SUPPORT POOL OF EXPERTS PROGRAMME

Praktikum za službenike za zaštitu osobnih podataka

ZAŠTITA PODATAKA U ZDRAVSTVU

by Tihomir Katulić

Professor at the University of Zagreb, ICT Law and Data Protection

As part of the SPE programme, the EDPB may commission contractors to provide reports and tools on specific topics.

The views expressed in the deliverables are those of their authors and they do not necessarily reflect the official position of the EDPB. The EDPB does not guarantee the accuracy of the information included in the deliverables. Neither the EDPB nor any person acting on the EDPB's behalf may be held responsible for any use that may be made of the information contained in the deliverables.

Some excerpts may be redacted or removed from the deliverables as their publication would undermine the protection of legitimate interests, including, inter alia, the privacy and integrity of an individual regarding the protection of personal data in accordance with Regulation (EU) 2018/1725 and/or the commercial interests of a natural or legal person.

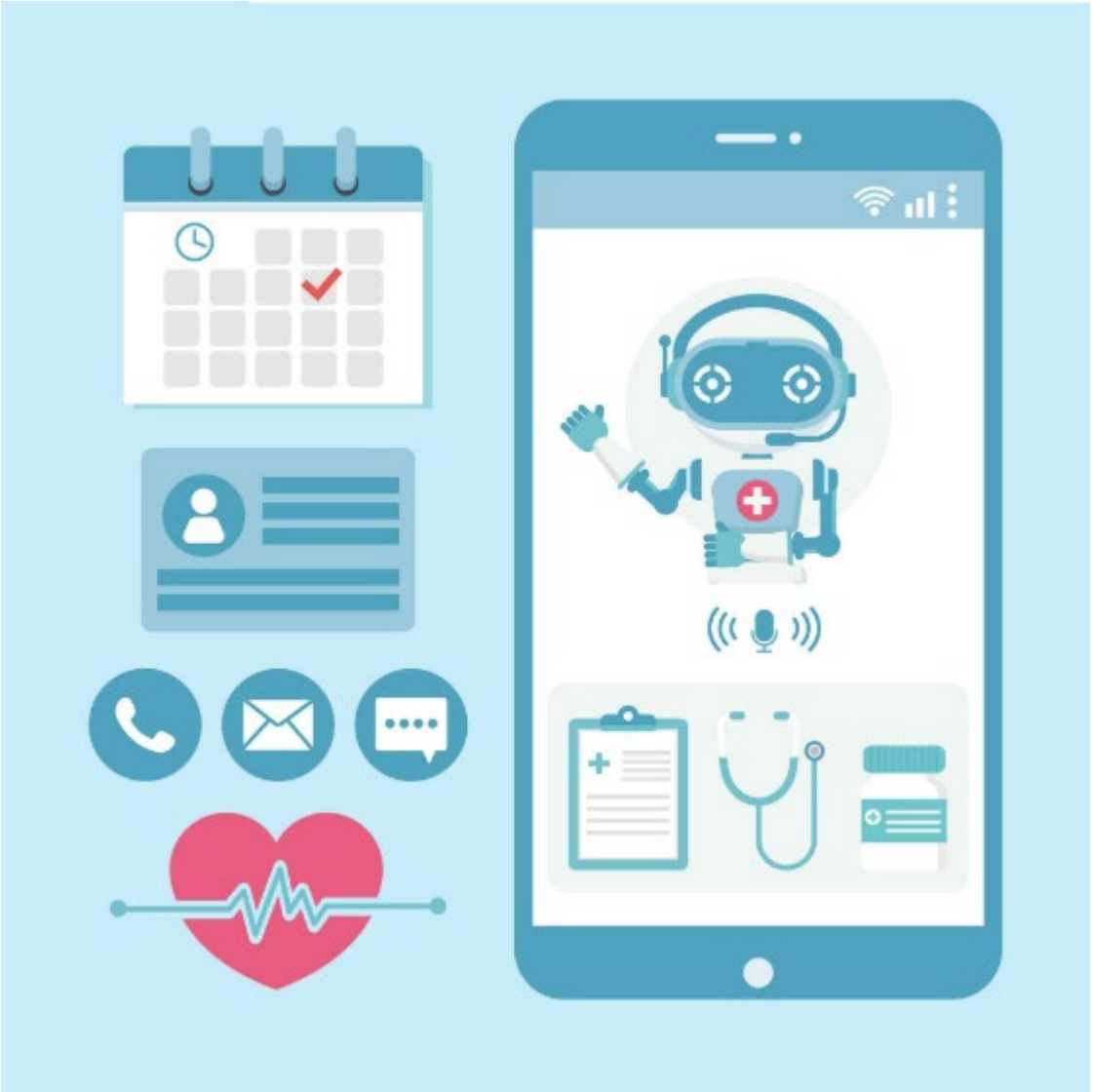
Document submitted in May 2024

SADRŽAJ 1/2

- Što su zdravstveni podaci
- Koje su obveze voditelja i izvršitelja obrade sukladno sektorskoj zdravstvenoj regulativi iz perspektive zaštite podataka
- Problemi s razumijevanjem i primjenom **osnovnih koncepata zaštite podataka**
- Karakteristične **obrade**, **pravne osnove**, najčešći rizici i kako ih tretirati
- **Gdje** su **naši podaci** i tko je za njih **odgovoran**
- Koji su **ključni informacijski sustavi zdravstvenog sustava** i kako su regulirani
- Poteškoće s primjenom mehanizama procjene učinka na zaštitu podataka (**DPIA),** testa razmjernosti (procjene legitimnog interesa, **LIA)** i institutom privole

SADRŽAJ 2/2

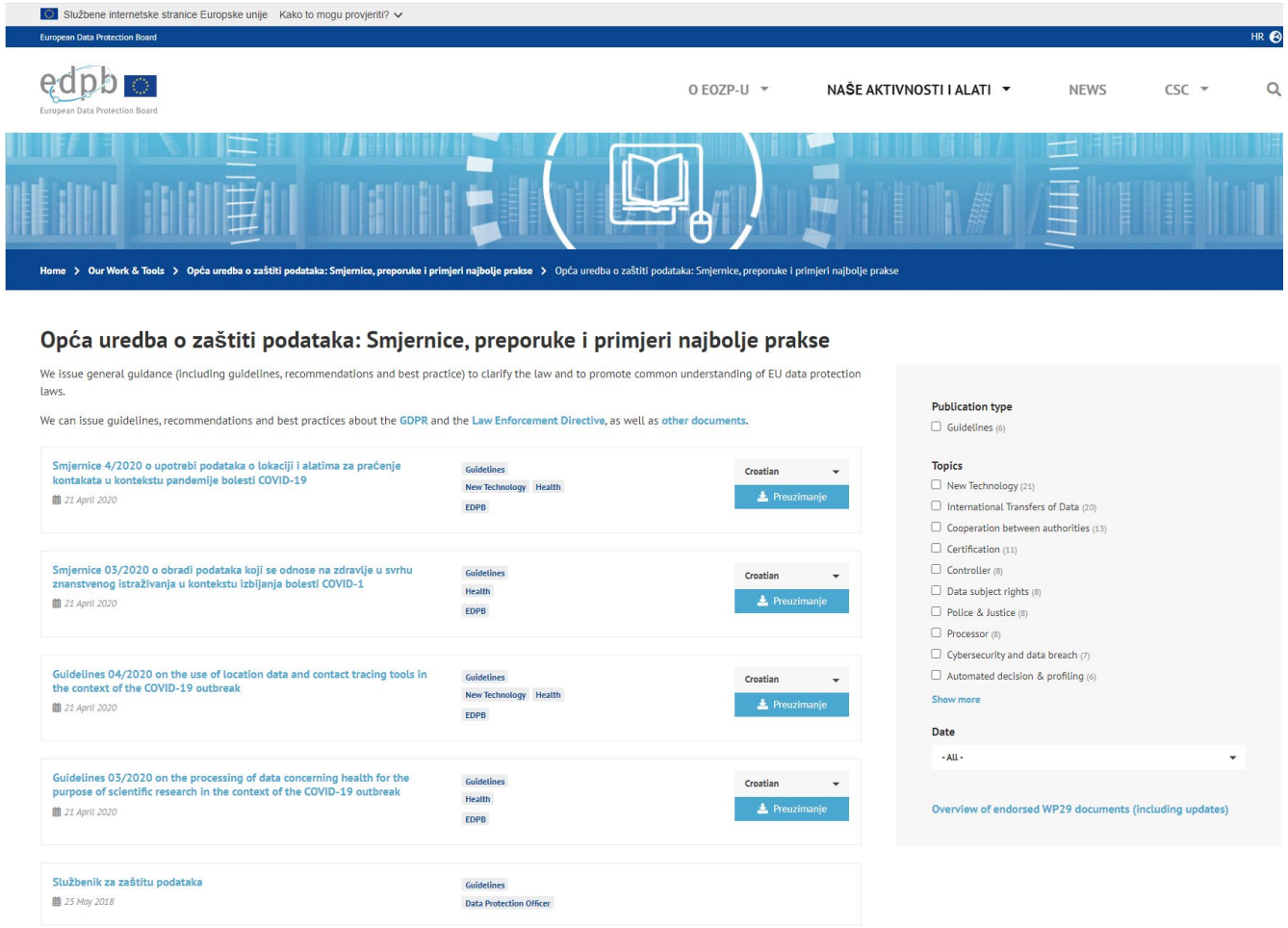
- Kako do **kompetentnog i učinkovitog SZOP**
- Primjenjiva mišljenja i smjernice **o zaštiti podataka i znanstvenim istraživanjima**
- Osvrt na **specifična pravila iz implementacijskog propisa**
- **Praksa nadzornih tijela**
- **Pitanja iz prakse zdravstvenih organizacija**



Izvori: smjernice, mišljenja nadzorna praksa

U pripremi ove edukacije korišteni su sljedeći izvori:

- Nacionalni propisi RH i drugih država članica
- Smjernice i mišljenja EDPB i nekadašnji WP29
- Upute nadzornih tijela i EDPS
- Presude Europskog suda (ECJ) i Europskog suda za ljudska prava (ECHR)
- Vodiči i mišljenja neovisnih stručnih udruga i organizacija
- Studije Europske komisije
- Samoregulacijski industrijski standardi
- Podaci neovisnih *trackera* nadzorne prakse



Umjesto uvoda – pogled u pravni okvir zdravstvenih usluga u RH

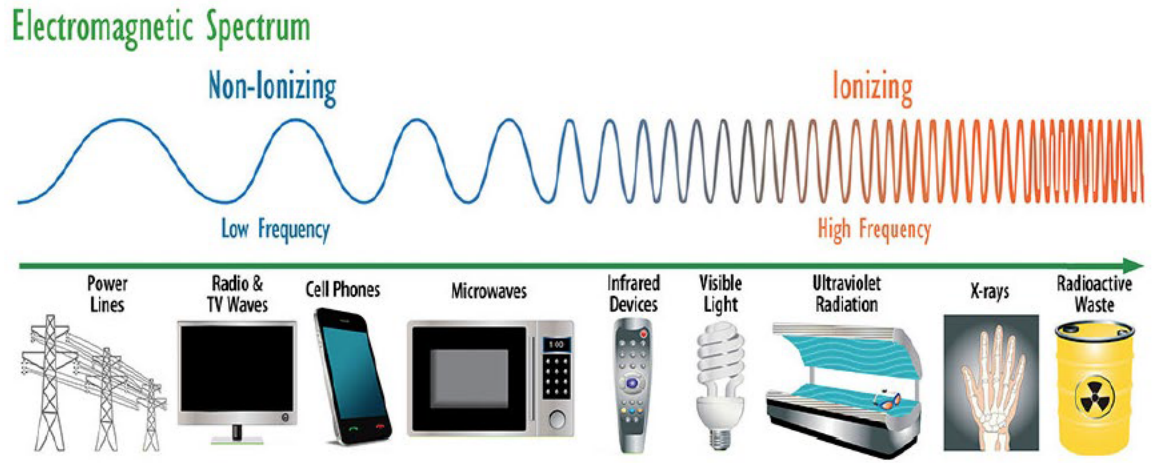
1. Zakon o podacima i informacijama u zdravstvu
2. Zakon o zdravstvenoj zaštiti
3. Zakon o obveznom zdravstvenom osiguranju
4. Zakon o obveznom zdravstvenom osiguranju i zdravstvenoj zaštiti stranaca u Republici Hrvatskoj Zakon o dobrovoljnom zdravstvenom osiguranju
5. Zakon o liječništvu
6. Zakon o ljekarništvu
7. Zakon o sestrinstvu
8. Zakon o dentalnoj medicini
9. Zakon o primaljstvu
10. Zakon o medicinsko-biokemijskoj djelatnosti
11. Zakon o fizioterapeutskoj djelatnosti
12. Zakon o djelatnostima u zdravstvu
13. Zakon o kvaliteti zdravstvene zaštite
14. Zakon o suzbijanju zlouporabe droga
15. Zakon o provedbi uredbi Europske unije iz područja prekursora za droge
16. Zakon o lijekovima
17. Zakon o provedbi Uredbe (EU) 2017/745 o medicinskim proizvodima i Uredbe (EU) 2017/746 o in vitro dijagnostičkim medicinskim proizvodima
18. Zakon o zaštiti osoba s duševnim smetnjama
19. Zakon o Hrvatskom Crvenom križu
20. Zakon o obeštećenju radnika profesionalno izloženih azbestu
21. Zakon o obveznom zdravstvenom nadzoru radnika profesionalno izloženih azbestu
22. Zakon o krvi i krvnim pripravcima
23. Zakon o primjeni ljudskih tkiva i stanica
24. Zakon o presađivanju ljudskih organa u svrhu liječenja
25. Zakon o medicinski pomognutoj oplodnji
26. Zakon o podacima i informacijama u zdravstvu
27. Zakon o provedbi Uredbe (EU) 2017/745 o medicinskim proizvodima i Uredbe (EU) 2017/746 o in vitro dijagnostičkim medicinskim proizvodima
28. Zakon o provedbi Uredbe (EU) br. 536/2014 Europskog parlamenta i vijeća od 16. travnja 2014. o kliničkim ispitivanjima lijekova za primjenu kod ljudi te ostavljanju izvan snage Direktive 2001/20/EZ
29. Zakon o privremenoj mjeri u području obveznog zdravstvenog osiguranja
30. Zakon o potvrđivanju Konvencije Vijeća Europe o krivotvorenju farmaceutskih proizvoda i sličnim kažnjivim dijelima koja uključuju prijetnje javnom zdravlju

Pravilnici

1. Pravilnik o iskaznici i znački sanitarnog inspektora
2. Pravilnik o specijalističkom usavršavanju doktora medicine
3. Pravilnik o osiguranju sljedivosti tkiva od darivatelja do primatelja, načinu praćenja ozbiljnih štetnih događaja i ozbiljnih štetnih reakcija, načinu vođenja evidencije i rokovima izvješćivanja te sadržaju tiskanice godišnjeg izvješća
4. Pravilnik o specijalističkom usavršavanju doktora medicine iz obiteljske medicine
5. Pravilnik o siguranju kvalitete krvi i krvnih pripravaka u zdravstvenim ustanovama
6. Pravilnik o načinu provedbe stručne procjene u ovlaštenoj zdravstvenoj ustanovi radi ostvarivanja statusa hrvatskog ratnog vojnog invalida
7. Pravilnik o načinu korištenja znaka crvenog križa u hrvatskom crvenom križu i njegovim ustrojstvenim oblicima
8. Pravilnik o uvjetima za unutarnji ustroj općih i specijalnih bolnica
9. Pravilnik o uvjetima za unutarnji ustroj kliničkih zdravstvenih ustanova
10. Pravilnik o minimalnim uvjetima u pogledu prostora, radnika i medicinsko-tehničke opreme za obavljanje zdravstvene djelatnosti
11. Pravilnik o posebnim uvjetima za proizvodnju i stavljanje na tržište predmeta opće uporabe
12. Pravilnik o pomoćnim tvarima u procesu proizvodnje
13. Pravilnik o načinu provedbe zaštitne mjere obveznog liječenja od ovisnosti
14. Pravilnik o uvjetima i načinu obavljanja opremanja, prijenosa, prijevoza, kremiranja, pogreba i iskopavanja umrlih osoba te o uvjetima glede prostora i opreme pravnih i fizičkih osoba za obavljanje opremanja, prijenosa, prijevoza, kremiranja, pogreba i iskopavanja umrlih osoba
15. Pravilnik o načinu obavljanja zdravstvenih pregleda osoba koje su kliconoše ili se sumnja da su kliconoše određenih zaraznih bolesti
16. Pravilnik o načinu, uvjetima i postupku za davanje akreditacije nositeljima zdravstvene djelatnosti
17. Pravilnik o početku, završetku i rasporedu radnog vremena zdravstvenih ustanova i privatnih zdravstvenih radnika u ordinaciji u mreži javne zdravstvene službe
18. Pravilnik o specijalističkom usavršavanju prvostupnika sestrinstva u djelatnosti hitne medicine
19. Pravilnik o opsegu i sadržaju podataka te načinu vođenja e-Kartona
20. Pravilnik o vrstama i načinu primjene mjera prisile prema osobi s težim duševnim smetnjama
21. Katalog informacijskih standarda u zdravstvu Republike Hrvatske

Srodne kategorije propisa

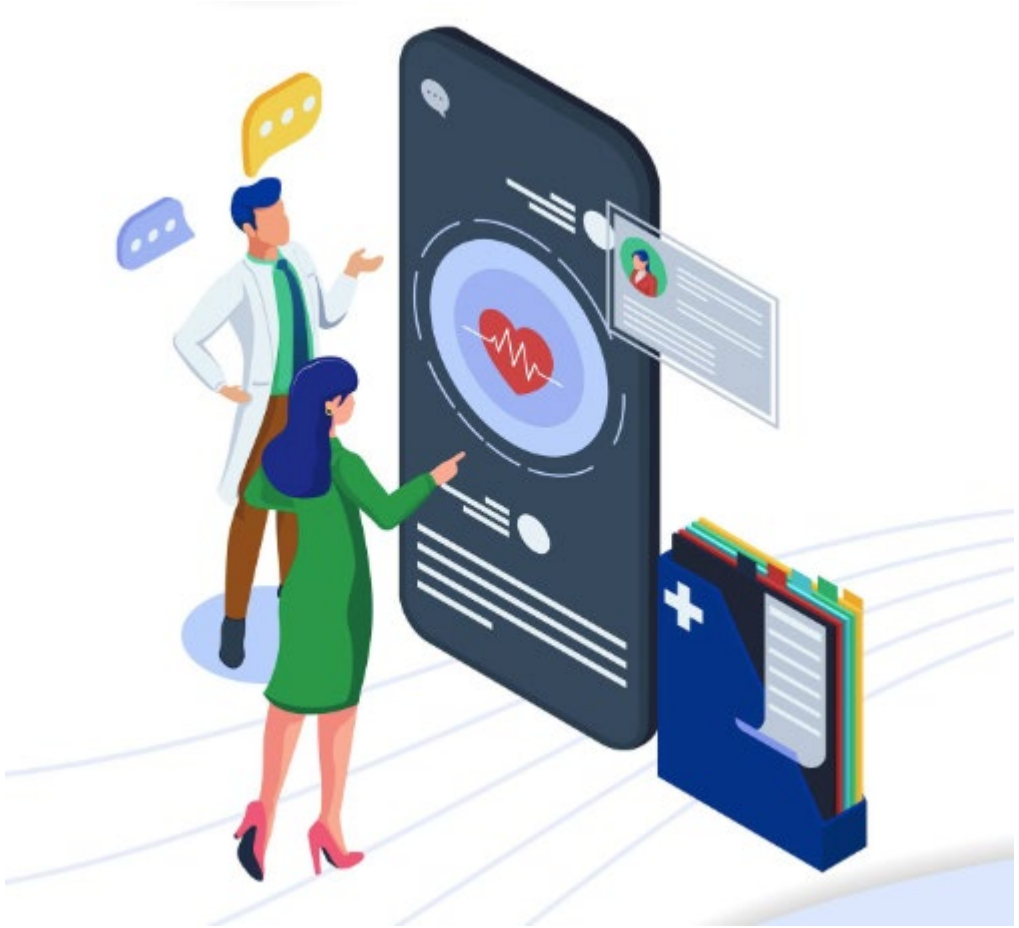
- Propisi iz područja javnozdravstvene zaštite
- Regulacija kemikalija i biocidnih proizvoda
- Zaštita od buke
- Ograničenje upotrebe duhanskih proizvoda
- Predmeti u općoj upotrebi, ne-ionizirajuće zračenje
- Zaštita pučanstva od zaraznih bolesti
- Zdravstvena sigurnost / ispravnost hrane
- Voda za ljudsku potrošnju
- Regulacija genetski modificiranih organizama



Uvodne napomene

Prije dubljeg osvrta na obveze zdravstvenih ustanova, upoznajmo se kratko sa specifičnostima obrade podataka u zdravstvenom sektoru

- Tko su voditelji obrade u zdravstvu?
- Koje obveze imaju zdravstvene ustanove?
- Zbog čega obrade u zdravstvu smatramo rizičnima?
- Koje su najčešće zabune kod voditelja obrade?



Općenito o zaštiti podataka u zdravstvenim ustanovama

- Podaci o zdravstvenom stanju pacijenata spadaju u tzv. posebne kategorije osobnih podataka
- Ovi podaci mogu uključivati detalje o fizičkom i mentalnom zdravlju, dijagnozama, tretmanima, medicinskoj povijesti, koji se u većini pravnih okvira dugotrajno čuvaju
- Zbog svoje osjetljive prirode, ovi podaci zahtijevaju viši stupanj zaštite zbog visoke opasnosti od zloupotrebe
- Pacijenti zaslužuju posebnu zaštitu u pogledu obrade njihovih osobnih podataka. Zbog svojeg stanja mogu biti manje svjesni rizika, posljedica i predmetnih zaštitnih mjera te svojih prava u vezi s obradom njihovih osobnih podataka
- Osobito vrijedi za situacije kad pacijenti nisu u stanju samostalno donositi odluke zbog bolesti, ograničene poslovne sposobnosti ili kad su pacijenti djeca

Općenito o obvezama zdravstvenih organizacija

- Informiranje ispitanika o obradi i osiguranje pristupa podacima
- Informiranje ispitanika o sadržaju i načinu ostvarivanja njihovih prava (članci 12. do 22. Opće uredbe o zaštiti podataka),
- Provođenje odgovarajućih tehničkih i organizacijskih mjera zaštite osobnih podataka (članci 25. i 32. Opće uredbe o zaštiti podataka),
- Vođenje evidencije aktivnosti obrade (članak 30. Opće uredbe o zaštiti podataka),
- Imenovanje službenika za zaštitu podataka (članak 37. Opće uredbe o zaštiti podataka)

- Koja prava imaju ispitanici?
- Koji je sadržaj obavijesti o obradi osobnih podataka?
- Kako ispuniti evidenciju aktivnosti obrade?
- Koga i kako odabiremo za funkciju SZOP?
- Koje tehničke i organizacijske mjere trebamo koristiti?

Zabune i greške oko pravnih osnova obrade

Privola **nije isto što i obavijest o obradi osobnih podataka**

Neki voditelji obrade neopravdano se oslanjaju na privolu kao pravnu osnovu, čak i kad je prikladnije koristiti drugu pravnu osnovu **(npr. ugovornu obvezu ili zakonsku obvezu).**

Za zakonitu obradu osobnih podataka **nužno** je da bude ispunjena barem jedna od taksativno navedenih pravnih osnova iz članka 6. Opće uredbe o zaštiti podataka, a u slučaju zdravstvenih podataka kao posebne kategorije osobnih podataka i barem jedna od osnova iz čl. 9 Uredbe

Općenito - mjere zaštite

- **dokumentaciju u papirnatom obliku** koja sadrži osobne podatke pohraniti, primjerice u ormare ili ladice **pod ključem** koja će biti pod nadzorom ovlaštenih osoba,
- **pristup osobnim podacima pohranjenim u elektroničkom obliku** trebao bi biti omogućen uporabom **korisničkog imena i lozinke**,
- **izrada sigurnosnih kopija** od strane ovlaštenih osoba, bilježenje pristupa podacima
- **potpisivanje izjava o povjerljivosti osoba** koje su u obradi osobnih podataka (Izjave o povjerljivosti možete pronaći na internet stranici ove Agencije https://azop.hr/info-servis/detaljnije/izjava-o-povjerljivosti),
- **pseudonimizacija ili enkripcija osobnih podataka** - osobito ako se radi o posebnim kategorijama (primjerice: podataka o zdravlju).
- Voditelj odabire tehničke i organizacijske mjere ovisno o riziku od nastanka povrede i utjecaju povrede na prava i slobode ispitanika.

Zakon o podacima i informacijama u zdravstvenom sustavu Republike Hrvatske

- Utvrđuje prava, obveze i odgovornosti pravnih i fizičkih osoba zdravstvenog sustava Republike Hrvatske u području upravljanja podacima i informacijama u zdravstvu
- Definira pojmove i temeljna načela prikupljanja, korištenja i obrade zdravstvenih podataka i informacija, nadležna tijela, kvalitetu i obrada zdravstvenih podataka, njihova zaštita te inspekcijski i stručni nadzor
- Osigurava sveobuhvatnog i djelotvorno korištenje zdravstvenih podataka i informacija u zdravstvenoj zaštiti radi unaprjeđenja i očuvanja zdravlja
- Ustrojava CEZIH i NAJS
- Propisuje uspostavu Kataloga informacijskih standarda u zdravstvu RH **koji se ima ustrojiti u roku od 6 mjeseci (NN 14/19)***
- Omogućuje uspostavu zdravstvenih i javnozdravstvenih registara
- Prekršajnim odredbama kažnjava:
  - Nedostupnost
  - Povrede kvalitete podataka
  - Propuste neredovitog nadziranja i kontroliranja vođenja podataka - kažnjavaju se i odgovorne osobe u pravnoj osobi*
  - Kažnjavaju se i liječnici pojedinci

Katalog informacijskih standarda RH – u izradi

- Čl. 41 Zakona o podacima i informacijama u zdravstvu:
  - Ministarstvo nadležno za zdravstvo i HZJZ obvezni su objaviti na svojim mrežnim stranicama Katalog informacijskih standarda u zdravstvu Republike Hrvatske, u roku od šest mjeseci od dana stupanja na snagu Zakona o podacima i informacijama u zdravstvu (2019)
    - Još uvijek nije usvojen
- Katalog informacijskih standarda u zdravstvu Republike Hrvatske je strukturirani skup pojmova, pravila, standarda i procedura stvaranja, prikupljanja i vođenja podataka i informacija u zdravstvu i dio je državne informacijske infrastrukture
  - Po uzoru na druge slične kataloge, trebao bi ponuditi standardizirane upute i mjere
- Katalog informacijskih standarda u zdravstvu Republike Hrvatske obuhvaća:
  1. popis informacijskih sustava i uređenje njihova odnosa unutar zdravstvene informacijske infrastrukture Republike Hrvatske
  2. opseg, sadržaj, način obrade i čuvanja podataka
  3. procese upravljanja zdravstvenim registrima i drugim evidencijama u području zdravstva
  4. popis i definicije nacionalnih zdravstvenih pokazatelja i obilježja podataka temeljem kojih nastaju pokazatelji
- PRIMJER
  1. Rokovi pohrane za specifične obrade (npr. podaci o plodnosti, podaci djece, podaci o bolestima koje nije nužno čuvati trajno)
  2. Tehničke mjere zaštite podataka osjetljivih podataka – smiju li CEZIH i NAJS aplikacije čuvati kopiju podataka lokalno?

Pojmovi

- zdravstveni podatak je podatak o pojedincu, o njegovu fizičkom ili mentalnom zdravlju, uključujući pružene mu zdravstvene usluge u zdravstvenom sustavu Republike Hrvatske
- zdravstvena informacija nastaje obradom zdravstvenih podataka sa svrhom njezine daljnje uporabe u zdravstvenom sustavu ili za potrebe sustava povezanih sa zdravstvenim sustavom
- izvorni zdravstveni podatak je **vjerodostojan zapis** o određenoj **zdravstveno relevantnoj činjenici, mjerenju odnosno zaključku**, koji se **bilježi na mjestu nastanka podatka** ili **na način za koji ovlaštena osoba može jamčiti njegovu izvornost, cjelovitost i vjerodostojnost u trenutku bilježenja**
- **Javnozdravstveni registar** je organizirani sustav prikupljanja, analize i distribucije podataka i informacija o populacijskim skupinama određenim prema njihovu zdravstvenom stanju, bolesti i korištenju zdravstvene zaštite i o pružateljima zdravstvenih usluga, koji je uspostavljen za unaprijed određene kliničke, javnozdravstvene, upravljačke i/ili znanstvene potrebe i vodi se u Nacionalnom javnozdravstvenom informacijskom sustavu (NAJS)
- **zdravstveni registar** je evidencija u području zdravstva koja nastaje prikupljanjem, analizom i distribucijom podataka i informacija o populacijskim skupinama s određenim zdravstvenim stanjem, izloženošću ili pruženom zdravstvenom uslugom, podataka i informacija o pružateljima zdravstvenih usluga, koji je uspostavljen za unaprijed definirane kliničke, javnozdravstvene, upravljačke i/ili znanstvene potrebe i vodi se u zdravstvenim ustanovama
- **CEZIH - Centralni zdravstveni informacijski sustav Republike Hrvatske** (u daljnjem tekstu: CEZIH) je središnji sustav pohrane zdravstvenih podataka i informacija za njihovu standardiziranu obradu na primarnoj, sekundarnoj i tercijarnoj razini zdravstvene zaštite i dio je zdravstvene informacijske infrastrukture Republike Hrvatske
- **NAJS - Nacionalni javnozdravstveni informacijski sustav (u daljnjem tekstu: NAJS)** je sustav pohrane zdravstvenih podataka i informacija za njihovu obradu i arhiviranje (zdravstvene evidencije i registri) radi ostvarenja javnozdravstvenih potreba i dio je zdravstvene informacijske infrastrukture Republike Hrvatske

Definicije

Opća uredba u članku 4. definira temeljne pojmove sustava zaštite osobnih podataka

Definiraju se ključni subjekti: voditelj obrade, izvršitelj obrade i ispitanik, predstavnik, zajednički voditelj

Ključni koncepti: obrada osobnih podataka, povreda osobnih podataka, osobni podatak, posebne kategorije osobnih podataka, biometrijski osobni podaci

Primjeri voditelja obrade: škola, bolnica, trgovačko društvo / poduzeće, općina, udruga s pravnom osobnošću, obrtnik pojedinac

Primjeri kategorija osobnih podataka: kontakt podaci, lokacijski podaci, zdravstveni podaci, podaci o obrazovanju, financijski podaci

Osobni podatak i ispitanik

Ispitanik = osoba čiji se osobni podaci obrađuju

Kad se informacija odnosi na pojedinca?

- Kada je informacija „o pojedincu” (relevantan je sadržaj)
- Kada se informacija obrađuje s ciljem da se na bilo koji način utječe na status ili ponašanje pojedinca (relevantna je svrha obrade)
- Kad obrada informacije može imati utjecaj na prava i interese ispitanika (relevantan je rezultat obrade).

Pojedinac = fizička osoba

Podaci umrlih osoba, nerođene djece

Podaci fizičkih osoba koje obavljaju posebne funkcije (državni dužnosnici, državni i javni službenici…)?

Podaci o pravnim osobama ne uživaju zaštitu prema OUZP, ali mogu biti zaštićeni kroz neka druga prava, primjerice intelektualnog vlasništva

Primjeri

Zdravstveni podatak – bilo koji podatak koji se odnosi na mentalno ili fizičko zdravlje pojedinca ili pruženu uslugu: laboratorijske vrijednosti, snimke pretraga, psihološki testovi = podaci o zdravlju, posebna kategorija podataka prema OUZP

Izvori zdravstvenih podataka

- pacijenti (=pojedinci o kojima se prikupljaju osobni podaci)
- pravne i fizičke osobe zdravstvenog sustava koje sudjeluju u stvaranju zdravstvenih podataka za upravljačke, poslovne, stručne, znanstvene, istraživačke, statističke, administrativne, nadzorne, sigurnosne, informativne i druge potrebe

Obrada, voditelj obrade, izvršitelj obrade isto analogno OUZP

Javnozdravstveni registri ustrojeni u NAJS: legionella, HIV, TBC, nuspojave cijepljenja

Zdravstveni registri: https://metaregistar.gov.hr/metareg/html/javno_pocetna.xhtml

Novčane kazne za prekršaje (ZoPiluZ)

- **povreda dostupnosti zdravstvenih podataka**
  - kazne za pravnu osobu 5-100 tisuća kn
  - kazne za odgovornu osobu u organizaciji 2-20 tisuća kuna
  - kazne za fizičku osobu pružatelja zaštite – 3-30 tisuća kn
- **pružatelj zdravstvene zaštite koji ne razmjenjuje podatke putem CEZIH**
  - kazne za pravnu osobu 5-50 tisuća kn
  - kazne za odgovornu osobu u organizaciji 2-20 tisuća kuna
  - kazne za fizičku osobu pružatelja zaštite – 3-30 tisuća kn
- **pružatelj zdravstvene zaštite koji ne provodi certifikacijski program za računalne aplikacije kroz koje se vode zdravstveni podaci i informacije te provjeru sigurnosti i povjerljivosti podataka**
  - kazne za pravnu osobu 5-50 tisuća kn
  - kazne za odgovornu osobu u organizaciji 2-20 tisuća kuna
  - kazne za fizičku osobu pružatelja zaštite – 3-30 tisuća kn

Obveze voditelja obrade:
Osigurati dostupnost
Razmjenjivati zdravstvene podatke isključivo putem CEZIH
Provoditi certifikaciju aplikacije i provjeru sigurnosti i povjerljivosti podataka

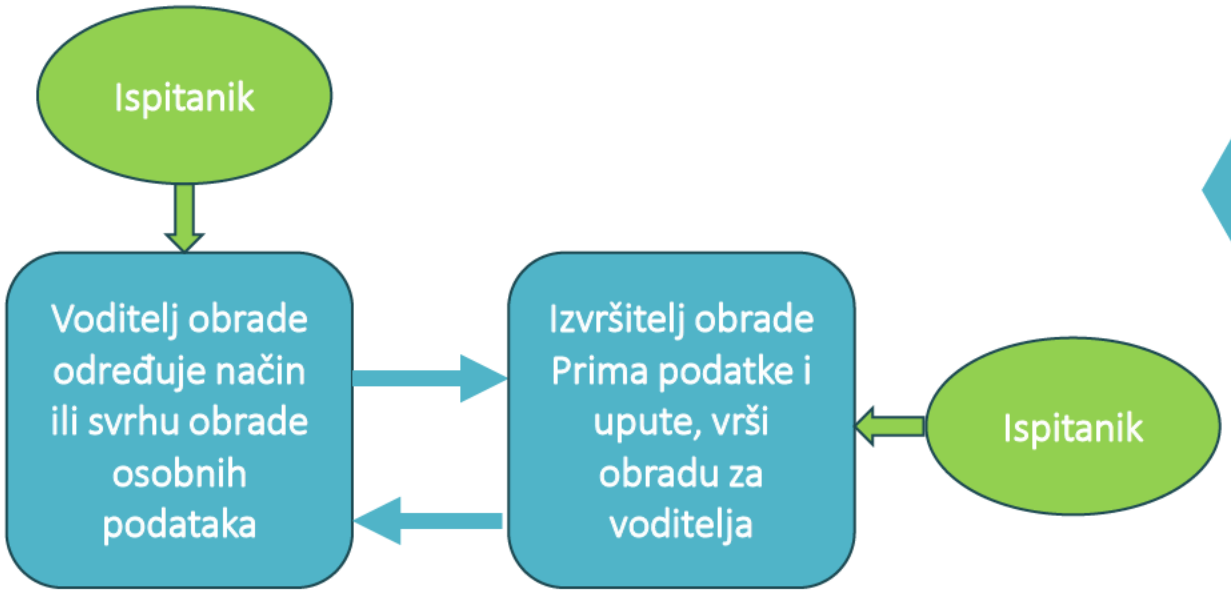
Kako se to radi?

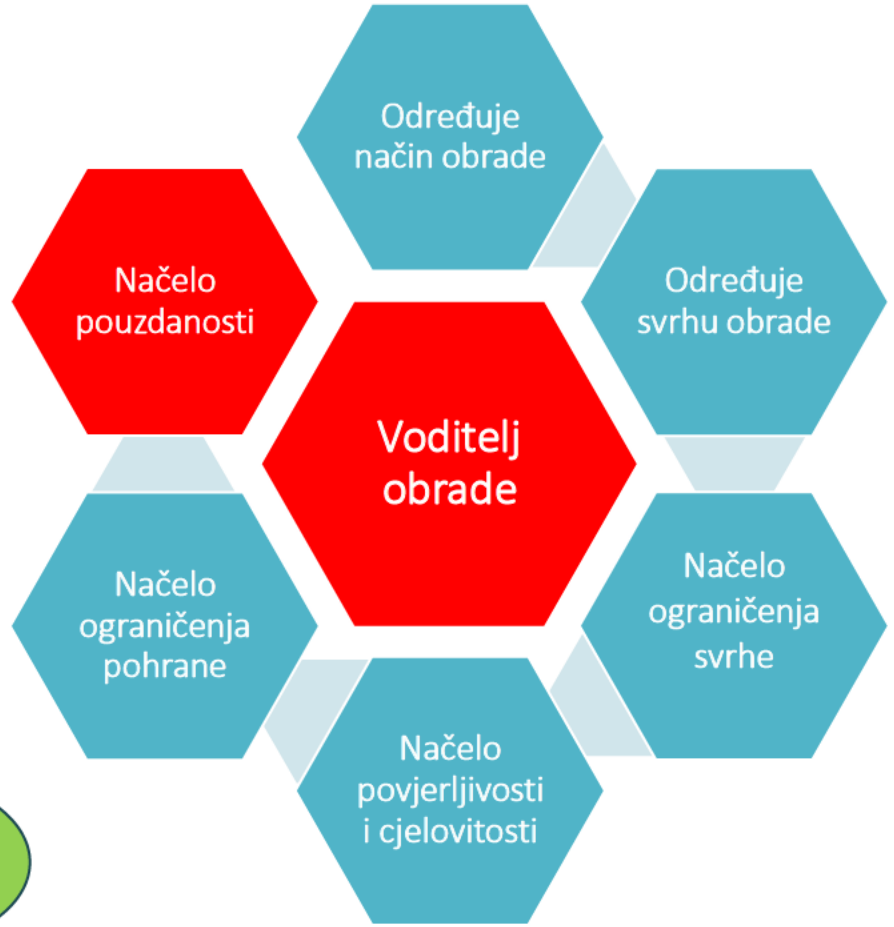
Internom politikom informacijske sigurnosti, primjenom odgovarajućih standarda odnosno kontrola koje osiguravaju dostupnost i omogućuju brz povrat podataka nakon incidenta

Gdje su naši podaci i tko je odgovoran?

Zdravstvene organizacije kao voditelji obrade:

- Nacionalne bolnice
- Klinički bolnički centri
- Opće i specijalne bolnice
- Domovi zdravlja
- Zavodi, instituti i druge ustanove
- Privatne poliklinike i klinike
- Laboratoriji
- Ordinacije liječnika pojedinaca





PODACI O VODITELJU OBRADE

ADRESA

KONTAKT PODACI

IZJAVA O POVJERLJIVOSTI

Ovom izjavom obvezujem se da ću sukladno propisima koji uređuju područje zaštite osobnih podataka, Uredbom (EU) 2016/679 europskog parlamenta i vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) i Zakonom o provedbi Opće uredbe o zaštiti podataka, čuvati povjerljivost svih osobnih podataka kojima imam pravo i ovlast pristupa, a koji se nalaze u sustavima pohrane koje vodi tijelo/društvo u kojem sam zaposlen/a te da ću iste osobne podatke koristiti isključivo u točno određenu (propisanu) svrhu.

Također se obvezujem da osobne podatke kojima imam pravo i ovlast pristupa neću dostavljati/davati na korištenje niti na bilo koji drugi način učiniti dostupnima trećim (neovlaštenim) osobama, te se obvezujem da ću povjerljivost istih osobnih podataka čuvati i nakon prestanka ovlasti pristupa osobnim podacima.

Upoznat/a sam da bilo kakvo neovlašteno raspolaganje osobnim podacima kojima imam pravo pristupa u svojem radu predstavlja povredu radne obveze.

Datum: _____

Ime i prezime: _____

Potpis: _____

naziv organizacije
adresa

U svojstvu zaposlenika *naziv organizacije* ovlaštenog za pristup i obradu podacima podataka za potrebe projekta *Naziv projekta* dajem sljedeću

IZJAVU O ČUVANJU TAJNOSTI PODATAKA

Ovom izjavom izričito izjavljujem da tajne podatke koji su dostupni kao i one koji će mi tijekom rada na projektu postati dostupni neću iznositi, niti na bilo koji drugi način učiniti dostupnim trećim osobama, osim osobama koje ovlasti *»zdravstvena organizacija«*, kao i da ću poduzeti sve mjere osiguranja zaštite tajnosti podataka i postupanja u skladu s pravilima o zaštiti osobnih podataka propisanima Općom uredbom o zaštiti podataka i Zakonom o provedbi Opće uredbe o zaštiti podataka.

Obvezujem se da ću u radu postupati s povećanom pažnjom, prema pravilima struke i običajima (pažnja dobrog stručnjaka). Ukoliko na bilo koji način dođe do otkrivanja gore navedenih podataka mojom krivnjom (namjerno ili nepažnjom), obvezujem se da ću naknaditi nastalu štetu.

Ovu izjavu dajem pod punom moralnom, radnopravnom, materijalnom i kaznenom odgovornošću.

Ova Izjava se daje isključivo u svrhu zaštite *naziv organizacije* od neovlaštenog raspolaganja tajnim podacima te se u druge svrhe ne može koristiti.

mjesto i datum

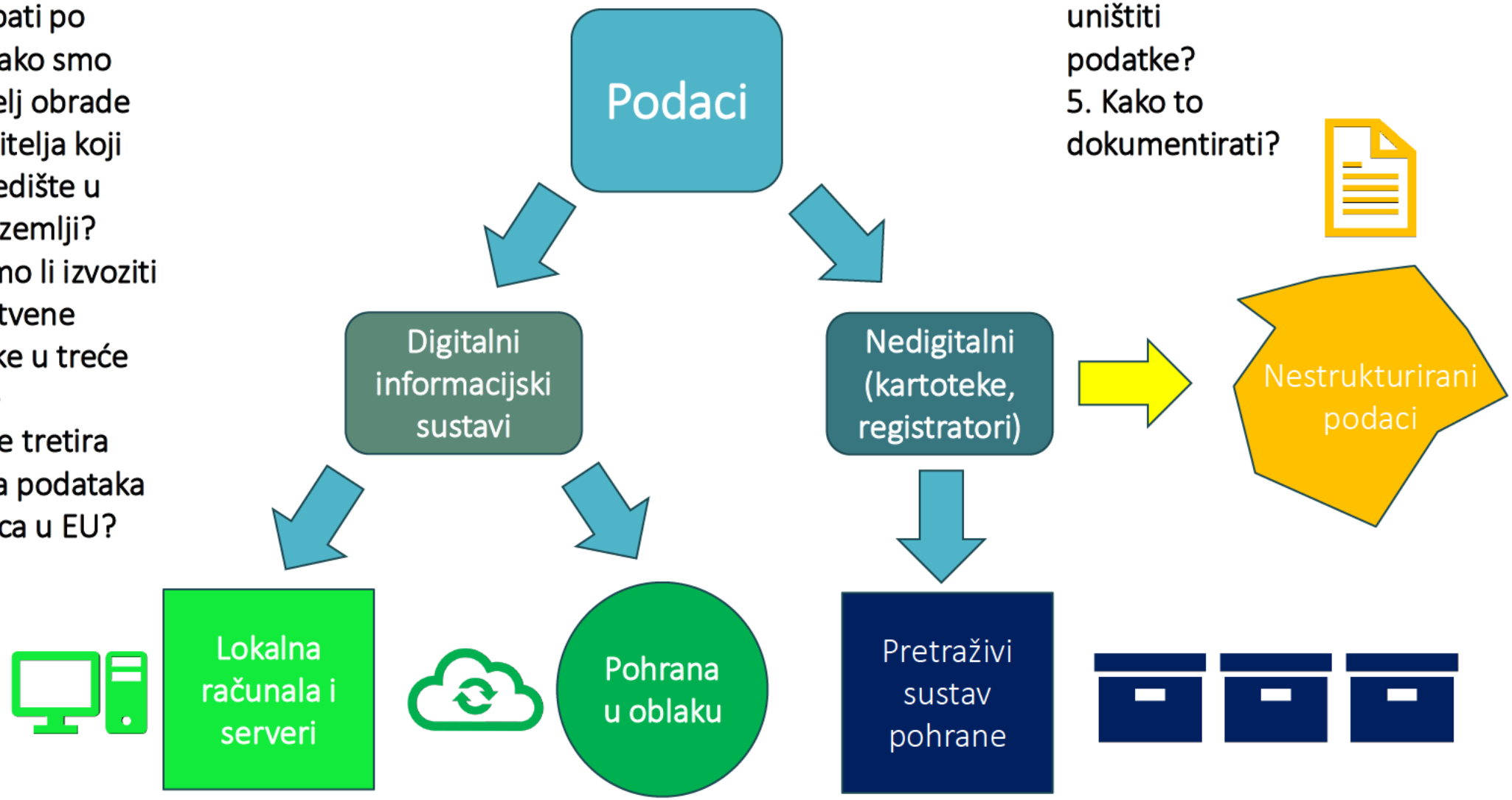
Ovu Izjavu sam u potpunosti pročitao/pročitala te ju u znak suglasnosti potpisujem.

potpis

ime i prezime

Gdje su naši podaci

1. Jesmo li obvezni postupati po OUZP ako smo izvršitelj obrade za voditelja koji ima sjedište u trećoj zemlji?
2. Smijemo li izvoziti zdravstvene podatke u treće zemlje
3. Kako se tretira obrada podataka stranaca u EU?



