Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Vodič za procjenu učinka na zaštitu podataka za male i srednje poduzetnike

Awareness raising campaign for SMEs

1. UVOD

Najbolji način za provjeru je li Vaše poslovanje usklađeno s Općom uredbom o zaštiti podataka je **provođenje procjene učinka na zaštitu podataka. U slučaju da je za neku vrstu obrade vjerojatno da će prouzročiti visok rizik za prava i slobode pojedinaca, provođenje procjene učinka je <u>obavezno.</u>**

Što je procjena učinka?

Procjena učinka za zaštitu podataka je postupak osmišljen za:

1. **opisivanje obrade** - procjenu njezine nužnosti i proporcionalnosti

2. **upravljanje rizicima za prava i slobode pojedinaca** koji nastaju obradom osobnih podataka što uključuje procjenu rizika i određivanjem mjera za njihovo ublažavanje.

Proučite osnovne pojmove iz Opće uredbe o zaštiti podataka koji će Vam trebati za razumijevanje provedbe procjene učinka.

Obrada je 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.

Rizik za prava i slobode ispitanika - rizici različitih vjerojatnosti i ozbiljnosti, koji mogu proizaći iz obrade osobnih podataka te prouzročiti fizičku, materijalnu ili nematerijalnu štetu, posebno ako ta obrada može dovesti do diskriminacije, krađe identiteta ili prijevare, financijskog gubitka, štete za ugled, gubitka povjerljivosti osobnih podataka zaštićenih poslovnom tajnom, neovlaštenog obrnutog postupka pseudonimizacije, ili bilo koje druge znatne gospodarske ili društvene štete ili su ispitanici spriječeni u obavljanju nadzora nad svojim osobnim podacima

Ovdje treba uzeti u obzir prava na zaštitu podataka i privatnosti, ali i druga temeljna prava poput slobode govora, slobode mišljenja, slobode kretanja, te prava na slobodu savjesti i vjeroispovijesti ne samo ispitanika već i svih pojedinaca na koje obrada osobnih podataka može utjecati.

2. DEVET KRITERIJA KOJI SE UZIMAJU U OBZIR PRILIKOM PROCJENE KOJI ĆE POSTUCI OBRADE VJEROJATNO PROUZROČITI VISOK RIZIK

1. Postupci obrade koji uključuju procjenu ili bodovanje, uključujući izradu profila i predviđanje, osobito na temelju aspekata ispitanikovog učinka na poslu, ekonomskog stanja, zdravlja, osobnih preferencija ili interesa, pouzdanosti ili ponašanja, lokacije ili kretanja

PRIMJER: poduzeće koje izrađuje bihevioralne i marketinške profile utemeljene na upotrebi ili pregledavanju njihove internetske stranice

PRIMJER: zapošljavanja putem interneta bez ikakve ljudske intervencije

2. Postupci obrade koji uključuju automatizirano donošenje odluka s pravnim ili sličnim znatnim učinkom

PRIMJER: osiguravatelji nude premije na temelju ponašanja pojedinaca u vožnji
Voditelj obrade mora osigurati zakonitu osnovu za tu vrstu obrade jer nepoštena izrada profila može dovesti do toga da se određenim potrošačima nude nepovoljnije ponude

3. Postupci obrade koji uključuju situacije u kojoj sama obrada sprečava ispitanike u ostvarivanju prava ili upotrebi usluge i ugovora

PRIMJER: banka koja provjerava kreditnu sposobnost klijenta pri odlučivanju o dodjeli kredita

4. Postupci obrade koji uključuju osjetljive podatke ili podatke vrlo osobne naravi

PRIMJER: obrada osobnih podataka koji odaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, članstvo u sindikatu i ako je riječ o obradi genetičkih podataka, podataka koji se odnose na zdravlje ili spolni život ili kaznene osude i kažnjiva djela

5. Postupci obrade koji uključuju podatke koji se odnose na osjetljive ispitanike

To su kategorije ispitanika kod kojih postoji neravnoteža moći između ispitanika i voditelja obrade.

