SUPPORT POOL OF EXPERTS PROGRAMME

Praktikum za službenike za zaštitu osobnih podataka

OPĆA UREDBA O ZAŠTITI PODATAKA U PRAKSI

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

- Općenito o zaštiti podataka – zadaci voditelja obrade
- Osvrt na okvir zaštite osobnih podataka u EU
- Razlike i novine prema DZP i ZZOP
  - Načela zaštite osobnih podataka
  - Prava ispitanika
  - Međunarodni transferi
  - Polje primjene OUZP
- Definicije temeljnih pojmova zaštite osobnih podataka
- Pravne osnove obrade osobnih podataka
- Prava ispitanika
- Obveze voditelja obrade
- Mehanizmi sukladnosti
  - DPIA, PBD&D, certifikacije
- Položaj i uloga SZOP/DPO
  - Utvrđivanje obveze imenovanja
  - Odabir kandidata
  - Imenovanje
  - Radno mjesto, prava i obaveze
- Uloga i aktivnosti regulatornih tijela
- Judikatura i regulatorna praksa
- Industrijski standardi
  - ISO obitelj standarda
  - NIST, TISAX, PCI DSS
- Praktični pristup usklađivanju
  - Analiza trenutnog stanja usklađenja
  - Faze projekta usklađivanja
  - Projektne aktivnosti
  - Praćenje i mjerenje usklađenosti
  - Mjere za održavanje usklađenosti
- Trendovi u zaštiti podataka
- Pitanja i odgovori
- Studije slučajeva
- Obrasci

Općenito o zaštiti podataka

- **OUZP stvara i osigurava slobodan protok osobnih podataka na zajedničkom tržištu**
- **Voditelj obrade uvijek je i primarno odgovoran je za sigurnost i povjerljivost obrade**
- **Temeljem načela odgovornosti (pouzdanosti) dužan je dokazati da postupa u skladu s obvezama propisanim OUZP i drugim propisima**
- **Pravila zaštite podataka postoje da bi se spriječile povrede osobnih podataka**
- **Uredba prvenstveno ima za cilj spriječiti masovne povrede – povrede koje se odnose na velik broj ispitanika, veliku količinu podataka i osjetljive podatke, osobito kod velikih internetskih platformi**
- **U slučaju povrede, nadzorna tijela mogu izreći različite mjere, uključujući i vrlo visoke kazne. Također postoji mogućnost tužbi za naknadu štete ispitanicima. Voditelji obrade trpe i reputacijsku štetu. U određenim slučajevima odgovaraju i odgovorne osobe u voditelju obrade.**

- **Koje su obveze voditelja obrade?**
- **Koje su sankcije za povrede?**
- **Kako ispuniti evidenciju aktivnosti obrade?**
- **Koga i kako odabiremo za funkciju SZOP?**
- **Koje tehničke i organizacijske mjere trebamo koristiti?**

Općenito o zaštiti - o korištenju i nužnosti privole

- Privola **nije isto što i obavijest o obradi osobnih podataka**
- **Za svaku obradu** osobnih podataka odgojno-obrazovna, obrazovna ili znanstveno-obrazovna ustanova kao voditelj obrade **treba imati zakonitu osnovu i svrhu**
- **Za zakonitu obradu** osobnih podataka **potrebno** je da bude ispunjena **JEDNA** od taksativno navedenih pravnih osnova iz članka 6. Opće uredbe o zaštiti podataka.
- **Privola je samo jedna od zakonitih pravnih osnova** za obradu osobnih podataka – ako se podaci prikupljaju i dalje obrađuju temeljem **neke druge pravne osnove** iz članka 6. Opće uredbe o zaštiti podataka (npr**. ugovor, pravna obveza, javne ovlasti/interes, legitimni interes voditelja obrade) ne tražiti privolu!**

- **Privola je samo jedna od pravnih osnova**
- **Privola nije uvijek nužna/obvezna**
- **Ukoliko se koristi, treba pažljivo dokumentirati njenu upotrebu**
- **Ispitanici uvijek mogu povući privolu**

Općenito o zaštiti podataka – prava ispitanika

- **Informiranje ispitanika o obradi** jedna je od temeljnih obveza voditelja obrade, kao voditelja obrade neovisno o pravnoj osnovi prikupljanja i daljnje obrade osobnih podataka te je isto potrebno u svakom slučaju obrade osobnih podataka.
- **Druge obveze :**
  - 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)
  - provođenje i nadzor tehničkih i organizacijskih mjera
  - **povjerljivo postupanje s osobnim podacima**

- **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?**

Obveza povjerljivosti

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

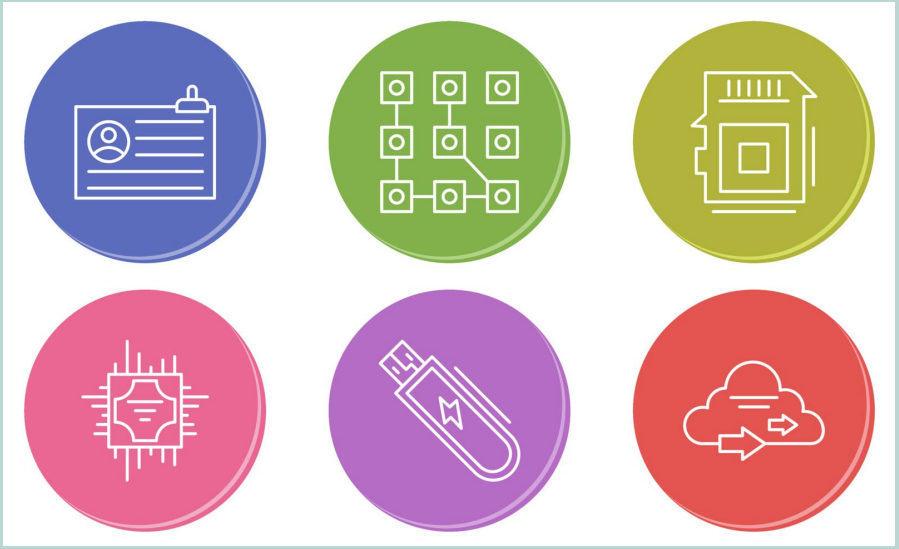
Ovu Izjavu sam u potpunosti pročitao/pročitala te ju u znak suglasnosti potpisujem.

potpis

ime i prezime

Općenito o zaštiti podataka – tehničke i organizacijske 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).



Pravni izvori i interpretacija odredaba Opće uredbe o zaštiti podataka (GDPR/OUZP)

- Opća uredba zamjenjuje stari okvir (Direktivu o zaštiti podataka iz 1995. te njene transpozicijske mjere - nacionalne zakone država članica poput hrvatskog Zakona o zaštiti osobnih podataka)
  - Direktiva o zaštiti podataka
  - E-Privacy direktiva
  - Nacionalni zakoni
- Europske uredbe se primjenjuju **izravno,** sa snagom iznad nacionalnog zakona države članice Unije
- **Uredbe se primjenjuju na jedinstven način** na čitavom području Unije i EEA
- EU Strategija kibersigurnosti, European Security Agenda 2015-2020 itd.
- Nije izoliran propis već dio sveobuhvatne zakonodavne strategije
  - 2015-2020 – EIDAS, NIS, reforma sustava intelektualnog vlasništva, GDPR
  - 2020 i dalje – NIS2, DORA, Digital Governance Act, Digital Markets Act, Digital Services Act., Data Act, AI Regulation itd.

Zašto GDPR/OUZP?

Intenzivan razvoj informacijskih usluga u proteklih 20 godina (1995-2014)

- Nove online usluge, širenje širokopojasnog interneta, 5+ milijardi korisnika interneta
- Big data (pohrana, analiza), cloud usluge, digitalizacija
- Monetizacija - osobni podaci – nova digitalna valuta

Zaštita osobnih podataka u EU je prepoznata kao temeljno pravo

Iskustva s dosadašnjim pravnim okvirom - fragmentarnost

- Nejednaka transpozicija
- Različita nacionalna praksa
- Nedoumice oko interpretacije i primjene

Iskustva s institucionalnim okvirom

- Nacionalni regulatori različitih sposobnosti i resursa
- Suprotstavljena praksa nadzornih tijela i nacionalnih sudova
- Manjkav nadzor izvoza osobnih podataka iz EU
- Generalno nezadovoljavajuća razina svijesti kako u javnim institucijama, tako i u privatnom sektoru i kod samih ispitanika

Novi europski pravni okvir zaštite osobnih podataka

- Povelja o temeljnim pravima EU
  - Čl. 7 Zaštita privatnosti
  - Čl. 8 Zaštita osobnih podataka
- General Data Protection Regulation (GDPR) odnosno Opća uredba o zaštiti podataka (OUZP)
- Direktiva o obradi podataka pojedinaca od strane nadležnih tijela u svrhu prevencije, istrage, otkrivanja i kaznenog progona počinitelja kaznenih djela
- Direktiva (EU) 2016/681 od 27. travnja 2016. o uporabi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela
- Uredba 2018/725 o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ
- U izradi:
  - E-Privacy Regulation – Uredba o e-privatnosti
  - AI Regulation, Data Act, European Public Healthspace itd.

Propisi primjenjivi u Republici Hrvatskoj

- Zakon o provedbi Opće uredbe o zaštiti podataka
- Sektorski propisi
  - Regulacija elektroničkih komunikacija – Zakon o elektroničkim komunikacijama
  - Pravo na pristup informacijama – Zakon o pravu na pristup informacijama
  - Policija, kazneni postupci, sigurnosne službe i nacionalna sigurnost, kibernetička sigurnost
  - Zdravstvena i socijalna skrb
  - Obrazovanje
  - Mediji – Zakon o medijima, Zakon o elektroničkim medijima, Zakon o HRT..
  - Regulirane profesije – Zakon o odvjetništvu, Zakon o liječništvu
  - Porezni propisi

Kako interpretirati OUZP?

- Uredba je opća norma, **snagom iznad nacionalnih propisa države članice**
- Tehnološki neutralna
- Uža (manje prostora za interpretaciju) i stroža od Direktive
- **Izravno se primjenjuje**
- Zbog svoje opće prirode, pravila sadržana u člancima su vrlo općenita što otvara vrata za pravnu nesigurnost
- Ostavlja određen predviđen prostor državama članicama za interpretaciju, primjerice:
  - U pogledu određivanja samostalnog učinka dobi maloljetnika kao korisnika usluga informacijskog društva
  - Institucionalnog ustroja nadzornih tijela
  - Postupka izricanja novčanih upravnih kazni
  - Obrada u kontekstu elektroničkih medija, znanstvenih, povijesnih i arhivskih istraživanja i dr.

Kako interpretirati OUZP?

Izvori za tumačenje Opće uredbe o zaštiti podataka:

1) Članci i recitali OUZP
2) Judikatura Suda Europske Unije (European Court of Justice)
3) Smjernice i mišljenja EDPB - Europskog odbora za zaštitu podataka odnosno od EDPB preuzeta mišljenja nekadašnje WP29 – Article 29 Working Party odnosno Radne skupine osnovane po čl. 29. Direktive o zaštiti podataka
4) Smjernice i mišljenja nacionalnih nadzornih tijela (Data Protection Authorites, DPA)
5) Shvaćanja nacionalnih sudova
6) Pravna doktrina

Sadržajno polje primjene

- Odnosi se na dijelom ili u potpunosti automatiziranu obradu osobnih podataka
- Ne odnosi se na obradu zbog razloga nacionalne sigurnosti te vanjske i sigurnosne politike Unije
- Ne odnosi se na obradu u svrhu sprečavanja, otkrivanja, istrage i progona kaznenih djela – poseban propis Direktiva 2016/680
- Ne odnosi se na fizičke osobe koje prikupljaju osobne podatke radi osobnih ili kućnih aktivnosti

Teritorijalno polje primjene

- Odnosi se na prikupljanje i obradu podataka fizičkih osoba na području EU, bez obzira odvija li se sama obrada na području EU ili negdje drugdje
- Odnosi se na obrade i na području EEA (europskog ekonomskog prostora) – Island, Lihtenštajn, Norveška…
- Švicarska je u posebnom statusu i također je dio zajedničkog tržišta
- Sporazumom o Brexitu, OUZP se i dalje primjenjuje i na području UK kao tzv. UK GDPR
- Nije presudno je li organizacija ima sjedište na području EU – za voditelje obrade koji nemaju sjedište u EU određuje se tzv. predstavnik (representative)
- Ako voditelj obrade nema sjedište u EU, svejedno je podvrgnut Uredbi ukoliko:
  - njegova obrada je povezana s nuđenjem robe ili usluga u Uniji
  - njegova obrada prati ponašanje ispitanika na teritoriju Unije

Primjer slučaja (1)

- Upravo vas je zaposlio proizvođač igračaka sa sjedištem u Shenzhenu, Narodna Republika Kina. Tvrtka prodaje široku paletu lutaka, akcijskih figurica i plišanih igračaka koje se mogu pronaći širom svijeta u raznim maloprodajnim trgovinama. Iako proizvođač nema urede izvan Kine, sklopio je niz lokalnih distribucijskih ugovora. Igračke koje proizvodi tvrtka mogu se naći u svim popularnim trgovinama igračaka diljem Europe, Sjedinjenih Država i Azije. Veliki dio prihoda tvrtke dolazi od međunarodne prodaje. Tvrtka sada želi lansirati novu ponudu povezanih igračaka, onih koje mogu razgovarati i komunicirati s djecom. Izvršni direktor tvrtke reklamira ove igračke kao pametne igračke, osobito mogućnosti interakcije koje se nude: figure mogu odgovarati na dječja pitanja o raznim temama, poput matematičkih izračuna ili vremena. Svaka figura opremljena je mikrofonom i zvučnikom i može se povezati s bilo kojim pametnim telefonom ili tabletom putem Bluetootha. Svaki mobilni uređaj u radijusu od 10 metara može se povezati s igračkama i putem Bluetootha. Figure se također mogu povezati s drugim figurama (od istog proizvođača) i komunicirati jedna s drugom za poboljšano iskustvo igranja.
- Kada dijete igrački postavi pitanje, zahtjev se šalje u oblak na analizu, a odgovor se generira na poslužiteljima u oblaku i šalje natrag figuri. Odgovor se daje preko integriranih zvučnika figure, zbog čega se čini kao da igračka zapravo odgovara na djetetovo pitanje. Pakiranje igračke ne pruža tehničke pojedinosti o tome kako to radi, niti se spominje da ova značajka zahtijeva internetsku vezu. Igračka također posjeduje NFC sučelje.
- Potrebna obrada podataka za to povjerena je podatkovnom centru koji se nalazi u Novom Sadu. Međutim, vaše trgovačko društvo još nije revidirala svoju politiku privatnosti usmjerenu na potrošače kako bi to naznačila.
- Što biste prepoznali kao najveću prepreku izlasku na tržište i najveći potencijalni problem iz perspektive zaštite podataka?

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

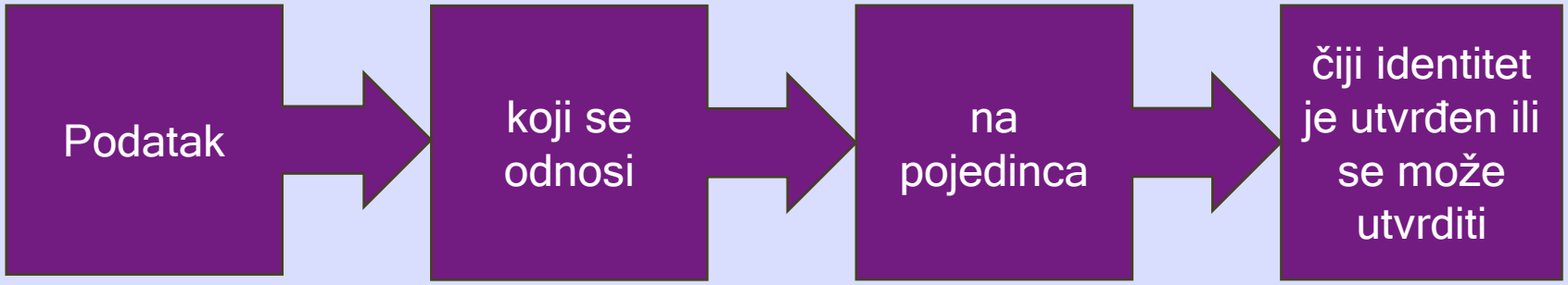
Osobni podatak

- svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („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

Primjeri: ime i prezime, adresa, email adresa, broj telefona, državljanstvo, nacionalnost, spol, seksualna orijentacija, visina, težina, biometrijski podaci poput boje glasa, očiju, otiska prsta, načina hoda, psihološke i zdravstvene značajke, članstvo u političkoj stranci, vjerska pripadnost, brojevi identifikacijskih dokumenata, osobni identifikacijski brojevi, IMEI, MAC itd.