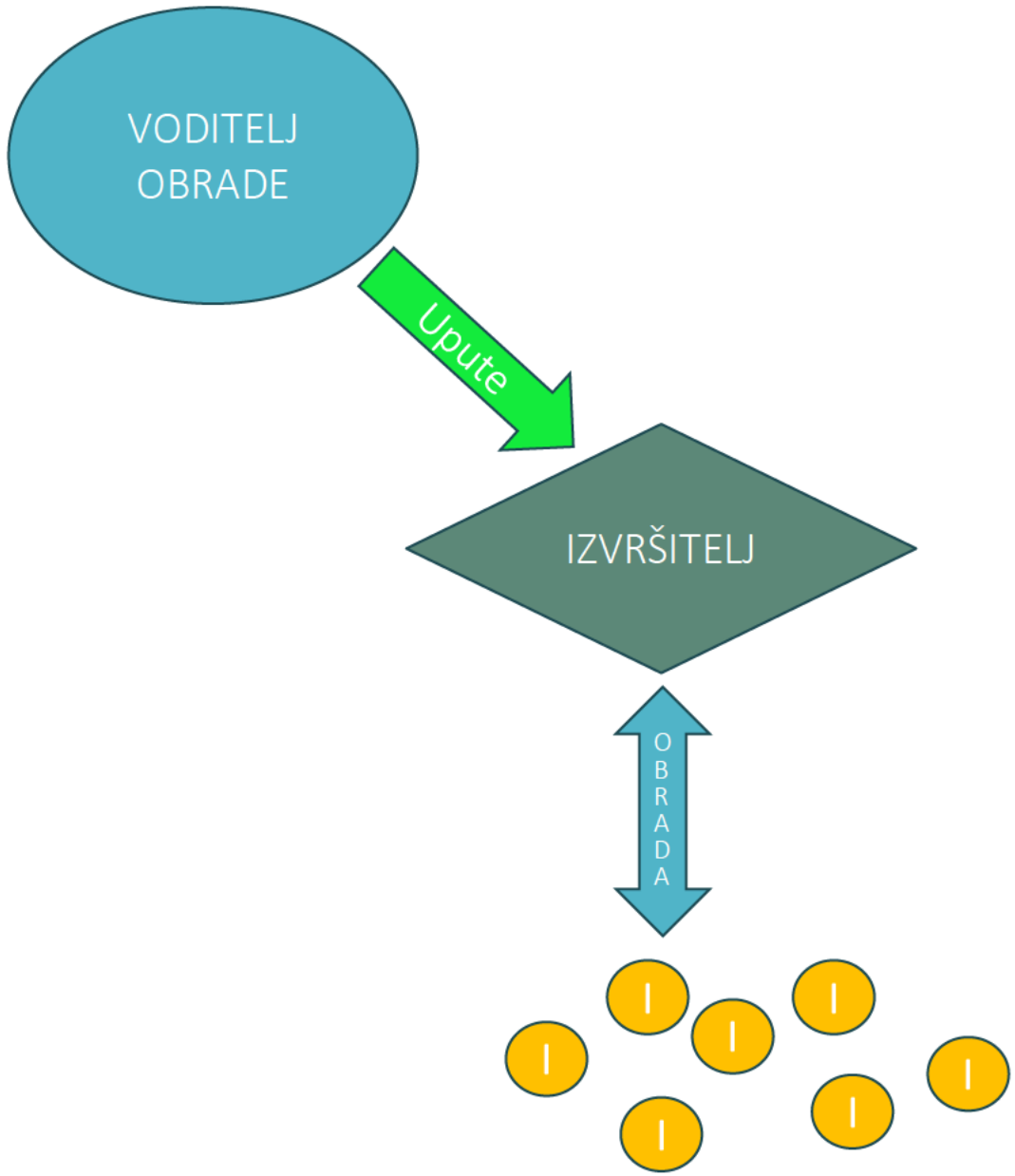
4. Kako sigurno uništiti podatke?
5. Kako to dokumentirati?

Odnos voditelja obrade i izvršitelja

Obrada osobnih podataka je svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima

Voditelj obrade - fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka

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



Voditelj ili izvršitelj – kriteriji prepoznavanja uloge

IZVRŠITELJ

Obrađujete osobne podatke za potrebe druge strane i u skladu s njezinim dokumentiranim uputama - nemate vlastitu svrhu obrade

Druga strana nadzire vaše aktivnosti obrade kako bi osigurala da se pridržavate uputa i uvjeta ugovora

U obradi ne slijedi vlastitu svrhu osim vlastitog poslovnog interesa za pružanje usluga

Angažirani ste za provođenje određenih aktivnosti obrade od strane nekoga tko je zauzvrat angažiran za obradu podataka u ime druge strane i prema dokumentiranim uputama te strane (vi ste podizvršitelj)

VODITELJ

- Imate interes u obradi (osim pukog plaćanja usluga primljenih od drugog voditelja obrade)
- Donosite odluke o ispitanicima kao dio ili kao rezultat obrade (npr. subjekti podataka su vaši zaposlenici)
- Aktivnosti obrade mogu se smatrati prirodno povezanima s ulogom ili aktivnostima vaše organizacije (npr. zbog tradicionalnih uloga ili profesionalne stručnosti) što uključuje odgovornosti sa stajališta zaštite podataka
- Obrada se odnosi na vaš odnos s ispitanicima kao što su zaposlenici, klijenti, članovi itd.
- Imate potpunu autonomiju u odlučivanju o načinu obrade osobnih podataka
- Povjerili ste obradu osobnih podataka vanjskoj organizaciji da obrađuje osobne podatke u vaše ime

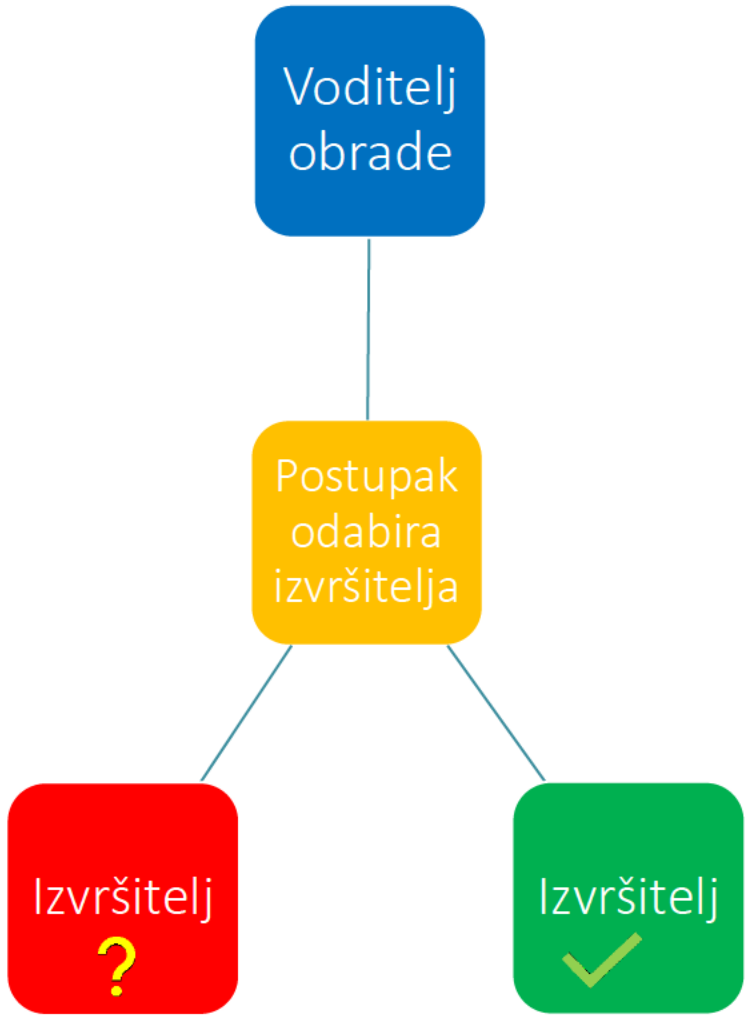
Odnos voditelja obrade i izvršitelja

Voditelj obrade je odgovoran za definiranje tehničkih i organizacijskih mjera.

- **Što ako ih voditelj obrade ne definira – na koji način ga izvršitelj obrade može upozoriti na njegovu obvezu?**

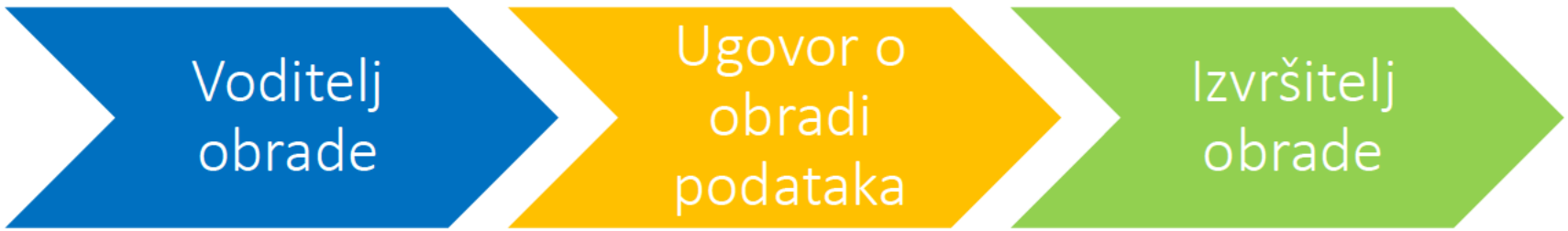
  Voditelj obrade smije koristiti samo izvršitelje koji daju dostatna jamstva za provedbu odgovarajućih tehničkih i organizacijskih mjera kako bi se osiguralo da je obrada u skladu sa zahtjevima OUZP.

  - *Stručno znanje izvršitelja obrade (na primjer, tehnička stručnost u sigurnosnim mjerama i povredama podataka)*
  - *Pouzdanost izvršitelja i njegovi resursi*
  - *Pridržavanje izvršitelja obrade odobrenog kodeksa ponašanja ili mehanizma certifikacije*



Odnos voditelja obrade i izvršitelja

- **Što ako ih voditelj obrade ne definira – na koji način ga izvršitelj obrade može upozoriti na njegovu obvezu?**
- *Svaka obrada osobnih podataka od strane izvršitelja obrade treba biti uređena ugovorom ili drugim pravnim aktom koji mora biti u pisanom obliku, uključujući i u elektroničkom obliku, i biti obvezujući.*
- *OUZP navodi elemente koji nužno trebaju biti navedeni u ugovoru o obradi.*
- *Ugovor o obradi ne bi trebao samo ponovno navesti odredbe OUZP **nego bi trebao uključivati specifičnije, konkretnije informacije o tome kako će zahtjevi biti ispunjeni** i koja je razina sigurnosti potrebna za obradu osobnih podataka koja je predmet ugovora o obradi.*



Obrada

- Umjesto „zbirki osobnih podataka” OUZP uvodi pojam **obrade**
- **Obrada osobnog podatka** je svaki **postupak** ili skup postupaka koji se obavljaju **na osobnim podacima** ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima…**u neku svrhu**.
- Može biti: prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje
- Obrade se razlikuju prema tome koji se podaci obrađuju, na kojoj pravnoj osnovi, u koju svrhu, gdje se nalaze, kome se otkrivaju ili prenose, koliko se dugo čuvaju, koliki je rizik za prava ispitanika od povrede, tko sudjeluje u obradi i u kojoj ulozi, koje tehničke i organizacijske mjere treba primijeniti da se smanji rizik od povrede
- **Svaka obrada je ograničenje prava na zaštitu osobnih podataka i ispitanikove privatnosti!**

Povreda osobnih podatka

- Svaka obrada osobnih podataka je ograničenje prava na zaštitu podataka, temeljnog prava prema EU Povelji o temeljnim pravima
- Ograničenja temeljnog prava propisana zakonom, a povrede povlače kazne
- Povreda osobnih podataka – povreda sigurnosti (cjelovitosti, i povjerljivosti – a kad padne npr. CEZIH i dostupnosti)
    - CIA Confidentiality Integrity Availability
- Pravila OUZP – spriječiti povredu ili umanjiti njen utjecaj (štetu)
- Tehničke mjere
- Organizacijske mjere
- Prisilne i ugovorne obveze
- Sektorski propisi poput Zakona o podacima i informacijama u zdravstvu – prekršajne odredbe

Prikaz slučaja (1)

Poliklinika ABC Zdravlje koristi komercijalno dostupni softver u svrhu obrade podataka nužne za pružanje zdravstvenih usluga.

Kako nema svojih zaposlenika s potrebnim kvalifikacijama, poliklinika zapošljava vanjskog informatičkog stručnjaka iz tvrtke XYZ d.o.o. da popravi grešku u softveru koji poliklinika koristi za unos podataka u zakonom propisane sustave javnog zdravstva.

IT-konzultant nije angažiran za obradu osobnih podataka, a poliklinika ABC utvrđuje da će svaki pristup osobnim podacima biti isključivo slučajan i stoga vrlo ograničen u praksi.

Poliklinika ABC stoga zaključuje da informatički stručnjak nije izvršitelj obrade (niti voditelj obrade sam po sebi) i da će tvrtka XYZ poduzeti odgovarajuće mjere u skladu s člankom 32. GDPR-a kako bi spriječila IT-konzultanta u obradi osobnih podataka u neovlašten način.

Prikaz slučaja (2)

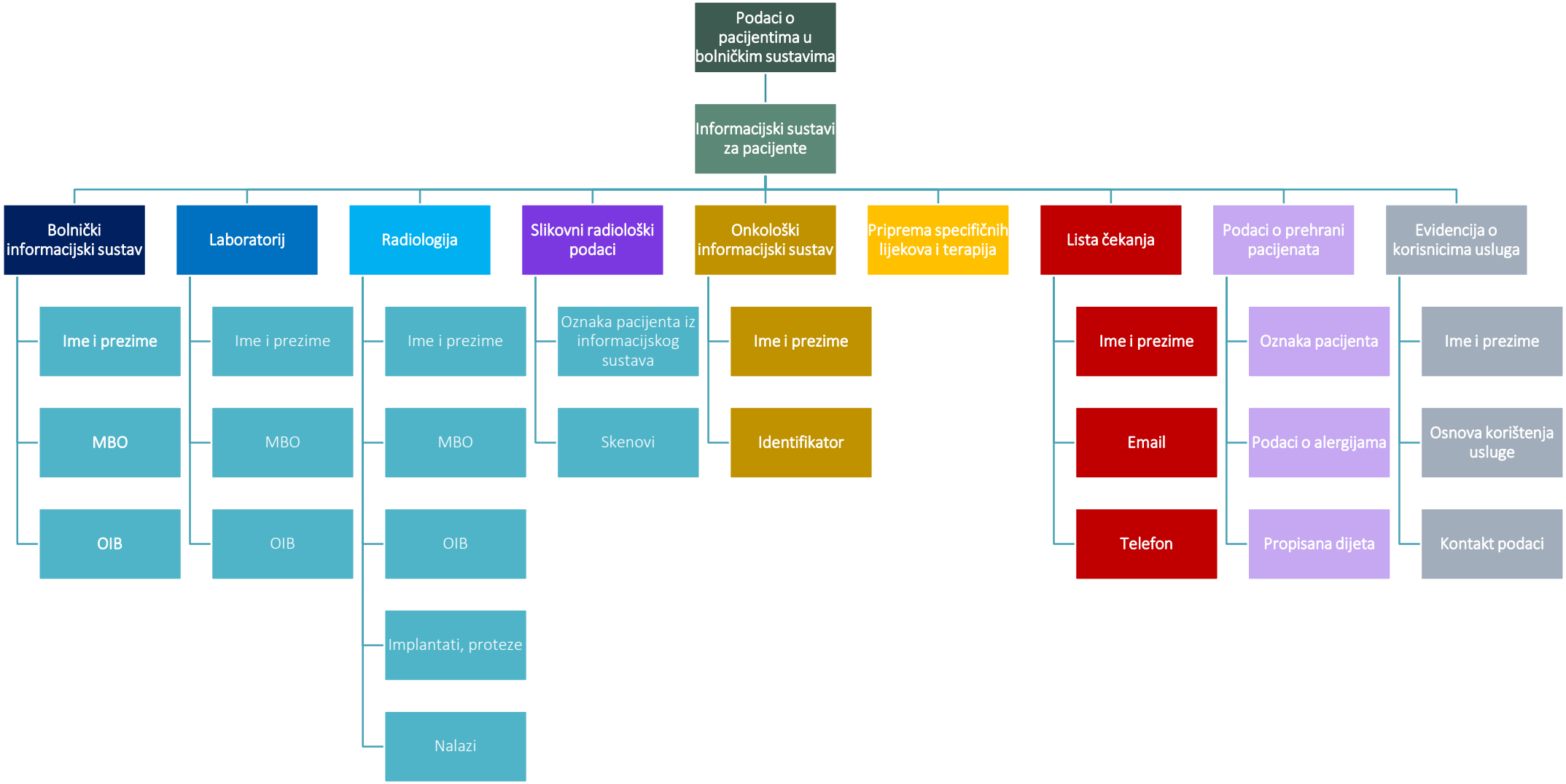
Poliklinika ABC Zdravlje i specijalizirana zdravstvena ustanova za rehabilitaciju pacijenata s bolestima koštanog sustava pripremaju zdravstveni program prevencije i rehabilitacije za pacijente s ozljedama kralježnice.

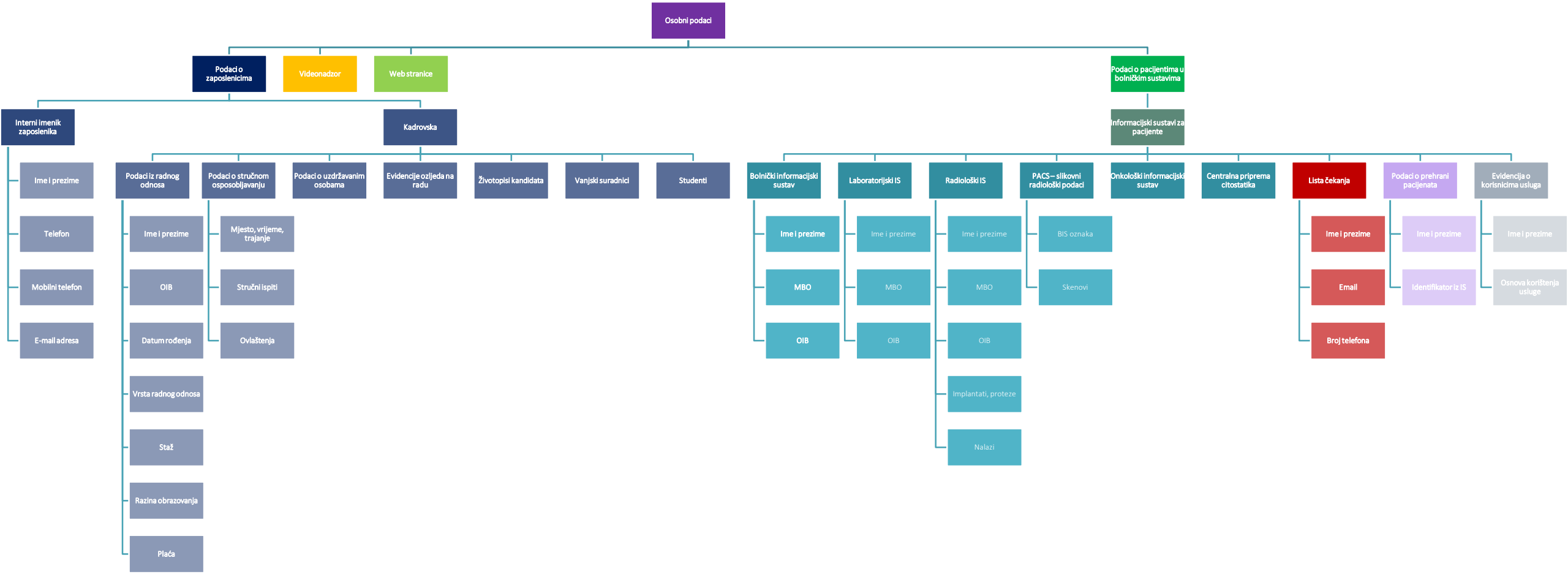
Svoje su odnose uredile ugovorom prema kojem su dogovorile zajedničke aktivnosti i raspodijelile obveze i odgovornosti prema korisnicima usluga kako i međusobno. Također su u svrhu lakšeg organizacijskog praćenja dogovorile angažman društva IT Support d.o.o. radi izrade specijalizirane web stranice koju će održavati zaposlenici Poliklinike.

Korisnici usluge – pacijenti s ozljedama ili kroničnim bolestima kralježnice prijavljuju se na web stranice programa i ostavljaju svoje kontakt i druge osobne podatke. Prema dogovoru, potencijalne upite i zahtjeve ispitanika rješavat će službenik za zaštitu podataka specijalizirane zdravstvene ustanove.

Kako biste karakterizirali, prema OUZP, odnos ovih organizacija u pogledu predloženog programa iz perspektive zaštite podataka?

Podaci unutar zdravstvene organizacije – samo zdravstvene usluge




Osobni podaci
Podaci o zaposlenicima
Videonadzor
Web stranice
Podaci o pacijentima u bolničkim sustavima
Interni imenik zaposlenika
Kadrovska
Informacijski sustavi za pacijente
Ime i prezime
Telefon
Mobilni telefon
E-mail adresa
Podaci iz radnog odnosa
Podaci o stručnom osposobljavanju
Podaci o uzdržavanim osobama
Evidencije ozljeda na radu
Životopisi kandidata
Vanjski suradnici
Studenti
Ime i prezime
OIB
Datum rođenja
Vrsta radnog odnosa
Staž
Razina obrazovanja
Plaća
Mjesto, vrijeme, trajanje
Stručni ispiti
Ovlaštenja
Bolnički informacijski sustav
Laboratorijski IS
Radiološki IS
PACS – slikovni radiološki podaci
Onkološki informacijski sustav
Centralna priprema citostatika
Lista čekanja
Podaci o prehrani pacijenata
Evidencija o korisnicima usluga
Ime i prezime
MBO
OIB
Ime i prezime
MBO
OIB
Ime i prezime
MBO
OIB
Implantati, proteze
Nalazi
BIS oznaka
Skenovi
Ime i prezime
Email
Broj telefona
Ime i prezime
Identifikator iz IS
Ime i prezime
Osnova korištenja usluge

Tipične obrade u zdravstvu

- Obrade podataka u primarnim, sekundarnim i tercijarnim javnim ustanovama
- Obrade podataka u privatnim zdravstvenim klinikama
- Obrade podataka u ljekarnama
- Obrade u kontekstu zdravstvenog osiguranja
- Obrada osnovnih podataka o pacijentima u **informacijskom sustavu** zdravstvene organizacije

  - ime, prezime, MBO, kontakt podaci, identifikator u sustavu obrade

  - povijest bolesti, pružene i tražene zdravstvene usluge
- Podaci prikupljeni u okviru specifičnih pretraga, smješteni u integrirani informacijski sustav ili u **posebne informacijske sustave** - laboratorijski sustavi, radiološki sustavi

  - identifikatori iz integriranih sustava, podaci prikupljeni pretragama
- **Podaci iz radnog odnosa i povezanih obrada** o zaposlenicima
- Podaci o dobavljačima, suradnicima, studentskoj praksi
- Prijenosi podataka temeljem nacionalnih i europskih propisa
- Prijenos podataka državnim zavodima, ministarstvu, europskim institucijama
- Referentni centri za specifične bolesti
- Istraživački registri i baze podataka znanstvenih projekata
- Lokalne obrade

Obrade u zdravstvenim ustanovama i privatnim klinikama

- Pružanje zdravstvenih usluga
  - Upis/prijem pacijenata
  - Sistematski pregledi
  - Operativna i postoperativna skrb
  - Laboratorijska obrada
  - Radiološka obrada – CT, MRI, RTG, moderniji ultrazvuk i drugi uređaji
  - Spirometrija
  - Obrade putem uređaja za vizualno snimanje
- Registri NAJS i CEZIH
- E-Karton
- Telemedicina i m-zdravstvo
- Edukacija zaposlenika
- Statusne, radno-pravne i socijalno-mirovinske obrade
- Zaštita ljudi i imovine
- Istraživanja i druge upotrebe
- Arhivske obrade

CEZIH – čl. 27. i 28. Zakona o podacima i informacijama u zdravstvu

CEZIH = Centralni informacijski sustav zdravstva Republike Hrvatske

- CEZIH se sastoji od središnjeg informacijskog sustava te informacijskih podsustava ovlaštenih pružatelja zdravstvene zaštite u Republici Hrvatskoj.
- Svrha CEZIH-a:
- podrška u funkcioniranju javnih zdravstvenih procesa,
- provedbi posebnih programa zdravstvene skrbi
- povezivanju drugih informacijskih sustava u zdravstvu

- HZZO je ovlašten putem CEZIH-a za izdavanje digitalnih certifikata za korisnike, podsustave i aplikacije zdravstvenog sustava Republike Hrvatske.
- Razmjena zdravstvenih podataka u CEZIH-u obavlja se automatiziranim sredstvima putem zaštićenog komunikacijskog kanala uz sigurnosne protokole između informacijskih sustava.
- Svi postupci obrade zdravstvenih i drugih osobnih podataka osiguravaju zaštitu osobnih podataka u CEZIH-u u skladu s propisima koji uređuju zaštitu osobnih podataka

Pitanja:

1. Tko je voditelj obrade pri upotrebi CEZIH sustava?
2. Je li to jedini voditelj obrade ili ih ima više?
3. Postoji li neki izvršitelj – ili više njih?
4. Tko su primatelji podataka iz CEZIH?
5. Je li CEZIH prošao procjenu učinka i trebaju li svi voditelji obrade koji koriste CEZIH provesti vlastitu DPIA?
6. Što se dogodi kad CEZIH padne?
7. Koji su rizici prilikom obrade putem CEZIH iz perspektive korisnika te usluge?
8. Mogu li / smiju li aplikacije koje se spajaju na CEZIH lokalno pohranjivati podatke?

Rizici upotrebe web aplikacija

Većina sustava koje Ministarstvo zdravstva, HZZO i HZJZ koristi, a čije je korištenje Zakonom o podacima i informacijama u zdravstvu obvezno voditeljima obrade koji pružaju zdravstvene usluge, zasnovani su na hibridnoj ili cloud arhitekturi.

Kod takvih aplikacija postoje brojni rizici, kako na strani ustanove koja je zadužena ustrojiti i voditi sustav, tako i na strani klijenata – sustava na strani voditelja obrade odnosno zdravstvenih ustanova

Najčešći rizici* su:

1. Neispravne kontrole pristupa – aplikacija podešena da ograničava pristup korisnicima sukladno dozvolama i kategorijama pristupa ne funkcionira i omogućuje korisniku niske razine ovlaštenja pristup podacima izvan ovlaštenja

2. Greške u enkripciji – ostavljaju osjetljive podatke bez zaštite i omogućuju krađu identiteta

3. *Injection* ranjivosti ili napadi – napadač pristupa aplikaciji, ali umjesto korisničkih podataka unosi posebno osmišljen kod koji mu omogućava pristup sustavu i podacima mimo ovlaštenja

4. Nesiguran dizajn aplikacije – različite ranjivosti koje omogućavaju napade itd.

CEZIH

Korisnici CEZIH-a su:

- ministarstvo nadležno za zdravstvo,
- HZZO i drugi zdravstveni zavodi
- svi pružatelji zdravstvene zaštite u Republici Hrvatskoj
- druge ovlaštene pravne i fizičke osobe.

Korisnici CEZIH-a obvezni su odrediti ovlaštene osobe koji koriste CEZIH i koji su obvezni pridržavati se odredaba ovoga Zakona i posebnih propisa koji uređuju zaštitu osobnih podataka.

1. odrediti ovlaštene osobe – **uvijek koristiti vlastite autentikacijske kartice**
2. kako provjeravamo koristi li ovlaštena osoba CEZIH odnosno aplikacije na CEZIHU – dakle sudjeluje u aktivnosti obrade upravo osoba čija je kartica?
3. razlikuje li CEZIH kategorije pristupa – koje podatke ovlašteni korisnik vidi i jesu li ti podaci nužni za obrade za koje je registriran u sustavu
4. primjer: može li liječnik opće medicine dobiti uvid u podatke drugog liječnika. Može li liječnik specijalist? Čime se treba urediti podjela prava pristupa (planira se spajanje s nacionalnom infrastrukturom, ovlastima koje mogu podijeliti i ispitanici, građani, prilikom odabira izabranih liječnika)

Pitanja

Obzirom na troškove aplikacija certificiranih za korištenje sustava CEZIH, kao i na rizik od nedostupnosti, smijemo li za uspostavu i pružanje zdravstvenih usluga koristiti za razmjenu podataka neki drugi sustav, a ne CEZIH?

Čl. 28 Zakona: Svi pružatelji zdravstvene zaštite u Republici Hrvatskoj obvezni su razmjenjivati zdravstvene podatke putem CEZIH-a.

Tko je voditelj, a tko izvršitelj pri korištenju CEZIH-a?

Ovisno o obradi, svi korisnici sustava na bilo kojoj zakonom uređenoj razini (primarnoj, sekundarnoj ili tercijarnoj) poput ordinacija, općih bolnica, ljekarni, privatnih klinika i kliničkih bolničkih centara su u pogledu svojih usluga u poziciji voditelja – CEZIH je sustav koji povezuje zdravstvene organizacije kao infrastruktura – kao što su i HZZO, HZJO i HZHM.

Izvršitelj je natječajem odabrano i ugovorom obvezano trgovačko društvo koje pruža usluge razvoja i održavanja CEZIH.

Koji zdravstveni sustavi mogu razmjenjivati podatke s CEZIH?

Prema Zakonu, samo proizvođači aplikacija koje su prošle certifikaciju

http://www.cezih.hr/certificirani_proizvodjaci_aplikacija.html

Broj javno dostupnih DPIA za certificirane aplikacije:0

NAJS – nacionalni javnozdravstveni informacijski sustav

Ustrojen pri HZJZ - Hrvatski zavod za javno zdravstvo

Nacionalni javnozdravstveni informacijski sustav vodi HZJZ i mogu mu pristupiti:

- ministarstvo nadležno za zdravstvo
- županijski zavodi za javno zdravstvo
- druge ovlaštene pravne i fizičke osobe

Svrha NAJS-a je upravljanje javnozdravstvenim podacima i informacijama između svih obveznika vođenja evidencija u području zdravstva

NAJS se koristi u postupcima obrade i arhiviranja zdravstvenih podataka i informacija koji se koriste za izradu javnozdravstvenih pokazatelja, u javnozdravstvene, upravljačke, statističke i znanstveno-istraživačke svrhe radi proučavanja i praćenja zdravlja stanovništva, pružanja zdravstvene zaštite, upravljanja zdravstvenim resursima, ranog prepoznavanja epidemija, procjene zdravstvenih intervencija i ostvarivanja programa za poboljšanjem zdravlja stanovništva, vođenja zdravstvene statistike i ispunjavanja drugih javnozdravstvenih potreba.

Podaci u registrima i evidencijama u području zdravstva u NAJS-u čuvaju se trajno

Pitanja – slično kao i kod CEZIH:

1. Tko je voditelj obrade pri upotrebi NAJS sustava?
2. Je li to jedini voditelj obrade ili ih ima više?
3. Postoji li neki izvršitelj – ili više njih?
4. Tko su primatelji podataka iz NAJS?
5. Je li NAJS prošao procjenu učinka?
6. Trebaju li svi voditelji obrade koji koriste NAJS provesti vlastitu DPIA?

NAJS – primjeri javnozdravstvenih registara

Nacionalni javnozdravstveni informacijski sustav organizirani je sustav informacijskih usluga Hrvatskog zavoda za javno zdravstvo kojeg koriste i druge ustanove.
Sustav omogućuje upravljanje javnozdravstvenim informacijama i procesima za bilježenje, prihvat, korištenje i arhiviranje zdravstvenih podataka.

NAJS je skup informacijskih usluga i procesa koji se sporazumno dijele sa suradnim ustanovama, i to na način da omogućuju:

- vođenje zdravstvenih evidencija/registara
- kontrolu velikih procesa u zdravstvu
- procjenu zdravstvenog stanja populacije i strateško planiranje
- rano prepoznavanje i odgovor na akutne pojave
- nadzor nad kroničnim bolestima
- usluge građanstvu i zdravstvenim stručnjacima
- nadzor nad kvalitetom zdravstvene zaštite
- druge napredne usluge i procese

Fizički je smješten na državnoj informacijskoj infrastrukturi Centra dijeljenih usluga Republike Hrvatske, s pričuvnom pohranom podataka na udaljenoj lokaciji unutar državnih granica i s dodatnom replikacijom na lokaciji Zavoda.

NAJS obuhvaća glavne registre i zdravstvene evidencije u Zavodu organiziranih poslovnih domena koje se kontinuirano proširuju i dodaju.

Registri/obrade koje provodi NAJS

Domena zaraznih bolesti:

Sustav prijavljivanja zaraznih bolesti u RH, registar za legionellu, Registar TBC, Registar nuspojava cijepljenja, Registar HIV/AIDS itd.

Domena kroničnih nezaraznih bolesti i stanja:

Registar osoba s invaliditetom, registar za rak, registar za dijabetes, registar osoba liječenih od bolesti ovisnosti itd.

Domena bolnice: Evidencija hospitalizacija, rehabilitacija i dnevnih bolnica, registar prekida trudnoće, registar poroda, registar psihoza

Domena uzroka smrti:

Baza uzroka smrti, registar izvršenih samoubojstava

Nacionalni registar pružatelja zdravstvene zaštite

1. Što se dogodi kad NAJS padne?
2. Tko prema odredbama Zakona o podacima i informacijama u zdravstvu odgovara za povrede podataka u NAJS?
3. Mogu li / smiju li aplikacije koje se spajaju na NAJS lokalno pohranjivati podatke?

E-karton

Nakon šest godina probnog rada pušten u rad 2022.

Trebao bi smanjiti administrativni dio posla i omogućiti liječnicima efikasniju organizaciju vremena, jer se putem eKartona otpusna pisma i specijalistički nalazi pacijenata mogu dijeliti između svih zdravstvenih ustanova.

Osim eRecepta, eUputnice, eNaručivanja, na Centralni zdravstveni informatički sustav (CEZIH) šalju se izvještaji nakon svakog posjeta liječniku primarne zdravstvene zaštite, koji sadrže dijagnoze, obavljene liječničke postupke, propisanu terapiju i uputnice te podatke o bolovanju.

Pravilnik o opsegu i sadržaju podataka te načinu vođenja e-kartona (NN 74/2023)

Elektronički zdravstveni zapis je skup medicinskih podataka o pacijentu koji se pohranjuju i prenose u elektroničkom obliku na zaštićeni način putem Centralnog zdravstvenog informacijskog sustava Republike Hrvatske (u daljnjem tekstu: CEZIH), a stvara ih i bilježi pružatelj zdravstvene zaštite

Portal zdravlja je portal dostupan putem sustava e-Građani, koji pacijentu omogućuje uvid u osobne i zdravstvene podatke iz e-Kartona u digitalnom obliku te korištenje zdravstvenih usluga usmjerenih prema pacijentu.

E-karton podaci

e-Karton sadrži sljedeće osobne podatke o pacijentu:

a) ime i prezime

b) spol

c) datum rođenja

d) matični broj osiguranika (u daljnjem tekstu: MBO)
e) OIB

f) prebivalište (adresa stanovanja)

g) razina i vrsta kvalifikacije

h) radno mjesto.

(2) e-Karton sadrži i sljedeće podatke:

a) broj mobilnog uređaja/telefona i adresu elektroničke pošte pacijenta

b) podatak o dobrovoljnom zdravstvenom osiguranju

c) podatak o članu obitelji pacijenta u vezi s ostvarivanjem prava iz obveznog zdravstvenog osiguranja

d) podatke o privolama/suglasnosti pacijenta za pristup podacima e-Kartona

e) podatak o izjavi pacijenta o darivanju organa, tkiva i stanica

f) ime, prezime i šifru izabranog doktora medicine/doktora medicine primarne zdravstvene zaštite

g) broj mobilnog uređaja/telefona i adresu elektroničke pošte izabranog doktora medicine/doktora medicine primarne zdravstvene zaštite.

E-karton podaci - kategorije

e-Karton sadrži **zdravstvene podatke o pacijentu:**

a) alergije i preosjetljivosti
b) cijepljenja
c) povijest bolesti
d) akutne bolesti i zdravstvena stanja
e) invazivne kirurške zahvate
f) aktivnu terapiju
g) propisane i izdane lijekove
h) medicinske proizvode ugrađene u tijelo – implantate
i) propisane i izdane medicinske proizvode.

E-karton zdravstveni podaci

(1**) Sadržaj podataka o alergiji i preosjetljivosti** pacijenta obuhvaća:
a) klinički status (aktivan, neaktivan, riješen)
b) uzrok alergije ili intolerancije (preosjetljivosti)
c) opis reakcije (osip, edem i slično)
d) datum početka i kraja.

(2) **Sadržaj podataka o cijepljenju pacijenta** obuhvaća:
a) datum cijepljenja
b) dozu u slijedu cijepljenja
c) vrstu cjepiva
d) način primjene
e) šifru cjepiva
f) zaštićeno ime cjepiva
g) naziv proizvođača
h) seriju cjepiva i LOT (serijski broj)
i) nuspojave.

(3) **Sadržaj podataka o povijesti bolesti** obuhvaća:
a) dijagnozu prema Međunarodnoj klasifikaciji bolesti
b) datum utvrđivanja bolesti
c) status bolesti.

(4) **Sadržaj podataka o akutnim bolestima i zdravstvenom stanju** pacijenta obuhvaća:
a) dijagnozu prema Međunarodnoj klasifikaciji bolesti
b) datum utvrđivanja bolesti
c) status bolesti.

(5) **Sadržaj podataka o invazivnim kirurškim zahvatima** obuhvaća:
a) šifru postupka
b) datum postupka.

(6) **Sadržaj podataka o propisanim i izdanim lijekovima i aktivnoj terapiji** obuhvaća:
a) originalan naziv lijeka
b) farmaceutski oblik doze, djelatnu tvar i jačinu
c) učestalost unosa i način primjene
d) broj jedinica po unosu
e) datum, vrijeme i izdavatelja lijeka
f) trajanje liječenja
g) nuspojave.

(7) Sadržaj podataka o medicinskim proizvodima ugrađenim u tijelo (implantati) obuhvaća:
a) dijagnozu prema Međunarodnoj klasifikaciji bolesti
b) opis medicinskog proizvoda i implantata (kada dijagnoza prema Međunarodnoj klasifikaciji bolesti nije dovoljno informativna)
c) šifru vrste implantata
d) datum ugradnje.

(8**) Sadržaj podataka o propisanim i izdanim medicinskim proizvodima** obuhvaća:
a) dijagnozu prema Međunarodnoj klasifikaciji bolesti
b) naziv medicinskog proizvoda
c) datum, vrijeme i izdavatelja medicinskog proizvoda
d) šifru medicinskog proizvoda.

E-karton zdravstveni podaci II

e-Karton sadrži i sljedeće zdravstvene podatke o pacijentu:

a) pruženoj zdravstvenoj zaštiti (vrsta posjeta, ustanova, liječnik, anamneza, status, dijagnoza prema Međunarodnoj klasifikaciji bolesti, preporuka)

b) slučajevima (dijagnoza prema Međunarodnoj klasifikaciji bolesti, anamneza, status, preporuka liječnika)

c) liječenju u zdravstvenim ustanovama (nalazi, otpusna dijagnoza, komorbiditetna dijagnoza)

d) planu njege

e) mjerenju krvnog tlaka

f) tjelesnom razvoju i druge važne podatke za zdravlje djeteta

g) dentalnom statusu i liječenju

h) sistematskim pregledima

i) preventivnim pregledima

j) radnoj sposobnosti i profesionalnoj bolesti i druge važne podatke za zdravlje pacijenta

k) dan, mjesec i godinu smrti pacijenta.

E-karton zdravstveni podaci o djeci, ginekološki, dentalni podaci te utvrđivanje radne i profesionalne bolesti

(1) **Sadržaj podataka e-Kartona djeteta predškolske i školske dobi** obuhvaća:

a) težinu

b) duljinu/visinu djeteta

c) podatke o porodu i dojenju

d) prehranu

e) sistematske preglede i probir

f) prilagodbe tijekom školovanja za djecu i studente s teškoćama u razvoju i zdravstvenim teškoćama

g) savjetovališni rad

h) zdravstveni odgoj.

(2) **Sadržaj podataka e-Kartona žene obuhvaća podatke o ginekološkom statusu:**

a) ginekološku povijest bolesti

b) obiteljsku povijest bolesti

c) ultrazvučne preglede

d) status trudnoće – očekivani datum poroda i datum kontrola

e) status ranijih trudnoća – termin i ishod poroda.

(3) Za utvrđivanje **dentalnog statusa i liječenja pacijenta** sadržaj podataka obuhvaća:

a) preventivne postupke (prema dijagnostičko-terapijskom postupku)

b) KEP indeks (karijes, ekstrakcija, plomba)

c) parodontni indeks.

(4) Za utvrđivanje **radne sposobnosti i profesionalne bolesti** pacijenta sadržaj podataka obuhvaća:

a) radnu anamnezu

b) vrstu profesionalne bolesti/ozljede na radu

c) ocjenu zdravstvene sposobnosti

d) ocjenu radne sposobnosti.

E-karton podaci o invaliditetu

Sadržaj podataka e-Kartona obuhvaća i zdravstvene podatke o invaliditetu pacijenta:

a) vrstu tjelesnog ili mentalnog oštećenja

b) uzrok koji je doveo do invaliditeta

c) vrijeme nastanka invaliditeta

d) invaliditet prema Međunarodnoj klasifikaciji bolesti

e) datum i opis funkcionalne procjene

f) pravnu osnovu i status

g) potrebu za medicinskim proizvodom

h) potreba rehabilitacije

i) ostale potrebe.

Prikaz slučaja (3)

Bolnica prikuplja podatke o svojim pacijentima u bolnički informacijski sustav (elektronički zdravstveni karton). Bolničko osoblje mora imati pristup dosjeima pacijenata kako bi informiralo svoje odluke o skrbi i liječenju pacijenata te za dokumentaciju svih poduzetih dijagnostičkih radnji, njege i liječenja.

Prema zadanim postavkama, pristup je dopušten samo onim članovima medicinskog osoblja koji su dodijeljeni liječenju dotičnog pacijenta na specijalističkom odjelu kojem je ona ili on dodijeljen.

Krug osoba s pristupom kartoteci bolesnika povećava se ako su u liječenje uključeni drugi odjeli ili dijagnostičke jedinice. Nakon što je pacijent otpušten i naplata je završena, pristup je smanjen na malu skupinu zaposlenika po odjelu specijalizacije koji odgovaraju na zahtjeve za medicinske informacije ili konzultacije koje su napravili ili zatražili drugi pružatelji medicinskih usluga uz odobrenje dotičnog pacijenta.

Postoji li u pravnom okviru zdravstvenih usluga u zakonodavstvu RH posebno uređena obveza voditelja obrade – zdravstvene organizacije – da ograniči pristup podacima pacijenta i prema kojem kriteriju?

Primjeri obrada i pravne osnove

PRIJEM PACIJENATA

Prikupljanje i obrada identifikacije pacijenata i demografskih podataka. Prikupljanje povijesti bolesti, alergija i drugih relevantnih zdravstvenih informacija koje se unose u informacijski sustav bolnice.

OBRAĐUJU SE

Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, MBO, podaci o zdravstvenom osiguranju),
Kontakt podaci (adresa, srodnici ili bliske osobe, za djecu imena roditelja, skrbnika, zakonskih zastupnika, telefon, e-mail),
Podaci potrebni za postavljanje dijagnoze i postupak liječenja, uključujući i subjektivni opis trenutnog zdravstvenog stanja,

GDJE SE NALAZE

Tipično, integrirani informacijski sustav zdravstvene ustanove kao što je tzv. bolnički informacijski sustav. Sustav je sinkroniziran sa CEZIH

PRAVNA OSNOVA

6.C + 9.h
Zakon o podacima i informacijama u zdravstvu (NN 14/19)
Zakon o zdravstvenoj zaštiti ("Narodne novine", broj NN 100/18, 125/19, 147/20, 119/22, 156/22, 33/23)
Pravilnik o opsegu i sadržaju podataka te načinu vođenja e-Kartona (74/2023)

TEHNIČKE I ORGANIZACIJSKE MJERE

Kontrola pristupa sustavu, enkripcija, redovita sigurnosna pohrana, pohrana podataka na odvojenoj lokaciji

PRAVA ISPITANIKA

Obavijest o obradi, pristup, ispravak ili dopuna

Primjeri obrada i pravne osnove

PRUŽANJE REHABILITACIJSKE SKRBI
Pacijenti se primaju na odjel u svrhu pružanja tretmana rehabilitacije nakon ozljede ili operacije

OBRAĐUJU SE
Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena, podaci o zdravstvenom osiguranju),
Kontakt podaci(adresa, srodnici ili bliske osobe, za djecu imena roditelja, skrbnika, zakonskih zastupnika, telefon, e-mail),
Podaci potrebni za postavljanje dijagnoze i postupak liječenja, uključujući i subjektivni opis trenutnog zdravstvenog stanja,
Podaci zaprimljeni o pacijentu od drugih zdravstvenih ustanova, od transportne službe, od službe spašavanja,
Podaci o zdravstvenom stanju, dobiveni neposrednim pregledom i dijagnostičkim postupcima (visina, težina, broj otkucaja srca i dr.)
Podaci o zdravstvenom stanju, dobiveni instrumentalnim pregledima tijela bolesnika (zapisi EKG-a, EEG-a, EMG krivulje, RTG i ultrazvučni snimci, zapisi s posebnih uređaja za preglede, snimci površine tijela i dr.)
Definirane glavne i sekundarne dijagnoze,
Alergije na hranu, specijalni dijetni režimi

GDJE SE NALAZE
Tipično, integrirani informacijski sustav zdravstvene ustanove kao što je tzv. bolnički informacijski sustav. Sustav je sinkroniziran sa CEZIH.

