, a za razumijevanje procedura ključni su članak 1. i 2.

Prema članku 36. stavak 1., voditelj obrade dužan je provesti konzultiranje s nadzornim tijelom u slučaju da DPIA pokazuje kako predviđene mjere ublažavanja visokih rizika na prava i slobode ispitanika ne dovode do očekivanog smanjenja. Ako nadzorno tijelo smatra da bi planirana obrada mogla povrijediti odredbe Uredbe, osobito ako voditelj obrade nije adekvatno identificirao ili smanjio rizike, nadzorno tijelo pisanim putem konzultira voditelja obrade i po potrebi izvršitelja (članak 36., stavak 2.).

Prikaz međuovisnosti i slijednosti postupanja, prema gore navedenim odredbama i načelima Uredbe koje se odnose na procjenu učinka na zaštitu podataka, vidljiv je je na slici 3.1.

[41] *Ibid* CNIL.



Slika 3.1 Dijagram osnovnih načela povezanih s procjenom učinka na zaštitu u Općoj uredbi o zaštiti podataka

Izvor: Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik" u smislu Uredbe 2016/679

3.4 Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik" u smislu Uredbe 2016/679

Iz gore prikazanih odredbi kojima se DPIA regulira unutar Opće uredbe, jasno je kako Uredba pruža generalni okvir. Kako bi se osigurala dosljednost prilikom tumačenja kriterija tj. okolnosti u kojima je procjena učinka na zaštitu obavezna, radna skupina 29 (*engl. Working Party 29 – WP29*), izdala je Smjernice o procjeni učinka zaštite podataka[42] (od sada Smjernice) da bi se pomoglo voditeljima obrade utvrditi da bi obrada mogla vjerojatno dovesti do visokog rizika.[43]

Smjernice o procjeni učinka prvotno je izradila Radna skupina za zaštitu podataka iz članka 29. Direktive o zaštiti podataka, neformalno tijelo predviđeno Direktivom čiji je zadatak bio pružati neobvezujuća tumačenja i upute oko primjene odredaba

[42] *Ibid.* Smjernice o procjeni učinka na zaštitu podataka
[43] *Ibid.* Smjernice o procjeni učinka na zaštitu podataka

Direktive, a koje je po njezinom ukidanju preuzeo Europski odbor za zaštitu podataka (*engl. European Data Protection Board – EDPB*).[44]

Kako bi se olakšala procjena koje sve obrade mogu prouzročiti visoki rizik[45] na prava i slobode ispitanika Smjernice upućuju da se razmotri sljedećih devet (9) kriterija:

I. **Procjena ili bodovanje**: Obrada koja uključuje izradu profila ili predviđanje na temelju različitih osobnih aspekata ispitanika, poput ekonomske situacije, zdravlja, osobnih preferencija, ili lokacije.[46]

II. **Automatizirano donošenje odluka s pravnim ili drugim znatnim učinkom**: Obrada koja ima za cilj donošenje odluka o ispitanicima s pravnim ili sličnim znatnim učincima[47], što može rezultirati isključivanjem ili diskriminacijom.

III. **Sustavno praćenje**: Obrada koja se koristi za promatranje, praćenje ili kontrolu ispitanika, uključujući podatke prikupljene putem mreža ili sustavnog[48] praćenja javno dostupnog područja.[49]

IV. **Osjetljivi podaci ili podaci vrlo osobne naravi**: Obrada posebnih kategorija osobnih podataka[50] (npr. rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, podatci koji se odnose na zdravlje ili spolni život, itd.) ili podataka koji se odnose na kaznene osude.[51]

[44] Tijekom svog prvog plenarnog sastanka, 25. svibnja 2018. godine, Europski odbor za zaštitu podataka (EDPB) prihvatio je WP29 Smjernice povezane s GDPR-om.
[45] Ibid. uvodne izjave 75., 76., 92. i 116.
[46] *Ibid*. uvodne izjave 71. i 91.
[47] *Ibid*. članak 35. stavak 3. točka (a)
[48] Radna skupina za zaštitu podataka iz članka 29. smatra da pojam sustavno može imati jedno značenje ili više njih, kako je navedeno u nastavku (vidjeti Smjernice Radne skupine za zaštitu podataka iz članka 29. o službeniku za zaštitu podataka, 16/EN WP 243):
- odvija se u skladu sa sustavom,
- planirano, organizirano ili metodično,
- odvija se kao dio općeg plana za prikupljanje podataka,
- provedeno kao dio strategije.
[49] *Ibid*. Članak 35. stavak 3. točka (c)
[50] *Ibid*. Članak 9.
[51] *Ibid*. Članak 10.

V. **Opsežna obrada podataka**: Obrada koja može uključivati veliki broj ispitanika, značajnu količinu podataka, dugotrajnost ili stalnost postupka obrade, ili široki geografski opseg aktivnosti obrade.[52]

VI. **Podudarajući ili kombinirani skupovi podataka**: Kombiniranje podataka iz različitih izvora ili postupaka obrade, provedenih od različitih voditelja obrade ili za različite svrhe.[53]

VII. **Podaci koji se odnose na osjetljive ispitanike**: Obrada podataka koji su povezani s osobama koje su u neravnoteži moći, poput djece, zaposlenika, ili drugih osjetljivih skupina (npr. tražitelji azila ili starije osobe, pacijenti itd.).[54] Time su obuhvaćene i situacije u kojima se može utvrditi neravnoteža između položaja ispitanika i voditelja obrade.

VIII. **Inovativna upotreba ili primjena novih tehnologija**: Korištenje novih tehnologija ili organizacijskih rješenja koja mogu povećati rizik za prava i slobode pojedinaca.

IX. **Obrada koja sprečava ostvarivanje prava ili upotrebu usluge i ugovora**: Obrada koja ograničava ispitanike u ostvarivanju njihovih prava ili pristupu određenoj usluzi ili sklapanju ugovora.[55]

U slučaju da obrada uključuje dva ili više kriterija, preporuka Smjernica je da se provede postupak procjene učinka na zaštitu podataka, iako u nekim slučajevima već i jedan ispunjen kriterij može biti dovoljan za takvu procjenu, primjerice kad je riječ o opsežnoj obradi podataka, osjetljivim podacima ili tehnologijama koje mogu povećati rizik za prava i slobode pojedinaca, kao što su tehnologije strojnog učenja odnosno umjetne inteligencije (*engl. Artificial Inteligence - AI*).

[52] Općom uredbom o zaštiti podataka nije određeno što obuhvaća pojam „opsežno", ali se u uvodnoj izjavi 91. nalaze određene smjernice. Dodatno, vidjeti Smjernice Radne skupine za zaštitu podataka iz članka 29. o službeniku za zaštitu podataka, 16/EN WP 243

[53] Vidjeti objašnjenje u Mišljenju Radne skupine za zaštitu podataka iz članka 29. o ograničavanju svrhe, 13/EN WP 203, str. 24.

[54] *Ibid*. Uvodna izjava 75.

[55] *Ibid*. članak 22. i uvodna izjava 91.

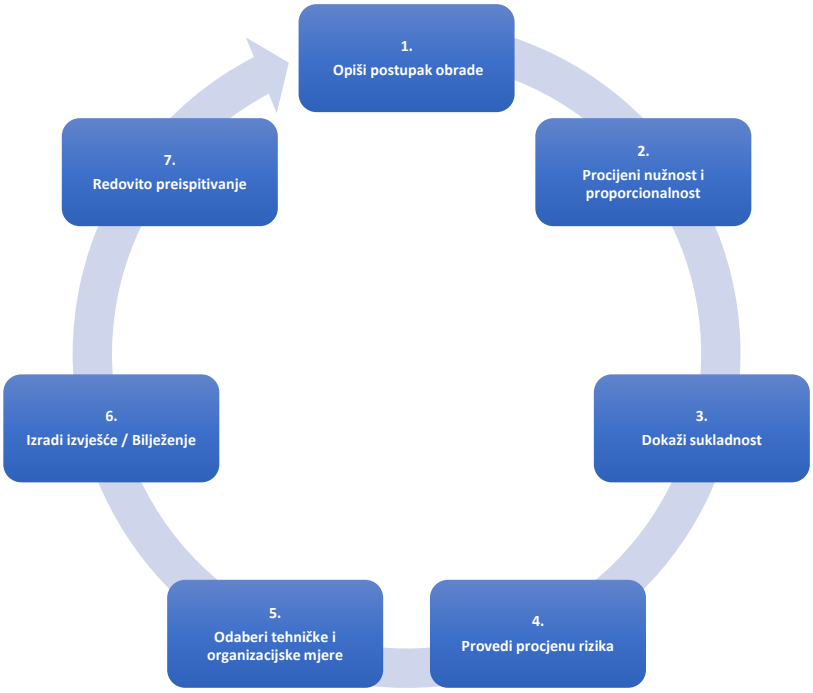
Općenito, Radna skupina za zaštitu podataka iz članka 29. smatra da što je više kriterija ispunjeno obradom, to je veća mogućnost da ona predstavlja visok rizik za prava i slobode ispitanika i stoga je nužno provođenje procjene učinka na zaštitu podataka.[56]

Nadalje, Smjernice također pojašnjavaju koje su to situacije kada nije potrebno provesti procjenu učinka na zaštitu podataka. Procjenu učinka na zaštitu podataka nije nužno provesti u sljedećim situacijama:

- Kada je malo vjerojatno da će obrada dovesti do značajnog rizika za prava i slobode pojedinaca.[57]
- Ako su priroda, opseg, kontekst i ciljevi obrade vrlo slični onima prethodno provedenih DPIA-a. U takvim slučajevima mogu se koristiti rezultati prethodnih DPIA-a.[58]
- Ako je aktivnosti obrade pregledalo nadzorno tijelo prije svibnja 2018. pod posebnim uvjetima koji ostaju nepromijenjeni.
- Ako obrada podataka ima pravnu osnovu u zakonodavstvu EU-a ili države članice prema članku 6. stavku 1. točki (c) ili (e), te ako je specifična obrada regulirana tim zakonodavstvom i već je provedena procjena utjecaja na zaštitu podataka kao dio uspostave te pravne osnove[59], tada nije potrebno provesti novu procjenu učinka na zaštitu podataka, osim ako to zahtijeva država članica prije provođenja same obrade.
- Kada je radnja obrade, na temelju članka 6. stavka 1. točke (c) ili (e) prava EU-a ili države članice, već prošla DPIA kao dio utvrđivanja pravne osnove za nju (članak 35. stavak 10.), osim ako država članica smatra da je DPIA neophodna prije aktivnosti obrade.
- Ako je obrada navedena kao neobvezna na listi koju je definiralo nadzorno tijelo prema članku 35. stavak 5. Ovaj popis može uključivati aktivnosti obrade koje ispunjavaju posebne uvjete koje je postavilo tijelo, kao što su smjernice, posebne odluke, ovlaštenja, pravila usklađenosti itd.

[56] *Ibid.* Smjernice o procjeni učinka na zaštitu podataka
[57] *Ibid*. članak. 35., stavak 1.
[58] *Ibid*. članak. 35., stavak 1.
[59] *Ibid*. članak 35., stavak 10.

Osim pojašnjenja kriterija koji mogu dovesti do visokog rizika za prava i slobode ispitanika te situacija u kojima nije potrebno provođenje postupka DPIA-e, Smjernice također daju opći prikaz iterativnog procesa i nužnih koraka provedbe procjene učinka na zaštitu podataka (slika 3.2). Procjena učinka provodi se prije početka obrade, a najbolje ju je provesti tijekom faze planiranja nove obrade.



Slika 3.2 Dijagram općeg iterativnog postupka provedbe procjene učinka na zaštitu podataka

Predradnja uključuje utvrđivanje radi li se o obradi koja će vjerojatno rezultirati visokim rizikom za prava i slobode pojedinaca. Ako obrada zadovoljava kriterije definirane stavcima 1., 3. i 4. unutar članka 35. te oni ne spadaju pod iznimke definirane stavcima 5. i 10. istog članka, nužno je provesti procjenu učinka na zaštitu podataka.

Nakon što je utvrđeno da je nužno provesti DIPA-u Smjernice predlažu sljedeće korake:

Korak 1 – Izrada sustavnog opisa predviđenih postupaka obrade i svrhe obrade.
U ovom koraku potrebno je opisati svrhu obrade i protok podataka u okviru razmatrane obrade. Treba dati odgovore na pitanja poput: "*Otkud podaci dolaze? Čemu služe*

(zašto se prikupljaju)? Kome se prosljeđuju? Tko im može pristupati? Koje će se tehnologije koristiti tijekom obrade? Kakva su oprema ili softver potrebni za provođenje postupka?, itd.".

Korak 2 – Procjena nužnosti i proporcionalnosti.
Kako bismo procijenili *nužnost* obrade, potrebno je utvrditi i dokazati pravnu osnovu obrade. Odnosno, nužno je moći dokazati da su ispunjeni svi preduvjeti kako bi se ona mogla smatrati zakonitom. Obradu možemo smatrati zakonitom kada je ispitanik dao privolu, kada je obrada nužna za izvršavanje ugovora, kada je nužna kako bi se zaštitili ključni interesi ispitanika ili drugih fizičkih osoba, kada je nužna radi poštovanja pravnih obveza voditelja obrade, kada je nužna za potrebe legitimnih interesa voditelja obrade (osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika).[60]

Kada govorimo o *proporcionalnosti* važno je osigurati da su podaci prikupljeni u posebne, izričite i zakonite svrhe te da se obrađuju u skladu s tim svrhama. Odnosno, da su podaci primjereni i ograničeni isključivo na ono što je nužno za planiranu svrhu. Također, bitno je osigurati da su podaci točni i da se čuvaju samo onoliko dugo koliko je potrebno za svrhu radi koje se obrađuju.

Korak 3. – Dokazivanje sukladnosti
Sukladnost se dokazuje vođenjem detaljnih evidencija koje bi trebale odražavati opću kulturu i pristup promoviranja zaštite podataka. Također, to podrazumijeva postupanje sukladno odobrenim kodeksima ponašanja, obvezujuća korporativna pravila i sl.

Korak 4. – Procjena rizika.
Procjena rizika mora uključivati sve relevantne rizike koje donosi razmatrana obrada, po pitanju prava i sloboda ispitanika. Taj proces podrazumijeva procjenu vjerojatnosti i ozbiljnosti svakog identificiranog rizika.

[60] *Ibid*. Članak 6.

Korak 5. – Definiranje organizacijskih i tehničkih mjera za ublažavanje rizika
Za sve relevantne/identificirane rizike potrebno je predložiti mjere za uklanjanje ili umanjenje rizika. To uključuje različite mjere koje mogu biti organizacijske ili tehničke naravi.

Korak 6. – Izrada izvješća / Bilježenje
Nakon što su utvrđeni i evaluirani rizici te za njih definirane mjere za tretiranje, provedeni postupak i dobivene rezultate po pitanju stanja rizika, prijetnji i vjerojatnosti potrebno je zabilježiti tj. izraditi DPIA Izvješće.

Korak 7. - Redovita provjera.
Bitno je naglasiti kako je cijeli postupak iterativan, kao i pojedine faze koje uključuje. Ovo posebno podrazumijeva ponovno provođenje postupka u slučaju promjene obrade ili tehnologija koje se koriste.

Smjernice definiraju isključivo generalni okvir za oblikovanje i provođenje procjene na zaštitu podataka. Ovo u praksi znači da je proceduru DPIA-e nužno uskladiti sa zahtjevima utvrđenim Općom uredbom o zaštiti podataka, dok se sama provedba procjene može prilagoditi kako bi bila prikladna određenom voditelju obrade i planiranim postupcima obrade .[61] U ovu svrhu unutar Smjernica, u Prilogu 2, definirani su kriteriji za prihvatljivu procjenu učinka na zaštiti podataka ili metodologija za provođenje procjene (prilog 1.)[62]. Cilj je bio pružiti jednostavnu listu za provjeru koja omogućava uvid je li procjena ili metodologija dostatno opsežna za potrebe usklađivanja s Općom uredbom o zaštiti podataka.

U nastavku ćemo obraditi glavna pitanja koja se javljaju prilikom praktične primjene postupka procjene učinka na zaštitu podataka te različite metodologije, pristupe koje definiraju postupak provedbe DPIA-e uz prikaz nekih od dostupni DPIA alata.

[61] *Ibid.* Smjernice o procjeni učinka na zaštitu podataka
[62] *Ibid.* Smjernice o procjeni učinka na zaštitu podataka

4 PRAKTIČNA PITANJA I IZAZOVI POSTUPKA PROCJENE UČINKA NA ZAŠTITU PODATAKA

Cilj Uredbe za zaštitu podataka je pružanje generalnog zakonodavnog okvira što uključuje generalni okvir za provedbu procjene učinka na zaštitu podataka. Ovo posljedično znači da Uredba nije ta koja pruža detaljne informacije kako DPIA-u provesti u praksi, što dovodi do određenih pitanja i izazova u pogledu praktične primjene ovih odredbi.

Prije nego se osvrnemo na različite pristupe provođenja DPIA-e i metode koje su dostupne, korisno je razmotriti proces procjene učinka na podatke na konkretnom primjeru.

Na slici 4.1 prikazan je slučaj hipotetskog razvoja proizvoda/usluge. Dijagramom su prikazane potencijalne ugroze, koraci koje se trebaju provesti kako bi se utvrdilo je li potrebno provesti DPIA-u te koraci kako bi se ona provela. Također, postavljena su i pitanja koja se mogu javiti ili na koja treba obratiti pažnju tijekom provedbe DPIA-e, uz glavne faze koje uključuju; (1.) pokretanje razvoja novog proizvoda ili usluge, (2.) osmišljavanje nove obrade, (3.) procjena rizika i (4.) ublažavanje rizika.

DPIA je proces koji treba započeti prije same obrade podataka[63], a treba se nastaviti za vrijeme čitavog životnog ciklusa definirane obrade.[64]

Glavni fokus ovog procesa je analiza rizika na prava i slobode ispitanika koje uzrokuje obrada na temelju čega se određuju adekvatne mjere za tretiranje rizika što uključuje implementaciju tehničkih i organizacijskih mjera.[65]

[63] *Ibid*. Opća uredba o zaštiti podataka, članak 35, stavak 1.
[64] *Ibid*., članak 35. stavak 11.
[65] Bieker, F., Martin, N., Friedewald, M., & Hansen, M., "*Data Protection Impact Assessment: A Hands-On Tour of the GDPR's Most Practical Tool*", Privacy and Identity Management. The Smart Revolution: 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers 12, str. 207-220.

Kod ispravno provedene DPIA-e rezultat je smanjenje rizika na prava i slobode ispitanika, usklađivanje s regulativom (Općom uredbom) i unapređenje povjerenja među ispitanicima i drugim dionicima.[66]

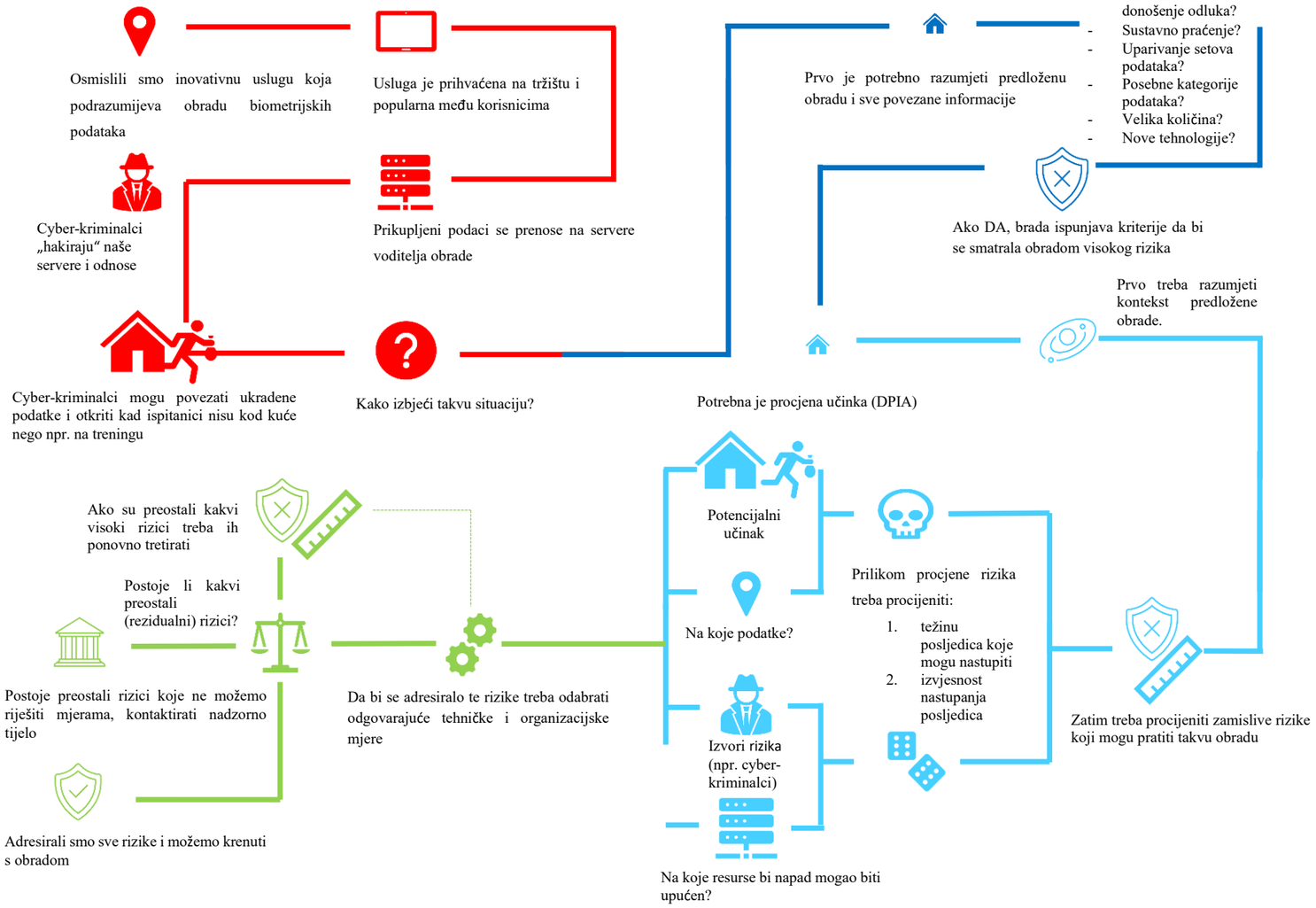
[66] Henriksen-Bulmer, J., Faily, S., Jeary, S., "*DPIA in Context: Applying DPIA to Assess Privacy Risks of Cyber Physical Systems*", Future internet, 12(5), 93., 2020, https://doi.org/10.3390/fi12050093

1.

Pokretanje razvoja novog proizvoda ili usluge

U svijetu se svakodnevno razvijaju brojne digitalne usluge. Te se usluge planiraju odvijati putem infrastrukture voditelja obrade koja je istovremeno podvrgnuta raznim sigurnosnim rizicima.

PROCJENA UČINKA



2.

Osmišljavanje nove obrade

Prije provođenje obrade potrebno je procijeniti rizike i razmotriti faktore poput nabrojanih lijevo. Ako su barem dva ispunjena, riječ je o obradi visokog rizika koja zahtijeva provođenje procjene učinka na zaštitu podataka.

3.

Procjena rizika

Procjena kreće od razumijevanja konteksta predložene obrade. Nakon procjene nužnosti i proporcionalnosti valja ocijeniti svaki pojedinačni rizik i odabrati odgovarajuće mjere koje ga mogu eliminirati ili svesti na prihvatljivu mjeru.

4.

Ublaživanje rizika

Jednom kad su rizici prepoznati, treba postići da se putem primijenjenih mjera prihvati preostala razina rizika, ili obavijestiti nadzorno tijelo. Nema obrade bez primjene adekvatnih mjera.

