Primjena Uredbe o zaštiti osobnih podataka

Dr.sc. Silvana Tomić Rotim

Zavod za informatičku djelatnost Hrvatske d.o.o.

Sadržaj

- Uobičajene aktivnosti usklađenja
- Osnovne informacije o GDPR-u
- GAP analiza
- Identifikacija evidencija osobnih podataka
- DPIA
- Tehničke i organizacijske mjere
- Rasprava

Uobičajene aktivnosti usklađenja

- Edukacija i savjetovanje (radionice) uprave i ključnih dionika poslovnih procesa
- Provedba GAP analize – radionice s odgovornim osobama s ciljem snimke trenutnog stanja i izrada preporuka za usklađivanje s Uredbom
- Identifikacija evidencija osobnih podataka
- DPIA - Analiza utjecaja na zaštitu osobnih podataka
- Implementacija organizacijskih i tehničkih sigurnosnih mjera

Opća uredba o zaštiti podataka - GDPR

- Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka - Opća uredba o zaštiti podataka – General Data Protection Regulation (GDPR).
- Stupila na snagu 24. svibnja 2016. godine.
- Izravno će se primjenjivati u EU od 25. svibnja 2018. godine.
- Napredak u području zaštite osobnih podataka.

Struktura Uredbe

- 173 recitala
  - Daje temeljna načela o zaštiti pojedinaca u vezi s obradom njihovih osobnih podataka
- 99 članaka u 11 poglavlja
  - Utvrđuju pravila povezana sa zaštitom pojedinaca u pogledu obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka
- Link: http://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&qid=1462363761441&from=HR

Svrha i cilj Uredbe

- Zaštita pojedinca i njegovih osobnih podataka te pružanje sigurnosti tvrtkama koje obrađuju osobne podatke.
- Zaštita osobnih podataka - temeljno pravo svakog pojedinca
- Osigurava jednaku razinu zaštite svakom pojedincu iz Europske unije

Na koga se Uredba odnosi?

- Na sve pravne osobe koje posluju u EU ili obrađuju osobne podatke građana EU, što uključuje:
  - Voditelje obrade osobnih podataka
  - Izvršitelje obrade osobnih podataka
- U konačnici, to obuhvaća:
  - Sve javne institucije, urede i agencije
  - Sve tvrtke (i privatne obrte) koje obrađuju osobne podatke u bilo kojem opsegu i količini, bez obzira na lokaciju sjedišta

Osnovni pojmovi - 1

- „osobni podaci" - svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi
- Primjer:
  - Ana Marić kao djelatnica tvrtke ABC je osobni podatak jer u toj tvrtki ne radi niti jedna druga osoba s istim imenom i prezimenom
  - Ana Marić kao stanovnica Zagreba nije osobni podatak jer ima više osoba takvog imena i prezimena i nije moguće jednoznačno identificirati jednu osobu
  - Ana Marić i njen OIB u kombinaciji čine osobni podatak jer je jednoznačno moguće identificirati tu osobu

Osnovni pojmovi - 2

- „ispitanik” - pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca

Osnovni pojmovi - 3

- „obrada” - svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su 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

Osnovni pojmovi - 4

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

Osnovni pojmovi - 5

- "sustav pohrane" - svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi
- Primjer:
  - Baza podataka i dosjei zaposlenika
  - Baza podataka postojećih i potencijalnih korisnika
  - Baza podataka sportaša
  - Baza podataka vlasnika osobnih automobila
  - Zdravstveni kartoni pacijenata

Osnovni pojmovi - 6

- „privola" - ispitanika znači svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose
- *Privola je **nužna** ako: obrada nije zakonski propisana, nema ugovorne osnove za obradu podataka, obrada nije nužna za zaštitu ključnih interesa pojedinaca ili za izvršavanje zadaće od javnog interesa te za potrebe legitimnih interesa voditelja obrade ili treće strane*

Osnovni pojmovi - 7

- „predmetno nadzorno tijelo" - nadzorno tijelo koje je povezano s obradom osobnih podataka jer:
  - voditelj ili izvršitelj obrade ima poslovni nastan na tom državnom području
  - obrada bitno utječe ili je izgledno da će bitno utjecati na ispitanike koji borave u državi članici tog nadzornog tijela
  - je podnesena pritužba tom nadzornom tijelu

Osnovni pojmovi - 8

- „pseudonimizacija” - obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama

Posebne kategorije osobnih podataka

- Podaci koji se odnose na rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca.