PRIMJER: obrada osobnih podataka djece, starijih osoba, zaposlenika, osoba s duševnim smetnjama, pacijenata, tražitelja azila

6. Postupci obrade koji uključuju podudarajuće ili kombinirane skupove podataka, na primjer oni koji potječu iz dva postupka obrade ili više njih, a koji su provedeni u različite svrhe i/ili koje su proveli različiti voditelji obrade podataka na način koji može premašiti razumna očekivanja ispitanika

Izradom profila mogu se prikupiti podaci iz posebne kategorije izvođenjem zaključaka iz podataka koji sami po sebi nisu podaci iz posebne kategorije, no to postaju kad ih se kombinira s drugim podacima.

PRIMJER: zaključci o nečijem zdravstvenom stanju mogli bi se izvući iz podataka o kupovanju hrane i podataka o instaliranim aplikacijama na mobitelu

7. Postupci obrade koji uključuju inovativnu upotrebu ili primjenu novih tehnoloških ili organizacijskih rješenja

Upotreba takve tehnologije može obuhvaćati inovativne oblike prikupljanja i upotrebe podataka s mogućim visokim rizikom za prava i slobode pojedinaca.

PRIMJER: otisak prsta i prepoznavanje lica za verifikaciju korisnika uređaja te pristup uređaju

8. Postupci obrade koji uključuju sustavno praćenje: odnosi se na obradu koja se koristi za promatranje, praćenje ili kontrolu ispitanika, uključujući primjerice podatke prikupljene putem interneta jer se osobni podaci mogu prikupljati u situacijama u kojima ispitanici nisu svjesni tko prikuplja njihove podatke i u koje će svrhe ti podaci biti upotrijebljeni

PRIMJER: sustavno praćenje javno dostupnog područja putem videonazdora

9. Pri utvrđivanju je li obrada opsežna, potrebno je razmotriti slijedeće čimbenike:

1. **broj uključenih ispitanika, bilo kao određeni broj ili udio relevantnog stanovništva; .**
2. **količina podataka i/ili niz različitih podataka koji se obrađuju;**
3. **trajanje ili stalnost postupka obrade podataka;**
4. **zemljopisni opseg aktivnosti obrade.**

PRIMJER: „livestream“ prijenos putem interneta sa gradskih kupališta

Ako je zadovoljeno 2 ili više kriterija, trebate provesti procjenu učinka prije same obrade.

Na taj način možete prije provođenja obrade primjenom načela zaštite osobnih podataka kao i tehničkih i organizacijskih mjerama ublažiti potencijalno visok rizik za prava i slobode pojedinaca.

Ukoliko ne uspijete ublažiti potencijalno visok rizik – SAVJETUJTE SE S AGENCIJOM ZA ZAŠTITU OSOBNIH PODATAKA PRIJE NASTAVKA OBRADE.

OSJETLJIVA KATEGORIJA ISPITANIKA + OPSEŽNA OBRADA = PROCJENA UČINKA

Na službenoj web stranici Agencije za zaštitu osobnih podataka https://azop.hr/odluka-o-uspostavi-i-javnoj-objavi-popisa-vrsta-postupaka-obrade-koje-podlijezu-zahtjevu-za-procjenu-ucinka-na-zastitu-podataka/ možete pronaći popis vrsta postupaka obrada kada je provođenje procjene učinka na zaštitu podataka obvezno, **no taj popis nije konačan te trebate uzeti u obzir ispunjava li obrada 2 ili više prethodnih kriterija te vjerojatno prouzročiti visok rizik**.