Slika 4.1 Shema praktične primjene DPIA-e prilikom razvoja novog proizvoda/ usluge – prijevod/prilagođeno prema smjernicama francuskog nadzornog tijela CNIL

4.1 Izazovi

Prema mišljenju određenog broja autora, trenutna regulacija procjene učinka na zaštitu podataka je nejasna i zbunjujuća za organizacije koje obrađuju osobne podatke zbog pomanjkanja jasnih smjernica i zbog mnoštva dostupnih različitih metoda – tekst Opće uredbe kao opća norma nema svrhu konkretnih uputa, već treba osigurati dugoročnu i tehnološki neutralnu pravnu sigurnost oko zahtjeva za voditelje obrade nužnih za osiguranje zaštite podataka ispitanika. Konkretnije upute kako to postići se očekuju kroz provedbene propise ili praksu i smjernice nadzornih tijela, odnosno Europskog odbora za zaštitu podataka. [67,68,69,70]

Prema izvještaju Stručne skupine različitih dionika (*engl. Multi-stakeholder Expert Group*) nakon prve godine od primjene Uredbe, kao jedan od čimbenika koji dovode do neizvjesnosti i nedosljednosti u primjeni DPIA-e jesu razlike između metodologija nadzornih tijela o tome kako je provesti. [71]

Istraživanje iz 2020. godine provedeno od strane Europskog nadzornika za zaštitu podataka (*engl. European Data Protection Supervisor – EDPS*) pokazuje slabe rezultate u odnosu na duljinu i kvalitetu DPIA-e koje provode institucije EU-a. Također, nekoliko preporuka ukazuje na potrebu za referentnom metodologijom procjene rizika unutar DPIA-e.[72]

---

[67] Meis, R., Heisel, M. "*Supporting privacy impact assessments using problem-based privacy analysis*", International Conference on Software Technologies., Springer, Cham, 2015., str. 79-98.
[68] Berendt, B., Littlejohn, A., Kern, P., Mitros, P., Shacklock, X., Blakemore, "Big data for monitoring educational systems". Publications Office of the European Union, Luxembourg, 2017.
[69] van Puijenbroek, J.P.M., Hoepman, J.H., "*Privacy Impact Assessments in Practice: Outcome of a Descriptive Field Research in the Netherlands*", Ceur Workshop Proceedings, Alamo, J.M. del (ed.), IWPE 2017: International Workshop on Privacy Engineering: Proceedings of the 3rd International Workshop on Privacy Engineering, co-located with 38th IEEE Symposium on Security and Privacy (S&P 2017) San Jose (CA), USA, May 25, 2017, str. 1-8.
[70] De, S.J., Le Métayer, D. "*A Refinement Approach for the Reuse of Privacy Risk Analysis Results*", Annual Privacy Forum, Springer, Cham, 2017., str. 52-83.
[71] *Contribution from the Multistakeholder Expert Group to the Stock-Taking Exercise of June 2019 on One Year of GDPR Application*, Multistakeholder Expert Group, Report, 13 June 2019, dostupno na: https://commission.europa.eu/system/files/2019-10/report_from_multistakeholder_expert_group_on_gdpr_application.pdf (09.02.2024.)
[72] *EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (case 2020-0066)*, EDPS (European Data Protection Supervisor), dostupno na: https://edps.europa.eu/sites/edp/files/publication/20-07-06_edps_dpias_survey_en.pdf (09.02.2024.)

Radi gore navedenog dolazi do različitih pitanja i poteškoća prilikom implementacije. Jedan od izazova u praksi je tumačenje apstraktnih zahtjeva čl. 5. Opće Uredbe koji se odnosi na načela obrade osobnih podataka. Na primjer, načela zakonitosti, poštenosti i primjerenosti mogu se smatrati zahtjevnim pravnim konceptima, a pošto njihova konkretna provedba u praksi spada pod odgovornost organizacija koje provode obradu podataka, ponekad nisu adekvatno operacionalizirana.[73]

Problem koji se također javlja u praksi je odgovarajuća razina uvida i detaljnosti prikaza prilikom opisa procesa obrade, odnosno postizanje optimalne razine koja će omogućiti pouzdanu identifikaciju i analizu rizika za prava i slobode ispitanika te posljedično odabir odgovarajućih mjera za tretiranje, a s druge strane neće uzrokovati da postupak procjene učinka postane previše složen.[74]

Nadalje, veliki broj pitanja javlja se prilikom određivanja što podrazumijeva provođenje procjene rizika kao dijela DPIA-e. Iako je „*procjena rizika*" prepoznata kao jedan od koraka DPIA-e (članak 35. stavak 7.), (c)), ne postoji jedinstveni koncept o tome što to znači provesti.[75,76,77] Naime, Smjernice nisu adresirale pitanje metodologije procjene rizika. U Prilogu 2. Smjernica o procjeni učinka na zaštitu podataka (prilog 1.) navedeni su isključivo generalni kriteriji za procjenu sveobuhvatnosti metodologije DIPA-e ili provedene procjene koja obuhvaća i proces procjene rizika (odražavajući članak 35. stavak 7. točka (c)). Ovaj pristup nažalost ne ukazuje jasno kako provesti segment procesa DPIA koji se odnosi na procjenu rizika. Također, izostaju informacije kako kvantificirati preostale (rezidualne) rizike za aktiviranje članka 36.

[73] Friedewald, M., Schiering, I., Martin, N., Hallinan, D., "*Data Protection Impact Assessments in Practice: Experiences from Case Studies*.", European Symposium on Research in Computer Security, Springer, Cham, 2021., str. 424-443.
[74] Martin, N., Friedewald, M., Schiering, I., Mester, B. A., Hallinan, D., & Jensen, M., "*The Data Protection Impact Assessment According to Article 35 GDPR*", ", Fraunhofer Institute for Systems and Innovation Research ISI, 2020.
[75] van Dijk, N., Gellert, R., Rommetveit, K., "*A risk to a right: beyond data protection impact assessments?*" Comput. Law Secur. Rev. 32(2), 2016., str. 286–306.
[76] Gellert, R., "*Understanding the notion of risk in the General Data Protection Regulation*", Comput. Law Secur. Rev. 34(2), 2018., str. 279–288.
[77] Hallinan, D., Martin, N., "*Fundamental rights, the normative keystone of DPIA*", Eur. Data Prot. Law Rev. 6(2), 2020., str. 178–193.

U narednom poglavlju dat ćemo prikaz na što se odnosi procjena rizika na prava i slobode ispitanika te koje elemente mora uključivati.

4.1.1 Procjena rizika i mjere za tretiranje rizika

Kako bi definirali što podrazumijeva procjena rizika definirana člankom 35, stavkom 7 u točki (c), prvo se moramo osvrnuti na to kako je rizik definiran Općom uredbom. U Općoj uredbi ne uvodi se jasna definicija rizika, već se umjesto toga nude interpretativne smjernice o tome što može predstavljati rizik i štetu za ispitanike.[78]

Prema jednoj često upotrebljavanoj definiciji u informacijskoj sigurnosti, rizik se definira kombinacijom vjerojatnosti događaja (incidenta) i njegovih posljedica.[79] S druge strane, Općom uredbom, u uvodnoj izjavi 75., pojam „*rizik*“ koristi znatno šire te označava rizične aktivnosti obrade ili „*prijetnje*“ koje bi mogle rezultirati štetom za ispitanika. Stoga bi definiciju rizika, u kontekstu Opće uredbe i DPIA-e mogli postaviti kao „vjerojatnost da će aktivnost obrade podataka rezultirati negativnim utjecajem, prijetnjom ili gubitkom (različitih razina težine) prava i sloboda ispitanika.[80] Prema tome, neprihvatljivi rizik je onaj koji rezultira znatnom prijetnjom ili gubitkom prava i sloboda ispitanika, a nije ga moguće umanjiti primjenom odgovarajućih mjera.

Ovo nas dovodi do koncepta „*procjene rizika*“ koji u praksi podrazumijeva identificiranje rizika, nakon čega slijedi uklanjanje tj. tretiranje neprihvatljivih rizika, s obzirom da je nemoguće ukloniti sve rizike.

Prilikom procesa procjene rizika u obzir je potrebno uzeti vjerojatnost povrede te ozbiljnost povrede za prava i slobode ispitanika, gdje „*vjerojatnost*“ podrazumijeva vjerojatnost ostvarivanja rizika ili utjecaja rizika, a „*ozbiljnost*“ očekivani učinak ako

[78] *Ibid*. uvodna izjava 75.
[79] Katsikas, S. K., “*Risk Management*”, Part V, Chapter 35 in “Computer and Information Security Handbook”, J. R. Vacca, Second Edition (2nd. ed.). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2013, str. 605-625
[80] *Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR*, White Paper, CIPL (Centre for Information Policy Leadership at Hunton & Williams LLP), 2016.

se rizik tj. štetni događaj ostvari.[81] Dodatno, Uvodna izjava 77., članak 31. u stavku 1. te članak 24. u stavku 1. definiraju kako se prilikom utvrđivanja rizika, osim vjerojatnosti i ozbiljnosti (težine) treba uzeti u obzir i prirodu, opseg, kontekst i svrhe obrade. Također, rizik bi trebalo procjenjivati na temelju objektivne procjene kojom se utvrđuje uključuju li postupci obrade podataka rizik ili visoki rizik.[82] Odnosno, organizacije moraju osigurati procese koji im omogućuju pouzdanu i dosljednu procjenu rizika i posljedica na prava i slobode ispitanika kako bi bile u skladu s odredbama Opće uredbe.

Sljedeći uvjet za usklađivanje je svakako odabir relevantnih tehničkih i organizacijskih mjera, tj. osiguravanje da organizacija ima sposobnost ublažavanja "*visokog rizika*". U slučaju nemogućnosti ublažavanja visokog rizika organizacije su prema Uredbi dužne provesti „*prethodno savjetovanje*“.[83]Odgovore kako konkretno pristupiti procjeni rizika i događaja koji mogu uzrokovati visoki rizik za prava i slobode ispitanika, tj. postupci kako identificirati i definirati razinu rizika, definirani su različitim metodologijama čiji je prikaz dan u narednom poglavlju (poglavlje 4.2). Također, poglavlje će se osvrnuti i na segment definiranja odgovarajućih tehničkih i organizacijskih mjera.

4.2 Najčešće korištene metodologije

Činjenica da Opća uredba definira samo generalne zahtjeve za provođenje procjene učinka na zaštitu podataka dovela je do razvoja velikog broja metodoloških okvira za

[81] *Ibid*. uvodna izjava 76.
[82] *Ibid*. uvodna izjava 76.
[83] *Ibid*. članak 36.

njeno provođenje, što uključuje metodologije različitih nadzornih tijela[84,85,86], akademije[87,88], standardizacijskih tijela[89, 90] i trgovačkih udruženja.[91]

Same smjernice WP29, u Prilogu 1 daju primjere dobrih praksi, odnosno postojećih općih i specifičnih okvira u pogledu procjene učinka na zaštitu podataka.

U radu će biti uključene sljedeće metodologije nadzornih tijela:

- Francuska: Procjena učinka na privatnost[92]
- Ujedinjeno Kraljevstvo: Primjena kodeksa postupanja tijekom provedbe učinka na privatnost, Ured povjerenika za pravo na pristup informacijama (ICO)[93]
- Njemačka: Standardni model zaštite podataka V3.0[94]

Također, osvrnut ćemo se na „*Vodič za procjenu učinka na zaštitu podataka za male i srednje poduzetnike*“ koje je izdala Agencija za zaštitu osobnih podataka (AZOP). Nadalje, bit će uključena analiza najčešće korištenih industrijskih standarda i to: OCTAVE Allegro, NIST 8000-30, ISTO 29314 i ITIL 4.

---

[84] Privacy Risk Assessment: Methodology, CNIL (Commission Nationale de l'Informatique et des Libertés), Paris, 2018, dostupno na: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-1-en-methodology.pdf (09.02.2024)

[85] Guide to the General Data Protection Regulation (GDPR), ICO (Information Commissioner's Office), Wilmslow, UK, 2021.

[86] The Standard Data Protection Model V3.0: A method for data protection advising and controlling on the basis of uniform protection goals, Conference of the independent data protection authorities of the Federal and State Governments of Germany, 2022., dostupno na: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM_V3_en.pdf (09.02.2024.)

[87] De, S.J., Le Métayer, D., „*Privacy Risks Analysis*“, Morgan & Claypool, 2016, ISBN: 1627054251.

[88] Kloza, D., et al., "*Towards a method for data protection impact assessment: making sense of GDPR requirements*", d.pia.lab Policy Brief 1/2019, VU Brussels, Brussels, 2019., https://doi.org/10.31228/osf.io/es8bm

[89] ISO/IEC 29134:2023: Information technology - Security techniques - Guidelines for privacy impact assessment. International Standardisation Organisation, Geneva

[90] ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection -Guidance on managing information security risks. International Standardisation Organisation, Geneva

[91] Risk Assessment & Data Protection Impact Assessment – Guide, Federal Association for Information Technology, Telecommunications and New Media (BITKOM), Berlin, 2017., dostupno na: https://www.bitkom.org/sites/main/files/file/import/170919-lf-risk-assessment-eng-online-final.pdf (09.02.2024.)

[92] *Ibid.* Privacy Risk Assessment: Methodology, CNIL

[93] *Ibid*. Guide to the General Data Protection Regulation (GDPR), ICO

[94] *Ibid.* The Standard Data Protection Model V3.0

4.2.1 Analiza smjernica odabranih nacionalnih nadzornih tijela o praktičnoj provedbi procjene učinka

Iako su tijela za zaštitu podataka objavila nekoliko metoda i smjernica, ona slijede različite pristupe i pružaju ograničenu pomoć u tome kako organizirati DPIA projekt. [95] U nastavku će biti prikazane tri različite metodologije, njihovi osnovi koncepti s naglaskom na procjenu rizika te osvrt na glavne prednosti i mane.

4.2.1.1 CNIL – PIA

Metodologija procjene utjecaja na privatnost[96] (engl. Privacy Impact Assessment - PIA) francuske Agencije za zaštitu podataka (*fr. Commission Nationale de l'Informatique et des Libertes - CNIL*) sastoji se od tri vodiča: (I) PIA metodologija[97] koja definira generalni pristup i daje smjernice kako je provesti, (II) PIA predlošci[98] koji sadrže činjenice strukturirane u predlošcima koji se mogu koristiti prilikom provedbe analize te (III) Baza znanja koja daje katalog kontrola usmjerenih na usklađivanje sa zakonskim zahtjevima i tretiranje rizika uz primjere[99].

Ovaj CNIL-ov pristup procjeni učinka na zaštitu podataka je visoko strukturiran i sastoji se od određene vrste sustava pitanja koji prate zakonske odredbe Opće uredbe i ispituje standardne tehničke implementacije. Također, CNIL na raspolaganju ima i podršku softverskog alata za provođenje procjene učinka na zaštitu podataka (više u

[95] Vemou, K., Karyda, M., "*An evaluation framework for privacy impact assessment methods*", The 12th Mediterranean Conference on Information Systems (MCIS), Corfu, Greece, 2018.
[96] Pojam „Procjena utjecaja na privatnost" i pripadajući akronim "PIA" (engl. Privacy Impact Assessment) koristi kao istoznačnica sa „Procjenom učinka na zaštitu podataka (engl. Data Protection Impact Assessment - DPIA)
[97] *Ibid.* Privacy Risk Assessment: Methodology, CNIL
[98] Privacy Impact Assessment (PIA) Templates, CNIL (Commission Nationale de l'Informatique et des Libertés), Paris, 2018, dostupno na: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-2-en-templates.pdf (09.02.2024.)
[99] Privacy Impact Assessment (PIA) Knowledge Bases, CNIL (Commission Nationale de l'Informatique et des Libertés), Paris, 2018., dostupno na: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf (09.02.2024.)

Poglavlju 4.3.1). Proces procjene učinka na zaštitu podataka provodi se u četiri koraka (slika 4.2).

Slika 4.2 Dijagram faza provedbe (D)PIA procesa – CNIL

Koraci podrazumijevaju sljedeće:

Korak 1. - definirati i opisati kontekst obrade osobnih podataka koji se razmatraju;

Korak 2. - analizirati kontrole koje jamče sukladnost s temeljnim načelima;

Korak 3. - procijeniti rizike privatnosti povezane sa sigurnošću podataka i osigurati da se s njima pravilno postupa;

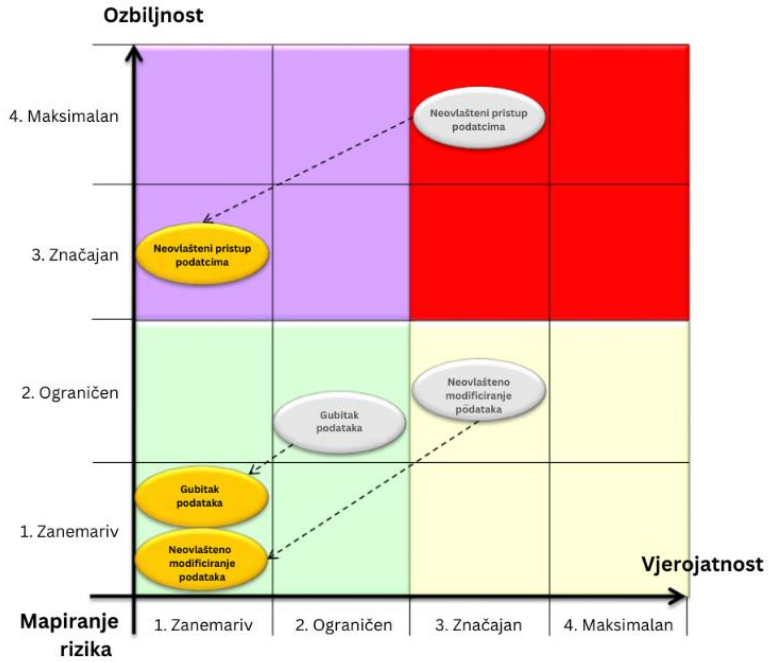
Korak 4. - službeno dokumentirati potvrđivanje PIA-e s obzirom na prethodne činjenice ili po potrebi revidirati prethodne korake.

Prema CNIL-ovom modelu komponente za određivanje razine rizika su: (I) Izvori rizika; (II) Imovina koja podržava osobne podatke; (III) Osobni podaci: (IV) Potencijalni utjecaj. Rizik se temelji na vjerojatnosti i ozbiljnosti povrede, kako slijedi.

Određivanje *ozbiljnosti* ovisi o štetnom učinku potencijalnog utjecaja (IV) na osobne podatke (III), dok je *vjerojatnost* određena temeljem razine ranjivosti imovine koja podržava osobne podatke (II) kada je suočena s prijetnjama te razinom sposobnosti izvora rizika (I) da iste iskoristi.[100]

[100] *Ibid.* Privacy Risk Assessment: Methodology, CNIL

Za procjenu razine rizika dan je prijedlog matrice prikazan na slici 4.3.



Slika 4.3 Matrica za strukturiranje procjene rizika – CNIL

Kao glavnu zamjerku ovog pristupa u literaturi navodi se „*sužena*“ interpretacija rizika, koju CNIL svodi na sigurnosni rizik podataka, dok se procjena rizika ne bi trebala isključivo odnositi na vjerojatnost i ozbiljnost povrede podataka.[101,102]

Iako je sigurnost podataka jedna od glavnih kategorija procjene rizika zaštite podataka, Uredbom je nužno uključiti i druge rizike. To svakako podrazumijeva rizike koji proizlaze iz profiliranja, velike obrade posebnih kategorija podataka, kao i velikog i sustavnog praćenja javno dostupnih područja, čiji se rizici mogu materijalizirati bez ikakve povrede podataka.[103]

[101] Korff, D., Georges, M., “The Data Protection Officer Handbook”, 2019. SSRN: https://ssrn.com/abstract=3428957.
[102] *Ibid.* Gellert, R., str. 279–288.
[103] *Ibid*. Korff, D., Georges, M.

Nadalje, ovom procesu savjetovanje s dionicima nije u središtu procjene već podaci za potrebe provođenja analize dolaze od voditelja obrade. Uključivanje ispitanika provodi se na kraju procesa u svrhu provjere valjanosti rezultata.[104]

Prednost ove metodologije je velika baza znanja s popisom kontrola. Ono što treba naglasiti je da se uglavnom radi o tehničkim kontrolama. Općenito, možemo kazati da CNIL-ova metoda operacionalizira DPIA-u kao provjeru usklađenosti s GDPR-om i IT sigurnosnim zahtjevima.[105]

4.2.1.2 ICO – DPIA

Drugi utjecajni okvir za provođenje DPIA-e razvio je Ured povjerenika za informiranje (*engl. Information Commissioner's Office – ICO*) u Ujedinjenom Kraljevstvu.[106]

ICO DPIA okvir uz smjernice[107] uključuje i predloške[108]. Za provođenje postupka, ICO DPIA smjernice definiraju ukupno devet (9) koraka, dok ih je u predlošcima navedeno sedam (7) (slika 4.4).

[104] *Ibid.* Friedewald, M., Schiering, I., Martin, N., Hallinan, D., str. 424-443.
[105] *Ibid.* Friedewald, M., Schiering, I., Martin, N., Hallinan, D., str. 424-443.
[106] Data protection impact assessments – Guidelines, Information Commissioner's Office (ICO), Wilmslow, UK, 2018., dostupno na: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/ (09.02.2024.)
[107] *Ibid.* Data protection impact assessments – Guidelines, Information Commissioner's Office (ICO)
[108] DPIA template v0.4, Information Commissioner's Office (ICO), Wilmslow, UK, 2018., dostupno na: https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf (09.02.2024.)

Slika 4.4 Dijagram faza provedbe DIPA procesa – ICO

Prvih sedam koraka su isti u oba dokumenta, dok su korak 8 i 9 navedeni isključivo u smjernicama, jer se odnose na uspostavu sustava provođenja DPIA-e, odnosno korake nakon završetka same procjene učinka na zaštitu podataka.

Koraci provođenja iterativnog postupka procjene učinka na zaštitu podataka podrazumijevaju sljedeće:

Korak 1. utvrđivanje potrebe za provođenjem DPIA-e;

Korak 2. – izrada opisa obrade koji mora uključivati prirodu, opseg, kontekst i svrhu obrade;

Korak 3. – razmatranje uključivanja drugih dionika i konzultiranje;

Korak 4. - procjena nužnosti i proporcionalnosti;

Korak 5. - identificiranje i procjena rizika;

Korak 6. – identificiranje adekvatnih mjera za tretiranje rizika;

Korak 7. - zaključivanje i zabilježba rezultata;

Korak 8. - integracija ishoda procjene u planove;

Korak 9. - redovita provjera.

U ICO DPIA predlošcima procjena rizika sugerira da se ovaj proces provodi opisivanjem "*izvora rizika i prirode potencijalnog utjecaja na pojedince*", za koji se potom određuje vjerojatnost povrede, ozbiljnost povrede te ukupni rizik. Smjernice o procjeni rizika daju generalne upute poput: „*Da biste procijenili je li rizik visok, morate uzeti u obzir i vjerojatnost i težinu moguće štete*"[109]. Ovim se ne pojašnjava kako provesti procjenu rizika, no pružaju matricu rizika kako bi dali prijedlog za strukturiranje vjerojatnosti i ozbiljnosti povrede (slika 4.5).

OZBILJNOST POVREDE	Značajna povreda	Niski rizik	Visoki rizik	Visoki rizik
	Srednja povreda	Niski rizik	Srednji rizik	Visoki rizik
	Niska povreda	Niski rizik	Niski rizik	Niski rizik
		Niska vjerojatnost	Srednja vjerojatnost	Visoka vjerojatnost
		VJEROJATNOST POVREDE		

Slika 4.5 Matrica za strukturiranje procjene rizika – ICO

Pristup koji ima ICO DPIA kritiziran je od strane autora kao metodološki neprikladan da bude referentni model procesa provođenja DPIA-e. Kao mana se ističe činjenica da ulazno-izlazni faktori za procjenu nisu opisani. Također, navodi se da su koraci procesa definirani generički (npr. „*prikupljanje informacija*", „*interna analiza*") te da pojedinačni rizici nisu usklađeni s odgovarajućim kontrolama.[110]

4.2.1.3 DSK – SDM

Standardni model zaštite podataka (*engl. Standard Data Protection Model – SDM*) razvilo je njemačko koordinacijsko tijelo koje okuplja državna (savezne države) i federalna tijela za zaštitu podataka - „*Konferencija za zaštitu podataka*" (*njem. Datenschutzkonferenz - DSK*)[111] u suradnji s regionalnim tijelima za zaštitu podataka

[109] Data protection impact assessments – Guidelines, Information Commissioner's Office (ICO)
[110] Oetzel, M. C., Spiekermann, S., "*A systematic methodology for privacy impact assessments: a design science approach*", European Journal of Information Systems, 23(2), 2014., str. 126-150.
[111] DSK - Neovisno tijelo kojeg čine predstavnici njemačkih saveznih i federalnih nadzornih tijela za zaštitu podataka, dostupno na: https://www.datenschutzkonferenz-online.de/dsk.html

i Saveznim povjerenikom za zaštitu podataka i slobodu informacija (*njem. Bundesbeauftragte für den Datenschutz und die Informationsfreiheit - BfDI*).