PRAVNA OSNOVA
6.C + 9.h
Zakon o podacima i informacijama u zdravstvu (NN 14/19)
Zakon o zdravstvenoj zaštiti ("Narodne novine", broj NN 100/18, 125/19, 147/20, 119/22, 156/22, 33/23)
Pravilnik o opsegu i sadržaju podataka te načinu vođenja e-Kartona (74/2023)

TEHNIČKE I ORGANIZACIJSKE MJERE
Kontrola pristupa sustavu, enkripcija, redovita sigurnosna pohrana, pohrana podataka na odvojenoj lokaciji

PRAVA ISPITANIKA
Obavijest o obradi, pristup, ispravak ili dopuna

Primjeri obrada i pravne osnove

PRUŽANJE BOLNIČKE SKRBI
Pacijent se zaprima u bolnicu radi dijagnostičkih aktivnosti, zdravstvenog tretmana/provođenja terapije ili operativnog zahvata te post-operativnog oporavka

OBRAĐUJU SE
Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena, podaci o zdravstvenom osiguranju),
Kontakt podaci(adresa, srodnici ili bliske osobe, za djecu imena roditelja, skrbnika, zakonskih zastupnika, telefon, e-mail),
Podaci potrebni za postavljanje dijagnoze i postupak liječenja, uključujući i subjektivni opis trenutnog zdravstvenog stanja,
Podaci zaprimljeni o pacijentu od drugih zdravstvenih ustanova, od transportne službe, od službe spašavanja,
Podaci o zdravstvenom stanju, dobiveni neposrednim pregledom i dijagnostičkim postupcima (visina, težina, broj otkucaja srca i dr.)

GDJE SE NALAZE
integrirani informacijski sustav zdravstvene ustanove kao što je tzv. bolnički informacijski sustav, CEZIH

PRAVNA OSNOVA
6.C + 9.h
Zakon o podacima i informacijama u zdravstvu (NN 14/19)
Zakon o zdravstvenoj zaštiti ("Narodne novine", broj NN 100/18, 125/19, 147/20, 119/22, 156/22, 33/23)
Pravilnik o opsegu i sadržaju podataka te načinu vođenja e-Kartona (74/2023)

TEHNIČKE I ORGANIZACIJSKE MJERE
Kontrola pristupa sustavu, enkripcija, redovita sigurnosna pohrana, pohrana podataka na odvojenoj lokaciji

PRAVA ISPITANIKA
Obavijest o obradi, pristup, ispravak ili dopuna

Primjeri obrada i pravne osnove

DIJAGNOSTIKA PAMETNOG „NOSEĆEG" (WEARABLE) UREĐAJA ILI UPOTREBOM TZV. HOLTER UREĐAJA

U mnogim područjima medicine, podatke o funkciji organizma ili zdravstvenom stanju treba prikupljati kroz određeno vremensko razdoblje da bi se mogao prepoznati obrazac funkcije. Tradicionalno se takve preglede obavljalo kroz ostanak pacijenta u ustanovi, no razvojem tehnologije i digitalne infrastrukture sve više takvih pretraga je moguće obavljati dok pacijent normalno obavlja svakodnevne aktivnosti. Npr. u slučaju holter uređaja pacijentu se na ograničeno vrijeme prikapča uređaj koji motri rad srca, krvni tlak i druge biometrijske podatke u svrhu dijagnoze srčanih ili krvožilnih bolesti ili mana. Takvi uređaji mogu imati i druge funkcije (npr. geolokacijsku)

OBRAĐUJU SE

Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena, podaci o zdravstvenom osiguranju),
Podaci o zdravstvenom stanju, dobiveni neposrednim pregledom i dijagnostičkim postupcima (visina, težina, broj otkucaja srca i dr.)
Podaci o zdravstvenom stanju, dobiveni instrumentalnim pregledima tijela bolesnika (zapisi EKG-a, EEG-a, EMG krivulje, RTG i ultrazvučni snimci, zapisi s posebnih uređaja za preglede, snimci površine tijela i dr.),

GDJE SE NALAZE

Specijalizirani informacijski sustav bolničkog odjela, posebna aplikacija koja prikuplja podatke na računalu operatera, CEZIH

PRAVNA OSNOVA

6.C + 9.h
Zakon o podacima i informacijama u zdravstvu (NN 14/19)
Zakon o zdravstvenoj zaštiti ("Narodne novine", broj NN 100/18, 125/19, 147/20, 119/22, 156/22, 33/23)
Pravilnik o opsegu i sadržaju podataka te načinu vođenja e-Kartona (74/2023)

TEHNIČKE I ORGANIZACIJSKE MJERE

Kontrola pristupa sustavu, kontrola pristupa aplikaciji, enkripcija datoteka

PRAVA ISPITANIKA

Obavijest o obradi, pristup, ispravak ili dopuna

Primjeri obrada i pravne osnove

OBRADA PODATAKA U LABORATORIJU

Laboratorijska jedinica u okviru bolnice provodi niz aktivnosti koje se sastoje u analizi bioloških uzoraka poput uzoraka krvi, urina, sjemene tekućine, uzoraka tkiva itd.

OBRAĐUJU SE

Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena, podaci o zdravstvenom osiguranju),
Kontakt podaci(adresa, srodnici ili bliske osobe, za djecu imena roditelja, skrbnika, zakonskih zastupnika, telefon, e-mail),
Podaci potrebni za postavljanje dijagnoze i postupak liječenja, uključujući i subjektivni opis trenutnog zdravstvenog stanja
Podaci o zdravstvenom stanju dobiveni laboratorijskim pretragama bioloških uzoraka (vrijednosti tjelesnih tekućina, briseva, uzoraka tkiva, daha, genetski rezultati na razini molekularne genetike i dr.)

GDJE SE NALAZE

Laboratorijski informacijski sustav zdravstvene ustanove, CEZIH

PRAVNA OSNOVA

6.C + 9.h

TEHNIČKE I ORGANIZACIJSKE MJERE

Kontrola pristupa sustavu, kontrola pristupa aplikaciji s podacima, enkripcija pohranjenih podataka, enkripcija prijenosa podataka, osigurana izrada sigurnosne kopije, pohrana sigurnosne kopije na udaljenoj lokaciji

PRAVA ISPITANIKA

Obavijest o obradi, pristup, ispravak ili dopuna

Primjeri obrada i pravne osnove

DIJAGNOSTIKA UPOTREBOM MRI UREĐAJA
Podaci se prenose i automatski podižu na integrirani informacijski sustav bolnice, no mogu ostati pohranjeni i na samom uređaju.
Također, kompleksni uređaji mogu imati i funkcije daljinskog održavanja i upravljanja i mogu biti osjetljivi na rizike kibernetičke sigurnosti

OBRAĐUJU SE
Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena, podaci o zdravstvenom osiguranju),
Podaci o zdravstvenom stanju, dobiveni instrumentalnim pregledima tijela bolesnika (zapisi EKG-a, EEG-a, EMG krivulje, RTG i ultrazvučni snimci, zapisi s posebnih uređaja za preglede, snimci površine tijela i dr.)

GDJE SE NALAZE
Tipično, integrirani informacijski sustav zdravstvene ustanove kao što je tzv. Bolnički informacijski sustav, potencijalno u vlastitoj pohrani uređaja

PRAVNA OSNOVA
6.C + 9.h
Zakon o podacima i informacijama u zdravstvu (NN 14/19)
Zakon o zdravstvenoj zaštiti ("Narodne novine", broj NN 100/18, 125/19, 147/20, 119/22, 156/22, 33/23)
Pravilnik o opsegu i sadržaju podataka te načinu vođenja e-Kartona (74/2023)

TEHNIČKE I ORGANIZACIJSKE MJERE
Kontrola pristupa sustavu, kontrola pristupa uređaju, enkripcija pohranjenih podataka, enkripcijom zaštićen prijenos podataka,

PRAVA ISPITANIKA
Obavijest o obradi, pristup, ispravak ili dopuna

CUS – centralni upravljački sustav

- Centralni upravljački sustav za upravljanje organizacijskom strukturom zdravstvenog sustava (CUS)
- Središnje mjesto za uvid u strukturu bolnica, odjela, djelatnika, kreveta i radnih mjesta koji je povezan s FINA RegZap i Centralnim obračunom plaća (COP-om).
- Ovaj sustav omogućuje centralizirano kreiranje i distribuciju obavijesti te olakšano slanje prijema i otpusta, računa te strukturiranih otpusnih pisama preko web sučelja i web servisa.
- Iz prikupljenih podataka radi se centralizirano izvještavanje o financijskim, organizacijskim i medicinskim parametrima faktura i stanja bolnica.
- CUS također koristi CEZIH i njegovu sigurnu komunikacijsku infrastrukturu - korištenje postojeće infrastrukture pametnih kartica – isprava 2 za sigurnu razmjenu podataka.

Druge obrade koje provode zdravstvene ustanove

OBVEZE PREMA ZAKONU O RADU, ZAKONU O ZAŠTITI NA RADU

- **Evidencija podataka o radnicima**
- **Podaci o uzdržavanim članovima obitelji zaposlenih radnika**
- **Evidencija podataka o povredama na radu, kolektivnim nesrećama, opasnim pojavama, profesionalnim bolestima i bolestima u svezi s radom**
- **Evidencija podataka o liječničkim pregledima radnika**
- **Evidencija podataka o obuci za sigurnost i zdravlje na radu**
- **Evidencija podataka o članovima radničkog vijeća**
- **Evidencija podataka o članovima upravnog vijeća**
- **Evidencija podataka o korištenju radnog vremena**
- **Evidencija podataka o kandidatima za rad**
- **Evidencija podataka o provjerama zloupotrebe alkohola, droga ili drugih sredstava ovisnosti**
- **Evidencija podataka o pohvalama i prigovorima**
- **Evidencija podataka o plaćama, službenim putovanjima i ostalim mjesečnim plaćanjima**
- **Evidencija podataka o ugovorima o djelu, autorskim ugovorima i ostalim ugovorima sklopljenim s fizičkim osobama**
- **Evidencija podataka o izdanim računima**
- **Evidencija podataka o kontaktnim osobama kod poslovnih partnera**
- **Evidencija podataka o platnom prometu**
- **Evidencija podataka o obavljenom nadzoru i utvrđenom stanju**
- **Evidencija podataka o procesuiranju prekršaja iz područja zaštite na radu, zaštite od požara, zaštite okoliša**
- **Evidencija podataka o kupnji/zakupu/prodaji nekretnina**
- **Evidencija podataka o korištenju i nadzoru korištenja mobilnih telefona, automobila, zaštitne opreme i drugih sredstava danih na korištenje**
- **Evidencija podataka o obrazovanju, razvoju i obuci zaposlenih**
- **Evidencija podataka o provedbi praktične nastave**

JAVNA NABAVA

- **Evidencija podataka o postupku javne i jednostavne nabave roba, radova i usluga**

SIGURNOST I VIDEONADZOR

- **Dopusnice za kretanje i snimanje**
- **Podaci o video nadzoru**

Druge obrade

EVIDENCIJA PODATAKA O RADNICIMA

ČIJI PODACI
Zaposlenici

OBRAĐUJU SE
Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena, podaci o zdravstvenom osiguranju),
Podaci zaprimljeni o pacijentu od drugih zdravstvenih ustanova

GDJE SE NALAZE
Lokalno računalo, lokalna pohrana, centralni upravljački sustav za upravljanje organizacijskom strukturom zdravstvenog sustava

PRAVNA OSNOVA
čl. 5 i čl. 29 Zakona o radu (NN 93/14, 127/17, 98/19, 151/22, 64/23),
čl. 3 – 7 Pravilnika o sadržaju i načinu vođenja evidencije o radnicima (NN 32/2015, 97/2015, NN 73/2017),
Pravilnika o elektroničkom zapisu podataka iz područja radnih odnosa (NN 32/2015),
čl. 61 Zakona o zaštiti na radu (NN 71/14, 118/14, 154/14 , 94/18, 96/18),
čl. 4 i čl. 7, t.1 (obavezno zdravstveno osiguranje) Zakona o obveznom zdravstvenom osiguranju (NN 137/13, 98/19, 33/23),
čl. 9., čl. 116., čl. 122. Zakona o mirovinskom osiguranju (NN 157/13, 151/14, 33/15, 93/15, 120/16, 18/18, 62/18, 115/18, 102/19, 84/21, 119/22),
čl. 66. Općeg poreznog zakona (115/16, 106/18, 121/19, 32/20, 42/20, 114/22)

TEHNIČKE I ORGANIZACIJSKE MJERE
Kontrola pristupa sustavu, kontrola pristupa uređaju, enkripcija pohranjenih podataka, enkripcijom zaštićen prijenos podataka

PRAVA ISPITANIKA
Obavijest o obradi, pristup, ispravak

Druge obrade

OBRADA PODATAKA O UZDRŽAVANIM ČLANOVIMA OBITELJI ZAPOSLENIH RADNIKA

ČIJI PODACI
Podaci o djeci, supružnik, uzdržavani član

OBRAĐUJU SE
Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena, podaci o zdravstvenom osiguranju),
Podaci zaprimljeni o pacijentu od drugih zdravstvenih ustanova
GDJE SE NALAZE
Lokalno računalo, lokalna pohrana, centralni server trgovačkog društva, COP

PRAVNA OSNOVA
Čl.9-11. Zakona o obveznom zdravstvenom osiguranju (NN 137/13, 98/19,3/23)
Rokovi min:
6 godina nakon kraja radnog odnosa prema čl. 5 st. 1. Pravilnika o sadržaju i načinu vođenja evidencije o radnicima (NN 32/2015, 97/2015, NN 73/2017) i 11 godina prema čl. 10. Zakona o računovodstvu (NN 109/07, 54/13, 121/14, 78/15, 134/15);

TEHNIČKE I ORGANIZACIJSKE MJERE
Kontrola pristupa sustavu, kontrola pristupa uređaju, enkripcija pohranjenih podataka, enkripcijom zaštićen prijenos podataka,

PRAVA ISPITANIKA
Obavijest o obradi, pristup, ispravak

Druge obrade

EVIDENCIJA PODATAKA O PROVEDBI PRAKTIČNE NASTAVE

ČIJI PODACI
Polaznici

OBRAĐUJU SE
Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena),

GDJE SE NALAZE
Ljekarničko računalo, lokalna pohrana, centralni server trgovačkog društva, CEZIH

PRAVNA OSNOVA
6.C i 6.B
čl. 4 Pravilnika o sadržaju i načinu vođenja evidencije o radnicima (NN 32/2015, 97/2015, NN 73/2017),
čl. 27. Zakona o strukovnom obrazovanju (NN 30/09, 24/10, 22/13, 25/18),
čl. 6. Zakona o državnoj potpori za obrazovanje i izobrazbu (NN 109/07, 134/07, 152/08, 14/14),
Ugovora/uputnice o provedbi praktične nastave;

TEHNIČKE I ORGANIZACIJSKE MJERE
Kontrola pristupa sustavu, kontrola pristupa uređaju, enkripcija pohranjenih podataka, enkripcijom zaštićen prijenos podataka,

PRAVA ISPITANIKA
Obavijest o obradi, pristup, ispravak

Druge obrade

DALNJE OBRAZOVANJE I OBUKA ZAPOSLENIKA
Sudjelovanje zaposlenika u programima cjeloživotnog obrazovanja radi ispunjavanja radnih obveza prema ugovoru o radu

ČIJI PODACI
Polaznici

OBRAĐUJU SE
Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena),

GDJE SE NALAZE
Lokalno računalo, lokalna pohrana, centralni server trgovačkog društva, CEZIH

PRAVNA OSNOVA
6.C
čl. 36, 40, 43, 54, 55, 56, 58 i 59 (osposobljavanje za rad) Zakona o radu (NN 93/14, 127/17, 98/19, 151/22, 64/23),
čl. 3 st. 1 podst. 9. Pravilnika o sadržaju i načinu vođenja evidencije o radnicima (NN 32/2015, 97/2015, NN 73/2017),

TEHNIČKE I ORGANIZACIJSKE MJERE
Kontrola pristupa sustavu, kontrola pristupa uređaju, enkripcija pohranjenih podataka, enkripcijom zaštićen prijenos podataka,

PRAVA ISPITANIKA
Obavijest o obradi, pristup, ispravak

Vremenski rokovi čuvanja podataka

- **Zakon o liječništvu NN 121/03, 117/08**
  čl 23. – 10 godina nakon završenog liječenja
- **Zakon o dentalnoj medicini ranije: Zakon o stomatološkoj djelatnosti NN 121/03, 117/08, 120/09, 46/21**
  čl.29. – 10 godina nakon završenog liječenja
- **Pravilnik o opsegu i sadržaju podataka te načinu vođenja e-kartona NN74/2023**
  Čl.18. - trajno!
- **Radnopravni, mirovinski-socijalni propisi**
  - **čl. 5 st. 1 Pravilnika o sadržaju i načinu vođenja evidencije o radnicima** (NN 32/2015, 97/2015, NN 73/2017
  - **čl. 10. Zakona o računovodstvu (NN 109/07, 54/13, 121/14, 78/15, 134/15);**
  - **čl. 66.18. Općeg poreznog zakona**
  - čl. 225 (opći rok zastare) **Zakona o obveznim odnosima** (NN 35/2005, 41/2008, 125/2011, 78/2015 i 29/2018);
  - čl. 82 **Zakona o porezu na dodanu vrijednost** (NN 73/13, 99/13, 148/13, 153/13, 143/14, 115/16)
  - čl. 10. **Zakona o zaštiti potrošača** (NN 41/14, 110/15);
  - čl. 13. st. 2. **Prekršajnog zakona** (NN 107/07, 39/13, 157/13, 110/15, 70/17, 118/18, 114/22);
  - čl. 38. **Zakona o zaštiti novčarskih institucija** (NN 56/15)

Primjeri djelatnosti u ljekarništvu

…koje uključuju obradu podataka pacijenata:

- Izdavanje lijeka temeljem papirnatog recepta
- Izdavanje lijeka temeljem e-recepta
- Izdavanje lijeka temeljem papirnatog recepta inozemnim pacijentima koji nisu osiguranici Hrvatskog zavoda za zdravstveno osiguranje
- Izdavanje lijeka temeljem privatnog recepta
- Izdavanje narkotika temeljem recepta
- Izdavanje pomagala temeljem doznake
- Prijava nuspojava
- Prodaja otrova

Primjeri obrada i pravne osnove

IZDAVANJE LIJEKA PUTEM ELEKTRONIČKOG RECEPTA

ČIJI PODACI
Pacijenti

OBRAĐUJU SE
Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena, podaci o zdravstvenom osiguranju),
Podaci zaprimljeni o pacijentu od drugih zdravstvenih ustanova
GDJE SE NALAZE
Ljekarničko računalo, lokalna pohrana, centralni server trgovačkog društva, CEZIH

PRAVNA OSNOVA
6.C + 9.h
1. Zakon o zdravstvenoj zaštiti (NN 150/08, 71/10, 139/10, 22/11, 84/11, 154/11, 12/12, 35/12, 70/12, 144/12, 82/13, 159/13, 22/14 , 154/14, 70/16, 131/17) 2. Pravilniku o načinu propisivanja i izdavanja lijekova na recept (NN 17/09., 46/09., 4/10., 110/10., 131/10., 1/11., 16/11., 52/11., 129/13., 146/13., 45/14., 81/14., 17/15., 113/16 i 129/17) 3.Pravilnik o mjerilima za razvrstavanje lijekova te o propisivanju i izdavanju lijekova na recept NN 86/13, 90/13, 102/14, 107/15 i 72/16)

TEHNIČKE I ORGANIZACIJSKE MJERE
Kontrola pristupa sustavu, kontrola pristupa uređaju, enkripcija pohranjenih podataka, enkripcijom zaštićen prijenos podataka,

PRAVA ISPITANIKA
Obavijest o obradi, pristup

Primjeri obrada i pravne osnove

IZDAVANJE LIJEKA TEMELJEM PAPIRNATOG RECEPTA INOZEMNIM PACIJENTIMA KOJI NISU OSIGURANICI HRVATSKOG ZAVODA ZA ZDRAVSTVENO OSIGURANJE

ČIJI PODACI
Pacijenti – inozemni osiguranici

OBRAĐUJU SE
Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena, podaci o zdravstvenom osiguranju),
Podaci zaprimljeni o pacijentu od drugih zdravstvenih ustanova

GDJE SE NALAZE
Ljekarničko računalo, lokalna pohrana, centralni server trgovačkog društva, CEZIH

PRAVNA OSNOVA
6.C + 9.h
1. Zakon o zdravstvenoj zaštiti (NN 150/08, 71/10, 139/10, 22/11, 84/11, 154/11, 12/12, 35/12, 70/12, 144/12, 82/13, 159/13, 22/14 , 154/14, 70/16, 131/17)
2. Pravilniku o načinu propisivanja i izdavanja lijekova na recept (NN 17/09., 46/09., 4/10., 110/10., 131/10., 1/11., 16/11., 52/11., 129/13., 146/13., 45/14., 81/14., 17/15., 113/16 i 129/17) 3.Pravilnik o mjerilima za razvrstavanje lijekova te o propisivanju i izdavanju lijekova na recept NN 86/13, 90/13, 102/14, 107/15 i 72/16)

TEHNIČKE I ORGANIZACIJSKE MJERE
Kontrola pristupa sustavu, kontrola pristupa uređaju, enkripcija pohranjenih podataka, enkripcijom zaštićen prijenos podataka,

PRAVA ISPITANIKA
Obavijest o obradi, pristup

Primjeri obrada i pravne osnove

IZDAVANJE POMAGALA TEMELJEM DOZNAKE

ČIJI PODACI
Pacijenti/Liječnici

OBRAĐUJU SE
Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena, podaci o zdravstvenom osiguranju),
Podaci zaprimljeni o pacijentu od drugih zdravstvenih ustanova

GDJE SE NALAZE
Ljekarničko računalo, lokalna pohrana, centralni server trgovačkog društva, CEZIH

PRAVNA OSNOVA
6.C + 9.h
1. Zakon o zdravstvenoj zaštiti (NN 150/08, 71/10, 139/10, 22/11, 84/11, 154/11, 12/12, 35/12, 70/12, 144/12, 82/13, 159/13, 22/14 , 154/14, 70/16, 131/17)
2. Pravilnik o ortopedskim i drugim pomagalima (NN broj 7/12., 14/12., 23/12., 25/12., 45/12., 69/12., 85/12., 92/12. – ispravak, 119/12., 147/12., 21/13., 38/13., 93/13., 119/13., 125/13. – ispravak, 129/13., 136/13., 141/13. – ispravak, 154/13., 11/14., 12/14. – ispravak, 22/14. – ispravak, 34/14., 45/14., 54/14., 59/14., 86/14., 92/14., 119/14., 129/14., 149/14., 17/15., 29/15., 41/15., 62/15., 77/15., 86/15., 124/15., 129/15., 132/15., 139/15., 25/16., 30/16., 53/16., 94/16., 106/16., 108/16. – ispravak, 36/17., 55/17., 102/17. , 131/17. i 10/18.)

TEHNIČKE I ORGANIZACIJSKE MJERE
Kontrola pristupa sustavu, kontrola pristupa uređaju, enkripcija pohranjenih podataka, enkripcijom zaštićen prijenos podataka,

PRAVA ISPITANIKA
Obavijest o obradi, pristup

Primjeri obrada i pravne osnove

IZDAVANJE NARKOTIKA TEMELJEM RECEPTA

ČIJI PODACI
Pacijenti/Liječnici

OBRAĐUJU SE
Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena, podaci o zdravstvenom osiguranju),
Podaci zaprimljeni o pacijentu od drugih zdravstvenih ustanova

GDJE SE NALAZE
Ljekarničko računalo, lokalna pohrana, centralni server trgovačkog društva, CEZIH

PRAVNA OSNOVA
6.C + 9.h
1. Zakon o zdravstvenoj zaštiti (NN 150/08, 71/10, 139/10, 22/11, 84/11, 154/11, 12/12, 35/12, 70/12, 144/12, 82/13, 159/13, 22/14 , 154/14, 70/16, 131/17)
2. Pravilnik o ortopedskim i drugim pomagalima (NN broj 7/12., 14/12., 23/12., 25/12., 45/12., 69/12., 85/12., 92/12. – ispravak, 119/12., 147/12., 21/13., 38/13., 93/13., 119/13., 125/13. – ispravak, 129/13., 136/13., 141/13. – ispravak, 154/13., 11/14., 12/14. – ispravak, 22/14. – ispravak, 34/14., 45/14., 54/14., 59/14., 86/14., 92/14., 119/14., 129/14., 149/14., 17/15., 29/15., 41/15., 62/15., 77/15., 86/15., 124/15., 129/15., 132/15., 139/15., 25/16., 30/16., 53/16., 94/16., 106/16., 108/16. – ispravak, 36/17., 55/17., 102/17. , 131/17. i 10/18.)

TEHNIČKE I ORGANIZACIJSKE MJERE
Kontrola pristupa sustavu, kontrola pristupa uređaju, enkripcija pohranjenih podataka, enkripcijom zaštićen prijenos podataka,

PRAVA ISPITANIKA
Obavijest o obradi, pristup

Primjeri obrada i pravne osnove

PRIJAVA NUSPOJAVA

ČIJI PODACI
Djelatnici ljekarne

OBRAĐUJU SE
Osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena, podaci o zdravstvenom osiguranju),
Podaci zaprimljeni o pacijentu od drugih zdravstvenih ustanova

GDJE SE NALAZE
Ljekarničko računalo, lokalna pohrana, centralni server trgovačkog društva, CEZIH

PRAVNA OSNOVA
6.C + 9.2.i (9. st. 2. točka (i) - osiguravanje sigurnosti zdravstvene skrbi te lijekova i medicinskih proizvoda)
Pravilnik o farmakovigilanciji (NN 83/13, 145/21)

TEHNIČKE I ORGANIZACIJSKE MJERE
Kontrola pristupa sustavu, kontrola pristupa uređaju, enkripcija pohranjenih podataka, enkripcijom zaštićen prijenos podataka,

PRAVA ISPITANIKA
Obavijest o obradi, pristup

Čuvanje podataka u ljekarništvu

Prema dokumentu Hrvatske ljekarničke komore – Dobre ljekarničke prakse

Evidencija	Rokovi pohrane
Kartice rokova i defekture	3 godine
Evidencija potrošnje lijekova	3 godine
Knjiga kopije recepata	5 godina
Evidencija o prometu i kupcima otrova	5 godina
Laboratorijski dnevnik	5 godina
Dnevnik analiza	5 godina
Knjiga narkotika	10 godina

Primjeri rokova čuvanja podataka u drugim članicama Unije

Ginekološki podaci:

Do 50 godina starosti

25 godina nakon zadnjeg porođaja

Podaci o djeci i maloljetnicima

Do 25 godina života

Podaci o mentalnom zdravlju

20 godina nakon zadnjeg pregleda

Opći zdravstveni podaci

8 godina nakon posljednjeg pregleda

6 godina nakon posljednjeg pregleda itd.

10-30 godina

Prikaz slučaja (4)

Pružatelj zdravstvenih usluga (istraživač) i sveučilište (sponzor) odlučuju zajedno pokrenuti kliničko ispitivanje s istom svrhom.

Obje organizacije surađuju u izradi protokola studije (tj. svrha, metodologija/dizajn studije, podaci koje treba prikupiti, kriteriji za isključivanje/uključivanje ispitanika, ponovna uporaba baze podataka (gdje je relevantno) itd.). Oni se mogu smatrati zajedničkim voditeljima za ovo kliničko ispitivanje budući da zajednički određuju i dogovaraju istu svrhu i osnovna sredstva obrade.

Prikupljanje osobnih podataka iz medicinskog kartona pacijenta u svrhu istraživanja treba razlikovati od pohranjivanja i korištenja istih podataka u svrhu skrbi o pacijentu, za što voditelj zdravstvene zaštite ostaje voditelj.

Što je sa slučajem kad istraživač ne sudjeluje u izradi protokola?

Svrhe obrade podataka u zdravstvu

Primarna funkcija obrade

- Obrada u svrhu pružanja zdravstvenih usluga pacijentu
  - Uživo
  - Putem tele-medicine
  - Putem e-Health, m-Health i AI usluga

Sekundarna funkcija obrade

- Obrade u šire svrhe javnog zdravstva
- Planiranje, upravljanje i unapređivanje sustava javnog zdravstva
- Prevencija i kontrola zaraznih bolesti
- Sprečavanje ozbiljnih prijetnji za javno zdravstvo
- Osiguravanje visoke razine kvalitete i sigurnosti zdravstva, medicinskih proizvoda i uređaja

Tercijarna funkcija obrade

- Obrada podataka u svrhu znanstvenih i povijesnih istraživanja od strane trećih strana (ne izvornih voditelja obrade)
- Obrada od strane farmaceutske industrije
- Obrada od strane industrije medicinskih uređaja
- Obrada od strane davatelja usluga osiguranja

Tzv. sekundarna obrada

- Izraz 'sekundarna uporaba' ne nalazi se u OUZP, ali treba ga shvatiti u skladu s pojmom „daljnja obrada" podataka kako je opisano u načelu ograničenja svrhe utvrđeno u članku 5. stavku 1. točki (b) OUZP

To je obrada podataka za namjenu drugačija od one navedene u trenutku prikupljanja. Takva obrada neće biti dopuštena kada nije kompatibilna s početnom svrhom osim ako je takva daljnja obrada (između ostalog) u istraživačke svrhe i poduzima se u skladu sa zaštitnim mjerama opisanim u članku 89(1) OUZP.

Korištenje zdravstvenih podataka u skladu s funkcijama 2 i 3 bit će ili u obliku „daljnje obrade" ili se ti podaci mogu posebno prikupljati za te funkcije.

Legitimitet (pravne osnove) općenito će ovisiti o postojanju određenog nacionalnog zakonodavstva kako je predviđeno člankom 9(h), (i) ili (j)

- obrada je nužna u svrhu preventivne medicine ili medicine rada
- obrada je nužna u svrhu javnog interesa u području javnog zdravlja
- obrada je nužna u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe

Gdje takvo zakonodavstvo ne postoji - **privola**.

Pravne osnove (temelji) obrade podataka u zdravstvu

- Podaci o zdravlju su posebna kategorija osobnih podataka
- Prikupljanje i obrada podataka za primarnu funkciju treba biti zasnovana na jednoj od pravnih osnova obrade osobnih podataka u članku 6. stavku 1. OUZP kao i na jednom od temelja navedenih u članku 9. stavku 2. OUZP koji daje iznimku od opće zabrane obrade osjetljivih podataka
- U obzir dolaze privola, pravna obveza, ugovor, javni interes ili služben ovlast, dok legitimni interes i životno važni interesi ispitanika rjeđe dolaze kao pravne osnove obrada zdravstvenih podataka.
- Obzirom na posebnu kategoriju i uvjete iz čl. 9, u obzir načelno dolazi sedam od deset mogućih osnova

Pravne osnove obrade zdravstvenih podataka prema OUZP

- Životno važni interesi ispitanika
- Legitimni interes
- Javni interes ili službena ovlast
- Ugovor
- Pravna obveza
- Privola

- Ispitanik je dao izričitu privolu
- Nužna za prava ispitanika ili voditelja obrade u pogledu radnog/socijalnog prava
- arhiviranje u javnom interesu, znanstveno ili povijesno istraživanje ili statističke svrhe
- Obrada je nužna za zaštitu životno važnih interesa ispitanika
- obrada je nužna za potrebe značajnog javnog interesa
- obrada je nužna u svrhu javnog interesa u području javnog zdravlja
- obrada je nužna u svrhu preventivne medicine ili medicine rada
- Radi legitimnih aktivnosti zaklade, udruženja, neprofitnog tijela
- obrada je nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva
- obrada se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik

Odabir odgovarajuće pravne osnove

- OUZP na europskoj razini usklađuje pravila koja uređuju obradu osjetljivih podataka kao što su zdravstveni, genetski i biometrijski podaci.
- U pružanju različitih zdravstvenih usluga, države članice mogu propisati specifične uvjete koje mogu tražiti dodatna sredstva osiguranja legalne obrade podataka, osobito u slučaju transfera podataka, korištenja raznih elektroničkih sustava u prekograničnim razmjenama i slično
- Države članice mogu usvojiti vlastita, stroža pravila u pogledu nekih kategorija takvih podataka.
- RH je to učinila kroz Zakon o provedbi OUZP:

a) čl.20. Obrada genetskih podataka u kontekstu osiguranja
b) Čl.21.-24. Obrada biometrijskih podataka u pogledu radnih odnosa

Pregled utvrđenih pravnih osnova u primarnoj zdravstvenoj obradi u EU
(Obrade od strane davatelja zdravstvene usluge ispitaniku)

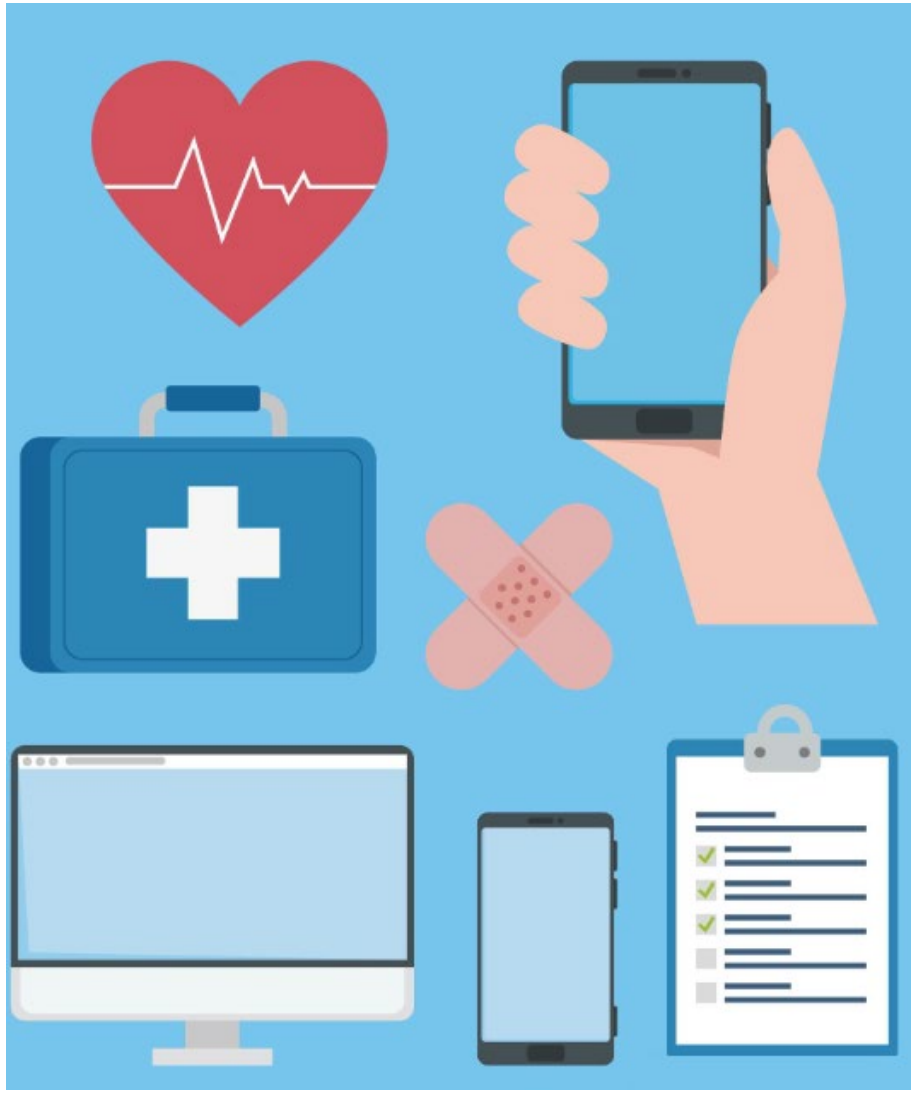
Pravna osnova obrade podataka prilikom pružanja zdravstvene usluge	Broj država članica	Države članice
6(1)(a) Privola and 9(2)(a) Izričita privola	12	BE, BG, CY, DK, DE, FR, HR, MT, AT, PT, SI, FI
6(1)(c) Pravna obveza + 9(2)(i) Javni interes u području javnog zdravlja	9	DK, EL, ES, HR, LV, MT, PT, RO, SI
6(1)(c) Pravna obveza + 9(2)(h) Pružanje zdravstvene ili socijalne pomoći	**21**	**BE, BG, CZ, DK, EL, ES, FR, HR, LV, LT, LU, HU, NL, AT, PL, PT, RO, SI, SK, FI, SE**
6(1)(e) Javni interes + 9(2)(h) Pružanje zdravstvene ili socijalne pomoći	12	BG, DK, EE, IE, EL, LV, LT, LU, MT, RO, FI, SE, [UK]
6(1)(e) Javni interes + 9(2)(i) Javni interes u području javnog zdravlja	8	BE, BG, DK, IE, EL, LV, MT, RO
6(1)(f) Legitimni interes + 9(2)(h) Pružanje zdravstvene ili socijalne pomoći	2	IE, AT
Druge osnove	6	DE, ES, IT, LV, HU, AT

Odgovarajuća pravna osnova za razmjenu podataka među davateljima zdravstvenih usluga

- Mnogi će pacijenti primati zdravstvene usluge od više od jednog davatelja zdravstvene usluge
- Sve veći broj starijih ljudi, sve veće medicinske tehničke mogućnosti i potreba za multidisciplinarnim pristupima, te sve viša uključenost pacijenata u upravljanje vlastitom skrbi, nastavit će povećavati potrebu za dijeljenje informacija.
- Sposobnost dijeljenja podataka između pružatelja skrbi i pacijenata je važan aspekt poboljšanja sigurnosti pacijenata, smanjenje broja pogrešaka koje se mogu izbjeći te poboljšati koordinaciju i kontinuitet skrbi

Razmjena podataka

- Nešto viši postotak privole – uzrok: povezanost privole za dijeljenje podataka i pristanka na liječenje u drugoj ustanovi
- I dalje je najčešći temelj kombinacija 6.1.c. + 9.2.h (ispunjenje pravne obveze davatelj zdravstvene usluge i obrada u svrhu preventivne medicine i medicine rada te pružanja zdravstvene i socijalne skrbi)
- Je li moguće da pacijent odbije daljnje dijeljenje podataka? U pet država Unije nije, u 17 jest, 5 se nije moglo izjasniti.
- Tamo gdje je moguće, često je riječ o podjeli temeljem privole, no u nekim državama članicama u kontekstu nekih (zaraznih) bolesti postoje zakonska ograničenja
- Visok rizik od povrede
- Velik utjecaj na prava i slobode ispitanika
- Velika opasnost od nastanka štete




Odvojena
Imenovana
Aktivna
PRIVOLA
Dokaziva
Dobrovoljna
Opoziva

Privola...podsjetimo se

Prilikom traženja privole trebamo provjeriti:

- Je li privola uopće najprikladnija pravna osnova?
  - Osigurati da se može povući bez negativnih posljedica
  - Nije preduvjet za pružanje usluge
- **Odvojiti zahtjev za privolom** od ostalih uvjeta pružanja usluge
- Tražiti izravan, afirmativan pristanak (da, pristajem…/dajem privolu)
- **Ne koristiti unaprijed označene kućice ili slične „defaultne" privole**
- Komunicirati na **jednostavan, izravan i jasan** način
- Specificirati **zašto** su podaci potrebni i **kako** će se koristiti
- Razdvojiti neovisne obrade i **tražiti pojedinačnu privolu za svaku obradu**
- **Identificirati voditelja obrade i treće strane**
- **Obavijestiti ispitanika o pravu na povlačenje privole**

Najčešće pogreške kod privole

Privola nije valjana ukoliko:

- Ispitanik ili voditelj obrade nemaju jasnu informaciju da je privola dana
  - *ispitanik nije obaviješten o identitetu voditelja obrade*
- Ne postoji dokumentacija o sadržaju privole i trenutku kad je privola dana
- Ispitanik nije imao slobodan izbor dati ili uskratiti privolu
- Ispitanik je privolu dao pod prijetnjom penala ili kazne za uskratu privole
- Privola je preduvjet za davanje usluge, ali obrada temeljena na privoli nije nužna za uslugu
- Privola nije odvojena od drugih uvjeta pružanja usluge
- Privola je nejasna ili previše općenita (ne odnosi se na konkretnu obradu)
- Ispitanik nije obaviješten o pravu da povuče privolu ili mu je otežano povući privolu
- Postoji jasna neravnoteža moći između voditelja obrade i ispitanika
  - *primjerice, poslodavac i zaposlenik*

Privola kao pravna osnova obrade podataka u zdravstvu

Često se (pogrešno) tvrdi da je izričita privola obvezna za obradu zdravstvenih podataka.

Razlog tome je možda to što se miješa pristanak na liječenje i pristanak na prikupljanje podataka povezanih s liječenjem.

Iako je privola važan aspekt obrade podataka u zdravstvenom okruženju, nije dominantna. Zašto?

Zato jer privola kako je definirana u članku 4. stavku 11. OUZP zahtijeva da je dana dobrovoljno i dana u kontekstu odnosa u kojem ispitanik ima ovlast uskratiti privolu bez ikakve štete za sebe.

Obzirom na to da je teško pružiti medicinsku skrb ako se ne daju potrebni podaci poput povijesti bolesti, opisa simptoma, prethodnih nalaza laboratorijskih pretraga i drugih podataka - takav je odnos teško uspostaviti

Javni interes i službene ovlasti kao pravna osnova obrade zdravstvenih podataka

Obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade

- Upravljanje listama čekanja
- Lokalna klinička revizija
- Optimizacija propisivanja i upotrebe lijekova
- Screening za različite programe ranog otkrivanja bolesti, pilot istraživanja
- Post-COVID obrade

Legitimni interes kao pravna osnova

- Legitimni interes je **najfleksibilniji** pravni temelj za obradu, **ali ne uvijek najprikladniji**
- Njegova primjena u kontekstu javnih ustanova zdravstva je **vrlo ograničena**
- Najprikladniji tamo gdje se podaci koriste na načine koji imaju **minimalan utjecaj na privatnost**
- Upotreba legitimnog interesa kao osnovi znači **dodatnu odgovornost za razmatranje i zaštitu ljudskih prava i interesa**
- Tijela javne vlasti mogu se osloniti na legitimne interese samo ako obrađuju iz legitimnog razloga koji nije obavljanje njihovih zadaća kao tijelo javne vlasti

O nužnosti i razmjernosti

Razmislite o nekoj obradi koja bi bila korisna za vašu organizaciju.

Nužnost:

Razmotrite i raspišite predloženu obradu.

Identificirajte temeljna prava i slobode ograničene obradom podataka. Odaberite opciju koja je učinkovita i najmanje nametljiva.

Razmislite o tome:

Koliko ispitanika bi bilo zahvaćeno obradom?

Koliko bi obrada trajala?

Koliko bi bili detaljni i precizni zaključci o pojedinačnim ispitanicima temeljem takve obrade?

Bi li mogli primijeniti neku mjeru koja bi ograničila invazivnost obrade (smanjiti broj ili vrstu podataka koji se obrađuju, trajanje obrade, uvesti neki oblik nadzora?)

Primjeri legitimnog interesa u zdravstvenim organizacijama

MOŽE POSTOJATI

- Otkrivanje podataka u kontekstu pripreme odgovora na tužbu
- Podizanje sigurnosti pacijenata kroz upotrebu senzora na medicinskom uređaju
- Osiguranje kvalitete usluge putem snimanja telefonskih poziva
- Komuniciranje s pacijentom e-poštom ili putem telefona (za otkazivanje termina, podsjetiti na bolnicu ili ambulantni posjet, upute kako pripremiti se za zakazani zahvat, ili obavijestiti gdje i kada prikupiti medicinsku dokumentaciju)
- Praćenje pristupa zaposlenika osjetljivim podacima kako bi se osigurala zaštita zdravstvenih podataka i sigurno korištenje IT sustava

NE MOŽE

- Korištenje key-logger softvera u kontekstu zapošljavanja u svrhu praćenja učinka
- Zadržavanje bankovnih podataka kako bi se olakšala kasnija plaćanja i optimizirale poslovne transakcije
- Psihološko testiranje kao alat za razvoj i provjeru profesionalizma zaposlenika
- Prijenos osobnih podataka drugom subjektu u marketinške svrhe
- Snimanje zaposlenika koji čini povredu u svrhu daljnjeg disciplinskog postupka

TEST RAZMJERNOSTI KOD LEGITIMNOG INTERESA

VITANOVA MEDICAL GRUPA d.d.

Ovaj predložak za procjenu legitimnih interesa osmišljen je kako bi vam pomogao da odlučite može li se legitiman interes kao pravni temelj primijeniti na Vašu obradu.