Mogu biti i: promjenjivi mrežni identifikatori poput dinamičke IP adrese

Osobni podatak



- Podaci mogu biti točni ili netočni, potpuni ili nepotpuni
- Mogu sadržavati informacije osobne naravi ili biti stručne, poslovne
- Obične i osjetljive/intimne prirode
- Podaci u bilo kojem obliku, odnosno formatu / zapisu
- U kontekstu zaštite podataka razlikujemo posebne kategorije podataka i podatke koji se odnose na kaznene osude i kaznena djela

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 osobnog podatka

Identitet ispitanika je utvrđen	Identitet ispitanika se može utvrditi
Hrvoje Horvat, OIB: 23468973216, radi na Filozofskom fakultetu Sveučilišta u Zagrebu kao docent	Vozač automobila registarskih oznaka RI-114-DS počinio je prometni prekršaj jer je vozio pod utjecajem opojnih sredstava
Mislav Marković, JMBG 1402939330068, umirovljenik iz Zagreba	Korisnik email adrese razbojnik@hotmail.com ostavlja uvredljive i klevetajuće komentare na internetskim stranicama davatelja usluge internetskog pristupa
Tea Tušek, broj telefona, 01-5533222, djelatnica Gradskog komunalnog poduzeća	Vozačica automobila parkira na posebno označenom parkirnom mjestu u garaži poslodavca

Posebne kategorije osobnih podataka

- Rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, članstvo u sindikatu, genetski podaci, podaci koji se odnose na zdravlje, podaci o spolnom životu ili seksualnoj orijentaciji pojedinca.
- Biometrijski podaci u svrhu jedinstvene identifikacije pojedinca (ne i u druge svrhe)
- U nekim državama izvan EU i lokacijski podaci (neke savezne države SAD)
- **Zašto baš ti podaci? Jer su pogodni za diskriminaciju!**

Kod obrade posebnih kategorija osobnih podataka potrebno je:

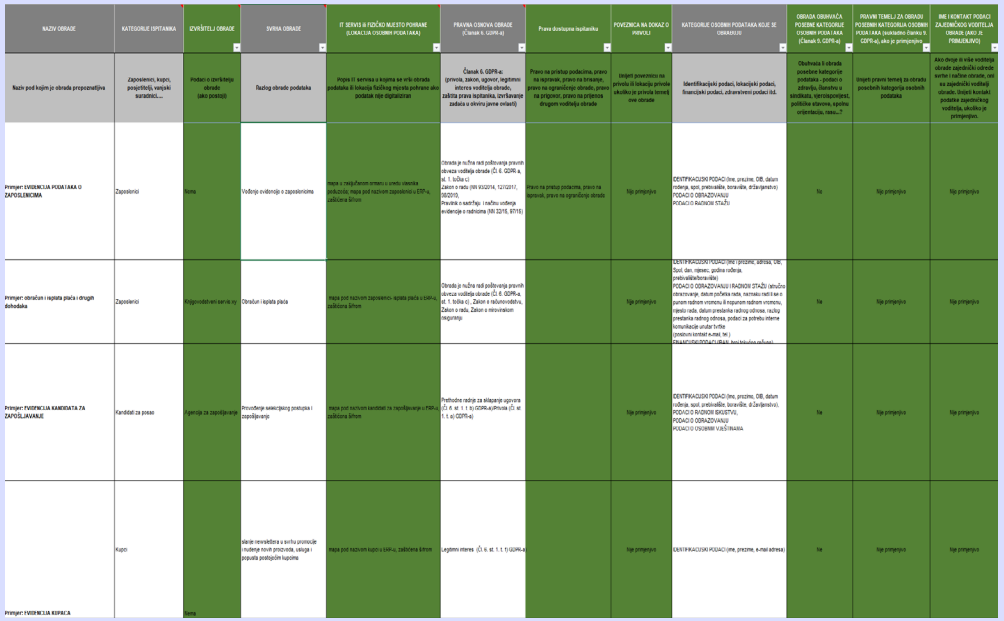
- Provjerili smo da je obrada podataka posebne kategorije nužna za svrhu koju smo identificirali i uvjereni smo da ne postoji drugi razuman i manje nametljiv način za postizanje te svrhe
- Identificirali smo pravni temelj iz članka 6. za obradu podataka posebne kategorije
- Identificirali smo odgovarajući uvjet iz članka 9. za obradu podataka posebne kategorije
- Dokumentirali smo koje posebne kategorije podataka obrađujemo
- Razmotrili smo trebamo li napraviti DPIA
- U naše podatke o privatnosti za pojedince uključujemo posebne informacije o našoj obradi podataka posebne kategorije
- Ako koristimo podatke posebne kategorije za automatizirano donošenje odluka (uključujući profiliranje), provjerili smo pridržavamo li se članka 22
- Razmotrili smo utječu li rizici povezani s našom upotrebom podataka posebne kategorije na naše druge obveze vezane uz smanjenje podataka, sigurnost i imenovanje službenika za zaštitu podataka (DPO) i predstavnika

Obrada

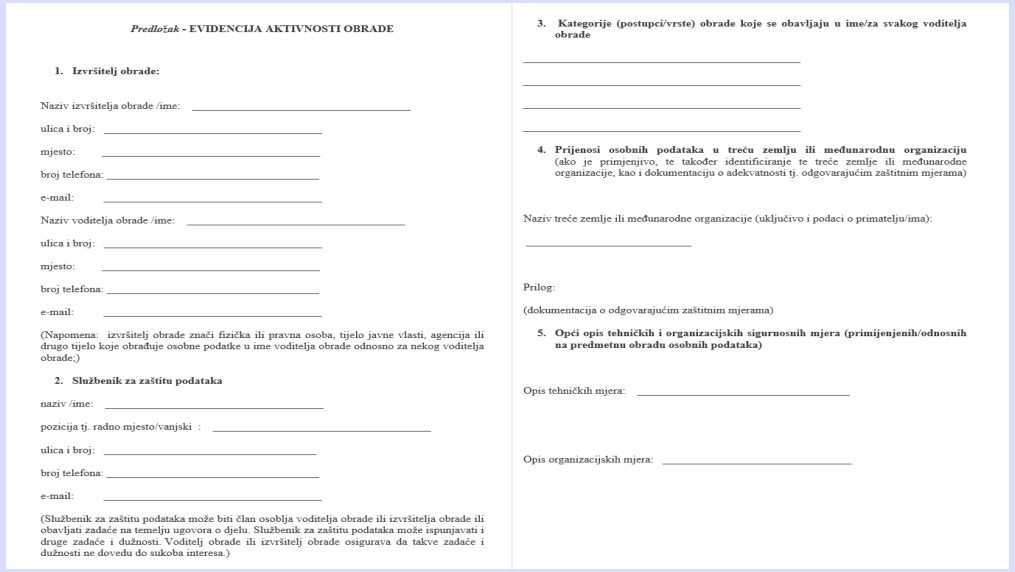
- Umjesto „zbirki osobnih podataka” OUZP uvodi pojam **obrade**
- **Obrada osobnog podatka** je svaki **postupak** ili skup postupaka koji se obavljaju **na osobnim podacima** ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima… **u neku svrhu**.
- Može biti: prikupljanje, 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!**

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	POVLAČENJE NA DORAZ 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 (navedeno članku 9. GDPR-a), ako je primjenjivo	IME I KONTAKT PODACI ZAJEDNIČKOG VODITELJA (AKO JE PRIMJENJIVO)
Naziv pod kojim je obrada prepoznatljiva	Zaposlenici, kupci, potpisnici, vanjski suradnici,...	Podaci o izvršitelju obrade (ako postoji)	Razlog obrade podataka	mapa ili naziv/lokacija računalnog programa gdje/kroz koje 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 otvorju 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 povremeno na privola ili lokaciju privola ukoliko je ta kvota temelj ove obrade	Identifikacijski podaci, lokacijski podaci, financijski podaci, zdravstveni podaci itd.	Obuhvata li obrada posebne kategorije podataka - podaci o zdravlju, članstvu u sindikatu, vjeroispovijesti, političke stavove, spolnu orijentaciju, rasu...?	Unijeti pravni temelj za obradu posebnih kategorija osobnih podataka	Ako obrađe ili više voditelja obrade zajednički odrede svrhe i načine obrade, ovo 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 nazivu/lokacija računalnog programa gdje/kroz koje se vrši obrada podataka ili lokacija fizičkog mjesta pohrane ako podatak nije digitaliziran	Obrada je nužna radi poštivanja pravnih obveza voditelja obrade (čl. 6. st. 1. točka c) GDPR-a, čl. 1. točka c) , Zakon o radu (NN 93/2014, 127/2017, 98/2019) Pravilnik o sadržaju i načinu vođenja evidencija o radnicima (NN 73/17, 87/17)	Pravo na pristup podacima, pravo na ispravak	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 d.o.o.	Obračun i isplata plaća	mapa pod nazivom zaposlenici, isplata plaća u SAP-u, zaštićena šifrom	Obrada je nužna radi poštivanja 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 (struč.sprema/naziv, datum početka rada, naziv/adresa radi kar-ti punom radnom vremenu ili nepunom radnom vremenu, vrsta rada, datum prestanka radnog odnosa, razlog prestanka radnog odnosa, podaci za potrebu interne komunikacije unutar tvrtke (poslovni kontakt e-mail, tel.)	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 na zapošljavanje u FIRMI, 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 i prezime, OIB, datum rođenja, spol, prebivalište, boravište, državljanstvo), PODACI O RADNOM ISKUSTVU, PODACI O OBRAZOVANJU PODACI O OSOBINAMA VAŠTINAMA	Ne	Nije primjenjivo	Nije primjenjivo
Primjer: EVIDENCIJA KUPACA	Kupci	Nema	slanje novosti/ponuda o svrhu promocije i slanje novih proizvoda, usluga i popusta postojećim kupcima	mapa pod nazivom kupci u SAP-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 dosadan 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 tvrtke, a ne službenika za zaštitu podataka (DPO). Međutim, zadatak se može delegirati DPO-u ako se on slaže. Prije GDPR-a to je bilo kontroverzno, ali sada nadzorna tijela priznaju mogućnost delegiranja.
- Ne treba podcijeniti trud koji je potreban za početnu uspostavu evidencije o aktivnostima obrade. Naknadno održavanje također veže resurse. Posebno u srednjim i većim tvrtkama to zahtijeva 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 "administracija razgovora za ocjenjivanje" ili dvije aktivnosti obrade "ciljani sporazum" 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, niža 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

Primjer evidencije aktivnosti obrade (ROPA) – 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										

Anonimizacija i pseudonimizacija

- Propisi o zaštiti osobnih podataka ne primjenjuju se na podatke koji su anonimizirani
- Anonimizacija je metoda uklanjanja informacija iz skupova podataka tako da ispitanici ne mogu biti izravno povezani s podacima
- Cilj anonimizacije je zaštititi privatnost pojedinaca uklanjanjem identificirajućih informacija iz skupova podataka, što omogućava da se podaci dalje koriste za istraživanje, analizu ili druge svrhe

Anonimizacija i pseudonimizacija – vrste i primjeri

- Anonimizacija podataka je postupak obrade osobnih podataka kojim se nepovratno onemogućuje identifikacija pojedinca iz podataka koji se obrađuju. Na primjer, razmotrite skup podataka o plaći koji sadrži zapise:

Prezime	Ime	E-mail	Opis posla	Odjel	Plaća
Horvat	Michelle	michelle@mailme.com	Zaštitarski poslovi	Sigurnost	3.500,00 €
Jurić	Ognjen	ognjen@mailme.com	Administrator u uredu	Administracija	2.000,00 €
Pranjić	Sonja	sonja@mailme.com	Voditelj marketinga	Marketing	5.000,00 €
Smješić	Tea	tea@mailme.com	Direktor prodaje	Prodaja	8.000,00 €
Zlatović	Alan	alan@mailme.com	Predsjednik Uprave	Uprava	14.000,00 €

Anonimizacija i pseudonimizacija – vrste i primjeri

- Jednostavan primjer anonimiziranja tog skupa podataka bilo bi uklanjanje informacija o imenu, prezimenu i adresi iz svakog zapisa.
- Iako bi to spriječilo izravnu identifikaciju pojedinaca, one bi mogle biti identificirane neizravno, posebno kada se koriste dodatni skupovi osobnih podataka:

Prezime	Ime	E-mail	Opis posla	Odjel	Plaća
xxxxxx	xxxxxx	xxxxx@xxxxx.xxx	Zaštitarski poslovi	Sigurnost	3.500,00 €
xxxxxx	xxxxxx	xxxxx@xxxxx.xxx	Administrator u uredu	Administracija	2.000,00 €
xxxxxx	xxxxxx	xxxxx@xxxxx.xxx	Voditelj marketinga	Marketing	5.000,00 €
xxxxxx	xxxxxx	xxxxx@xxxxx.xxx	Direktor prodaje	Prodaja	8.000,00 €
xxxxxx	xxxxxx	xxxxx@xxxxx.xxx	Predsjednik Uprave	Uprava	14.000,00 €

Anonimizacija i pseudonimizacija – vrste i primjeri

- Pseudonimizacija je postupak zamjene identifikacijskih podataka pojedinca u skupu podataka pseudonimom ili nasumičnim identifikatorom, a da se podaci još uvijek mogu ponovno povezati s ispitanikom ako je potrebno
- I pseudonimizacija i anonimizacija su metode za zaštitu privatnosti osobnih podataka, ali se razlikuju u stupnju sigurnosti koji nude i u kojoj mjeri dopuštaju korištenje podataka u pravne svrhe.
- Pseudonimizirani podaci još uvijek se mogu povezati s određenom osobom ako je potrebno. To je glavna razlika između pseudonimizacije i anonimizacije.
- Iako pseudonimizacija povećava slobodu korištenja podataka, ona također može povećati opasnost od izlaganja osobnih podataka ako pseudonimi nisu primjereno zaštićeni.
- Kao metoda sigurnosti podataka, pseudonimizacija zamjenjuje osobne podatke ili elemente osobnih podataka kodovima ili drugim pseudonimima kako bi se zaštitila privatnost tih informacija. Cilj ove metode je spriječiti izravnu identifikaciju pojedinaca, a istovremeno dopustiti da se podaci koriste u legitimne svrhe.

Primjer slučaja (2)

- Poduzeće za javni prijevoz želi prikupiti statističke podatke na temelju putničkih ruta, što može biti korisno u svrhu donošenja ispravnih odluka o promjenama u rasporedu javnog prijevoza i ispravnim rutama kompozicija.
- Putnici trebaju kartu provući kroz čitač svaki put kada ulaze ili izlaze iz prijevoznog sredstva. Provedenom procjenom rizika vezano za prava i slobode putnika u vezi prikupljanja ruta putovanja putnika, voditelj obrade utvrđuje da je putnike moguće identificirati u okolnostima gdje žive ili rade u slabo naseljenim područjima, temeljem jedinstvene identifikacije rute zahvaljujući identifikatoru karte.
- Stoga, budući da nije potrebno u svrhu optimizacije rasporeda javnog prijevoza i ruta vlakova, voditelj obrade ne pohranjuje identifikator karte. Nakon što je putovanje završeno, pohranjuje se samo pojedinačne putne rute kako ne bi mogli identificirati putovanja povezana na jednu kartu, ali se zadržavaju informacije o odvojenim rutama putovanja. Ukoliko bi i dalje bilo moguće identificirati putnika, voditelj obrade treba:

Genetski i biometrijski podaci

- **„genetski podaci”**
- osobni podaci koji se odnose na naslijeđena ili stečena genetska obilježja pojedinca koja daju jedinstvenu informaciju o fiziologiji ili zdravlju tog pojedinca,
- dobiveni osobito analizom biološkog uzorka dotičnog pojedinca;
- **„biometrijski podaci”**
- osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca
- fotografije lica, otisak prsta, šarenica oka, zvuk glasa

Profiliranje korisnika

- izrada profila je automatizirana obrada osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s pojedincem
- Ovakva obrada je korisna za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca;

Primjeri pseudonimizacije

- Prije pseudonimizacije:

Ime: Stjepan

Prezime: Horvath

Datum rođenja: 01.01.1980

Spol Muški

Nacionalnost: Nijemac

JMBG: 123-45-6789

Kućna adresa: 123 Ilica Zagreb

Nakon pseudonimizacije:

Ime: penehspet

Prezime: havaroht

Datum rođenja: XX/XX/0000

Spol:

Nacionalnost: mnarGe

JMBG: XXX-YY-6789

Kućna adresa: XXX 123 Ilica Zagreb

- U gornjem primjeru, podaci su šifrirani, maskirani ili uklonjeni ostavljajući pseudonimizirane podatke s malim rizikom od povrede osobnih podataka za nositelja podataka

Primjeri pseudonimizacije

- Prije pseudonimizacije:

Ime autora: David

Prezime: Zindel

Zemlja porijekla: SAD

Žanr: znanstvena fantastika

Nakon pseudonimizacije:

Ime autora:
a6b54c20a7b96eeac1a911e6da3124a560fe6
dc042ebf270e3676e7095b95652

Prezime:
aee714d921bccc21f1586266552f80e9a72b2
5e12d074214029f11e244e04a48

Zemlja podrijetla:
5fc90ab335783816990ffd960cbad0afd64510
a53f895b4d02b9f8b279c0ed08

Žanr: znanstvena fantastika

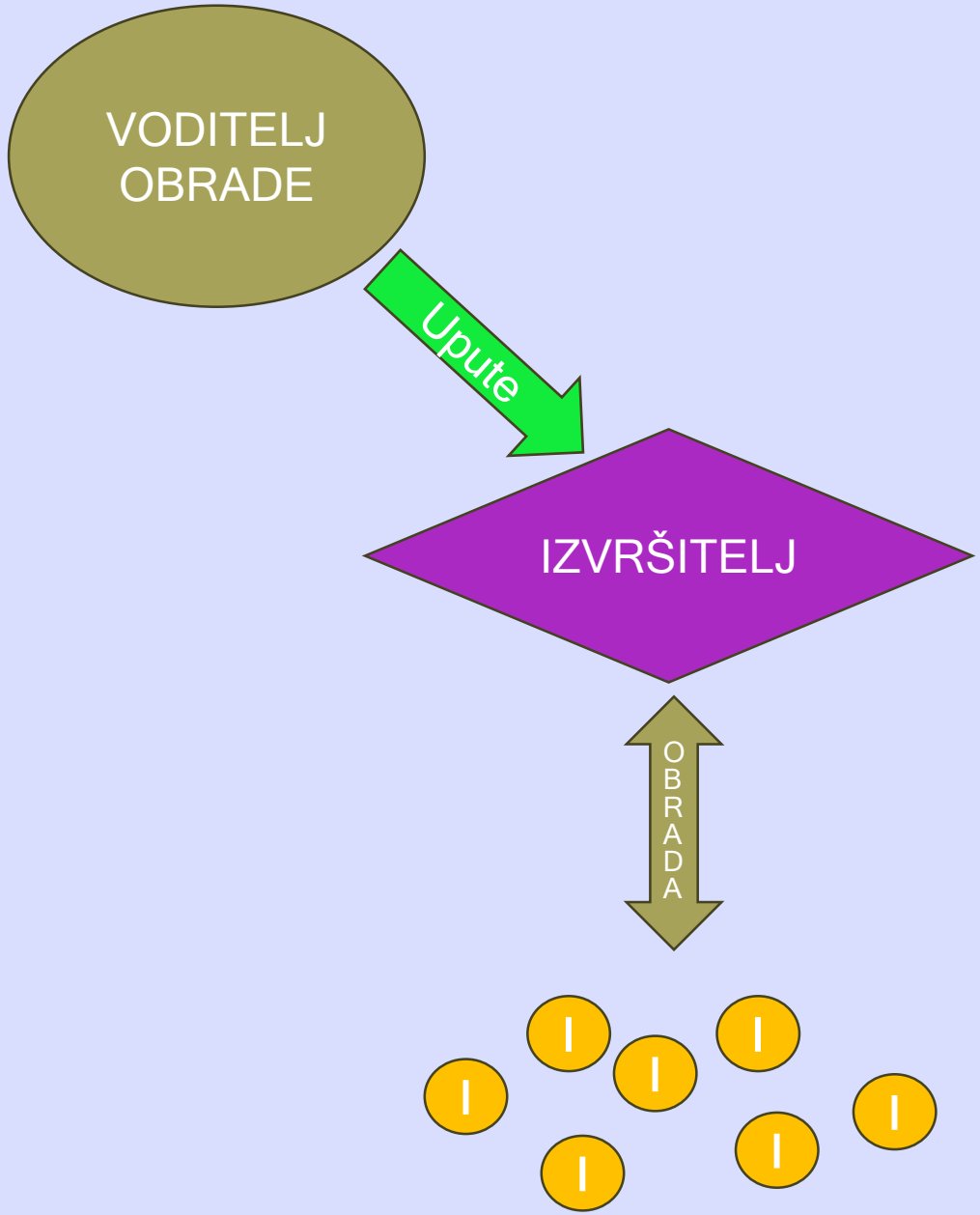
- U gornjem primjeru, podaci su hashirani korištenjem javnog SHA-256 hash kalkulatora ostavljajući pseudonimizirane podatke smanjenim rizikom povrede osobnih podataka nositelju podataka.