Standardni model zaštite podataka pruža generalni koncept za implementaciju Opće uredbe za zaštitu podataka, što uključuje i okvir za provedbu DPIA-e uz katalog referentnih mjera s modulima.[112],[113] Dodatno, DSK je objavio i kratke dokumente koji odražavaju jedinstvena stajališta dogovorena od strane njemačkih nadzornih tijela o različitim ključnim temama GDPR-a. Dva su dokumenta ključna za provedbu DPIA-e, kako slijedi:

- Kratki dokument 5 - procjena učinka zaštite podataka prema članku 35. Opće uredbe za zaštitu podataka;[114]
- Kratki dokument 18 - Rizik za prava i slobode fizičkih osoba.[115]

Specifičnost SDM modela je uvođenje koncepta „*ciljeva zaštite*“ (*engl. Protection goals*), a služe umjesto standardnog pristupa zadovoljavanja osnovnih načela definiranih člankom 5. Opće uredbe. Važno je napomenuti da ovaj pristup osigurava apsolutnu sukladnost s osnovnim načelima u čl. 5 uz prevođenje načela u jezik informacijske sigurnosti radi lakše implementacije od strane praktičara.[116] Dodatno, SDM model također uvodi model za operacionalizaciju „*Tehničke i integrirane zaštite podataka*“ gdje se ovi ciljevi mogu ugraditi u dizajn sustava. To rezultira zaštitom osobnih podataka prema unaprijed zadanim postavkama.

Sam proces provedbe DPIA-e organiziran je u 4 osnovne faze prema „*PDCA*“ principu (*engl. Plan-Do-Check-Act*). Svaka od četiri faze: (1) Priprema, (2) Provedba, (3) Primjena i (4) Provjera ima definirane pod-faze (slika 4.6).

---

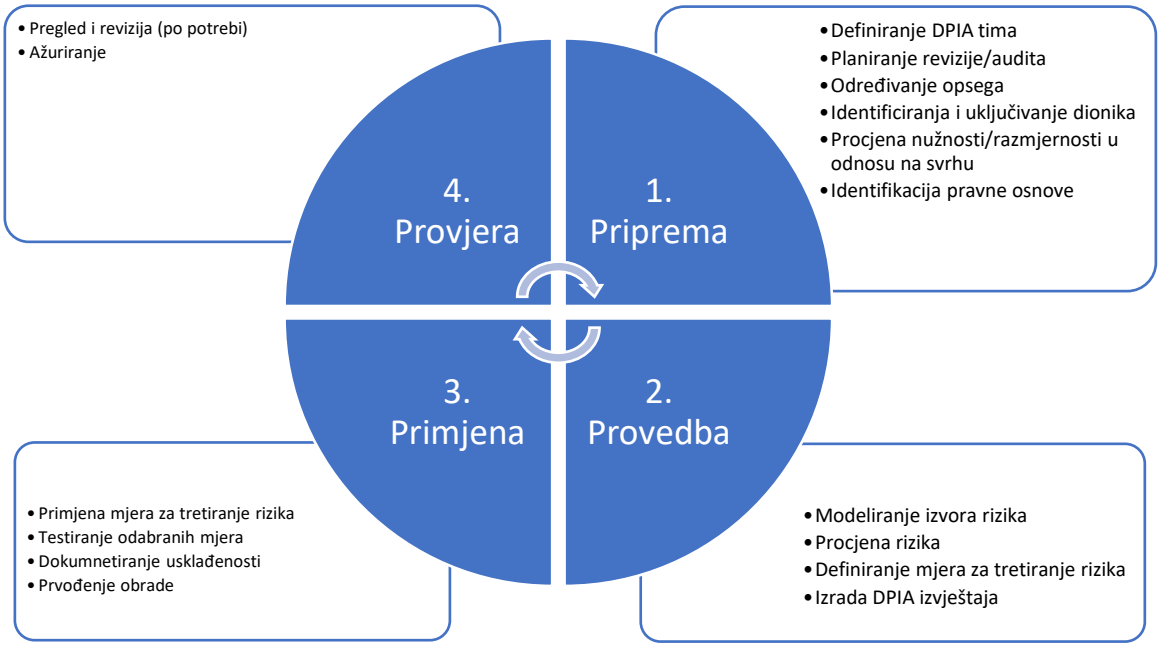
[112] *Ibid.* The Standard Data Protection Model V3.0

[113] SDM Katalog referentnih mjera s modulima, Conference of the independent data protection authorities of the Federal and State Governments of Germany, dostupno na: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ (09.02.2024.)

[114] Kratki rad 5 - procjena učinka zaštite podataka prema članku 35. GDPR-a , Conference of the independent data protection authorities of the Federal and State Governments of Germany, dostupno na: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf (09.02.2024.)

[115] Kratki rad 18 - Rizik za prava i slobode fizičkih osoba, Conference of the independent data protection authorities of the Federal and State Governments of Germany, dostupno na: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (09.02.2024.)

[116] *Ibid*. The Standard Data Protection Model V3.0



Slika 4.6 Dijagram faza provedbe DIPA procesa – DSK

Procjena rizika uključena u SDM dodatno je pojašnjena kroz kratke dokumente 5. i 18.. Dokument 5. koji se odnosi na DPIA-u daje generalnu uputu da se procjena rizika temelji na prirodi, opsegu, konteksta i svrsi obrade podataka.[117] Dok je u dokumentu 18. procjena rizika raščlanjena na 3 faze: identifikacija rizika, procjena vjerojatnosti nastanka i težine mogućih šteta te stupnjevanje rizika.[118] Svaka od faza vođena je nizom pitanja koja bi trebala olakšati implementaciju.

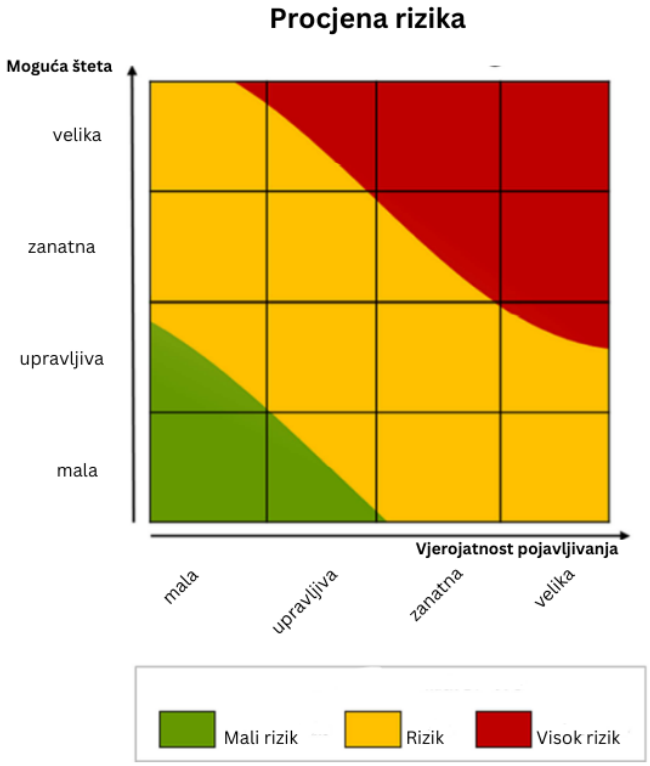
Tako su na primjer za potrebe identifikacije rizika postavljena sljedeća pitanja:

a. Kakva šteta može nastati fizičkim osobama temeljem podataka koji se obrađuju?
b. Kako, tj. koji događaji mogu uzrokovati štetu?
c. Koje radnje i okolnosti mogu uzrokovati pojavu ovih događaja?[119]

[117] *Ibid*. Kratki rad 5 - procjena učinka zaštite podataka prema članku 35. GDPR-a
[118] *Ibid.* Kratki rad 18 - Rizik za prava i slobode fizičkih osoba
[119] *Ibid.* Kratki rad 18 - Rizik za prava i slobode fizičkih osoba

Osim objašnjenja svakog pitanja kako bi se pomoglo procjenitelju rizika, DSK-ov kratki dokument dalje identificira prirodu prijetnji i štete koje bi mogle proizaći iz povrede zaštite podataka.

Za procjenu vjerojatnosti i ozbiljnosti rizika, dokument postavlja neke parametre procjene, koji dovode do ocjenjivanja razine rizika kao "*niskog rizika*", "*rizika*" i "*visokog rizika*".[120] U radu je također predložena matrica rizika (slika 4.7).



Slika 4.7 Matrica za strukturiranje procjene rizika – DSK

[120] *Ibid.* Kratki rad 18 - Rizik za prava i slobode fizičkih osoba

4.2.1.4 AZOP - Vodič za procjenu učinka na zaštitu podataka za male i srednje poduzetnike

Agencija za zaštitu osobnih podataka republike Hrvatske - AZOP u sklopu projekta ARC II[121] razvila je „*Vodič za procjenu učinka na zaštitu podataka za male i srednje poduzetnike*“[122]. Cilj je bio pružiti metodološki pristup i smjernice provođenja DPIA-e primarno za male i srednje poduzetnike (MSP) koji su identificirani kao najvažnija ciljna skupina.

Vodič prvo daje informacije o tome kada je nužno provesti procjenu učinka na zaštitu podataka navodeći devet (9) kriterija iz Smjernica WP29[123] uz praktične primjere. Također, navedena je i poveznica službenog AZOP-ovog popisa vrsta postupaka obrada kada je provođenje procjene učinka na zaštitu podataka obvezno[124]. AZOP dalje uključuje osnovne informacije o odgovornosti za provođenje DPIA-e, kao i nužni sadržaj DPIA-e.

Sam proces provođenja DPIA procesa definiran je u četiri (4) koraka s definiranim pod-koracima, kako slijedi:
Korak 1. – Opis postupka obrade;
Korak 2. – Procjena primjene temeljnih načela - (a) Procjena kontrola koje jamče proporcionalnost i nužnost obrade, (b) Procjena kontrola koje jamče prava ispitanika;
Korak 3. – Procjena rizika – (a) Identificiranje potencijalnih utjecaja na prava i slobode pojedinaca, (b) Identificiranje izvora prijetnje, (c) Procjena vjerojatnosti pojave prijetnje na prava ispitanika, (d) Procjena ozbiljnosti posljedica za prava i slobode ispitanika;

---

[121] Arc II projekt sufinanciran iz programa Europske unije "Prava, jednakost i građanstvo", Ugovor o dodjeli bespovratnih sredstava № 874524, voditelj projekta – AZOP, talijansko nadzorno tijelo za zaštitu podataka Garante Privacy – partner, https://arc-rec-project.eu/o-projektu/
[122] Vodič za procjenu učinka na zaštitu podataka za male i srednje poduzetnike, AZOP (Agencija za zaštitu podataka), dostupno na: https://arc-rec-project.eu/wp-content/uploads/2021/10/Vodic-za-procjenu-ucinka-na-zastitu-podataka-za-SMEs.pdf (09.02.2024.)
[123] *Ibid.* Smjernice o procjeni učinka na zaštitu podataka
[124] Odluka o uspostavi i javnoj objavi popisa vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka, AZOP, dostupno na: https://azop.hr/odluka-o-uspostavi-i-javnoj-objavi-popisa-vrsta-postupaka-obrade-koje-podlijezu-zahtjevu-za-procjenu-ucinka-na-zastitu-podataka/ (09.02.2024.)

Korak 4. – Primjena mjera predviđenih za rješavanje problema rizika.[125]
Kao što je navedeno gore, proces procjene rizika uključuje više pod-faza, a započinje identificiranjem potencijalnih utjecaja na prava i slobode pojedinaca koji mogu uključivati slučajeve poput: neovlaštenog pristupa osobnim podacima, neovlaštene izmjene osobnih podataka te gubitka podataka.

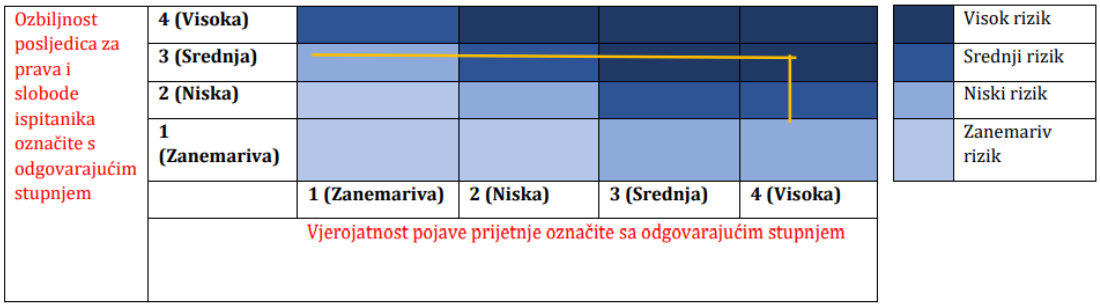
U fazi identificiranja izvora rizika Vodič definira dvije osnovne kategorije: ljudski faktor (djelatnici, korisnici, treće osobe) te ostale faktore (hardware, software, mreža, lokacija, elementarne nepogode, itd.). U fazi identificiranja vjerojatnosti pojave prijetnje dan je prijedlog razina vjerojatnosti s opisom svake od kategorija i primjerima iz prakse:

- Zanemariv – čini se nevjerojatnim da će se rizik ostvariti i materijalizirati u prijetnju (pr. čini se nevjerojatnim da će doći do neovlaštene izmjene podataka u bazi ako se koristi opcija „*zapis logova*“. Ona omogućuje praćenje izmjena te bazi mogu pristupiti samo ovlaštene osobe);
- Nizak - čini se da će teško doći do ostvarenja rizika (pr. čini se da će teško doći do neovlaštene izmjene podataka u bazi kojoj pristup imaju samo ovlaštene osobe);
- Srednji – čini se mogućim da se rizik ostvari (pr. čini se mogućim da dođe do neovlaštene izmjene podataka u bazi koja je osigurana samo lozinkom te dostupna svim zaposlenicima);
- Visok – čini se da je rizik lako ostvariv (pr. čini se da je lako da dođe do neovlaštene izmjena podataka u bazi kojoj se može slobodno pristupiti, bez lozinke).[126]

Za pod-fazu procjene ozbiljnosti posljedica za prava i slobode ispitanika dana je slična skala koja također uključuje opis kategorije i primjer iz prakse radi lakšeg shvaćanja.

Na temelju definiranih razina vjerojatnosti i utjecaja rizik se određuje temeljem matrice. Prikaz matrice za strukturiranje razine rizika prikazan je na slici 4.8.

[125] *Ibid.* Vodič za procjenu učinka na zaštitu podataka za male i srednje poduzetnike
[126] *Ibid.* Vodič za procjenu učinka na zaštitu podataka za male i srednje poduzetnike



Slika 4.8 Matrica za strukturiranje procjene rizika – AZOP

Izvor: AZOP - Vodič za procjenu učinka na zaštitu podataka za male i srednje poduzetnike

Vodič u nastavku daje popis od ukupno 15 generalnih tehničkih i organizacijskih mjera za tretiranje rizika. Na AZOP-ovim stranicama nisu pronađeni dokumenti s ekstenzivnim popisom mjera koje bi bile usmjerene na praktičnu primjenu, ali je dostupna poveznica na različite predloške[127]. Ona uključuje i predložak za procjenu učinka na zaštitu podataka (razvijen u sklopu ARC II projekta).[128]

4.2.2 Pregled primjenjivih industrijskih standarda za procjenu rizika

Prikazane metodologije odabranih nacionalnih tijela daju više ili manje detaljne preporuke kako provesti procjenu rizika tijekom procjene utjecaja na zaštitu podataka, no ostavljaju prostor da organizacije ovaj proces prilagode svojim potrebama. U ovom poglavlju osvrnut ćemo se na često upotrebljavane industrijske standarde za procjenu rizika, a u pregled ćemo uključiti okvire OCATVE Allegro, NIST 800-30, ISO 29134 i ITIL 4.

Prije pregleda je važno napomenuti da metodologije za provođenje procjene rizika koje nude navedeni okviri nisu uvijek u potpunosti usklađeni s Općom uredbom za zaštitu podataka. Odnosno, imaju određena ograničenja koja se mogu manifestirati kao nemogućnost identificiranja rizika ili nekih aspekata rizika kojima su osobni podaci izloženi.

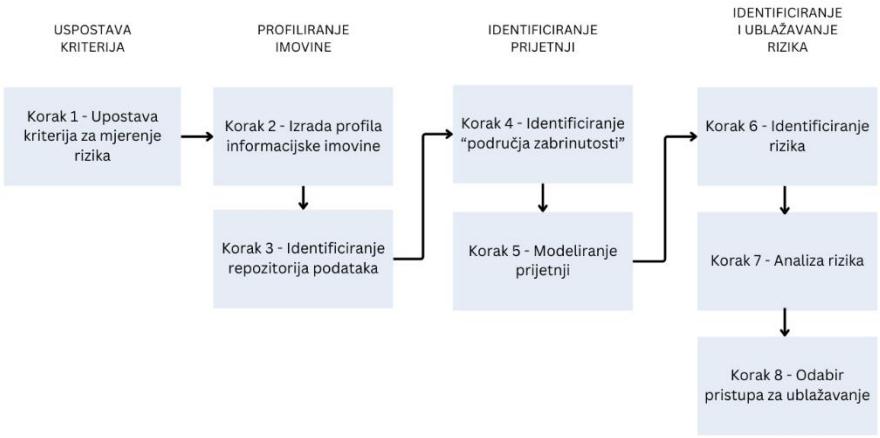
[127] AZOP predlošci - https://azop.hr/obrasci-predlosci/
[128] Predložak za procjenu učinka na zaštitu podataka, AZOP (Agencija za zaštitu podataka), dostupno na: https://azop.hr/wp-content/uploads/2020/12/7-DPIA-obrazac_procjena_ucinka-1.docx (09.02.2024.)

4.2.2.1 OCTAVE Allegro

OCTAVE Allegro je metodologija u čijem imenu je definiran i njen fokus: odnosi se na operativno kritične prijetnje, imovinu i procjenu ranjivosti. (*eng. Operationally Critical Threat, Asset, and Vulnerability Evaluation - OCTAVE*). Ovu metodologiju od strane akademije razvija Sveučilište Carnegie Mellon iz Sjedinjenih Američkih Država.[129]

Primarno se koristi kod manjih organizacija radi pojednostavljenja postupka te velikog raspona radnih listova i predložaka koji pomažu u procesu procjene rizika. To je čini jednostavnom za korištenje i lakše razumljivom za korisnike s manje iskustva te smanjuje potrebu za stručnjacima iz područja informacijske sigurnosti.[130]

Proces procjene rizika podijeljen je u 8 koraka kako je prikazano na slici 4.9.



Slika 4.9 Koraci provođenja procjene rizika - OCTAVE Allegro

Prvi korak u procesu OCTAVE Allegro uključuje uspostavljanje kriterija za mjerenje rizika tijekom procesa procjene rizika usmjerenih na misiju i poslovne ciljeve organizacije. Ove kvalitativne mjere čine temelj procjene rizika informacijske imovine, osiguravajući dosljedno donošenje odluka za ublažavanje rizika.[131]

[129] Caralli, R. A., Stevens, J. F., Young, L. R., Wilson, W. R., "Introducing octave allegro: Improving the information security risk assessment process", Hansom AFB, MA, 2007., dostupno na: https://insights.sei.cmu.edu/documents/786/2007_005_001_14885.pdf (09.02.2024.)
[130] *Ibid.*
[131] *Ibid.*

Metodologija OCTAVE Allegro u fokus stavlja informacijsku imovinu organizacije te **drugi korak** uključuje stvaranje profila za tu imovinu. Profil predstavlja jedinstvene značajke, kvalitete, karakteristike i vrijednost imovine. Ovaj proces profiliranja osigurava jasne i dosljedne opise imovine s definiranim granicama i sigurnosnim zahtjevima. Svako sredstvo ima jedan radni list koji bilježi njegov profil za usmjeravanje identifikacije prijetnji i rizika u kasnijim koracima.[132]

U **trećem koraku** definiraju se repozitoriji podataka koji omogućuju pohranu, transport i obradu informacijske imovine kako bi se naknadno moglo adekvatno procijeniti rizike informacijske imovine.[133]

Četvrti korak podrazumijeva proces identifikacije rizika razmišljanjem o mogućim uvjetima ili situacijama koje mogu ugroziti informacijsku imovinu tzv. „*područjima zabrinutosti*“. Ovi scenariji iz stvarnog svijeta predstavljaju prijetnje i njihove neželjene ishode kako bi se zabilježile jedinstvene prijetnje koje mogu biti specifične za organizaciju.[134]

Daljnja razrada identificiranih „*područja zabrinutosti*“ nastavlja se u **petom koraku** koji se provodi u dvije faze. U prvoj fazi petog koraka, identificirana „*područja zabrinutosti*“ proširuju se u scenarije prijetnji koji dodatno opisuju svojstva prijetnje, dok se u drugoj fazi razmatra široki raspon dodatnih prijetnji ispitivanjem scenarija prijetnji. [135]

U **šestom koraku** identificiraju se u posljedice za organizaciju ako se prijetnja ostvari, čime se upotpunjuje slika rizika. Provođenje ovog koraka omogućava da se zabilježe različite posljedice rizika.[136]

U **sedmom koraku** određuje se kvantitativna mjera razine utjecaja identificiranih prijetnji koja se temelji na odnosu posljedica rizika i definiranih razina važnosti

[132] *Ibid*. Caralli, R. A., Stevens, J. F., Young, L. R., Wilson, W. R.
[133] *Ibid*.
[134] *Ibid*.
[135] *Ibid*..
[136] *Ibid*.

različitih područja utjecaja za neku organizaciju. Za primjer možemo uzeti situaciju u kojoj je reputacija najvažnija za organizaciju. U tom slučaju rizici koji utječu na reputaciju organizacije će generirati više ocjene od rizika s jednakim učincima i vjerojatnostima u nekom drugom, manje važnom području.[137]

U **osmom** i posljednjem koraku procesa OCTAVE Allegro, određuju se prioriteti te se razvija strategija ublažavanja za identificirane rizike na temelju njihove ocjene. Strategije ublažavanja uzimaju u obzir vrijednost imovine, sigurnosne zahtjeve, informacijske repozitorije i jedinstveno okruženje organizacije.[138]

OCTAVE Allegro metodologija se fokusira na imovinu te rizik definira kao događaj s odgovarajućom posljedicom i neizvjesnošću. Umjesto vjerojatnosti, OCTAVE Allegro uvodi subjektivne procjene posljedica u obliku područja utjecaja, što otežava razlikovanje, određivanje prioriteta i komuniciranje rizika s jednakim posljedicama. S obzirom na opisani pristup, OCTAVE Allegro ne zadovoljava nužne kriterije za provođenje procjena rizika prema WP29 Smjernicama.[139]

4.2.2.2 NIST 800-30

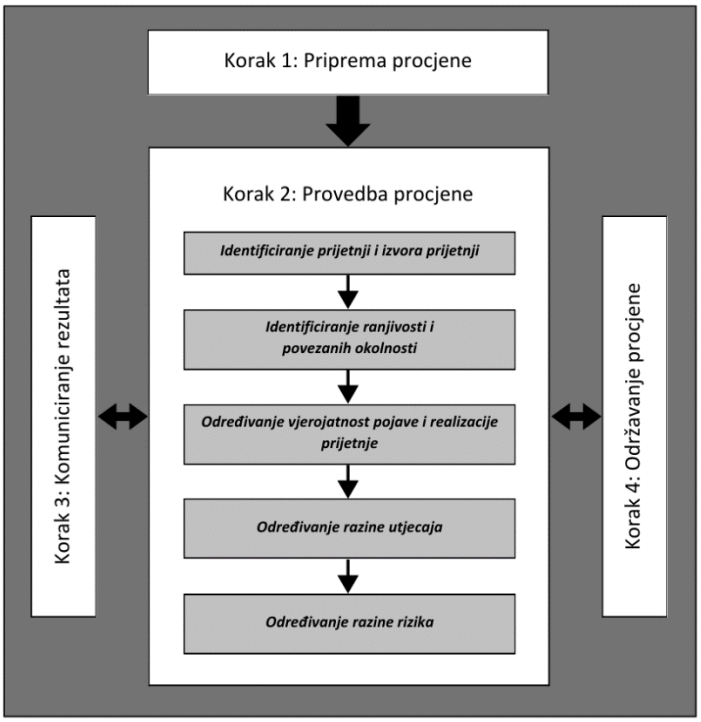
NIST 800-30 je posebna publikacija Nacionalnog instituta za standarde i tehnologiju Sjedinjenih Američkih Država (*engl. National Institute of Standards and Technology – NIST*) koja pruža smjernice za provođenje procjene rizika organizacija i IT sustava kao dijela ukupnog procesa upravljanja rizicima.[140]

NIST 800-30 pruža strukturirani pristup za procjenu i upravljanje rizicima koji uključuje identificiranje specifičnih čimbenika rizika, razine rizika te kontinuirano praćenje i identifikaciju promjena razine rizika.[141]

---

[137] *Ibid*. Caralli, R. A., Stevens, J. F., Young, L. R., Wilson, W. R.
[138] *Ibid*..
[139] Wangen, G., "*Information Security Risk Assessment: A Method Comparison*", Journal of latex class files, 6 (1), 2007., str.1-7.
[140] NIST Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments, 2012.
[141] *Ibid*. NIST Special Publication (SP) 800-30

Prema NIST-u, proces procjene rizika podijeljen je u 4 osnovna koraka (slika 4.10) koji su zatim podijeljeni u pod-korake tj. zadatke.