KORAK 1: TEST SVRHE

Morate procijeniti postoji li legitiman interes za obradu. Zašto želite obraditi podatke? Kakvu korist očekujete od obrade? Postoji li koristi od obrade za treću stranu?Postoji li šira javna korist za obradu? Koliko su važne prednosti koje ste identificirali? Kakav bi bio utjecaj na Vas ako ne biste mogli nastaviti s obradom? Pridržavate li se nekih posebnih pravila o zaštiti podataka koja se primjenjuju na Vašu obradu (npr. zahtjevi za profiliranje ili zakonodavstvo o e-privatnosti)?Pridržavate li se drugih relevantnih zakona? Pridržavate li se industrijskih smjernica ili kodeksa prakse?Postoje li drugi etički problemi s obradom?

VITANOVA Medical Grupa, poliklinika, lanac ljekarni i distributer medicinskih proizvoda želi podatke za kontakt sljedećih kategorija ispitanika u svrhu izravnog marketinga i pružanja ažuriranja i biltena:

Pojedinci koji su se pretplatili na ažuriranja i biltene putem web stranice (Pratitelji)

Postojeći kupci

Zdravstveni radnici (uključujući konzultante, liječnike opće prakse i njihovo tajničko osoblje) Klinika želi obrađivati ove osobne podatke kako bi slala izravni marketinški materijal, biltene i ažuriranja tim pojedincima, u cilju rasta poslovanja.

VITANOVA dobiva osobne podatke ovih kategorija ispitanika ili izravno (putem pretplate ili kupnje) ili od dviju trećih strana. VITANOVA želi obrađivati ove osobne podatke kako bi slala izravni marketinški materijal, biltene i ažuriranja tim pojedincima, u cilju rasta poslovanja i to smatra legitimnim poslovnim interesom. Jedan od proizvoda koji stavlja na tržište jesu sterilni instrumenti za jednokratnu upotrebu zdravstvenom sektoru i tvrdi da postoji šira javna korist od toga što su zdravstveni radnici svjesni VITANOVA proizvoda i njihove dostupnosti za kupnju. Ako im se ne može pružiti izravni marketinški materijal to bi ograničilo njihov pristup proizvodima VITANOVE i njihovu mogućnost pristupa informacijama o inovacijama, razvoju i novim proizvodima.

VITANOVA-ina obavijest o obradi podataka uključuje odjeljak za pratitelje na bilten i ažuriranja te odjeljak o izravnom marketingu koji jasno ukazuje na mogućnost pojedinca da se usprotivi primanju izravnog marketinga u bilo kojem trenutku i daje poveznicu koja to omogućuje pojedincu.

Osim toga, svaka poslana komunikacija koja sadrži izravni marketing uključuje poveznicu za odjavu pretplate koja pojedincu omogućuje odjavu i prekid izravnog marketinga od VITANOVA.

VITANOVA se oslanja mogućnost da fizička ili pravna osoba trgovca može upotrebljavati podatke o adresama elektroničke pošte, koje je pribavila od svojih potrošača u svrhu prodaje proizvoda i usluga, za izravnu promidžbu i prodaju isključivo vlastitih sličnih proizvoda ili usluga, uz uvjet da ti potrošači imaju jasnu i nedvojbenu mogućnost bespl naznačenu u čl. 50.2 Zakona o elektroničkim komunikacijama. VITANOVA nije upoznata s postojanjem etičkih problema koji bi utjecali na dopustivost obrade.

KORAK 2: TEST NUŽNOSTI

Morate procijeniti je li obrada nužna u svrhu koju ste utvrdili. Hoće li vam ova obrada zaista pomoći da ostvarite svoju svrhu?Je li obrada proporcionalna toj svrsi?Možete li postići istu svrhu bez obrade?Možete li istu svrhu postići obradom manje podataka ili obradom podataka na drugi očitiji ili manje nametljiv način?

Obrada osobnih podataka pratitelja, postojećih kupaca i zdravstvenih radnika omogućit će VITANOVI da plasira svoje proizvode, informira te pojedince o inovacijama i razvoju te razvija svoje poslovanje. VITANOVA smatra da je obrada razmjerna tim svrhama. Mogućnost otkazivanja pretplate dostupna je svakom pojedincu u odnosu na svaku poslanu marketinšku komunikaciju, što im omogućuje da odustanu od primanja daljnjih marketinških informacijam. te se uklanjaju s popisa za slanje e-pošte. Bez obrade osobnih podataka pratitelja, postojećih kupaca i zdravstvenih radnika na ovaj način ne postoji alternativni način slanja marketinškog materijala ovim kategorijama pojedinaca.

KORAK 3: TEST RAVNOTEŽE

Morate razmotriti utjecaj na interese i prava i slobode ispitanika i procijeniti nadjačavaju li vaše legitimne interese.

A. Priroda osobnih podataka

Radi li se o podacima posebne kategorije ili podacima o kaznenim osudama i kažnjivim djelima?Jesu li to podaci koje bi ispitanici vjerojatno smatrati posebno "privatnima"? Obrađujete li podatke o djeci ili podatke koji se odnose na druge ranjive skupine? Jesu li podaci o ispitanicima odnosni na njihovo osobno ili profesionalno svojstvo?

Ne obrađuju se podaci o posebnim kategorijama ili kaznenim djelima. Osobni podaci ne bi se smatrali privatnim, dapače, u većini slučajeva to su osobni podaci koji su javno dostupni od od upisnika zdravstvenih organizacija i drugih izvora. Osobni podaci koji se obrađuju ne odnose se na djecu ili ranjive osobe, ograničeni su na zdravstvene djelatnike i one koji rade u sektoru zdravstva.

B. Razumna očekivanja pojedinaca

Imate li postojeći odnos s pojedincem? Kakva je priroda veze i kako ste koristili podatke u prošlosti? Jeste li podatke prikupljali izravno od pojedinca? Što ste im tada rekli? Ako ste podatke dobili od treće strane, što je rečeno pojedincima o ponovnoj upotrebi od strane trećih strana u druge svrhe?Prije koliko vremena ste prikupili podatke? Postoje li od tada promjene u tehnologiji ili kontekstu koje bi mogle utjecati na očekivanja pojedinaca?Jesu li Vaša svrha i metoda razumljiva?Namjeravate li učiniti nešto novo ili inovativno? Imate li dokaza o očekivanjima - npr. od istraživanja tržišta, fokus grupa ili drugih oblika savjetovanja? Postoje li neki drugi čimbenici u određenim okolnostima koji znače da pojedinci bi ili ne bi očekivali obradu?

VITANOVA ima postojeći odnos s pratiteljima i postojećim kupcima. Svoje osobne podatke daju izravno prilikom pretplate na newsletter i ažuriranja (putem web stranice) ili kupnjom proizvoda (također putem web stranice).. Obavijest o privatnosti tvrtke VITANOVA uključuje odjeljke o obradi osobnih podataka u svrhu pružanja biltena, ažuriranja i izravnog marketinškog materijala. Ovi odjeljci pružaju informacije pojedincima o tome kako se mogu usprotiviti obradi svojih osobnih podataka u te svrhe

C. Vjerojatni učinak na pojedince

Koji su mogući učinci obrade na pojedince?Hoće li pojedinci izgubiti kontrolu nad korištenjem njihovih osobnih podataka?Koja je vjerojatnost i ozbiljnost bilo kojeg potencijalnog utjecaja?Da li će se pojedinci vjerojatno usprotiviti obradi ili će je smatrati nametljivom?Hoćete li rado objasnili obradu pojedincima?Možete li usvojiti neke zaštitne mjere kako biste utjecaj sveli na najmanju moguću mjeru?

VITANOVA ne smatra da bi obrada njihovih osobnih podataka na ovaj način mogla primjetno utjecati na prava i slobode ispitanika. Ako se žele usprotiviti obradi, VITANOVINA obavijest o obradi daje im način na koji to mogu učiniti, osim toga opcija odjave uključena je u odnosu na svaku poslanu komunikaciju. Ove metode u kombinaciji daju pojedincu mogućnost da odustane od marketinških komunikacija u bilo kojem trenutku. VITANOVA se potrudila detaljno objasniti obradu osobnih podataka pojedincima u obavijesti o privatnosti.

Hoćete li ponuditi pojedincima mogućnost prigovora?	**Da**/ Ne

ODLUČIVANJE

Ovdje upotrebljavate svoje odgovore na korake 1, 2 i 3 da biste odlučili možete li primijeniti osnovu legitimnih interesa.

Možete li se osloniti na legitiman interes kao temelj za obradu?	**Da** / Ne
Komentari?	Da / **Ne**
Test popunio:	Hrvoje Horvat
Datum:	30. rujna 2023

ŠTO JE SLJEDEĆE?

Dokumentirajte ovaj test razmjernosti i revidirajte po potrebi.
Ako je potrebno, napravite procjenu učinka na zaštitu podataka.
U svoje obavijesti/politike privatnosti uključite detalje o svojim svrhama i zakonskoj osnovi za obradu.

TEST RAZMJERNOSTI KOD LEGITIMNOG INTERESA

VITANOVA MEDICAL GRUPA d.d.

Ovaj predložak za procjenu legitimnih interesa osmišljen je kako bi vam pomogao da odlučite može li se legitiman interes kao pravni temelj primijeniti na Vašu obradu.

KORAK 1: TEST SVRHE

Morate procijeniti postoji li legitiman interes za obradu.Zašto želite obraditi podatke? Kakvu korist očekujete od obrade? Postoji li koristi od obrade za treću stranu?Postoji li šira javna korist za obradu? Koliko su važne prednosti koje ste identificirali? Kakav bi bio utjecaj na Vas ako ne biste mogli nastaviti s obradom? Pridržavate li se nekih posebnih pravila o zaštiti podataka koja se primjenjuju na Vašu obradu (npr. zahtjevi za profiliranje ili zakonodavstvo o e-privatnosti)?Pridržavate li se drugih relevantnih zakona? Pridržavate li se industrijskih smjernica ili kodeksa prakse?Postoje li drugi etički problemi s obradom?

VITANOVA Medical Grupa, poliklinika, lanac ljekarni i distributer medicinskih proizvoda želi podatke za kontakt sljedećih kategorija ispitanika u svrhu izravnog marketinga i pružanja ažuriranja i biltena:

Pojedinci koji su se pretplatili na ažuriranja i biltene putem web stranice (Pratitelji)

Postojeći kupci

Zdravstveni radnici (uključujući konzultante, liječnike opće prakse i njihovo tajničko osoblje) Klinika želi obrađivati ove osobne podatke kako bi slala izravni marketinški materijal, biltene i ažuriranja tim pojedincima, u cilju rasta poslovanja.

VITANOVA dobiva osobne podatke ovih kategorija ispitanika ili izravno (putem pretplate ili kupnje) ili od dviju trećih strana. VITANOVA želi obrađivati ove osobne podatke kako bi slala izravni marketinški materijal, biltene i ažuriranja tim pojedincima, u cilju rasta poslovanja i to smatra legitimnim poslovnim interesom. Jedan od proizvoda koji stavlja na tržište jesu sterilni instrumenti za jednokratnu upotrebu zdravstvenom sektoru i tvrdi da postoji šira javna korist od toga što su zdravstveni radnici svjesni VITANOVA proizvoda i njihove dostupnosti za kupnju. Ako im se ne može pružiti izravni marketinški materijal to bi ograničilo njihov pristup proizvodima VITANOVE i njihovu mogućnost pristupa informacijama o inovacijama, razvoju i novim proizvodima.

VITANOVA-ina obavijest o obradi podataka uključuje odjeljak za pratitelje na bilten i ažuriranja te odjeljak o izravnom marketingu koji jasno ukazuje na mogućnost pojedinca da se usprotivi primanju izravnog marketinga u bilo kojem trenutku i daje poveznicu koja to omogućuje pojedincu.

Osim toga, svaka poslana komunikacija koja sadrži izravni marketing uključuje poveznicu za odjavu pretplate koja pojedincu omogućuje odjavu i prekid izravnog marketinga od VITANOVA.

VITANOVA se oslanja mogućnost da fizička ili pravna osoba trgovca može upotrebljavati podatke o adresama elektroničke pošte, koje je pribavila od svojih potrošača u svrhu prodaje proizvoda i usluga, za izravnu promidžbu i prodaju isključivo vlastitih sličnih proizvoda ili usluga, uz uvjet da ti potrošači imaju jasnu i nedvojbenu mogućnost bespl naznačenu u čl.

50.2 Zakona o elektroničkim komunikacijama. VITANOVA nije upoznata s postojanjem etičkih problema koji bi utjecali na dopustivost obrade.

KORAK 2: TEST NUŽNOSTI

Morate procijeniti je li obrada nužna u svrhu koju ste utvrdili. Hoće li vam ova obrada zaista pomoći da ostvarite svoju svrhu?Je li obrada proporcionalna toj svrsi?Možete li postići istu svrhu bez obrade?Možete li istu svrhu postići obradom manje podataka ili obradom podataka na drugi očitiji ili manje nametljiv način?

Obrada osobnih podataka pratitelja, postojećih kupaca i zdravstvenih radnika omogućit će VITANOVI da plasira svoje proizvode, informira te pojedince o inovacijama i razvoju te razvija svoje poslovanje. VITANOVA smatra da je obrada razmjerna tim svrhama. Mogućnost otkazivanja pretplate dostupna je svakom pojedincu u odnosu na svaku poslanu marketinšku komunikaciju, što im omogućuje da odustanu od primanja daljnjih marketinških informacijam. te se uklanjaju s popisa za slanje e-pošte. Bez obrade osobnih podataka pratitelja, postojećih kupaca i zdravstvenih radnika na ovaj način ne postoji alternativni način slanja marketinškog materijala ovim kategorijama pojedinaca.

KORAK 3: TEST RAVNOTEŽE

Morate razmotriti utjecaj na interese i prava i slobode ispitanika i procijeniti nadjačavaju li vaše legitimne interese.

A. Priroda osobnih podataka

Radi li se o podacima posebne kategorije ili podacima o kaznenim osudama i kažnjivim djelima?Jesu li to podaci koje bi ispitanici vjerojatno smatrati posebno "privatnima"? Obrađujete li podatke o djeci ili podatke koji se odnose na druge ranjive skupine? Jesu li podaci o ispitanicima odnosni na njihovo osobno ili profesionalno svojstvo?

Ne obrađuju se podaci o posebnim kategorijama ili kaznenim djelima. Osobni podaci ne bi se smatrali privatnim, dapače, u većini slučajeva to su osobni podaci koji su javno dostupni od od upisnika zdravstvenih organizacija i drugih izvora. Osobni podaci koji se obrađuju ne odnose se na djecu ili ranjive osobe, ograničeni su na zdravstvene djelatnike i one koji rade u sektoru zdravstva.

B. Razumna očekivanja pojedinaca

Imate li postojeći odnos s pojedincem? Kakva je priroda veze i kako ste koristili podatke u prošlosti? Jeste li podatke prikupljali izravno od pojedinca? Što ste im tada rekli? Ako ste podatke dobili od treće strane, što je rečeno pojedincima o ponovnoj upotrebi od strane trećih strana u druge svrhe?Prije koliko vremena ste prikupili podatke? Postoje li od tada promjene u tehnologiji ili kontekstu koje bi mogle utjecati na očekivanja pojedinaca?Jesu li Vaša svrha i metoda razumljiva?Namjeravate li učiniti nešto novo ili inovativno? Imate li dokaza o očekivanjima - npr. od istraživanja tržišta, fokus grupa ili drugih oblika savjetovanja? Postoje li neki drugi čimbenici u određenim okolnostima koji znače da pojedinci bi ili ne bi očekivali obradu?

50.2 Zakona o elektroničkim komunikacijama. VITANOVA nije upoznata s postojanjem etičkih problema koji bi utjecali na dopustivost obrade.

KORAK 2: TEST NUŽNOSTI

Morate procijeniti je li obrada nužna u svrhu koju ste utvrdili. Hoće li vam ova obrada zaista pomoći da ostvarite svoju svrhu?Je li obrada proporcionalna toj svrsi?Možete li postići istu svrhu bez obrade?Možete li istu svrhu postići obradom manje podataka ili obradom podataka na drugi očitiji ili manje nametljiv način?

Obrada osobnih podataka pratitelja, postojećih kupaca i zdravstvenih radnika omogućit će VITANOVI da plasira svoje proizvode, informira te pojedince o inovacijama i razvoju te razvija svoje poslovanje. VITANOVA smatra da je obrada razmjerna tim svrhama. Mogućnost otkazivanja pretplate dostupna je svakom pojedincu u odnosu na svaku poslanu marketinšku komunikaciju, što im omogućuje da odustanu od primanja daljnjih marketinških informacijam. te se uklanjaju s popisa za slanje e-pošte. Bez obrade osobnih podataka pratitelja, postojećih kupaca i zdravstvenih radnika na ovaj način ne postoji alternativni način slanja marketinškog materijala ovim kategorijama pojedinaca.

KORAK 3: TEST RAVNOTEŽE

Morate razmotriti utjecaj na interese i prava i slobode ispitanika i procijeniti nadjačavaju li vaše legitimne interese.

A. Priroda osobnih podataka

Radi li se o podacima posebne kategorije ili podacima o kaznenim osudama i kažnjivim djelima?Jesu li to podaci koje bi ispitanici vjerojatno smatrati posebno "privatnima"? Obrađujete li podatke o djeci ili podatke koji se odnose na druge ranjive skupine? Jesu li podaci o ispitanicima odnosni na njihovo osobno ili profesionalno svojstvo?

Ne obrađuju se podaci o posebnim kategorijama ili kaznenim djelima. Osobni podaci ne bi se smatrali privatnim, dapače, u većini slučajeva to su osobni podaci koji su javno dostupni od od upisnika zdravstvenih organizacija i drugih izvora. Osobni podaci koji se obrađuju ne odnose se na djecu ili ranjive osobe, ograničeni su na zdravstvene djelatnike i one koji rade u sektoru zdravstva.

B. Razumna očekivanja pojedinaca

Imate li postojeći odnos s pojedincem? Kakva je priroda veze i kako ste koristili podatke u prošlosti? Jeste li podatke prikupljali izravno od pojedinca? Što ste im tada rekli? Ako ste podatke dobili od treće strane, što je rečeno pojedincima o ponovnoj upotrebi od strane trećih strana u druge svrhe?Prije koliko vremena ste prikupili podatke? Postoje li od tada promjene u tehnologiji ili kontekstu koje bi mogle utjecati na očekivanja pojedinaca?Jesu li Vaša svrha i metoda razumljiva?Namjeravate li učiniti nešto novo ili inovativno? Imate li dokaza o očekivanjima - npr. od istraživanja tržišta, fokus grupa ili drugih oblika savjetovanja? Postoje li neki drugi čimbenici u određenim okolnostima koji znače da pojedinci bi ili ne bi očekivali obradu?

VITANOVA ima postojeći odnos s pratiteljima i postojećim kupcima. Svoje osobne podatke daju izravno prilikom pretplate na newsletter i ažuriranja (putem web stranice) ili kupnjom proizvoda (također putem web stranice).. Obavijest o privatnosti tvrtke VITANOVA uključuje odjeljke o obradi osobnih podataka u svrhu pružanja biltena, ažuriranja i izravnog marketinškog materijala. Ovi odjeljci pružaju informacije pojedincima o tome kako se mogu usprotiviti obradi svojih osobnih podataka u te svrhe

C. Vjerojatni učinak na pojedince

Koji su mogući učinci obrade na pojedince?Hoće li pojedinci izgubiti kontrolu nad korištenjem njihovih osobnih podataka?Koja je vjerojatnost i ozbiljnost bilo kojeg potencijalnog utjecaja?Da li će se pojedinci vjerojatno usprotiviti obradi ili će je smatrati nametljivom?Hoćete li rado objasnili obradu pojedincima?Možete li usvojiti neke zaštitne mjere kako biste utjecaj sveli na najmanju moguću mjeru?

VITANOVA ne smatra da bi obrada njihovih osobnih podataka na ovaj način mogla primjetno utjecati na prava i slobode ispitanika. Ako se žele usprotiviti obradi, VITANOVINA obavijest o obradi daje im način na koji to mogu učiniti, osim toga opcija odjave uključena je u odnosu na svaku poslanu komunikaciju. Ove metode u kombinaciji daju pojedincu mogućnost da odustane od marketinških komunikacija u bilo kojem trenutku. VITANOVA se potrudila detaljno objasniti obradu osobnih podataka pojedincima u obavijesti o privatnosti.

Hoćete li ponuditi pojedincima mogućnost prigovora?	**Da**/ Ne

ODLUČIVANJE

Ovdje upotrebljavate svoje odgovore na korake 1, 2 i 3 da biste odlučili možete li primijeniti osnovu legitimnih interesa.

Možete li se osloniti na legitiman interes kao temelj za obradu?	**Da** / Ne
Komentari?	Da / **Ne**
Test popunio:	Hrvoje Horvat
Datum:	30. rujna 2023

ŠTO JE SLJEDEĆE?

Dokumentirajte ovaj test razmjernosti i revidirajte po potrebi.
Ako je potrebno, napravite procjenu učinka na zaštitu podataka.
U svoje obavijesti/politike privatnosti uključite detalje o svojim svrhama i zakonskoj osnovi za obradu.

Prikaz slučaja (4)

One Leg, One Prosthesis (OLOP) je trgovačko društvo koje prodaje prilagodljive proteze za osobe s amputiranim udovima. Sjedište im je u Njemačkoj i imaju dvije fizičke trgovine, jednu u Berlinu i jednu u Stuttgartu.

Međutim, većina njihove zarade dolazi od njihove online trgovine. Web stranica koristi kolačiće za bolju izvedbu i prikuplja podatke od kupaca širom svijeta. Narasli su i ne mogu pratiti narudžbe u svojoj maloj radionici u Njemačkoj. Zbog toga je OLOP kontaktirao tvornicu u Maleziji koja bi mogla izraditi proteze i zatim ih poslati kupcima.

Da bi to učinili, trebaju imati biometrijske podatke kupca. Ne bi zahtijevali nikakve druge podatke, poput brojeva kreditnih kartica, nacionalnosti ili dobi. Ti bi podaci bili pohranjeni samo u njemačkoj bazi podataka. OLOP je istražio malezijsku tvornicu i otkrio da nikada nije došlo do povrede podataka, iako njihovo djelovanje nije usklađeno s odredbama OUZP već postupaju po svom nacionalnom propisu.

Smije li OLOP uopće prenositi podatke kupaca u tvornicu u drugoj zemlji? Koji je najpreciznji od ponuđenih odgovora?

Evidencija aktivnosti obrade

Temeljni dokument kojim se dokazuje (dokumentira) ponašanje voditelja usklađeno s obvezama prema OUZP – direktna primjena načela pouzdanosti

Postoje različiti obrasci – svako nadzorno tijelo može pripremiti svoj obrazac – svi su jednako primjenjivi

Evidencija aktivnosti obrade sastojati je skup podataka o obradama koje provodi voditelj ili izvršitelj obrade

Evidencije mogu biti koncipirane tako da svaka aktivnost obrade bude zasebni dokument ili da sve budu sastavljene u jednu cjelovitu evidenciju

Evidencije se mogu voditi putem obrasca ili putem posebnog softvera (Data Protection Management System) iz kojeg se mogu eksportirati u bilo kojem standardnom formatu

Primjeri obrazaca koje je pripremio AZOP dostupni su ovdje:

https://azop.hr/obrasci-predlosci/

NAZIV OBRADE	KATEGORIJE ISPITANIKA	IZVRŠITELJ OBRADE	SVRHA OBRADE	IT SERVIS ili FIZIČKO MJESTO POHRANE (LOKACIJA OSOBNIH PODATAKA)	PRAVNA OSNOVA OBRADE (Članak 6. GDPR-a)	Prava dostupna ispitaniku	POVEZNICA NA DOKAZ O PRIVOLI	KATEGORIJE OSOBNIH PODATAKA KOJE SE OBRAĐUJU	OBRADA OBUHVAĆA POSEBNE KATEGORIJE OSOBNIH PODATAKA (Članak 9. GDPR-a)	PRAVNI TEMELJ ZA OBRADU POSEBNIH KATEGORIJA OSOBNIH PODATAKA (sukladno članku 9. GDPR-a), ako je primjenjivo	IME I KONTAKT PODACI ZAJEDNIČKOG VODITELJA OBRADE (AKO JE PRIMJENJIVO)
Naziv pod kojim je obrada prepoznatljiva	Zaposlenici, kupci, posjetitelji, vanjski suradnici....	Podaci o izvršitelju obrade (ako postoji)	Razlog obrade podataka	Popis IT servisa u kojima se vrši obrada podataka ili lokacija fizičkog mjesta pohrane ako podatak nije digitaliziran	Članak 6. GDPR-a: (privola, zakon, ugovor, legitimni interes voditelja obrade, zaštita prava ispitanika, izvršavanje zadaća u okviru javne ovlasti)	Pravo na pristup podacima, pravo na ispravak, pravo na brisanje, pravo na ograničenje obrade, pravo na prigovor, pravo na prijenos drugom voditelju obrade	Unijeti poveznicu na privolu ili lokaciju privole ukoliko je privola temelj ove obrade	Identifikacijski podaci, lokacijski podaci, financijski podaci, zdravstveni podaci itd.	Obuhvaća li obrada posebne kategorije podataka - podaci o zdravlju, članstvu u sindikatu, vjeroispovijest, političke stavove, spolnu orijentaciju, rasu...?	Unijeti pravni temelj za obradu posebnih kategorija osobnih podataka	Ako dvoje ili više voditelja obrade zajednički određe svrhe i načine obrade, oni su zajednički voditelji obrade. Unijeti kontakt podatke zajedničkog voditelja, ukoliko je primjenjivo.
Primjer: EVIDENCIJA PODATAKA O ZAPOSLENICIMA	Zaposlenici	Nema	Vođenje evidencije o zaposlenicima	mapa u zaključanom ormaru u uredu vlasnika poduzeća; mapa pod nazivom zaposlenici u ERP-u, zaštićena šifrom	Obrada je nužna radi poštovanja pravnih obveza voditelja obrade (Čl. 6. GDPR-a, st. 1. točka c) Zakon o radu (NN 93/2014, 127/2017, 98/2019, Pravilnik o sadržaju i načinu vođenja evidencije o radnicima (NN 32/15, 97/15)	Pravo na pristup podacima, pravo na ispravak, pravo na ograničenje obrade	Nije primjenjivo	IDENTIFIKACIJSKI PODACI (ime, prezime, OIB, datum rođenja, spol, prebivalište, boravište, državljanstvo) PODACI O OBRAZOVANJU PODACI O RADNOM STAŽU	Ne	Nije primjenjivo	Nije primjenjivo
Primjer: obračun i isplata plaća i drugih dohodaka	Zaposlenici	Knjigovodstveni servis xy	Obračun i isplata plaća	mapa pod nazivom zaposlenici- isplata plaća u ERP-u, zaštićena šifrom	Obrada je nužna radi poštovanja pravnih obveza voditelja obrade (Čl. 6. GDPR-a, st. 1. točka c) , Zakon o računovodstvu, Zakon o radu, Zakon o mirovinskom osiguranju		Nije primjenjivo	IDENTIFIKACIJSKI PODACI (ime i prezime, adresa, OIB, Spol, dan, mjesec, godina rođenja, prebivalište/boravište) PODACI O OBRAZOVANJU I RADNOM STAŽU (stručno obrazovanje, datum početka rada, naznaku radi li se o punom radnom vremenu ili nepunom radnom vremenu, mjesto rada, datum prestanka radnog odnosa, razlog prestanka radnog odnosa, podaci za potrebu interne komunikacije unutar tvrtke (poslovni kontakt e-mail, tel.) FINANCIJSKI PODACI (IBAN, broj tekućeg računa)	Ne	Nije primjenjivo	Nije primjenjivo
Primjer: EVIDENCIJA KANDIDATA ZA ZAPOŠLJAVANJE	Kandidati za posao	Agencija za zapošljavanje	Provođenje selekcijskog postupka i zapošljavanje	mapa pod nazivom kandidati za zapošljavanje u ERP-u, zaštićena šifrom	Prethodne radnje za sklapanje ugovora (Čl. 6. st. 1. t. b) GDPR-a)/Privola (Čl. st. 1. t. a) GDPR-a)		Nije primjenjivo	IDENTIFIKACIJSKI PODACI (ime, prezime, OIB, datum rođenja, spol, prebivalište, boravište, državljanstvo), PODACI O RADNOM ISKUSTVU, PODACI O OBRAZOVANJU PODACI O OSOBNIM VJEŠTINAMA	Ne	Nije primjenjivo	Nije primjenjivo
Primjer: EVIDENCIJA KUPACA	Kupci	Nema	slanje newslettera u svrhu promocije i nuđenje novih proizvoda, usluga i popusta postojećim kupcima	mapa pod nazivom kupci u ERP-u, zaštićena šifrom	Legitimni interes (Čl. 6. st. 1. t. f) GDPR-a)		Nije primjenjivo	IDENTIFIKACIJSKI PODACI (ime, prezime, e-mail adresa)	Ne	Nije primjenjivo	Nije primjenjivo

Predložak **- EVIDENCIJA AKTIVNOSTI OBRADE**

1. Izvršitelj obrade:

Naziv izvršitelja obrade /ime: ______________________

ulica i broj: ______________________

mjesto: ______________________

broj telefona: ______________________

e-mail: ______________________

Naziv voditelja obrade /ime: ______________________

ulica i broj: ______________________

mjesto: ______________________

broj telefona: ______________________

e-mail: ______________________

(Napomena: izvršitelj obrade znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade odnosno za nekog voditelja obrade;)

2. Službenik za zaštitu podataka

naziv /ime: ______________________

pozicija tj. radno mjesto/vanjski : ______________________

ulica i broj: ______________________

broj telefona: ______________________

e-mail: ______________________

(Službenik za zaštitu podataka može biti član osoblja voditelja obrade ili izvršitelja obrade ili obavljati zadaće na temelju ugovora o djelu. Službenik za zaštitu podataka može ispunjavati i druge zadaće i dužnosti. Voditelj obrade ili izvršitelj obrade osigurava da takve zadaće i dužnosti ne dovedu do sukoba interesa.)

3. Kategorije (postupci/vrste) obrade koje se obavljaju u ime/za svakog voditelja obrade

____

____

____

____

4. Prijenosi osobnih podataka u treću zemlju ili međunarodnu organizaciju (ako je primjenjivo, te također identificiranje te treće zemlje ili međunarodne organizacije, kao i dokumentaciju o adekvatnosti tj. odgovarajućim zaštitnim mjerama)

Naziv treće zemlje ili međunarodne organizacije (uključivo i podaci o primatelju/ima):

____

Prilog:

(dokumentacija o odgovarajućim zaštitnim mjerama)

5. Opći opis tehničkih i organizacijskih sigurnosnih mjera (primijenjenih/odnosnih na predmetnu obradu osobnih podataka)

Opis tehničkih mjera: ______________________

Opis organizacijskih mjera: ______________________

Sadržaj i ispunjavanje evidencije aktivnosti obrade

Sukladno članku 30. OUZP, evidencija aktivnosti obrade osobnih podataka voditelja obrade treba se sastojati od skupa evidencija svake aktivnosti obrade i sadržavati osobito:

- ime i kontaktne podatke voditelja obrade i, ako je primjenjivo, zajedničkog voditelja obrade, predstavnika voditelja obrade i službenika za zaštitu podataka;
- svrhe obrade;
- opis kategorija ispitanika i kategorija osobnih podataka (uključujući i to pripadaju li bilo koji podaci unutar popisa u „posebne kategorije podataka“ / osjetljivi podaci);
- kategorije primateljâ kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodne organizacije;
- podaci o prijenosima osobnih podataka u treću zemlju ili međunarodnu organizaciju
- predviđene rokove za brisanje različitih kategorija podataka
- opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka

1. Koliko detaljno treba ići u raspisivanje aktivnosti obrade?
2. Koliko često treba mijenjati sadržaj evidencije?
3. Čemu uopće služi evidencija?
4. Kako je najučinkovitije pristupiti izradi i održavanju evidencije?
5. Tko je odgovoran za njen sadržaj?
6. Koji voditelji nisu dužni voditi evidenciju aktivnosti obrade?
7. U čemu je razlika između evidencije koju voditelj i one koju vodi izvršitelj?

Evidencija aktivnosti obrade

Evidencija o aktivnostima obrade često se doživljava kao iscrpljujuć i birokratski dokumentacijski zahtjev, ali je središnja komponenta za osiguravanje usklađenosti zaštite podataka u tvrtki i ostvarenje aspekta dokumentiranja postupanja s podacima prema načelu pouzdanosti

Održavanje evidencije o aktivnostima obrade odgovornost je voditelja obrade, a ne službenika za zaštitu podataka (DPO).

Početna uspostava evidencije o aktivnostima obrade je značajan napor. Naknadno održavanje također veže resurse. Posebno u srednjim i većim organizacijama to zahtjeva jasne procese i uključenost svih odjela uključenih u obradu osobnih podataka.

„Aktivnost obrade" može se shvatiti kao skup koraka obrade koji služe jednoj, sveobuhvatnoj svrsi, npr. određeni poslovni proces ili IT alat.

Primjeri aktivnosti obrade su:

Korištenje posebnog softvera ili uređaja pomoću kojih se podaci o zaposlenicima bilježe, pohranjuju ili vrednuju (npr. sustav za bilježenje radnog vremena, digitalne dosjee osoblja, sustav elektroničke pristupne kartice, videonadzor).

Standardizirani interni procesi u kojima se podaci o zaposlenicima kontinuirano ili sustavno prikupljaju, pohranjuju ili koriste (npr. rukovanje podacima o kandidatima za posao, administracija i obrada mjera obuke, obračun plaća, e-mail bilteni za kupce).

Primjeri kriterija za EAO

Primjer: Trebate li imati jednu aktivnost obrade „godišnje ocjenjivanje zaposlenika" ili dvije aktivnosti obrade "ciljani razgovori i ankete zaposlenika" i "mjerenje ciljanog postignuća"?

Visoka granularnost dovodi do zbunjujućeg broja aktivnosti obrade i nepotrebno povećava administrativni teret.

Pregruba granularnost (npr. "upravljanje podacima o osoblju") više ne dopušta smislen pregled usklađenosti sa zaštitom podataka.

Za određivanje sveobuhvatne svrhe korisna je orijentacija na postojeće poslovne procese ili područja odgovornosti.

Razgraničenje se također može temeljiti na tehničkim sustavima koji su u osnovi aktivnosti obrade. Međutim, ne mora se svaki IT sustav smatrati zasebnom aktivnošću obrade.

Ako bi aktivnost obrade spadala pod odgovornost nekoliko odjela, možda bi bilo prikladno podijeliti aktivnost.

U čisto pragmatičnom smislu, viša razina granularnosti u definiciji aktivnosti obrade mogla bi se prihvatiti za manje tvrtke.

PRIMJER

Ne bi trebalo smatrati obradom:
čisto apstraktna obrada bez posebne svrhe

opća uporaba uredskog softvera, opća organizacija projekta

samo povremene operacije obrade

vođenje popisa sudionika sastanaka

NAZIV EVIDENCIJE	VRSTA OSOBNIH PODATAKA KOJI SE OBRAĐUJU	SVRHA OBRADE	IZVOR PODATAKA	OSNOVA OBRADE	VLASNICI OBRADE	NAČIN OBRADE OSOBNIH PODATAKA (ručno, video snimka, pohrana, scan, računalni zapis na internom serveru	ROKOVI ČUVANJA	ULOGE, ZADACI I OVLAŠTENJA RADNIKA KOJI SUDJELUJU U OBRADI PODATAKA	TKO IMA PRAVO UVIDA, KADA I PO KOJOJ OSNOVI
HIGIJENSKO-EPIDEMIOLOŠKI ODJEL									
Registar spolno prenosivih bolesti	Ime, prezime, spol, OIB, MBO, dijagnoza, datum oboljenja, mjesto rada, adresa	Zakon	Prijava i ispitanik	Zakon	HEO odjel	Papirnato u registratoru	Sukladno Pravilniku o zaštiti i obradi arhivskog i registraturnog gradiva - popis gradiva s rokovima čuvanja	Prijava zarazne bolesti od strane liječnika, ispitanik dolazi, liječnik epidemiolog anketira ispitanika, daje mu upute za postupanje	Liječnik koji ispunjava prijavu, NAJS
Evidencija raznih zaraznih bolesti (npr. ušljivost, dječje gliste)	Ime, prezime, spol, OIB, MBO, dijagnoza, datum oboljenja, mjesto rada, adresa	Zakon	Prijava zarazne bolesti od strane liječnika primarne zdravstvene zaštite ili iz bolnice	Zakon	HEO odjel	Papirnato u registratoru, upis podataka iz prijavnice u NAJS	Sukladno Pravilniku o zaštiti i obradi arhivskog i registraturnog gradiva - popis gradiva s rokovima čuvanja	Prijavnica zarazne bolesti od liječnika primarne zdravstvene zaštite, upis podataka iz prijavnice u NAJS program HZJZ-a - pristupa se lozinkom koju imaju svi radnici HEO, anketiranje osobe i upute za daljnje postupanje	Liječnik koji ispunjava prijavu, NAJS
Evidencija ubodnih incidenata	Ime, prezime, mjesto rada, datum i sat ozljede, vrsta ozljede, MBO	Zakon	Obrazac prijave, ispitanik	Zakon	HEO odjel	Papirnato u registratoru	Sukladno Pravilniku o zaštiti i obradi arhivskog i registraturnog gradiva - popis gradiva s rokovima čuvanja	Osoba dolazi temeljem obrasca prijave ubodnog incidenta i uputnice, upućuje se na testiranje i po potrebi cijepi protiv hepatitisa b	
Registar transplantiranih	Ime, prezime, OIB, MBO, dijagnoza, nalaz, datum rođenja, povijest bolesti	Zakon	Osoba koja je transplantirana ili obitelj	Zakon	HEO odjel	Papirnato u registratoru	Sukladno Pravilniku o zaštiti i obradi arhivskog i registraturnog gradiva - popis gradiva s rokovima čuvanja	Ispitanik dolazi epidemiologu koji izrađuje plan cijepljenja	

Evidencija cijepljenih protiv gripe, hepatitisa, ospica, tetanusa, pneumokoka, hpv, itd.	Ime, prezime, OIB, datum rođenja, kategorija za cijepljenje	Zakon	Osoba koja se cijepi - ispitanik	Zakon	HEO odjel	Papirnato u registratoru	Sukladno Pravilniku o zaštiti i obradi arhivskog i registraturnog gradiva - popis gradiva s rokovima čuvanja	Ispitanik dolazi i radnici HEO odjela vrše dobrovoljno cijepljenje	
Registar oboljelih od virusnih hepatitisa	Ime, prezime, datum rođenja, zanimanje, spol, dijagnoza, kontakt, potvrda da više nisu zaraženi	Zakon	Prijava oboljenja od zarazne bolesti i oboljela osoba	Zakon	HEO odjel	Papirnato u registratoru, kompjuterski	Sukladno Pravilniku o zaštiti i obradi arhivskog i registraturnog gradiva - popis gradiva s rokovima čuvanja	Prijava zarazne bolesti, ispitanik se pozove, provjere se kontakti, anketira se, upućuje na pretrage i analizira nalaz te se procijenjuje potreba za cijepljenjem	Liječnik koji prijavljuje, HZJZ kroz Registar oboljelih od hepatitisa, NAJS
Registar oboljelih od svraba	Ime, prezime, datum rođenja, zanimanje, spol, dijagnoza, kontakt, potvrda da više nisu zaraženi	Zakon	Prijava i oboljela osoba - ispitanik	Zakon	HEO odjel	Papirnato u registratoru	Sukladno Pravilniku o zaštiti i obradi arhivskog i registraturnog gradiva - popis gradiva s rokovima čuvanja	Prijavnica zarazne bolesti od liječnika primarne zdravstvene zaštite, epidemiolog anketira ispitanika i daje upute za daljnje postupanje	Liječnik koji prijavljuje, NAJS
Registar oboljelih od legionarske bolesti	Ime, prezime, mjesto stanovanja, godina rođenja, broj prijave zarazne bolesti, mjesto boravka u vrijeme inkubacije, kontakt, nalaz, obrazac ishoda liječenja	Zakon	Epidemiološka služba HZJZ-a	Zakon	HEO odjel	Papirnato u registratoru, kompjuterski	Sukladno Pravilniku o zaštiti i obradi arhivskog i registraturnog gradiva - popis gradiva s rokovima čuvanja	Telefonska dojava HZJZ-a o oboljeloj osobi, epidemiolog anketira oboljelog i provodi izvide u objektu gdje je oboljeli boravio	NAJS
Registar za tuberkolozu	Ime, prezime, mjesto stanovanja, godina rođenja, broj prijave zarazne bolesti, kontakt, nalaz, obrazac ishoda liječenja	Uvid u pobol - legitimni interes voditelja obrade	Prijava zarazne bolesti od strane liječnika primarne zdravstvene zaštite ili iz bolnice	Zakon	HEO odjel	Papirnato u registratoru, komjuterski	Sukladno Pravilniku o zaštiti i obradi arhivskog i registraturnog gradiva - popis gradiva s rokovima čuvanja	HEO odjel zaprimi prijavu, ide se u izvid i ispitanik se anketira o kontaktima te se temeljem toga odlučuje o potrebnim pretragama, ispitanik se vraća sa nalazom u HEO odjel	Nadležni liječnik primarne zdravstvene zaštite, specijalisti, NAJS
Evidencija osoba koje su cijepljene	Ime, prezime, datum rođenja, OIB, datum cijepljenja	Legitimni interes voditelja obrade	Ispitanik	Zakon	HEO odjel	Papirnato, komjuterski	Sukladno Pravilniku o zaštiti i obradi arhivskog i registraturnog gradiva - popis gradiva s rokovima čuvanja	Ispitanik dolazi u ambulantu, uzimaju se podaci od ispitanika i upisuju u evidenciju	Sanitarna inspekcija

Primjer evidencije aktivnosti obrade (Records of processing activity, ROPA) – obrade u okviru zdravstvenih usluga

Voditelj/Izvršitelj	Naziv obrade	Kategorija ispitanika	Vrste osobnih podataka	Organizacijska jedinica / Vlasnik obrade	Podatak prikupljen od:	Svrha obrade	Pravna osnova	Gdje se podaci nalaze	Rok pohrane podataka	Primatelj	Posebna kategorija podatka (da/ne)	Prijenos u treće zemlje (da/ne)	DPIA (da/ne)
Voditelj	**Informacijski sustav zdravstvene ustanove**	pacijenti	ime i prezime	Služba zdravstvenih poslova i usluga	ispitanik/osoblje bolnice	Skrb za pacijente	Pravna obveza (6.1.c) + 9.2.h. Preventivna medicina, medicina rada, medicinska dijagnostika	Centralni server	10 godina	interno - ne izlazi iz organizacije	DA	ne	DA
			broj osiguranika										
			ostali zdravstveni podaci i medicinske informacije										
Voditelj	**Laboratorijske pretrage**	pacijenti	ime i prezime	Služba zdravstvenih poslova i usluga	ispitanik/osoblje bolnice	Skrb za pacijente	Pravna obveza (6.1.c) + 9.2.h. Preventivna medicina, medicina rada, medicinska dijagnostika	Laboratorijski server	10 godina	interno - ne izlazi iz organizacije	DA	ne	DA
			broj osiguranika										
			ostali zdravstveni podaci i medicinske informacije										
Voditelj	**Podaci u radiološkim sustavima**	pacijenti	ime i prezime	Služba zdravstvenih poslova i usluga	ispitanik/osoblje bolnice	Skrb za pacijente	Pravna obveza (6.1.c) + 9.2.h. Preventivna medicina, medicina rada, medicinska dijagnostika	Lokalna pohrana sustava radiologije	10 godina	interno - ne izlazi iz organizacije	DA	ne	DA
			broj osiguranika										
			ostali zdravstveni podaci i medicinske informacije										
Voditelj	**Radiološki imaging**	pacijenti	šifra pacijenta iz informacijskog sustava zdravstvene ustanove	Služba zdravstvenih poslova i usluga	ispitanik/osoblje bolnice	Skrb za pacijente	Pravna obveza (6.1.c) + 9.2.h. Preventivna medicina, medicina rada, medicinska dijagnostika	Lokalna pohrana sustava radiologije	10 godina	interno - ne izlazi iz organizacije	DA	ne	DA
			radiološke snimke										
Voditelj	**Prehrambeni i dijetalni podaci pacijenata**	pacijenti	šifra pacijenta iz informacijskog sustava zdravstvene ustanove	Služba zdravstvenih poslova i usluga	ispitanik/osoblje bolnice	Skrb za pacijente	Pravna obveza (6.1.c) + 9.2.h. Preventivna medicina, medicina rada, medicinska dijagnostika	Centralni server	10 godina	interno - ne izlazi iz organizacije	DA	ne	DA
			Prehrambene alergije										
			Dijetalni zahtjevi										