Voditelj i izvršitelj obrade

- „Voditelj obrade” znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka
- Kada su svrhe i sredstva obrade utvrđeni pravom Unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom Unije ili pravom države članice;
- „Izvršitelj obrade” znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade;
- Oznake voditelj ili izvršitelj **nisu apsolutne – odnose se na konkretnu obradu**

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

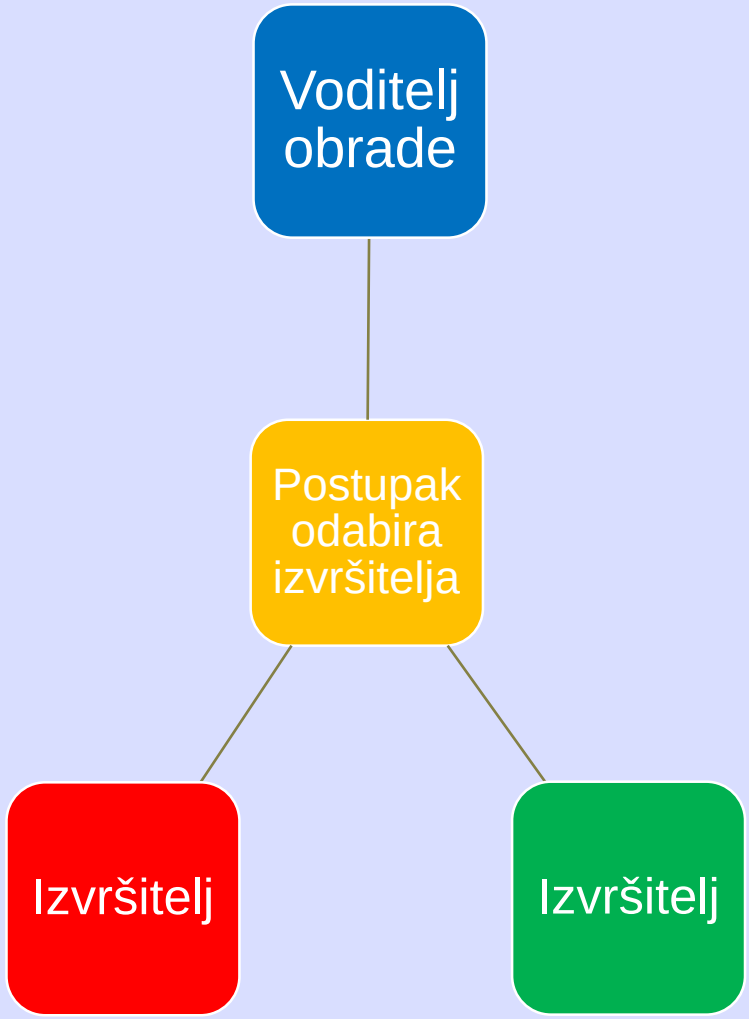
- Obrađujete osobne podatke za potrebe druge strane i u skladu s njezinim dokumentiranim uputama - nemate vlastitu svrhu obrade
- Druga strana nadzire vaše aktivnosti obrade kako bi osigurala da se pridržavate uputa i uvjeta ugovora
- U obradi ne slijedi vlastitu svrhu osim vlastitog poslovnog interesa 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 podobrađivač)

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 vašeg subjekta (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

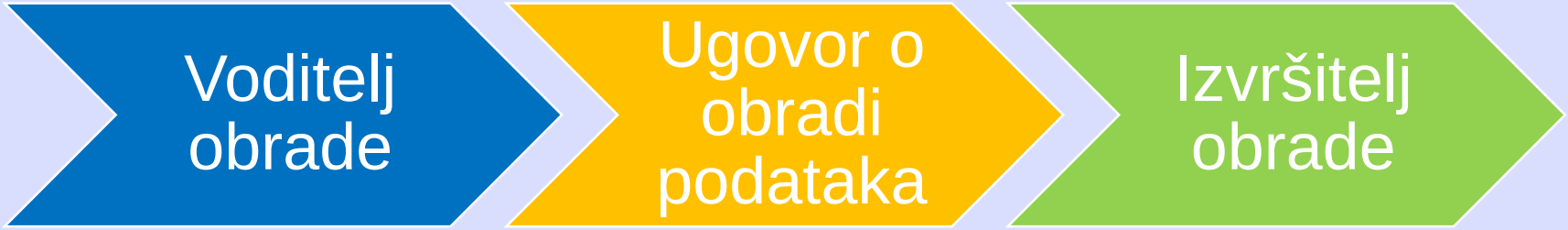
Odnos voditelja obrade i izvršitelja

- **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.



Primjer slučaja (3)

- Usluge čišćenja - tvrtka A sklapa ugovor s tvrtkom B za usluge čišćenja kako bi ih angažirala za čišćenje svojih ureda.
- Zaposlenici tvrtke B – čistači i čistačice ne bi smjeli pristupati osobnim podacima niti ih na drugi način obrađivati. Iako povremeno mogu naići na takve podatke dok se kreću u uredu, mogu obavljati svoj zadatak bez pristupa podacima te im je ugovorom zabranjen pristup ili drugačija obrada osobnih podataka koje tvrtka A vodi kao voditelj obrade.
- Čistačice nisu zaposlene u tvrtki A niti se smatraju pod izravnom nadležnošću te tvrtke. Ne postoji namjera angažirati tvrtku za čišćenje ili njezine zaposlenike da obrađuju osobne podatke u ime tvrtke A. Tvrtku za usluge čišćenja i njezine zaposlenike stoga ne treba promatrati kao izvršitelje, a voditelj obrade treba osigurati da postoje odgovarajuće sigurnosne mjere kako bi se spriječio njihov pristup podacima i propisati obvezu povjerljivosti u slučaju da slučajno dođu do osobnih podataka.
- Kakav je odnos tvrtke A i tvrtke B?

Primjer slučaja (4)

- Putnička agencija na tržištu nudi turist-pakete koji uključuju prijevoz avionom, odsjedanje u nizu hotela, prijevoz između hotela i turističkog vodiča. Kako bi mogla nuditi takvu uslugu, agencija šalje osobne podatke svojih klijenata zračnom prijevozniku i lancu hotela, u svrhu rezervacije turističkog paketa.
- Zrakoplovna tvrtka i hoteli potvrđuju dostupnost traženih sjedala i soba. Turistička agencija za klijente izdaje putne dokumente i vaučere za odsjedanje u hotelu.
- Svaki od organizacija obrađuje podatke za obavljanje vlastitih aktivnosti i koristeći vlastita sredstva. U ovom slučaju, putnička agencija, zrakoplovni prijevoznik i hotel tri su različita voditelja obrade podataka koji obrađuju podatke za svoje vlastite i odvojene svrhe i ne postoji zajedničko upravljanje.
- Međutim, zbog bolje procjene troškova, uže suradnje i konkurentnosti na tržištu agencija, lanac hotela i zračni prijevoznik odlučuju zajednički sudjelovati u uspostavljanju zajedničke internetske platforme za zajedničku svrhu pružanja paket aranžmana. Dogovaraju se o osnovnim sredstvima koja će se koristiti, kao što su podaci koji će biti pohranjeni, kako će se rezervacije dodjeljivati i potvrđivati i tko može imati pristup pohranjenim informacijama.
- Nadalje, odlučuju dijeliti podatke svojih kupaca kako bi proveli zajedničke marketinške akcije. Iz perspektive odredbi OUZP, kako se zove takav odnos odnosno kako nastupaju navedeni voditelji obrade?

Primjer ugovora o obradi osobnih podataka

Ugovor o obradi podataka između voditelja obrade i izvršitelja obrade prema članku 28. st. 3. Opće uredbe o zaštiti podataka sklapa se između

izvršitelja obrade (Ime i kontakt podaci izvršitelja)

i

voditelja obrade (Ime i kontakt podaci voditelja obrade)

Uvodne odredbe

Voditelj obrade želi ugovoriti izvršenje usluga navedenih u čl. 3. ovog ugovora s Izvršiteljem. Ugovorene usluge uključuju obradu osobnih podataka. Opća uredba o zaštiti podataka (Uredba), posebice čl. 28. Uredbe postavlja određene zahtjeve u pogledu obrade osobnih podataka koje je izvršitelj dužan ispunjavati u ime voditelja obrade. Kako bi se osiguralo ispunjenje tih zahtjeva, stranke sklapaju ovaj Ugovor.

Čl. 1. Definicije pojmova

Pojmovi korišteni u ovom Ugovoru, a koji su definirani člancima Opće uredbe o zaštiti podataka imat će značenje kako je utvrđeno primjenjivim odredbama Uredbe.

Čl. 2 Predstavnici na području Europske unije

(ukoliko je primjenjivo): Prema odredbama čl. 27. st.1. Opće uredbe, izvršitelj je za predstavnika na području Europske unije odabrao:

_____

(Ime i prezime, trgovačko društvo (ukoliko je primjenjivo), e-mail adresa i telefonski broj Predstavnika)

3. Predmet ugovora

3.1. U ime voditelja obrade i temeljem glavnog ugovora sklopljenog dan/mjesec/godina („Glavni ugovor"), izvršitelj će pružati usluge voditelju obrade na sljedećim područjima:

_____

U tu svrhu, voditelj obrade ustupit će potrebne osobne podatke Izvršitelju obrade koji će obrađivati te podatke isključivo u ime voditelja obrade i prema uputama koje će mu dati voditelj obrade, osim ukoliko je drukčije uređeno pravom Europske unije ili zakonskim odredbama zakonodavstva neke države članice Unije primjenjivim na Izvršitelja obrade. Svrha i opseg obrade osobnih podataka od strane izvršitelja određene su Glavnim ugovorom i uputama voditelja obrade te opisane u Dodatku 1 ovog Ugovora. Voditelj obrade odgovoran je za zakonitost obrade podataka prema čl.6.st.1. Opće uredbe o zaštiti podataka.

3.2. Stranke su suglasne urediti ovim Ugovorom svoj odnos u pogledu prava i obveza prema primjenjivim propisima iz područja zaštite osobnih podataka. U slučaju dvojbe, odredbe ovog Ugovora imaju prednost nad odredbama Glavnog ugovora.

3.3. Odredbe ovog Ugovora primjenjive su na sve aktivnosti koje se poduzimaju u svezi s Glavnim ugovorom od strane Izvršitelja obrade, njegovih zaposlenika ili agenata u pogledu osobnih podataka koji potječu od voditelja obrade, koji su prikupljeni za voditelja obrade ili koji se obrađuju u ime voditelja obrade.

3.4. Ovaj se Ugovor primjenjuje za vrijeme primjene Glavnog ugovora, osim ukoliko neke od sljedećih odredbi određuju daljnje obveze ili pravo na raskid ugovora.

3.5. Svaka dogovorena obrada osobnih podataka odvijat će se isključivo na području države članice Europske unije ili na području države članice Ugovora o europskom gospodarskom prostoru. Premještanje bilo kojeg dijela usluge ili cijele usluge u treću zemlju može se dopustiti samo ukoliko su ispunjeni uvjeti iz čl. 44. Opće uredbe o zaštiti podataka i ukoliko o tome postoji prethodni sporazum s voditeljem obrade u pisanom ili dokumentiranom elektroničkom obliku.

Čl. 4. Kategorije podataka koji se obrađuju i kategorije ispitanika

4.1. Postupajući prema Glavnom ugovoru, izvršitelju obrade omogućit će se pristup osobnim podacima specificiranima u Dodatku 1, a koji pripadaju kategorijama ispitanika također specificiranima u Dodatku 1.

4.2.(*Opcionalno)* Među navedenim podacima nema podataka koji se ubrajaju u posebne kategorije osobnih podataka.

4.2. (*Opcionalno)* Među navedenim podacima nalaze se osobni podaci koji pripadaju u posebne kategorije osobnih podataka i označeni su u Dodatku 1 Ugovoru kao takvi.

Čl. 5. Voditeljeve upute izvršitelju

5.1. Izvršitelj smije prikupljati, koristiti ili na drugi način obrađivati osobne podatke unutar opsega predviđenog Glavnim ugovorom i u skladu s uputama voditelja obrade, posebno u pogledu potencijalnog prijenosa podataka u treću zemlju ili prema međunarodnoj organizaciji. Ukoliko izvršitelj obrade treba dalje obrađivati podatke temeljem obveze iz prava Europske unije ili prava države članice Unije primjenjivog na Izvršitelja obrade, izvršitelj će o tim obvezama notificirati voditelja obrade prije nego započne s takvom obradom.

5.2. Voditeljeve upute izvršitelju početno će se urediti ovim Ugovorom, no te se upute mogu izmijeniti, nadopuniti ili zamijeniti pojedinačnim uputama u pisanom ili dokumentiranom elektroničkom formatu. Voditelj obrade ima pravo izdavati takve upute u bilo kojem trenutku. Izmjene mogu uključivati upute oko ispravka, brisanja i obustave obrade podataka. Osobe koje su ovlaštene da izdaju ili primaju upute bit će posebno naznačene u Dodatku 5 ovog Ugovora. U slučaju promjene ili dugotrajne spriječenosti ovlaštenih osoba, stranke će komunicirati tko su njihovi zamjenici drugoj strani bez odgode.

5.3. Voditelj obrade i izvršitelj dokumentirati će sve upute koje su izdane izvršitelju i čuvat će navedenu dokumentaciju za vrijeme trajanja ovog Ugovora te pet godina kasnije. Upute koje se odnose na razdoblje nakon isteka Glavnog ugovora smatrat će se izmjenom uputa. Odredbe ovog Ugovora neće utjecati na moguću nadoknadu dodatnih troškova koji proizlaze iz takvih dodatnih uputa koje je voditelj obrade izdao izvršitelju obrade.

5.4. Ukoliko Izvršitelj obrade sumnja da upute koje mu je voditelj obrade dao nisu u skladu s propisima iz područja zaštite osobnih podataka, izvršitelj će bez odgode o tome obavijestiti voditelja obrade. Izvršitelj obrade ima pravo u takvom slučaju odgoditi primjenu takvih uputa dok od strane voditelja obrade ne dobije potvrdu ili izmjenu takvih uputa. Izvršitelj obrade ima pravo odbiti upute očito nezakonitog sadržaja.

Čl. 6. Izvršiteljeve zaštitne mjere

6.1. Izvršitelj će djelovati u skladu s pravnim zahtjevima iz područja zaštite osobnih podataka i neće prenositi ili činiti dostupnim trećima podatke koji potječu od voditelja obrade. Izvršitelj će poduzeti mjere u skladu s industrijskim sigurnosnim standardima i standardima na području informacijske sigurnosti kako bi se podaci i dokumenti adekvatno zaštitili od neovlaštenog pristupa i drugih rizika za tajnost i cjelovitost podataka.

6.2. U pogledu odgovornosti za postupke obrade u kojima sudjeluje, izvršitelj obrade će ustrojiti svoju unutarnju organizaciju na način koji je sukladan zahtjevima iz područja zaštite osobnih podataka. Osobito, izvršitelj će osigurati adekvatnu implementaciju svih nužnih tehničkih i organizacijskih mjera prema čl. 32. Opće uredbe o zaštiti podataka, a osobito mjere koje su naznačene u Dodatku 2 ovog Ugovora. U pogledu obrade posebnih kategorija osobnih podataka, izvršitelj će dodatno implementirati tehničke i organizacijske mjere propisane nacionalnim propisom o zaštiti osobnih podataka primjenjivim na voditelja obrade. Na zahtjev voditelja obrade, izvršitelj obrade će voditelju dostaviti detaljne podatke o tome kako su navedene tehničke i organizacijske mjere određene i implementirane. Izvršitelj obrade ima pravo izmijeniti implementirane sigurnosne mjere pod uvjetom da to ne ugrozi ugovorenu razinu zaštite.

6.3. (*Opcionalno*) U slučaju da je izvršitelj obrade dužan imenovati službenika za zaštitu osobnih podataka:

_____

Ime, prezime, adresa elektroničke pošte (koja se odnosi na funkciju SZOP, ne osobna), broj telefona

_____

Ukoliko je riječ o vanjskom SZOP, dodatno navesti trgovačko društvo, kontakt podatke

Primjer ugovora o obradi osobnih podataka

6.3. (*Opcionalno*) U slučaju da izvršitelj obrade nije prema Uredbi i drugim primjenjivim propisima dužan imenovati službenika za zaštitu podataka izvršitelj će imenovati savjetnika za zaštitu podataka:

(Ime, prezime, adresa elektroničke pošte (koja se odnosi na funkciju SZOP, ne osobna), broj telefona)

6.4. Zaposlenicima izvršitelja obrade koji obavljaju poslove vezane uz obradu osobnih podataka za izvršitelja zabranjuje se prikupljanje, korištenje ili druga obrada osobnih podataka bez odobrenja. Izvršitelj obrade osigurat će da svi zaposlenici koji sudjeluju u poslovima obrade osobnih podataka i ispunjenja ovog Ugovora potpišu odgovarajući ugovor o tajnosti podataka prema odredbama Čl. 28. st. 3. točka b Opće uredbe o zaštiti podataka. Izvršitelj obrade ima zadatak adekvatno educirati i uputiti zaposlenike o postojanju posebnih obveza iz područja zaštite osobnih podataka koje proizlaze iz ovog Ugovora, kao i o postojećem ograničenju svrhe obrade osobnih podataka i obvezi pridržavanja uputa. Izvršitelj obrade osigurat će da te obveze traju i nakon isteka ili raskida ovog Ugovora i nakon prestanka radnog odnosa zaposlenika kod izvršitelja. Voditelj obrade može zatražiti, a izvršitelj je dužan osigurati dokaz da se ove obveze ispunjavaju na adekvatan način.