Slika 4.10 Koraci provođenja procjene rizika – NIST

Prvi korak u ovom procesu je priprema za procjenu rizika. [142] To uključuje nekoliko važnih zadataka, uključujući utvrđivanje svrhe i opsega procjene. Osim toga, identificiraju se sve pretpostavke i ograničenja koja mogu utjecati na proces procjene. Nadalje, korak uključuje identificiranje izvora informacija koji će se koristiti kao ulazni parametri za procjenu, što se ističe kao ključno za dobivanje pouzdanih i relevantnih podataka.

Na kraju slijedi određivanje odgovarajućeg modela rizika i analitičkih pristupa koji će se koristiti tijekom faze procjene. NIST definira ove zadatke kao osnovu za uspostavu čvrstog temelja za provođenje procesa procjene rizika koji je sljedeći korak.[143]

[142] *Ibid*. NIST Special Publication (SP) 800-30
[143] *Ibid*. NIST Special Publication (SP) 800-30

Drugi korak započinje identificiranjem relevantnih izvora prijetnji temeljem čega se identificiraju prijetnje (događaji) koje mogu izazvati ti izvori. Sljedeći zadatak je identificiranje ranjivosti koje različiti izvori prijetnje mogu iskoristiti, uzimajući u obzir identificirane specifične prijetnje i povezane okolnosti koje bi mogle utjecati na realizaciju. Slijedeća 2 zadatka podrazumijevaju određivanje vjerojatnosti pojave i realizacije prijetnje te određivanje razine posljedica/utjecaja tj. štete koje proizlaze iz iskorištavanja ranjivosti od strane izvora prijetnji. Na temelju ove dvije vrijednosti definira se konačna razina rizika koji se razmatrao.[144]

Treći i četvrti korak podrazumijevaju komuniciranje nalaza o procijenjenim rizicima te kontinuiranu provjeru razine rizika kao segmenta sveukupnog upravljanja rizicima.[145]

NIST-ove smjernice osiguravaju skup predložaka, tablica i ljestvica za procjenu faktora rizika te omogućuju fleksibilnost u dizajniranju procjena rizika na temelju svrhe, opsega, pretpostavki i ograničenja koje su uspostavile organizacije.

Valja napomenuti kako proces odabira i procjene mjera za tretiranje rizika nije uključen u ovom NIST dokumentu, već u odvojenim dokumentima NIST SP 800-53 i NIST SP 800-53A.[146,147]
NIST 800-30 pruža pristup procjene rizika koji se fokusira na prijetnje uz dobro adresiranje zahtjeva Opće uredbe za uključivanje faktora rizika prilikom procjene – izvora i prirode rizika, prijetnji te vjerojatnosti i ozbiljnosti utjecaja.[148,149,150]

[144] *Ibid*. NIST Special Publication (SP) 800-30
[145] *Ibid*. NIST Special Publication (SP) 800-30
[146] NIST Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, 2020
[147] NIST Special Publication (SP) 800-53A, Assessing Security and Privacy Controls in Information Systems and Organizations, 2022
[148] *Ibid.* članak 35. stavak 7. točka (c)
[149] *Ibid.* uvodna izjava 90.
[150] *Ibid.* uvodna izjava 84.

4.2.2.3 ISO 29134

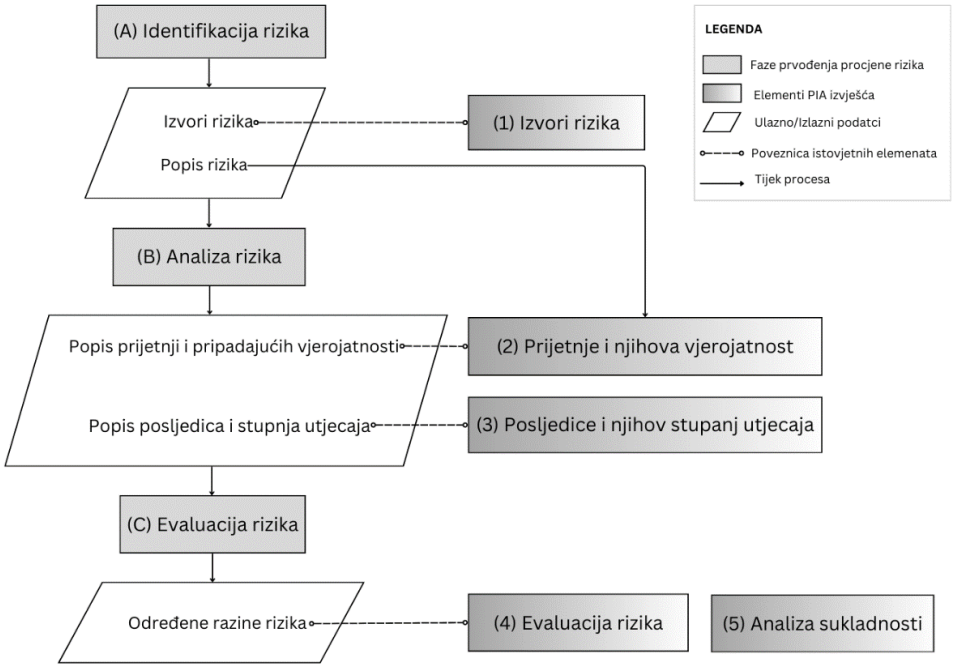
Međunarodna organizacija za standardizaciju (*engl. International Organization for Standardization – ISO*) objavila je smjernice za procjenu utjecaja na privatnost s ciljem pružanja okvira za provođenje procesa procjene utjecaja na privatnost i strukture te sadržaja finalnog izvješća. [151,152] Izrađen je na način da bude široko primjenjiv za različite vrste i veličine organizacija, uključujući javna poduzeća, privatne tvrtke, vladine subjekte i neprofitne organizacije.[153]

Ovaj standard nudi detaljne smjernice o tome kako provesti PIA, posebno o procesu procjene rizika. Usvaja ISO rječnik za upravljanje rizikom[154] pa tako koristi izraz "*osobni podaci za identifikaciju*" (*engl. Personally Identifying Information - PII*), dok Opća uredba u tu istu svrhu koristi izraz „*osobni podaci*“.[155]

U nastavku ćemo se osvrnuti primarno na proceduru procjene rizika i njenu promjenjivost prilikom provođenja DPIA-e, uz osvrt na usklađenost s Općom uredbom i WP29 smjernicama.

Proces procjene rizika podijeljen je u 3 osnovna koraka: (A) Identifikacija rizika, (B) Analiza rizika i (C) Evaluacija rizika. U izvješću o provedenoj procjeni moraju se navesti sljedeći elementi: (1) Izvori rizika; (2) Prijetnje i njihova vjerojatnost; (3) Posljedice i njihov stupanj utjecaja; (4) Evaluacija rizika; (5) Analiza sukladnosti (slika 4.11).[156]

[151] *Ibid.* ISO/IEC 29134:2023
[152] Pojam „Procjena utjecaja na privatnost“ i pripadajući akronim "PIA" (engl. Privacy Impact Assessment) koristi kao istoznačnica sa „Procjenom učinka na zaštitu podataka (engl. Data Protection Impact Assessment - DPIA)
[153] *Ibid.* ISO/IEC 29134:2023
[154] Prva verzija rječnika bila je dana u ISO Vodič 73:2009 Upravljanje rizikom – Rječnik, koja je zamijenjena s ISO 31073:2022 Upravljanje rizikom — Rječnik.
[155] *Ibid.* Opća uredba o zaštiti podataka
[156] *Ibid.* ISO/IEC 29134:2023



Slika 4.11 Dijagram toka procjene učinka na privatnost i elementi (D)PIA izvješća – ISO

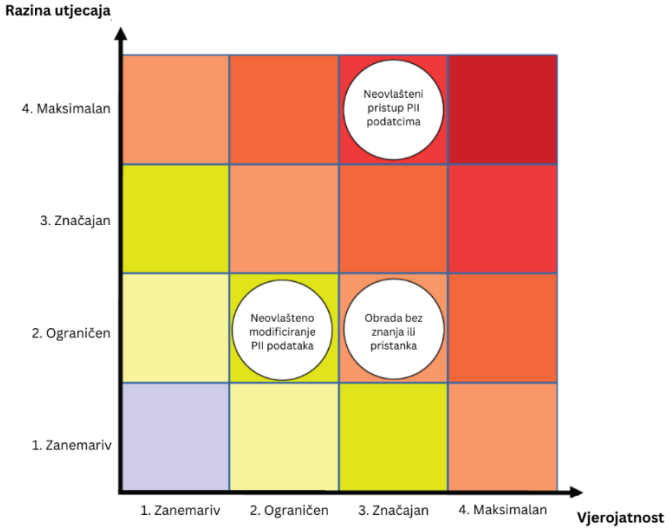
Prvi korak ima za cilj identificirati rizike privatnosti i izvore rizika koji proizlaze iz programa, informacijskog sustava ili procesa koji se procjenjuje.[157] ISO 29134 navodi popis rizika privatnosti (uz napomenu da popis nije konačan) koji uključuje neovlašteni pristup, modificiranje, gubitak osobnih podataka, prekomjerno prikupljanje podataka, neprikladno povezivanje, nedostatak transparentnosti obrade, neuvažavanje prava ispitanika po pitanju prava na pristup, obradu bez znanja ili pristanka, dijeljenje s trećim stranama bez pristanka i nepotrebno produljeno zadržavanje.[158] Ovim ISO 29134 adresira temeljna načela Uredbe[159] te ih postavlja kao osnovu za provođenje procesa procjene rizika.

Na temelju rezultata prvog koraka, u **drugom koraku** provodi se identificiranje i vrednovanje utvrđenih prijetnji koje mogu omogućiti pojavu definiranih rizika. Također, određuju se moguće posljedice i stupanj njihovog utjecaja. Analiza rizika uključuje identifikaciju PII podataka i prateće imovine koja bi mogla biti izložena

[157] *Ibid.* ISO/IEC 29134:2023
[158] *Ibid.* ISO/IEC 29134:2023
[159] *Ibid.* članak 5.

riziku, ranjivosti povezanih s tom imovinom, prijetnji koje bi mogle iskoristiti te ranjivosti, vjerojatnosti i utjecaja da se to dogodi, kao i svih postojećih kontrola koje bi mogle utjecati na rizik.[160] Moraju se uzeti u razmatranje uzroci i izvori rizika, njihove posljedice te vjerojatnost njihove realizacije što podrazumijeva i identificiranje čimbenika koji utječu i na posljedicu i na vjerojatnost.

Treći korak ima za cilj odrediti prioritete identificiranih rizika privatnosti. Razina rizika privatnosti trebala bi proizaći iz procjene razine utjecaja i vjerojatnosti procijenjenih rizika, za što ISO standard prilaže primjer matrice (slika 4.12).



Slika 4.12 Matrica za strukturiranje procjene rizika – ISO

Iako Opća uredba za zaštitu podataka nije korištena kao normativni okvir za izradu ISO 29134 standarda, možemo zaključiti da je procedura definirana za procjenu rizika sukladna sa zahtjevima Opće uredbe i WP29 smjernica.

[160] *Ibid.* ISO/IEC 29134:2023

4.2.2.4 ITIL 4

ITIL 4 je razvila je AXELOS grupa s ciljem pružanja sveobuhvatnih, praktičnih i fleksibilnih smjernica upravljanje informacijskom tehnologijom u modernoj uslužnoj ekonomiji, uključuje robustan pristup procjeni rizika.[161, 162]

ITIL 4 sastoji se od dvije ključne komponente koje uključuju (i) četvero-dimenzionalni model upravljanja uslugama te (ii) sustav vrijednosti usluga. Model upravljanja uslugama definira ključne elemente koji se moraju uzeti u obzir kako bi se osigurao holistički pristup, a podrazumijeva (1) organizaciju i ljude, (2) informacije i tehnologiju, (3) partnere i podizvođače te (4) tokove vrijednosti i procese.[163] Sustav vrijednosti usluge stvara koncept sinergije svih komponenti i aktivnosti organizacije u svrhu olakšavanja stvaranja vrijednosti.

ITIL 4 praksa upravljanja rizikom uključuje sljedeće obavezne elemente tj. faze: (I) Uspostava upravljačkog okvira za upravljanje rizicima, (II) osiguravanje povoljnog okruženja za upravljanje rizicima i prepoznavanje rizika, (III) analiziranje i procjena rizika te (IV) tretiranje, praćenje i pregled rizika.[164]

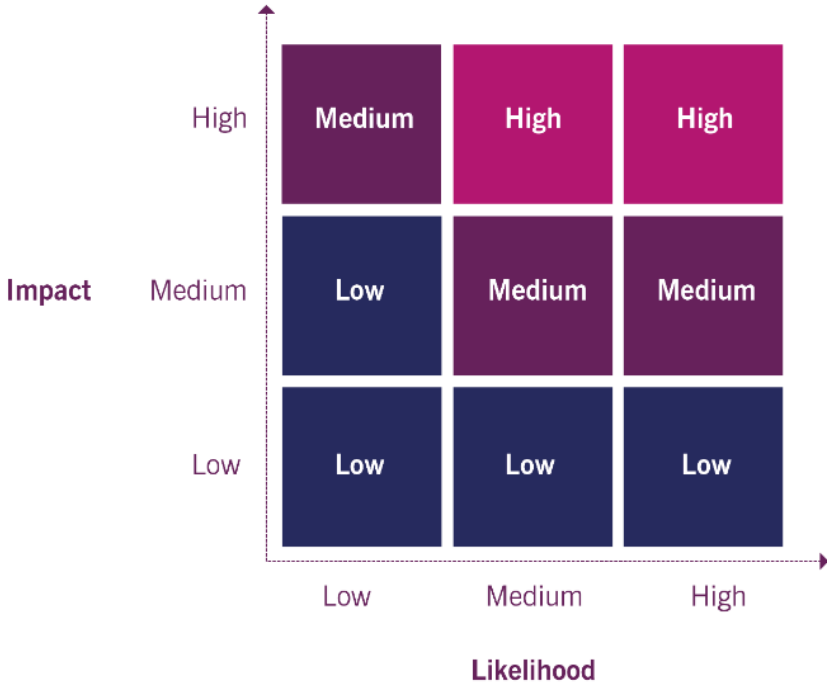
Prva faza podrazumijeva definiranje kapaciteta organizacije za rizik, apetita za rizike i strateških rizika. Ovo je aktivnost koju provode ključne osobe za upravljanje organizacijom.[165]

Druga faza kao ključnu aktivnost uključuje identificiranje rizika. Za identificiranje rizika po ITIL 4 potrebno je provesti analizu okoline što uključuje analizu političkih, ekonomskih, socijalnih tehnologijskih i okolišnih faktora (*engl. Political, Economic,*

[161] ITIL 4 wiki, informacije dostupne na: https://wiki.en.it-processmaps.com/index.php/ITIL_4
[162] ITIL 4, informacije dostupne na: https://www.axelos.com/certifications/itil-service-management/what-is-itil (09.02.2024.)
[163] ITIL 4, informacije dostupne na: https://wiki.en.it-processmaps.com/index.php/ITIL_4 (09.02.2024.)
[164] ITIL 4, informacije dostupne na: https://wiki.en.it-processmaps.com/index.php/ITIL_4 (09.02.2024.)
[165] ITIL 4, informacije dostupne na: https://www.axelos.com/certifications/itil-service-management/what-is-itil (09.02.2024.)

Social, Technological, Legal and Environmental - PESTLE), analizu konkurencije, regulatorne zahtjeve te prijetnje. Nadalje, potrebno je dokumentirati utvrđeni kapacitet i apetit za rizike, kao i izraditi politiku i proračun za upravljanje rizicima. Na temelju provedene analize i izrađene dokumentacije daju se jasne upute upravi organizacije za daljnje postupanje. Nakon što je rizik identificiran, organizacija ga može evidentirati u registar rizika i njime upravljati.

Uz ovaj proces, kao ključni segment, ITIL 4 ističe i osiguravanje povoljnog okruženja za upravljanje rizicima.[166] **U trećoj fazi** provodi se analiza i procjena rizika u kojoj se definiraju vjerojatnosti i posljedice za svaki rizik. Analiza se može provesti kvalitativnim ili kvantitativnim metodama. Kvalitativna analiza rizika koristi jednostavne ljestvice i matrice kako bi se razlikovale različite razine vjerojatnosti i posljedice te time posljedično definirala razina rizika (slika 4.13).



Slika 4.13 Matrica za strukturiranje procjene rizika – ITIL 4

Izvor: Risk management: ITIL 4 Practice Guide, https://www.axelos.com/resource-hub/practice/risk-management-itil-4-practice-guide

[166] ITIL 4, informacije dostupne na: https://www.axelos.com/certifications/itil-service-management/what-is-itil (09.02.2024.)

Kvantitativna analiza rizika provodi se primarno razmatranjem rizika na financijskoj osnovi. ITIL 4 kao primjere navodi sljedeće metode: Godišnja stopa pojavljivanja (*engl. Annual rate of occurrence - ARO*), Očekivanje pojedinačnog gubitka (*engl. Single loss expectancy – SLE*) te Očekivani gubitak na godišnjoj razini (*engl. Annualized loss expectancy – ALE*).

Razine rizika se potom bilježe u registru rizika na temelju čega se potom definiraju odgovarajuće mjere za tretiranje rizika.[167]

Četvrta faza uključuje tretiranje, praćenje i pregled rizika**.** Kada se donese odluka o upravljanju rizikom, potrebno je dizajnirati i implementirati odgovarajuće mjere za tretiranje rizika. Ovaj postupak uključuje primjenu ali i praćenje provedbe mjera i rizika kako bi se osiguralo da su mjere relevantne za identificiranu razinu rizika te da ih se pravilno provodi.[168]

4.3 Pregled i analiza softverskih alata za provedbu procjene učinka na zaštitu podataka

Nakon što je Općom uredbom uvedena obaveza provođenja procjene učinka na zaštitu podataka u situacijama kada će obrada vjerojatno uzrokovati visoki rizik na prava i slobode pojedinaca, došlo je do razvoja digitalnih alata za automatizaciju tog procesa. Ranije se taj proces provodio koristeći uredske alate za tablično računanje te pisanje i oblikovanje tekstualnih dokumenata.

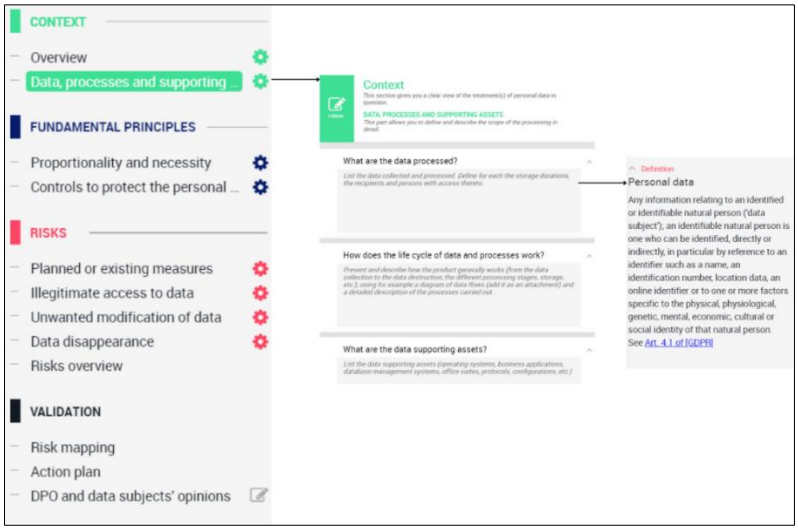
Automatizacija DPIA procesa kao posljedicu ima određenu vrstu „*standardizacije*“ procesa tj. osiguravanje dosljedne kvalitete, što je posebno bitno uzmemo li u obzir da je proces iterativan. Također, vođeni pristup olakšava samu provedbu te je čini učinkovitijom. Na raspolaganju je veliki broj rješenja, od kojih su neka besplatna i

[167] ITIL 4, informacije dostupne na: https://www.axelos.com/certifications/itil-service-management/what-is-itil
[168] ITIL 4, informacije dostupne na: https://www.axelos.com/certifications/itil-service-management/what-is-itil

javno dostupna, a druga komercijalna. U nastavku poglavlja bit će dan pregled odabranih alata i njihove osnovne funkcionalnosti.

4.3.1 CNIL - PIA digitalni alat

Primjer besplatnog digitalnog alata za provođenje postupka procjene učinka na zaštiti podataka je alat razvijen od francuskog nadzornog tijela (CNIL).[169] Alat je razvijen tako da pruža predloške koji vode korisnika kroz cijeli proces, a podijeljeni su u četiri tematske cjeline: Kontekst, Temeljna načela, Rizici i Validacija. Tematske cjeline definiraju glavne faze procesa i unutar sebe imaju definirane segmente tj. zadatke sa predlošcima za popunjavanje, uz podršku informacija iz CNIL „*baze znanja*“ u obliku principa i definicija uz referenciranje na Opću uredbu (slika 4.14).



Slika 4.14 Izgled sučelja i primjer funkcionalnosti u CNIL PIA alatu

Izvor: CNIL PIA alat

Proces započinje definiranjem konteksta tj. obrade, nakon čega je potrebno opisati usklađenost s temeljenim principima. Potom slijedi proces procjene rizika.

[169] CNIL PIA software, dostupno na: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment (09.02.2024.)

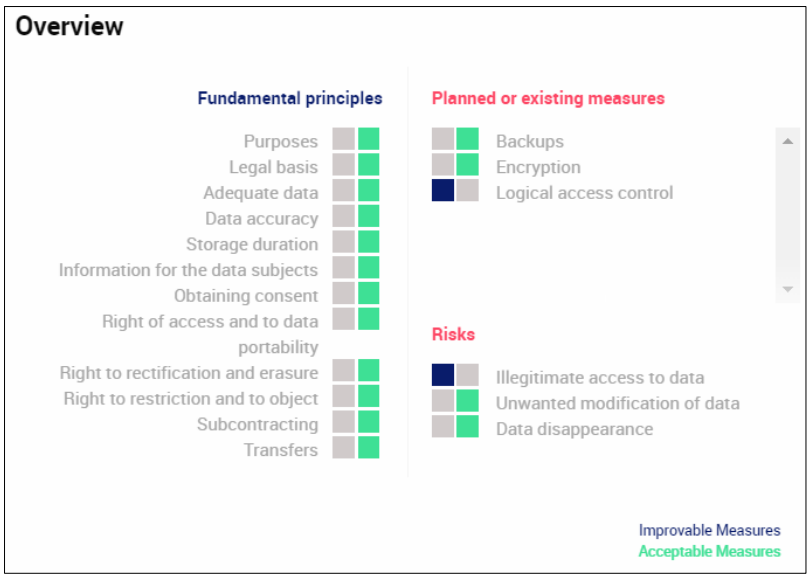
Prvi zadatak unutar segmenta „*Rizici*“ je definiranje postojećih i budućih mjera za tretiranje rizika. CNIL „*baza znanja*“ nudi listu različitih tehničkih i organizacijskih mjera uz mogućnost definiranja vlastitih od strane korisnika.