Primjer evidencije aktivnosti obrade u zdravstvu – obrade podataka zaposlenika

Voditelj/Izvršitelj	Naziv obrade	Kategorija ispitanika	Vrste osobnih podataka	Organizacijska jedinica / Vlasnik obrade	Izvor osobnog podatka	Svrha obrade	Pravna osnova	Gdje se podaci nalaze	Rok pohrane podataka	Primatelj	Posebna kategorija podatka (da/ne)	Prijenos u treće zemlje (da/ne)	DPIA (da/ne)
Voditelj	Interni imenik zaposlenika	zaposlenici	ime i prezime	Kadrovska služba	ispitanik/osoblje bolnice	Organizacija rada u ustanovi	Pravna obveza (6.1.c)	HR SUSTAV	10 godina	interno - ne izlazi iz organizacije	NE	NE	NE
			broj telefona										
			email adresa										
Voditelj	Evidencija podataka o radnicima	zaposlenici	ime i prezime	Kadrovska služba	ispitanik/osoblje bolnice	Ispunjavanje obveza po Zakonu o radu	Pravna obveza (6.1.c) + 9.2.h. Preventivna medicina, medicina rada, medicinska dijagnostika	HR SUSTAV	Trajno	HZZO	DA	ne	DA
			broj osiguranika							HZMO			
			ostali zdravstveni podaci i medicinske informacije							Porezna uprava Ministarstva financija			
Voditelj	Evidencije ozljeda na radu	zaposlenici	ime i prezime	Kadrovska služba	ispitanik/osoblje bolnice	Sigurnost radnog okruženja	Pravna obveza (6.1.c) + 9.2.h. Preventivna medicina, medicina rada, medicinska dijagnostika	Centralni server	5 godina nakon prestanka radnog odnosa	HZZO	DA	NE	DA
			broj osiguranika										
			ostali zdravstveni podaci i medicinske informacije										
Voditelj	Stručno osposobljavanje	zaposlenici	ime i prezime, akademski stupanj, programi edukacije, certifikacije	Kadrovska služba	ispitanik/osoblje bolnice	Ispunjavanje obveza prema Zakonu o liječništvu	Pravna obveza (6.1.c)	HR SUSTAV	5 godina nakon prestanka radnog odnosa	interno - ne izlazi iz organizacije	NE	NE	NE
			radiološke snimke										
Voditelj	Životopisi kandidata	kandidati za radni odnos	Ime i prezime	Kadrovska služba	ispitanik/osoblje bolnice	Odabir kandidata za zasnivanje radnog odnosa	Predugovorne radnje prije sklapanja ugovora o radu	HR SUSTAV	2 godine	interno - ne izlazi iz organizacije	NE	NE	DA
			Podaci o obrazovanju										
			Podaci o radnom iskustvu										
Voditelj	Analitika web stranica	posjetitelji web stranica	identifikacijski podaci putem kolačića	Web uredništvo	ispitanik	Marketing	Legitimni interes	Google Analytics	3 mjeseca	Google	NE	Prijenos temeljem EU-SAD Odluke o primjerenosti okvira za zaštitu podataka između EU i SAD	NE
Voditelj	Podaci o dobavljačima	zaposlenici partnerskih organizacija	ime i prezime	Računovodstvo	ispitanik/osoblje bolnice	Dostava opskrbe	Ugovor	ERP	Godinu dana nakon prestanka ugovora	interno - ne izlazi iz organizacije	NE	NE	NE
			Broj telefona										
			email adresa										

Poslovna funkcija	Svrha obrade	Ispitanici	Kategorije osobnih podata	Kategorije primatelja	Raspored zadržavanja (ako	Opći opis tehničkih i organizacijskih sigurnosnih mjera (ako je primjenjivo	Temelji zakonite obrade osobnih	Temelji obrade posebnih kategor	Poveznica na dokaz o procjeni legitimnih interesa (ako je primjenjivo)	Prava dostupna ispitanicim	Postojanje automatiziran	Izvor osobnih podataka (ako i	Poveznica na dokaz o privoli
Ljekarnička jedinica	Izdavanje lijeka temeljem e-recepta	Pacijenti	Podaci koji se odnose na zdravlje	Hrvatski zavod za zdravstveno osiguranje	7 godina nakon izdavanja lijeka (minimalno)	Enkriptirana pohrana, enkripcija prometa, pametne kartice za ovlaštene korisnike	Članak 6. st. 1. točka (c) - pravna obaveza 1. Zakon o zdravstvenoj zaštiti 2. Pravilniku o načinu propisivanja i izdavanja lijekova na recept 3.Pravilnik o mjerilima za	Članak 9. st. 2. točka (i) - osiguravanje sigurnosti zdravstvene skrbi te lijekova i medicinskih proizvoda	1. Zakon o zdravstvenoj zaštiti 2. Pravilniku o načinu propisivanja i izdavanja lijekova na recept 3.Pravilnik o mjerilima za razvrstavanje lijekova te o propisivanju i izdavanju lijekova na recept	Pravo na pristup	N/A	liječnički recept	N/A
Ljekarnička jedinica	Izdavanje lijeka temeljem e-recepta	Liječnici	Kontakt podaci	N/A	7 godina nakon izdavanja lijeka (minimalno)	Enkriptirana pohrana, enkripcija prometa, pametne kartice za ovlaštene korisnike	Članak 6. st. 1. točka (c) - pravna obaveza 1. Zakon o zdravstvenoj zaštiti 2. Pravilniku o načinu propisivanja i izdavanja lijekova na recept 3.Pravilnik o mjerilima za	Članak 9. st. 2. točka (i) - osiguravanje sigurnosti zdravstvene skrbi te lijekova i medicinskih proizvoda	1. Zakon o zdravstvenoj zaštiti 2. Pravilniku o načinu propisivanja i izdavanja lijekova na recept 3.Pravilnik o mjerilima za razvrstavanje lijekova te o propisivanju i izdavanju lijekova na recept	Pravo na pristup	N/A	liječnički recept	N/A
Ljekarnička jedinica	Izdavanje lijeka temeljem e-recepta	Liječnici	Šifra zdravstvenog djelatnika	Hrvatski zavod za zdravstveno osiguranje	7 godina nakon izdavanja lijeka (minimalno)	Enkriptirana pohrana, enkripcija prometa, pametne kartice za ovlaštene korisnike	Članak 6. st. 1. točka (c) - pravna obaveza 1. Zakon o zdravstvenoj zaštiti 2. Pravilniku o načinu propisivanja i izdavanja lijekova na recept 3.Pravilnik o mjerilima za	Članak 9. st. 2. točka (i) - osiguravanje sigurnosti zdravstvene skrbi te lijekova i medicinskih proizvoda	1. Zakon o zdravstvenoj zaštiti 2. Pravilniku o načinu propisivanja i izdavanja lijekova na recept 3.Pravilnik o mjerilima za razvrstavanje lijekova te o propisivanju i izdavanju lijekova na recept	Pravo na pristup	N/A	liječnički recept	N/A
Ljekarnička jedinica	Izdavanje lijeka temeljem papirnatog recepta	Pacijenti	Kontakt podaci	Hrvatski zavod za zdravstveno osiguranje	7 godina nakon izdavanja lijeka (minimalno)	Enkriptirana pohrana, enkripcija prometa, pametne kartice za ovlaštene korisnike	Članak 6. st. 1. točka (c) - pravna obaveza 1. Zakon o zdravstvenoj zaštiti 2. Pravilniku o načinu propisivanja i izdavanja lijekova na recept 3.Pravilnik o mjerilima za	Članak 9. st. 2. točka (i) - osiguravanje sigurnosti zdravstvene skrbi te lijekova i medicinskih proizvoda	1. Zakon o zdravstvenoj zaštiti 2. Pravilniku o načinu propisivanja i izdavanja lijekova na recept 3.Pravilnik o mjerilima za razvrstavanje lijekova te o propisivanju i izdavanju lijekova na recept	Pravo na pristup	N/A	liječnički recept	N/A
Ljekarnička jedinica	Izdavanje lijeka temeljem papirnatog recepta	Liječnici	Šifra zdravstvenog djelatnika	Hrvatski zavod za zdravstveno osiguranje	7 godina nakon izdavanja lijeka (minimalno)	Enkriptirana pohrana, enkripcija prometa, pametne kartice za ovlaštene korisnike	Članak 6. st. 1. točka (c) - pravna obaveza 1. Zakon o zdravstvenoj zaštiti 2. Pravilniku o načinu propisivanja i izdavanja lijekova na recept 3.Pravilnik o mjerilima za	Članak 9. st. 2. točka (i) - osiguravanje sigurnosti zdravstvene skrbi te lijekova i medicinskih proizvoda	1. Zakon o zdravstvenoj zaštiti 2. Pravilniku o načinu propisivanja i izdavanja lijekova na recept 3.Pravilnik o mjerilima za razvrstavanje lijekova te o propisivanju i izdavanju lijekova na recept	Pravo na pristup	N/A	liječnički recept	N/A

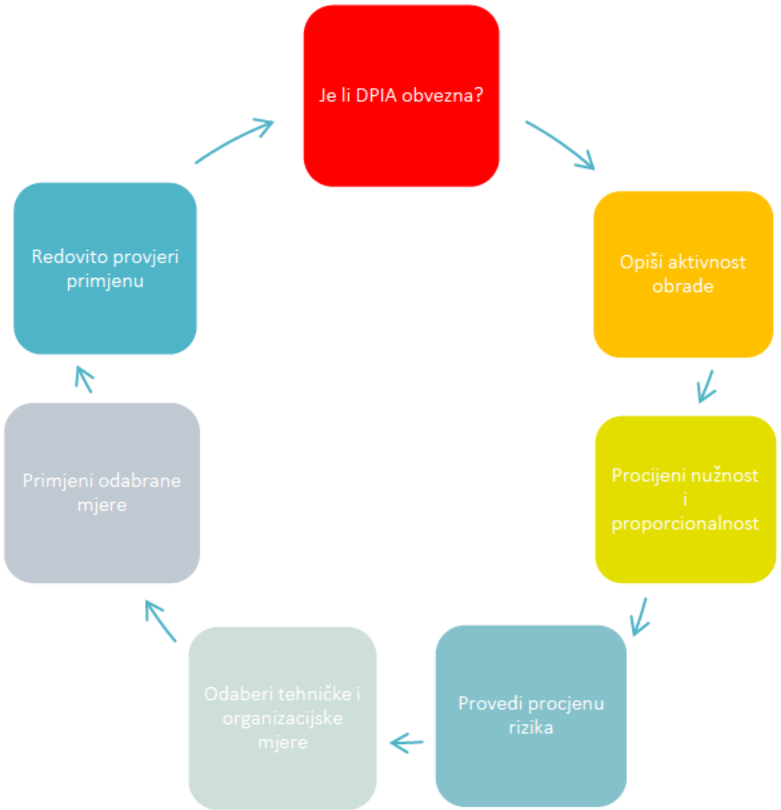
Procjena učinka na zaštitu podataka – DPIA

Što je i čemu služi procjena učinka

- Tko u njoj sudjeluje
- Koje su koristi za ispitanike i voditelje obrada

Smjernice i mišljenja nadzornih tijela

- Kako provesti procjenu učinka
- Industrijski standardi i metodologije
- Praktična primjena – primjer tipične obrade u okruženju zdravstvenih organizacija
- Praktična primjena – primjer obrade temeljene na pametnoj senzorskoj tehnologiji



Zašto nam treba procjena učinka?

- Procjena učinka je jedan od alata **za postizanje i dokazivanje sukladnosti** s odredbama Uredbe
  - Čl.24.st.1 OUZP:" Uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere..."
- Cilj **identificirati rizike u fazi planiranja i odabrati mjere tretiranja rizika** kad je to jednostavnije i manje skupo
  - Otkriti rizike za prava i slobode ispitanika
  - Predložiti mjere za njihovo uklanjanje ili ublažavanje
- Njena provedba rezultira boljom organizacijom zaštite podataka, efikasnijom politikom zaštite podataka i boljim odnosom s ispitanicima

Tko sudjeluje u procjeni učinka?

- Procjenu učinka provodi voditelj obrade – zaposlenici uz pomoć službenika za zaštitu podataka
- U tome treba imati, ukoliko je nužna, osiguranu pomoć i suradnju izvršitelja obrade
- Procjena se može i *outsourceati*, no odgovornost je voditeljeva
- Voditelj je dužan konzultirati službenika za zaštitu podataka te dokumentirati svoje odluke i njegove preporuke

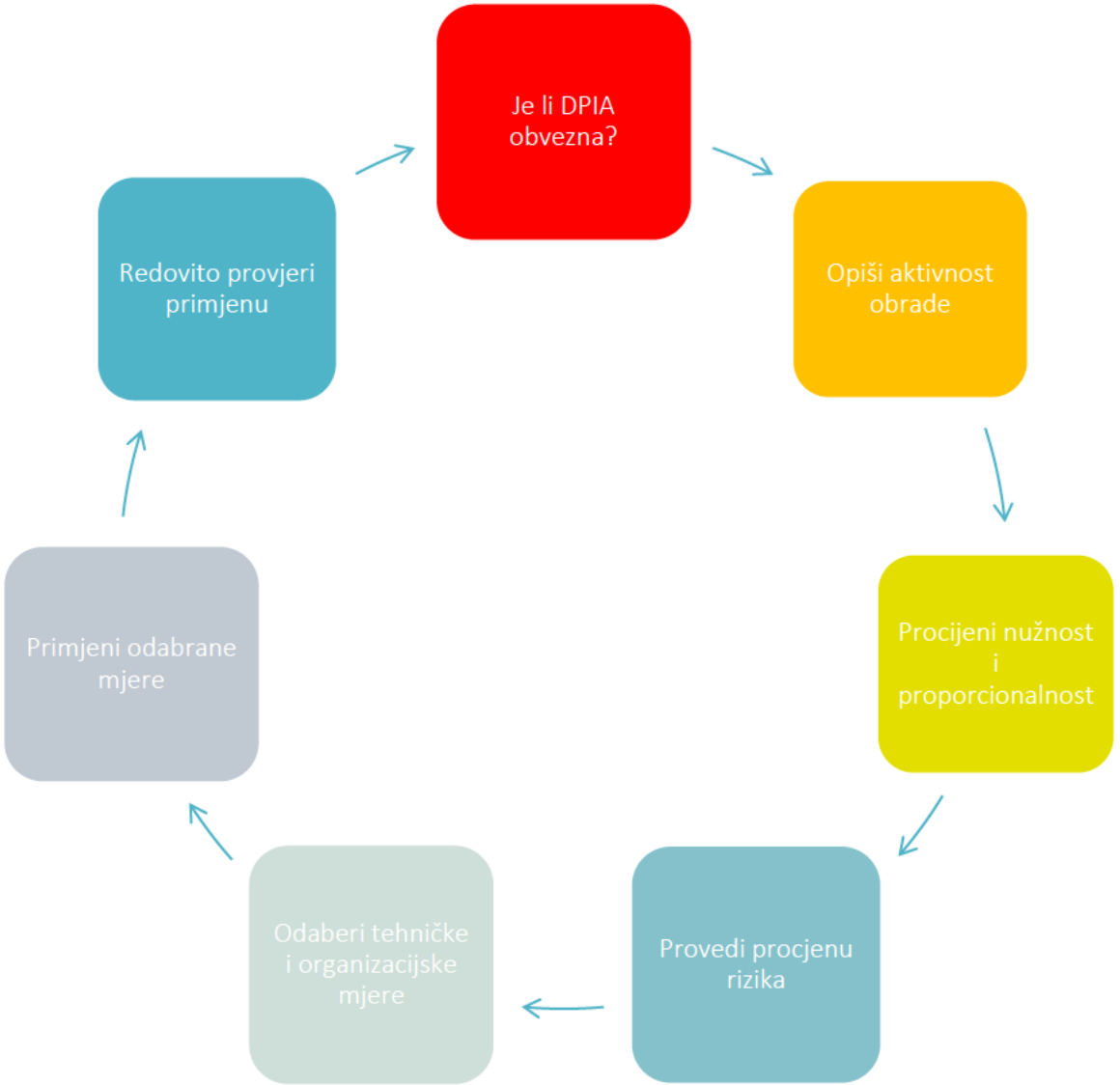
Kada je procjena učinka obvezna?

- Kod onih koje rezultiraju *„visokim rizikom”* za prava ispitanika (čl.35.st.3 OUZP)

  evaluacija i bodovanje ispitanika,
  automatsko donošenje odluka,
  sustavno praćenje,
  posebne kategorije osobnih podataka,
  velik obujam podataka,
  ukrštavanje ili kombiniranje podatkovnih skupova,
  podaci o ranjivim kategorijama ispitanika itd.

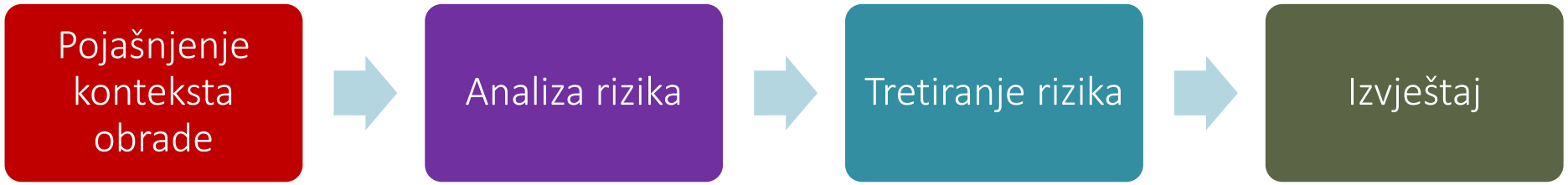
Kada se provodi procjena učinka?

- Procjena učinka provodi se **prije početka obrade**
- Najbolje ju je **provesti tijekom faze planiranja** nove obrade
- Zakonodavac će ju provoditi u zakonodavnom postupku
- Ne čekati s procjenom samo zato što će se karakter obrade mijenjati
- Procjena je **trajni proces**, ne aktivnost koju treba provesti samo jednom



Što obuhvaća procjena učinka?

- Uredba uređuje minimalni sadržaj procjene učinka koja treba sadržavati (OUZP čl. 35.7):
  - Opis i svrhu planiranih obrada
  - Procjenu nužnosti i proporcionalnosti obrade
  - Procjenu rizika za prava i slobode ispitanika
  - Mjere namijenjene umanjenju rizika
  - Druge mjere namijenjene osiguranju sukladnosti s Uredbom



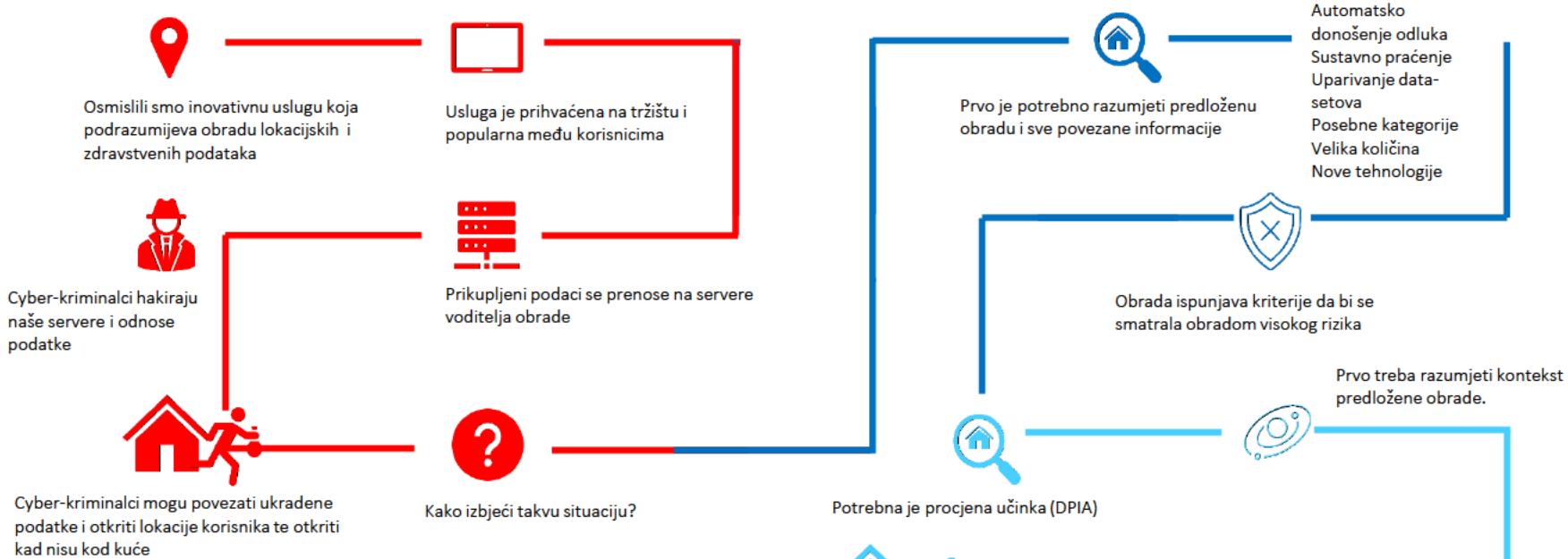
Koju metodologiju odabrati?

- DPIA prema odredbama Uredbe predstavlja alat za procjenu rizika *iz perspektive i u svrhu zaštite prava ispitanika*
- Uredba ne propisuje konkretnu metodologiju. WP29/EDPB potiče razvoj sektorski specifičnih metodologija za određene tipove obrada i setova osobnih podataka
    - Primjerice, u financijskoj industriji, zdravstvu, prometu, turizmu itd.
- Smjernice WP29/EDPB upućuju na kriterije za odabir odgovarajuće metodologije koja treba omogućiti:
    - Sustavni opis obrade
    - Voditi računa o načelima obrade i pravima ispitanika
    - Adekvatno procijeniti rizike za prava i slobode ispitanika
    - Osigurati sudjelovanje DPO i u slučaju potrebe predstavnika ispitanika

PROCJENA UČINKA

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.

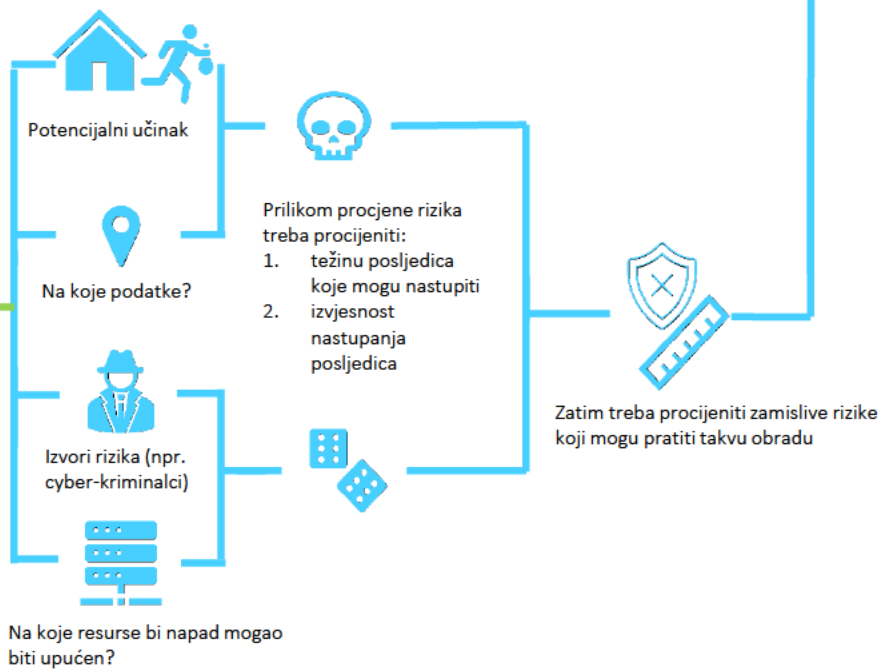


2. Osmišljavanje nove obrade

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.

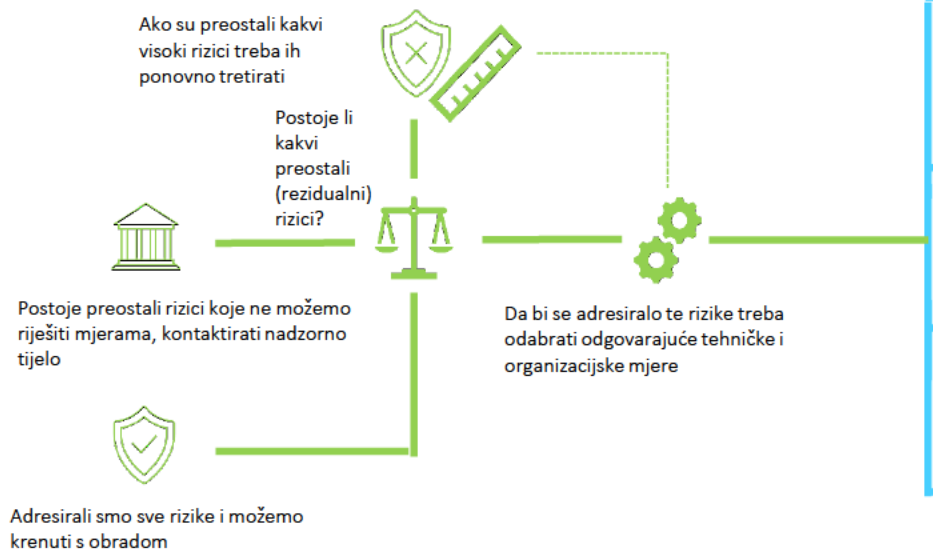
3. Procjena rizika

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



4. Ublažavanje 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.



Nacionalna bolnica za plućne bolesti

PROCJENA UČINKA NA ZAŠTITU PODATAKA (eng. DPIA)

OZNAKA:RRPD Registar rijetkih plućnih bolesti

Ovaj predložak je primjer kako možete bilježiti svoj postupak/ishod procjene učinka na zaštitu podataka. Uz njega je potrebno proučiti pravne propise, Smjernice[1] o procjeni učinka na zaštitu podataka-https://azop.hr/images/dokumenti/217/wp248_rev.01_hr.pdf te pogledati Odluku o popisu vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka https://azop.hr/aktualno/detaljnije/odluka-o-uspostavi-i-javnoj-objavi-popisa-vrsta-postupaka-obrade-koje-podli

PODACI O VODITELJU OBRADE

Ime	Nacionalna bolnica za plućne bolesti
Službenik za zaštitu podataka (eng. DPO)	Hrvoje Bronhić, mag.iur
Kontakt voditelja obrade/službenika za zaštitu podataka	szop@nbpb.hr
Voditelj istraživanja	Prof. dr. sc. Živko Dišić

KORAK 1: IDENTIFICIKACIJA POTREBE

Zašto smatrate da je potrebno provesti postupak procjene učinka na zaštitu podataka?
Prema Općoj uredbi o zaštiti podataka i Pravilniku o zdravstvenim istraživanjima iz 2018., Nacionalna bolnica ima zakonsku obvezu provesti procjenu učinka tamo tamo gdje se provodi projekt zdravstvenog istraživanja (u daljnjem tekstu 'Projekt') i moguće je da takvo istraživanje može dovesti do visokih rizika kada postoji namjera prikupljanja, stvaranja ili korištenja osobnih podataka. U našoj instituciji, temeljem uputa Agencije za zaštitu osobnih podataka, kao i odluke Europskog odbora o zaštiti podataka, pripremili smo dokument za probir potencijalnih aktivnosti koje će zahtijevati izradu procjene učinka. Svjesni smo da naše istraživačke aktivnosti mogu dovesti do visokih rizika i posljedica za prava i slobode naših pacijenata. Popunjavanjem upitnika zaključili smo da je postupak procjene učinka na

[1] Posebice pogledati Kriterije za prihvatljivu procjenu učinka na zaštitu podataka (Prilog II dokumenta)

zaštitu podataka nužan za predloženi projekt obzirom na velik obujam podataka i činjenicu da planiramo obrađivati zdravstvene podatke naših pacijenata.

Također, predložena obrada u bitnom je slična postojećoj obradi koju Bolnica provodi, a koja je također zahtjevala provođenje procjene učinka na zaštitu podataka obzirom da je prepoznata kao obrada koja potpada pod definiciju obrade visokog rizika.

Obzirom na specifične okolnosti ove obrade, ako nije moguće ublažiti rizike zaštite podataka projekta na prihvatljivu razinu, planirani projekt će se možda morati znatno izmijeniti ili čak prekinuti.

Naziv projekta: Registar rijetkih plućnih bolesti (RRPB)

Svrha ove studije je uspostaviti središnji repozitorij koji može podržati buduća istraživanja usmjerena na poboljšanje prevencije, dijagnoze i liječenja plućnog virusnog atrofirajućeg emfizema.

Dvije su komponente projekta:

1) Registar koji sadrži podatke o zdravstvenoj skrbi pacijenata i demografiju. Ovaj registar će se koristiti za proučavanje ishoda za plućni virusni atrofirajući emfizem (PVAE).

2) Biobanka/bioresurs koji sadrži pohranjene biološke uzorke (tkiva, krvi, limfe i DNK) koji se koriste uz podatke iz registra za dubinsko proučavanje bolesti i identifikaciju potencijalnih biomarkera za bolest provođenjem etički odobrenih istraživačkih studija.

PVAE se odnosi se na skupinu rijetkih autoimunih infekcijom potaknutih poremećaja s godišnjom incidencijom od 1/sto tisuća ili 250 – 500 slučajeva godišnje u Republici Hrvatskoj i javlja se primarno u odraslih osoba s prosječnom dobi od 32 godine.

Stanje je popraćeno širokim rasponom medicinskih komplikacija koje često predstavljaju dijagnostičku dilemu budući da mnogi kliničari neće biti upoznati sa stanjem, što odgađa postavljanje dijagnoze za 6-12 mjeseci. Posljedično, uništavanje organa napreduje tako da 30% završi s krajnjim stadijem bolesti pluća, a skrb na razini jedinice intenzivne njege često je potrebna zbog disfunkcije više organa. Iako su dostupni učinkoviti tretmani, PVAE ostaje uglavnom smrtonosna bolest praćena kroničnim relapsirajućim stanjem bez izlječenja koje zahtijeva koordinirani dugoročni multidisciplinarni doprinos.

RRPB je inicijativa usmjerena na rješavanje ove nezadovoljene potrebe i sastoji se od namjenskih multidisciplinarnih centara diljem zemlje koji pružaju koordiniranu skrb od dijagnoze do relapsa i dugoročne remisije, te omogućuju pristup kliničkim ispitivanjima za pacijente s PVAE.

Kako bi podržala visokokvalitetno translacijsko istraživanje, ova je mreža uspostavila PVAE Registar i Bioresurs koji bi sadržavali podatke o ispitanicima. Pacijente koji ispunjavaju uvjete identificira vodeći kliničar u studiji u lokalnim bolničkim mjestima, a u studiju ih uključuje lokalni istraživački tim. Svakom novaku se dodjeljuje broj studije koji se bilježi u medicinskom kartonu pacijenta i obrascu za pristanak.

Podaci po kojima se pacijent može identificirati pohranjuju se u u našoj ustanovi. Biološki uzorci (tkiva, krv, limfa i DNK) obrađuju se i pohranjuju lokalno uz upravljanje arhiviranjem pomoću standardnog softvera Smrzosken2000. Pohranjene uzorke može zatražiti u istraživačke svrhe akademski ili industrijski (komercijalni) laboratorij sklapanjem ugovora o prijenosu materijala (putem ureda za tehnički prijenos). Povezane kodirane kliničke podatke bilježi (koristeći broj studije umjesto imena) istraživački tim u bazi podataka RRPB registra, koja se nalazi u NBPBu (od strane IT usluga) i kontrolira siguran pristup.

Sustav baze podataka korišten za ovu studiju kreiran je korištenjem OpenClinica rješenja. Ima web sučelje za izradu i upravljanje online anketama i bazama podataka. Sigurnošću i infrastrukturom ove baze podataka upravlja odjel IT usluga u NBPB. Host poslužitelj, glavni poslužitelj baze podataka i veza između njih dvoje sigurno su zaštićeni vatrozidom hosta i institucije.

Voditelji obrade podataka uključeni u projekt identificirani su na sljedeći način:

Voditelji obrade podataka: 1) Nacionalna Bolnica (za RKD Biobank i Registar - kodirani uzorci i podaci), u okviru Bolnice kao voditelj studije označen je: Živko Dišić

Upravljanje bazom podataka i pohrana: IT odjel, Nacionalna Bolnica

2) Voditelji obrade podataka o pacijentima navedeni su u nastavku:

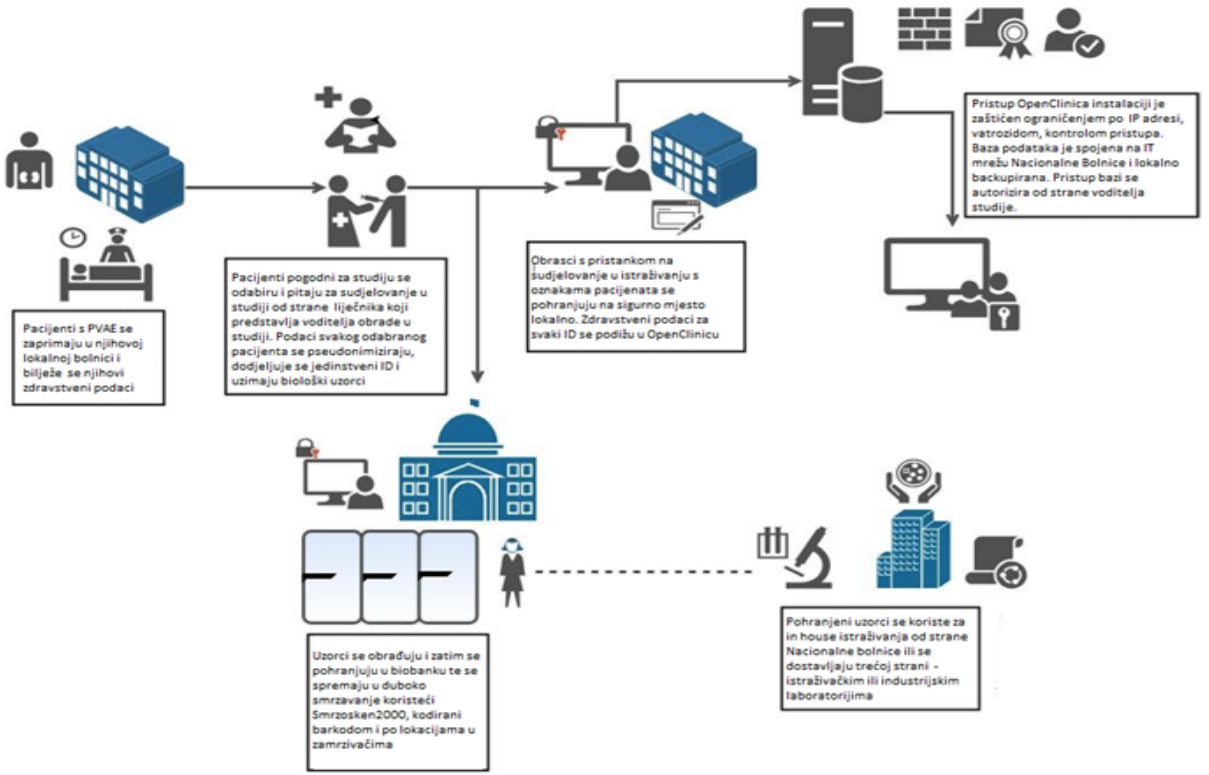
a) KBC Rijeka (za medicinsku dokumentaciju regrutiranih sudionika)

b) Opća bolnica Karlovac (za medicinsku dokumentaciju regrutiranih sudionika)

c) Opća bolnica Sisak (za medicinsku dokumentaciju regrutiranih sudionika)

d) Sveučilišna klinička bolnica Mostar (za medicinsku dokumentaciju regrutiranih sudionika)

Također, ako se koristi međunarodni podatkovni centar, može doći do obrade podataka izvan EU. NPBP će koristiti samo usluge koje su u skladu s Općom uredbom o zaštiti podataka i koje zadovoljavaju uvjete za obradu osobnih podataka izvan EU. Za dobavljače treće strane koristit će se odgovarajući ugovori o obradi podataka te mehanizmi prijenosa podataka sukladno OUZP.



Opišite opseg obrade: koja je priroda podataka i uključuju li podaci posebne kategorije ili obradu osobnih podataka koji se odnose na kaznene osude i kažnjiva djela? Na koji period ćete pohraniti podatke? O kojem broju pojedinaca se radi te koje teritorijalno područje obuhvaća?

Ova studija uključuje prikupljanje i obradu osjetljivih osobnih podataka koji se odnose na demografske podatke sudionika studije koji uključuju spol, datum rođenja, etničku pripadnost i status zaposlenja te zdravstvene podatke koji uključuju detaljnu medicinsku dokumentaciju koja opisuje kliničke karakteristike bolesti, karakteristike biopsije, liječenje, detalje o komorbiditetima, dijagnozu i nastavak liječenja.

Dodatno, detaljna procjena bolesti pri sljedećim susretima i, ako je primjenjivo, pojedinosti o transplantaciji uključujući vrstu donora i imunosupresivne lijekove. U registar se unose samo kodirani podaci (označeni ID-om studije). Studija također uključuje prikupljanje bioloških i genetskih podataka koji uključuju uzorke tkiva, krvi, limfe i DNA koji se centralno obrađuju i pohranjuju u NBPB biobanci do daljnjih istraživanja.

Uzorci biopsije pohranjuju se u lokalnim bolnicama. Podaci se obrađuju na period od dvadeset godina, koliko procjenjujemo da će biti interesa za istraživačkim radom na uzorcima koje prikupljamo. Očekujemo nekoliko tisuća uzoraka iz područja Republike Hrvatske i regije. Vrijednost uzoraka u biobanci za istraživanje implicitno je povezana s podacima koji se čuvaju u registru. Kako bismo bili sigurni da su uzorci prikupljeni uz izričit pristanak, zadržati ćemo obrasce pristanka - to će omogućiti vezu između uzorka i identiteta sudionika; stoga će se podaci smatrati 'pseudonimiziranim' tijekom životnog vijeka uzorka.

Budući da ova studija uključuje longitudinalno praćenje sudionika, bit će potrebno zadržati vezu između koda studije i pojedinca na razini mjesta kako bi se omogućilo praćenje progresije bolesti. Kako je ovo biobanka, u ovoj je fazi nepoznato koji će se konkretni istraživački projekti izvoditi i kada - i trenutačno očekujemo da će biobanka ostati aktivna (ovo će djelomično ovisiti o kontinuiranom financiranju izvora) dvadeset godina ili kraće.

Opišite kontekst obrade: kakva je priroda Vašeg odnosa s pojedincima? Koliku će kontrolu nad obradom imaju pojedinci imati? Bi li očekivali da na taj način koristite njihove podatke? Uključuje li obrada podatke djece ili druge ranjive[3] skupine? Postoje li prethodne zabrinutosti zbog ove vrste obrade ili sigurnosni nedostatci? Postoje li u trenutku obrade pitanja od javnog interesa koja biste trebali ubrojiti? Postoji li odobreni kodeks ponašanja ili sustav certificiranja u Vašem poslovnom subjektu?

Podaci koje planiramo obrađivati dolaze od pacijenata koji se dolaze liječiti u partnerske institucije. Ispitanici mogu odustati od daljnjeg sudjelovanja u bilo kojem trenutku. Pretpostavljamo da postoji racionalno očekivanje da bi njihovi uzorci i podaci mogli biti korišteni na ovaj način obzirom na status naših ustanova kao ustanova zdravstvene zaštite, ali i istraživačkih ustanova sukladno odredbama Zakon o zdravstvenoj zaštiti, osobito: čl. 21, 30, 46, 70, 112-127 itd. Poštivat će se prava pojedinaca:

•Pravo pristupa: ispitanici imaju pravo pristupa svojim podacima, organizacije članovi istraživačkog tima imaju uspostavljene procese za odgovor na zahtjeve za pristup podacima.

•Pravo na ispravak: NPBP i partneri prikupljaju podatke koji su točni u trenutku uzimanja uzorka. Ako se ti podaci naknadno promijene (npr. ispitanik je promijenio ime ili adresu), podaci se mogu ažurirati za buduću upotrebu, ali će zapis iz vremena vađenja uzorka ostati, jer je bio točan u trenutku vađenja zuba.

•Pravo na prigovor: pojedinac ima pravo uložiti prigovor na obradu svojih podataka od strane NBPB i biti uklonjen iz sustava.

•Pravo na ograničenje obrade: pojedinac ima pravo ograničiti obradu svojih podataka od strane NBPB i biti privremeno ograničen unutar sustava, na obostrano dogovoreno vremensko razdoblje. Ograničenje će se izvršiti označavanjem podataka na sustavu kako bi se spriječila njihova obrada.

•Pravo na prenosivost podataka: Ovo se pravo ne primjenjuje jer zakonska osnova za obradu podataka nije privola ili izvršenje ugovora

. •Pravo na brisanje: pojedinac ima pravo na brisanje svojih podataka iz NBPB sustava. Zapisi se brišu iz sustava nakon 20 godina.

•Prava u odnosu na automatizirano donošenje odluka i profiliranje: Obrada podataka ne uključuje automatizirano donošenje odluka i profiliranje.

Postoji li prethodna zabrinutost zbog ove vrste obrade ili sigurnosnih nedostataka? Ne.

Postoje li aktualna pitanja od javnog značaja koja biste trebali uzeti u obzir? Ništa o čemu smo bili obaviješteni u našim javnim anketama.

Jeste li potpisali odobreni kodeks ponašanja ili shemu certificiranja (nakon što su odobreni)? Ne postoji ništa takvo, ali čekamo da Ministarstvo zdravstva usvoji Katalog informacijskih standarda u zdravstvu Republike Hrvatske

Opišite svrhe obrade: što želite postići? Koji je predviđeni učinak na pojedince? Koje su prednosti obrade – za vas i šire?

Što želite postići? Želimo ustrojiti:

1) Registar koji sadrži podatke o zdravstvenoj skrbi pacijenata i demografiju. Ovaj registar će se koristiti za proučavanje ishoda za plućni virusni atrofirajući emfizem (PVAE).

2) Biobanka/bioresurs koji sadrži pohranjene biološke uzorke (tkiva, krvi, limfe i DNK) koji se koriste uz podatke iz registra za dubinsko proučavanje bolesti i identifikaciju potencijalnih biomarkera za bolest provođenjem etički odobrenih istraživačkih studija.

Zašto to želimo i koji je učinak na pojedince?

PVAE je teška bolest koja nepovoljno utječe na bolesnike i članove njihovih obitelji. Ustrojavanje ove obrade privući će nova istraživanja na području terapije i mogućeg izliječenja bolesti.

KORAK 3: SAVJETOVANJE

Kako ćete se posavjetovati s relevantnim dionicima: opišite kada i kako ćete upitati za stavove ispitanika[4] ili njihovih predstavnika – ili obrazložite zašto to nije prikladno. Koga još trebate uključiti u proces iz Vašeg poslovnog subjekta? Postoji li potreba da zamolite izvršitelje obrade za pomoć? Planirate li se savjetovati sa stručnjacima za informacijsku sigurnost ili bilo kojim drugim stručnjacima?

Pacijenti očekuju najvišu razinu kvalitet skrbi i najnovija znanstvena dostignuća u liječenju bolesti od sustava javnog zdravstva. Istraživačke aktivnosti naših zdravstvenih ustanova dobro su poznate i javnost je s njima familijarna i generalno pozitivno reagira na sve istraživačke napore usmjerene na unapređenje zdravstvenih usluga, terapije i tretmane, kojih nema bez istraživanja ove vrste.

U pripremi istraživačkih projekata poput ovog redovito se konzultiramo s pravnom službom, odjelom IT usluga i stručnjacima za informacijsku sigurnost.

4. KORAK: PROCJENA POTREBE/PROPORCIONALNOSTI

Opišite mjere usklađenosti i proporcionalnosti: koja je Vaša zakonska osnova za obradu? Postiže li obrada zapravo Vašu svrhu? Postoji li još koji način da se postigne isti ishod? Kako ćete osigurati minimiziranje podataka? Koje ćete informacije dati pojedincima? Kako ćete pomoći u ostvarivanju njihovih prava? Koje mjere poduzimate kako biste osigurali da se izvršitelji obrade pridržavaju mjera? Kako štitite prijenose osobnih podataka prema trećim zemljama i međunarodnim organizacijama?

Pravna osnova za obradu osobnih podataka: 6.1.e: Javna zadaća: obrada je nužna voditelju obrade podataka za obavljanje zadaće od javnog interesa ili za obavljanje službene dužnosti, a zadaća ili funkcija ima jasnu osnovu u zakonu.

Pravna osnova za obradu podataka posebne kategorije: Za obradu podataka NPBP i parteri se oslanjaju na pravnu osnovu: 9.2.g: Obrada je nužna iz razloga značajnog javnog interesa, na temelju prava Unije ili prava države članice koji će biti razmjerni cilju koji se želi postići, poštovati bit prava na zaštitu podataka i predviđati prikladne i posebne mjere za zaštitu temeljnih prava i interesa ispitanika.

Nema drugog načina obzirom na izvor podataka i svrhu obrade. Naši istraživački protokoli uključuju obradu samo najnužnijeg seta podataka.

Ispitanicima se prilikom informiranja o obradi dostavlja obavijest o obradi podataka. NBPB i partneri imaju uhodane standardne procedure za ostvarivanje prava ispitanika. Za eventualne

prijenose podataka izvan EU koristit ćemo ugovore o obradi podataka i standardne ugovorne klauzule odobrene od strane Europskog odbora za zaštitu podataka.