Glavne odlike Opće uredbe o zaštiti osobnih podataka

Ispitanici i njihova prava

- Pravo na informiranje o određenoj obradi i pravo na prigovor obradi ako za to ima dobar razlog, npr. profiliranje u svrhu izravnog marketinga
- Pravo na pristup i ispravak svojih podataka
- Blokiranje podataka čija točnost nije dokazana
- Pravo na ograničavanje obrade vlastitih podataka
- Pravo na brisanje ili „pravo na zaborav“
- Obavijest o svakom brisanju, mijenjanju ili blokiranju podataka prema trećoj strani kojoj su podaci otkriveni
- Pravo na prijenos podataka u strukturiranom obliku
- Pravo na naknadu štete

Prvi korak: GAP analiza i izrada preporuka usklađivanja s Uredbom

- *Cilj:* utvrditi razinu sukladnosti / odstupanja od zahtjeva Uredbe
- *Način provedbe:*
  - Primjena check liste
  - Razgovori / radionice s odgovornim osobama
  - Analiza dokumentacije
  - Provjera postojećih mjera zaštite osobnih podataka
- *Rezultat:*
  - Izvješće o provedenoj analizi stanja – status trenutnog stanja i odstupanja od GDPR s identificiranim mjerama usklađenja

GAP analiza_GDPR

Analiza stanja – grupe zahtjeva

- Temelji se na 13 grupa zahtjeva:
  - Politika privatnosti
  - Upravljanje zahtjevima i prigovorima ispitanika
  - Upravljanje rizikom treće strane
  - Nadzor u novim operativnim postupcima
  - Nadzor postupaka rukovanja podacima
  - Struktura upravljanja privatnošću
  - Integracija zaštite osobnih podataka u poslovanje
  - Upravljanje rizicima informacijske sigurnosti
  - Registar osobnih podataka
  - Privole i izjave o privatnosti
  - Program edukacije i podizanja svijesti
  - Upravljanje incidentima
  - Praćenje vanjskih zbivanja

Obveze voditelja obrade 1

- Identificirati i voditi sve evidencije osobnih podataka
- Provesti procjenu utjecaja na zaštitu osobnih podataka (DPIA – Data Protection Impact Assessment)
- Upravljati zahtjevima ispitanika i odgovoriti u roku od 30 dana
- Osigurati zahtjev „jedna obrada – jedna privola”
- Osigurati „pravo na zaborav” za sve ispitanike i čuvanje podataka samo onoliko koliko je potrebno

Obveze voditelja obrade- 2

- Osigurati pravo na pristup i ispravak osobnih podataka
- Osigurati pravo na prijenos osobnih podataka
- Implementirati „privacy by design" principe
- Osigurati prijavu sigurnosnog incidenta u roku od 72 sata
- Imenovati službenika za zaštitu podataka (DPO)
- Implementirati ostale sigurnosne mjere koje proizlaze iz DPIA-e

Drugi korak: Identificirati i voditi sve evidencije osobnih podataka

- Evidencije osobnih podataka

B	C	D	E	F	G	H	I	J	K
Šifra evidencije	Naziv evidencije	Aplikacijski sustav	Vlasnik	Aplikacija sadrži potpis korisnika (digitalni potpis, slika...)	Aplikacija sadrži OIB ili MBG fizičkih osoba	Aplikacija sadrži druge osobne podatke fizičkih osoba	Osobni podaci se pohranjuju u sustav	Osobni podaci se samo čitaju iz drugih sustava za potrebe prikaza u aplikaciji	Postoji mogućnost ispisa / izvoza (pdf, xls, xml...) osobnih podataka
				DA/NE	DA/NE	DA/NE	DA/NE	DA/NE	DA/NE

Atributi evidencije osobnih podataka - 1

- Naziv evidencije:
  - Npr. kadrovska evidencija
- Aplikacijski sustav – u slučaju da se vodi kroz aplikaciju:
  - Npr. aplikacija Evidencija rada
- Vlasnik – funkcija koja je odgovorna za tu evidenciju:
  - Npr. pomoćnik glavnog tajnika HOO