Drugi zadatak se odnosi na definiranje utjecaja, prijetnje, izvora prijetnje te dodjeljivanje razine vjerojatnosti i utjecaja (slika 4.15). Ovaj postupak provodi za 3 tipa rizika, definirana unutar alata: neovlašteni pristup podacima, neželjena modifikacija podataka i gubitak podataka, dok jedan tip rizika može imati veći broj prijetnji, izvora prijetnji, utjecaja i nužnih mjera za tretiranje rizika.

Slika 4.15 Primjer prikaza rizika koji se odnosi na neovlašteni pristup podatcima u CNIL PIA alatu

Izvor: CNIL PIA alat

Nakon završenog procesa mapiranja svih rizika, potrebno je provesti validaciju do tada svih unesenih podataka koji omogućavaju unos komentara te označavanje segmenata koji zahtijevaju unaprjeđenje ili korekciju. Na temelju provedene validacije omogućen je pregled akcijskog plana koji po svim ključnim elementima daje informacije što je prihvatljivo, a što treba unaprijediti (slika 4.16).



Slika 4.16 Pregled akcijskog plana u CNIL PIA alatu

Izvor: CNIL PIA alat

Po završetku procesa alat omogućava izradu DPIA izvješća u odabranom formatu, uključujući i izrađene slikovne elemente.

Provedenim testiranjem ovog alata možemo zaključiti da je CNIL PIA digitalni alat jednostavan za instalaciju i korištenje. Vođeni pristup olakšava snalaženje u alatu i koracima procesa, dok „*baza znanja*“ pruža ključne informacije i prijedloge ubrzavajući provođenje (D)PIA procesa. Alat omogućava definiranje vlastitih mjera za tretiranje rizika uz korištenje onih iz „*baze znanja*“ i pokriva sve ključne korake DPIA procesa izuzev pred-faze koja se odnosi na odluku je li DPIA potrebna ili ne.

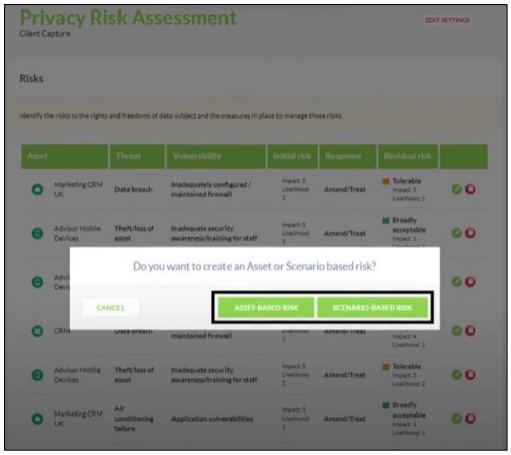
4.3.2 Vigilant – DPIA alat

Tvrtka Vigilant Software[170] razvila je veći broj komercijalnih alata za dosljedno upravljanje i nadziranje rizika privatnosti podataka i kibernetičke sigurnosti od kojih je jedan specifično razvijen za procjenu učinka na zaštitu podataka – DPIA Tool.[171] Prema definiranim funkcionalnostima, alat pruža vođeni pristup kroz sve faze DPIA-e uključujući i fazu odluke je li potrebno provesti DPIA-u ili ne, uz usklađenost sa WP29 Smjernicama[172] i ICO Smjernicama.[173]

Proces započinje definiranjem inventara imovine koji uključuje informacijsku imovinu te onu koja podržava istu u okviru obrade za koju se provodi procjena. Zatim je potrebno opisati predmetnu obradu uključujući svrhu te relevantne mjere za tretiranje rizika, nakon čega slijedi faza provjere nužnosti provođenja DPIA-e. U slučaju da je DPIA potrebna, alat traži unos podataka koji se odnose na uključenost relevantnih dionika – službenika za zaštitu podataka, ispitanika, izvršitelja obrade, IT stručnjaka, itd. U sljedećem se koraku kroz upitnik provjerava usklađenost s temeljnim principima Opće uredbe koji se odnose na nužnost i proporcionalnost obrade uz referenciranje relevantnih članaka Opće uredbe. Prije nego što se započne procjena rizika, alat ostavlja mogućnost prilagodbe broja razina vjerojatnosti i utjecaja koje se želi implementirati u DPIA proces, odnosno korisnik ima na raspolaganju odrediti skalu te prilagoditi opise istih. Također, u ovoj fazi potrebno je definirati kriterije za prihvaćanje rizika.

Provođenje procjene rizika može se prilagoditi preferencijama korisnika te omogućava odabir između 2 principa – procjena rizika koja se temelji na imovini ili koja se temelji na definiranim scenarijima (slika 4.17).

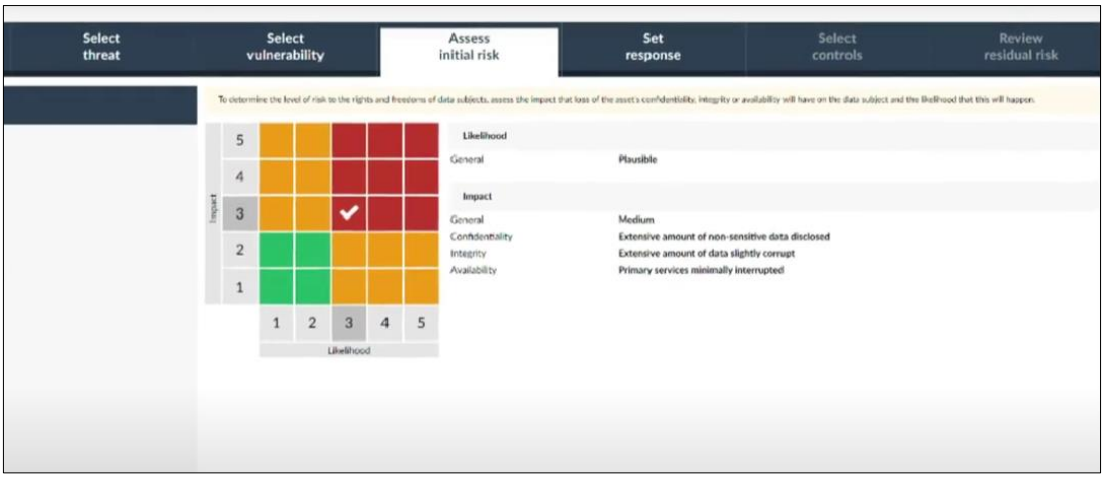
[170] Informacije o tvrtki Vigilant Software dostupne na: https://www.vigilantsoftware.co.uk/topic/about (09.02.2024.)
[171] Vigilant DPIA Tool, dostupno na: https://www.vigilantsoftware.co.uk/topic/dpia (09.02.2024.)
[172] *Ibid.* Smjernice o procjeni učinka na zaštitu podataka
[173] *Ibid.* Data protection impact assessments – Guidelines, Information Commissioner's Office (ICO)



Slika 4.17 Odabir principa za provođenje procjene rizika – Vigilant DPIA alat

Izvor: Vigilant Software – DPIA Tool video: https://www.youtube.com/watch?v=3ug7yVGN9Zc

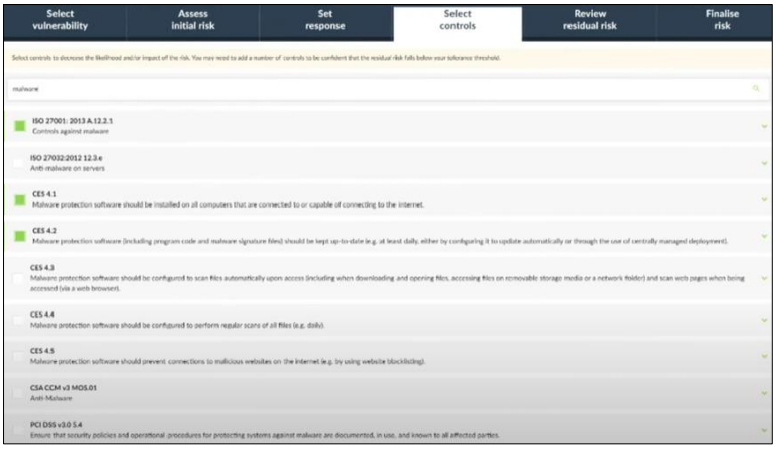
U sljedećoj fazi definiraju se prijetnje i ranjivosti odabirom iz ponuđene baze za koje je potom potrebno odrediti razine te time posljedično i razinu rizika (slika 4.18).



Slika 4.18 Evaluacija rizika temeljem razina vjerojatnosti i utjecaja - Vigilant DPIA alat

Izvor: Vigilant Software – DPIA Tool video: https://www.youtube.com/watch?v=3ug7yVGN9Zc

Za svaki od definiranih rizika u sljedećim fazama korisnik određuje strategiju upravljanja rizicima (*engl. Tolerate/Terminate/Treat/Transfer*) te shodno tome odabire mjere za tretiranje rizika iz već ponuđene liste mjera (slika 4.19).



Slika 4.19 Odabir mjera za tretiranje rizika - Vigitant DPIA alat

Izvor: Vigilant Software – DPIA Tool video: https://www.youtube.com/watch?v=3ug7yVGN9Zc

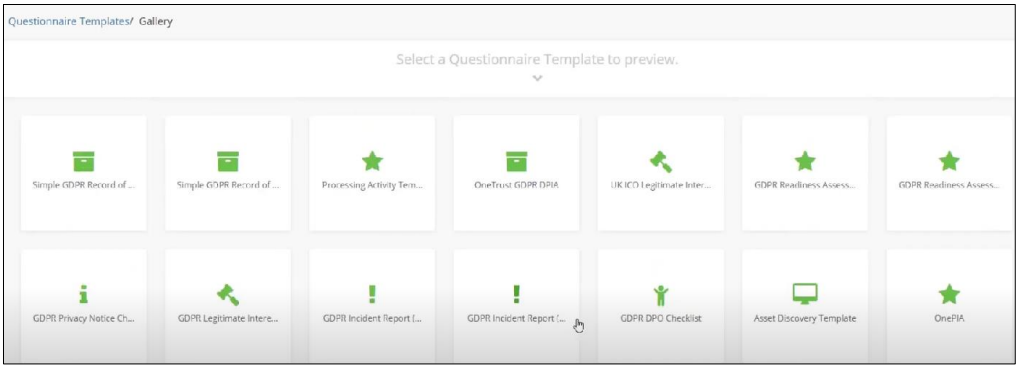
Alat također pruža mogućnost procjene rezidualnih rizika, nakon čega je moguće završiti proces te izraditi DPIA izvješće. Nakon razmatranja Vigilant DPIA alata, možemo zaključiti da alat uključuje sve bitne faze DPIA procesa uz vođeni proces i izrazito jednostavno sučelje koje omogućava korištenje alata od strane manje iskusnih korisnika.

4.3.3 One Trust – DPIA modul

OneTrust platforma nudi integralno rješenje koje povezuje privatnost, upravljanje rizicima, okolišno, društveno i korporativno upravljanje, osiguravanje usklađenosti, etiku, te podatke i procese.[174]

Jedan od segmenata platforme razvijen je s ciljem automatizacije DPIA procesa.[175] Alat je primarno namijenjen većim organizacijama koje putem ovog modula mogu kreirati i implementirati različite upitnike za procjenu te pratiti njihovu realizaciju. Također, omogućeno je korištenje već izrađenih predložaka unutar rješenja (slika 4.20).

[174] OneTrust platforma, informacije dostupne na: https://www.onetrust.com/platform/ (09.02.2024.)
[175] OneTrust Assessment Automation (PIA/DPIA), informacije dostupne na: https://www.onetrust.com/products/pia-and-dpia-automation/ (09.02.2024.)



Slika 4.20 Odabir unaprijed definiranih predložaka – OneTrust Assessment Automation

Izvor: OneTrust Assessment Automation video: https://www.youtube.com/watch?v=xHIP25WlZks&t=967s

Funkcionalnosti za kreiranje predložaka omogućavaju definiranje slijednosti, obaveznih i dodatnih polja te različitih logičkih pravila. Također, alat omogućava jednostavno upravljanje i praćenje procesa uz definiranje odgovornih osoba za provođenje i reviziju procjene. Snaga alata leži upravo u funkcionalnostima koje su ugrađene za samostalnu izradu predložaka. One omogućuju organizacijama da proces utjecaja na zaštitu podataka prilagode svojim potrebama uz uspješno integriranje u postojeći sustav osiguravanja usklađenosti i upravljanje rizicima.

4.3.4 Acuity Group – DPIA modul

Acuity Grpup razvila je rješenje RegTech[176] s modulom za provođenje procjene učinka na zaštitu podataka koji omogućava ekstrapolaciju kritičnih podataka kroz dinamičke profile rizika. Rješenje se nudi kao usluga odnosno SaaS (*engl. Softvare as a Service*).

Detaljni opisi o samom modulu tj. alatu nisu javno dostupni na stranicama tvrtke, već se navode generalne funkcionalnosti i ciljevi. Alat omogućava izradu popisa imovine osobnih podataka i utvrđivanje svrhe i pravne osnove za obradu osobnih podataka. Procjena rizika uključuje kategorije rizike koji se odnose na neovlašteni pristup osobnim podacima, neovlaštene izmjene osobnih podataka te gubitak, odnosno uključuje tri stupa informacijske sigurnosti – povjerljivost, integritet i dostupnost. Za

[176] RegTech rješenje, informacije dostupne na: https://www.acuitygroup.com/products/regtech/ (09.02.2024.)

svaki se rizik definira razina prijetnje i vjerojatnosti. Također, definiraju se kriteriji za procjenu izlaznih dokumenata zapisa obrade (*engl. Records of Processing Activity – RoPA,* obveza voditelja obrade prema čl. 30 OUZP[177]) procjene učinka na zaštitu podataka. Definirana usluga pokriva strateško i taktičko upravljanje operativnim sigurnosnim kontrolama i ulaganjima kako bi se izloženost neusklađenosti svela na najmanju moguću mjeru.[178]

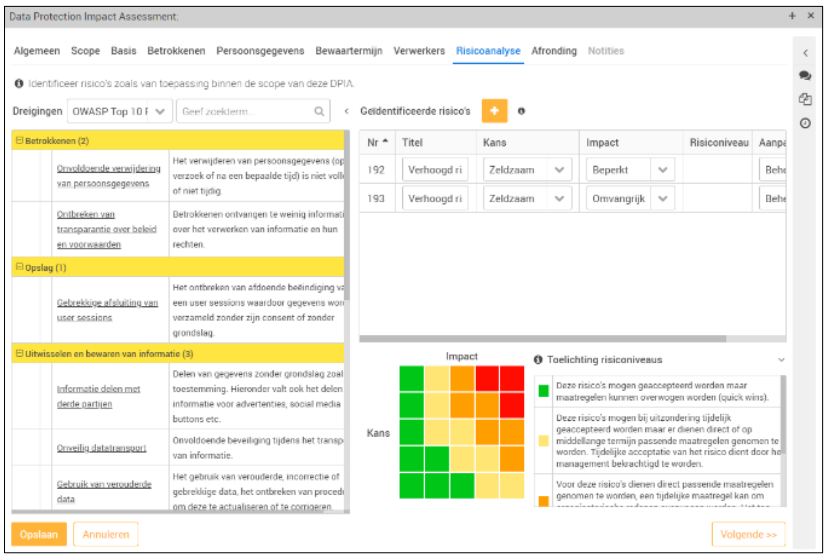
4.3.5 Axxemble – Base27

Base27[179] je sveobuhvatan sustav za upravljanje informacijama o privatnosti i sigurnosti koji je razvila nizozemska tvrtka Axxemble. Sustav je dizajniran za pomoć malim i srednjim organizacijama u održavanju usklađenosti s međunarodnim standardima i zakonima, uključujući i obavezu provođenja procjene učinka na zaštitu podataka prema Općoj uredbi. Alat omogućuje registraciju procesa i obrada, upravljanje rizikom, podršku za usklađivanje s Općom uredbom za zaštitu podataka, jasne nadzorne ploče za praćenje te izradu izvještaja koji se mogu izvesti u različite formate (Word, Excel).[180]

Za provođenje DPIA-e razvijen je modul s definiranim koracima za provođenje. Prvi korak podrazumijeva procjenu obaveze za provođenje DPIA-e, nakon čega se detaljno opisuje opseg obrade, uključujući identificiranje povezanih informacijskih sustava, procesa, dijelova organizacije, itd. U trećem koraku definira se svrha obrade i relevantna pravna osnova i primjenjivi zakoni. U sljedećem koraku identificiraju se uključene skupine uz odabir kategorija kojoj pripadaju. Base27 također nudi opciju za označavanje je li identificirana skupina ranjiva uz mapiranje prava uključenih. Peti korak usmjeren je na identificiranje osobnih podataka koji će se prikupljati. To uključuje podatke o imenu i adresi, ali i posebnih kategorija podataka.[181] Base27 nudi nekoliko standardnih opcija uz smjernice za podršku koje se treba uzeti u obzir. U sljedećem koraku alat stavlja u fokus označavanje zakonom definiranih rokova čuvanja podataka koji se ne smiju prekoračiti,

[177] v. OUZP, čl. 30.
[178] RegTech rješenje, informacije dostupne na: https://www.acuitygroup.com/products/regtech/ (09.02.2024.)
[179] Base17 rješenje, informacije dostupne na: https://www.base27.eu/features (09.02.2024.)
[180] Base17 rješenje, informacije dostupne na:https://www.base27.eu/features (09.02.2024.)
[181] *Ibid*. članak 9. stavak 1.

što omogućava naknadna upozorenja kod približavanja isteku rokova. Sedmim korakom definiraju se odgovornosti, nakon čega slijedi procjena rizika. Ovaj korak ima za cilj identificirati gdje leže rizici i prijetnje. Za svaki identificirani rizik određuje se vjerojatnost i utjecaj na temelju čega se predlaže razina rizika (slika 4.21).[182]



Slika 4.21 Prikaz sučelja procjene rizika u alatu Base27

Izvor: https://www.base27.eu/blog/dpia-data-protection-impact-assessment

Završni korak u alatu odnosi se na upravljanje rizicima tj. na definiranje odgovarajućih mjera za tretiranje rizika i odgovornih osoba i rokova za implementaciju.

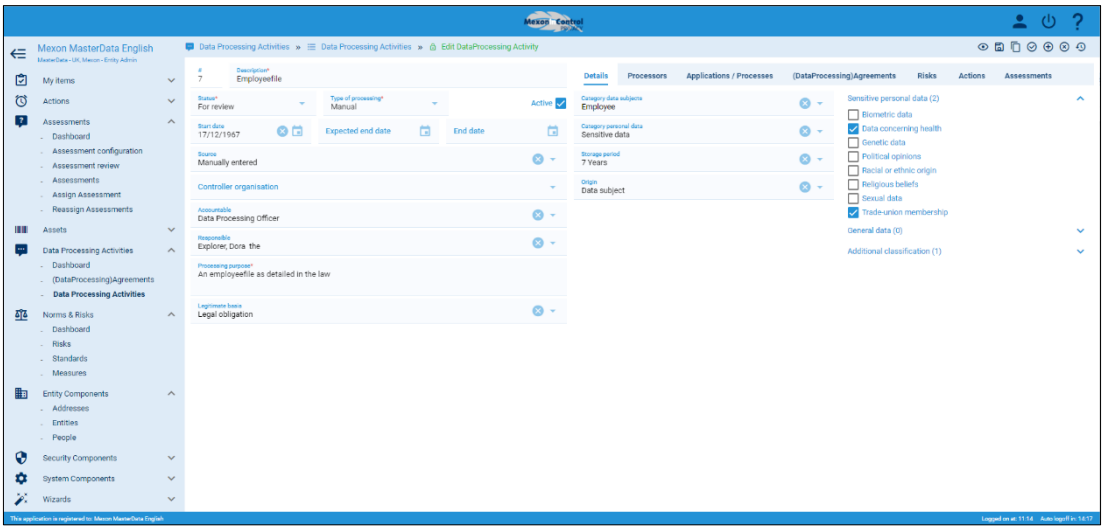
Base 27 je sustav s fokusom na sveobuhvatno upravljanje informacijskom sigurnošću i zaštitom privatnosti s implementiranim jednostavnim koracima za provođenje DPIA procesa. Prema dostupnim informacijama[183], zadovoljava uvjete iz Priloga 2 općih WP29 Smjernica (prilog 1).

[182] Base27 DPIA, informacije dostupne na: https://www.base27.eu/blog/dpia-data-protection-impact-assessment (09.02.2024.)
[183] Base27 DPIA, informacije dostupne na: https://www.base27.eu/blog/dpia-data-protection-impact-assessment (09.02.2024.)

4.3.6 Mexon Technology – MexonInControl

MexonInControl[184] je alat koji je razvila tvrtka Mexon Technology. Alat sadrži registre koji pokazuju usklađenost s Općom uredbom za zaštitu podataka i podržava proces DPIA procjene, uz mogućnost izrade predložaka prema potrebama korisnika. MexonInControl sastoji se od registara aktivnosti obrade podataka, registra povreda podataka, ugovora o obradi podataka, sigurnosnih incidenta, rizika, mjera, povezanih standarda, imovine i odnosa između njima.[185]

Početak procesa podrazumijeva postavljanje i ispravno popunjavanje registra aktivnosti obrade na temelju čega se potom provodi ostatak DPIA procesa (slika 4.22).



Slika 4.22 Definiranje procesa obrade u MexonInControl alatu

Izvor: https://www.mexontechnology.com/mexonincontrol-for-privacy/

Unutar alata MexonInControl dostupan je niz predložaka za provođenje nužnih koraka čime se omogućavaju sljedeće funkcionalnosti alata: Provjera je li DPIA potrebna; Definiranje nove obrade; Definiranje postojeće obrade; Bilježenje (potencijalne) povrede podataka; Bilježenje sigurnosnih incidenata; Provjera implementiranih mjera za tretiranje rizika; Osiguravanje prava ispitanika.

---

184 MexonInControl alat, informacije dostupne na: https://www.mexontechnology.com/mexonincontrol-for-privacy/ (09.02.2024.)

185 MexonInControl alat, informacije dostupne na: https://www.mexontechnology.com/mexonincontrol-for-privacy/ (09.02.2024.)

Alat podržava cijeli životni ciklus obrade podataka što uključuje definiranje svrhe i opsega obrade, procjene, delegiranja zadataka u organizaciji, praćenja statusa provedbe procesa, pregleda rezultata, revizije, spremanja i ispisa DPIA izvješća.[186]

4.3.7 Coalescent Limited - Dapian

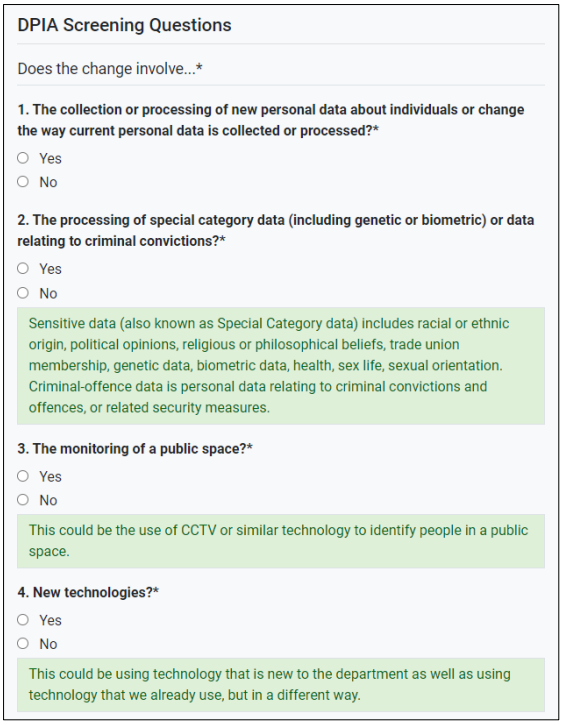
Alat Dapian[187] je razvila tvrtka Coalescent Limited s primarnim fokusom za provođenje procjene učinka na zaštitu podataka.