6.5. Obrada osobnih podataka temeljem ovog Ugovora od strane zaposlenika u njihovim domovima ili drugim privatnim prostorima (rad na daljinu/home office zaposlenika izvršitelja obrade) dopušta se isključivo uz pristanak voditelja obrade. Ukoliko se osobni podaci obrađuju u domu zaposlenika, izvršitelj obrade dužan je ugovorom osigurati pristup tom prostoru u svrhe nadzora sigurnosti obrade osobnih podataka, osobito primjene odgovarajućih tehničkih i organizacijskih mjera nastavno na odredbe čl. 6.st.1. i 6.st.2. ovog Ugovora i odredbe čl. 32. Opće uredbe o zaštiti podataka.

Čl.7. Obveze izvršitelja obrade oko informiranja voditelja obrade

7.1. U slučaju smetnji, sumnje na povredu podataka, povrede ugovornih obveza od strane izvršitelja obrade, sumnje na sigurnosne incidente ili druge nepravilnosti u vezi s obradom osobnih podataka od strane izvršitelja obrade, od strane osoba zaduženih u okviru Ugovora ili od strane trećih osoba, izvršitelj obrade će o tome bez odlaganja obavijestiti voditelja obrade u pisanom obliku ili u dokumentiranom elektroničkom obliku. Navedeno vrijedi i za slučaj nadzora kojeg provodi Agencija za zaštitu osobnih podataka ili drugo nadzorno tijelo na području zaštite osobnih podataka. U opsegu koliko je to moguće, obavijest o mogućoj povredi treba sadržavati sljedeće podatke:

a) Opis i prirodu povrede osobnih podataka, osobito koje su kategorije osobnih podataka i ispitanika potencijalno pogođene povredom te koliki je broj osobnih podataka u pitanju
b) Opis mogućih posljedica povrede osobnih podataka i
c) Opis mjera koje su poduzete ili predložene od strane izvršitelja kako bi se ublažile posljedice povrede osobnih podataka i spriječile buduće povrede

7.2 Izvršitelj obrade poduzet će bez odlaganja sve nužne mjere da bi se zaštitili osobni podaci i spriječile moguće daljnje negativne posljedice na prava i slobode ispitanika. Izvršitelj obrade obavijestit će voditelja obrade o poduzetim mjerama i zatražiti daljnje upute.

7.3. U slučaju da se povreda podataka navedena u čl.7.1. ovog Ugovora odnosila i na podatke voditelja obrade, izvršitelj obrade će voditelju obrade pružiti sve potrebne informacije bez odlaganja.

7.4. U slučaju potrebe, izvršitelj obrade će na adekvatan način pomoći voditelju obrade da osigura sukladnost s voditeljevim obvezama prema čl. 33. i čl. 34. Opće uredbe o zaštiti podataka. Izvršitelj obrade će obavijesti o povredi u ime voditelja obrade izvršiti nakon primitka uputa u skladu s čl. 5. ovog Ugovora.

7.5. U slučaju da su podaci voditelja obrade potencijalno ugroženi postupcima zapljene ili oduzimanja stvari koji se vode kod izvršitelja obrade uslijed postupka ovrhe, stečaja ili stečajne nagodbe ili uslijed drugih događaja ili mjera koje je poduzela neka treća strana, izvršitelj će obavijestiti voditelja obrade o takvom postupku bez odlaganja, osim ukoliko je spriječen odlukom u sudskom ili upravnom postupku. U tom slučaju, izvršitelj obrade će bez odlaganja izvijestiti sva relevantna tijela i organizacije da prema odredbama Opće uredbe o zaštiti podataka voditelj obrade nosi isključivo pravo donošenja odluka u pogledu osobnih podataka.

7.6. U slučaju značajnih izmjena sigurnosnih mjera određenih čl. 6.2. ovog Ugovora, izvršitelj obrade će bez odlaganja izvijestiti voditelja obrade.

7.7. U slučaju promjene osobe koja obavlja zadatke službenika za zaštitu osobnih podataka ili savjetnika za zaštitu podataka, izvršitelj obrade će bez odlaganja izvijestiti voditelja obrade.

7.8. Izvršitelj obrade, i ukoliko je primjenjivo njegov predstavnik, vodit će evidenciju aktivnosti obrade za sve obrade koje se provode u ime voditelja obrade u skladu sa zahtjevima iz čl. 30.st.2. Opće uredbe o zaštiti podataka. Izvršitelj obrade dostavit će na zahtjev evidenciju aktivnosti obrade voditelju obrade.

7.9. Izvršitelj obrade će na odgovarajući način pomoći voditelju obrade u pogledu ispunjavanja njegove evidencije aktivnosti obrade, kao i pomoći oko provedbe procjene učinka na zaštitu podataka koju voditelj obrade provodi temeljem čl. 35. Opće uredbe o zaštiti podataka. Izvršitelj obrade također će pomoći voditelju obrade oko postupka prethodnog savjetovanja sa nadzornim tijelom temeljem čl. 36. Opće uredbe o zaštiti podataka. Izvršitelj obade će u oba slučaja na odgovarajući način dostaviti voditelju obrade potrebne pojedinosti.

Čl.8. Pravo voditelja obrade na nadzor nad radom izvršitelja obrade

8.1. Prije početka obrade podataka, a zatim redovito tijekom trajanja obrade, voditelj obrade dužan je provjeriti osiguravaju li tehničke i organizacijske mjere koje je poduzeo izvršitelj obrade adekvatnu razinu sigurnosti postupka obrade osobnih podataka. U tu svrhu, on može tražiti informacije od izvršitelja obrade ili zahtijevati da se provede nadzor od strane neovisnih stručnjaka, da se usvoje i provjeravaju odgovarajući industrijski certifikati ili rezultati interne revizije. Voditelj obrade također može, nakon pravovremene koordinacije i tijekom normalnog radnog vremena osobno nadzirati tehničke i organizacijske mjere izvršitelja obrade ili ih dati na provjeru neovisnim stručnjacima, osim ako su potonji tržišna konkurencija u odnosu na izvršitelja obrade. Voditelj obrade će kontrolirati rad izvršitelja obrade samo u u mjeri u kojoj je to potrebno kako ne bi nepotrebno ometalo poslovanje izvršitelja obrade.

8.2. Temeljem usmenog, pismenog ili elektroničkim putem dostavljenog zahtjeva voditelja obrade, izvršitelj obrade će na vrijeme obavijestiti voditelja obrade o svim pojedinostima i informacijama vezanim uz nadzor nad izvršiteljevim tehničkim i organizacijskim mjerama.

8.3. Voditelj obrade će dokumentirati nalaze nadzora i o tome obavijestiti izvršitelja na odgovarajući način. U slučaju da voditelj obrade otkrije greške ili nepravilnosti u radu izvršitelja, osobito u pogledu primjene uputa voditelja obrade, voditelj obrade će o tome bez odlaganja obavijestiti izvršitelja obrade. Ukoliko je potrebno izmijeniti upute ili način na koji izvršitelj obrade izvršava upute voditelja obrade, voditelj obrade će o tim izmjenama bez odlaganja obavijestiti izvršitelja obrade.

8.4. Na zahtjev voditelja obrade, izvršitelj obrade će voditelju obrade osigurati uvid u poduzeti sustav zaštite podataka i sustav provjere ovlasti zaposlenika za pristup podacima

8.5. Na zahtjev voditelja obrade, izvršitelj obrade će voditelju obrade predočiti dokumentaciju o ispunjenju obveze propisane čl. 6. st. 4. ovog Ugovora u pogledu osiguranja tajnosti podataka koje zaposlenici doznaju ili kojima imaju pristup u obavljanju svojih dužnosti.

8.6. *(Opcionalno)* Voditelj obrade naknadit će izvršitelju obrade troškove koji su nastali u okviru nadzora rada izvršitelja.

9. Odabir i ugovaranje podizvršitelja

9.1. (*Opcionalno):* Prema odredbama ovog Ugovora izvršitelj obrade nema mogućnost ugovoriti obradu osobnih podataka čija obrada je predmet ovog ugovora s podizvršiteljem.

9.1. (*Opcionalno):* Usluge obrade ugovorene ovim Ugovorom ili dijelovi tih usluga koj su dalje podrobnije opisani, izvršit će se uz pomoć podizvršitelja koji su navedni u Dodatku 4 Ugovora. U okviru svojih ugovornih obveza, izvršitelj obrade može koristiti usluge daljnjih podizvršitelja pod uvjetom da se voditelj obrade, u pismenom obliku ili elektronički dokumentiranim putem suglasi s izborom podizvršitelja i da je o odabiru podizvršitelja obavješten unaprijed. Izvršitelj obrade će pažljivo odabrati podizvršitelje prema kriteriju njihove pouzdanosti i mogućnosti da ispune zahtjeve sigurnosti i povjerljivosti obrade. Kod odabira podizvršitelja, izvršitelj će osigurati da je voditelj obrade u mogućnosti izravno ostvarivati svoja prava prema ovom Ugovoru, osobito prava nadzora i kontrole rada, nad podizvršiteljima. Ukoliko su odabrani podizvršitelji iz trećih zemalja, izvršitelj obrade će osigurati da takvi podizvršitelji osiguraju odgovarajuću razinu zaštite osobnih podataka (primjerice, sklapanjem ugovora temeljenog na standardnim ugovornim klauzulama Europske unije). Na zahtjev voditelja obrade, izvršitelj obrade će dokazati da su takvi ugovori sklopljeni s podizvršiteljima.

Primjer ugovora o obradi osobnih podataka

9.1. (*Opcionalno*) Usluge obrade ugovorene ovim Ugovorom ili dijelovi tih usluga koj su dalje podrobnije opisani, izvršit će se uz pomoć podizvršitelja koji su navedni u Dodatku 4 Ugovora. U okviru svojih ugovornih obveza, izvršitelj obrade može koristiti usluge daljnjih podizvršitelja. Izvršitelj obrade će pažljivo odabrati podizvršitelje prema kriteriju njihove pouzdanosti i mogućnosti da ispune zahtjeve sigurnosti i povjerljivosti obrade. Kod odabira podizvršitelja, izvršitelj će osigurati da je voditelj obrade u mogućnosti izravno ostvarivati svoja prava prema ovom Ugovoru, osobito prava nadzora i kontrole rada, nad podizvršiteljima. Ukoliko su odabrani podizvršitelji iz trećih zemalja, izvršitelj obrade će osigurati da takvi podizvršitelji osiguraju odgovarajuću razinu zaštite osobnih podataka (primjerice, sklapanjem ugovora temeljenog na standardnim ugovornim klauzulama Europske unije). Na zahtjev voditelja obrade, izvršitelj obrade će dokazati da su takvi ugovori sklopljeni s podizvršiteljima.

9.2. Kad izvršitelj obrade ugovori s trećom stranom obavljanje pomoćnih poslova, to se neće smatrati podizvršiteljem u smislu odredbi ovog Ugovora. U takve pomoćne poslove ubrajaju se usluge poštanskog prometa, transporta i brodskog prijevoza, usluge čišćenja, usluge fizičke sigurnosti, telekomunikacijske usluge koje nisu u svezi s uslugama koje izvršitelj obrade temeljem ovog ugovora pruža voditelju obrade. Usluge održavanja i provjere IT opreme predstavljaju usluge podizvršitelja i traže prethodni pristanak voditelja obrade obzirom da se odnose na informacijske sustave koji se koriste u okviru izvršiteljevog davanja usluga za voditelja obrade.

10. Zahtjevi i prava ispitanika

10.1. Izvršitelj obrade pomagat će voditelju obrade primjenom odgovarajućih tehničkih i organizacijskih mjera ispunjavati obveze voditelja obrade kako su uređene člancima 12.-22., 32. i 36. Opće uredbe o zaštiti podataka.

10.2. Ukoliko ispitanik zatraži ostvarenje svojih prava izravno od izvršitelja obrade, izvršitelj obrade neće postupiti neovisno o voditelju obrade, već će ispitanika uputiti bez odlaganja voditelju obrade i pričekati upute voditelja obrade kako postupiti.

(Opcionalno) 10.3. Voditelj obrade nadoknadit će izvršitelju obrade troškove koji su nastali davanjem podrške voditelju obrade u ispunjenu zahtjeva i prava ispitanika.

11. Odgovornost voditelja obrade i izvršitelja obrade

11.1. Voditelj obrade i izvršitelj obrade bit će odgovorni prema ispitanicima u skladu s odredbama čl. 82. Opće uredbe o zaštiti podataka. Izvršitelj obrade će surađivati s voditeljem obrade oko mogućih slučajeva odgovornosti za štetu.

11.2. Na zahtjev voditelja obrade, izvršitelj obrade izuzet će voditelja obrade od odgovornosti za sve zahtjeve ispitanika protiv voditelja obrade koji su nastali temeljem povrede obveze koju izvršitelj ima prema voditelju obrade temeljem Opće uredbe o zaštiti podataka ili ukoliko izvršitelj obrade nije postupao u skladu s uputama koje su mu dane od strane voditelja obrade ovim Ugovorom ili posebno.

11.3. Ugovorne strane će osloboditi jedna drugu od odgovornosti ukoliko jedna od njih dokaže da nije odgovorna za okolnosti koje su dovele do nastanka štete za ispitanika. U ostalim slučajevima primjenjuju se odredbe čl. 82. st. 5. Opće uredbe o zaštiti podataka.

12. Pravo na izvanredni raskid ugovora

Voditelj obrade može raskinuti glavni ugovor u cijelosti ili otkazati neke njegove odredbe ukoliko izvršitelj obrade ne ispunjava svoje obveze temeljem Ugovora, ukoliko namjerno ili kroz krajnju nepažnju povređuje odredbe Opće uredbe o zaštiti podataka, nacionalnog zakona o zaštiti osobnih podataka i druge zakone ili propise koji se odnose na zaštitu osobnih podataka, ukoliko nije u mogućnosti ili ne želi ispuniti upute koje mu je dao voditelj obrade ili se protivi ostvarivanju prava voditelja obrade da nadzire provedbu obrade osobnih podataka prema uvjetima ugovorenima ovim Ugovorom.

13. Raskid Ugovora

13.1. Nakon raskida glavnog ugovora ili bilo u kojem trenutku na zahtjev voditelja obrade izvršitelj obrade će vratiti voditelju obrade sve dokumente, podatke i podatkovne medije koje je voditelj obrade ustupio izvršitelju obrade ili ih obrisati na zahtjev voditelja obrade, osim ukoliko je takvo brisanje zabranjeno propisima Europske unije ili Republike Hrvatske. Ova se obveza odnosi i na sve sigurnosne kopije (*backup*) koje je izvršitelj učinio. Izvršitelj također treba dokumentirati i na zahtjev pružiti dokumentaciju da je učinkovito obrisao voditeljeve podatke.

13.2. Voditelj obrade ima pravo provjeriti da li je izvršitelj obrade ispunio ugovorne obveze u pogledu vraćanja podataka ili učinkovitog brisanja podataka. Voditelj obrade može takvu provjeru povjeriti neovisnim ekspertima pod uvjetom da nisu u tržišnom natjecanju s izvršiteljem obrade.

13.3. Izvršitelj obrade treba osigurati povjerljivost podataka koji su mu postali poznati vezano uz glavni ugovor i nakon isteka glavnog ugovora. Odredbe ovog Ugovora ostat će na snazi i nakon isteka glavnog ugovora onoliko dugo koliko izvršitelj obrade bude u posjedu osobnih podataka koje je primio od voditelja obrade ili koje je prikupio u ime voditelja obrade.

14. Zaključne odredbe

14.1. Sve izmjene i dopune ovog Ugovora trebaju biti u pisanom obliku ili u obliku elektroničkog dokumenta. Ovaj Ugovor, kao i njegovi Dodaci, mogu biti izmijenjeni ili dopunjeni samo suglasnom odlukom ugovornih strana.

14.2. Odredbe ovog Ugovora tumačit će se u skladu s pravom Republike Hrvatske. Ugovorne strane se obvezuju da će sve eventualne sporove proizašle iz ovog Ugovora nastojati riješiti mirnim putem, a ukoliko to ne bude moguće ugovaraju nadležnost suda u _____ .

14.3. Ukoliko bi bilo koja odredba ovog Ugovora bila ili postala djelomično ili potpuno ništetna ili neprovediva to ne utječe na valjanost i održivost ostalih ugovornih odredbi.

14.4. Ovaj Ugovor stupa na snagu kad ga potpišu odgovorne osobe obiju ugovornih strana.

Dodaci ovom Ugovoru:

Dodatak 1 – Opis kategorija podataka, podataka koji uživaju posebnu razinu zaštite i ispitanika odnosno kategorija ispitanika

Dodatak 2 – Tehničke i organizacijske mjere koje primjenjuje izvršitelj obrade

Dodatak 3 – Popis odobrenih podizvršitelja obrade osobnih podataka

Dodatak 4 – Popis osoba autoriziranih za izdavanje odnosno primanje uputa

Za voditelja obrade:	Za izvršitelja obrade:
_____	_____
(Ime i prezime, funkcija u organizaciji)	*(Ime i prezime, funkcija u organizaciji)*
_____	_____
(Mjesto i datum, potpis)	*(Mjesto i datum, potpis)*

Dodatak 1 – Opis kategorija podataka, podataka koji uživaju posebnu razinu zaštite i ispitanika odnosno kategorija ispitanika, primjerice:

- Zaposlenici, klijenti, radnici poslovnih partnera itd.
- Ime, prezime, e-mail adresa, broj telefona itd.