5. KORAK: IDENTIFIKACIJA/PROCJENA RIZIKA

Opišite izvor rizika i prirodu potencijalnog utjecaja na pojedince.	vjerojatnost povrede	ozbiljnost povrede	cjelokupni rizik
1. Neovlašteni pristup podacima putem informacijskih sustava	srednja	visoka	visok
2. Zloupotreba osobnih podataka	srednja	visoka	visok
3. Povreda dostupnosti podataka	srednja	visoka	visok
4. Krađa identiteta ili prijevara	srednja	mala	srednji
5. Ponovna identifikacija pseudonimiziranih osobnih podataka	srednja	visok	visok

KORAK 6: IDENTIFIKACIJA MJERA ZA SMANJENJE RIZIKA

identificirajte dodatne mjere koje biste mogli poduzeti za smanjenje ili uklanjanje rizika identificiranih kao srednji ili visoki rizik u koraku broj 5				
rizik	**Opcije za smanjenje ili uklanjanje rizika**	**Učinak na rizik**	**Preostali rizik**	**Odobrena mjera**
1. Neovlašteni pristup podacima putem informacijskih sustava	1. Pristup svim informacijskim sustavima bit će kontroliran kako bi se osiguralo da samo ovlašteni korisnici imaju pristup sustavu i informacijama kojima su ovlašteni pristupiti. Podatkovni sustavi imaju funkciju revizije koja bilježi pristup korisnika povjerljivim podacima i korištenje tipki. Podaci revizije koristit će se za pregled stvarnih ili potencijalnih povreda/incidenata. Provest će se i rutinska revizija pristupa. Kada više od jednog korisnika pristupa informacijskom sustavu, svaki korisnik tog sustava imat će jedinstven i provjerljiv identitet. Sve transakcije na zajedničkim informacijskim sustavima bit će pripisane osobi koja ih je pokrenula. Svi će računi biti zaštićeni lozinkom: Sve lozinke se mijenjaju jednom u tri mjeseca. Sve lozinke moraju imati najmanje 16 znakova i moraju sadržavati barem jedno	smanjen	Nizak	Da

	od sljedećeg: velika i mala slova, brojeve i simbole. Niti jedna lozinka ili slična se ne može ponoviti unutar godinu dana korištenja. Sustav bilježi prethodne lozinke godinu dana za svakog korisnika radi usklađenosti. Svim podacima pristupat će se putem pristupa zaštićenog lozinkom. Pristup zgradama je putem osobne iskaznice, a zgrade nadzire videonadzor. Poslužitelji se nalaze u klimatiziranim, zaključanim prostorijama kojima pristup ima samo ovlašteno IT osoblje. Pristup zgradi je putem ID kartice i stalno je nadziran videonadzorom, protuprovalnim alarmima i sustavima za detekciju požara. Odvojeni rezervni poslužitelji smješteni su u zasebnoj zgradi s druge strane kompleksa Nacionalne bolnice, na udaljenosti od oko 300 m. Poslužitelji se svakodnevno ažuriraju softverom kako bi se zaštitili od poznatih i novoobjavljenih virusa i zlonamjernog softvera. Poslužitelji bilježe sve pristupe sustavima za svo osoblje, uključujući administratore sustava. Dnevnici revizije su konfigurirani za bilježenje svih radnji poduzetih korištenjem administratorskih ili povišenih povlastica. Svi revizijski zapisnici zaštićeni su od neovlaštenih izmjena. Svaki neovlašteni pristup			

		poslužiteljima na ovoj razini može se otkriti, a račun i korisnik automatski se zamrzavaju. Za poslužitelje se svakodnevno izrađuje sigurnosna kopija i sigurnosne kopije se čuvaju mjesec dana, nakon čega se rutinski i sigurno prepisuju. Poslužitelji usluga mogu se postaviti tako da spriječe neovlašteno elektroničko kopiranje podataka. Ako se to pokuša pristupiti računima i korisniku se automatski zamrzava. Svi korisnici potpisuju korisnički ugovor o povjerljivosti podataka koji zabranjuje neovlašteno kopiranje podataka na bilo koji drugi način.			
2.	Zloupotreba osobnih podataka	2. Svi će podaci biti pseudonimizirani, a identifikatori će biti pohranjeni sigurno i odvojeno od podataka prije nego što budu uništeni.	Smanjen	Nizak	DA
3.	Povreda dostupnosti podataka	Vidjeti pod 1.	Smanjen	Nizak	DA
4.	Krađa identiteta ili prijevara	Svi će podaci biti pseudonimizirani, a identifikatori će biti pohranjeni sigurno i odvojeno od podataka prije nego što budu uništeni.	Smanjen	Nizak	DA
5.	Ponovna identifikacija pseudonimiziranih osobnih podataka	Vidjeti pod 1. i pod 2.	Smanjen	Nizak	DA

KORAK 7: DOKUMENTIRAJTE ISHOD

Stavka	Ime/pozicija/datum	Bilješka (pomoć)
Odobrene mjere:	Predstojnik IT službe	Integracija prepoznatih mjera u postupak obrade
Preostali rizici [5] odobreni od:	Nema	Ako prihvaćate bilo koji preostali visok rizik, konzultirajte AZOP prije nego što nastavite
Pruženi savjet od službenika za zaštitu podataka (DPO):	Hrvoje Bronhić, mag.iur	DPO treba savjetovati o usklađenosti, mjerama iz koraka 6 i o tome može li se obrada nastaviti
Sažetak savjeta koji je DPO pružio: DPO savjetuje koordinacijski sastanak s DPO i voditeljima istraživanja u ostalim voditeljima obrade kako bi se osiguralo da su svi razumjeli i u stanju provesti odabrane zaštitne mjere.		
savjeti DPO prihvaćeni ili odbačeni:	PRIHVAĆENO	Ako se odbaci, morate objasniti svoje razloge
Komentar:		
Odgovore na konzultacije s ispitanicima ili njihovim predstavnicima pregledali:	KONZULTACIJE NISU BILE POTREBNE	Ako Vaša odluka odstupa od stavova pojedinaca, morate objasniti svoje razloge
Komentar:		

Ovaj DPIA će biti pod nadzorom:	Pravna služba IT Služba Hrvoje Bronhić, mag.iur	DPO bi također trebao nadgledati usklađenost procesa s DPIA-om

PROCJENA UČINKA NA ZAŠTITU PODATAKA (eng. DPIA)

DPIA Razvoj algoritam biometrijskog prepoznavanja psihofizičkog stanja

PODACI O VODITELJU OBRADE

Ime	**Medicinskotehnološka kompanija d.o.o.**
Službenik za zaštitu podataka (eng. DPO)	Hrvoje Službenik, dipl. ing
Kontakt voditelja obrade/službenika za zaštitu podataka	dpo@mtkdoo.hr

KORAK 1: IDENTIFICIKACIJA POTREBE

Zašto smatrate da je potrebno provesti postupak procjene učinka na zaštitu podataka?

Cilj projekta je poboljšati točnost razlučivosti lica na Near Infra-Red (NIR) videozapisima lica snimljenih našim medicinskim uređajem

Funkcionalnost prepoznavanja lica koristit će se kao dio sustava za praćenje pacijenata (DMS) dizajniranog za razumijevanje pacijentove pažnje, pospanosti i drugih korisnih informacija u svrhu provođenja liječenja.

Trgovačko društvo Medicinskotehnološka kompanija d.o.o. ubrzano razvija softver koji se koristi u različitim postavkama omogućujući brzo i pouzdano prepoznavanje mentalnog i fizičkog stanja pacijenta.

Podaci koji se koriste u ovoj obradi su biometrijski podaci koji se inače mogu koristiti za identifikaciju pojedinaca, međutim, ova posebna obrada ne koristi biometrijske podatke za identifikaciju pojedinačnih subjekata podataka.

Umjesto toga – koristi biometriju za uvježbavanje algoritma za otkrivanje promjena u ponašanju pacijenata koje ukazuju na neželjeni učinak strojno primijenjenog tretmana.

Ovaj će razvoj u jednom trenutku uključiti veliku obradu osobnih podataka. Voditelj obrade je uzeo u obzir i pridržavao se načela „privacy by design“ od faze konceptualizacije obrade te aktivno radi na osiguravanju najviše moguće razine sigurne i sigurne obrade osobnih podataka.

KORAK 2: OPIŠITE OBRADU[1] OSOBNIH PODATAKA

Opišite prirodu obrade? Kako ćete prikupljati, koristiti, pohranjivati i brisati podatke? Koji je izvor podataka? Hoćete li s nekim dijeliti podatke? Za koje vrste obrade postoji vjerojatnost visokog rizika na zaštitu osobnih podataka?

Podaci se prikupljaju interno korištenjem pravilno postavljenih kamera više izvora i vrsta koje snimaju različite digitalne slikovne sadržaje.

Podaci se pohranjuju na lokalnom poslužitelju u sigurnoj šifriranoj mapi. Ovisno o namjeni skupa podataka, on se pohranjuje na poslužitelj kojemu može pristupiti samo odjel za obuku algoritama. Podaci dolaze iz digitalnog snimanja u sigurnom i kontroliranom okruženju prema specifikacijama utvrđenim istraživačkim projektom.

Izvor podataka

Voditelj obrade podataka prikuplja podatke uključujući osobne podatke pomoću alata za video snimanje. Podaci se prikupljaju analizom digitalne fotografije različitim metodama digitalne analize i strojnim učenjem.

Dijeljenje podataka

Tvrtka prikuplja, obrađuje i pohranjuje podatke sama, lokalno. Osobni podaci korišteni u ovoj obradi neće se prenositi trećim stranama.

Identificiranje potencijalnih rizika

Potencijalni rizici za prava i slobode ispitanika mogu uključivati nemogućnost subjekta podataka da ostvari prava uključujući prava na zaštitu osobnih podataka, gubitak povjerljivosti, krađu identiteta ili prijevaru.

Osim toga, prikupljene podatke teoretski može usporediti nezakoniti akter s drugim podacima kako bi se otkrilo ponašanje korisnika i potencijalno podaci koji su prepoznati kao podaci posebne kategorije.

Opišite opseg obrade: koja je priroda podataka i uključuju li podaci posebne kategorije ili obradu osobnih podataka koji se odnose na kaznene osude i kažnjiva djela? Na koji period ćete pohraniti podatke? O kojem broju pojedinaca se radi te koje teritorijalno područje obuhvaća?

Priroda podataka

Osobni podaci koji se obrađuju su slike i videozapisi, koji su upareni s datotekom koja može sadržavati podatke o dobi, spolu, izrazu lica, položaju glave, rotaciji glave, kao i koordinate orijentira lica za dano lice na slici.

Podaci nisu posebna kategorija podataka jer se unatoč snimanju lica ispitanika, obrada ne vodi s ciljem zaključivanja o kategorijama poput rasne odnosno etničke pripadnosti niti upotrebe biometrijskog podatka u svrhu konkretne identifikacije ispitanika, već s ciljem hranjenja postupka strojnog učenja/treniranja algoritma koji služi drugoj funkciji – detekciji psihofizičke reakcije.

Opseg, opseg i trajanje obrade

Podaci se sastoje od prosječno 100 videozapisa od 20 sekundi po subjektu, što daje 2000 sekundi videa ili 60 000 slika koje sadrže lice subjekta. Podaci će se čuvati 6 mjeseci, a bit će cca. Pogođeno je 10 000 osoba.

Opišite kontekst obrade: kakva je priroda Vašeg odnosa s pojedincima? Koliku će kontrolu nad obradom imaju pojedinci imati? Bi li očekivali da na taj način koristite njihove podatke? Uključuje li obrada podatke djece ili druge ranjive[2] skupine? Postoje li prethodne zabrinutosti zbog ove vrste obrade ili sigurnosni nedostatci? Postoje li u trenutku obrade pitanja od javnog interesa koja biste trebali ubrojiti? Postoji li odobreni kodeks ponašanja ili sustav certificiranja u Vašem poslovnom subjektu?

Kontrola korisnika/subjekta podataka nad podacima i odnos s voditeljem obrade podataka

Podaci se primarno prikupljaju i obrađuju korištenjem uređaja za video snimanje. Ispitanici su volonteri koji su potpisali ugovor kao temelj obrade.

Ispitanici će biti odgovarajuće obaviješteni o svrsi, prirodi i načinima obrade putem obavijesti o privatnosti koja je dostupna ovdje:

(poveznica na obavijest o obradi)

Obrada podataka o djeci/maloljetnicima

Ispitanici ne uključuju djecu, stoga se ne obrađuju osobni podaci koji pripadaju djeci ili maloljetnicima.

Sigurnost i sigurnost obrade

Voditelj obrade provodi redovite revizije informacijske sigurnosti. Sigurnost i sigurnost obrade svih vrsta podataka je od najveće važnosti za voditelja obrade podataka.

U tu svrhu tvrtka je usvojila politike - politike informacijske sigurnosti i sigurne obrade osobnih podataka dostupne ovdje:

(poveznica na politiku informacijske sigurnosti)

(poveznica na internu politiku privatnosti)

Tvrtka koristi najsuvremeniju tehnologiju šifriranja kako bi smanjila rizik od povrede podataka i pažljivo odvagnula potrebu za prikupljanjem i obradom osobnih podataka u odnosu na rizike za ispitanike

Opišite svrhe obrade: što želite postići? Koji je predviđeni učinak na pojedince? Koje su prednosti obrade - za vas i šire?

Svrha obrade

Svrha obrade je osposobiti algoritam strojnog učenja za poboljšanje računalno potpomognutog razumijevanja statusa pacijenta koji prima automatizirani strojni tretman.

Učinak na pojedince

Voditelj obrade podataka ne predviđa štetne učinke na pojedince na temelju prirode obrade (istraživanje i razvoj u sigurnim laboratorijskim uvjetima) i primijenjenih tehničkih i organizacijskih mjera zaštite.

Prednosti obrade

Ova tehnologija, ako se uspješno razvije, omogućit će širu primjenu strojnog ili potpomognutog liječenja pacijenata.

KORAK 3: SAVJETOVANJE

Kako ćete se posavjetovati s relevantnim dionicima: opišite kada i kako ćete upitati za stavove ispitanika[3] ili njihovih predstavnika – ili obrazložite zašto to nije prikladno. Koga još trebate uključiti u proces iz Vašeg poslovnog subjekta? Postoji li potreba da zamolite izvršitelje obrade za pomoć? Planirate li se savjetovati sa stručnjacima za informacijsku sigurnost ili bilo kojim drugim stručnjacima?

Konzultacije s dionicima (udjelničarima?)

Voditelj obrade podataka trenutno još uvijek testira i razvija tehnologiju prepoznavanja koja je predmet ove procjene, provodeći odgovarajuću kontrolu nad korisničkim podacima i osiguravajući sigurnu i sigurnu obradu te pravovremeno rješavanje svih potencijalnih problema u vezi s obradom osobnih podataka.

Integrirana i tehnička zaštita podataka (PBD&D)

U projekt su od samog početka uključeni interni stručnjaci za informacijsku sigurnost, pravna služba i DPO.

4. KORAK: PROCJENA POTREBE/PROPORCIONALNOSTI

Opišite mjere usklađenosti i proporcionalnosti: koja je Vaša zakonska osnova za obradu? Postiže li obrada zapravo Vašu svrhu? Postoji li još koji način da se postigne isti ishod? Kako ćete osigurati minimiziranje podataka? Koje ćete informacije dati pojedincima? Kako ćete pomoći u ostvarivanju njihovih prava? Koje mjere poduzimate kako biste osigurali da se izvršitelji obrade pridržavaju mjera? Kako štitite prijenose osobnih podataka prema trećim zemljama i međunarodnim organizacijama?

Pravna osnova za obradu

Svrha obrade prvenstveno je obrada podataka koja je nužna voditelju obrade za istraživanje i razvoj bolje, pouzdanije tehnologije analize statusa pacijenta.

Obrada se temelji na odredbama ugovora između voditelja obrade podataka i ispitanika koji je dostupan ovdje:

poveznica na primjer ugovora

Svrha obrade

Cilj projekta je poboljšati točnost razlučivosti lica na Near Infra-Red (NIR) videozapisima lica snimljenih našim medicinskim uređajem. Funkcionalnost prepoznavanja lica koristit će se kao dio sustava za praćenje pacijenata (DMS) dizajniranog za razumijevanje pacijentove pažnje, pospanosti i drugih korisnih informacija u svrhu provođenja liječenja.

Kvaliteta podataka i minimizacija podataka

Prikupljaju se samo nužni podaci za treniranje algoritma.

Obavijest o obradi

Korisnici/ispitanici se putem obavijesti o obradi obavještavaju o opsegu obrade, kategorijama osobnih podataka koji se obrađuju i drugim informacijama koje zahtijeva OUZP.

Ostvarivanje prava ispitanika

Kontrolor podataka ima ugovorne obveze s subjektima podataka kako bi olakšao ostvarivanje njihovih prava ispitanika.

Sukladnost izvršitelja

Voditelj obrade podataka neće angažirati nikakve obrađivače u svrhu ove obrade.

Međunarodni transferi

Voditelj obrade podataka neće prenositi nikakve osobne podatke trećim zemljama ili organizacijama izvan EU.

5. KORAK: IDENTIFIKACIJA/PROCJENA RIZIKA

Opišite izvor rizika i prirodu potencijalnog utjecaja na pojedince.	vjerojatnost povrede	ozbiljnost povrede	ukupni rizik
1. Nemogućnost ostvarivanja prava uključujući i pravo na zaštitu osobnih podataka	Slaba	Minimalna	Slab
2. Gubitak kontrole nad korištenjem osobnih podataka	Slaba	Minimalna	Slab
3. Gubitak povjerljivosti	Slaba	Srednja	Srednji
4. Krađa identiteta ili prijevara	Slaba	Visoka	Srednji
5. Ponovna identifikacija pseudonimiziranih osobnih podataka	Slaba	Srednja	Srednji

[3] trebi od ispitanika ili njihovih predstavnika traži mišljenje (članak 35. stavak 9. GDPR)

KORAK 6: IDENTIFIKACIJA MJERA ZA SMANJENJE RIZIKA

Identificirajte dodatne mjere koje biste mogli poduzeti za smanjenje ili uklanjanje rizika identificiranih kao srednji ili visoki rizik u koraku broj 5

rizik	Opcije za smanjenje ili uklanjanje rizika	Učinak na rizik	Preostali rizik	Odobrena mjera
	Redovito održavanje sustava, backup podataka	Smanjen	Nizak	Da
	Redovito održavanje sustava, backup podataka, enkripcija podataka, kontrola pristupa	Smanjen	Nizak	Da
	Redovito održavanje sustava, backup podataka, enkripcija podataka, kontrola pristupa	Smanjen	Nizak	Da
	Redovito održavanje sustava, backup podataka, enkripcija podataka, kontrola pristupa	Smanjen	Nizak	Da
	Redovito održavanje sustava, backup podataka, enkripcija podataka, kontrola pristupa	Smanjen	Nizak	Da

KORAK 7: DOKUMENTIRAJTE ISHOD

Stavka	Ime/pozicija/datum	Bilješka (pomoć)
Odobrene mjere:		Integracija prepoznatih mjera u postupak obrade
Preostali rizici * odobreni od:		Ako prihvaćate bilo koji preostali visok rizik, konzultirajte AZOP prije nego što nastavite

Pruženi savjet od službenika za zaštitu podataka (DPO):	Hrvoje Službenik, dipl. ing	DPO treba savjetovati o usklađenosti, mjerama iz koraka 6 i o tome može li se obrada nastaviti
Sažetak savjeta koji je DPO pružio: Upotreba enkripcije i kontrole pristupa, može se nastaviti obrada		
savjeti DPO prihvaćeni ili odbačeni:	Prihvaćeni	Ako se odbaci, morate objasniti svoje razloge
Komentar:		
Odgovore na konzultacije s ispitanicima ili njihovim predstavnicima pregledali:	Hrvoje Službenik, dipl. ing	Ako Vaša odluka odstupa od stavova pojedinaca, morate objasniti svoje razloge
Komentar: Ispitanike je zanimao proces obrade, objašnjen prilikom sklapanja ugovora.		
Ovaj DPIA će biti pod nadzorom:	DPO Pravna služba R&D team lead	DPO bi također trebao nadgledati usklađenost procesa s DPIA-om

Zaključno o DPIA

- DPIA/Procjena učinka je važan mehanizam osiguranja sukladnosti s Uredbom
- Jedan od najvažnijih mehanizama usklađenosti
- Još jedan dokaz povezanosti informacijske sigurnosti i zaštite osobnih podataka
- Zahtjeva organizacijski i tehnički know-how
- Nužan input službenika za zaštitu podataka, ako postoji
- Odaberite službenika s adekvatnim kompetencijama!

Primjeri tehničkih i organizacijskih mjera

- Pseudonimizacija osobnih podataka
- Pružanje informacija o pohrani osobnih podataka
- Omogućavanje ispitanicima da utječu na obradu
- Uspostava sustava za detekciju zlonamjernog softvera
- Pohrana dostupnih osobnih podataka u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu
- Osposobljavanje zaposlenika o osnovnoj „kiberhigijeni”
- Ugovorno obvezivanje izvršitelja obrade
- Utvrđivanje sustava za upravljanje zaštitom podataka i sigurnošću informacija

Primjeri tehničkih i organizacijskih mjera

Kontrole odabrane kako bi se osigurala usklađenost s temeljnim načelima

- Kontrole koje jamče proporcionalnost i nužnost obrade
- Svrha(e): navedena, eksplicitna i legitimna
- Osnova: zakonitost obrade, zabrana zlouporabe
- Minimiziranje podataka: primjereno, relevantno i ograničeno
- Kvaliteta podataka: točni i ažurni
- Trajanje skladištenja: ograničeno

Kontrole za zaštitu prava ispitanika

- Informacije za nositelje podataka (poštena i transparentna obrada)
- Dobivanje suglasnosti
- Ostvarivanje prava na pristup i prava na prenosivost podataka
- Ostvarivanje prava na ispravak i brisanje
- Ostvarivanje prava na ograničenje obrade i prava na prigovor
- Izvršitelji: identificirani i uređeni ugovorom
- Prijenosi: usklađenost s obvezama koje se odnose na prijenos podataka izvan Europske unije

Implementirane kontrole za tretiranje rizika povezanih sa sigurnošću podataka

- Procjena
- Šifriranje
- Anonimizacija
- Particioniranje podataka (u odnosu na ostatak informacijskog sustava)
- Logička kontrola pristupa
- Sljedivost (bilježenje)
- Praćenje integriteta
- Arhiviranje
- Sigurnost papirnatih dokumenata

Opće sigurnosne kontrole u vezi sa sustavom u kojem se obrada provodi

Radna sigurnost
Suzbijanje zlonamjernog softvera
Upravljanje radnim stanicama
Sigurnost web stranice
Sigurnosne kopije
Održavanje
Sigurnost računalnih kanala (mreža)
Praćenje
Fizička kontrola pristupa
Sigurnost hardvera
Izbjegavanje izvora rizika
Zaštita od neljudskih izvora rizika

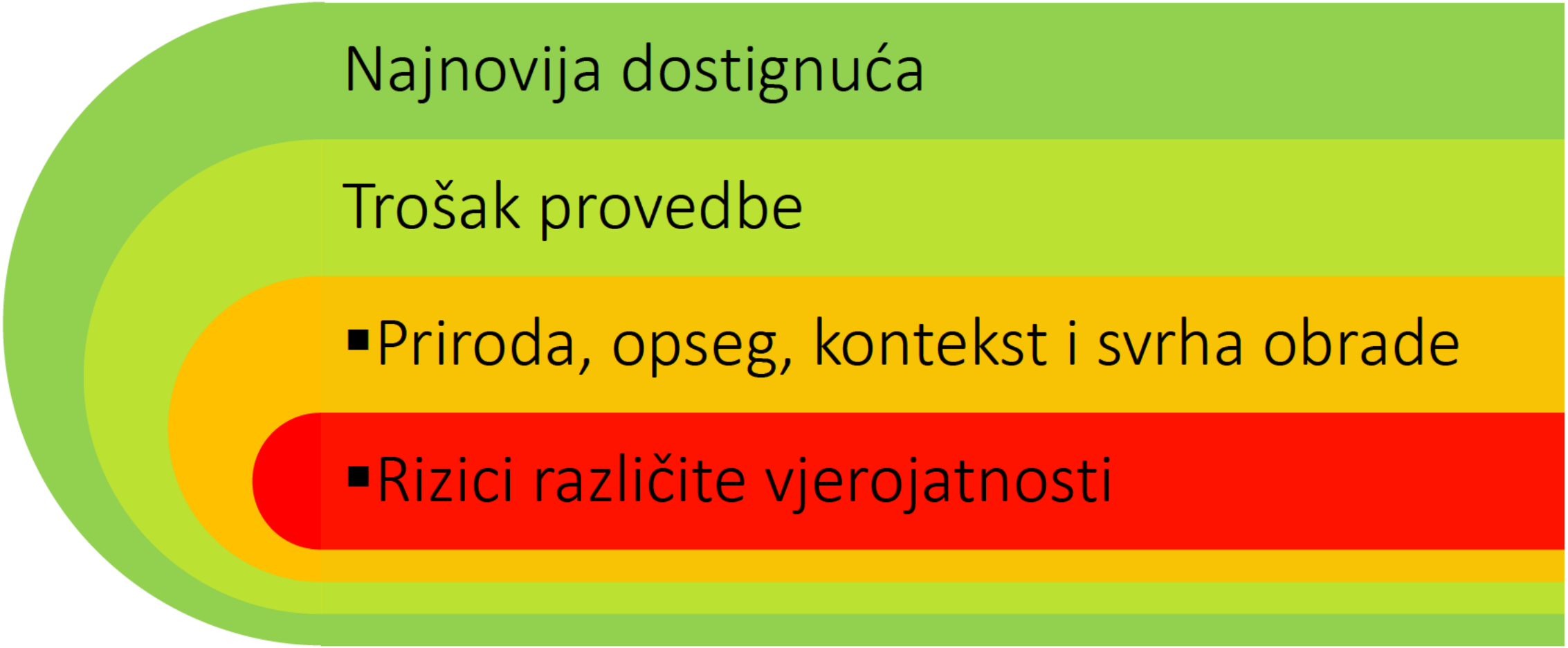
Organizacijske kontrole (upravljanje)

Organizacija
Politika (upravljanje pravilima)
Upravljanje rizicima
Upravljanje projektima
Upravljanje incidentima i povredama podataka
Upravljanje osobljem
Odnosi s trećim stranama
Nadzor

Tehnička i integrirana zaštita podataka

- Voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere koje su osmišljene radi provedbe načela zaštite podataka
- Voditelji obrade dužni su integrirati zaštitne mjere u obradu kako bi se zaštitila prava i slobode ispitanika
- Mjere trebaju biti „odgovarajuće” kako bi se postigla „učinkovita” zaštita podataka

Data protection by design – tehnička zaštita podataka



Integrirana zaštita podataka – Data protection by default (čl. 25.2)

- "Zadana vrijednost”, odnosi se na već postojeću ili unaprijed odabranu vrijednost konfigurabilne postavke koja je dodijeljena softverskoj aplikaciji, računalnom programu ili uređaju.
- Takve se postavke također nazivaju "unaprijed postavljene" ili "tvorničke postavke", posebno za elektroničke uređaje.
- „Prema zadanim postavkama” pri obradi osobnih podataka, odnosi se na izbore u vezi konfiguracijskih vrijednosti ili opcija obrade koje su postavljene ili propisane u sustavu obrade, kao što je softverska aplikacija, usluga ili uređaj ili postupak ručne obrade koji utječe na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje njihove pohrane i njihovu dostupnost.
- Obveza voditelja obrade odabrati takve izbore koji će omogućiti obradu osobnih podataka u skladu s načelima obrade osobnih podata (čl. 5 Uredbe)

Transparentnost

Ključni tehnički i integrirani elementi transparentnosti mogu biti sljedeći:

- **Jasnoća** – informacije moraju biti jasne i jednostavno sročene, kratke i razumljive.
- **Semantika** – priopćenje bi za predmetnu publiku trebalo imati jasno značenje.
- **Dostupnost** – informacije moraju ispitaniku biti lako dostupne.
- **Kontekstualnost –** informacije bi se trebale dostaviti u odgovarajućem trenutku i u odgovarajućem obliku.
- **Relevantnost** – informacije bi trebale biti relevantne i primjenjive na određenog ispitanika.
- **Univerzalni dizajn** – informacije moraju biti dostupne svim ispitanicima, uključivati uporabu strojno čitljivih jezika kako bi se olakšale i automatizirale čitljivost i jasnoća.
- **Razumljivo** – ispitanici bi trebali dobro razumjeti ono što mogu očekivati u vezi s obradom svojih osobnih podataka, posebno kada su ispitanici djeca ili druge ranjive skupine.
- **Dostupnost putem više kanala** – informacije bi se trebale dostavljati različitim kanalima i u različitim medijima, a ne samo u tekstnom obliku, kako bi se povećala vjerojatnost da će informacije uspješno doći do ispitanika.
- **Slojevit pristup** – struktura informacija trebala bi biti višeslojna kako bi one istodobno bile potpune i razumljive te ispunile razumna očekivanja ispitanika.

Poštenost

Poštenost je sveobuhvatno načelo kojim se zahtijeva da se osobni podatci ne obrađuju na način koji je neopravdano štetan, nezakonito diskriminirajući, neočekivan ili obmanjujući za ispitanika.

Ključni tehnički i integrirani elementi poštenosti mogu biti sljedeći:

• **Nediskriminacija** – voditelj obrade ne smije nepošteno diskriminirati ispitanike.

• **Neiskorištavanje** – voditelj obrade ne bi smio iskorištavati potrebe ili ranjivost ispitanika.

• **Odabir potrošača** – voditelj obrade ne smije nepošteno „zaključati" svoje korisnike. Ako je riječ o vlasničkoj usluzi obrade osobnih podataka, može nastati učinak zaključavanja u okviru te usluge, što može biti nepošteno ako se time ispitanicima onemogućuje da ostvaruju svoje pravo prenosivosti podataka u skladu s člankom 20.

• **Ravnoteža moći** – ravnoteža moći trebala bi biti ključan cilj odnosa između voditelja obrade i ispitanika. Trebalo bi izbjegavati svaki oblik neravnoteže moći. Kad to nije moguće, trebalo bi je prepoznati i poduzeti odgovarajuće protumjere.

• **Zabrana prijenosa rizika** – voditelji obrade ne smiju na ispitanike prenositi rizike povezane s poduzećem.

• **Zabrana obmanjivanja** – informacije o obradi podataka i mogućnosti za njihovu obradu trebale bi se iznositi na objektivno i neutralno, tako da se izbjegne svaka vrsta obmanjujućeg ili manipulativnog jezika ili dizajna.

• **Poštovanje prava** – voditelj obrade mora poštovati temeljna prava ispitanika i provoditi odgovarajuće mjere i zaštitne mjere. U ta se prava ne smije zadirati ako to nije izričito opravdano zakonom.

• **Etičnost** – voditelj obrade trebao bi sagledati širi utjecaj obrade na prava i dostojanstvo pojedinaca.

• **Istinitost** – voditelj obrade mora staviti na raspolaganje informacije o načinu na koji obrađuje osobne podatke. Trebao bi postupati kako je predvidio i ne smije obmanjivati ispitanike.

• **Ljudska intervencija** – voditelj obrade mora uključiti kvalificiranu ljudsku intervenciju kojom se mogu otkriti potencijalne pristranosti strojeva u skladu s pravom ispitanika na to da ne podliježu automatiziranom pojedinačnom donošenju odluka iz članka 22

Ograničenje svrhe

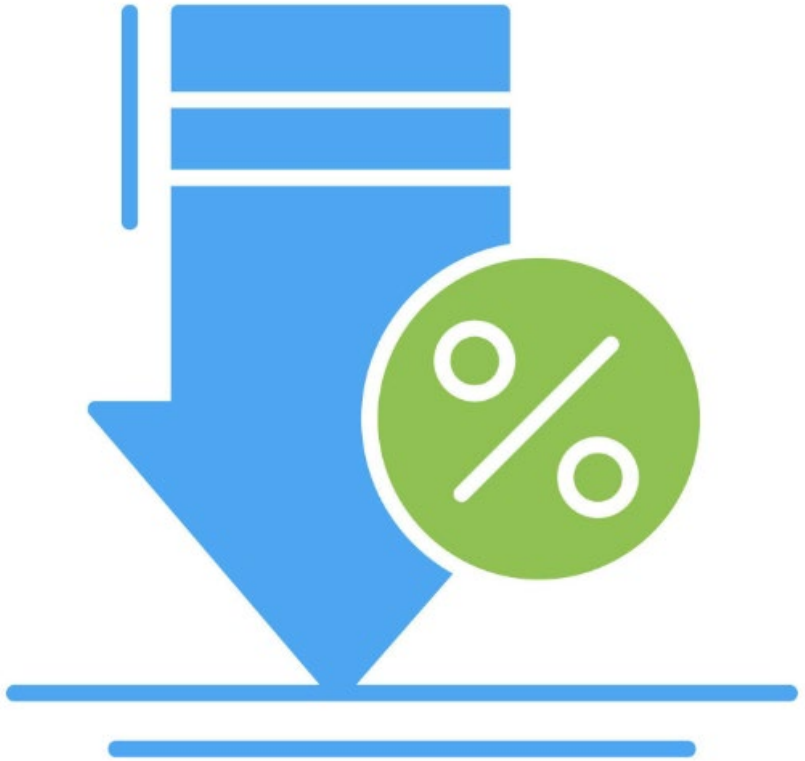
Ključni tehnički i integrirani elementi ograničavanja svrhe mogu biti sljedeći:

- **Prethodno utvrđivanje** – zakonite svrhe moraju se utvrditi prije osmišljavanja obrade.
- **Posebnost** – svrhe obrade osobnih podataka moraju biti posebno i izričito navedene.
- **Usmjerenost na svrhu** – svrha obrade trebala bi usmjeravati strukturu obrade i na njoj bi se trebale temeljiti granice obrade.
- **Nužnost**– na temelju svrhe određuje se koji su osobni podatci potrebni za obradu.
- **Kompatibilnost** – svaka nova svrha mora biti u skladu s izvornom svrhom za koju su podatci prikupljeni te se na njoj moraju temeljiti relevantne promjene u strukturi.
- **Ograničenje daljnje obrade** – voditelj obrade ne bi trebao povezivati skupove podataka ili obavljati daljnju obradu za nove neusklađene svrhe.
- **Ograničenja ponovne uporabe** – voditelj obrade trebao bi upotrebljavati tehničke mjere, uključujući raspršeno adresiranje (eng. hashing) i šifriranje kako bi ograničio mogućnost prenamjene osobnih podataka. Voditelj obrade trebao bi imati uspostavljene i organizacijske mjere, kao što su politike i ugovorne obveze, kojima se ograničava ponovna uporaba osobnih podataka.
- **Preispitivanje** – voditelj obrade trebao bi redovito preispitivati je li neka obrada potrebna u svrhe za koje su podatci prikupljeni i ispitivati strukturu u odnosu na ograničavanje svrhe.

Smanjenje količine podataka

Ključni tehnički i integrirani elementi smanjenja količine podataka mogu biti sljedeći:

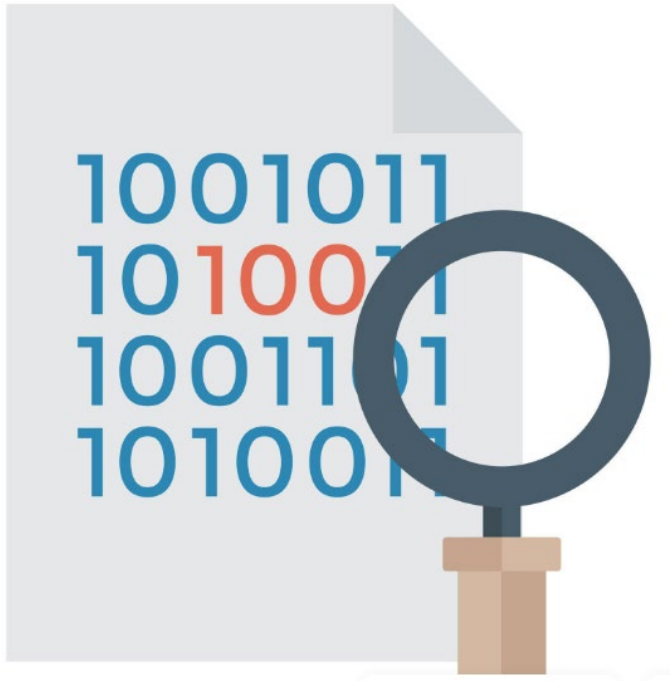
- **Izbjegavanje podataka** – izbjegavajte obradu osobnih podataka kada god je to moguće u relevantnu svrhu.
- **Ograničavanje** – ograničite količinu prikupljenih osobnih podataka na onu koja je nužna za tu svrhu.
- **Ograničenje pristupa** – organizirajte obradu podataka tako da minimalan broj osoba treba pristup osobnim podatcima za izvršavanje svojih dužnosti te u skladu s time ograničite pristup.
- **Relevantnost** – osobni podatci trebali bi biti relevantni za predmetnu obradu, a voditelj obrade trebao bi moći dokazati tu relevantnost.
- **Nužnost** – svaka kategorija osobnih podataka potrebna je u određene svrhe i treba se obrađivati samo ako tu svrhu nije moguće ostvariti drugim sredstvima.
- **Agregiranje** – kada je to moguće, upotrijebite agregirane podatke.
- **Pseudonimizacija** – pseudonimizirajte osobne podatke čim više nije potrebno imati osobne podatke kojima se omogućuje izravno utvrđivanje identiteta pojedinaca i odvojeno pohranjujte identifikacijske ključeve.
- **Anonimizacija i brisanje** – ako osobni podatci nisu potrebni ili nisu više potrebni u tu svrhu, osobni podatci anonimiziraju se ili brišu.
- **Najnovija dostignuća** – voditelj obrade trebao bi primijeniti suvremene i prikladne tehnologije za izbjegavanje podataka i smanjenje količine podataka.



Točnost

Ključni tehnički i integrirani elementi točnosti mogu biti sljedeći:

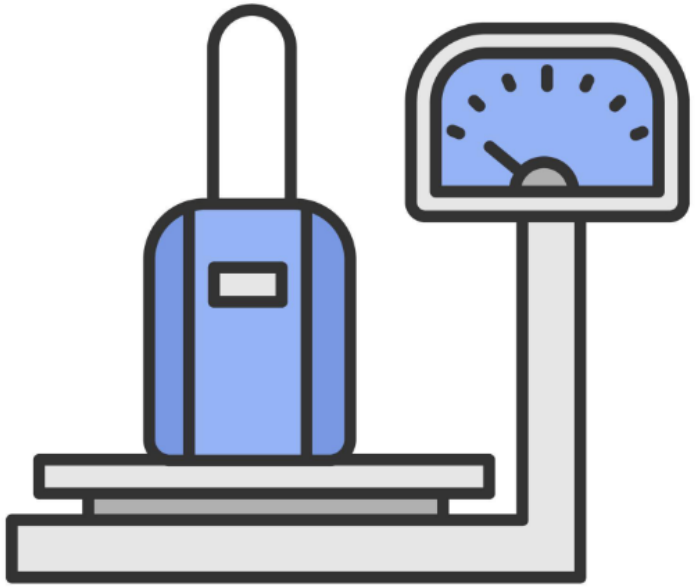
- **Izvor podataka** – izvori osobnih podataka trebali bi biti pouzdani u smislu točnosti podataka.
- **Stupanj točnosti** – svaki element osobnih podataka trebao bi biti onoliko točan koliko je potrebno za određene svrhe.
- **Mjerljiva točnost** – mora se smanjiti količina lažno pozitivnih/negativnih rezultata, na primjer, zbog pristranosti u sklopu automatiziranog donošenja odluka i umjetne inteligencije.
- **Provjera** – ovisno o prirodi podataka i o tome koliko se često ti podatci mogu promijeniti, voditelj obrade trebao bi prije obrade i u različitim fazama obrade s ispitanikom provjeriti točnost osobnih podataka (npr. zahtjevi u pogledu starosne dobi).
- **Brisanje/ispravak** – voditelj obrade mora bez odlaganja izbrisati ili ispraviti netočne podatke. Voditelj obrade mora taj postupak posebno olakšati ako su ispitanici djeca i ako oni naknadno žele ukloniti takve osobne podatke.
- **Izbjegavanje propagacije pogrešaka** – voditelji obrade trebali bi ublažiti učinak akumulirane pogreške u lancu obrade.
- **Pristup** – ispitanicima bi trebalo dostaviti informacije o osobnim podatcima i omogućiti učinkovit pristup takvim podatcima u skladu s člancima 12. i 15. Opće uredbe o zaštiti podataka kako bi mogli nadzirati njihovu točnost i ispraviti ih prema potrebi.
- **Kontinuirana točnost** – osobni podatci trebali bi biti točni u svim fazama obrade, a ispitivanja točnosti trebala bi se provoditi tijekom kritičnih koraka.
- **Ažurnost** – osobni se podatci ažuriraju ako je to potrebno za određenu svrhu.



Ograničenje pohrane

Ključni tehnički i integrirani elementi ograničenja pohrane mogu biti sljedeći:

- **Brisanje i anonimizacija** – voditelj obrade trebao bi imati uspostavljene jasne interne postupke i funkcije za brisanje i/ili anonimizaciju.
- **Učinkovitost anonimizacije/brisanja** – voditelj obrade mora se pobrinuti da nije moguće ponovno prepoznati anonimizirane podatke ili obnoviti izbrisane podatke te bi trebao ispitati je li to moguće
- **Automatizacija** – brisanje određenih osobnih podataka trebalo bi biti automatizirano.
- **Kriteriji pohrane** – voditelj obrade mora odrediti koji su podatci i trajanje pohrane potrebni za određenu svrhu.
- **Obrazloženje** – voditelj obrade trebao bi moći obrazložiti zašto je određeno razdoblje pohrane nužno za predmetnu svrhu i predmetne osobne podatke te moći iznijeti razlog i pravnu osnovu za razdoblje zadržavanja.



Cjelovitost i povjerljivost

Ključni tehnički i integrirani elementi cjelovitosti i povjerljivosti mogu biti sljedeći:

• Sustav upravljanja informacijskom sigurnošću– uspostavljena su operativna sredstva za upravljanje politikama i postupcima za informacijsku sigurnost.

• Analiza rizika– procijenite rizike za sigurnost osobnih podataka tako da razmotrite učinak na prava pojedinaca i poduzmete mjere za suzbijanje utvrđenih rizika. Kad je riječ o primjeni u procjeni rizika, izradite i održavajte sveobuhvatan, sustavan i realan „model za utvrđivanje prijetnji" i analizu površine napada u okviru za to izrađenog softvera kako biste smanjili vektore napada i mogućnosti za iskorištavanje slabosti i ranjivosti.

• Tehnička sigurnost– što prije razmotrite sigurnosne zahtjeve u pogledu dizajna i razvoja sustava te kontinuirano integrirajte i provodite odgovarajuća ispitivanja.

• Održavanje – redovito preispitujte i ispitujte softver, hardver, sustave i usluge itd. kako biste otkrili slabosti sustava koji služe kao pomoć pri obradi.

• Upravljanje kontrolom pristupa – pristup osobnim podatcima trebalo bi imati samo ovlašteno osoblje koje tim podatcima treba pristupiti radi obavljanja zadaća povezanih s obradom, a voditelj obrade trebao bi razlikovati različite vrste povlaštenog pristupa za ovlašteno osoblje.

• Sigurni prijenosi – prijenosi se moraju zaštititi od neovlaštenog i slučajnog pristupa i promjena.

• Sigurna pohrana – pohrana podataka mora biti sigurna od neovlaštenog pristupa i promjena. Trebali bi biti uspostavljeni postupci za procjenu rizika povezanih s centraliziranim i decentraliziranim sustavom pohrane te kategorija osobnih podataka na koje se to primjenjuje. Na neke će podatke možda trebati primijeniti dodatne sigurnosne mjere ili će se ti podatci trebati odvojiti od ostalih. Pseudonimizacija – osobni podatci i sigurnosne kopije/zapisi trebali bi se pseudonimizirati kao sigurnosna mjera za svođenje rizika od mogućih povreda podataka na najmanju moguću mjeru, na primjer upotrebom raspršivanja ili šifriranja.

• Sigurnosne kopije/zapisi – zadržavanje sigurnosnih kopija i zapisa ako su potrebni za informacijsku sigurnost; upotreba revizijskih tragova i praćenje događaja kao rutinska sigurnosna kontrola. One se moraju zaštititi od neovlaštenog i slučajnog pristupa i promjena te redovito preispitivati, a svi bi se incidenti trebali odmah rješavati.

• Oporavak u slučaju katastrofe / kontinuitet poslovanja – odgovorite na zahtjeve informacijskog sustava u pogledu oporavka u slučaju katastrofe / kontinuiteta poslovanja kako biste ponovno uspostavili dostupnost osobnih podataka nakon velikih incidenata.

• Zaštita u skladu s rizikom – sve kategorije osobnih podataka trebale bi se zaštititi prikladnim mjerama s obzirom na rizik povrede sigurnosti. Podatci koji su podložni posebnim rizicima trebali bi se, kad je to moguće, čuvati odvojeno od ostalih osobnih podataka.

• Upravljanje odgovorima na sigurnosne incidente – uspostavite rutine, postupke i resurse za otkrivanje i suzbijanje povreda podataka, njihovo rješavanje, izvješćivanje o njima i učenje na temelju njih.

• Upravljanje incidentima – voditelj obrade trebao bi uspostaviti postupke za rješavanje povreda i incidenata, kako bi sustav za obradu bio otporniji. To uključuje postupke obavješćivanja kao što je upravljanje obavijestima (za nadzorno tijelo) i informacijama (za ispitanike).

Preporuke EDPB

- Voditelji obrade trebali bi uzeti u obzir zaštitu podataka od početnih faza planiranja obrade, čak i prije utvrđivanja načina obrade
- Ako voditelj obrade ima svojeg službenika za zaštitu podataka, Europski odbor za zaštitu podataka potiče aktivno sudjelovanje tog službenika u uključivanju tehničke i integrirane zaštite podataka u postupke nabave i izrade te u cijeli životni ciklus obrade.
- Postupak obrade moći će se certificirati
- Proizvođači i izvršitelji obrade trebali bi nastojati olakšati provedbu načela tehničke i integrirane zaštite podataka kako bi se poduprla sposobnost voditelja obrade za ispunjavanje obveza iz članka 25.
- S druge strane, voditelji obrade ne bi trebali odabrati proizvođače ili izvršitelje obrade koji ne nude sustave koji voditeljima obrade omogućuju usklađivanje s člankom 25.