Atributi evidencije osobnih podataka - 2

- Osobni podaci koje evidencija sadrži:
  - Npr. OIB, ime, prezime, adresa...
- Otvorenost aplikacije prema drugim sustavima:
  - Voditelja obrade, drugih institucija, izvan RH...
- Postoji praćenje logova nad aplikacijom:
  - DA/NE

Atributi evidencije osobnih podataka - 3

- 5 Ws:
  - WHY – Zašto prikupljamo osobne podatke?
  - WHO/WHOSE – Čije podatke prikupljamo?
  - WHEN – Kad se podaci obrađuju i koliko dugo se čuvaju?
  - WHERE – Gdje se podaci nalaze: u papirnatom obliku, datotekama ili aplikacijama?
  - WHAT – Koje tipove osobnih podataka prikupljamo i koja je pravna osnova za njihovo prikupljanje?

Zašto je potrebna DPIA?

- Svaka obrada podataka potencijalno može ugroziti nečija prava
- Procjena bi trebala utvrditi postoji li štetan utjecaj na prava i slobodu ispitanika na temelju prirode, opsega ili potrebe planiranih operacija obrade
- Uredba definira kad je obvezno provoditi procjenu utjecaja na zaštitu osobnih podataka

Kada je potrebna DPIA? - 1

GDPR Uredba kaže da je tvrtka dužna provesti procjenu utjecaja na privatnost samo kada obrada:

vjerojatno rezultira visokim rizikom za prava i slobode pojedinca (članak 35 (1)).

Kada je potrebna DPIA? - 2

Procjena utjecaja na zaštitu podataka (DPIA) obvezna je osobito za slučaj:

- Sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima, a koja se temelji na automatskoj obradi, uključujući izradu profila, te na temelju koje se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca ili pak značajno utječu na pojedinca.

- Opsežna obrada posebnih kategorija osobnih podataka ili podataka u vezi s kaznenim presudama i kažnjivim djelima

- Sustavno praćenje javno dostupnog područja u velikoj mjeri.

Kada procjena utjecaja na zaštitu podataka nije nužna?

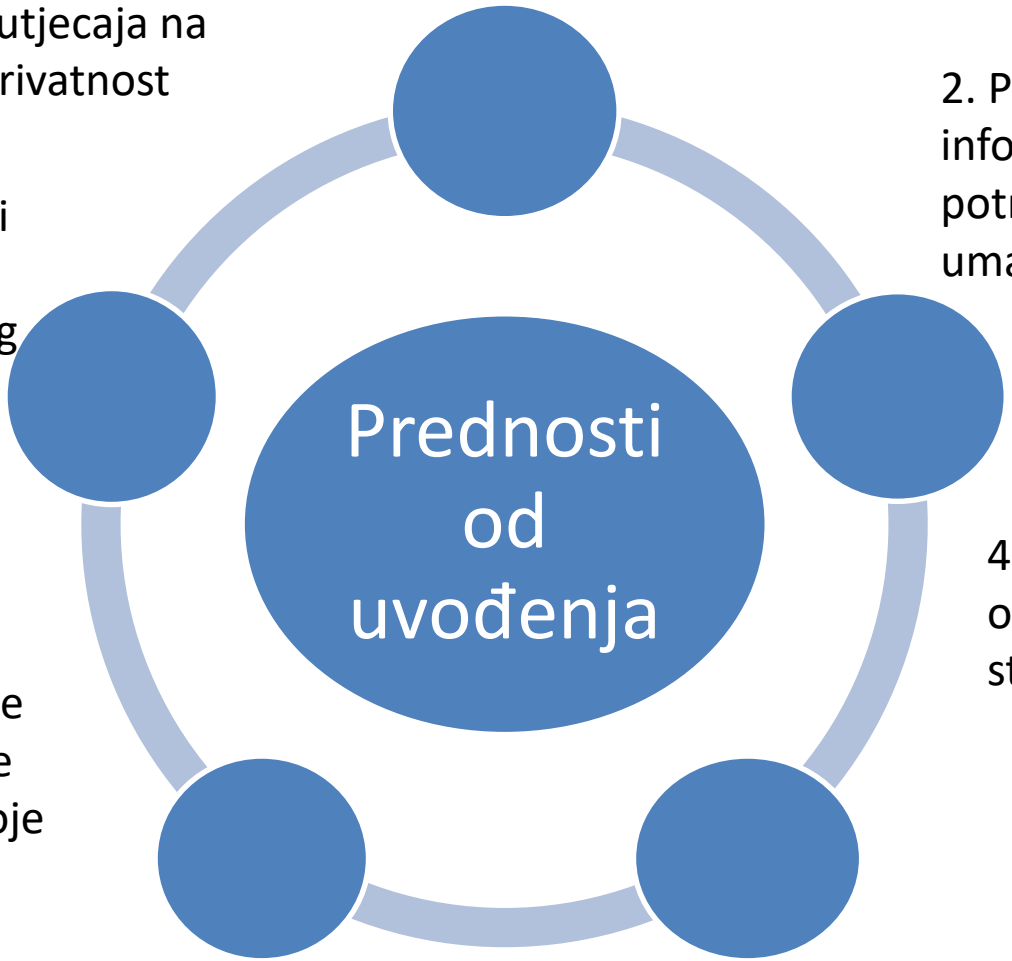
- Kod obrade podataka vezanih samo uz administraciju ili plaće
- Kod obrade administrativnih podataka o osoblju ako podaci nisu povezani s njihovim zdravljem
- Kod računovodstvenih tvrtki, kada se koristi samo za tu svrhu
- Kod obrade podataka za dioničare
- U slučajevima kada se podaci obrađuju jedino i isključivo za registraciju posjetitelja
- U slučajevima kada podatke koriste obrazovne institucije za komunikaciju sa svojim studentima