Dodatak 2 – Tehničke i organizacijske mjere koje primjenjuje izvršitelj obrade

Dodatak 3 - Popis odobrenih podizvršitelja obrade osobnih podataka

Dodatak 4 - Popis osoba autoriziranih za izdavanje odnosno primanje uputa

Osobe koje u ime voditelja obrade mogu izdavati upute:

_____

Osobe koje u ime izvršitelja obrade trebaju primati upute:

_____

Komunikacijski kanali korišteni za slanje i primanje uputa:

_____

(poštanska adresa, adresa elektroničke pošte, broj telefona)

Predstavnik, grupa poduzetnika, poslovni nastan

- „predstavnik” znači fizička ili pravna osoba s poslovnim nastanom u Uniji koju je voditelj obrade ili izvršitelj obrade imenovao pisanim putem, a koja predstavlja voditelja obrade ili izvršitelja obrade u pogledu njihovih obveza na temelju OUZP
- „grupa poduzetnika” znači poduzetnik u vladajućem položaju te njemu podređeni poduzetnici
- „glavni poslovni nastan” - što se tiče voditelja obrade s poslovnim nastanima u više od jedne države članice, mjesto njegove središnje uprave u Uniji, osim ako se odluke o svrhama i sredstvima obrade osobnih podataka donose u drugom poslovnom nastanu voditelja obrade u Uniji te je potonji poslovni nastan ovlašten provoditi takve odluke, u kojem se slučaju poslovni nastan u okviru kojeg se donose takve odluke treba smatrati glavnim poslovnim nastanom

1. **Što je to predstavnik?**
2. **Koje on obveze ima u odnosu na voditelja obrade ili izvršitelja obrade?**
3. **Koje obveze ima prema ispitanicima i nadzornom tijelu?**

Primjer slučaja (5)

- Talijanska agencija DPA (Garante) pokrenula je istragu o parkirnim automatima u Rimu. Posebno zabrinjava činjenica da su vozači morali unijeti registarsku pločicu svog vozila kako bi dobili kartu za parkiranje.
- Sustavom koji je prikupljao informacije poput vremena početka i završetka parkiranja, iznosa duga i registarskih oznaka automobila upravljala je tvrtka Atac s.p.a. u ime Grada Rima.
- Nakon istrage pokrenute izvješćem koje je optužilo općinu za nezakonitu obradu osobnih podataka vozača, Garante je utvrdio da je voditelj obrade (Grad) povrijedio članak 25. OUZP jer nije obavijestio privatne tvrtke koje djeluju kao izvršitelji obrade o tome da djeluju kao izvršitelji, kao i koliko dugo trebaju obrađivati osobnih podataka i pobliže definirao svoje uloge pisanim ugovorom.
- Za ovaj slučaj može se zaključiti (moguće je više točnih odgovora):
  a) Garante je vjerojatno izdao novčanu upravnu kaznu
  b) Izvjesno je da povreda čl. 25 nije i jedina otkrivena povreda (koje bi još mogle biti prisutne?)
  c) Grad Rim zapravo nije počinio povredu
  d) Grad Rim bio je dužan provesti DPIA prije provođenja ove obrade

Privola

- „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;
- Jedna od šest pravnih osnova predviđenih člankom 6. Uredbe, često pogrešno shvaćena kao nužna i primarna
- Uvjeti i kvaliteta privole predmet su brojnih mišljenja nadzornih tijela, smjernica EDPB/WP29 i judikature ECJ

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

VODITELJ OBRADE:
OBRAZOVNA USTANOVA
ULICA, KUĆNI BROJ
POŠTANSKI BROJ, GRAD
EMAIL, TELEFON

PRIVOLA ZA OBRADU OSOBNIH PODATAKA
(prema čl. 7. Opće uredbe o zaštiti podataka)

IME I PREZIME

IDENTIFIKACIJSKA OZNAKA

KONTAKT PODATAK email@adresa.com

VRSTA PODATAKA Kontakt podaci elektroničke pošte

VRSTA PLANIRANE OBRADE Prikupljanje i upotreba adrese elektroničke pošte za slanje poruka elektroničke pošte

DAJEM PRIVOLU ZA OBRADU PODATAKA U SLJEDEĆE ODABRANE SVRHE:

- ☐ Slanje informacija o našim uslugama
- ☐ Organizacije školskog izleta (datum, lokacija, prijevoznik)
- ☐ Dostavu datoteke s posebnim kategorijama podataka

☐ Potvrđujem da sam upoznat/upoznata da ovu privolu mogu odbiti ili u bilo kojem trenutku povući te da je obrada podataka temeljem ove privole zakonita do trenutka povlačenja.

Datum: **Potpis:**

Privola se odnosi samo na navedene svrhe obrade i navedene kategorije osobnih podataka.
Privola se može povući pisanim putem na adresu: xxxx, putem e-pošte na adresu: xxx@xx.xx ili osobno na adresu sjedišta: adresa xx

PODACI O VODITELJU OBRADE
sjedište/kontakt
logo

PRIVOLA ZA OBRADU OSOBNIH PODATAKA
(sukladno uvjetima propisanim čl. 7 Opće uredbe o zaštiti podataka)

Posebne napomene:
- za dijete privolu daje roditelj/zakonski zastupnik, osim u slučaju nuđenja usluga informacijskog društva izravno djetetu starijem od 16 godina
- potrebno je informirati pojedinca o obradi podataka za automatizirano donošenje odluka te o mogućim rizicima prijenosa podataka zbog nepostojanja odluke o primjerenosti i odgovarajućim zaštitnim mjerama

Važno!!!
Obrazac ove privole služi kao predložak/kretaljka te se mora prilagoditi svakom konkretnom slučaju, dakle ne radi se o zadanom formatu privole!

Ime i prezime

Identifikacijska oznaka[1]

Ime i prezime roditelja/zakonskog zastupnika

Kontakt

Vrsta/kategorija[2] **prikupljenih podataka**

Vrsta obrade[3] **koja će se provesti**

DAJEM PRIVOLU ZA OBRADU OSOBNIH PODATAKA U SLJEDEĆE ODABRANE SVRHE:

- ☐ **tekst posebne obrade u specifične svrhe**
- ☐ **tekst posebne obrade u specifične svrhe**
- ☐ **tekst posebne obrade u specifične svrhe**

☐ **Potvrđujem da sam upoznat/upoznata s tim da ovu privolu mogu odbiti ili u svakom trenutku povući te da je obrada do trenutka povlačenja zakonita.**

**NAPOMENA: Privola se odnosi samo na navedene svrhe obrade i navedene kategorije osobnih podataka te se obrada osobnih podataka ne smije koristiti u druge svrhe. Obrada navedenih kategorija osobnih podataka provodit će se sukladno Općoj uredbi o zaštiti podataka i Zakonu o provedbi Opće uredbe o zaštiti podataka. Ako pojedinac želi povući privolu, to može učiniti pisanim putem na adresu: xxxx, putem e-pošte na adresu: xxx@xx.xx ili osobno na adresu sjedišta: adresa xx.

Mjesto/Datum

/Potpis/

[1] Primjerice, broj indeksa studenta, **a ne oib studenta** (kako bi se student ipak mogao identificirati prilikom povlačenja privole)
[2] Primjerice, fotografija studenta
[3] Primjerice: 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

Povreda osobnih podataka

- „povreda osobnih podataka” znači povreda sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani;

Kako prijaviti povredu osobnih podataka?

- Ukoliko se dogodi povreda, **voditelj obrade ima rok od 72 sata da povredu prijavi nadzornom tijelu**.
- Provjerite jeste li pripremili sljedeće podatke:
- **Pojedinosti o povredi** – opći pregled povrede, datum i vrijeme kada se dogodila, kako i kada ste saznali za nju, je li riječ o povredi kibernetičkim putem
- **Pojedinosti o podacima i osobama koje su pogođene** – koliko je podataka, koje vrste podataka, jesu li povrijeđeni podaci posebne kategorije, koliko ispitanika je pogođeno te mogući rizik za pojedince kao rezultat povrede.
- **Pojedinosti o zaposlenicima** – je li određeni zaposlenik voditelja obrade bio uključen i kakvu su obuku o zaštiti podataka prošli
- **Vaši napori da spriječite povredu i posljedice** - koje su TOMs primjenjuju, koje ste radnje poduzeli da spriječite nove povrede, jeste li se obratili ispitanicima, što ste drugim organizacijama rekli ili trebate reći o povredi

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

Nadzorno tijelo i predmetno nadzorno tijelo

- nadzorno tijelo” znači neovisno tijelo javne vlasti koje je osnovala država članica
- „predmetno nadzorno tijelo” znači nadzorno tijelo koje je povezano s obradom osobnih podataka zato što voditelj obrade ili izvršitelj obrade ima poslovni nastan na državnom području države članice tog nadzornog tijela ili obrada bitno utječe ili je izgledno da će bitno utjecati na ispitanike koji borave u državi članici tog nadzornog tijela ili podnesena je pritužba tom nadzornom tijelu.

Prava ispitanika u pogledu zaštite podataka prema OUZP i pravu EU

1. Pravo na informaciju o obradi osobnih podataka (transparentnost obrade)
2. Pravo na pristup svojim osobnim podacima
3. Pravo na ispravak podataka
4. Pravo na brisanje podataka
5. Pravo na ograničenje obrade
6. Pravo na prenosivost podataka
7. Pravo na prigovor
8. Pravo na prigovor automatiziranom pojedinačnom donošenju odluka, uključujući izradu profila

pravo ispitanika na pritužbu nadzornom tijelu

pravo ispitanika na učinkoviti pravni lijek protiv odluke nadzornog tijela

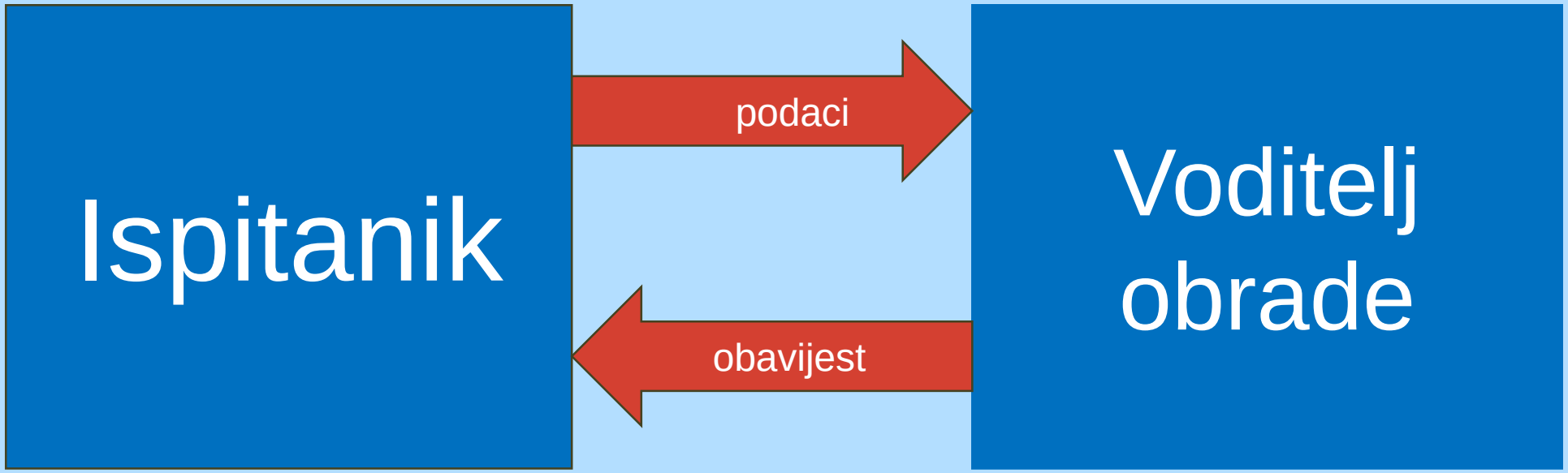
pravo ispitanika na učinkoviti pravni lijek protiv voditelja obrade ili izvršitelja obrade

pravo ispitanika na naknadu štete

Pravo ispitanika na informaciju o obradi osobnih podataka

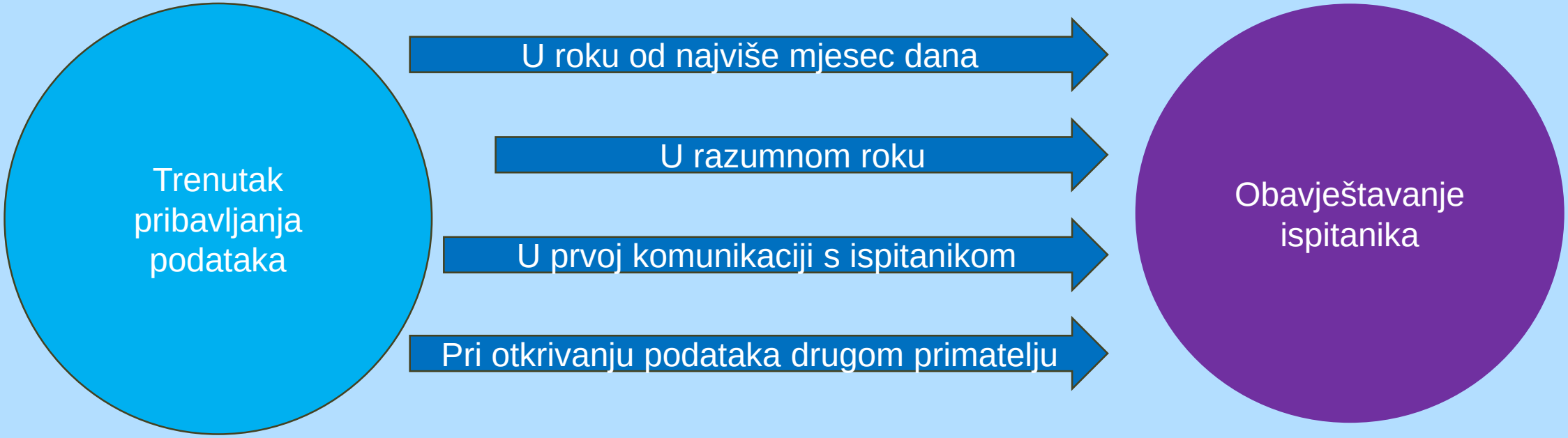
Ispitaniku treba učiniti dostupnim sljedeće informacije:
• podatke o identitetu i kontaktne podatke voditelja obrade
• svrhu obrade u koju se podaci prikupljaju te pravnu osnovu obrade
• krajnje primatelje ili kategorije primatelja osobnih podataka
• informaciju o prijenosu podataka u treće zemlje ili međunarodne organizacije
• vrijeme pohrane osobnih podataka prava ispitanika u pogledu konkretne obrade
• postoji li obveza ispitanika na davanje osobnih podataka i koje su posljedice uskrate
• upotrebljava li se sustav automatiziranog donošenja odluka ili profiliranja
• postojanje prava na pritužbu nadzornom tijelu

Trenutak davanja obavijesti ispitaniku



Iznimka – ukoliko ispitanik već raspolaže tim informacijama

Ako podaci nisu pribavljeni od ispitanika



Obavijest 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 velikog voditelja obrade
  - Primjer – obavijest za mali web-shop

Prvi sloj –kratka obavijest

Kratka obavijest o obradi osobnih podataka

Poštujemo Vašu privatnost i željeli bismo Vam u ovom dokumentu („Izjava“) na jasan i transparentan način dati informacije o tome koje osobne podatke prikupljamo, kao i o pravnim osnovama na temelju kojih obrađujemo osobne podatke.

Molimo Vas da pažljivo pročitate ovaj dokument, koji sadrži našu politiku privatnosti i informacije o tome na koji način koristimo Vaše osobne podatke kada posjećujete našu web stranicu, rezervirate smještaj, boravite u nekom od naših objekata ili ako iz drugih razloga komunicirate s nama.

O nama
Za potrebe ove Izjave i primjenjivih propisa o zaštiti osobnih podataka, uključujući i Opću uredbu o zaštiti osobnih podataka (EU) 2016/679 (dalje u tekstu; „Opća uredba“ ili „OUZP“) Voditelj obrade i društvo koje je odgovorno za obradu Vaših osobnih podataka je Trgovačko društvo d.d., OIB, Adresa.

Potpunu obavijest o obradi možete pronaći na ovoj adresi:

www.drustvo.com/obavijestoobradi.html

Osobni podaci obuhvaćaju bilo koje podatke koji se odnose na identificiranu fizičku osobu ili druge podatke pomoću kojih se osoba može identificirati. Podaci koje o Vama prikupljamo i obrađujemo ovise o Vašem odnosu s nama i razlozima naše komunikacije.

Primjeri osobnih podataka koje prikupljamo su:

Identifikacijski podaci, kontakt podaci, financijski podaci. Ne prikupljamo posebne kategorije osobnih podataka.

Vaša prava u vezi s obradom osobnih podataka
• Imate pravo pristupa Vašim osobnim podacima u svakom trenutku, slanjem zahtjeva kojim ćete zatražiti da Vam dostavimo sve Vaše osobne podatke koje obrađujemo.
• Imate pravo prigovoriti određenim aktivnostima obrade, primjerice ako obrađujemo Vaše osobne podatke na temelju legitimnog interesa.
• Imate pravo zatražiti prijenos osobnih podataka drugom pružatelju usluge – u praksi ovo znači da imate pravo tražiti da Vam dostavimo sve osobne podatke koje obrađujemo u strojno čitljivom obliku ili zatražiti da ih dostavimo izravno drugom društvu.
• Imate pravo zatražiti ažuriranje Vaših osobnih podataka, ispravak ili dopunu Vaših osobnih podataka u svakom trenutku.
• Imate pravo zatražiti brisanje Vaših osobnih podataka. Udovoljit ćemo Vašem zahtjevu, ako nemamo pravnu obvezu ili opravdani razlog pravne ili poslovne prirode zbog kojih bismo ih morali i dalje čuvati.
• U slučaju da obrađujemo Vaše podatke na temelju privole, u svakom trenutku ste ovlašteni povući danu privolu. Bez odgode ćemo prestati s obradom osobnih podataka prikupljenih na temelju te pravne osnove.

Primatelji osobnih podataka:
Vaše podatke ne dijelimo u svrhu oglašavanja. U određenim slučajevima vaše podatke možemo podijeliti s drugim primateljima – članicama naše grupe, u svrhu ispunjenja ugovora, u svrhu ispunjenja pravnih obveza, s pružateljima IT i drugih usluga.