Kao glavne značajke alata navode se:

- Provjera nužnosti provođenja DPIA-e;
- Jasno definirani proces obrade podataka;
- Vođeni DPIA predlošci;
- Automatizirano generiranje rizika;
- Etičke procjene podataka i procjene učinka na jednakost;
- Pretraživanje knjižnica dovršenih DPIA-a za referencu;
- Alati za sve faze životnog ciklusa obrade podataka – alati za reviziju, praćenje, izvještavanje i izvoz podataka;
- Povezivanje sličnih DPIA-a prema potrebi.[188]

Proces procjene učinka na zaštitu podataka započinje inicijalnom procjenom radi utvrđivanja potrebe za provođenjem sveobuhvatne procjene učinka na zaštitu podataka. U tu svrhu izrađen je upitnik kojim se provjerava hoće li obrada prouzročiti visoki rizik na prava i slobode (slika 4.23).

[186]MexonInControl alat, informacije dostupne na: https://www.mexontechnology.com/mexonincontrol-for-privacy/ (09.02.2024.)
[187] Dapian alat, informacije dostupne na: https://dapian.uk/features/ (09.02.2024.)
[188] Dapian alat, informacije dostupne na: https://dapian.uk/features/ (09.02.2024.)



Slika 4.23 Izgled sučelja za procjenu nužnosti provođenja DPIA-e unutar Dapian alata

Izvor: Dapian alat

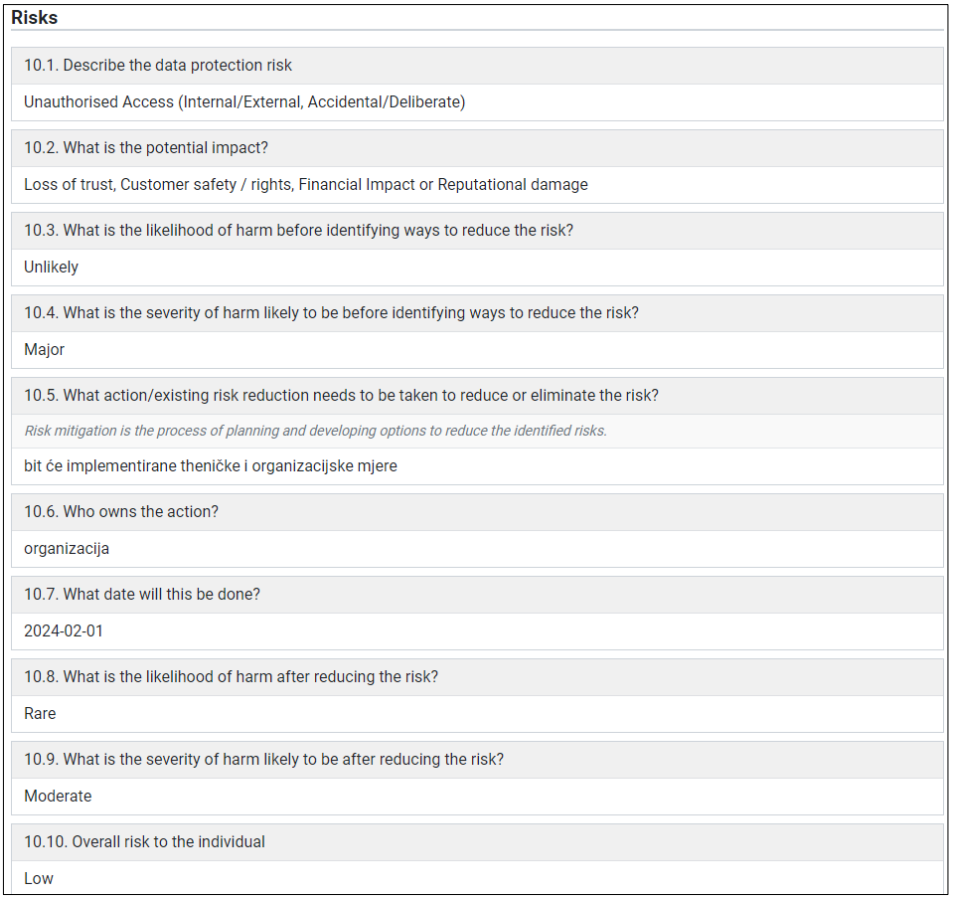
Ako je inicijalnom procjenom utvrđeno da je DPIA potrebna, alat nudi strukturirani upitnik koji pokriva cjeline prikazane na slici 4.24.

Slika 4.24 Izgled sučelja s prikazom tematskih DPIA cjelina unutar Dapian alata

Izvor: Dapian alat

Strukturirani upitnici pružaju polja s pojašnjenjima za olakšano popunjavanje te se prilagođavaju s obzirom na dane odgovore. Proces procjene rizika je olakšan jer sustav sam predlaže određeni broj rizika temeljem danih odgovora. Korisnik je također u

mogućnosti definirati dodatne rizike koji nisu predloženi. Za svaki rizik, potrebno je opisati utjecaj na ispitanike te procijeniti vjerojatnost i razinu utjecaja te nužne mjere za tretiranje rizika. Sustav omogućava procjenu rezidualnog rizika temeljem procjene vjerojatnosti i razine utjecaja nakon implementacije mjera (slika 4.25).



Slika 4.25 Izgled sučelja za procjenu rizika unutar Dapian alata

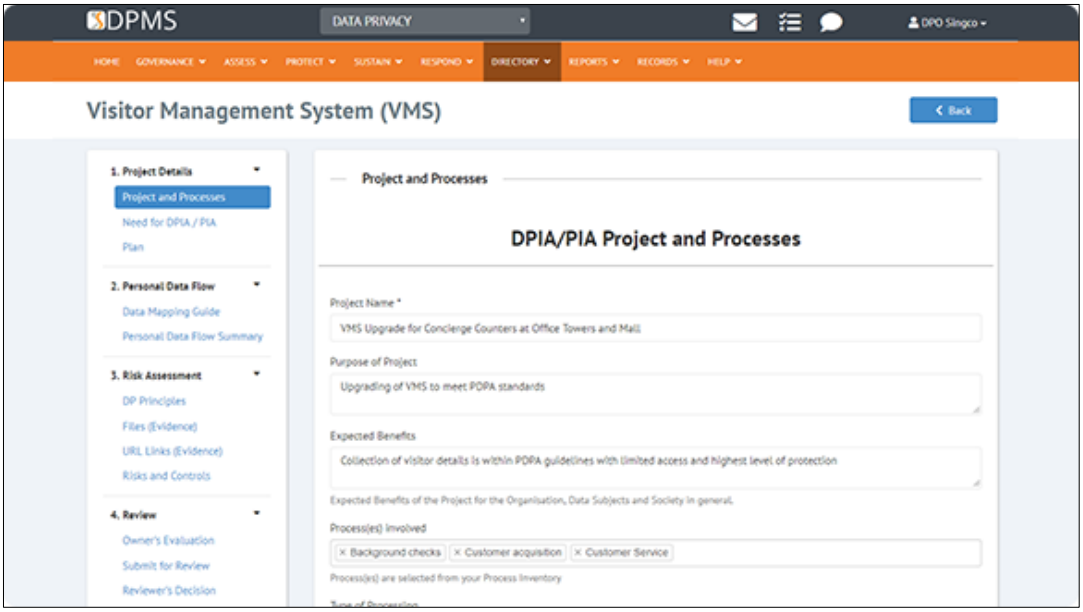
Izvor: Dapian alat

Testiranjem je utvrđeno da je alat prilagodljiv i jednostavan za korištenje te zadovoljava kriterije definirane u prilogu 2 WP29 smjernica za procjenu učinka na zaštitu podataka (prilog 1).

4.3.8 Straits Interactive – DPOinBOX

DPOinBOX alat razvila je tvrtka Straits Interactive s ciljem pružanja podrške tijekom upravljanja cjelokupnim programom zaštite podataka i privatnosti.[189]Alat omogućava kontinuirano nadziranje identificiranih rizika te pomaže korisnicima da izrade politike, akcijske planove i mjere za tretiranje rizika te dostignu usklađenost zaštite podataka i privatnosti. U tu svrhu ključna je funkcionalnost izrade inventara informacijske imovine uz mogućnost definiranja posebnih kategorija podataka i relevantne legislative za osiguravanje usklađenosti. Alat kao funkcionalnost podržava i provjeru nužnosti za provođenjem DPIA-e.[190]

Iako detaljne informacije o postupku provođenja DPIA-e i načinu kako je proces strukturiran unutar alata, nisu javno dostupne, slika 4.26 prikazuje sučelje alata s osnovnim elementima DPIA-e: (1.) Definiranje osnovnih informacija o obradi, (2.) Tijek osobnih podataka, (3.) Procjena rizika (4.) Pregled/Kontrola.



Slika 4.26 Sučelje DPOinBOX alata za provođenje DPIA-e

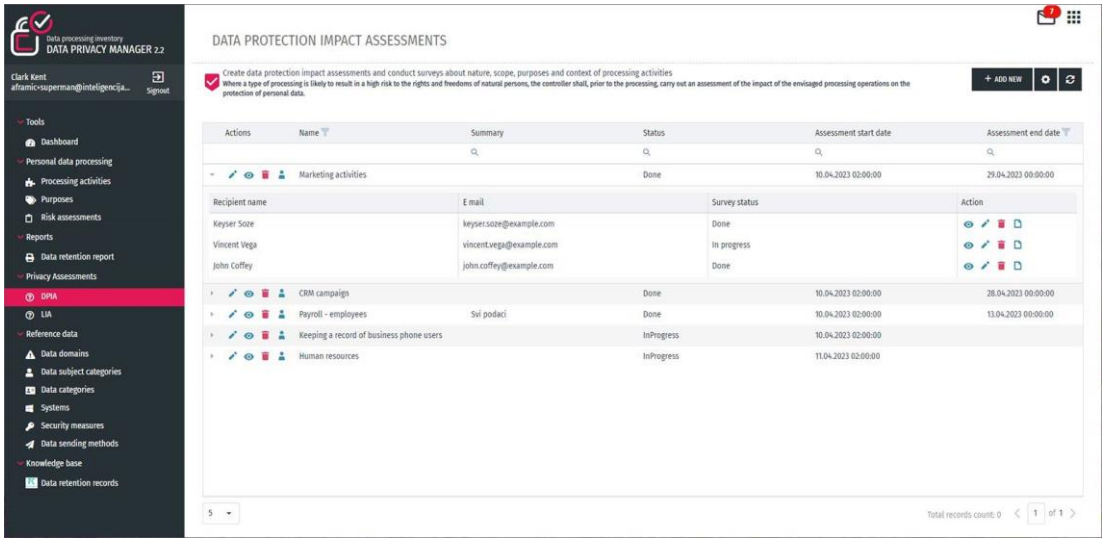
Izvor: https://www.dpoinbox.com/features/

[189] DPOinBOX alat, informacije dostupne na: https://www.dpoinbox.com/features/ (09.02.2024.)
[190] DPOinBOX alat, informacije dostupne na: https://www.dpoinbox.com/features/ (09.02.2024.)

4.3.9 Legit Software - Data Privacy Manager

Rješenje Data Privacy Manager razvila je hrvatska tvrtka Legit Software. Data Privacy Manager sa svojim modulima i uslugama (*Personal Data Discovery, Privacy Program Automation, Consent and Preference Management i Data Removal Orchestration*) je Cloud platforma za upravljanje i automatizaciju privatnosti dizajnirana kako bi voditeljima obrade omogućila jednostavno upravljanje osobnim podacima u skladu s propisima o zaštiti osobnih podataka, uključujući OUZP, te omogućila automatizaciju svih procesa i aktivnosti vezanih za usklađivanje, uz smanjenje regulatornih rizika.[191]

Unutar *Privacy Program Automation* podržani su različiti segmenti upravljanja privatnosti od kojih jedan, pod nazivom *Assessment Automation,* adresira procjenu učinka na zaštitu podataka (slika 4.27).



Slika 4.27 Sučelje Data Privacy Manager alata za provođenje DPIA-e

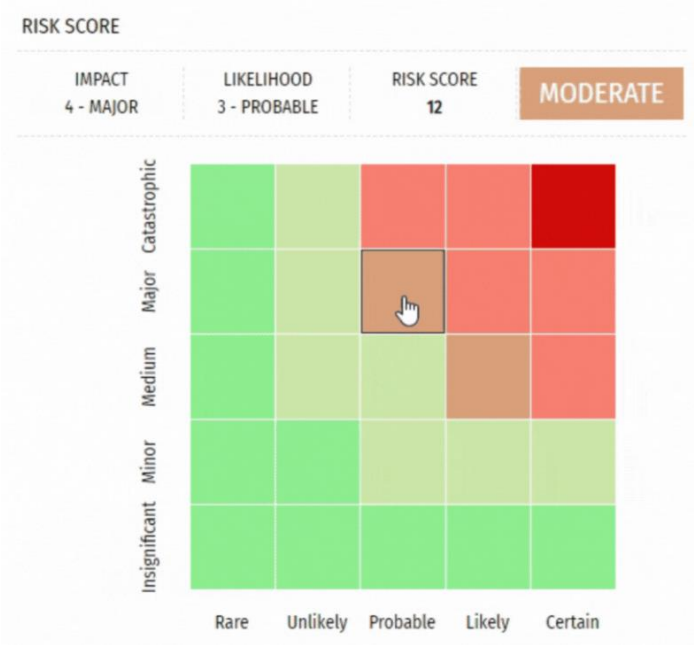
Izvor: https://dataprivacymanager.net/products/privacy-program-automation/assessment-automation/

Ovaj modul je dizajniran kako bi pojednostavio proces prikupljanja informacija od dionika voditelja obrade i pružio predloške za procjenu utjecaja na zaštitu podataka (DPIA) i procjenu legitimnog interesa (*engl. legitimate interests assessment - LIA*). Nadalje, modul automatizira prikupljanje podataka i procese provjere valjanosti povezane s tim procjenama, osiguravajući usklađenost s najnovijim propisima o zaštiti

[191] Data Privacy Manager alat, informacije dostupne: https://legit.eu/ (09.02.2024.)

podataka, uključujući i Opću uredbu. Omogućuje jednostavno identificiranje potencijalnih rizika za privatnost te identificiranje i primjenu mjera za njihovo rješavanje, pružajući kontrolu i transparentnost aktivnostima obrade podataka.[192]

Za procjenu rizika na raspolaganju imaju kompatibilni modul (*Risk Managment*) koji pruža upravljanje rizicima povezanima sa svakom aktivnošću obrade i omogućuje detaljniji uvid u preostale rizike koji stoje iza određene aktivnosti obrade tako što ga povezuje s relevantnom procjenom utjecaja na zaštitu podataka (DPIA). Nadalje, metodologiju rizika je moguće definirati prema potrebama voditelja obrade uz mogućnost prilagodbe matrice rizika prema utjecaju i vjerojatnosti i razinama rizika (slika 4.28).[193]



Slika 4.28 Matrica za strukturiranje procjene rizika – Data Privacy Manager

Izvor: https://dataprivacymanager.net/products/privacy-program-automation/risk-management/

[192] Assessment Automation modul (Data Privacy Manager alat), informacije dostupne na: https://dataprivacymanager.net/products/privacy-program-automation/assessment-automation/ (09.02.2024.)

[193] Risk Managment modul (Data Privacy Manager alat), informacije dostupne na https://dataprivacymanager.net/products/privacy-program-automation/risk-management/ (09.02.2024.)

Kao glavne funkcionalnosti izdvajaju jednostavno upravljanje procesom i dodjela zadataka unutar tima, pružanje unaprijed pripremljenih predložaka za provođenje DPIA-e uz mogućnost prilagodbi procesa procjene prema korisnikovim potrebama.[194]

4.4 Razmatranje uloge službenika za zaštitu podataka u provedbi procjene učinka

Općom uredbom za zaštitu podataka uvedena je obaveza imenovanja službenika za zaštitu podataka (engl. Data Protection Officer – DPO) situacijama kada obradu provodi tijelo javne vlasti ili javno tijelo te kada osnovne djelatnosti voditelja/izvršitelja obrade uključuju redovito i sustavno praćenje ispitanika u velikom opsegu, odnosno kada se obrada provodi u velikom opsegu nad osjetljivim osobnim podatcima.[195,196] Valja napomenuti da organizacije koje nisu dužne imenovati DPO-a mogu to učiniti na dobrovoljnoj bazi.[197]

Zadaće DPO-a definirane su člankom 39 Opće uredbe od koji se jedna odnosi na davanje savjeta u vezi s procjenom učinka na zaštitu podataka i praćenje njezina izvršavanja u skladu s Općom uredbom. Ova je obaveza navedena i u članku 35. stavku 2. gdje se definira nužno savjetovanje s DPO-om tijekom provođenja DPIA-e, ako je takva pozicija određena.

Također, prema članku 39., DPO je dužan djelovati kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje i prethodno savjetovanje iz članka 36. Isto tako, ističe se da službenik za zaštitu podataka pri obavljanju svojih zadaća

[194] Assessment Automation modul (Data Privacy Manager alat), informacije dostupne na: https://dataprivacymanager.net/products/privacy-program-automation/assessment-automation/ (09.02.2024.)
[195] *Ibid.* članak 37, stavak 1. i uvodna izjava 97.
[196] *Ibid.* Smjernice o službenicima za zaštitu podataka
[197] Gabel, D., Hickman, T., „*Chapter 12: Impact Assessments, DPOs and Codes of Conduct – Unlocking the EU General Data Protection Regulation*“, White & Case, dostupno na: https://www.whitecase.com/insight-our-thinking/chapter-12-impact-assessments-dpos-and-codes-conduct-unlocking-eu-general-data (09.02.2024.)

treba voditi računa o riziku povezanom s postupcima obrade i uzimati u obzir prirodu, opseg, kontekst i svrhe obrade, što spada u ključne elemente DPIA-e.[198]

Radna skupina iz članka 29. razradila je spomenute odredbe te preporučuje da voditelj obrade traži savjet od službenika za zaštitu podataka u pogledu sljedećih pitanja:

- provesti ili ne procjenu učinka na zaštitu podataka;
- kojom se metodologijom služiti pri provedbi procjene učinka na zaštitu podataka;
- provesti procjenu učinka na zaštitu podataka interno ili je povjeriti vanjskim izvršiteljima;
- koje mjere za tretiranje rizika (uključujući tehničke i organizacijske) primijeniti radi ublažavanja mogućih rizika za prava i interese ispitanika;
- je li procjena učinka na zaštitu podataka pravilno provedena te jesu li njezini zaključci (provesti obradu ili ne te koje su mjere za tretiranje rizika primjenjive) u skladu s Općom uredbom o zaštiti podataka.[199]

Smjernice o službenicima za zaštitu podataka[200] dalje navode da u slučajevima kada voditelj obrade nije suglasan s danim mišljenjem DPO-a, isto treba biti zabilježeno i objašnjeno u pisanom obliku kao dio DPIA dokumentacije. Ovim navodom Radna skupina iz članka 29. u fokus stavlja činjenicu da je voditelj obrade taj koji je u konačnici odgovoran za procjenu učinka na zaštitu podataka, što je definirano člankom 82. Dok je nepristranost uloge DPO-a osigurana člankom 38., stavak 2 gdje se navodi: „*Voditelj obrade i izvršitelj obrade osiguravaju da službenik za zaštitu podataka ne prima nikakve upute u pogledu izvršenja zadaća. Voditelj obrade ili izvršitelj obrade ne smiju ga razriješiti dužnosti ili kazniti zbog izvršavanja njegovih zadaća.*"

Iz gore prikazanog možemo zaključiti da je nepristrana uloga DPO zagarantirana Općom uredbom te ključna tijekom provođenja DPIA-e. Također, kako bi DPO adekvatno obnašao svoju ulogu, WP29 u Smjernicama o službenicima za zaštitu

[198] *Ibid.* članak 39., stavak 2.
[199] *Ibid.* Smjernice o službenicima za zaštitu podataka
[200] *Ibid.* Smjernice o službenicima za zaštitu podataka

podataka navodi minimalne zahtjeve u pogledu stručnosti i vještina DPO-a. Po pitanju stručnosti, kao ključno ističu se kompetencije u izradi, implementaciji i upravljanju programima za zaštitu podataka. Također, znanje o zakonima i praksama zaštite podataka. Ovo ne podrazumijeva obavezu da ulogu DPO-a obnašaju kvalificirani odvjetnici, već stručnost u nacionalnom i europskom pravu o zaštiti podataka, uključujući dubinsko poznavanje Opće uredbe o zaštiti podataka. Nadalje, DPO mora imati znanja za razumijevanje tehničkih i organizacijskih mjera te biti upoznat s informacijskim tehnologijama.[201]

4.5 Pregled prakse nadzornih tijela u pogledu povrede odredbi o procjeni učinka te povredi načela cjelovitosti i povjerljivosti obrade osobnih podataka u europskoj praksi od početka primjene Opće uredbe o zaštiti podataka

Opća uredba za zaštitu podataka jasno definira obaveze i odgovornosti voditelja obrade[202,203] te uvjete za izricanje novčanih kazni u slučajevima nepridržavanja mjera[204], odnosno uspostavlja okvir za sankcioniranje voditelja obrade kao odgovornih za povredu osobnih podataka, bez obzira na izvor i uzrok incidenta.[205]Uspostava ovakvog okvira i rizici za potencijalno visoke kazne kao posljedicu imaju razvoj svijesti o privatnosti i zaštiti podataka te uspostavu poboljšane sigurnosti obrade u praksi.[206]

[201] *Ibid.* Smjernice o službenicima za zaštitu podataka
[202] *Ibid.* članak 24.
[203] *Ibid.* članak 82.
[204] *Ibid.* članak 83.
[205] Katulić, T., Protrka, N., "*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: Institute of Electrical and Electronics Engineers (IEEE), 2019., str. 1420-1426 doi: 10.23919/mipro.2019.8757153
[206] Report on the Experience Gained in the Implementation of the GDPR, DPA (The German Data Protection Authorities), 2019., dostupno na: https://www.datenschutzkonferenz-online.de/media/dskb/20191213_evaluation_report_german_dpa_s_clean.pdf (09.02.2024.)

U nastavku ćemo se osvrnuti na povrede odredbi o procjeni učinka s primarnim fokusom na povredu načela cjelovitosti i povjerljivosti obrade osobnih podataka, kao ključnih načela za osiguravanje informacijske sigurnosti.