Prednosti provedbe DPIA

1. Identifikacija rizika i utjecaja na privatnost

2. Pruža vrijedne informacije za definiranje potrebnih mjera za umanjenje rizika

3. Procjena utjecaja i vjerojatnosti rizika novog informacijskog sustava



4. Pruža informacije o privatnosti na strukturiran način

5. Pruža infomacije potrebne za druge funkcionalnosti koje utječu na osobne podatke

6. Pruža dokaze i dijeli rizike za privatnost sa svim zainteresiranim stranama

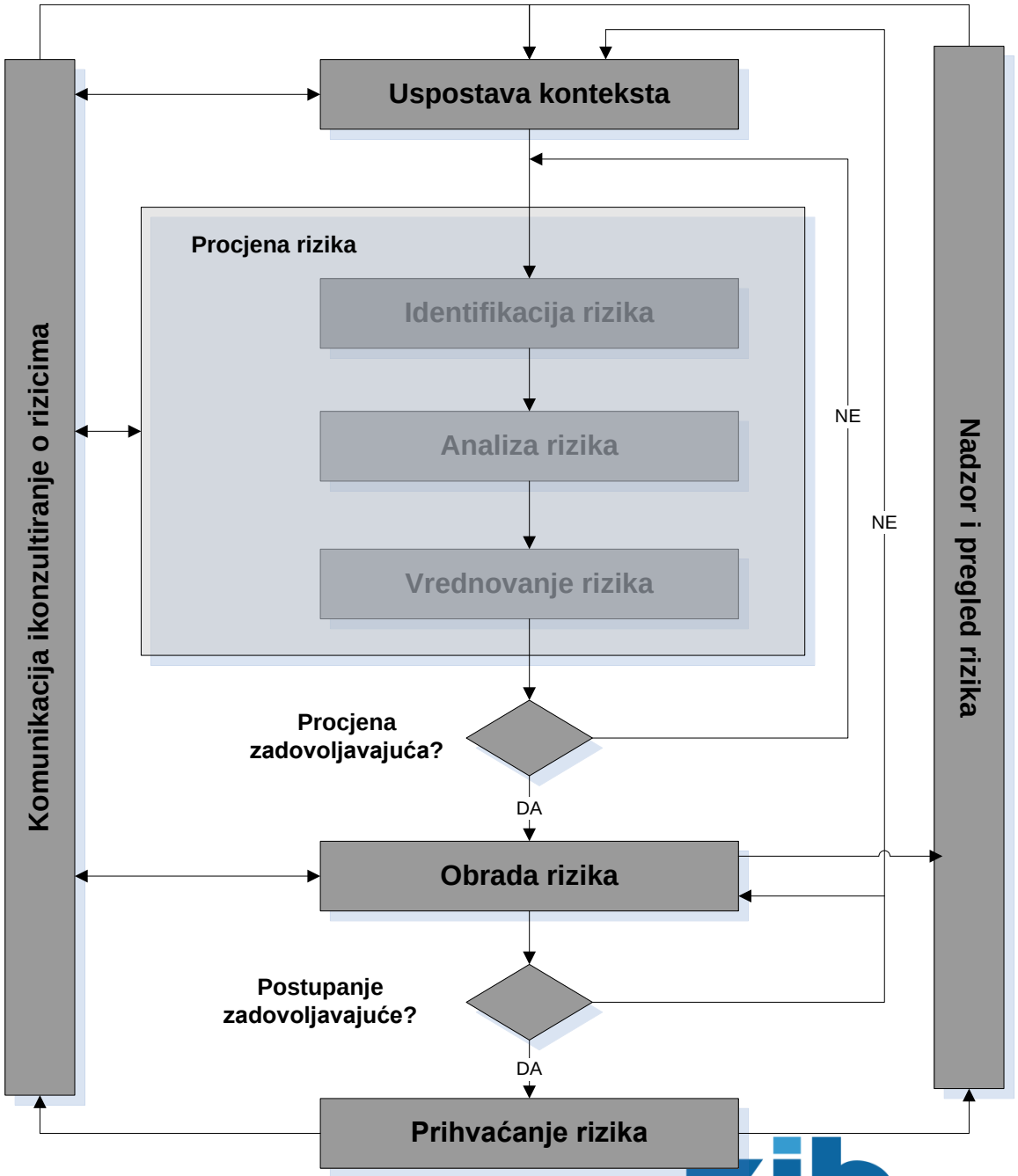
Što DPIA treba sadržati?