Nadzorna tijela i Privacy by Design/Default

- Nadzorna tijela mogu procijeniti usklađenost s člankom 25. u skladu s postupcima navedenima u članku 58.
- Korektivne ovlasti navedene su u članku 58. stavku 2. i uključuju izdavanje upozorenja, službenih opomena, naloga za poštovanje prava ispitanika, ograničenja ili zabrane obrade, upravne novčane kazne itd.
- **Dodatni čimbenik u određivanju iznosa novčanih kazni za povrede Opće uredbe o zaštiti podataka jest tehnička i integrirana zaštita podataka**; vidjeti članak 83. stavak 4

Imenovanje službenika

Obrazac služi za podnošenje izjave o imenovanju službenika za zaštitu osobnih podataka unutar Vaše organizacije Agenciji za zaštitu osobnih podataka. Službenik za zaštitu podataka obavezno se imenuje u slučajevima propisanim **člankom 37. stavkom 1. Opće uredbe o zaštiti podataka. Možete imenovat službenika za zaštitu podataka dobrovoljno, čak i ako to niste obavezni.** Međutim, u tom slučaju važno je istaknuti da se isti zahtjevi iz Opće uredbe o zaštiti podataka primjenjuju kao i u slučaju kad je voditelj ili izvršitelj obrade u obvezi imenovati službenika za zaštitu podataka. Nakon što ispunite i pošaljete obrazac, primit ćete obavijest o primitku. **Sve rubrike u obrascu potrebno je ispravno ispuniti, a navedeni podaci moraju biti točni.** Više o obradi osobnih podataka službenika za zaštitu podataka u Agenciji za zaštitu osobnih podataka možete pronaći ovdje: https://azop.hr/politika-privatnosti/.

OBRAZAC ZA IMENOVANJE SLUŽBENIKA ZA ZAŠTITU PODATAKA

OBAVJEŠTAVAM AZOP O IMENOVANJU SLUŽBENIKA ZA ZAŠTITU PODATAKA *

- ○ Prvi put
- ○ Službenik za zaštitu podataka je već imenovan, želim unijeti izmjene

Organizacija koja obavještava AZOP o imenovanju službenika za zaštitu podataka je:

- ☐ tijelo javne vlasti (ministarstvo, tijelo državne uprave, jedinica lokalne i regionalne samuprave)
- ☐ bolnica/poliklinika ili neka druga organizacija iz zdravstvenog sektora
- ☐ škola/dječji vrtić
- ☐ mikro, malo, srednje poduzeće ili obrt
- ☐ javno poduzeće
- ☐ udruga
- ☐ nešto drugo (navedite što)

Naznaka radi li se o službeniku za zaštitu podataka kod: *

- ○ Voditelja obrade
- ○ Izvršitelja obrade

Naziv voditelja ili izvršitelja obrade: *

Matični broj subjekta: *

DPO - Odabir, kompetencije, položaj, zadaci

- Koje kvalifikacije treba imati SZOP u zdravstvenoj organizaciji?
- Kakva je pozicija (radno mjesto) SZOP u zdravstvenoj ustanovi?
- Koji su zadaci i obveze SZOP?
- Kako spriječiti sukob interesa
- Kako podići i održavati kompetencije službenika?

Koja zdravstvena organizacija treba imenovati službenika

- Klinički bolnički centri - da
- Opće bolnice - da
- Specijalne bolnice - da
- Domovi zdravlja - da
- Zavodi, instituti i druge ustanove - da
- Laboratoriji - da
- Ljekarne i privatne poliklinike -
- Klinike i ordinacije liječnika pojedinaca - ne

Kriteriji:

Veliki obujam obrade: u odnosu na broj ispitanika
- količina podataka o ispitaniku ili raznovrsnost/razni tipovi podataka
- trajanje obrade
- teritorij/geografsko područje obrade

Kvalifikacije?

- Službenik za zaštitu podataka imenuje se na temelju stručnih kvalifikacija:
- Osobito, stručno znanje o pravu i praksama na području zaštite podataka
- *Stručnjaci na području nacionalnog i europskog prava koji dubinski razumiju Uredbu*
- *Poznavanje sektora aktivnosti i poslovnih procesa organizacije voditelja obrade*
- *Dobro razumijevanje postupaka, informacijskih sustava voditelja i informacijske sigurnosti*
- Sposobnost izvršavanja zadaća iz članka 39. Uredbe
- *Poštenje, profesionalna etika*

Adekvatna razina stručnosti

- Posebne kategorije viši rizik
- Složene obrade
- Velik obujam obrada
- Sustavni ili povremen izvoz iz EU
- Razmjerna osjetljivosti, složenosti i količini podataka koju organizacija obrađuje

- Dokazuje se kontinuiranom edukacijom, potvrdama o tečajevima, stručnim savjetovanjima, programima cjeloživotnog obrazovanja i drugim aktivnostima
- Pohađanje specijaliziranih komercijalnih programa koji se certificiraju nije obvezno, no takvi programi imaju vidljivost u industriji i mogu pomoći osigurati službeniku bolje uvjete i konkurentnost na tržištu rada

Zadaće DPO:

- Čl 39. Uredbe:
- Informiranje i savjetovanje voditelja/izvršitelja/zaposlenika o njihovim obvezama
- Praćenje poštivanja Uredbe i drugih propisa u pogledu zaštite osobnih podataka
- Savjetovanje u pogledu procjene učinka i praćenje njenog izvršavanja
- Suradnja s nadzornim tijelom
- Vodi računa o riziku povezanom s postupcima obrade

Informiranje i savjetovanje voditelja/izvršitelja/zaposlenika o njihovim obvezama

- SZOP obavještava upravu organizacije o stanju zaštite podataka u organizaciji
- Prati razvoj i primjenu regulative na europskoj i nacionalnoj razini koja se odnosi na zaštitu podataka u području aktivnosti organizacije
- Prati aktivnosti nadležnog nacionalnog nadzornog tijela, kao i aktivnosti europskih tijela kao što je EDPB u pogledu tumačenja i usmjeravanja prakse primjene OUZP
- Osmišljava program edukacije svih strana koje utječu na obradu podataka u organizaciji – od najviše razine uprave, preko voditelja organizacijskih sektora, jedinica, timova do kategorija pojedinaca koji sudjeluju u aktivnostima koje uključuju obradu podataka
- Unutar organizacije treba osigurati adekvatnu komunikaciju sa svim organizacijskim jedinicama – ustrojiti „privacy network” odnosno neformalnu komunikacijsku grupu kako bi imala/imao relevantne informacije o svakodnevnom radu i budućem razvoju obrada u organizaciji

Praćenje poštivanja Uredbe i drugih propisa u pogledu zaštite osobnih podataka

- Savjetujući upravu i druge aktere u organizaciji koji određuju svrhu i sredstva obrade osobnih podataka, pazi na zakonitost obrade i upozorava na ponašanje suprotno načelima obrade osobnih podataka
- Osim Uredbe i ZOPOUZP, SZOP poznaje i pravni okvir specifičan za sektor u kojem organizacija koja ga je imenovala djeluje i njegove specifične zahtjeve u pogledu obrade osobnih podataka
- Poduzima redovite procjene usklađenosti aktivnosti organizacije sa zakonskim obvezama iz zaštite osobnih podataka
- Predlaže upotrebu vanjske revizije temeljem industrijskih standarda informacijske sigurnosti ili drugih primjenjivih samo-regulacijskih industrijskih standarda primjenjivih na obveze zaštite podataka, osobito prema načelu cjelovitosti i povjerljivosti

Suradnja s nadzornim tijelom

SZOP služi kao kontaktna točka za ispitanike koji imaju pitanja ili nedoumice u vezi s njihovim osobnim podacima koje organizacija obrađuje.

SZOP također može djelovati kao veza između organizacije i nadzornog tijela kada ispitanici podnose pritužbe ili zahtjeve.

SZOP djeluje kao veza između voditelja obrade i nadzornog tijela u postupku prethodnog savjetovanja pri izradi procjene učinka

Primjer: SZOP prima pritužbu od ispitanika tome kako organizacij koristi njegove osobne podatke. SZOP istražuje pritužbu i daje odgovor subjektu podataka, dok također ukoliko je došlo do povrede koju je nužno prijaviti obavještava nadzorno tijelo o povredi.

Prikaz slučaja (5)

Lanac bolnica sa sjedištem u Zagrebu djeluje u dvadesetak zemalja, uključujući nekoliko država Europske unije, ali i Tursku, Bosnu i Hercegovinu, Saudijsku Arabiju, Kanadu te Sjedinjene Države.

U navedenim zemljama, na snazi su različiti pravni propisi iz područja zaštite osobnih podataka koji sadrže određen broj zajedničkih, ali i mnoge različite obveze.

Također, neke od tih država osim federalnih, razvijaju i posebne propise za određene teritorijalne jedinice, poput pokrajina ili saveznih država.

Organizacijski, kako biste kao DPO osigurali učinkovitiju usklađenost s različitim regulatornim zahtjevima?

Položaj službenika

- Čl. 37.st.6 Uredbe:
  - Službenik može biti član osoblja voditelja / izvršitelja obrade ili obavljati zadaće temeljem „service agreement” (<> ugovor o djelu).
  - Funkcija službenika može se obavljati i temeljem ugovora sklopljenog s pojedincom izvan organizacije ili drugom organizacijom
  - Mogu se kombinirati osobne vještine i stručnosti kako bi više pojedinaca koji djeluju zajedno mogli biti djelotvorniji
  - Radi pravne jasnoće i dobre organizacije – osigurati jasnu raspodjelu zadaća i imenovanje jednog pojedinca kao odgovorne osobe
- Čl. 38.st.6 Uredbe:
  - Službenik može ispunjavati i druge zadaće i dužnosti.
  - Voditelj / izvršitelj obrade osigurava da takve zadaće i dužnosti ne dovedu do sukoba interesa

Položaj službenika

- Čl. 38 Uredbe - Voditelj/izvršitelj dužni osigurati da službenik:
- Bude pravodobno i primjereno uključen u sva pitanja z.o.p.
- Dobije podršku i potrebna sredstva za izvršavanje zadaća, ostvarivanje pristupa podacima i održavanje stručnosti
- Samostalan, ne prima upute, izravno odgovara najvišoj rukovodećoj razini voditelja/izvršitelja, ne može odgovarati zbog izvršavanja svojih zadaća
- Vezan je tajnošću ili povjerljivošću

„Pravodobno i primjereno uključen”

- Sudjeluje na sastancima visokog i srednjeg menadžmenta
- Nazočan kad se donose odluke od utjecaja na zaštitu podataka
- Pravodobno obaviješten o donošenju takvih odluka uz pristup svim potrebnim informacijama kako bi mogao dati odgovarajući savjet
- Mišljenje službenika uvijek uzeti u obzir. Ako se mišljenje službenika ne uzima u obzir, zabilježiti razloge zašto se nije uzelo u obzir
- Ukoliko dođe do povrede osobnih podataka ili drugog incidenta, odmah provesti savjetovanje sa službenikom

„Podrška i potrebna sredstva”

- Aktivna potpora najviše razine menadžmenta
- Osigurano adekvatno vrijeme za ispunjavanje njihovih zadaća
- *Osobito ako ne radi puno radno vrijeme*
- Osigurana odgovarajuća potpora u smislu financijskih sredstava, infrastrukture (poslovni prostori, objekti, oprema) i osoblja
- Službena obavijest o imenovanju službenika kako bi se osiguralo da su svi djelatnici upoznati s njegovim postojanjem i dužnostima
- Omogućen nužan pristup ostalim službama kao što su ljudski resursi, pravna služba, IT, sigurnost itd. kako bi službenici mogli dobiti neophodnu potporu i informacije
- Kontinuirano osposobljavanje
- Ukoliko je potrebno, uspostava odjela – jedinice SZOP

Upute i „…obavljanje svoje dužnosti i zadaća na neovisan način”

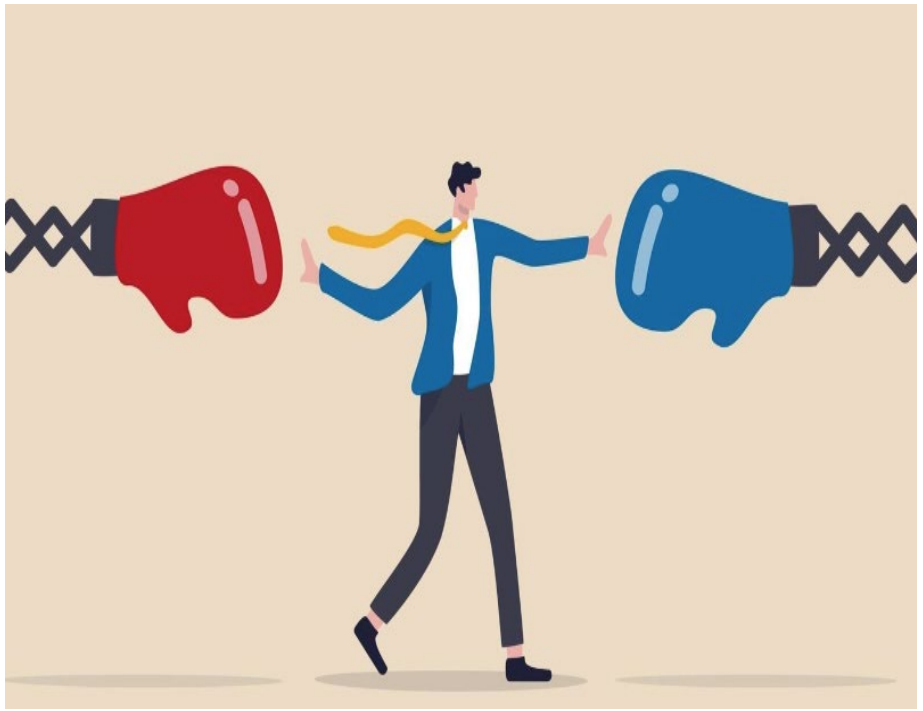
- Službenicima koji ispunjavaju zadaće u skladu s čl. 39 **ne smiju se davati upute:**
  - O rješavanju predmeta, odnosno ishodu
  - O načinu vođenja istrage o pritužbi
  - O tome treba li tražiti savjet nadzornog tijela
  - Da zauzmu neko određeno stajalište ili prihvate određeno tumačenje zakona
- U slučaju da voditelj/izvršitelj donese odluku nespojivu s Uredbom i savjetima službenika, **omogućiti da svoje suprotno mišljenje jasno do znanja da najvišoj rukovodećoj razini**
  - Primjerice, **sastavljanjem godišnjeg izvješća o aktivnostima službenika** za najvišu razinu uprave

Službenik i sukob interesa

Čl. 38.st.6 Uredbe uređuje mogućnost da se službeniku povjere i drugi zadaci dok god njihovo izvršavanje ne rezultira sukobom interesa

Koji zadaci bi bili u konfliktu?

- Zadaci vezani uz obradu osobnih podataka
- WP 29 kao kriterij navodi poziciju ili zaduženje koje uključuje: „određivanje svrhe i načina obrade osobnih podataka”
- Konkretno, pozicija službenika je u praksi uglavnom nespojiva s pozicijama uprave
- Konflikt je čest na pozicijama voditelja IT odjela, marketinga i ljudskih resursa (HR)
- Moguć je i na nižim pozicijama ukoliko uključuju određivanje svrhe i načina obrade osobnih podatka



Kako do kompetentnog DPO?

- Multidisciplinarni pristup!
- Poznavanje regulative zaštite osobnih podataka
- Poznavanje prakse zaštite podataka
- Poznavanje suvremenih informacijskih tehnologija
- Poznavanje prakse informacijske sigurnosti i upravljanja rizicima
- Razumijevanje poslovnih procesa

Poznavanje regulative i prakse zaštite osobnih podataka

Vodiči, tumačenja i upute nadzornih tijela
- Nacionalna nadzorna tijela – AZOP, ICO, CNIL itd.

Specijalizirane stručne organizacije
- International Association of Privacy Professionals (IAPP)

Nacionalna i europska sudska praksa
- Dostupna na stranicama sudova
- Specijalizirana izdanja s relevantnom praksom

Specijalizirani pravni portali
- Domaći i strani

Suradnja sa zajednicom službenika za zaštitu podataka

Redovita stručna edukacija

Praksa zaštite podataka je praksa poznavanja informacijskih sustava, praksa informacijske sigurnosti, poznavanje poslovnih procesa i poznavanje metodologije procjene rizika

ISO 27000 obitelj standarda za informacijsku sigurnost

Američki NIST standardi

Razne metodologije procjene rizika

Službenik kao zaposlenik	Eksternalizirani službenik
Bolji uvid u poslovne procese organizacije	Predvidljivo, odabrat će se stručnjak i profesionalac s odgovarajućim iskustvom
Posljedično, bit će efikasniji u postavljanju vlastitog DPMS	Bolji uvid u najbolje prakse na tržištu
Što je organizacija veća, poslovni procesi kompleksniji, to će obujam praćenja i aktivnosti biti veći	Nije zaposlenik organizacije, nema radnopravnih obveza već se sve regulira service ugovorom
Nalazi se u centru čitave korporativne privacy mreže kao jedinstveni kontakt za sva pitanja koja poslovne jedinice ili članice grupe mogu imati	Po definiciji neovisan i objektivan u sagledavanju obveza u odnosu na odnose unutar organizacije
Preporučljiv za: Velike organizacije, povezana društva, visokorizične obrade	**Preporučljiv za:** Manje i srednje organizacije Organizacije sa standardnim setom obrada specifičnim za gospodarske sektore

Uloge i odgovornosti

- **Službenik za zaštitu podataka**
- savjetuje i educira
- nadgleda postupanje u skladu s odredbama Uredbe
- **Zaposlenici**
- vode računa pri radu s osobnim podacima
- razumiju okruženje osobnih podataka i postupaju u skladu s procedurama i po radnim uputama
- **Uprava**
- podržava službenika u radu
- ističe važnost zaštite osobnih podataka
- osigurava potrebne resurse

- **Voditelji poslovnih procesa**
- Oblikuju zahtjeve i poslovne procese
- Prepoznaju potrebu za edukacijom zaposlenika
- **CISO/CIO/CSO**
- predlažu tehnička rješenja u skladu sa funkcionalnim zahtjevima (i budžetima!)
- osiguravaju implementaciju
- odabiru i vode implementaciju tehničkih kontrola

Primjer kratke i potpune obavijesti o obradi podataka (privacy notice)

Tzv. slojevita obavijest:

- Obavijest o zaštiti podataka osmišljena je da pruži potpunu informaciju ispitaniku.
- Takva obavijest može na prvi pogled biti preduga i nepregledna
- Kratka obavijest — gornji sloj — pruža korisniku ključne elemente obavijesti o privatnosti kao što su identitet voditelja obrade, svrhe obrade, prava ispitanika, kontakt SZOP
- Potpuna obavijest — donji sloj — u potpunosti pokriva sve detalje oko vrsta podataka, svrha obrade, prava ispitanika itd.
- Ostvarenje načela transparentnosti – sadržaj i prezentacija razrađeni smjernicama
- Primjer – kratka i potpuna obavijest o obradi za veliki zdravstveni sustav

Prikaz slučaja (5)

Velika zdravstvena ustanova poput Kliničkog bolničkog centra dnevno obrađuje podatke tisuća pacijenata.

Prilikom prijave u bolnicu na liječenje, pacijentima se pruža izjava kojom se traži da imenuju najbližu rodbinu za slučaj potrebe i kontakta.

Treba li KBC obavijestiti te osobe da su njihovi podaci primljeni i obrađeni u okviru pružanja zdravstvene skrbi ispitaniku

Prvi sloj

Kratka obavijest o obradi osobnih podataka

Punu informaciju o obradi osobnih podataka možete pronaći na sljedećoj adresi:

www.sbg.hr/obavijestoobradi.html

Kontakt podaci voditelja osobnih podataka:
Sveučilišna bolnica Grad
Gradska avenija 1
13234 Grad

Podatke prikupljamo u svrhu pružanja najviše razine zdravstvene skrbi, rehabilitacije, izdavanja recepta i lijekova, ispunjavanja obveza prema sustavu obveznog zdravstvenog osiguranja

Podaci koje obrađujemo uključuju identifikacijske podatke, kontaktne podatke, podatke nužne za postavljanje dijagnoze, podatke prikupljene putem medicinskih uređaja i druge podatke

Ispitanik ima pravo biti informiran o obradi svojih osobnih podataka. Ostala prava ispitanika, temeljem zahtjeva ispitanika, uključuju:

- pravo na pristup osobnim podacima,
- pravo na ispravak ili dopunu,
- pravo na brisanje,
- pravo na ograničenje obrade,
- pravo na prenosivost podataka,
- pravo na prigovor,
- pravo da ne bude podvrgnut automatiziranom pojedinačnom odlučivanju s pravnim ili sličnim učincima, uključujući profiliranje

Podaci ispitanika mogu se ustupati primateljima poput: Hrvatski zavod za zdravstveno osiguranje, Hrvatski zavod za javno zdravstvo, Ministarstvo zdravstva, Ministarstvo rada i socijalne skrbi

Kontakt podaci službenika za zaštitu osobnih podataka:
Sluzbenik@bolnicagrad.hr
Gradska avenija 1
13234 Grad
e-pošta: szop@bolnicagrad.hr

Obavijest o obradi podataka (privacy notice) – potpuna

- Oznaka voditelja obrade
- Izvori i kategorije podataka
- Vrste osobnih podataka o pacijentima
- Vrste osobnih podataka o zaposlenicima
- Vrste osobnih podataka o rođacima, bliskim osobama, zakonskim zastupnicima i skrbnicima
- Podaci o donorima krvi, organa i krvnih preparata
- Podaci o dobavljačima, volonterima i klaunovima doktorima – Crvenim nosovima ☺
- Podaci zabilježeni sustavom videonadzora
- Podaci o osobama koje ulaze u čuvane prostore bolnice
- Podaci o osobama koje zovu ili koje se zove putem praćenih telefonskih linija
- Svrhe obrade
- Pravne osnove obrade u vezi s pružanjem zdravstvenih usluga
- Pravne osnove obrade za druge usluge
- Primatelji osobnih podataka
- Prijenos podataka u treće zemlje
- Prava ispitanika
- Ostvarivanje pristupa svojim podacima
- Kontakt službenika za zaštitu podataka

Obavijest o obradi podataka (privacy notice)

Sveučilišna bolnica Grad o uvjetima i sadržaju obrade obavještava pacijente, zaposlenike i sve druge osobe čiji se osobni podaci obrađuju na temelju članka 13. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća o zaštiti fizičkih osoba u vezi s obradom osobnih podataka i slobodnim kretanjem tih podataka te drugih propisa iz područja javnog zdravstva:

Kontakt podaci voditelja osobnih podataka:

Sveučilišna bolnica Grad

Gradska avenija 1

13234 Grad

Kontakt podaci službenika za zaštitu osobnih podataka:

Sluzbenik@bolnicagrad.hr

Gradska avenija 1

13234 Grad

e-pošta: szop@bolnicagrad.hr

Izvori i kategorije osobnih podataka

IZVORI OSOBNIH PODATAKA

Osobne podatke voditelj obrade prikuplja posebice na sljedeći način:

- od ispitanika, posebno u vezi s pružanjem zdravstvenih usluga i vođenjem zdravstvene dokumentacije, za potrebe legitimnih interesa voditelja obrade, temeljem ugovora ili privole dane od strane ispitanika,
- usmeno, pismeno, e-mailom, telefonom, putem kontakt obrazaca na web stranici
- pristupom sustavu CEZIH

KATEGORIJE OSOBNIH PODATAKA KOJI SU PREDMET OBRADE

- bolnica o ispitaniku obrađuje posebno one kategorije osobnih podataka koji su potrebni za obavljanje dužnosti voditelja obrade:
- adresu i identifikacijske podatke,
- osobni podaci koji se obrađuju u sklopu pružanja zdravstvenih usluga (odnosno posebna kategorija osobnih podataka),
- podatke potrebne za izvršavanje ugovornih odnosa
- podaci dani izvan okvira relevantnih zakona koji se obrađuju temeljem privole koju je dao nositelj podataka ili ugovora,
- osobni podaci dobiveni za potrebe legitimnih interesa voditelja obrade
- snimke sa sustava kamera (video snimke)

Vrste osobnih podataka koji se obrađuju o pacijentima

O pacijentima se obrađuju sljedeće vrste podataka:

- osobni podaci potrebni za utvrđivanje identiteta (datum rođenja, OIB i imena, podaci o zdravstvenom osiguranju),
- osobni podaci potrebni za komunikaciju (prebivalište, srodnici ili bliske osobe, za djecu imena roditelja, skrbnika, zakonskih zastupnika, telefon, e-mail),
- podaci potrebni za postavljanje dijagnoze i postupak liječenja, uključujući i subjektivni opis trenutnog zdravstvenog stanja,
- osobni podaci zaprimljeni o pacijentu od drugih zdravstvenih ustanova, od transportne službe, od službe spašavanja,
- podaci o zdravstvenom stanju, dobiveni neposrednim pregledom i dijagnostičkim postupcima (visina, težina, broj otkucaja srca i dr.),
- podaci o zdravstvenom stanju, dobiveni instrumentalnim pregledima tijela bolesnika (zapisi EKG-a, EEG-a, EMG krivulje, RTG i ultrazvučni snimci, zapisi s posebnih uređaja za preglede, snimci površine tijela i dr.),
- podaci o zdravstvenom stanju, dobiveni laboratorijskim pretragama bioloških uzoraka (vrijednosti tjelesnih tekućina, briseva, uzoraka tkiva, daha, genetski rezultati na razini molekularne genetike i dr.),
- definirane glavne i sekundarne dijagnoze,
- alergije na hranu, specijalni dijetni režimi
- lijekovi u obliku elektroničkog recepta,
- planovi zdravstvenih aktivnosti (plan liječenja, plan njege i sl.),
- opisi medicinskih aktivnosti (zapisnik o ambulantnom pregledu, operativni protokol, plan liječenja, plan njege i dr.),
- opisi ishoda skrbi (otpusno izvješće, smrtovnica, izvješće obdukcije, itd.),
- financijski podaci (plaćanje plaćenih usluga, participacije za lijekove i sl.),
- snimke sa sustava kamera,
- evidentiranje identifikacijskih podataka osobe prilikom ulaska u objekte koji nisu javni,
- snimanje telefonskih poziva na odabrane telefonske brojeve

Vrste osobnih podataka o zaposlenicima

O zaposlenicima se bilježe i obrađuju:

- identifikacijski podaci, tj. ime uključujući diplome, broj socijalnog osiguranja, broj osobne iskaznice, putovnicu, vozačku dozvolu, broj bankovnog računa,
- kontakt osobni podaci – mjesto prebivališta, članovi obitelji, brojevi telefona, e-mail adrese,
- obrazovanje – svjedodžbe, diplome, dokumenti o stručnim tečajevima i treninzima itd.
- profesionalni životopis uključujući recenzije rada,
- sistematizacija poslova - radno mjesto, radno mjesto,
- rad i aktivnosti u svezi s radom - izvedeni nastupi, uključivanje u smjene i usluge,
- pristupi računalnim sustavima, postavljanje pristupa određenim osobnim podacima koji se obrađuju,
- pristup zaštićenim područjima,
- evidenciju prisutnosti i radnog vremena,
- catering – narudžbe i plaćanja,
- Podaci o plaći i plaćama - klasifikacija plaća, nagrađivanje, izvješća o radu, iznos isplaćenih na žiro račun, iznosi isplaćeni u gotovini, godišnji odmor i njegovo korištenje, nesposobnost za rad, odsutnost s radnog mjesta, iznosi odbitaka od plaće koji se šalju na korist sindikata uz suglasnost sindikalista,
- evidentirani i poslani podaci za potrebe mirovinskog osiguranja,
- podatke koje zaposlenik daje u svrhu provjere svojih primanja kod bankarske institucije,
- podaci dani ovršiteljima, sudovima, policiji i drugim državnim ili privatnim organizacijama prema njihovim potrebama na temelju zakona,
- zdravstveno osiguranje – medicinske usluge uz naknadu troškova zdravstvenoj ustanovi za njihovo izvršenje,
- snimke sa sustava kamera,
- evidentiranje identifikacijskih podataka osobe prilikom ulaska u objekte koji nisu javni,
- snimanje telefonskih poziva na odabrane telefonske brojeve

Vrste osobnih podataka o drugim posjetiteljima

O srodnicima, bolesnicima bliskim osobama, skrbnicima, zakonskim zastupnicima evidentiraju se i obrađuju:

- identifikacijski podaci – ime, prezime (uključujući organizaciju sa zakonskim zastupnicima),
- kontakt podaci – mjesto stanovanja (adresa organizacije), telefon, e-mail, broj faksa,
- djelomične podatke o zdravstvenom stanju (po potrebi u obiteljskoj anamnezi bolesnika),
- snimke sa sustava kamera,
- evidentiranje identifikacijskih podataka osobe prilikom ulaska u objekte koji nisu javni,
- snimanje telefonskih poziva na odabrane telefonske brojeve

O darivateljima krvi, krvnih derivata i organa upisuju se:

- identifikacijski podaci – ime, prezime, matični broj, datum rođenja, zdravstveno osiguranje,
- kontakt podaci - prebivalište, telefon, e-mail,
- podatke o zdravstvenom stanju (anamneza, prvi pregled, podaci liječnika opće medicine i sl.),
- broj obavljenih uzimanja krvi i krvnih sastojaka, uključujući i broj vađenja u drugim zbirnim centrima,
- prema broju uzoraka predanih Crvenom križu ili dobivanje nagrade za zdravstveno osiguranje,
- snimke sa sustava kamera,
- evidentiranje identifikacijskih podataka osobe prilikom ulaska u objekte koji nisu javni,
- snimanje telefonskih poziva na odabrane telefonske brojeve

Podaci zabilježeni sustavom videonadzora

O prolasku osoba kroz prostorije i objekte Sveučilišne bolnice Grada praćene snimkom kamera bilježe se:

- video snimanje lika i lica

Obrađuju se podaci iz sustava kamera, koji se sastoje od snimanja snimljenih kadrova, koji će se koristiti za identifikaciju fizičkih osoba u vezi s određenom akcijom.

Svrha snimanja i obrade evidencije su zakonom uređeni interesi upravitelja, odnosno zaštita imovine upravitelja od oštećenja i krađe, imovine zaposlenika i pacijenata, kao i sigurnost i zaštita života i zdravlja zaposlenika, pacijenata i drugih osoba koje se nalaze u prostorijama Bolnice.

Osobnim podacima iz sustava kamera upravlja samo voditelj obrade. Mogu se dostaviti u slučaju zahtjeva državnim tijelima, ili javnim tijelima (tj. sudovima, tijelima za provođenje zakona, administrativnim tijelima), ili drugim zainteresiranim subjektima za ispunjenje svrhe obrade (npr. komercijalna osiguravajuća društva).

Rok pohrane snimljenih kamera je 14 dana, nakon čega se podaci brišu. U slučaju da snimke kamera trebaju poslužiti kao dokaz, kopije snimaka mogu se čuvati i duže, do 5 godina.

Podaci o osobama koje ulaze u čuvane prostore bolnice

O ulasku osoba u nejavne dijelove zgrada bilježe se:

- evidentiranje imena i prezimena osobe koja ulazi u objekt,
- broja osobne iskaznice,
- datuma i vremena ulaska,
- cilja i svrhe ulaska (samo za objekte koji nisu javni)

Podaci se obrađuju u obliku upisa u knjigu posjetitelja.

Svrha obrade su zakonom zaštićeni interesi upravitelja, odnosno zaštita imovine upravitelja od oštećenja i krađe, imovine zaposlenika i pacijenata, kao i sigurnost i zaštita života i zdravlja zaposlenika, pacijenata i drugih osoba koje se nalaze u prostorijama upravitelja.

Osobnim podacima iz knjige gostiju upravlja samo voditelj obrade. Mogu se dostaviti u slučaju zahtjeva državnim tijelima, ili javnim tijelima (tj. sudovima, tijelima za provođenje zakona, administrativnim tijelima), ili drugim zainteresiranim subjektima za ispunjenje svrhe obrade (npr. komercijalna osiguravajuća društva).

Podaci o osobama koje zovu ili koje se zove putem praćenih telefonskih linija

Pozivni (pozvani) telefonski broj, kontakt podaci (prema potrebi), zdravstveni podaci - prema razlogu poziva, ostali podaci koji utječu na zahtjev usluge, sadržaj poziva

Podaci se obrađuju u obliku snimke telefonskog poziva.

Svrha snimanja je volja pozivatelja ili poziva da obavijesti ili primi informacije, odnosno zaštiti zdravlje i sigurnost uključene osobe/osoba.

Osobnim podacima sa snimanja poziva upravlja samo voditelj obrade. Mogu se dostaviti na zahtjev uprave upravitelja, državnih tijela ili javnih tijela (tj. sudova, tijela kaznenog progona, upravnih tijela) ili drugih zainteresiranih subjekata.

Rok čuvanja zapisa telefonskih poziva je 14 dana, nakon čega se podaci brišu. U slučaju da se telefonski zapisi koriste kao dokaz, preslike zapisa mogu se čuvati duže, do 5 godina.

Svrhe obrade

- Pružanje izvanbolničke i bolničke skrbi
- Pružanje naknadne skrbi
- Opskrba lijekovima i drugim pripravcima
- Uspostavljanje elektroničkog recepta
- Pružanje rehabilitacijske skrbi
- Laboratorijska obrada biološkog materijala
- Izvođenje kirurških zahvata
- Darivanje krvi i krvnih sastojaka
- Obrada obveza prema sustavu zdravstvenog osiguranja (zdravstvena osiguranja, zdravstveni registri i sl.)
- Upravljanje sustavom kamera
- Snimanje telefonskih poziva na odabrane telefonske brojeve
- Pružanje plana obroka
- Pružanje usluga medicinskog prijevoza
- Provedba programa volontiranja
- Procjena i poboljšanje sigurnosti pacijenata
- Osposobljavanje drugih zdravstvenih djelatnika
- Provođenje kliničkih istraživanja i revizija te analiza podataka kako bi se razumjelo više o zdravstvenim rizicima i uzrocima razvoja novih tretmana
- Priprema statistike o učinku i praćenje kako trošimo javni novac
- Prijavljivanje i istraživanje pritužbi, zahtjeva i neželjenih incidenata.
- Pregled pružene skrbi kako bi se osiguralo da je na najvišem mogućem standardu; poboljšanje individualne dijagnoze i skrbi;
- Procjena i poboljšanje sigurnosti pacijenata
- Osposobljavanje drugih zdravstvenih djelatnika

Propisi koji sadrže pravne obveze u vezi obrade podataka u kontekstu pružanja zdravstvenih usluga

1. Zakon o podacima i informacijama u zdravstvu (NN 14/19)
2. Zakon o zdravstvenoj zaštiti ("Narodne novine", broj NN 100/18, 125/19, 147/20, 119/22, 156/22, 33/23)
3. Zakon o obveznom zdravstvenom osiguranju ("Narodne novine", broj 80/13, 137/13, 98/19, 33/23)
4. Zakon o obveznom zdravstvenom osiguranju i zdravstvenoj zaštiti stranaca u Republici Hrvatskoj ("Narodne novine", broj 80/13, 15/18, 26/21, 46/22)
5. Zakon o dobrovoljnom zdravstvenom osiguranju ("Narodne novine", broj 85/06, 150/08, 71/10, 53/20, 120/21, 23/23)
6. Zakon o liječništvu ("Narodne novine", broj 121/03 i 117/08)
7. Zakon o ljekarništvu ("Narodne novine", broj 121/03, 35/08 i 117/08)
8. Zakon o sestrinstvu (NN 121/03, 117/08 i 57/11)
9. Zakon o dentalnoj medicini ("Narodne novine", broj 121/03, 117/08, 120/09, 46/21)
10. Zakon o primaljstvu ("Narodne novine", broj 120/08 i 145/10)
11. Zakon o medicinsko-biokemijskoj djelatnosti ("Narodne novine", broj 121/03 i 117/08)
12. Zakon o fizioterapeutskoj djelatnosti ("Narodne novine", broj 120/08)
13. Zakon o djelatnostima u zdravstvu ("Narodne novine", broj 87/09)
14. Zakon o kvaliteti zdravstvene zaštite ("Narodne novine", broj 118/18)
15. Zakon o suzbijanju zlouporabe droga ("Narodne novine", broj 107/01, 87/02, 163/03, 141/04, 40/07,149/09, 84/11, 80/13 i 39/19)
16. Zakon o provedbi uredbi Europske unije iz područja prekursora za droge ("Narodne novine", broj 80/13)
17. Zakon o lijekovima ("Narodne novine", broj 76/13, 90/14 i 100/18)
18. Zakon o zaštiti osoba s duševnim smetnjama ("Narodne novine", broj 76/14)
19. Zakon o Hrvatskom Crvenom križu ("Narodne novine", broj NN 71/10, 136/20)
20. Zakon o obeštećenju radnika profesionalno izloženih azbestu ("Narodne novine", broj 79/07, 139/10 i 111/18)
21. Zakon o krvi i krvnim pripravcima ("Narodne novine", broj 79/06 i 124/11)
22. Zakon o primjeni ljudskih tkiva i stanica ("Narodne novine", broj 144/12)
23. Zakon o presađivanju ljudskih organa u svrhu liječenja ("Narodne novine", broj 144/12)
24. Zakon o medicinski pomognutoj oplodnji ("Narodne novine", broj 86/12)
25. Zakon o podacima i informacijama u zdravstvu ("Narodne novine", broj 14/2019)
26. Zakon o provedbi Uredbe (EU) 2017/745 o medicinskim proizvodima i Uredbe (EU) 2017/746 o in vitro dijagnostičkim medicinskim proizvodima ("Narodne novine, broj 100/18)
27. Pravilnik o načinu vođenja, čuvanja, prikupljanja i raspolaganja medicinskom dokumentacijom pacijenata iz obveznog zdravstvenog osiguranja u Centralnom informacijskom sustavu zdravstva Republike Hrvatske (NN 82/10)
28. Pravilnik o uporabi i zaštiti podataka iz medicinske dokumentacije pacijenata u Centralnom informacijskom sustavu zdravstva Republike Hrvatske (NN 14/10.)
29. Pravilnik o opsegu i sadržaju podataka te načinu vođenja e-Kartona (74/2023)
30. Pravilnik o vrstama i načinu primjene mjera prisile prema osobi s težim duševnim smetnjama (2015/16)

Propisi relevantni za druge obrade

- Zakon o radu
- Zakon o mirovinskom osiguranju
- Zakon o javnoj nabavi
- Zakon o ustanovama
- Zakon o potvrđivanju međunarodne konvencije protiv dopinga u sportu (NN međunarodni ugovori
- Zakon o radu
- Pravilnik o sadržaju i načinu vođenja evidencije o radnicima
- Zakon o plaćama u javnim službama

Primatelji osobnih podataka

KATEGORIJE PRIMATELJA OSOBNIH PODATAKA

Voditelj obrade ovlašten je dati osobne podatke posebno sljedećim primateljima:

- društvima za zdravstveno osiguranje
- davateljima zdravstvenih i socijalnih usluga
- pacijentima na koje se osobni podaci odnose
- državnim i drugim tijelima u okviru ispunjavanja zakonskih obveza utvrđenih odgovarajućim zakonskim propisima
- osobama u ugovornom odnosu na koje se osobni podaci odnose
- drugim primateljima (npr. prijenos osobnih podataka u treće zemlje u skladu s relevantnim zakonima ili privolom nositelja podataka)

PRIMATELJI OSOBNIH PODATAKA

Pristup osobnim podacima pacijenata imaju osobe ovlaštene za uvid u medicinsku dokumentaciju pacijenta (općenito, uz privolu, članovi obitelji, zakonski zastupnici i dr.) ili za dobivanje informacija o zdravstvenom stanju pacijenta (zaposlenici zdravstvene ustanove, nadležna tijela i dr.) .).

U granicama radnog opsega to su odgovarajući liječnici, nemedicinski zdravstveni djelatnici (npr. medicinske sestre, primalje, radni terapeuti, radiološki suradnici, zdravstveni laboratorijski tehničari, farmaceutski suradnici itd.) i, u mjeri u kojoj je to potrebno, drugi zaposlenici koji, prema svom opterećenju i internim propisima ovlaštenja administratora za rukovanje tim zapisima.

U nekim slučajevima, u granicama relevantnih zakonskih propisa, voditelj obrade može biti obvezan osobne podatke učiniti dostupnim tijelima javne vlasti (sudovi, upravna tijela, vlasti). Ispitanik na kojeg se osobni podaci odnose može pregledavati osobne podatke bez daljnjih ograničenja. Nadalje, ovlaštena osoba može pristupiti svojim osobnim podacima na uvid uz privolu nositelja podataka. Uvid u iste bez suglasnosti mogu izvršiti voditelj obrade, revizijsko tijelo, tijela kaznenog progona i druge zakonom ovlaštene osobe.

Prijenos podataka u treće zemlje

U opravdanim slučajevima, u mjeri u kojoj je to potrebno i sukladno zakonskim propisima, voditelj obrade može bez privole prenijeti osobne podatke pacijenata u državu izvan Europske unije, ako je to potrebno radi zaštite njegovih životno važnih interesa, ako takav pacijent nije fizički ili pravno sposoban dati pristanak na transfer (npr. tijekom transfera/repatrijacije pacijenta koji zbog svog zdravstvenog stanja nije u mogućnosti dati pristanak).

Prijenos osobnih podataka u treću državu ili međunarodnu organizaciju može se, u opravdanim slučajevima, odvijati na temelju privole i upute ispitanika.

Prava ispitanika

Ispitanik ima pravo biti informiran o obradi svojih osobnih podataka.

Ostala prava ispitanika, temeljem zahtjeva ispitanika, uključuju:

- pravo na pristup osobnim podacima,
- pravo na ispravak ili dopunu,
- pravo na brisanje,
- pravo na ograničenje obrade,
- pravo na prenosivost podataka,
- pravo na prigovor,
- pravo da ne bude podvrgnut automatiziranom pojedinačnom odlučivanju s pravnim ili sličnim učincima, uključujući profiliranje

PRISTUP OSOBNIM PODACIMA

- Ispitanik ima pravo dobiti potvrdu o tome obrađuju li se osobni podaci koji se na njega odnose ili ne, a ako je tako, ima pravo pristupiti tim osobnim podacima i dobiti opće informacije o osobnim podacima koji se obrađuju.
- Međutim, za sve dodatne kopije bolnica ima pravo zahtijevati razumnu naknadu koja odgovara administrativnim troškovima koje bolnica ima.
- Ako trebate dobiti detaljnije informacije o tijeku liječenja (izvođenje, lijekovi, dijagnostika i sl.), zatražite od ordinirajućeg liječnika izvadak iz medicinske dokumentacije. Prijenos ovih podataka nije u nadležnosti službenika za zaštitu osobnih podataka.

NAČIN PODNOŠENJA ZAHTJEVA I SADRŽAJ ZAHTJEVA Ispitanik svoja prava na zaštitu osobnih podataka može ostvariti pisanim putem ili elektroničkim putem na sljedećim adresama:

- pisanim putem dopisom upućenim na adresu Sveučilišne bolnice Grada Službeniku za zaštitu podataka
- elektroničkim putem e-mailom poslanim na adresu: sluzbenik@bolnicagrad.hr

U zahtjevu, prigovoru ili drugom podnesku za zaštitu osobnih podataka navesti:

- Vaše ime, prezime i datum rođenja,
- Vašu adresu ili poštansku adresu,
- Vaš broj telefona i e-mail adresu,
- Sadržaj vašeg podneska

Ostvarivanje prava ispitanika – primjer standardne operativne procedure

Procedura upravljanja zahtjevima

Tko može podnijeti zahtjev?

Zahtjev za pristup osobnim podacima može se podnijeti organizaciji voditelja obrade na bilo koji od sljedećih načina.

Ovaj popis nije konačan:

- Pojedinac
- Osoba koju je pojedinac ovlastio za podnošenje zahtjeva o tome u ime pojedinca
- U slučaju djeteta, osoba s roditeljskom odgovornošću za to dijete može ostvarivati djetetova prava sukladno Obiteljskom zakonu
- Osoba koju sud imenuje da vodi poslove pojedinca
- Ako je pojedinac preminuo, osobni zastupnik i bilo koja osoba koji mogu imati zahtjev koji proizlazi iz smrti pojedinca

Obrazac zahtjeva za pristup podacima

temeljem Opće uredbe o zaštiti podataka (EU) 2016/679 i Zakona o provedbi Opće uredbe o zaštiti podataka

Podaci o ispitaniku

Titula: .....
Imena: .....
Prezime: .....
Prethodno prezime (ako postoji):
Datum rođenja: .....
MBO broj (ako je poznat): .....
Trenutna adresa: .....

Podaci o podnositelju zahtjeva (ako podnosite zahtjev u ime ispitanika)

Ime i prezime: .....
Adresa: .....
Odnos prema pojedincu u odjeljku 1: .....

Dodatne informacije

- Bit će od pomoći ako možete opisati specifične informacije koje želite vidjeti i navesti što više detalja kako bismo mogli brzo identificirati vaše zapise.
- Ako se traže podaci o pacijentima, navedite pojedinosti kao što su usluge koje ste posjećivali, datumi, tretmani, bolnice itd.
- Ako se traže podaci o osoblju, navedite je li sadašnji ili bivši član osoblja i navedite broj platne liste ako je poznat.

Pružanje informacija

Molimo potvrdite format u kojem želite primati informacije navodeći u nastavku. Ako se preferencija ne odabere, najprikladniji format odabrat će voditelj obrade.

E-mail adresa (ako je primjenjivo): .....