3. POPIS VRSTA POSTUPAKA OBRADE KOJE PODLIJEŽU ZAHTJEVU ZA PROCJENU UČINKA NA ZAŠTITU PODATAKA

1) Obrada osobnih podataka radi sustavnog i opsežnog profiliranja ili automatiziranog odlučivanja kako bi se donijeli zaključci koji u značajnoj mjeri utječu ili mogu utjecati na pojedinca i/ili više osoba ili koji služe kao pomoć u donošenju odluka o nečijem pristupu nekoj usluzi ili servisu ili pogodnosti (npr. kao što je obrada osobnih podataka odnosnih na ekonomski ili financijski status, zdravlje, osobne preferencije, interese, pouzdanost, ponašanje, podatke o lokaciji i dr.);

2) Obrada posebnih kategorija osobnih podataka u svrhu profiliranja ili automatiziranog odlučivanja;

3) Obrada osobnih podataka djece u svrhu profiliranja ili automatiziranog odlučivanja ili za marketinške svrhe, ili za izravnu ponudu usluga namijenjenu njima;

4) Obrada osobnih podatka prikupljenih od trećih strana koji se uzimaju u obzir za donošenje odluke vezane za sklapanje, raskidanje, odbijanje ili produženje ugovora o pružanju usluga fizičkim osobama;

5) Obrada posebnih kategorija osobnih podataka ili osobnih podataka o kaznenoj ili prekršajnoj odgovornosti u velikom opsegu;

6) Obrada osobnih podataka korištenjem sustavnog nadzora javno dostupnih mjesta u velikom opsegu;

7) Uporaba novih tehnologija ili tehnoloških rješenja za obradu osobnih podatka ili sa mogućnošću obrade osobnih podataka (npr. primjena „interneta stvari“, poput pametnih televizora, pametnih kućanskih aparata, komunikacijski povezanih igračaka, sustava „pametni gradovi“, pametnih mjerača energije, itd.) koji služe za analizu ili predviđanje ekonomske situacije, zdravlja, osobnih preferencija ili interesa, pouzdanosti ili ponašanja, lokacije ili kretanja fizičkih osoba;

8) Obrada osobnih podataka povezivanjem, usporedbom ili provjerom podudarnosti iz više izvora.

4. KAD PROVOĐENJE PROCJENE UČINKA NIJE OBAVEZNO?

Provođenje procjene učinka nije obvezno za obradu osobnih podataka ako postupak obrade neće rezultirati visokim rizikom za prava i slobode pojedinaca.

PRIMJERI KAD PROVOĐENJE PROCJENE UČINKA NIJE OBAVEZNO:

- obrada podataka pacijenata pojedinih liječnika
- obrada podataka klijenata odvjetnika
- obrada podataka potrebnih za uobičajeno upravljanje školama i vrtićima (npr. registriranje, izdavanje računa, prehrana, prijevoz, školski izleti)
- obrada podataka od strane odjela za ljudske potencijale ako zapošljavate manje od 250 zaposlenika
- obrada podataka za administrativne radnje u vezi s ugovorima s dobavljačima, narudžbama i naplatama
- obrada podataka za procese kontrole fizičkog pristupa zgradi ako se pri tome ne obrađuju biometrijski podaci ili druge posebne kategorije osobnih podataka
- obrada podataka koja je nužna radi poštovanja pravnih obveza voditelja obrade ili izvršavanja zadaće od javnog interesa, ako je procjena učinka na zaštitu podataka već provedena kao dio donošenja pravne osnove, osim ako države članice smatraju da je isto potrebno.

U slučaju da procjena učinka nije obvezna, uzmite u obzir kako je provođenje procjene učinka jedan od načina kako ćete dokazati da ste usklađeni sa pravnim obvezama iz Opće uredbe o zaštiti podataka.

5. TKO JE ODGOVORAN I TKO MORA PROVESTI PROCJENU UČINKA NA ZAŠTITU PODATAKA?

Voditelj obrade (mikro, malo ili srednje poduzeće) odgovorno je za osiguravanje provođenja procjene učinka na zaštitu podataka, a **procjenu učinka na zaštitu podataka može provesti i druga osoba unutar i izvan poduzeća uz pomoć službenika za zaštitu podataka i izvršitelja obrade.**

VODITELJ OBRADE	DPO	IZVRŠITELJ OBRADE
(odgovoran je za provedbu)	(praćenje izvršavanja DPIA)	(ustupa informacije)

* DPO – Službenik za zaštitu osobnih podataka (eng. Data Protection Officer)

* Više informacija o službeniku za zaštitu podataka možete pronaći na https://azop.hr/sluzbenik-za-zastitu-podataka-2/

Savjet: zatražite savjet od službenika za zaštitu podataka te službenika za informacijsku sigurnost, informatičke službe, neovisnih stručnjaka (odvjetnika, stručnjaka za IT, stručnjaka za sigurnost, itd.).