GDPR, članak 35

Procjena treba uključiti barem sljedeće:

- opis predviđene obrade i svrhu obrade
- procjenu nužnosti i proporcionalnosti postupaka obrade povezanih s njihovim svrhama
- procjenu rizika za prava i slobode ispitanika
- mjere predviđene za rješavanje problema rizika, sigurnosne mjere i druge mehanizme za zaštitu osobnih podataka

Proces upravljanja rizicima u skladu s ISO 31000



Zavod za informatičku djelatnost Hrvatske d.o.o.

Treći korak: DPIA

Vjerojatnost rizika

Utjecaj	**1 - Niska**	**2 - Srednja**	**3 - Visoka**
1 - Nizak	1	2	3
2 - Srednji	2	4	6
3 - Visok	3	6	9

Razine vjerojatnosti ostvarenja rizika

- **1 - niska** (malo vjerojatno da bi se razmatrani rizik mogao dogoditi, odnosno vjerojatnost njegove pojave je otprilike jednom u dvije godine, ali postoje slučajevi, statistike ili motivi koji bi naznačili njegovo ostvarivanje, povezane ranjivosti procesa, postojeće kontrole koje mogu spriječiti takav događaj su učinkovite),
- **2 - srednja** (vjerojatnost pojave razmatranog rizika je jednom u godini, postoje slučajevi, statistike ili druge informacije koje ukazuju na to da se ovaj ili sličan događaj dogodio, ili postoji naznaka da bi mogli postojati neki razlozi za realizaciju scenarija; povezane ranjivosti bi se mogle iskoristiti; postojeće kontrole su uglavnom učinkovite),
- **3 - visoka** (vjerojatnost pojave razmatranog rizika je više puta u godini, očekuje se pojava, odnosno postoje slučajevi, statistike ili druge informacije koje ukazuju na to da će se razmatrani scenarij vjerojatno pojaviti ili postoje jaki razlozi ili motivi za realizaciju scenarija; povezane ranjivosti se mogu vrlo lako iskoristiti; nisu implementirane kontrole, vjerojatnost pojave događaja je više puta u godini).

Razine utjecaja rizika

- **1 - nizak** (Zanemariv utjecaj na privatnost pojedinaca),
- **2 - srednji** (Srednji utjecaj na privatnost – pojedinačni slučajevi ugrožavanja osobnih podataka),
- **3 - visok** (Veliki utjecaj na privatnost – vrlo veliki broj slučajeva ugrožavanja osobnih podataka i posebne kategorije osobnih podataka).