Sve zahtjeve možete ostvariti slanjem pisanog zahtjeva na poslovnu adresu Društvo d.d., adresa ulica, broj, poštanski broj, grad, Službenik za zaštitu podataka ili na e-mail **szop@drustvo.hr**

Ispitanici mogu podnijeti pritužbu nadzornom tijelu za zaštitu podataka – Agenciji za zaštitu osobnih podataka:
Agencija za zaštitu osobnih podataka
Selska cesta 136
HR – 10 000 Zagreb
Tel. +385 (01) 4609-000
Fax. + 385 (01) 4609-099
E-mail: azop@azop.hr
Web: www.azop.hr

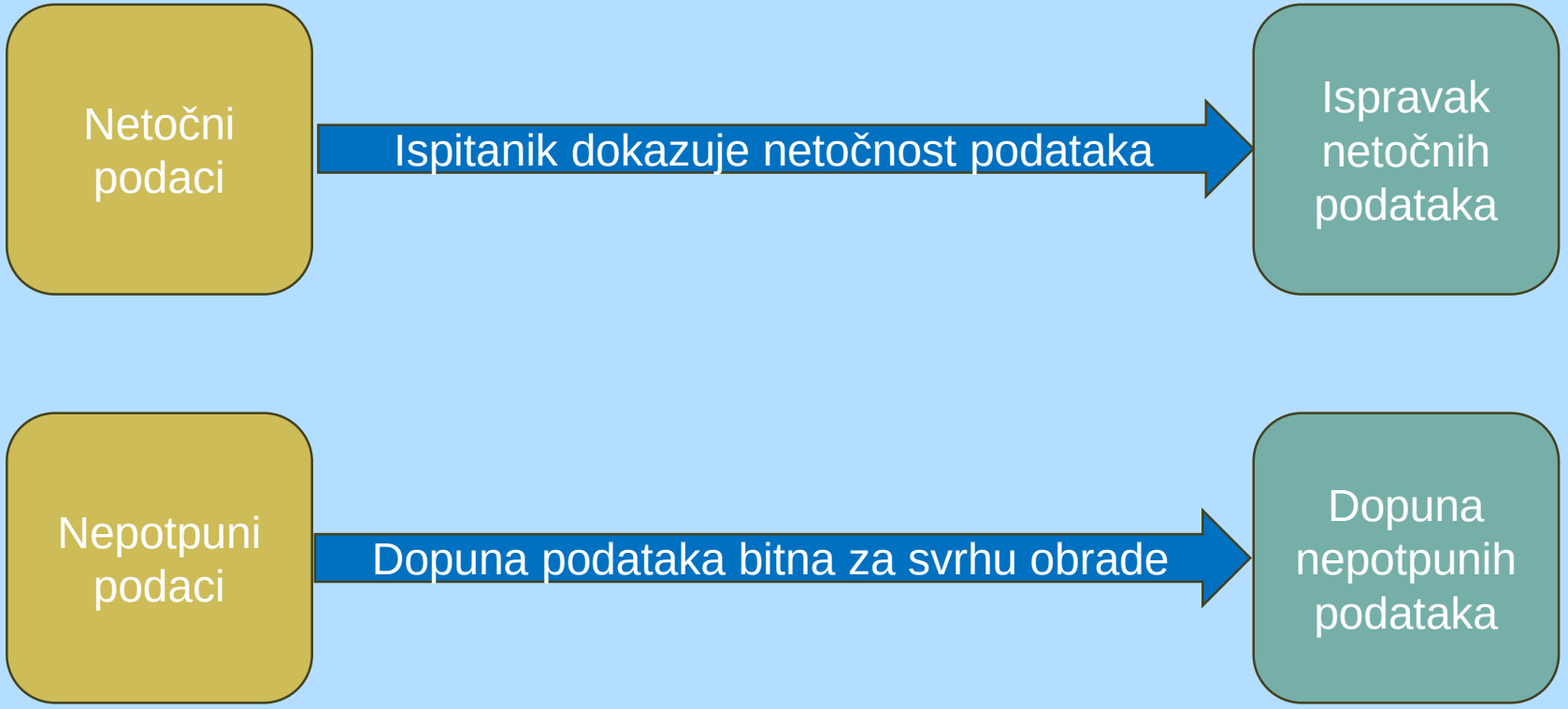
Primjer slučaja (6)

- Ispitanik je nadzornom tijelu podnio pritužbu na rad voditelja obrade, nezadovoljan što je njegov zahtjev za pristup kopiji podataka koje o podnositelju vodi voditelj obrade podataka u elektroničkom i ručnom obliku odbijen.
- Voditelj obrade podataka je umjesto toga obavijestio podnositelja pritužbe da su tražene datoteke dostupne na internetu ili za pregled u prostorijama voditelja obrade podataka. Tijekom istrage ove pritužbe, podnositelj pritužbe je tvrdio da datoteke koje je voditelj obrade podataka stavio na raspolaganje podnositelju pritužbe ne predstavljaju sve osobne podatke koji se odnose na podnositelja pritužbe koje posjeduje voditelj obrade podataka.
- Međutim, voditelj obrade smatrao je da je zahtjev za pristup koji je podnio podnositelj pritužbe bio ograničen na osobne podatke koji se čuvaju u vezi s dvije aplikacije koje je podnositelj naveo u zahtjevu za pristup. Sukladno navedenom, voditelj obrade nastojao je razlučiti osobne podatke aplikacija koje je ispitanik naveo u svom zahtjevu od onih koje nije naveo. Zahtjev za pristupom podacima bio je izražen općenito i tražio je pristup "svim podacima koje o meni čuvate elektronički ili u ručnom obliku" .
- Tko je u pravu?

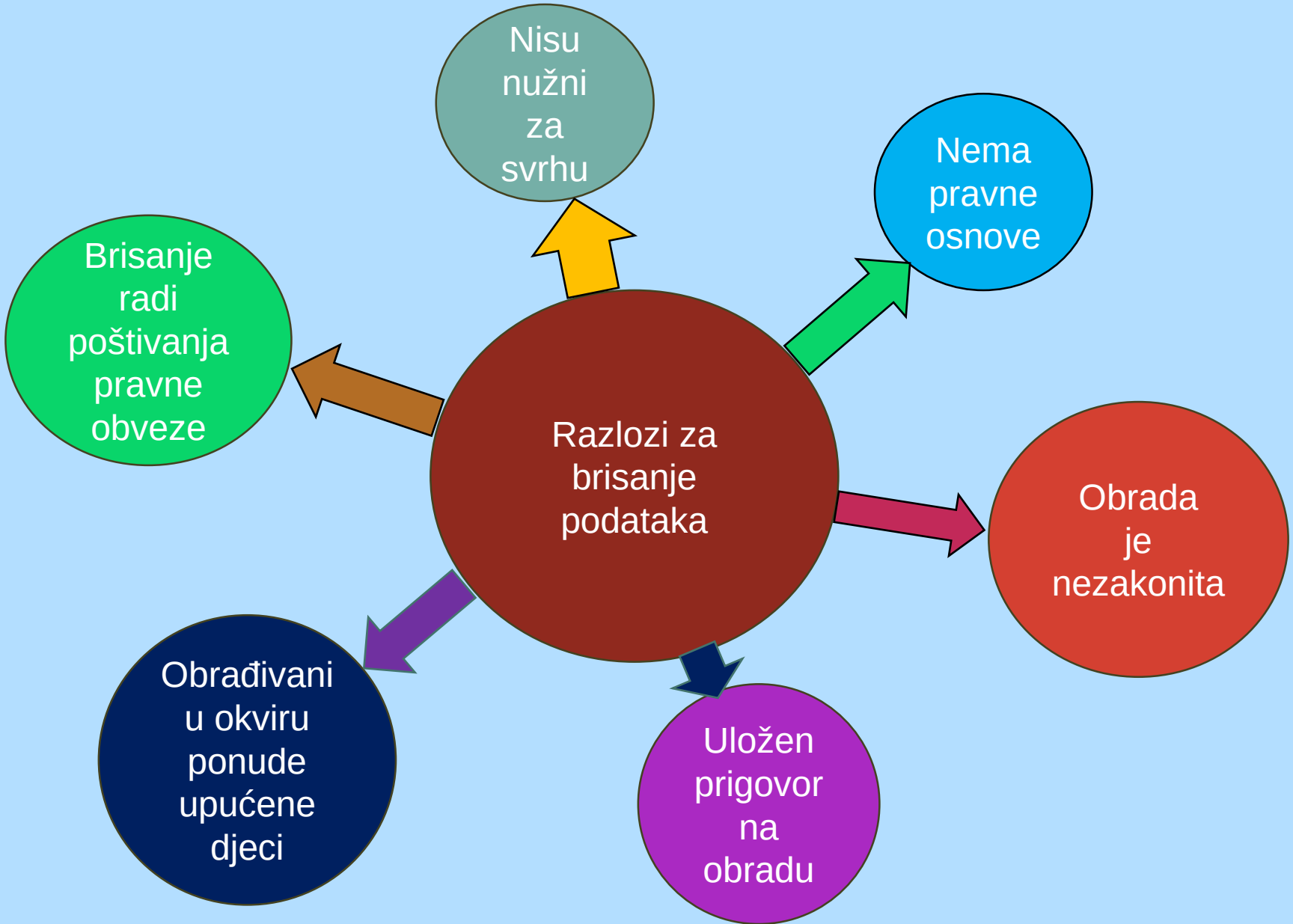
Pravo na pristup osobnim podacima

Ispitanik ima pravo saznati obrađuju li se podaci koji se odnose na njega	Dobiti pristup podacima i informacijama o obradi	Dobiti kopiju svojih podataka od voditelja obrade
Potvrda voditelja ispitaniku da se podaci koji se odnose na ispitanika obrađuju unutar obrada koje voditelj provodi	Podaci o obradi: svrha, kategorije podataka, primatelji, razdoblje čuvanja, obavijest o pravima, izvor podataka, logika automatske obrade… + zaštitne mjere u slučaju izvoza podataka	Ispitanik može dobiti kopiju podataka bez naknade (čl. 12/5, čl. 15/3) Dodatne kopije = razumna naknada troškova Ako je zahtjev elektronički, informacije se pružaju u „uobičajenom elektroničkom obliku” (mail, web sučelje, …)