6. ŠTO PROCJENA UČINKA NA ZAŠTITU PODATAKA MORA SADRŽAVATI?

- sustavan opis predviđenih postupaka obrade i svrha obrade – specifikacija obrade
- procjenu nužnosti i proporcionalnosti postupaka obrade – prepoznavanje opasnosti
- procjenu rizika za prava i slobode ispitanika – ocjena rizika (nizak/umjeren/**visok**)
- mjere predviđene za rješavanje problema rizika (procjena i ublažavanje rizika ukoliko je isto potrebno)

7. ČETIRI KORAKA ZA PROVOĐENJE PROCJENE UČINKA NA ZAŠTITU OSOBNIH PODATAKA

KORAK 1: OPIŠITE SVE POSTUPKE OBRADE OSOBNIH PODATAKA I SREDSTVA KOJIMA KORISTITE PRILIKOM OBRADE (HARDWARE, SOFTWARE, MREŽA, PAPIRNATA i DIGITALNA DOKUMENTACIJA)

Od koga ćete prikupljati osobne podatke? Od samih ispitanika, javno dostupnih izvora, trećih? Jesu li uključene i posebne kategorije ispitanika? Koje kategorije podataka ćete prikupljati? Uključuju li one posebne kategorije osobnih podataka ili podatke u vezi s kaznenim osudama i kažnjivim djelima? Radi li se o uvođenu novina? Koliko često će podaci biti prikupljani? Može li se obrada smatrati sustavnom? Funkcionalni opis postupka obrade? Koje se tehnologije koriste prilikom obrade? O kojim sredstvima ovisi obrada osobnih podataka (oprema, računalni programi, mreže, osobe, dokumenti u papirnatom i digitalnom obliku …)? Koji se sustavi, programi ili mreže koriste u poslovnim procesima prilikom obrade osobnih podataka? Na koliko pojedinaca može imati utjecaja obrada? Koje geografsko područje obuhvaća?

KORAK 2: PROCIJENITE PRIMJENU TEMELJNIH NAČELA

a. procjena kontrola koje jamče proporcionalnost i nužnost obrade

- ✓ **Ograničenje svrhe** (Provjerite jesu li podaci prikupljeni u posebne, izričite i zakonite svrhe te da li se podaci obrađuju na način koji nije u skladu s tim svrhama.)

- ✓ **Pravna osnova** (Koja je pravna osnova za obradu? Je li obrada zakonita? Možete li dokazati pravnu osnovu? Jesu li ispunjeni svi preduvjeti kako bi se obrada mogla smatrati zakonitom?

Obrada je zakonita samo ako (pravni temelji za zakonitu obradu):

a. ispitanik je dao **privolu** za obradu svojih osobnih podataka u jednu ili više posebnih svrha;
b. obrada je **nužna za izvršavanje ugovora** u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora *daljnja pohrana osobnih podataka trebala bi biti zakonita ako je nužna za ostvarivanje prava za postavljanje, ostvarivanje ili obranu pravnih zahtjeva
c. obrada je nužna kako bi se **zaštitili ključni interesi ispitanika** ili druge fizičke osobe
d. obrada je nužna za potrebe **legitimnih interesa** voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete. U posljednja dva slučaja nije potrebno provesti procjenu učinka, ako je procjena učinka na zaštitu podataka već provedena kao dio donošenja pravne (npr. zakonske) osnove, osim ako države članice smatraju da je isto potrebno.
e. obrada je nužna radi poštovanja pravnih obveza voditelja obrade;
f. obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade)

✓ **Smanjenje količine podataka** (Provjerite jesu li prikupljeni podaci primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju.)