Potencijalni rizici za ispitanike

- Slučajno ili nezakonito uništenja osobnih podataka
- Gubitak osobnih podataka
- Slučajne ili namjerne izmjene osobnih podataka
- Neovlašteno odavanje ili pristup osobnim podacima koji su prenešeni, pohranjeni ili na drugi način obrađivani, a što osobito može dovesti do fizičke, materijalne ili nematerijalne štete

Primjer mape rizika privatnosti

Naziv grupe/ evidencije osobnih podataka	Rizik	Trenutno implementirane mjere	Vjerojatnost ostvarenja rizika	Utjecaj na privatnost	Razina rizika
Kadrovska evidencija	odavanje osobnih podataka zbog neadekvatne kontrole pristupa	• ograničen broj osoba s pravom pristupa • implementirana kontrola pristupa	1	4	4
	odavanje osobnih podataka od strane ovlaštenih osoba	• ugovor i pravilnik o radu • disciplinski postupak	1	4	4
	neovlaštena izmjena osobnih podataka zbog neadekvatnih sigurnosnih mjera	• ograničen broj osoba s pravom pristupa • implementirana kontrola pristupa • praćenje logova o aktivnostima u aplikaciji	1	4	4
	nekontrolirana izmjena osobnih podataka od strane ovlaštene osobe	• ugovor i pravilnik o radu • disciplinski postupak	1	4	4
	nedostupnost osobnih podataka zbog neadekvatnih tehničko-sigurnosnih mjera	• virtualni WIN server u visoko dostupnoj okolini • DR lokacija za pohranu podataka • postoji backup podataka • postoje dosjei radnika u papirnatom obliku koji se nalaze u sefu pod ključem	1	2	2
	namjerno uništenje osobnih podataka od strane ovlaštenih osoba	• virtualni WIN server u visoko dostupnoj okolini • DR lokacija za pohranu podataka • postoji backup podataka • postoje dosjei radnika u papirnatom obliku koji se nalaze u sefu pod ključem	1	2	2

Postupanje s rizicima

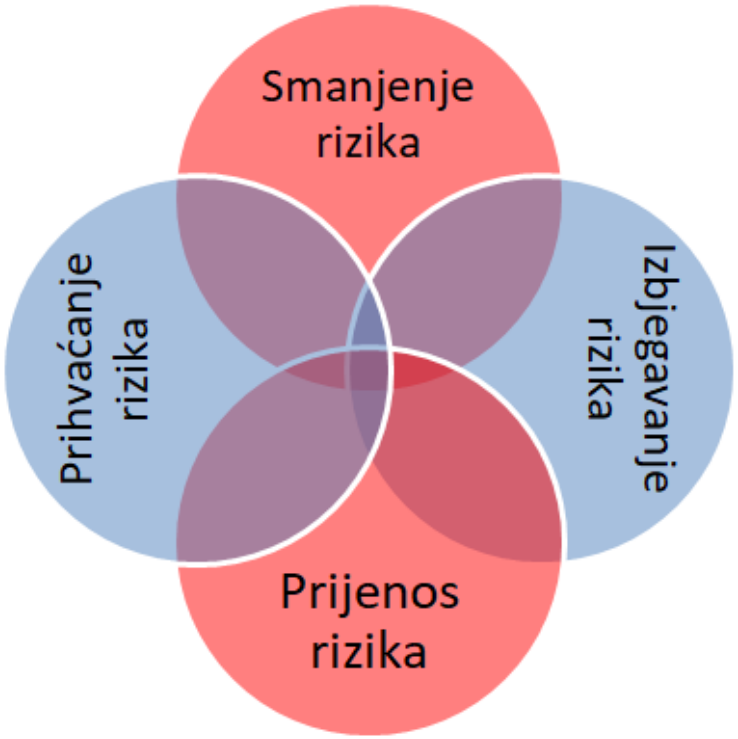
- Identificirani rizici se dalje obrađuju ovisno o njihovoj procijenjenoj razini
- Rizici se grupiraju u tri grupe:

Rizik = 1 - 2 Rizik se prihvaća bez daljnjih analiza	**Rizik = 3 - 6** Vlasnik rizika donosi odluku o prihvaćanju rizika i potrebi provedbe cost-benefit analize	**Rizik = 8 - 25** Rizik ulazi u obradu rizika

DPIA HOO

Opcije postupanja s rizicima

Prijedlog mjera – temeljem rezultata DPIA



Smanjenje rizika	• Ostvaruje se odabirom prihvatljivih organizacijskih i tehničkih mjera
Prihvaćanje rizika	• Rizik zadovoljava postavljene kriterije i kao takav može se prihvatiti
Prijenos rizika	• Prenijeti rizik na vanjskog partnera (osiguravajuća kuća, data centar...)
Izbjegavaje rizika	• Otkazati izvođenje aktivnosti koje mogu dovesti do rizika

Kada je potrebno konzultirati nadzorno tijelo?