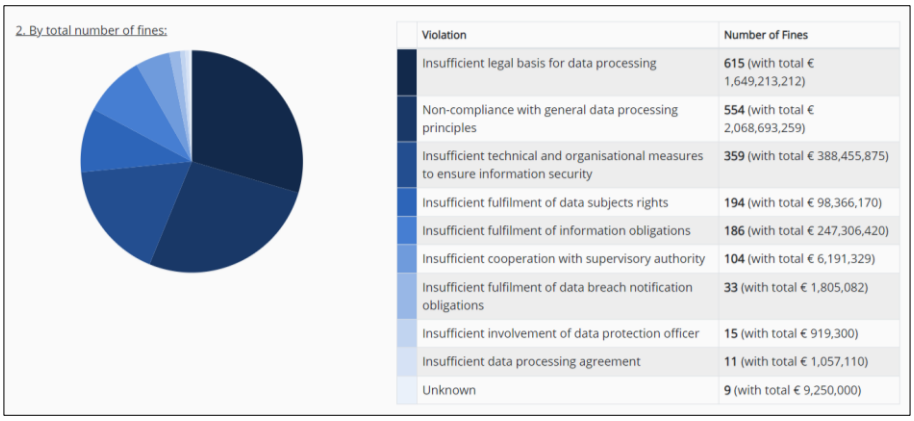
Načelo cjelovitosti i povjerljivosti definirano je Člankom 5. Opće uredbe uz proširenje dano člankom 32. u kojem su, između ostalog, definirane generalne tehničke i organizacijske mjere koje se primjenjuju kao alati za osiguravanje cjelovitosti i povjerljivosti podataka. Odabir mjera mora biti odgovarajući, odnosno biti u skladu s prirodom, opsegom, kontekstom i svrhom obrade, kao i rizicima različitih razina vjerojatnosti i posljedica za prava i slobode pojedinaca. Dodatno, definira se obaveza implementiranja odgovarajućih procesa za redovito testiranje, procjenu i evaluaciju učinkovitosti tehničkih i organizacijskih mjera namijenjenih osiguravanju sigurnosti obrade.[207],[208]

U praksi, voditelji obrade odgovorni su za povrede osobnih podataka koje dovode do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka, neovlaštenog pristupa osobnim podacima ili drugog neovlaštenog prijenosa, pohrane ili obrade osobnih podataka.[209]

Kako bi dokazali odgovorno postupanje, voditelji obrade moraju osigurati odgovarajuće sigurnosne kontrole. Prema članku 83. stavak 2. točka (d), implementacija odgovarajućih tehničkih i organizacijskih kontrola u skladu s člancima 25. i 32, jedan je od ključnih kriterija prilikom odlučivanja o izricanju novčane kazne i odluke o njezinom iznosu.

Od početka primjene Opće uredbe za zaštitu podataka, nedovoljne tehničke i organizacijske mjere za osiguranje informacijske sigurnosti spadaju pod treći najčešći razlog izricanja kazni prema Enforcement Trackeru[210] s ukupno 359 izrečenih kazni i iznosom od preko 388 milijuna eura (slika 4.29).

[207] *Ibid.* Katulić, T., Protrka, N., str. 1420-1426
[208] *Ibid.* članak 24.
[209] *Ibid.* Katulić, T., Protrka, N., str. 1420-1426
[210] Enforcement Tracker omogućava pregled prijavljenih novčanih kazni i kazni koje su tijela za zaštitu podataka unutar EU do sada izrekla, dostupno na: https://www.enforcementtracker.com/ (09.02.2024.)



Violation	Number of Fines
Insufficient legal basis for data processing	**615** (with total € 1,649,213,212)
Non-compliance with general data processing principles	**554** (with total € 2,068,693,259)
Insufficient technical and organisational measures to ensure information security	**359** (with total € 388,455,875)
Insufficient fulfilment of data subjects rights	**194** (with total € 98,366,170)
Insufficient fulfilment of information obligations	**186** (with total € 247,306,420)
Insufficient cooperation with supervisory authority	**104** (with total € 6,191,329)
Insufficient fulfilment of data breach notification obligations	**33** (with total € 1,805,082)
Insufficient involvement of data protection officer	**15** (with total € 919,300)
Insufficient data processing agreement	**11** (with total € 1,057,110)
Unknown	**9** (with total € 9,250,000)

Slika 4.29 Pregled najčešćih razloga izricanja kazni od strane nadzornih tijela EU

Izvor: https://www.enforcementtracker.com/?insights

Nadalje, treća najveća kazna, od početka primjene Opće uredbe, s ukupnim iznosom od 265 milijuna eura izdana je upravo radi neprovođenja odgovarajućih tehničkih i organizacijskih mjera u skladu s člankom 25. Opće uredbe. Kaznu je izdalo nadzorno tijelo Irske (*engl. Data Protection Commission - DPC*). protiv trgovačkog društva Meta IE, voditelja obrade društvene platforme za kojeg je utvrđeno da su implementirane mjere bile nedostatne.[211]

Tijekom 2023. godine nadzorna tijela izdala su ukupno 65 kazni zbog manjkavosti implementiranih tehničkih i organizacijskih mjera.[212] Jedan od primjera je i izricanje kazne od strane nadzornog tijela Ujedinjenog Kraljevstva (engl. Information Commissioner's Office – ICO) u iznosu od 5 milijuna eura. Kazna je izrečena tvrtki Interserve Group Limited jer nije provela odgovarajuće tehničke i organizacijske mjere za zaštitu osobnih podataka (u suprotnosti s člancima 5(1)(f) i 32 GDPR).[213]

Općenito govoreći, od početka primjene Opće uredbe broj kazni s godinama se značajno povećava (slika 4.30, lijevo) kao i njihov ukupni iznos (slika 4.30, desno).

[211] GDPR Fines and Data Breach Survey: January 2023, DLA Piper, 2023., dostupno na: https://www.dlapiper.com/en/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023
[212] Enforcement Tracker, dostupno na: https://www.enforcementtracker.com/ (09.02.2024.)
[213] *Ibid*. GDPR Fines and Data Breach Survey: January 2023

Slika 4.30 Prikaz rasta broja i iznosa kazni nadzornih tijela EU od početka primjene Opće uredbe o zaštiti podataka; lijevo – rast broja kazni, desno – rast ukupnog iznosa kazni

Izvor: Enforcement Tracker, dostupno na: https://www.enforcementtracker.com/?insights

4.6 Zaključna razmatranja o praksi procjene učinka i prijedlozi za bolju usklađenost voditelja obrade u Republici Hrvatskoj

U Republici Hrvatskoj, uz Opću uredbu o zaštiti podataka, nacionalni provedbeni Zakon o provedbi Opće uredbe o zaštiti podataka[214] predstavlja ključni pravni instrument koji regulira pitanja vezana uz obradu osobnih podataka. Međutim, važno je istaknuti da ovaj zakon ne pruža konkretne upute ili obvezujuće propise o procjeni učinka na zaštitu podataka.

DPIA predstavlja važan alat za procjenu potencijalnih rizika i utjecaja na prava i slobode pojedinaca prilikom obrade osobnih podataka. Međutim, u Hrvatskoj nema konkretnih zakonskih odredbi niti odredbi provedbenih propisa poput uredbi ili drugih akata nadzornih tijela koje bi detaljnije propisale postupak provedbe DPIA-e, kao ni službenih smjernica nadzornog tijela. Ovaj nedostatak može stvoriti izazove i nejasnoće za voditelje obrade, posebno kod onih koji sustavno i opsežno obrađuju podatke, što može rezultirati neadekvatnim poimanjem rizika prilikom uvođenja novih obrada, osobito kad je riječ o invazivnim i rizičnim tehnologijama poput strojnog učenja, *Internet-of-things (*IoT) i slično, te rezultirati konačno nedovoljnom zaštitom

[214] Zakon o provedbi Opće uredbe o zaštiti podataka, NN 42/2018, stupio na snagu: 25. svibnja 2018., dostupan na: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html

prava pojedinaca u kontekstu obrade njihovih osobnih podataka. Bez jasnih praktičnih smjernica, postoji rizik da voditelji obrade podataka neće adekvatno procijeniti potencijalne rizike ili poduzeti adekvatne mjere za tretiranje rizika.

Nadalje, nepostojanje nacionalnih provedbenih propisa koji propisuju obavezu provođenja DPIA-e za voditelje obrade moguće je pronaći i u drugim zemljama Europske Unije, od koji neke zemlje imaju, a neke nemaju smjernice donesene od strane nacionalnih nadzornih tijela.[215] Dodatno, neke zemlje imaju stroge propise, dok druge imaju blaže zahtjeve ili uopće nemaju posebne propise. Ova situacija u praksi rezultira nedosljednošću u pogledu kvalitete i opsega provedene DPIA-e te također pojave fenomena poznatog kao „*forum shopping*". Pojam „*forum shopping*" odnosi se na situacije gdje voditelji obrade strateški odabiru obavljanje aktivnosti obrade podataka u zemljama EU s nižom razinom obveza tj. u zemljama s „*light touch*" regulatornim pristupom. Ova praksa „*forum shoppinga*" rezultira nedostatkom dosljednosti i ujednačenosti u zaštiti prava pojedinaca na privatnost.

Na manjkavosti provedenih DPIA-a od strane institucija EU-a, kako je već spomenuto u poglavlju 4.1., ukazalo je EDPS-ovo istraživanje iz 2020. godine.[216] Jedan od potencijalnih razloga su i različiti pristupi dostupnih smjernica nadzornih tijela koja se međusobno razlikuju te time otvaraju prostor za različitu interpretaciju. Ovo se posebno odnosi na različite i neunificirane pristupe procjene rizika kao dio procesa procjene učinka na zaštitu podataka, što je prepoznato kao jedan od čimbenika nedosljednosti u primjeni DPIA-e.[217]

Bitno je za naglasiti, Općom uredbom o zaštiti podataka predviđa se izrada smjernica preporuka i primjera najbolje prakse kako bi se poticala dosljedna primjena Uredbe.[218]

---

[215] Vidi istraživanje - Custers, B., Dechesne, F., Sears, A. M., Tani, T., & Van der Hof, S., „*A comparison of data protection legislation and policies across the EU*", Computer Law & Security Review, 34(2), 2018., str. 234-243.

[216] *Ibid.* EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (case 2020-0066)

[217] *Ibid*. Contribution from the Multistakeholder Expert Group to the Stock-Taking Exercise of June 2019 on One Year of GDPR Application

[218] *Ibid.* članak 70., stavak 1.

Radi gore navedenih razloga prijedlog unapređenja postupka procjene učinka na zaštitu podataka odnosio bi se na donošenje smjernica od strane AZOP-a, odnosno ažuriranje smjernica od strane EDPB-a (*engl. European Data Protection Board – EDPB*), kojima bi se adresirali utvrđeni problemi. Smjernice bi trebale pružiti jasnu i nedvosmislenu metodologiju uz visoku primjenjivost u praksi. Također, trebale bi biti prilagodljive, ali isto tako dati nedvosmislena pojašnjenja kako tumačiti rizik na prava i slobode pojedinaca te koje alate koristi prilikom identificiranja, analize i evaluacije rizika.

Druga preporuka koja bi imala utjecaj na kvalitetu i ujednačenost procesa procjene utjecaja na zaštitu podataka bila bi izrada detaljnijih kriterija prihvatljivosti postupaka DPIA-e, odnosno unapređenje kriterija definiranih u Prilogu 2 Smjernica o procjeni učinka na zaštitu podataka (prilog 1).[219] Pružanje detaljnijih kriterija omogućilo bi voditeljima i izvršiteljima obrade jasne kriterije za provođenje i osiguravanje kvalitete procesa provođenja procjene učinka na zaštitu podataka, dok bi nadzornim tijelima pružile okvir za davanje mišljenja i ocjenu tijekom revizija.

Zaključno, s obzirom na dinamičnost područja zaštite podataka i sve veću važnost privatnosti podataka u suvremenom digitalnom društvu, moguće je da će se zakonodavstvo u Hrvatskoj uskoro prilagoditi kako bi obuhvatilo i detaljnije reguliralo postupak procjene učinka na zaštitu podataka. Očekuje se da će takve promjene doprinijeti boljoj zaštiti privatnosti podataka i osigurati veću transparentnost i odgovornost u postupcima obrade osobnih podataka.

[219] *Ibid.* Smjernice o procjeni učinka na zaštitu podataka

5 ZAKLJUČAK

DPIA je važan alat za procjenu mogućih rizika i utjecaja na prava i slobode pojedinaca u obradi osobnih podataka te uspostavu i dokazivanje usklađenosti s Općom uredbom. Međutim, postoje značajne razlike u načinima na koje su zemlje članice EU-a implementirale zaštitu privatnosti i osobnih podataka u nacionalnim zakonima, politikama i praksama. Ovo se odnosi na različite regulatorne pristupe s obzirom na propisanu razinu obaveza, kao i različite metodološke pristupe objavljene u smjernicama nadzornih tijela zemalja EU, od kojih su neke prikazane u radu. Značajna raznorodnost u pristupima očituje se u segmentu procjene učinka na zaštitu podataka koja se odnosi na procjenu rizika. Opisana situacija može stvoriti izazove i nesigurnosti za voditelje obrade podataka te rezultirati neadekvatnom zaštitom prava pojedinca u kontekstu obrade njihovih osobnih podataka.

Kako bi se unaprijedila opisana situacija i dosegla veća usklađenost i kvaliteta procjene učinka na zaštitu podataka, nužno je pružiti jasnu i nedvosmislenu metodologiju uz visoku primjenjivost u praksi. Također bilo bi nužno unaprijediti kriterije za procjenu kvalitete procesa DPIA-e te uvesti i uskladiti regulatorne pristupe i definirane razine obaveza.

6 POPIS LITERATURE

Monografije:

1. Death, D., "*Information security handbook: develop a threat model and incident response strategy to build a strong information security framewor*k", Packt Publishing Ltd, 2017.
2. Katsikas, S. K., "*Risk Management*", Part V, Chapter 35 in "*Computer and Information Security Handbook*", J. R. Vacca, Second Edition (2nd. ed.). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2013, str. 605-625
3. De, S.J., Le Métayer, D., „*Privacy Risks Analysis*", Morgan & Claypool, 2016, ISBN: 1627054251.
4. Brynjolfsson E., Kahin B., editors. Understanding the Digital Economy: Data, Tools, and Research. MIT Press; Cambridge, MA, 2002.

Pravni izvori:

1. Povelja Europske unije o temeljnim pravima, 2007/C 303/01:, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:12016P/TXT&from=RO (09.02.2024.)
2. Ugovor o funkcioniranju Europske unije, članak 16, dostupno na: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0011.01/DOC_3&format=PDF (09.02.2024.)
3. Zakon o zaštiti osobnih podataka, NN 103/03, 118/06, 41/08, 130/11, 106/12, prestao važiti 25.05.2018.
4. Priručnik o europskom zakonodavstvu o zaštiti podataka, Agencija Europske unije za temeljna prava, Europski nadzornik za zaštitu podataka, Europski sud za ljudska prava, Vijeće Europe, . Izdanje iz 2018.," 2018, doi: 10.2811/266278.
5. Dodatni protokol uz Konvenciju o zaštiti pojedinaca pri automatskoj obradi osobnih podataka, koji se tiče nadzornih tijela i prekograničnih prijenosa podataka, Vijeće Europe, CET br. 223
6. Opća uredba o zaštiti podataka, Europski parlament i Vijeće Europske unije, "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," 2016, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679, (09.02.2024.).
7. Odluka o uspostavi i javnoj objavi popisa vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka, AZOP, dostupno na: https://azop.hr/odluka-o-uspostavi-i-javnoj-objavi-popisa-vrsta-postupaka-obrade-koje-podlijezu-zahtjevu-za-procjenu-ucinka-na-zastitu-podataka/ (09.02.2024.)
8. Zakon o provedbi Opće uredbe o zaštiti podataka, NN 42/2018, stupio na snagu: 25. svibnja 2018., dostupan na: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html

Publikacije:

1. Katulić, T., Mladinić, A., "Prava ispitanika prema Općoj uredbi o zaštiti podataka i Zakonu o provedbi Opće uredbe o zaštiti podataka", Zagreb, 2021.
2. Conducting privacy impact assessments code of practice, ICO (Information Commissioner's Office), UK Information Commissioner's Office, 2014., str. 1–55.
3. Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik" u smislu Uredbe 2016/679, Radna skupina za zaštitu podataka iz članka 29., Donesene 4. travnja 2017. Posljednji put revidirane i donesene 4. listopada 2017.
4. Smjernice o službenicima za zaštitu podataka, Radna skupina za zaštitu podataka iz članka 29., Donesene 13. prosinca 2016. Posljednji put revidirane i donesene 5. travnja 2017.
5. Berendt, B., Littlejohn, A., Kern, P., Mitros, P., Shacklock, X., Blakemore, "Big data for monitoring educational systems". Publications Office of the European Union, Luxembourg, 2017.
6. Contribution from the Multistakeholder Expert Group to the Stock-Taking Exercise of June 2019 on One Year of GDPR Application, Multistakeholder Expert Group, Report, 13 June 2019, dostupno na: https://commission.europa.eu/system/files/2019-10/report_from_multistakeholder_expert_group_on_gdpr_application.pdf (09.02.2024.)
7. EDPS „Survey on Data Protection Impact Assessments under Article 39 of the Regulation (case 2020-0066)", EDPS (European Data Protection Supervisor), dostupno na: https://edps.europa.eu/sites/edp/files/publication/20-07-06_edps_dpias_survey_en.pdf (09.02.2024.)
8. Martin, N., Friedewald, M., Schiering, I., Mester, B. A., Hallinan, D., & Jensen, M., "The Data Protection Impact Assessment According to Article 35 GDPR", Fraunhofer Institute for Systems and Innovation Research ISI, 2020.
9. Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, White Paper, CIPL (Centre for Information Policy Leadership at Hunton & Williams LLP), 2016.
10. Privacy Risk Assessment: Methodology, CNIL (Commission Nationale de l'Informatique et des Libertés), Paris, 2018, dostupno na: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-1-en-methodology.pdf (09.02.2024)
11. Guide to the General Data Protection Regulation (GDPR), ICO (Information Commissioner's Office), Wilmslow, UK, 2021.
12. The Standard Data Protection Model V3.0: A method for data protection advising and controlling on the basis of uniform protection goals, Conference of the independent data protection authorities of the Federal and State Governments of Germany, 2022., dostupno na: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM_V3_en.pdf (09.02.2024.)
13. ISO/IEC 29134:2023: Information technology - Security techniques - Guidelines for privacy impact assessment. International Standardisation Organisation, Geneva

14. ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection -Guidance on managing information security risks. International Standardisation Organisation, Geneva
15. Risk Assessment & Data Protection Impact Assessment – Guide, Federal Association for Information Technology, Telecommunications and New Media (BITKOM), Berlin, 2017., dostupno na: https://www.bitkom.org/sites/main/files/file/import/170919-lf-risk-assessment-eng-online-final.pdf (09.02.2024.)
16. Privacy Impact Assessment (PIA) Templates, CNIL (Commission Nationale de l'Informatique et des Libertés), Paris, 2018., dostupno na: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-2-en-templates.pdf (09.02.2024.)
17. Privacy Impact Assessment (PIA) Knowledge Bases, CNIL (Commission Nationale de l'Informatique et des Libertés), Paris, 2018., dostupno na: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf (09.02.2024.)
18. Korff, D., Georges, M., "The Data Protection Officer Handbook", 2019. SSRN: https://ssrn.com/abstract=3428957.
19. Data protection impact assessments – Guidelines, Information Commissioner's Office (ICO), Wilmslow, UK, 2018., dostupno na: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/ (09.02.2024.)
20. DPIA template v0.4, Information Commissioner's Office (ICO), Wilmslow, UK, 2018., dostupno na: https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf (09.02.2024.)
21. SDM Katalog referentnih mjera s modulima, Conference of the independent data protection authorities of the Federal and State Governments of Germany, dostupno na: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ (09.02.2024.)
22. Kratki rad 5 - procjena učinka zaštite podataka prema članku 35. GDPR-a , Conference of the independent data protection authorities of the Federal and State Governments of Germany, dostupno na: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf (09.02.2024.)
23. Kratki rad 18 - Rizik za prava i slobode fizičkih osoba, Conference of the independent data protection authorities of the Federal and State Governments of Germany, dostupno na: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (09.02.2024.)
24. Vodič za procjenu učinka na zaštitu podataka za male i srednje poduzetnike, AZOP (Agencija za zaštitu podataka), dostupno na: https://arc-rec-project.eu/wp-content/uploads/2021/10/Vodic-za-procjenu-ucinka-na-zastitu-podataka-za-SMEs.pdf (09.02.2024.)
25. Predložak za procjenu učinka na zaštitu podataka, AZOP (Agencija za zaštitu podataka), dostupno na: https://azop.hr/wp-content/uploads/2020/12/7-DPIA-obrazac_procjena_ucinka-1.docx (09.02.2024.)
26. Caralli, R. A., Stevens, J. F., Young, L. R., Wilson, W. R., "Introducing octave allegro: Improving the information security risk assessment process", Hansom AFB, MA, 2007., dostupno na:

https://insights.sei.cmu.edu/documents/786/2007_005_001_14885.pdf (09.02.2024.)
27. NIST Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments, 2012.
28. NIST Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, 2020
29. NIST Special Publication (SP) 800-53A, Assessing Security and Privacy Controls in Information Systems and Organizations, 2022
30. Report on the Experience Gained in the Implementation of the GDPR, DPA (The German Data Protection Authorities), 2019., dostupno na: https://www.datenschutzkonferenz-online.de/media/dskb/20191213_evaluation_report_german_dpa_s_clean.pdf (09.02.2024.)
31. GDPR Fines and Data Breach Survey: January 2023, DLA Piper, 2023., dostupno na: https://www.dlapiper.com/en/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023

Znanstveni i stručni radovi:

1. Wang, C., Zhang, N., Wang, C, „*Managing privacy in the digital economy*“, Fundamental Research, 1(5), str. 543-551, 2021.
2. Bevanda, M., Čolaković, M., “*Pravni okvir za zaštitu osobnih podataka (u vezi sa zdravljem) u pravu Europske unije*”, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 37, no. 1, 2016, str. 125–154, doi: 10.30925/zpfsr.37.1.5.
3. Voigt, P., Bussche, A., “*The EU General Data Protection Regulation (GDPR): A Practical Guide*”, 2017., doi: 10.1007/978-3-319-57959-7.
4. Bieker, F., Martin, N., Friedewald, M., & Hansen, M., “*Data Protection Impact Assessment: A Hands-On Tour of the GDPR's Most Practical Tool*”, Privacy and Identity Management. The Smart Revolution: 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Ispra, Italy, September 4-8, 2017, Revised Selected Papers 12, str. 207-220.
5. Henriksen-Bulmer, J., Faily, S., Jeary, S., “*DPIA in Context: Applying DPIA to Assess Privacy Risks of Cyber Physical Systems*”, Future internet, 12(5), 93., 2020, https://doi.org/10.3390/fi12050093
6. Meis, R., Heisel, M. “*Supporting privacy impact assessments using problem-based privacy analysis*”, International Conference on Software Technologies., Springer, Cham, 2015., str. 79-98.
7. van Puijenbroek, J.P.M., Hoepman, J.H., “*Privacy Impact Assessments in Practice: Outcome of a Descriptive Field Research in the Netherlands*”, Ceur Workshop Proceedings, Alamo, J.M. del (ed.), IWPE 2017: International Workshop on Privacy Engineering: Proceedings of the 3rd International Workshop on Privacy Engineering, co-located with 38th IEEE Symposium on Security and Privacy (S&P 2017) San Jose (CA), USA, May 25, 2017, str. 1-8.
8. De, S.J., Le Métayer, D. “*A Refinement Approach for the Reuse of Privacy Risk Analysis Results*”, Annual Privacy Forum, Springer, Cham, 2017., str. 52-83.

9. Friedewald, M., Schiering, I., Martin, N., Hallinan, D., "*Data Protection Impact Assessments in Practice: Experiences from Case Studies*.", European Symposium on Research in Computer Security, Springer, Cham, 2021., str. 424-443.
10. van Dijk, N., Gellert, R., Rommetveit, K., "*A risk to a right: beyond data protection impact assessments?*" Comput. Law Secur. Rev. 32(2), 2016., str. 286–306.
11. Gellert, R., "*Understanding the notion of risk in the General Data Protection Regulation*", Comput. Law Secur. Rev. 34(2), 2018., str. 279–288.
12. Hallinan, D., Martin, N., "*Fundamental rights, the normative keystone of DPIA*", Eur. Data Prot. Law Rev. 6(2), 2020., str. 178–193.
13. Kloza, D., et al., "*Towards a method for data protection impact assessment: making sense of GDPR requirements*", d.pia.lab Policy Brief 1/2019, VU Brussels, Brussels, 2019., https://doi.org/10.31228/osf.io/es8bm
14. Vemou, K., Karyda, M., "*An evaluation framework for privacy impact assessment methods*", The 12th Mediterranean Conference on Information Systems (MCIS), Corfu, Greece, 2018.
15. Oetzel, M. C., Spiekermann, S., "*A systematic methodology for privacy impact assessments: a design science approach*", European Journal of Information Systems, 23(2), 2014., str. 126-150.
16. Wangen, G., "*Information Security Risk Assessment: A Method Comparison*", Journal of latex class files, 6 (1), 2007., str.1-7.
17. Custers, B., Dechesne, F., Sears, A. M., Tani, T., & Van der Hof, S., „*A comparison of data protection legislation and policies across the EU*", Computer Law & Security Review, 34(2), 2018., str. 234-243.