✓ **Točnost podataka** (Provjerite poduzimate li sve razumne mjere da se osobni podaci koji nisu točni bez odlaganja izbrisali ili ispravili. Koliko često ažurirate podatke?)

✓ **Ograničenje pohrane** (Provjerite čuvaju li se osobni podaci u obliku koji omogućuje identifikaciju ispitanikâ samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju. Brišu li se podaci ili se anonimiziraju nakon proteka svrhe?)

b. procjena kontrola koje jamče prava ispitanika

- ✓ **Transparentne informacije** (Jeste li ispitanike informirali o obradi njihovih osobnih podataka? Jeste li upoznali ispitanike sa svrhama i pravnim osnovama obrade? Jeste li upoznali ispitanike s njihovim pravima?)
- ✓ **Privola ispitanika kao pravna osnova** (Jesu li zadovoljeni svi uvjeti kako bi se privola mogla smatrati zakonitom pravnom osnovom?)
- ✓ **Pravo ispitanika na pristup podacima i prenosivost podataka** (Jeste li omogućili ispitanicima podnošenje zahtjeva za pristup podacima? Na koji način ćete zahtjev provesti?)
- ✓ **Pravo na ispravak i brisanje** (Jeste li omogućili ispitanicima podnošenje zahtjeva za ispravak/brisanje podataka? Na koji način ćete zahtjev provesti?)
- ✓ **Pravo na ograničenje obrade i pravo na prigovor** (Jeste li omogućili ispitanicima podnošenje zahtjeva za ograničenje obrade/ prigovor na obradu? Na koji način ćete zahtjev provesti?)

- ✓ **Izvršitelji obrade** (Jeste li potpisali ugovor o obradi osobnih podatka s izvršiteljem obrade u kojim su uređena prava i obveze koje proizlaze iz Opće uredbe o zaštiti podataka?)
- ✓ **Prijenos podataka u treće zemlje/međunarodne organizacije** (Postoji li odluka Komisije da treća zemlja, područje, ili jedan ili više određenih sektora unutar te treće zemlje, ili međunarodna organizacija o kojoj je riječ osigurava primjerenu razinu zaštite? Ako ne: Da li su na prijenos podataka primijenjene odgovarajuće zaštitne mjere? Da li ispitanici mogu raspolagati svojim pravima? Postoji li u toj trećoj zemlji učinkovita sudska zaštita?)

KORAK 3: PROCIJENITE RIZIK

a) Identificirajte potencijalni utjecaj na prava i slobode pojedinaca u slučaju:

- ✓ **neovlaštenog pristupa osobnim podacima** (Koje bi mogle biti posljedice na prava i slobode ispitanika u slučaju da osobne podatke sazna neovlaštena osoba? Odnosno, postavite pitanje što u slučaju ako izgubite kontrolu nad podacima i oni postanu dostupni osobama čije vam namjere nisu poznate?)

- ✓ **neovlaštene izmjene osobnih podataka** (Koje bi mogle biti posljedice na prava i slobode ispitanika u slučaju izmjene podataka? Odnosno, postavite pitanje što u slučaju da su podaci netočni ili nečitljivi?)

- ✓ **gubitka podataka** (Koje bi mogle biti posljedice na prava i slobode ispitanika u slučaju gubitka podataka? Odnosno, postavite pitanje što u slučaju da ne može pristupiti podacima?)

b) Identificirajte izvor prijetnje:

- ✓ ljudski faktor (djelatnici, korisnici, treće osobe)
- ✓ ostali faktori (hardware, software, mreža, lokacija, elementarne nepogode…)

c) Napravite procjenu vjerojatnosti i ozbiljnosti posljedica za prava ispitanika

VJEROJATNOST POJAVE PRIJETNJE TREBA RANGIRATI OD ZANEMARIVE DO VISOKE:

1. Zanemariv – čini se nevjerojatnim da će se rizik ostvariti i materijalizirati u prijetnju (pr. čini se nevjerojatnim da će doći do neovlaštena izmjena podataka u bazi ako se koristi opcija „zapis logova“ koja omogućuje praćenje izmjena te bazi mogu pristupiti samo ovlaštene osobe)

2. Nizak - čini se da će teško doći do ostvarenja rizika (pr. čini se da će teško doći do neovlaštene izmjene podataka u bazi kojoj pristup imaju samo ovlaštene osobe)

3. Srednji – čini se mogućim da se rizik ostvari (pr. čini se mogućim da dođe do neovlaštene izmjene podataka u bazi koja je osigurana samo lozinkom te dostupna svim zaposlenicima)

4. Visok – čini se da je rizik lako ostvariv (pr. čini se da lako da dođe do neovlaštene izmjena podataka u bazi kojoj se može slobodno pristupiti, bez lozinke)

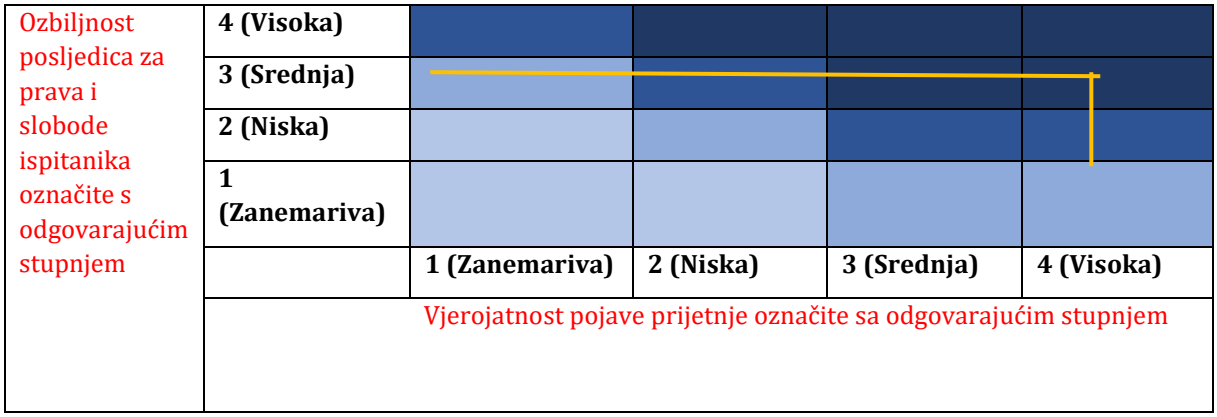
d) Napravite procjenu ozbiljnosti na posljedice za prava i slobode ispitanika

1. Zanemariva – ispitanici će prevladati posljedicu bez problema (spam, izgubit će vremena na ponavljanje zahtjeva i sl.)

2. Niska – ispitanici će prevladati posljedicu uz manje poteškoće (neće moći pristupiti usluzi, neočekivani trošak, propuštena prilika za zaposlenje i sl.)

3. Srednja – ispitanici će prevladati posljedicu uz ozbiljne poteškoće (financijski gubitak kao rezultat prijevare i sl.)

4. Visoka – ispitanici neće moći prevladati posljedice (smrt, značajni financijski gubici, nemogućnost zaposlenja i sl.)



	Visok rizik
	Srednji rizik
	Niski rizik
	Zanemariv rizik

KORAK 4: PRIMIJENITE MJERE PREDVIĐENE ZA RJEŠAVANJE PROBLEMA RIZIKA

MEHANIZMI ZA OSIGURAVANJE ZAŠTITE OSOBNIH PODATAKA:

- **obvezujuća korporativna pravila**
- **standardne klauzule o zaštiti podataka koje donosi Komisija** (standardne ugovorne klauzule koje nude dovoljne mjere zaštite podataka za prijenos podataka u inozemstvo -ne-EU ili EEA zemlje)
- **standardne klauzule o zaštiti podataka koje donosi nadzorno tijelo**.;
- **odobreni kodeks ponašanja**
- **odobreni mehanizam certificiranja**