GDPR, članak 36

Nadzorno tijelo treba konzultirati prije obrade u slučajevima kada DPIA otkriva da obrada može rezultirati visokim rizikom, u slučaju da voditelj obrade ne donese mjere za ublažavanje rizika.

Vođenje registra DPIA

- Voditelj obrade treba informirati zainteresirane strane o ishodu procjene utjecaja na privatnost
- Treba održavati registar rizika identificiranih kroz DPIA
- Registar može biti jednostavan popis svih procjena utjecaja, razina i predloženih mjera za one rizike koji su iznad prihvatljive razine

Revizija rezultata DPIA

Cilj: dobiti odgovarajući pregled provedene procjene utjecaja na privatnost

Pregled primjerenosti DPIA – redovito / pri značajnijim promjenama

- Izvještaj o procjeni utjecaja (PIA report)
- Pregled Izvješća o procjeni utjecaja (PIA report)
- Izvješće o pregledu PIA reporta

Četvrti korak: Implementacija tehničkih i organizacijskih mjera

- Voditelji i izvršitelji su obavezni implementirati prikladna tehnička i organizacijska rješenja kako bi osigurali razinu sigurnosti prikladnu riziku:
  - Pseudonimizacija i enkripcija
  - Osiguravanje povjerljivosti, integriteta, dostupnosti i otpornosti za sisteme i procese obrade
  - Privatnost ugrađena u svaki korak procesa – od početnog razvoja novog IT projekta, programa, sustava ili kampanje do dizajna, razvoja, kvalitete i puštanja u pogon („privacy by design”)
  - Sposobnost pravovremenog vraćanja dostupnosti i pristupa osobnim podacima u slučaju incidenta
  - Redovno testiranje i procjenjivanje tehničkih i organizacijskih mjera dizajniranih za osiguravanje sigurnosti obrade podataka (npr. pen test)

Pravilnik o zaštiti osobnih podataka u HOO

- Pravilnik
  - Definicije pojmova
  - Svrha obrade osobnih podataka ispitanika
  - Načela obrade i zaštite osobnih podataka
  - Odgovornosti i ovlasti
  - Transparentnost obrade podataka
  - Prava fizičkih osoba
  - Tehničke i organizacijske mjere za sigurnost podataka
  - Izvršitelj obrade

Pravilnik o zaštiti osobnih podataka u HOO - 2

- Pravilnik
  - Evidencija obrade osobnih podataka
  - Prijenos osobnih podataka u treće zemlje
  - Web stranica HOO
  - Upravljanje incidentima
  - Službenik za zaštitu osobnih podataka
  - Način čuvanja osobnih podataka
  - Završne odredbe

Implementacija „privacy by design" principa

- Svaka nova usluga ili poslovni proces koji koriste osobne podatke moraju uzeti u obzir sigurnost
- Organizacija mora moći demonstrirati prisutnost odgovarajućih mjera sigurnosti i nadgledanje sukladnosti
- U praksi to znači da IT odjel mora imati privatnost na umu tijekom cijelog životnog ciklusa projekta
- Pseudonimizacija je osnovna odlika „privacy by design" politike

Obveze izvršitelja obrade – reguliraju se ugovorom s voditeljem obrade:

- Primjenjivanje odgovarajućih tehničkih i organizacijskih mjera sigurnosti, u cilju zaštite prava ispitanika
- Zaposlenici ovlašteni za obradu osobnih podataka obavezuju se na poštivanje povjerljivosti
- Obrada osobnih podataka samo prema zabilježenim uputama voditelja obrade
- Angažiranje drugog izvršitelja obrade samo uz prethodno posebno ili opće pisano odobrenje voditelja obrade
- Na zahtjev voditelja obrade, brisanje ili vraćanje svih osobnih podataka nakon dovršetka pružanja usluga vezanih za obradu
- Pružanje podrške voditelju obrade u dokazivanju poštivanja obveza utvrđenih Uredbom

Analiza i specifikacija sigurnosnih zahtjeva

- Specifikacije poslovnih zahtjeva za novim informacijskim sustavima ili poboljšanjima postojećih informacijskih sustava trebaju sadržati i sigurnosne zahtjeve:
  - Kontrola pristupa
  - Nadzor logova
  - Sigurnosne kopije
  - Kontrola ulaznih podataka
  - Kontrola obrada
  - Zaštita informacija u aplikacijama na javnim mrežama
  - Zaštita informacija u on-line transakcijama itd.