Pravo na ispravak podataka

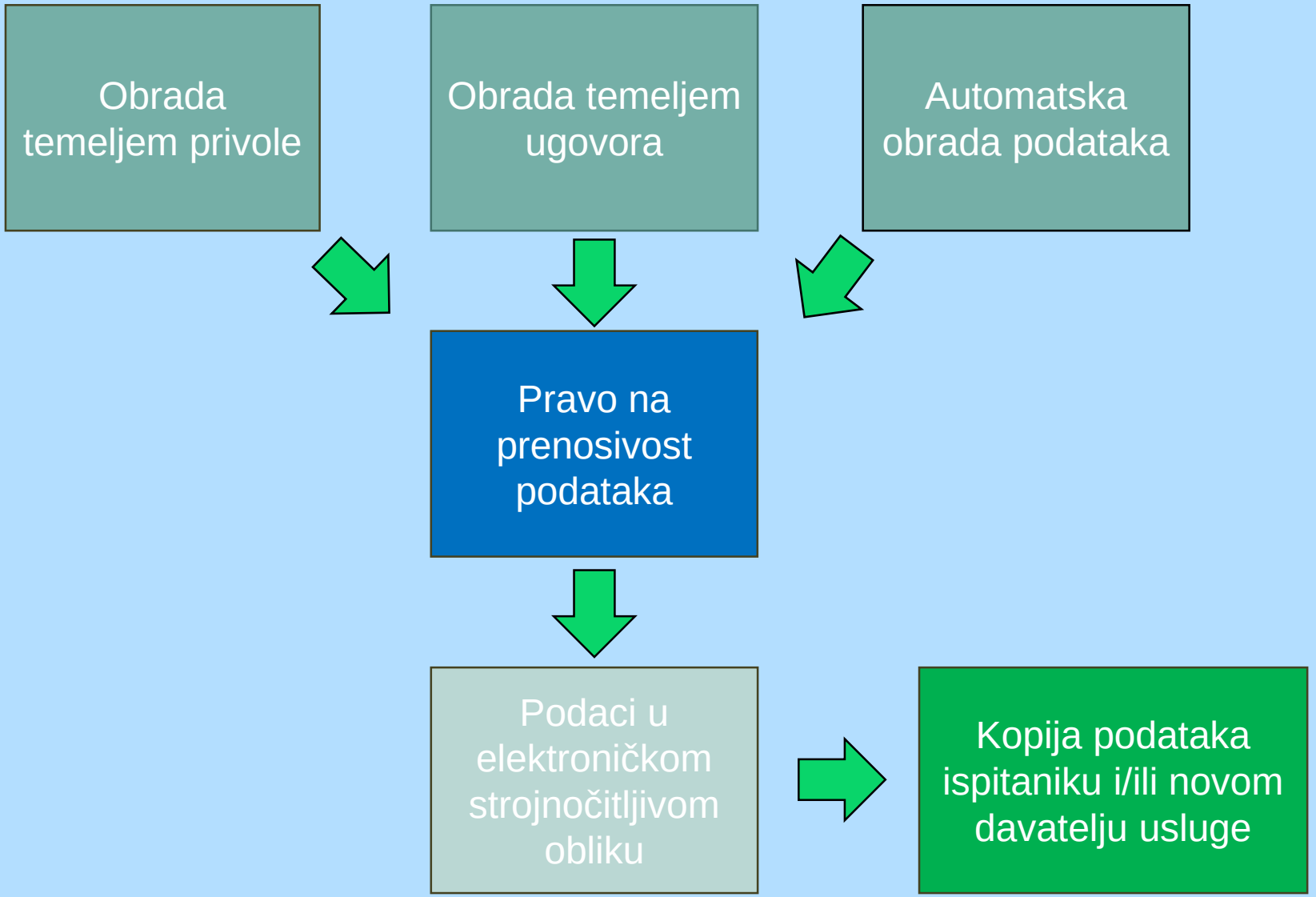


Pravo na brisanje podataka

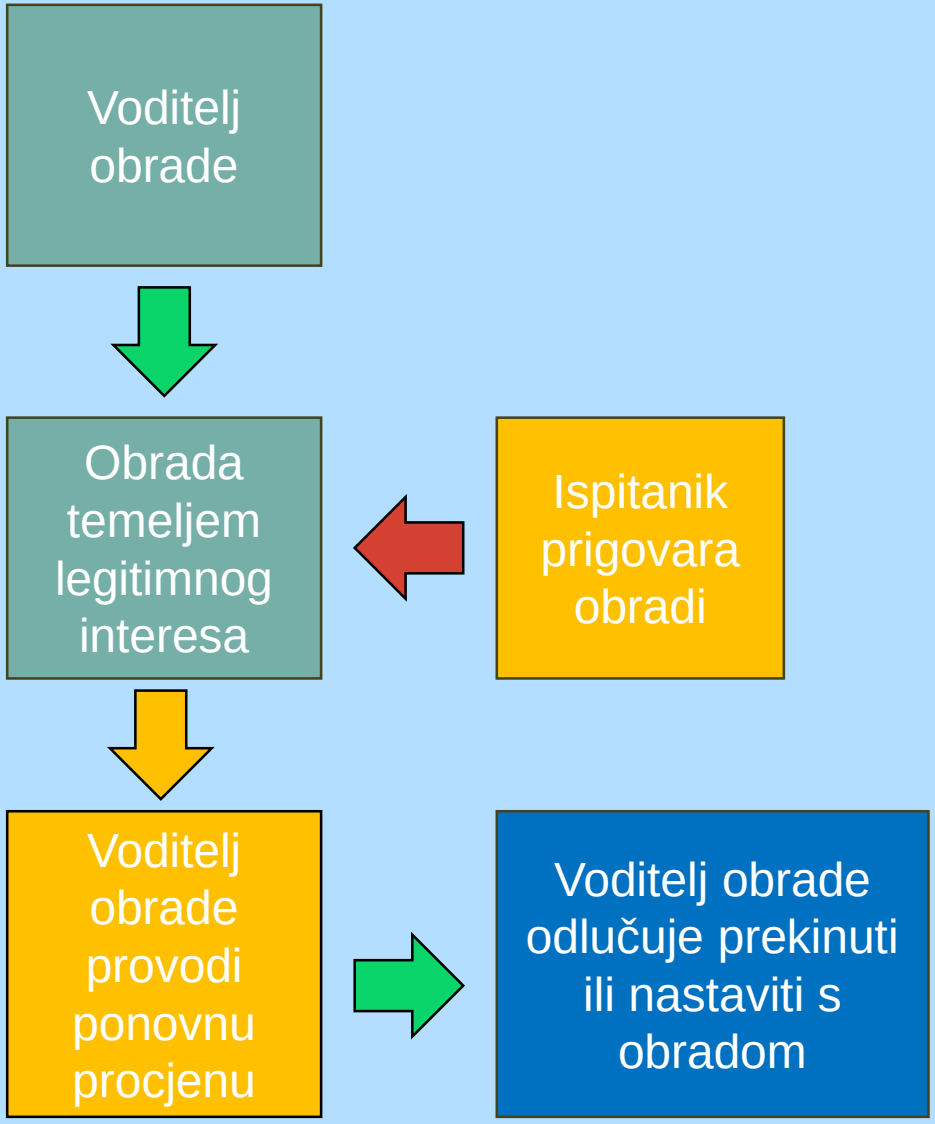


Pravo na ograničenje obrade osobnih podataka

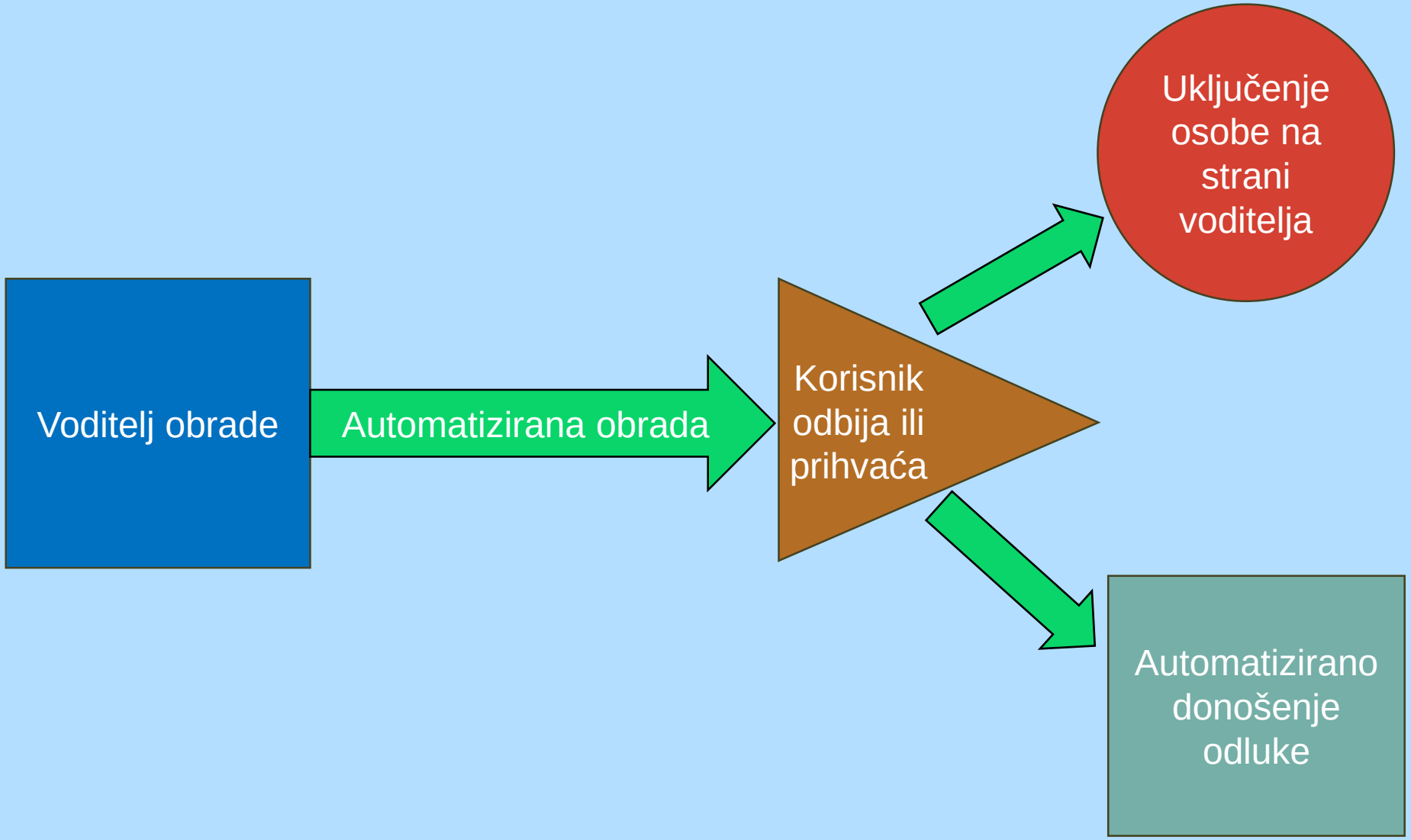
Pravo na prenosivost osobnih podataka



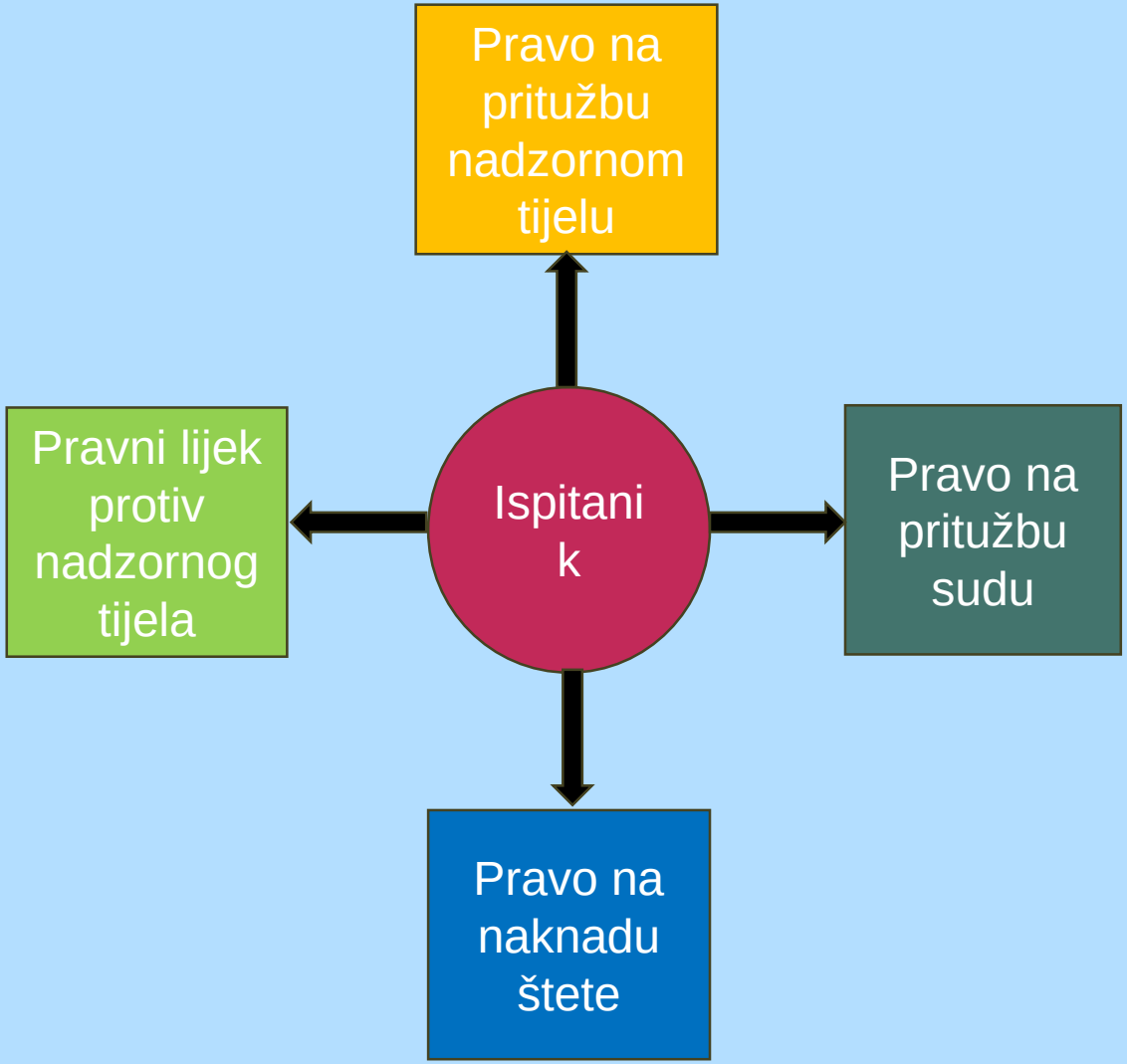
Pravo na prigovor osobnih podataka



Pravo na prigovor automatiziranom pojedinačnom donošenju odluka, uključujući izradu profila



Prava koja ispitanici imaju u pogledu ostvarivanja zaštite osobnih podataka u RH



Standardna operativna procedura (SOP) postupanja prema zahtjevu ispitanika za ostvarivanje prava

- **Što je sve nužno provjeriti?**
  - Tko sve može podnijeti zahtjev za ostvarivanje prava?
  - Koji su nužni elementi zahtjeva iz perspektive podnositelja kao i osobe čiji se podaci traže
  - Kako pronaći i pripremiti podatke
  - Kako dostaviti podatke
- **Što sve treba sadržavati obrazac koji će se ponuditi ispitaniku?**
  - Podaci o podnositelju
  - Podaci o ispitaniku
  - Kontakt podaci

Ograničenja prava

Primjer slučaja (7)

- Janko, dugogodišnji klijent Gorica osiguranja, prije nekoliko mjeseci doživio je manju prometnu nesreću. Iako nitko nije ozlijeđen, Janka su mučile poruke i pozivi iz tvrtke Nesreća d.o.o. koja mu je nudila pomoć u povratu naknade za osobnu ozljedu. Janko je čuo priče o osiguravajućim društvima koja prodaju podatke klijenata trećim stranama i uvjeren je da je Nesreća podatke dobila od Gorica osiguranja. Također, u istom razdoblju Janku se čini da je počeo primati povećanu količinu marketinških informacija od Gorice, s ciljem prodaje cijelog niza njihovih polica osiguranja.
- Janko je počeo pregledavati stranice za usporedbu cijena na internetu i bio je šokiran kada je otkrio da druga osiguravatelja nude mnogo niže cijene za slične usluge od Gorice, iako je on bio vjeran klijent dugi niz godina. Kada njegova polica dođe na red za obnovu, odlučio se prebaciti na Osiguranje Zaprešić. Kako bi aktivirao svoju novu policu osiguranja, dužan je dostaviti informacije o svom bonusu bez potraživanja, svom vozilu i povijesti vožnje.
- Nakon što je istražio svoja prava prema OUZP Janko se javlja Gorici kako bi zamolio da sukladno pravu na prijenos podataka prenesu njegove podatke izravno Zaprešiću. Također koristi ovu priliku kako bi ih zamolio da prestanu koristiti njegove osobne podatke u marketinške svrhe. Gorica isporučuje PDF i XML setove podataka Janku, ali kažu da ne mogu prenijeti njegove podatke izravno u Zaprešić jer to nije tehnički izvedivo. Također iz Gorice dolazi objašnjenje da je Jankov ugovor uključivao odredbu prema kojoj je pristao da se njegovi podaci mogu koristiti u marketinške svrhe i prekasno je da se Janko predomisli o ovome. Janka cijela ta situacija jako naljuti, a kad se prisjeti teksta ugovora, koji je bio pun pravničkog žargona i vrlo zbunjujuć, nije siguran što je od svega navedenog istina. Što biste savjetovali Janku?

Tehničke i organizacijske mjere

- Voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere:
  - pseudonimizaciju i enkripciju osobnih podataka
  - sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade;
  - sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta;
  - proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

Tehnička i organizacijska 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
- Mjere trebaju odgovarati karakteru rizika – iz načela pouzdanosti odnosno odgovornosti proizlazi da konačna odluka o odabiru i primjeni mjera, ali i odgovornost, pada na voditelja obrade

Tehnička i integrirana zaštita podataka – Data Protection by Design and by Default (Čl. 25 GDPR)

- "**Privacy by design and by default**" je koncept koji je uveden Općom uredbom o zaštiti podataka (GDPR) kako bi se osigurala ugrađena i automatska zaštita privatnosti u svim proizvodima i uslugama koje obrađuju osobne podatke
- **Privacy by design…**znači da organizacije moraju ugraditi zaštitu podataka u rane faze razvoja proizvoda, usluga ili sustava, a ne dodati ih retroaktivno.
- **Privacy by default**…znači da su prema zadanim postavkama trebale biti implementirane mjere zaštite osobnih podataka, minimizacija prikupljanja podataka, ograničenje svrhe i povećanje sigurnosti.
- **Čemu služi?**
  - Da bi se osigurala zaštita osobnih podataka korisnika.
  - Da bi se smanjio rizik od curenja podataka i drugih sigurnosnih incidenata.
  - Da promovira transparentnost i povjerenje među korisnicima.

Što je i čemu služi obveza primjene Privacy by Design And By Default?

- **Zašto je bitna?**
  - Potiče organizacije da razmišljaju o zaštiti podataka od samog početka planiranja obrade
  - Pomaže u izgradnji povjerenja između organizacija i njihovih klijenata ili korisnika
  - Može prevenirati visoke novčane kazne koje su povezane s povredom OUZP
- **Kako ju adekvatno primijeniti?**
  - Integriranjem zaštite podataka u ranoj fazi dizajna proizvoda ili usluga.
  - Minimizacijom količine prikupljenih podataka i korištenjem pseudonimizacije gdje je to moguće.
  - Provedbom redovitih procjena rizika i testiranja sigurnosti.
  - Educiranjem i treniranjem zaposlenika o važnosti i principima privacy by design and by default.
- **Tko sudjeluje u njenom provođenju?**
  - Službenik za zaštitu podataka (DPO): Koordinira i nadgleda provedbu pravila.
  - Razvojni tim koji implementira tehničke i organizacijske mjere zaštite podataka u fazi dizajna proizvoda ili usluga.
  - Voditelji projekta ili proizvoda osiguravaju da su pravila zaštite podataka integrirana u planiranje projekta.
  - Uprava organizacije osigurava resurse i potporu za implementaciju i održavanje pravila.
  - Zaposlenici razumijevanjem i pridržavanjem pravila o zaštiti podataka u svakodnevnom radu

Primjeri tehničkih i organizacijskih mjera

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

Kriteriji utvrđivanja mjera prema Uredbi - Data protection by design (Čl. 25. st.1)

- Uzimajući u obzir **najnovija dostignuća**, **trošak provedbe te prirodu**, **opseg, kontekst i svrhe obrade**, kao **i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca** koji proizlaze iz obrade podataka, voditelj obrade, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, provodi odgovarajuće tehničke i organizacijske mjere
- **Elementi:**
  - Najnovija dostignuća
  - Trošak provedbe
  - Priroda obrade
  - Opseg i kontekst obrade
  - Svrha obrade
  - Rizici različitih razina vjerojatnosti i ozbiljnosti

Integrirana zaštita podataka – Data Protection by Default (čl. 25.2)

- "Zadana vrijednost" se odnosi na već postojeću ili unaprijed odabranu vrijednost neke konfigurabilne postavke (setting) koja je dodijeljena softverskoj aplikaciji, računalnom programu ili uređaju, a koja se može odabrati ili prilagoditi.
- 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.
- To mogu biti 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)

Integrirana zaštita osobnih podataka – obveza smanjivanja količine podataka

- U članku 25. stavku 2. OUZP navode se aspekti obveze smanjenja količine podataka za integriranu obradu
- Utvrđuje se da se ta obveza primjenjuje na **količinu prikupljenih osobnih podataka**, **opseg njihove obrade**, **razdoblje njihove pohrane** i **njihovu dostupnost**.
- **Elementi obveze:**
  - Količina prikupljenih osobnih podataka
  - Opseg njihove obrade
  - Razdoblje njihove pohrane
  - Dostupnost podataka

Primjer slučaja (8)

- U kojoj je mjeri voditelj obrade odgovoran za propuste izvršitelja koji dovedu do povrede osobnih podataka? Energetska kompanija iz Poljske odabrala je davatelja informatičkih usluga kao izvršitelja obrade primarno prema kriteriju cijene i učinkovitosti, ali s nedovoljnom pažnjom iz perspektive zaštite povjerljivosti podataka. Odabrani izvršitelj nije proveo odgovarajuće mjere, pa su treće strane neovlašteno pristupile njegovim informacijskim sustavima i iz njih eksfiltrirale (izvukle) osobne podatke preko 130 tisuća kupaca energetske kompanije.
- Prema poljsko nadzorno tijelo provelo je nadzor nad voditeljem i izvršiteljem i ustanovilo da energetska kompanija, unatoč svojoj statutarnoj obvezi prema OUZP nije adekvatno nadzirala postupanje svojeg izvršitelja, osobito odabir i primjenu tehničkih i organizacijskih mjera.
- Među ostalim, nadzorno tijelo ustanovilo je da neprovođenje revizija, uključujući inspekcije, izvršitelja obrade predstavlja povredu članka 25. stavka 1. GDPR-a budući da ova odredba obvezuje voditelje obrade na provođenje odgovarajućih mjera, ne samo pri određivanju metoda obrade, već i tijekom same obrade. Energetska kompanija ni u jednom trenutku nije nadzirala implementaciju novog sustava od strane izvršitelja, a osobito je li potonja primjenjivala općeprihvaćene sigurnosne standarde.
- U kojoj bi mjeri učinkovit nadzor nad izvršiteljem oslobodio voditelja obrade odgovornosti i što bi se tražilo da se dokaže da je takav učinkovit nadzor vođen nad ponašanjem izvršitelja?

Primjeri mjera osiguranja načela obrade kroz integriranu zaštitu podataka - 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.

Ključni tehnički i integrirani elementi zakonitosti mogu biti sljedeći:

- **Relevantnost** – na obradu se primjenjuje pravilna pravna osnova.
- **Diferencijacija** – pravna osnova koja se primjenjuje za svaku aktivnost obrade mora se razlikovati.
- **Određena svrha** – odgovarajuća pravna osnova mora biti jasno povezana s posebnom svrhom obrade
- **Nužnost** – kako bi bila zakonita, obrada mora biti nužna i bezuvjetna.
- **Autonomija** – ispitanicima bi se trebala dodijeliti najviša moguća razina autonomije kad je riječ o nadzoru nad osobnim podatcima u okvirima pravne osnove.
- **Dobivanje privole** – privola mora biti dobrovoljna, posebna, informirana i nedvosmislena28. Posebno bi se trebala razmotriti sposobnost djece i mladih osoba da daju informiranu privolu.
- **Povlačenje privole** – ako je privola pravna osnova, u okviru obrade trebalo bi se olakšati povlačenje privole. Povlačenje privole mora biti jednako lako kao i davanje privole. Ako nije tako, mehanizam za davanje privole voditelja obrade nije u skladu s Općom uredbom o zaštiti podataka
- **Prethodno utvrđivanje** – pravna osnova utvrđuje se prije početka obrade.
- **Prestanak postojanja pravne osnove** – ako pravna osnova prestane važiti, u skladu s time obrada se prekida.
- **Raspodjela odgovornosti** – ako je predviđen zajednički nadzor, strane moraju jasno i transparentno raspodijeliti svoje odgovornosti prema ispitaniku i u skladu s tom raspodjelom osmisliti mjere obrade.

Ključni tehnički i integrirani elementi poštenosti

- **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.**
  - **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

Ključni tehnički i integrirani elementi ograničavanja svrhe

- **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.

Ključni tehnički i integrirani elementi smanjenja količine podataka

- **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.

Ključni tehnički i integrirani elementi točnosti

- **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.

Ključni tehnički i integrirani elementi ograničenja pohrane

- **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.

Ključni tehnički i integrirani elementi cjelovitosti i povjerljivosti

- **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).

Načelo odgovornosti i PBD&D

- **U skladu s načelom pouzdanosti / odgovornosti voditelj obrade odgovoran je za usklađenost sa svim spomenutim načelima i mora dokazati tu usklađenost.**
  - Voditelj obrade treba moći dokazati usklađenost s tim načelima.
  - Pritom može dokazati da su mjere koje je poduzeo kako bi zaštitio prava ispitanika proizvele određene učinke i pokazati zašto se te mjere smatraju odgovarajućima i učinkovitima.
  - Na primjer, može pokazati zašto je određena mjera odgovarajuća za učinkovito osiguravanje provedbe načela ograničenja pohrane.

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.
- **Tehnička i integrirana zaštita podataka dodatni je čimbenik utjecaja na određivanje iznosa novčanih kazni za povrede Opće uredbe o zaštiti podataka tehnička i integrirana zaštita podataka (**vidjeti članak 83. stavak 4.)

Preporuke EDPB 1/2

- 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 sugerira i potiče aktivno sudjelovanje službenika u uključivanju tehničke i integrirane zaštite podataka u postupke nabave i izrade te u cijeli životni ciklus obrade.
- Postupak obrade može se certificirati (bolje rečeno, moći će se).
- 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.

Preporuke EDPB 2/2

- Proizvođači i izvršitelji obrade trebali bi imati aktivnu ulogu u osiguravanju da su ispunjeni kriteriji za „najnovija dostignuća” i trebali bi voditelje obrade obavijestiti o svim promjenama u „najnovijim dostignućima” koje bi mogle utjecati na učinkovitost mjera koje oni provode.
- Europski odbor za zaštitu podataka preporučuje voditeljima obrade da od proizvođača i izvršitelja obrade zahtijevaju da pokažu na koji način njihovi hardver, softver, usluge ili sustavi omogućuju voditelju obrade da ispuni zahtjeve u pogledu odgovornosti u skladu s tehničkom i integriranom zaštitom podataka.
- Voditelji obrade trebali bi biti pošteni prema ispitanicima i transparentno ocjenjivati i dokazivati učinkovitu provedbu tehničke i integrirane zaštite podataka
- Postojeći naslijeđeni (legacy) sustavi obuhvaćeni su istim obvezama u pogledu tehničke i integrirane zaštite podataka kao i novi sustavi.
- Ako naslijeđeni sustavi već nisu usklađeni s obvezama u pogledu tehničke i integrirane zaštite podataka i ne mogu se izvršiti promjene kako bi se ispunile te obveze, naslijeđeni sustavi jednostavno nisu usklađeni s obvezama iz Opće uredbe o zaštiti podataka i ne mogu se upotrebljavati za obradu osobnih podataka.