Molimo označite jedno od sljedećih polja i potpišite se ispod:
a) Potvrđujem da sam osoba spomenuta u odjeljku 1 i trebam pristup svojim osobnim podacima.
b) Potvrđujem da sam osoba spomenuta u odjeljku 1 i ovlašćujem izdavanje kopija mojih osobnih zapisa (opisanih u odjeljku 3) osobi spomenutoj u odjeljku 2.
c) Potvrđujem da sam ja osoba spomenuta u odjeljku 2 i imam roditeljsku odgovornost za dijete u odjeljku 1.
d) Potvrđujem da sam osoba navedena u odjeljku 2 i da sam ovlašten djelovati kao agent/punomoć za osobu iz odjeljka 1.

Podnositelj zahtjeva treba dostaviti dokaze za sljedeće:
e) Zastupnik pacijenta (to će biti izvršitelj oporuke ili upravitelj ostavine).
f) Podnositelj zahtjeva koji može imati zahtjev koji proizlazi iz smrti pacijenta. Podnositelj zahtjeva treba navesti o kakvom zahtjevu se radi i samo informacije koje su relevantne za zahtjev se razmatraju za objavljivanje.

Imajte na umu da vaš zahtjev neće biti obrađen osim ako ne primimo i ne potvrdimo adekvatnu identifikaciju podnositelja zahtjeva.

Odobreni obrasci identifikacije dostupni su na našoj web stranici.

Ime i prezime: .....

Potpis: .....

Datum: .....

Vratiti na adresu:

Voditelj obrade,
Ulica i kućni broj
Poštanski broj, mjesto

Ili na našu email adresu: adresa@voditeljobrade.hr

Za daljnje informacije o tome kako obrađujemo vaše podatke, pogledajte našu obavijest o obradi podataka ovdje: **link na obavijest o obradi podataka**

Pristup podacima

Pojedinci imaju pravo na pristup podacima koji se o njima nalaze, iako postoje iznimni razlozi i strogo definirane situacije u kojima se to može uskratiti uz jasno obrazloženje relevantnog registriranog zdravstvenog djelatnika, tj. na temelju potencijalne štete za fizičko ili mentalno zdravlje pacijenta.

Identitet pojedinca koji je dao/snimio informacije ne smije se otkriti, niti identitet bilo koje druge osobe/osoba koji se spominju u zapisu(ima) pojedinca koji traži pristup, osim ako je dat izričit pristanak ili ako informacije je već dostupan ili poznat pojedincu. Ovo ne uključuje unose registriranog zdravstvenog djelatnika koji je sastavio ili sudjelovao u zdravstvenim kartonima ili koji je bio uključen u njegu pacijenta.

Odvjetnik koji djeluje u ime ispitanika može zatražiti kopije svih podataka koji se vode o ispitaniku. Odvjetnik mora pružiti odgovarajuće dokaze o ovlaštenju pojedinca da ima dopuštenje za pristup traženim podacima.

Policija može povremeno zatražiti pristup osobnim podacima pojedinaca. Iako postoji izuzeće u OUZP koje dopušta voditelju obrade da otkrije podatke policiji kako bi se poduprla prevenciju i otkrivanje kriminala, policija nema automatsko pravo pristupa no mogu dobiti sudski nalog.

Druge organizacije također mogu zatražiti osobne podatke pojedinaca prema OUZP, a otkrivanje će se morati pregledati i ocijeniti prema relevantnom zakonodavstvu od slučaja do slučaja

Elementi zahtjeva

Iako je u rijetkim okolnostima dopušteno primiti zahtjev za pristup informacijama/zahtjev za pristup usmeno, preporučuje se, gdje je to moguće, da bude u pisanom obliku.

Zahtjev sadržava sljedeće elemente o podnositelju:

- Dovoljno informacija kako bi voditelj obrade mogao locirati informacije koje se traže
- Dovoljno informacija da bi voditelj obrade mogao identificirati ispitanika
- Zahtjev ispitanika, od osoba s roditeljskom skrbi, ako se zahtjev odnosi na dijete mlađe od 16 godina, osobe kojoj je dana punomoć, zastupnika kojeg imenuje sud, ako je pojedinac preminuo, bilo koja osoba koja može imati zahtjev koji proizlazi iz smrti pojedinca

Elementi o osobni čiji se podaci traže:

- Puno ime, uključujući prethodna imena ako je primjenjivo
- Puna adresa, uključujući prethodnu adresu(e) ako je primjenjivo
- Datum rođenja
- Matični broj osiguranika (nije nužno)
- Kratak opis informacija koje su potrebne
- Ime i adresa predstavnika pojedinca (ako je primjenjivo)
- Dokaz o identitetu

Prikaz slučaja (6)

Ima li zdravstvena ustanova obvezu prijaviti slučajeve povrede sigurnosti osobnih podataka uzrokovane napadom zlonamjernog programa na informacijski sustav ili drugim kibernetičkim napadom?

U slučajevima kada su osobni podaci pacijenata učinjeni nedostupnima (gubitak dostupnosti, kriptirani) napadom na informacijski sustav zlonamjernim programom, drugim kibernetičkim napadom ili tehničkom greškom voditelja ili izvršitelja obrade (također slučajevi privremene nedostupnosti osobnih podataka, kada se isti naknadno vraćaju iz sigurnosne kopije) postavlja se pitanje postojanja obveze prijave povrede nadzornom tijelu.

Prema Uredbi, svaka povreda sigurnosti osobnih podataka voditelja obrade prijavljuje se nadležnom tijelu.

Jedina iznimka su slučajevi u kojima je malo vjerojatno da bi ova povreda rezultirala rizikom za prava i slobode fizičkih osoba.

Obzirom na odredbe Uredbe, kao i na smjernice EDPB i nadzornih tijela, treba li takvu situaciju prijaviti nadzornom tijelu?

Kada ne treba prijaviti povredu nadzornom tijelu ili ispitanicima?

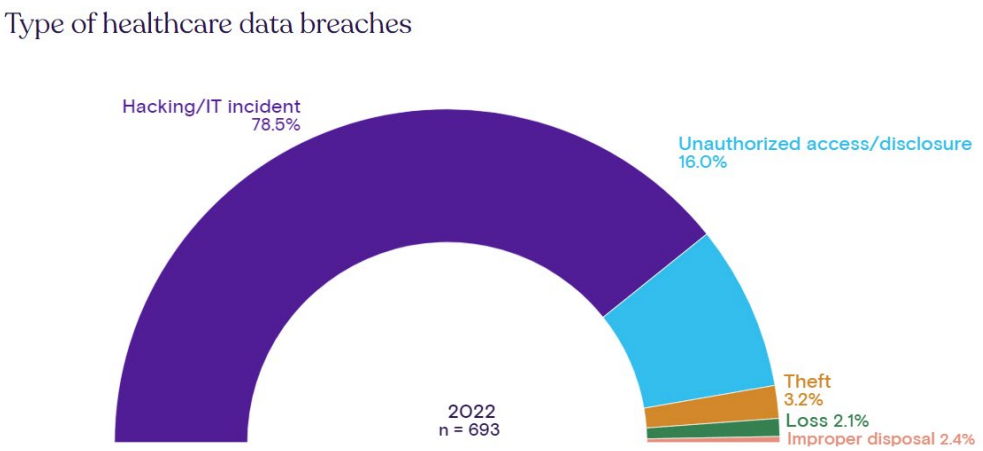
Primjer	Obavijestiti DPA	Obavijestiti ispitanike	Preporuke
Voditelj je pohranio sigurnosnu kopiju arhive osobnih podataka kriptiranih na USB ključ. Ključ je ukraden tijekom provale.	Ne	Ne	Ako je state of the art enkripcija, te postoji backup
Voditelj održava online uslugu. Uslijed kibernetičkog napada na taj servis dolazi do eksfiltracije osobnih podataka pojedinaca.	Da, ako ima posljedica za ispitanike	Da	
Kratak prekid struje koji je trajao nekoliko minuta u pozivnom centru voditelja obrade, što znači da korisnici ne mogu nazvati uslugu i pristupiti podacima	Ne	Ne	Nije povreda koju treba prijaviti, ali treba zabilježiti da se dogodila
Voditelj obrade trpi napad ransomwarea koji rezultira šifriranjem svih podataka. Nema dostupnih sigurnosnih kopija i podaci se ne mogu vratiti.	Da – gubitak dostupnosti	Da	Ako bi postojao backup ne bi trebalo prijaviti

Najčešće povrede podataka u zdravstvu (globalno)

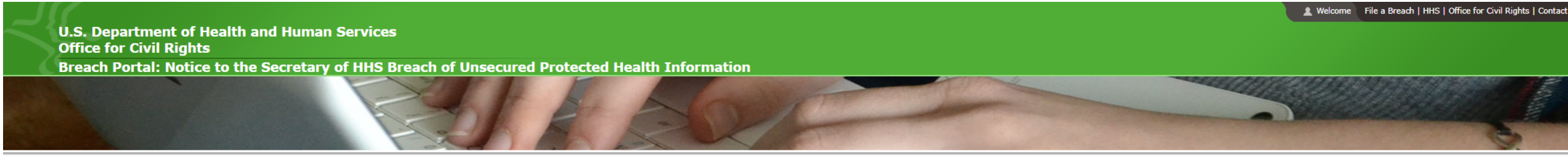
Sjedinjene Države

693 incidenta povrede osobnih podataka u zdravstvu u 2022.

Propis HIPAA na snazi od 1996, uređuje protok elektroničkih podataka u zdravstvu



US DHHS: Breach Portal



Under Investigation | Archive | Help for Consumers

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

Show Advanced Options

Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Health First, Inc.	FL	Healthcare Provider	14171	09/22/2023	Hacking/IT Incident	Email
	Arkansas Total Care, Inc.	AR	Health Plan	578	09/21/2023	Hacking/IT Incident	Network Server
	Virginia Dept. of Medical Assistance Services	VA	Health Plan	1229333	09/18/2023	Hacking/IT Incident	Network Server
	Erlanger Health, Inc.	TN	Healthcare Provider	2753	09/18/2023	Hacking/IT Incident	Other
	Nuance Communications, Inc.	MA	Business Associate	1225054	09/15/2023	Hacking/IT Incident	Network Server
	Oak Valley Hospital District	CA	Healthcare Provider	283629	09/15/2023	Hacking/IT Incident	Network Server
	VA Dept. of Medical Assistance Services	VA	Health Plan	928	09/14/2023	Hacking/IT Incident	Network Server
	Pharm-Pacc Corporation	FL	Business Associate	3749	09/12/2023	Hacking/IT Incident	Network Server
	Sutter North Surgery Center	CA	Healthcare Provider	861	09/08/2023	Hacking/IT Incident	Network Server
	Laboratory Corporation of America Holdings dba LabCorp	NC	Healthcare Provider	1431	09/08/2023	Unauthorized Access/Disclosure	Other
	Ryders Health Management LLC	CT	Healthcare Provider	7252	09/07/2023	Hacking/IT Incident	Network Server
	United Healthcare Services, Inc. Single Affiliated Covered Entity	CT	Health Plan	315915	09/07/2023	Unauthorized Access/Disclosure	Network Server, Other
	Roseman University of Health Sciences	NV	Healthcare Provider	4622	09/06/2023	Hacking/IT Incident	Network Server
	Amerita	KS	Healthcare Provider	219707	09/05/2023	Hacking/IT Incident	Network Server
	Delta Dental of California	CA	Health Plan	500	09/05/2023	Hacking/IT Incident	Network Server
	Bloom Health Centers	MD	Healthcare Provider	1545	09/01/2023	Unauthorized Access/Disclosure	Email
	North Mississippi Medical Center, Inc.	MS	Healthcare Provider	950	09/01/2023	Hacking/IT Incident	Email
	MedMinder Systems, Inc.	MA	Healthcare Provider	12146	09/01/2023	Hacking/IT Incident	Network Server
	Enzo Clinical Labs, Inc.	NY	Healthcare Provider	1700	08/31/2023	Hacking/IT Incident	Network Server

Primjeri povreda u zdravstvu

- Najveća kazna u iznosu od 1,5 milijuna eura izrečena je u Francuskoj zbog curenja podataka kod dobavljača softverskih rješenja za medicinske laboratorije. Incident je rezultirao curenjem podataka o gotovo 500,000 ispitanika.
- Francuski DPA (CNIL) identificirao je nekoliko povreda OUZPa - **nedostatne tehničke i organizacijske mjere zaštite podataka** - podaci koji miruju nisu bili pohranjeni u kriptiranom obliku, nije implementiran standardizirani postupak za operacije migracije podataka i da su (javna) područja relevantnih poslužitelja bila dostupna bez autentifikacije.
- Slučaj pokazuje da je u osmišljavanju, provedbi i procjeni tehničkih i organizacijskih mjera zaštite podataka potrebno također uzeti u obzir područja koja se nalaze uz "osnovne" aktivnosti obrade podataka, kao što su procesi migracije podataka i druga (javna) područja IT sustava koji se koriste.
- Interni procesi koji se odnose na IT podršku trebaju biti poznati službeniku – a on u tom smislu treba moći dati svoje sugestije kako ih osigurati od povrede primjenom mjera kao što je enkripcija, penetracijsko testiranje, otkrivanje neovlaštenog pristupa i drugih mjera koje se odnose na zaštitu IT sustava

Primjeri povreda u zdravstvu

- **(Ne)dostupnost podataka** također je postala podložna novčanim kaznama. Irski DPA (DPC) je s 460.000 eura drugu najveću novčanu kaznu u zdravstvenom sektoru u izvještajnom razdoblju izrekao voditelju obrade koji je pretrpio napad ransomwarea. Tijekom napada pristupljeno je, izmijenjeno i/ili uništeno podataka koji se tiču oko 70.000 ispitanika. Trajno je pogođeno oko 2500 zapisa.
- Novčanu kaznu (od 20.000 eura) zbog **nedostupnosti podataka** također je odredio Hellenic DPA. U ovom slučaju, zahtjev pacijenta za pristup neobrađenim podacima slikovnog pregleda nije mogao biti ispunjen jer su originalne slike bile izbrisane, a pohranjena je samo liječnička procjena.
- Kao ponavljajući razlog za novčane kazne javlja se **nedostatak (ili nedovoljna provedba) pravila pristupa podacima** pacijenata. Na primjer, talijanski DPA (Garante) izrekao je novčane kazne od 70.000 EUR, 50.000 EUR i 40.000 EUR u slučajevima kada su zaposlenici zdravstvene ustanove čak pristupili zdravstvenim podacima pacijenata iako nisu bili uključeni u liječenje pacijenata i takav pristup nije bio potreban.

Primjeri povreda u zdravstvu

- Nekoliko slučajeva odnosilo se na **nenamjerno otkrivanje** podataka pacijenata. Izrečene kazne pokrivaju posebno širok raspon.
- Talijanski DPA odredio je kaznu od 7.000 EUR u dva slučaja u kojima je pojedinac greškom primio medicinsku dokumentaciju drugog pacijenta putem e-pošte (ETid-1528, ETid-1274) i 3.000 EUR za gubitak kartona jednog pacijenta (ETid-1416).
- S druge strane, u slučaju kada su povjerljivi zdravstveni podaci pacijenta poslani e-poštom na više od 1870 primatelja u nezaštićenom privitku, kazna koju je odredio DPA otoka Man iznosila je 202 000 eura (ETid-1352).

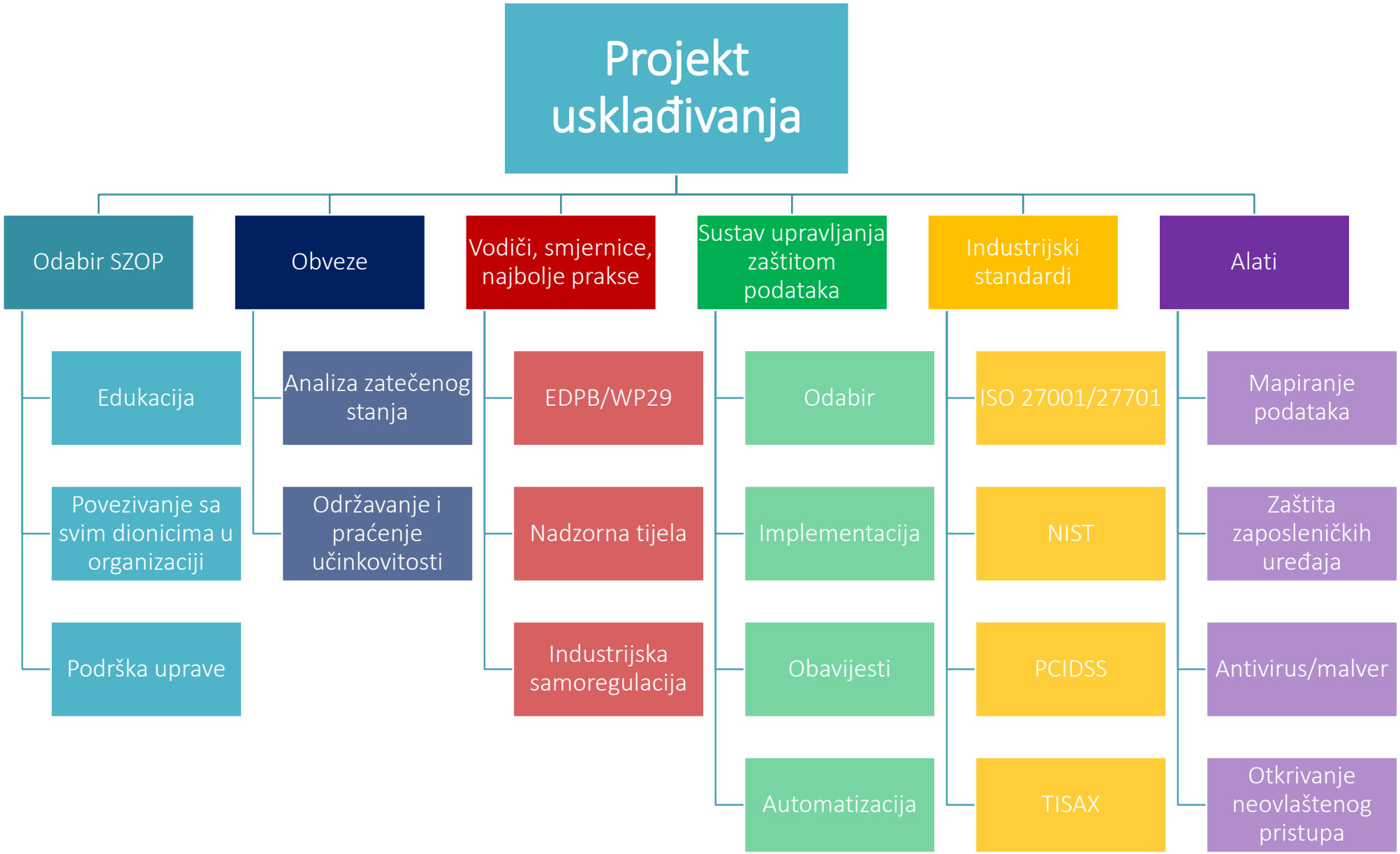
Kazne u zdravstvenom sektoru

- Do sada je 25 nadzornih tijela izreklo **194 kazne** (94 2022., 46 sredinom 2021.) za povrede podataka na području zdravstvenih usluga
- Kazne su izrečene **bolnicama, lancima ljekarni, privatnim klinikama, dobavaljačima farmaceutskih i medicinskih potrepština**
- Prema broju izrečenih kazni u ovom sektoru, prednjači Italija
- U proteklih godinu dana, izrečen je broj kazni dva puta (!) viši od ukupnog broja kazni izrečenih voditeljima obrade u tom sektoru u do sredine 2021

Kazne u zdravstvenom sektoru

- Kazne i dalje relativno **skromne**
- Kažnjeno petnaestak bolnica
  - Najviša kazna 400,000 € portugalskoj bolnici
- Kažnjeno šest laboratorija
  - Najviša kazna 1,500,000 eura francuskom laboratoriju
- Desetak ljekarni
- Desetak manjih klinika
- Najčešći uzrok kazni jesu:
  - **Nedovoljne tehničke i organizacijske mjere**
  - **Povrede odredbi o notifikaciji DPA i ispitanika u slučaju povrede**
  - **Nedostatna suradnja s nadzornim tijelom**
  - **Povreda načela obrade**

Kako do usklađivanja?



Popis aktivnosti u planu usklađivanja

Prepoznati informacijske sustave i usluge	Ustanoviti i i pripremiti vođenje evidencije aktivnosti obrade	Dopuna i daljnji razvoj interne politike zaštite podataka	Edukacija uprave organizacije i djelatnika o obvezama zaštite podataka
Utvrditi uloge organizacije i obveze obavijesti ispitanika o obradi	Upravljanje privolama ako se koriste i provjera kontakata, obavijesti o pravima	Popis tehničkih i organizacijskih mjera, procjena rizika i drugih sigurnosnih kontrola	Definirati program i kalendar aktivnosti edukacije i pripremiti sadržaj
Pripremiti postupke za ispunjenje zahtjeva ispitanika	Redovita provjera odnosa voditelj i izvršitelj	Uspostavljanje i razrada položaja, zadataka i izvještavanja službenika za zaštitu podataka, uspostava tzv. Privacy Networka u organizaciji	Organizirati pohađanje programa inhouse ili pohađanje na tržištu etabliranih ili certificiranih programa
Upravljanje incidentima povrede osobnih podataka	Redovita provjera obrada pod obvezom procjene učinka i drugih periodičnih obveza	Uspostava sustava za mjerenje sukladnosti organizacije – periodične provjere, dijagnostika i izrada izvještaja	Osigurati resurse i plan razvoja kompetencija službenika za zaštitu podataka i njegovog tima (ako postoji)

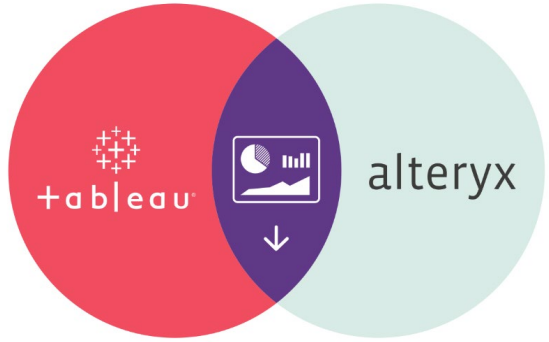
Data discovery/ dana mapping alati

Što su i čemu služe alati za data mapping?

Alati za data mapping, ili mapiranje podataka, su softverska rješenja koja omogućavaju vizualizaciju, analizu i upravljanje tokom podataka unutar organizacije

Pomažu u identifikaciji kako i gdje se podaci pohranjuju, obrađuju i prenose, omogućavajući bolje upravljanje i zaštitu informacija.

- Poboljšana sigurnost i zaštita podataka
- Optimizacija poslovnih procesa
- Bolja integracija sustava
- Podrška donošenju odluka



Zašto koristiti okvire za usklađivanje (compliance frameworks)

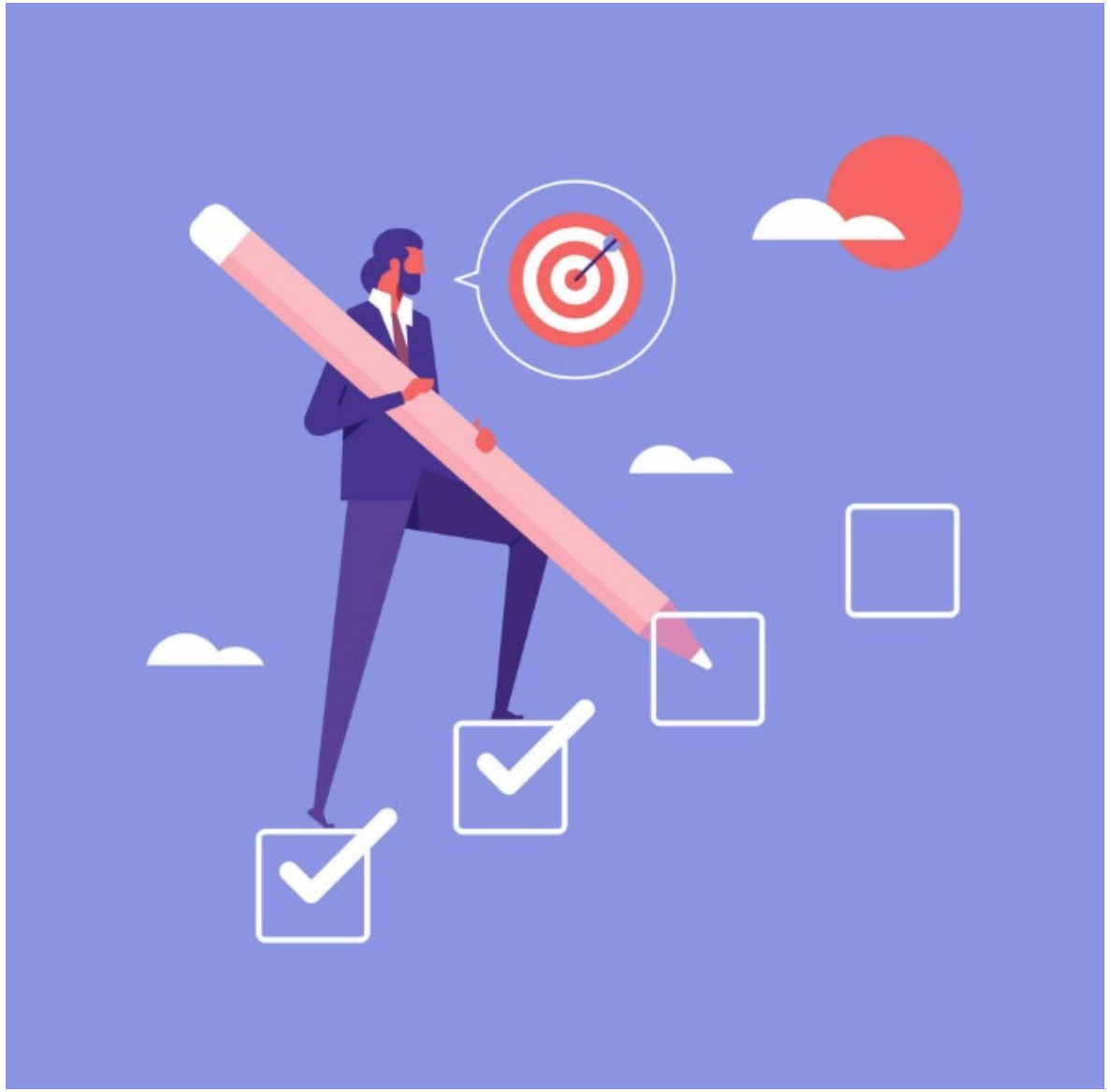
Strukturirani pristup - pružaju jasan i strukturiran način za pristup pitanjima usklađenosti s OUZP-om.

Upravljanje rizicima - pomažu u identifikaciji i upravljanju rizicima povezanim s obradom osobnih podataka.

Efikasna implementacija - omogućuju organizacijama da efikasno implementiraju i održavaju politike i procedure za zaštitu podataka.

Dokumentacija i izvještavanje - pomažu u stvaranju potrebne dokumentacije i izvještaja za praćenje i dokazivanje usklađenosti s regulatornim zahtjevima.

Obrazovanje i svijest o zahtjevima zaštite podataka - Potiču svijest o zaštiti podataka unutar organizacije



Kojim kategorijama voditelja se isplati koristiti takve okvire?

Velika trgovačka društva i multinacionalne kompanije
- Imaju kompleksnije operacije
- Veći volumen podataka za upravljanje

Zdravstvene i financijske institucije
- Organizacije koje rukuju osjetljivim osobnim podacima
- Stroži, često sektorski pobliže definirani zahtjevi (EHealth Data Space, DORA itd.)

E-commerce i davatelji digitalnih usluga
- Imaju velike količine korisničkih podataka
- Mogu biti posebno podložni rizicima povezanim s obradom podataka

Javne institucije i vladine agencije
- Također imaju stroge zahtjeve za zaštitu osobnih podataka
- Često upravljaju velikim količinama podataka
- Specifični, stroži propisi

Brzorastuće start-up tvrtke
- Nemaju resurse kao veće organizacije, ali rastu brže od sposobnosti da se urede
- Primjena okvira može pomoći u uspostavirobustnih procedura za zaštitu podataka od samog početka
- Lakše je uvesti pravila o zaštiti podataka na novu, rastuću organizaciju nego na postojeću

Velika trgovačka društva

Organizacije u zdravstvu

Financijske organizacije

Vladine agencije i tijela državne vlasti

Brzorastući startupi

Industrijski samoregulacijski standardi korisni na području usklađivanja s OUZP

Industrijski samoregulacijski standardi mogu biti koristan način da organizacije postave čvrste osnove za zaštitu podataka u skladu s OUZP.

Slijedi pregled nekoliko ključnih standarda, njihove specifičnosti i primjera kontrola koje koriste:

ISO/IEC 27001 (Sustav upravljanja sigurnošću informacija - ISMS)

- Fokusira se na upravljanje rizikom i sigurnost informacija kroz postavljanje politika i postupaka koji štite informacijske resurse organizacije.
- Sadrži kontrole pristupa, upravljanja incidentima, kontinuirano praćenje i poboljšanje, obrazovanje i svijest o sigurnosti.

ISO/IEC 27701 (Upravljanje osobnim informacijama)

- Dodatak prethodno navedenom ISO/IEC 27001
- Sadrži kontrole procjena rizika povezane s osobnim informacijama, upravljanje pravima ispitanika, osiguranjem povjerljive obrade podataka i transparentnosti obrade
- Evidencija i dokumentacija odgovornog postupanja s podacima

NIST Privacy Framework

- Američki nacionalni standard koji nudi fleksibilan i prilagodljiv pristup upravljanju rizikom privatnosti, fokusirajući se na etičke prakse u vezi s osobnim podacima
- Široko prepoznat i korišten u globalnoj industriji
- Sadrži brojne kontrole koje se mogu primijeniti na području zaštite podataka poput identifikacije i mapiranja podataka, minimizacije prikupljanja podataka, osiguranjem pravodobne reakcije na incidente i zahtjeve ispitanika

Kibernetičke prijetnje i maliciozni programi

- usluge otkrivanja i prevencije upada koje se nadziru 24 sata dnevno / 7 dana u tjednu i uključuju mogućnost provođenja revizijske analize i provjere integriteta sustava
- skeniranja tehničkih ranjivosti koja pravodobno identificiraju i zakrpaju stavke, odgovarajuće testiranje zakrpa i dokumentacija o testiranju zakrpa koja se održava i povremeno pregledava
- mehanizmi izvješćivanja za procjenu i poduzimanje popravnih radnji
- uspostavljeni sustavi za primanje ranih upozorenja, upozorenja i zakrpa
- tamo gdje sustav dopušta, mobilni uređaji koji se spajaju na mrežu moraju biti usklađeni s trenutnim zahtjevima za zaštitu od zlonamjernog softvera i redovito se skeniraju
- sigurnosne zakrpe koje osiguravaju dobavljači trebaju se instalirati na vrijeme kako bi se ublažile ranjivosti i zaštitile od kibernetičkih prijetnji. Pružatelji zdravstvenih usluga trebaju imati standardne procese kontrole promjena s obavijesti o prekidima i zakazanim prozorima za primjenu ovih zakrpa.
- mrežni vatrozidi trebaju se pregledavati u redovitim intervalima, u skladu s pristupom temeljenim na riziku za zamjenu/ili nadogradnju, te redovito testirati na upad
- centralno upravljanu antimalware uslugu

Pohrana podataka u zdravstvenim organizacijama

Pohrana u podatkovnim centrima

Sve informacije o zdravstvenom sustavu trebaju biti hostane, transakcije, obrada i podrška u podatkovnim centrima koji su povezani visokom propusnošću, komunikacijom niske latencije i podržani pouzdanom infrastrukturom i uslužnim programima.

To je zbog kritičnosti, volatilnosti, osjetljivosti i količine podataka o pacijentima i osigurat će da su informacije dostupne 24 sata dnevno, svaki dan u godini.

Bez obzira na to upravljaju li podatkovnim centrima i uslugama izravno pružatelji zdravstvenih usluga, ugovorni subjekt ima odgovornost osigurati odgovarajuće mjere za zaštitu podataka.

Pohrana podataka

Pohranjivanje na radnim stanicama računala

Tvrdi diskovi/SSD računala radne stanice ne smiju se koristiti kao primarna ili trajna pohrana zdravstvenih informacija.

Tamo gdje se ovi tvrdi diskovi koriste za privremenu pohranu, podaci moraju biti podvrgnuti strogim sigurnosnim kontrolama (vidi fizičku sigurnost) Povjerljivi ili osobni podaci ne smiju se pohranjivati na tvrdim diskovima radnih stanica.

Pohranjivanje u izlaznim uređajima

Pisači, faksimilni uređaji i drugi uređaji koji ispisuju povjerljive ili osobne podatke su podvrgnute sigurnosnim kontrolama. Ove kontrole mogu uključivati fizičku lokaciju u sigurnim područjima, kontrole PIN-a/ lozinke i/ili nadzor osoblja.

Ispis iz sustava koji sadrže visokorizične ili klasificirane podatke ne bi se trebao odvijati bez kontrole PIN-a ili lozinke. Gdje to nije moguće, moraju se primijeniti odgovarajuće fizičke sigurnosne mjere kako bi se zaštitili podaci.

Ako izlazni uređaji pohranjuju podatke na unutarnje tvrde diskove, oni se moraju uništiti u skladu s pravilima o odlaganju medija za pohranu

USB uređaji

Samo USB uređaji odobreni od zdravstvenog sustava mogu se povezati s informacijskim i ICT okruženjem zdravstvenog sustava kako bi bio zaštićen od zlonamjernih kodova i virusa. Ovi šifrirani USB uređaji sigurni su za korištenje i prikazuju logo Ministarstva zdravstva na bočnoj strani jedinice.
Upotreba USB uređaja zdravstvenog sustava koji nisu certificirani u mreži zdravstvenog sustava zabranjena je i predstavlja povredu sigurnosti

Prijenos podataka i odlaganje medija za pohranu

Kada se informacije prenose izvan mreže zdravstvenog sustava (npr. šalju se epoštom, SMS-om ili društvenim medijima preko interneta, javnih komutiranih telekomunikacijskih mreža ili nezaštićenih bežičnih mreža), smatraju se nezaštićenim informacijama u prijenosu.

Povjerljive ili zdravstvene informacije ne smiju se prenositi nezaštićenim kanalima bez upotrebe odgovarajuće kriptografije. Prijenos osobnih podataka također može zahtijevati posebna odobrenja

Odlaganje medija za pohranu

Medij za pohranjivanje koji više nije potreban, treba se zbrinuti na siguran način koji odgovara osjetljivosti informacija.

Podaci sadržani u fizičkim medijima ili opremi trebaju se ukloniti korištenjem odgovarajućih metoda dezinfekcije podataka u vrijeme stavljanja izvan pogona ICT opreme (uključujući mobilne telefone).

Jedine sigurne metode podatkovne higijene i uništavanja su:

- fizičko uništavanje medija za pohranu podataka nakon uklanjanja iz ICT opreme, na primjer, fizičko bušenje kroz tvrde diskove ili elektroničke medije za pohranu;
- korištenje usluga dezinfekcije i uništavanja ICT opreme koje se pružaju u okviru usluge odlaganja i recikliranja otpada
- sigurno brisanje diska ili medija za pohranu pomoću softvera.
- Pisanu potvrdu da su podaci uklonjeni s medija za pohranu treba dobiti i zadržati pružatelj zdravstvenih usluga.

Fizička sigurnost 1/3

Potrebno je slijediti pristup upravljanja rizikom kako bi se identificirale i provele fizičke kontrole.

Ovaj pristup uzetima u obzir sljedeće:

- Perimetar fizičke sigurnosti – zaštitite područja koja sadrže osjetljive ili kritične informacije i ICT objekte (npr. odgovarajuću građevinsku strukturu od poda do stropa, protupožarna vrata, sustave za otkrivanje uljeza, CCTV)
- Kontrole fizičkog ulaska – sigurna područja koja dopuštaju pristup samo ovlaštenom osoblju (tj. evidencija datuma/vremena posjetitelja, mehanizmi autentifikacije kao što su pristupne kartice, revizijski trag, posjetitelji/osoblje nosi vidljivu identifikaciju, trećim stranama odobren je ograničeni pristup)
- Sigurni uredi, prostorije i objekti – fizička sigurnost ureda, prostorija i objekata uključena je u planiranje i izgradnju
- Rad u sigurnim područjima – postupci za osoblje i pružatelje usluga treće strane na temelju 'potrebe znanja', rad bez nadzora ograničen kako bi se izbjegle zlonamjerne aktivnosti, korištenje fizičkih brava za prazna područja s planovima pregleda.

Fizička sigurnost 2/3

- Položaj i zaštita opreme – razmatranje lokacije i zaštite kako bi se smanjile prijetnje okolišu i opasnosti ili mogućnosti za neovlašteni pristup (tj.položaj ICT objekata koji čuvaju osjetljive podatke kako bi se smanjilo gledanje od strane neovlaštenog osoblja, sigurne skladišne prostorije, nadzor okoline kao što su vlažnost i umjerena temperatura). Opremu treba pravilno održavati kako bi se osigurala njezina stalna dostupnost i cjelovitost
- Pomoćni uređaji – osigurajte da je oprema zaštićena od nestanka struje i drugih poremećaja uzrokovanih kvarovima na pomoćnim uređajima (dostupna rasvjeta i komunikacije u nuždi, prekidači/ventili za nuždu za isključivanje struje, voda, plin i drugi uređaji koji se nalaze i rade). Upravu treba upozoriti u slučaju problema
- Oprema bez nadzora – osigurajte da je oprema koja se ne koristi dovoljno zaštićena (tj. čuvar zaslona zaštićen lozinkom na računalima, odjava iz aplikacija koje se ne koriste, sigurnosne kontrole poput lozinki na mobilnim uređajima)
- Politika čistog stola i čistog zaslona – osjetljive ili kritične poslovne informacije treba sigurno zaključati kako bi se spriječilo neovlašteno gledanje ili reprodukcija informacija, računala zaključana ili odjavljena kada su bez nadzora.

Fizička sigurnost 3/3

- Zaštita od vanjskih prijetnji i prijetnji iz okoliša – fizička zaštita i izbjegavanje prirodnih katastrofa, zlonamjernih napada ili nesreća (tj. odluke o planiranju za izbjegavanje štete od požara, poplave, potresa, eksplozije, građanskih nemira i drugih oblika prirodnih katastrofa ili katastrofa uzrokovanih ljudskim djelovanjem)
- Područja za isporuku i utovar – kontrola pristupnih točaka za područja za isporuku i utovar s izolacijom gdje je to moguće od ICT obradnih objekata (tj. ograničenje osoblja, osigurana vanjska vrata, inspekcija ulaznih materijala i evidentirano prema zahtjevima upravljanja imovinom)
- Sigurnost kablova – energetski i telekomunikacijski kablovi koji prenose podatke ili prateće informacijske usluge trebaju biti zaštićeni od presretanja, smetnji ili oštećenja
- Imovina izvan lokacije – oprema, informacije ili softver ne smiju se odnositi izvan lokacije bez prethodnog odobrenja. Kada je izvan lokacije, sigurnost bi se trebala primijeniti na imovinu izvan lokacije uzimajući u obzir različite rizike rada izvan prostorija organizacije.

Rad na daljinu i daljinski pristup

Rad na daljinu odnosi se na sve oblike rada izvan ureda, uključujući netradicionalna radna okruženja, kao što su rad na daljinu, fleksibilno radno mjesto, rad na daljinu i virtualna radna okruženja.

Pružatelji zdravstvenih usluga odgovorni su osigurati da ICT infrastruktura bude primjerena za podršku funkcijama rada na daljinu njihovog osoblja i odgovorni su za financiranje ICT zahtjeva za rad na daljinu.

Zahtjevi za daljinski pristup nisu automatski i neki zahtjevi mogu biti odbijeni zbog sigurnosnih ili infrastrukturnih razloga. Zahtjevi navedeni u nastavku također se primjenjuju:

- odgovarajuća infrastruktura mora se temeljiti na zahtjevima (procjenama troškova i prikladnosti)
- softver za zaštitu od virusa mora biti instaliran i redovito ažuriran
- sigurnosne softverske zakrpe moraju se primijeniti gdje je to moguće
- ako koristite radne stanice i objekte preko interneta za pristup uslugama zdravstvenog sustava, osoblje ne smije koristiti funkcije pred-memoriranja korisničkog ID-a/lozinke niti pohranjivati nezaštićeni osjetljivi materijal na ovim uređajima.
- infrastruktura mora biti pohranjena na sigurnom mjestu
- (Radne stanice zdravstvenog sustava RH povezane su s mrežom zdravstvenog sustava putem namjenskih veza i ne smiju biti povezane s drugim mrežama ili internetom ni na koji način osim putem veze zdravstvenog sustava)
- poduzeti razumne zaštitne mjere za zaštitu opreme i podataka od krađe, gubitka ili oštećenja na lokaciji izvan zdravstvene ustanove
- podatkovne datoteke procesa koji se lokalno odvijaju trebaju se redovito sigurnosno kopirati, po mogućnosti na sigurne poslužitelje datoteka, kako bi se izbjegao gubitak zbog kvara opreme, oštećenja ili krađe
- ICT imovina koju osigurava zdravstveni sustav resursi su javnog sektora i njima se mora upravljati u skladu s tim. Za savjete o upravljanju softverskom imovinom obratite se Jedinici za upravljanje softverskom imovinom (koju naravno nemamo)

Nabava, razvoj i održavanje sustava

Zahtjevi informacijske sigurnosti trebali bi biti uključeni kao sastavni dio cjelokupnog životnog ciklusa razvoj a i održavanja informacijskih sustava:

Ovo uključuje:
- integriranje zahtjeva informacijske sigurnosti u ranim fazama prikupljanja zahtjeva i dizajna za nove informacijske sustave ili poboljšanja postojećih informacijskih sustava;
- zaštita informacija uključenih u transakcije aplikacijskih usluga kako bi se spriječio nepotpuni prijenos, krivo usmjeravanje, neovlaštena izmjena poruka, neovlašteno otkrivanje, umnožavanje ili ponovno reproduciranje poruka.
- odgovarajuću zaštitu okruženja za razvoj sustava, testiranje i obuku, uzimajući u obzir osjetljivost podataka, kontrolu pristupa, praćenje promjena okruženja i koda koji je u njemu pohranjen, te stupanj outsourcinga povezanog s razvojem sustava;
- testiranje sigurnosne funkcionalnosti tijekom razvoja. Treba odabrati podatke o ispitivanju pažljivo, zaštićeno i kontrolirano;
- zabranu korištenja operativnih podataka koji sadrže osobne podatke ili druge povjerljive podatke u testne svrhe;
- implementacija formalnih i strukturiranih procesa kontrole promjena kako bi se osiguralo odgovarajuće upravljanje promjenama;
- odvajanje razvojnih, testnih i operativnih okruženja kako bi se smanjili rizici od neovlaštenog pristupa ili promjena u radnom okruženju;
- rješavanje ciljeva informacijske sigurnosti u fazama upravljanja projektom i uključivanje sigurnosnih rizika u procjenu operativnih i projektnih rizika;
- podržavanje potrebne raspoloživosti ICT infrastrukture kroz mjere kao što su redundancija, failover, pristupi otporni na greške i upravljanje kapacitetima.

Upravljanje sigurnosnim incidentima

Incident informacijske sigurnosti je svaki događaj koji rezultira neovlaštenim pristupom podacima, aplikacijama, uslugama, mrežama i/ili uređajima, zaobilazeći temeljne sigurnosne mehanizme.

Sigurnosni incidenti mogu biti slučajni ili namjerni, a mogu uključivati:

- povrede pristupa od strane pojedinca ili softvera;
- povrede integriteta ili povjerljivosti informacija;
- korupcija ili otkrivanje zdravstvenih informacija;
- gubitak dostupnosti informacijskih sustava;
- nepoštivanje pravila ili smjernica;
- povrede mjera fizičke sigurnosti; i
- nekontrolirane promjene sustava.

Kazneni zakon – čl. 146 Nedozvoljena upotreba osobnih podataka

(1) Tko protivno uvjetima određenima u zakonu prikuplja, obrađuje ili koristi osobne podatke fizičkih osoba, kaznit će se kaznom zatvora do jedne godine.

(2) Tko protivno uvjetima određenima u zakonu iznosi osobne podatke iz Republike Hrvatske u svrhu daljnje obrade ili ih objavi ili na drugi način učini dostupnim drugome ili tko radnjom iz stavka 1. ovoga članka sebi ili drugome pribavi znatnu imovinsku korist ili prouzroči znatnu štetu, kaznit će se kaznom zatvora do tri godine.

(3) Kaznom iz stavka 2. ovoga članka kaznit će se tko djelo iz stavka 1. ovoga članka počini prema djetetu ili tko protivno uvjetima određenima u zakonu prikuplja, obrađuje ili koristi osobne podatke fizičkih osoba koji se odnose na rasno ili etničko podrijetlo, politička stajališta, vjerska ili druga uvjerenja, sindikalno članstvo, zdravlje ili spolni život te osobne podatke fizičkih osoba o kaznenom ili prekršajnom postupku.

(4) Ako kazneno djelo iz stavka 1. do 3. ovoga članka počini službena osoba u obavljanju svojih ovlasti, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

Glava XXV KZ Kaznena djela protiv računalnih sustava, programa i podataka

Članak 266.: Neovlašteni pristup

Članak 267.: Ometanje rada računalnog sustava

Članak 268.: Oštećenje računalnih podataka

Članak 269.: Neovlašteno presretanje računalnih podataka

Članak 270.: Računalno krivotvorenje

Članak 271.: Računalna prijevara

Članak 272.: Zloporaba naprava

Članak 273.: Teška kaznena djela protiv računalnih sustava, programa i podataka

Hvala na pažnji!


edpb
European Data Protection Board