Internetski izvori:

1. Arc II projekt sufinanciran iz programa Europske unije "Prava, jednakost i građanstvo", Ugovor o dodjeli bespovratnih sredstava № 874524, voditelj projekta – AZOP, talijansko nadzorno tijelo za zaštitu podataka Garante Privacy – partner, https://arc-rec-project.eu/o-projektu/
2. AZOP predlošci - https://azop.hr/obrasci-predlosci/
3. CNIL PIA software, dostupno na: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment (09.02.2024.)
4. Informacije o tvrtki Vigilant Software dostupne na: https://www.vigilantsoftware.co.uk/topic/about (09.02.2024.)
5. Vigilant DPIA Tool, dostupno na: https://www.vigilantsoftware.co.uk/topic/dpia (09.02.2024.)
6. OneTrust platforma, informacije dostupne na: https://www.onetrust.com/platform/ (09.02.2024.)
7. OneTrust Assessment Automation (PIA/DPIA), informacije dostupne na: https://www.onetrust.com/products/pia-and-dpia-automation/ (09.02.2024.)
8. Informacije o RegTech rješenju dostupne su na: https://www.acuitygroup.com/products/regtech/ (09.02.2024.)
9. Više informacija o alatu Base17 dostupno na: https://www.base27.eu/features (09.02.2024.)
10. Baze27 DPIA, dostupno na: https://www.base27.eu/blog/dpia-data-protection-impact-assessment (09.02.2024.)

11. Informacije o alatu MexonInControl dostupne na: https://www.mexontechnology.com/mexonincontrol-for-privacy/ (09.02.2024.)
12. Informacije o Dapian alatu dostupne na: https://dapian.uk/features/ (09.02.2024.)
13. Informacije o DPOinBOX alatu dostupne na: https://www.dpoinbox.com/features/ (09.02.2024.)
14. Gabel, D., Hickman, T., „Chapter 12: Impact Assessments, DPOs and Codes of Conduct – Unlocking the EU General Data Protection Regulation“, White & Case, dostupno na: https://www.whitecase.com/insight-our-thinking/chapter-12-impact-assessments-dpos-and-codes-conduct-unlocking-eu-general-data (09.02.2024.)
15. Enforcement Tracker, dostupno na: https://www.enforcementtracker.com/ (09.02.2024.)
16. ITIL 4 - wiki, informacije dostupne na: https://wiki.en.it-processmaps.com/index.php/ITIL_4 (09.02.2024.)
17. ITIL 4, informacije dostupne na: https://www.axelos.com/certifications/itil-service-management/what-is-itil (09.02.2024.)
18. Data Privacy Manager alat, informacije dostupne: https://legit.eu/ (09.02.2024.)
19. Assessment Automation modul (Data Privacy Manager alat), informacije dostupne na: https://dataprivacymanager.net/products/privacy-program-automation/assessment-automation/ (09.02.2024.)
20. Risk Managment modul (Data Privacy Manager alat), informacije dostupne na https://dataprivacymanager.net/products/privacy-program-automation/risk-management/ (09.02.2024.)

PRILOZI

Prilog 1. – Kriteriji za prihvatljivu procjenu učinka na zaštitu podataka

Radna skupina za zaštitu podataka iz članka 29. predlaže slijedeće kriterije kojima se voditelji obrade podataka mogu koristiti kako bi procijenili je li procjena učinka na zaštitu podataka ili metodologija za provođenje procjene učinka na zaštitu podataka dostatno opsežna za potrebe usklađivanja s Općom uredbom o zaštiti podataka:

- ☐ procjena sadržava sustavan opis obrade (članak 35. stavak 7. točka (a)):
  - ☐ u obzir su uzeti priroda, opseg, kontekst i svrhe obrade (uvodna izjava 90.);
  - ☐ zabilježeni su osobni podaci, primatelji i razdoblje pohrane osobnih podataka;
  - ☐ naveden je funkcionalni opis postupka obrade;
  - ☐ utvrđena su sredstva o kojima ovise osobni podaci (oprema, računalni programi, mreže, osobe, dokumenti u papirnatom obliku ili kanali za slanje dokumenata u papirnatom obliku);
  - ☐ u obzir je uzeta i usklađenost s odobrenim kodeksima ponašanja (članak 35. stavak 8.);
- ☐ procijenjene su nužnost i proporcionalnost (članak 35. stavak 7. točka (b)):
  - ☐ određene su mjere predviđene za usklađivanje s Uredbom (članak 35. stavak 7. točka (d) i uvodna izjava 90.), uzimajući u obzir:
    - ☐ mjere koje pridonose proporcionalnosti i nužnosti obrade na temelju:
      - ☐ posebnih, izričitih i zakonitih svrha (članak 5. stavak 1. točka (b));
      - ☐ zakonitosti obrade (članak 6.);
      - ☐ primjerenih i relevantnih osobnih podataka, ograničenih na ono što je nužno (članak 5. stavak 1. točka (c));
      - ☐ ograničenog trajanja pohrane (članak 5. stavak 1. točka (e));
    - ☐ mjere koje pridonose pravima ispitanika:
      - ☐ informacije pružene ispitaniku (članak 12., 13. i 14.);
      - ☐ pravo na pristup i prenosivost podataka (članci 15. i 20.);
      - ☐ pravo na ispravak i brisanje (članci 16., 17. i 19.);
      - ☐ pravo na prigovor i ograničavanje obrade (članci 18., 19. i 21.);
      - ☐ odnosi s izvršiteljima obrade (članak 28.);
      - ☐ zaštitne mjere koje se odnose na međunarodni prijenos (poglavlje V.);
      - ☐ prethodno savjetovanje (članak 36.).
- ☐ kontrolirani su rizici za prava i slobode ispitanika (članak 35. stavak 7. točka (c)):
  - ☐ uvaženi su izvor, priroda, osobitost i ozbiljnost rizika (vidjeti uvodnu izjavu 84.) ili detaljnije, za svaki rizik (neovlašteni pristup, neželjene izmjene i nestanak podataka) iz perspektive ispitanika:
    - ☐ u obzir su uzeti izvori rizika (uvodna izjava 90.);
    - ☐ mogući učinci na prava i slobode ispitanika utvrđeni su među ostalim u slučaju neovlaštenog pristupa, neželjene izmjene i nestanka podataka;
    - ☐ utvrđene su prijetnje koje mogu dovesti do neovlaštenog pristupa, neželjene izmjene i nestanka podataka;
    - ☐ procijenjene su vjerojatnost i ozbiljnost (uvodna izjava 90.);

- ☐ određene su mjere predviđene za uklanjanje tih rizika (članak 35. stavak 7. točka (d) i uvodna izjava 90.);

☐ <u>uključene su zainteresirane strane:</u>

- ☐ zatražen je savjet službenika za zaštitu podataka (članak 35. stavak 2.);
- ☐ prema potrebi zatražena su mišljenja ispitanika ili njihovih predstavnika (članak 35. stavak 9.).

ŽIVOTOPIS

Tamara Ivelja diplomirana je inženjerka geodezije i geoinformatike, stručnjakinja za daljinska istraživanja. Stekla je kvalifikaciju prvostupnice (2009.) i magistre (2011.) geodezije i geoinformatike na Geodetskom fakultetu Sveučilišta u Zagrebu.

Radila je kao istraživačica na EU FP7 projektu „TIRAMISU“ (2012.-2016). tijekom kojeg je sudjelovala na razvoju multisenzorskih akvizicijskih sustava i metoda analize hiperspektralnih i multispektralnim podataka. Tijekom 2014. godine vodila je operacije dva tima daljinski upravljanih zrakoplovnih sustava u istraživanju minskih polja oštećenih poplavama, bujicama i klizištima u projektu „Protuminsko djelovanje nakon poplava – regionalna sinergija, tehnološki razvoj i izgradnja kapaciteta“.

Izabrana je u nastavno zvanje predavača u području tehničkih znanosti, polje računarstvo pri Tehničkom veleučilištu u Zagrebu (2019.), gdje je od 2015. do 2021. godine sudjelovala na provedbi kolegija: Digitalna obrada slike, Inovacije u informatici, Upravljanje kontinuitetom poslovanja, Upravljanje rizicima i incidentima informacijske sigurnosti, Integrirani sustavi informacijske sigurnosti, Geodezija, Uvod u umjetnu inteligenciju, Upravljanje okolišem te GIS i prostorne baze podataka.

Ima veliko iskustvo u vođenju i upravljanju projektima u obrazovnom sektoru i području istraživanja i razvoja s posebnim naglaskom na informacijske tehnologije. Specijalizirala se u pripremi i vođenju projekata financirani iz sredstava Europske unije koja je stekla obnašajući ulogu Voditelji projektnog centra na Tehničkom veleučilištu u Zagrebu te radom u konzultantskoj tvrtki Speculum. Trenutno je zaposlena u udruzi „MI“ – Split kao voditelj projekta istraživanja i razvoja sustava za tele-medicinu.

U svom dosadašnjem radu objavila je sljedeće stručne i znanstvene radove:

1. Bechor, B., Sivan, D., Miko, S., Hasan, O., Grisonić, M., Rossi, I. Radić, Lorentzen, B., Artioli, G., Ricci, G., Ivelja, T. et al., “*Salt pans as a new archaeological sea-level proxy: A test case from Dalmatia*”, Croatia //

Quaternary Science Reviews, 250, 106680, 18, 2020., doi:10.1016/j.quascirev.2020.106680

2. Ivelja, T., Bechor, B., Hasan, O., Miko, S., Sivan, D., Brook, A., "*Improving vertical accuracy of UAV digital surface models by introducing terrestrial laser scans on a point-cloud level*", The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences, Nica, Francuska: Copernicus GmbH, 2020., str. 457-463, doi:10.5194/isprs-archives-xliii-b1-2020-457-2020
3. Krtalić, A., Bajić, M., Ivelja, T. & Racetin, I., "*The AIDSS Module for Data Acquisition in Crisis Situations and Environmental Protection*", Sensors, 20 (5), 2020., str. 1-29, doi:10.3390/s20051267.
4. Krtalić, A., Ivelja, T., & Racetin, I., "*Analysis of vegetation indices of urban vegetation in Zagreb (Croatia)*", The 18th International Multidisciplinary Scientific Geoconference SGEM 2018. Vol. 18, Informatics, Geoinformatics and Remote Sensing, Isue:2.3, Photogrammetry and Remote Sensing, Cartography and GIS., 2018.
5. Bajić, M., & Ivelja, T., "*The rationale and concept of collecting IED, UXO and landmines signatures*", The 15th International Symposium "Mine Action 2018.", 9th to 12th April 2018, Slano, Croatia, Book of papers, 2018., str. 49 – 52.
6. Horvat, M., Žagar, M., & Ivelja, T., "*Detection of strong mine presence indicators using intelligent algorithms*". The 15th International Symposium "Mine Action 2018.", 9th to 12th April 2018, Slano, Croatia, Book of papers, 2018., str. 25 - 28.
7. Ivelja, T., & Roić, M., "*Standards comparison for the implementation of 3D cadastre*", VI. hrvatski kongres o katastru, 11th to 14th April 2018, Zagreb, Croatia, Book of papers, 2018., str. 82-89.
8. Ivelja, T., & Brook, A., "*Vegetation Indices Correlation Of Different Calibration Stages Of The Hyperion And Landsat 8 Imagery*", 37th EARSeL Symposium, 2017., Prague. http://symposium.earsel.org/37th-symposium-Prague/wp- content/uploads/2016/06/2017_EARSeL_abppact_book.pdf (reported)
9. Bajić, M., Ivelja, T., & Brook, A., "*Developing a Hyperspectral Non-Technical Survey for Minefields via UAV and Helicopter*". Journal of Conventional Weapons Destruction, 21(1), 11, 2017.
10. Bajić, M., & Ivelja, T., "*Transfer of knowledge and technologies from mine action to counter improvised explosive devices (C-IED) domain*", Polytechnic and design, 4(3), 2016., str. 300-309.
11. Čosović Bajić, S., Ivelja, T., & Bajić, M., "*Detection of preconditioned honeybees on data in visible wavelengths range collected from RPAS*", The 13th International Symposium "Mine Action 2016", 26th to 29th April 2016, Biograd, Croatia, Book of papers, 2016, str. 195-199.
12. Bajić, M., & Ivelja, T., "*New technology for mine action – the hyperspectral Non-Technical Survey from UAV and helicopter*", The 13th International Symposium "Mine Action 2016", 26th to 29th April 2016, Biograd, Croatia, Book of papers, 2016., str. 179-183.

13. Ivelja, T., & Bajić, M., "*Destructive impact of natural disaster on minefields, endangerment - Geodesign response*", 2015 Geodesign Summit Europe, 11th to 13th October, 2015, Salzburg. http://proceedings.esri.com/library/userconf/geodesign-euro15/index.html (reported)
14. Bajić, M., Ivelja, T., Hadžić, E., Balta, H., Skelac, G., & Grujić, Z., "*Impact of Flooding on Mine Action in Bosnia and Herzegovina, Croatia, and Serbia*", Journal of Conventional Weapons Destruction, 19(1), 12., 2015., str. 43-49.
15. Avdić, E., Balta, H., & Ivelja, T., "*UAS deployment and data processing of natural disaster with impact to mine action in B&H, case study: Region Olovo*", The 12th International Symposium "Mine Action 2015", 27th to 30th April 2015, Biograd, Croatia, Book of papers, 2015., str. 5-12.
16. Ivelja, T., Bajić, M. & Skelac, G., "*UAV deployment in Survey with Hyperspectral Line Scanner*", The 12th International Symposium "Mine Action 2015", 27th to 30th April 2015, Biograd, Croatia, Book of papers, 2015., str. 37- 42.
17. Kukuruzović, N., Skelac, G., Ivelja, T. & Petričević, R., "*Integration of RPAS in mine action procedures of non-technical area survey that is under destructive impact of the landslides and sediment torrents – Case study: Krsno polje – Maglaj*", The 12th International Symposium "Mine Action 2015", 27th to 30th April 2015, Biograd, Croatia, Book of papers, 2015., str. 77- 83.
18. Bajić, M., Ivelja, T., "*Spatial, situation statistical models of the uas's survey of the mine suspected areas damaged by landslides, torrents and floods*", The 12th International Symposium "Mine Action 2015", 27th to 30th April 2015, Biograd, Croatia, Book of papers, 2015., str. 214.
19. Bajić, M., Ivelja, T., Pavković & N., Vuletić, N., "*Results, limitations of the applied available technologies for the aerial surveillance of mine fields destructed by landslides, torrents and floods at very large area*", RISE 2015 Workshop, Lisbon, Portuguese Naval Academy, 28.01.2015. http://sig.inescporto.pt/proj-rise2015/program (reported)
20. Bajić, M., Krajnović, M., Brook, A. & Ivelja,T., "*Ground vehicle-based system for hyper spectral measurement of minefields*", The 11th International Symposium "Mine Action 2014", 23rd to 25th April 2014, Zadar, Croatia, Book of papers, 2014., str. 13-15.
21. Ivelja, T., Racetin, I., & Krtalić, A., "*Data acquisition within T-AI DSS*", The 11th International Symposium "Mine Action 2014", 23rd to 25th April 2014, Zadar, Croatia, Book of papers, 2014., str. 84-87.
22. Bajić, M., Ivelja, T., Krtalić, A., Tomić, M., & Vuletić, D., "*The multisensor and hyper spectral survey of the UXO around the exploded ammunition depot, of the land mines test site vegetation*", In The 10th International Symposium″ Humanitarian demining 2013″, 2013.
23. Ivelja, T.& Bajić, M., "*Parametric Geocoding of the Aerial Hyperspectral Images of the Mine Suspected Area in Mountainous Terrain*", The 8th International Symposium on "Humanitarian Demining 2011", 26th to 28th April 2011, Šibenik, Croatia, Book of papers, 2011., str. 97-100.

BIOGRAPHY

Tamara Ivelja is a Geodesy and Geoinformatics engineer, land survey and remote sensing data analysis specialist. She holds BEng (2009) and MEng (2011) degrees in Geodesy and Geoinformatics from Faculty of Geodesy, the University of Zagreb.

She worked as a researcher on the EU FP7 project TIRAMISU (2012-2016). During the project, she was working on the development of multisensor acquisition systems and data analysis methods on hyperspectral and multispectral imagery. During 2014. she led operations of two Remotely Piloted Aircraft Systems teams in a survey of minefields damaged by flooding, torrents, and landslides in project “Mine Action After the Floods – Regional Sinergy, Technology Development and Capacity”.

She was elected to the teaching position of lecturer in the field of technical sciences - computing at the Zagreb University of Applied Sciences (2019), where she participated in the implementation of the following courses (2015 - 2021): Digital Image Processing, Innovations in IT, Business Continuity Management, Risk Management and Information Security Incidents, Integrated Information Security Systems, Geodesy, Introduction to Artificial Intelligence, Environmental Management and GIS and Spatial databases.

She specializes in the project proposal preparation and EU project management, which she acquired while holding the role of Head of the Project Center at Zagreb University of Applied Sciences and working in the consulting company Speculum. She is currently employed in the association "MI" - Split as a project manager for research and development of telemedicine system.

So far, she has published the following professional and scientific pappers:

1. Bechor, B., Sivan, D., Miko, S., Hasan, O., Grisonić, M., Rossi, I. Radić, Lorentzen, B., Artioli, G., Ricci, G., Ivelja, T. et al., “*Salt pans as a new archaeological sea-level proxy: A test case from Dalmatia*”, Croatia // Quaternary Science Reviews, 250, 106680, 18, 2020., doi:10.1016/j.quascirev.2020.106680

2. Ivelja, T., Bechor, B., Hasan, O., Miko, S., Sivan, D., Brook, A., "*Improving vertical accuracy of UAV digital surface models by introducing terrestrial laser scans on a point-cloud level*", The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences, Nica, Francuska: Copernicus GmbH, 2020., str. 457-463, doi:10.5194/isprs-archives-xliii-b1-2020-457-2020
3. Krtalić, A., Bajić, M., Ivelja, T. & Racetin, I., "*The AIDSS Module for Data Acquisition in Crisis Situations and Environmental Protection*", Sensors, 20 (5), 2020., str. 1-29, doi:10.3390/s20051267.
4. Krtalić, A., Ivelja, T., & Racetin, I., "*Analysis of vegetation indices of urban vegetation in Zagreb (Croatia)*", The 18th International Multidisciplinary Scientific Geoconference SGEM 2018. Vol. 18, Informatics, Geoinformatics and Remote Sensing, Isue:2.3, Photogrammetry and Remote Sensing, Cartography and GIS., 2018.
5. Bajić, M., & Ivelja, T., "*The rationale and concept of collecting IED, UXO and landmines signatures*", The 15th International Symposium "Mine Action 2018.", 9th to 12th April 2018, Slano, Croatia, Book of papers, 2018., str. 49 – 52.
6. Horvat, M., Žagar, M., & Ivelja, T., "*Detection of strong mine presence indicators using intelligent algorithms*". The 15th International Symposium "Mine Action 2018.", 9th to 12th April 2018, Slano, Croatia, Book of papers, 2018., str. 25 - 28.
7. Ivelja, T., & Roić, M., "*Standards comparison for the implementation of 3D cadastre*", VI. hrvatski kongres o katastru, 11th to 14th April 2018, Zagreb, Croatia, Book of papers, 2018., str. 82-89.
8. Ivelja, T., & Brook, A., "*Vegetation Indices Correlation Of Different Calibration Stages Of The Hyperion And Landsat 8 Imagery*", 37th EARSeL Symposium, 2017., Prague. http://symposium.earsel.org/37th-symposium-Prague/wp- content/uploads/2016/06/2017_EARSeL_abppact_book.pdf (reported)
9. Bajić, M., Ivelja, T., & Brook, A., "*Developing a Hyperspectral Non-Technical Survey for Minefields via UAV and Helicopter*". Journal of Conventional Weapons Destruction, 21(1), 11, 2017.
10. Bajić, M., & Ivelja, T., "*Transfer of knowledge and technologies from mine action to counter improvised explosive devices (C-IED) domain*", Polytechnic and design, 4(3), 2016., str. 300-309.
11. Čosović Bajić, S., Ivelja, T., & Bajić, M., "*Detection of preconditioned honeybees on data in visible wavelengths range collected from RPAS*", The 13th International Symposium "Mine Action 2016", 26th to 29th April 2016, Biograd, Croatia, Book of papers, 2016, str. 195-199.
12. Bajić, M., & Ivelja, T., "*New technology for mine action – the hyperspectral Non-Technical Survey from UAV and helicopter*", The 13th International Symposium "Mine Action 2016", 26th to 29th April 2016, Biograd, Croatia, Book of papers, 2016., str. 179-183.
13. Ivelja, T., & Bajić, M., "*Destructive impact of natural disaster on minefields, endangerment - Geodesign response*", 2015 Geodesign Summit Europe, 11th to 13th October, 2015, Salzburg.

http://proceedings.esri.com/library/userconf/geodesign-euro15/index.html (reported)
14. Bajić, M., Ivelja, T., Hadžić, E., Balta, H., Skelac, G., & Grujić, Z., "*Impact of Flooding on Mine Action in Bosnia and Herzegovina, Croatia, and Serbia*", Journal of Conventional Weapons Destruction, 19(1), 12., 2015., str. 43-49.
15. Avdić, E., Balta, H., & Ivelja, T., "*UAS deployment and data processing of natural disaster with impact to mine action in B&H, case study: Region Olovo*", The 12th International Symposium "Mine Action 2015", 27th to 30th April 2015, Biograd, Croatia, Book of papers, 2015., str. 5-12.
16. Ivelja, T., Bajić, M. & Skelac, G., "*UAV deployment in Survey with Hyperspectral Line Scanner*", The 12th International Symposium "Mine Action 2015", 27th to 30th April 2015, Biograd, Croatia, Book of papers, 2015., str. 37- 42.
17. Kukuruzović, N., Skelac, G., Ivelja, T. & Petričević, R., "*Integration of RPAS in mine action procedures of non-technical area survey that is under destructive impact of the landslides and sediment torrents – Case study: Krsno polje – Maglaj*", The 12th International Symposium "Mine Action 2015", 27th to 30th April 2015, Biograd, Croatia, Book of papers, 2015., str. 77- 83.
18. Bajić, M., Ivelja, T., "*Spatial, situation statistical models of the uas's survey of the mine suspected areas damaged by landslides, torrents and floods*", The 12th International Symposium "Mine Action 2015", 27th to 30th April 2015, Biograd, Croatia, Book of papers, 2015., str. 214.
19. Bajić, M., Ivelja, T., Pavković & N., Vuletić, N., "*Results, limitations of the applied available technologies for the aerial surveillance of mine fields destructed by landslides, torrents and floods at very large area*", RISE 2015 Workshop, Lisbon, Portuguese Naval Academy, 28.01.2015. http://sig.inescporto.pt/proj-rise2015/program (reported)
20. Bajić, M., Krajnović, M., Brook, A. & Ivelja,T., "*Ground vehicle-based system for hyper spectral measurement of minefields*", The 11th International Symposium "Mine Action 2014", 23rd to 25th April 2014, Zadar, Croatia, Book of papers, 2014., str. 13-15.
21. Ivelja, T., Racetin, I., & Krtalić, A., "*Data acquisition within T-AI DSS*", The 11th International Symposium "Mine Action 2014"**,** 23rd to 25th April 2014, Zadar, Croatia, Book of papers, 2014., str. 84-87.
22. Bajić, M., Ivelja, T., Krtalić, A., Tomić, M., & Vuletić, D., "*The multisensor and hyper spectral survey of the UXO around the exploded ammunition depot, of the land mines test site vegetation*", In The 10th International Symposium″ Humanitarian demining 2013″, 2013.
23. Ivelja, T.& Bajić, M., "*Parametric Geocoding of the Aerial Hyperspectral Images of the Mine Suspected Area in Mountainous Terrain*", The 8th International Symposium on "Humanitarian Demining 2011", 26th to 28th April 2011, Šibenik, Croatia, Book of papers, 2011., str. 97-100.