TEHNIČKE I ORGANIZACIJSKE MJERE:

- fizička zaštita od nedozvoljenog pristupa
- tehnička zaštita od nedozvoljenog pristupa (alarma, videonadzor, pametne kartice...)
- korištenje lozinke za pristup opremi, računalnim programima i datotekama
- vođenje evidencije pristupa osobnim podacima
- praćenje logiranja - pratiti radnje koje provode zaposlenici tijekom postupka obrade kako bi ih kasnije u slučaju potrebe mogli analizirati i utvrditi tko je od zaposlenika odgovoran
- suzbijanje zlonamjernog softvera (antivirus, vatrozid, pravila za korištenje elektroničke pošte, korištenje sigurnih mreža…)
- održavanje hardvera i softvera (onemogućavanje instaliranja proizvoljnih aplikacija na računalnu opremu od strane zaposlenika, pravovremeno ažuriranje softvera, osiguravanje dostatnog prostora za pohranu podataka, osiguravanje udaljenog pristupa mobilnoj opremi (laptop, mobitel)..)
- redovita edukacija zaposlenika o važnosti zaštite osobnih podataka
- politika (upravljanje pravilima) - propišite pravila postupanja kroz interne akte koji su u svakom trenutku dostupni vašim zaposlenicima
- upravljanje incidentima i povredama podataka – propišite internu proceduru u slučaju pojave „povrede osobnih podataka“ te zadužite odgovorne osobe za postupanje po istoj
- odnosi s trećim stranama – ugovori s izvršiteljima obrade
- sigurnosne kopije – osiguravaju dostupnost i/ili integritet osobnih podataka
- anonimizacija
- enkripcija
- mehanizam periodičnog preispitivanja primijenjenih mjera

Primjer: Koje su posljedice na prava i slobode ispitanika u slučaju da haker neovlašteno iz vaše baze podataka prikupi identifikacijske, financijske podatke vaših klijenata?

Postoji mogućnost da će isti biti upotrijebljeni u svrhu prijevare. Ispitanici će pokretanjem kaznenih postupaka bit u mogućnosti dokazati prijevaru. Obzirom na poteškoće u vidu kaznenog postupka te ozbiljne financijske posljedice možemo reći kako se radi o srednje (3) ozbiljnim posljedicama na prava i slobode ispitanika.

Kako bi procijenili vjerojatnost pojave prijetnje provjerite koje ste sve sigurnosne i zaštitne mjere primijenili. Koliko je vjerojatno da će isto dogoditi ovisi o tehničkim i organizacijskim mjerama koje ste predvidjeli kako bi spriječili neovlašteni pristup bazama podataka.

Ukoliko ste primijenili odgovarajuće sigurnosne i zaštitne mjere te ipak dođe do neovlaštenog pristupa nećete za isto biti odgovorni. Vaša obveza je dokazati da ste primijenili odgovarajuće mjere

za ublažavanje rizika. Provođenje procjene učinka na zaštitu osobnih podataka može Vam pomoći pri dokazivanju.

Objava procjene učinka na zaštitu podataka nije obvezna, no objava određenih dijelova, kao što je sažetak ili zaključak njihove procjene učinka na zaštitu podataka svakako pridonosi transparentnosti poslovanja te pravima ispitanika na informiranost, a samim time doprinosi i povjerenju klijenata/korisnika u Vaše usluge/proizvode.

Procjena učinka na zaštitu podataka provodi se kontinuirano, a ne jednom. Svi voditelji obrade pa tako i mali i srednji poduzetnici moraju kontinuirano procjenjivati rizike nastale njihovim aktivnostima obrade kako bi utvrdili kada će neka vrsta obrade „vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca".

*obrazac koji Vam može pomoći prilikom provedbe procjene učinka na zaštitu osobnih podataka možete pronaći na https://azop.hr/obrasci-predlosci/