Razvoj povjeren vanjskim izvršiteljima

- Organizacija treba nadgledati i nadzirati razvoj povjeren vanjskim izvršiteljima
- U slučaju takvog razvoja treba razmotriti:
  - sporazume o licenci, vlasništvo i prava intelektualnog vlasništva
  - ovjeravanje kvalitete i ispravnosti obavljenog posla
  - sporazume o čuvanju kod treće strane, u slučaju neuspjeha
  - prava pristupa zbog provjere kvalitete i ispravnosti obavljenog posla
  - ugovorne zahtjeve za kvalitetom koda, ukoliko se razvija SW
  - testiranje prije instalacije, radi detekcije malicioznog koda

Zaštita testnih podataka sustava

- Za zaštitu podataka koji se koriste u testne svrhe treba razmotriti sljedeće smjernice:
  - procedure za kontrolu pristupa, koje se odnose na produkcijske aplikacijske sustave, trebaju biti primijenjene i na testne aplikacijske sustave
  - mora postojati odvojeno ovlaštenje za svako kopiranje produkcijskih informacija u testni aplikacijski sustav
  - produkcijske informacije trebaju biti obrisane iz testnih aplikacijskih sustava odmah po završetku testiranja
  - kopiranje i korištenje produkcijskih informacija treba biti zabilježeno radi osiguravanja nadzora

Pravni temelj obrade

Za zakonitu obradu osobnih podataka potrebno je ispuniti barem jedno od narednih pravnih temelja:

- ispitanik je dao **privolu** za obradu svojih osobnih podataka u jednu ili više posebnih svrha
- obrada je **nužna za izvršavanje ugovora** u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora
- obrada je **nužna radi poštivanja pravnih obveza voditelja obrade**
- obrada je nužna kako bi se **zaštitili ključni interesi ispitanika** ili druge fizičke osobe
- obrada je nužna za **izvršavanje zadaće od javnog interesa** ili pri izvršavanju službene ovlasti voditelja obrade
- obrada je nužna **za potrebe legitimnih interesa voditelja obrade ili treće strane**


Prikupi sve podatke koje možeš, sve ćemo im odrediti kasnije.

Kriteriji koje privola mora zadovoljiti

Novosti Uredbe u odnosu na Zakon o zaštiti osobnih podataka RH

- Šira definicija osobnog podatka (IP adresa, cookies…)
- Prijava povrede osobnih podataka nadzornom tijelu unutar 72h
- Nužna implementacija „privacy by design”
- Jedna obrada – jedna privola
- Pravo na zaborav, čuvanje podataka koliko je potrebno za predmetnu svrhu
- Potiče se izrada kodeksa ponašanja, a organizacije se mogu i certificirati
- Mnogo veće kazne

Posljedice za nesukladnost

- Za obavljanje nadzora nad obradom osobnih podataka nadležna je Agencija za zaštitu osobnih podataka (AZOP)
- Agencija može izricati kazne u slučaju nepoštivanja zahtjeva Uredbe
- Potreba da se politika zaštite podataka diljem EU ujednači kako bi sva nadzorna tijela postupala slično ili identično
- Kada je prijestup dovoljno ozbiljan, izriču se vrlo visoke novčane kazne

Certificiranje voditelja i izvršitelja obrade

- Države članice, nadzorna tijela, Odbor i Komisija potiču uspostavu mehanizama certificiranja
- Mehanizmi certificiranja mogu se uspostaviti kako bi se dokazalo postojanje odgovarajućih mjera zaštite podataka
- Certificiranje je **dobrovoljno** i dostupno putem procesa koji je transparentan
- Certifikate izdaju certifikacijska tijela ili nadležno nadzorno tijelo

Hvala na pažnji