Primjer slučaja (9)

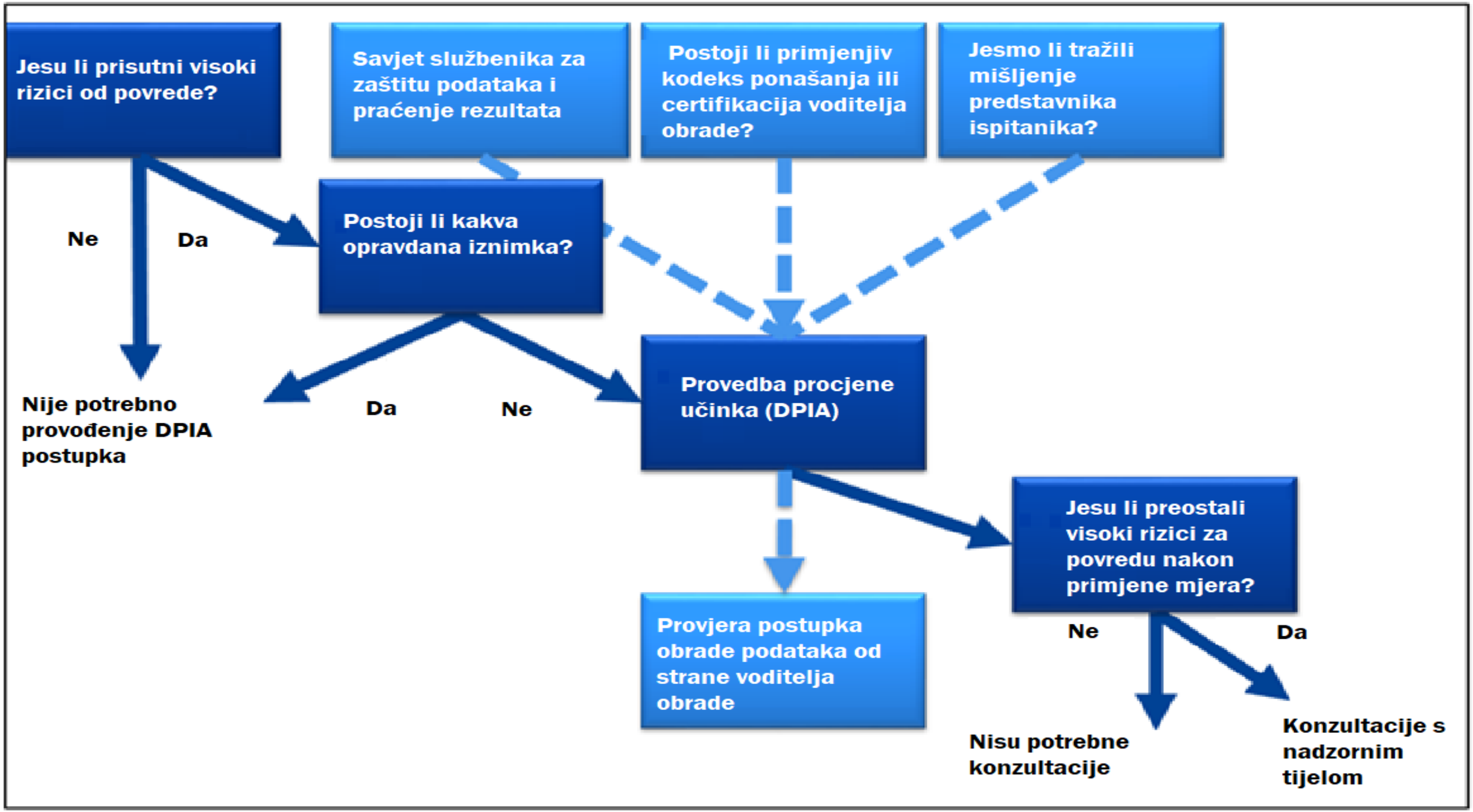
- Voditelj obrade upravlja tražilicom koja uglavnom obrađuje osobne podatke koje generiraju korisnici. Voditelj ima koristi od velike količine osobnih podataka i mogućnosti korištenja tih osobnih podataka za ciljane oglase. Voditelj obrade stoga želi utjecati na subjekte podataka da dopuste opsežnije prikupljanje i korištenje svojih osobnih podataka.
- Privola se prikuplja predstavljanjem mogućnosti obrade subjektu podataka. Prilikom provedbe načela poštenja, uzimajući u obzir prirodu, opseg, kontekst i svrhu obrade, voditelj obrade shvaća da ne može predstaviti opcije na način koji gura ispitanika u smjeru dopuštanja voditelju obrade prikupljanje više osobnih podataka nego ako opcije su predstavljene na ravnopravan i neutralan način.
- To znači da ne mogu predstaviti mogućnosti obrade na takav način koji ispitanicima otežava suzdržavanje od dijeljenja svojih podataka ili otežava prilagodbu svojih postavki privatnosti i ograničavanje obrade. Ovo su primjeri mračnih obrazaca koji su u suprotnosti s duhom članka 25. Zadane opcije za obradu ne smiju biti invazivne, a izbor za daljnju obradu treba biti predstavljen na način koji ne vrši pritisak na nositelja podataka da da privolu. Stoga voditelj obrade daje mogućnosti dva jednako vidljiva izbora, točno predstavljajući grananje svakog izbora ispitaniku.

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

Zašto nam treba procjena učinka?

- Procjena učinka je alat za postizanje i dokazivanje sukladnosti s odredbama Uredbe
  - Čl.24.st.1:” 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 probleme u fazi planiranja kad je to jednostavno 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


Jesu li prisutni visoki rizici od povrede?
Savjet službenika za zaštitu podataka i praćenje rezultata
Postoji li primjenjiv kodeks ponašanja ili certifikacija voditelja obrade?
Jesmo li tražili mišljenje predstavnika ispitanika?
Ne
Da
Postoji li kakva opravdana iznimka?
Nije potrebno provođenje DPIA postupka
Da
Ne
Provedba procjene učinka (DPIA)
Provjera postupka obrade podataka od strane voditelja obrade
Jesu li preostali visoki rizici za povredu nakon primjene mjera?
Ne
Da
Nisu potrebne konzultacije
Konzultacije s nadzornim tijelom

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 kategorijima ispitanika itd.

Treba li provesti procjenu učinka?

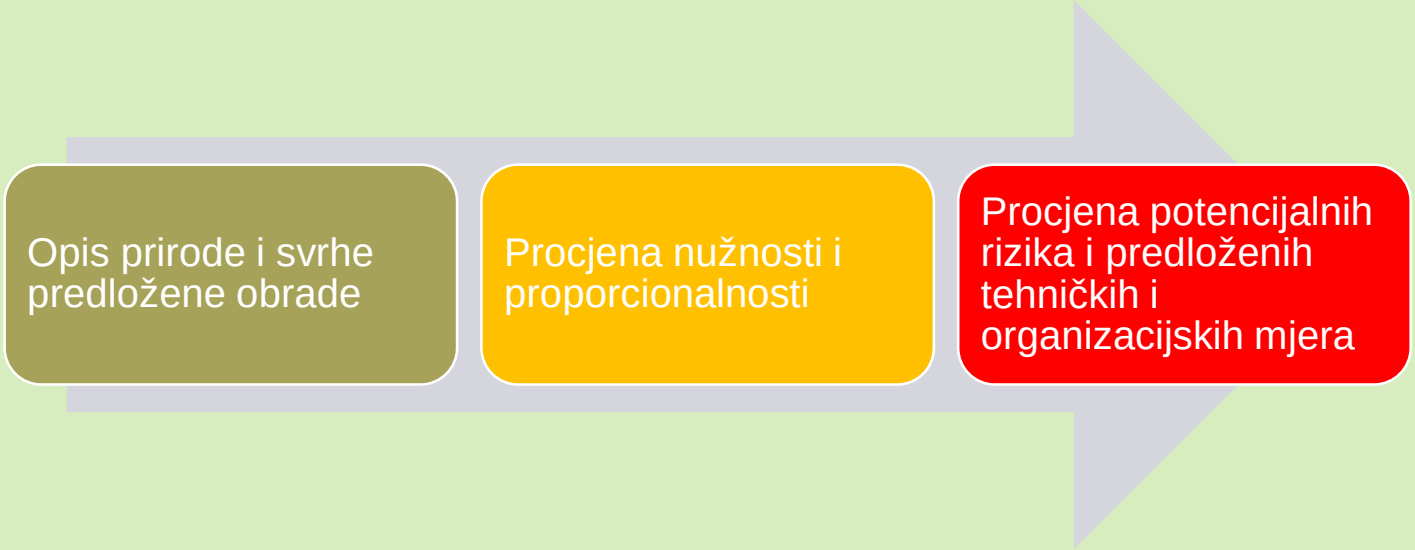
Primjeri obrade	Mogući kriterij	Je li DPIA obvezna?
Bolnički informacijski sustav koji obrađuje zdravstvene podatke	Osjetljivi podaci ili podaci izrazito osobne prirode Veliki opseg podataka	DA
Sustav kamera na autocesti koji prepoznaje pojedinačne automobile i registracije	Sustavno praćenje Inovativne metode	Vjerojatno DA
Sustav nadzora informacijskih sustava zaposlenika uključujući desktop i Internet aktivnost	Sustavno praćenje Podaci koji se odnose na ranjivu skupinu - zaposlenike	DA
Stvaranje baze podataka o potrošačima koji zlorabe pogodnosti za kupce	Evaluacija ili skoring Automatsko donošenje odluka Kombiniranje datasetova	DA
Online časopis koji šalje dnevni izbor vijesti mailom	Velika količina podataka	Vjerojatno NE

Treba li provesti procjenu učinka?

Primjeri obrade	Mogući kriterij	Je li DPIA obvezna?
Obrada podataka preko profila na društvenim mrežama	Kombiniranje više datasetova Evaluacija ili skoring Veliki opseg podataka	DA
Pohrana pseudonimiziranih podataka posebne kategorije u svrhu kliničkih istraživanja	Osjetljivi podaci Ranjivi ispitanici	Vjerojatno DA
Obrada podataka pojedinačnog odvjetnika, liječnika, terapeuta	Osjetljivi podaci Ranjivi ispitanici	NE
Online dućan koji objavljuje oglase temeljem ograničenog profiliranja vlastitih kupaca	Skoring	NE
Banka objavljuje oglase temeljem profiliranja klijenata	Velika količina podataka Osjetljivi podaci, skoring, automatsko donošenje odluka	DA

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

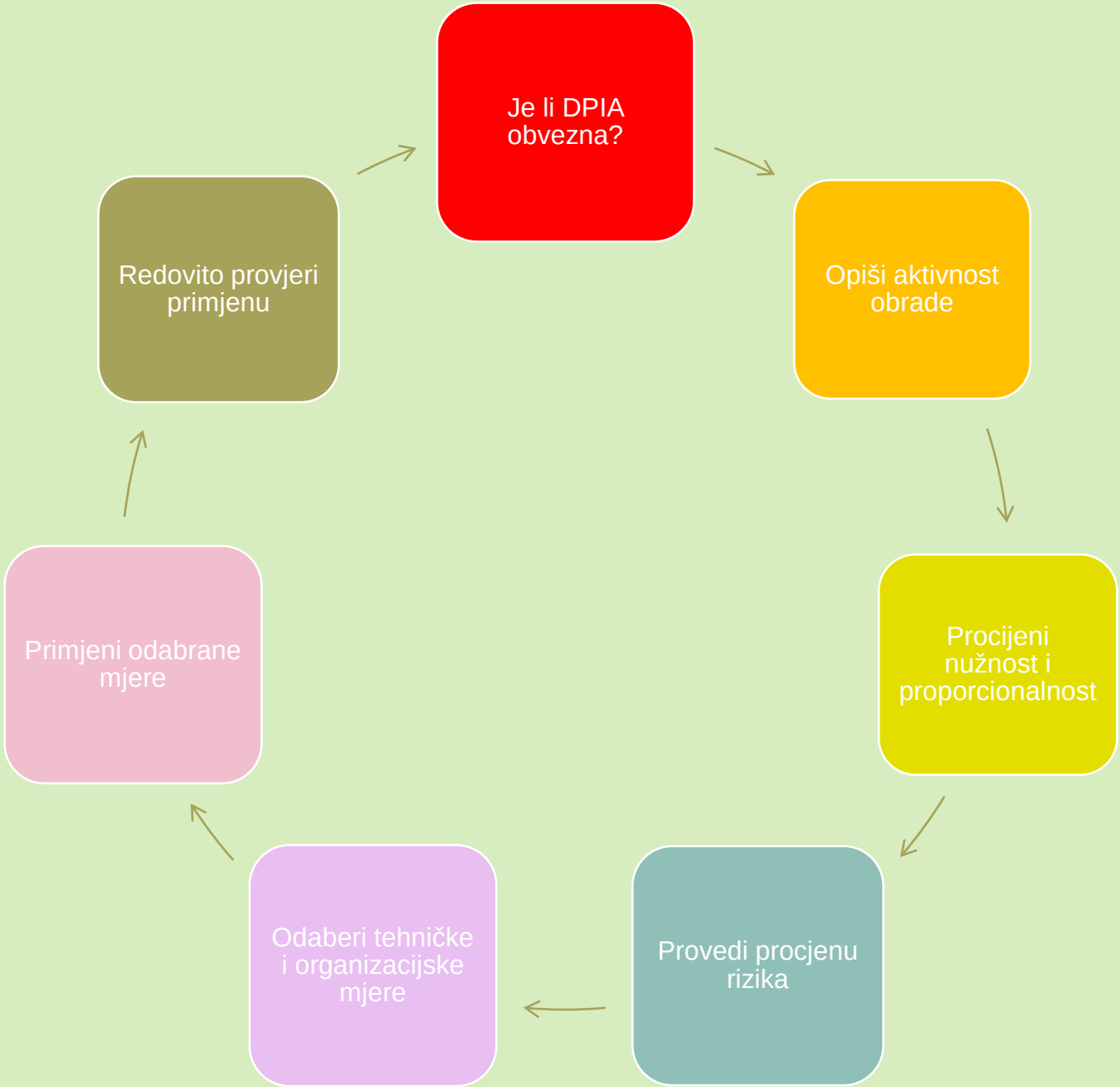


Kako provesti procjenu učinka?

1. Utvrditi potrebu provođenja DPIA
2. Opisati protok podataka u okviru pojedine obrade
   - Otkud podaci dolaze, čemu služe (zašto se prikupljaju), kome se prosljeđuju, tko im može pristupati i slično
3. Identificirati rizike
   - Opasnost neovlaštenog pristupa, šteta od nepotpunih ili pogrešnih podataka, pretjerani ili nepotrebni podaci itd.
4. Predložiti mjere za uklanjanje ili umanjenje prepoznatog rizika
5. Priprema izvještaja o rezultatima procjene i njihova integracija u poslovne aktivnosti

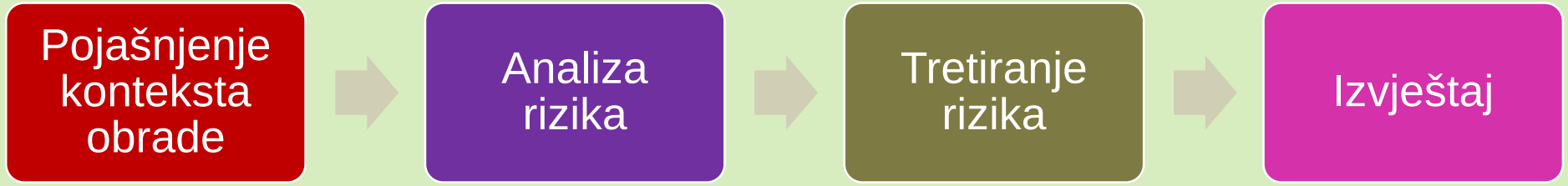
Tko sudjeluje u procjeni učinka?

- Procjenu učinka provodi voditelj obrade
- 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


Je li DPIA obvezna?
Opiši aktivnost obrade
Procijeni nužnost i proporcionalnost
Provedi procjenu rizika
Odaberi tehničke i organizacijske mjere
Primjeni odabrane mjere
Redovito provjeri primjenu

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



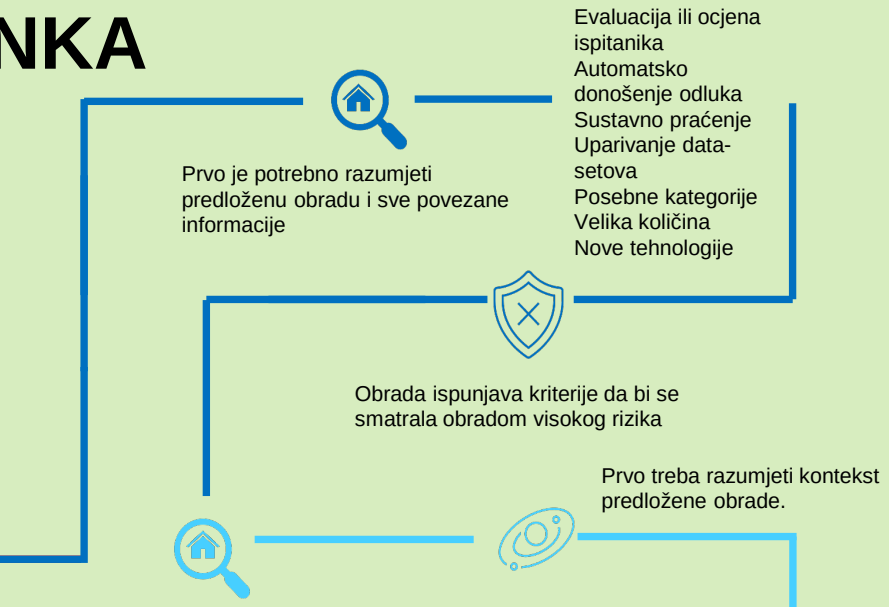
PROCJENA UČINKA

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.

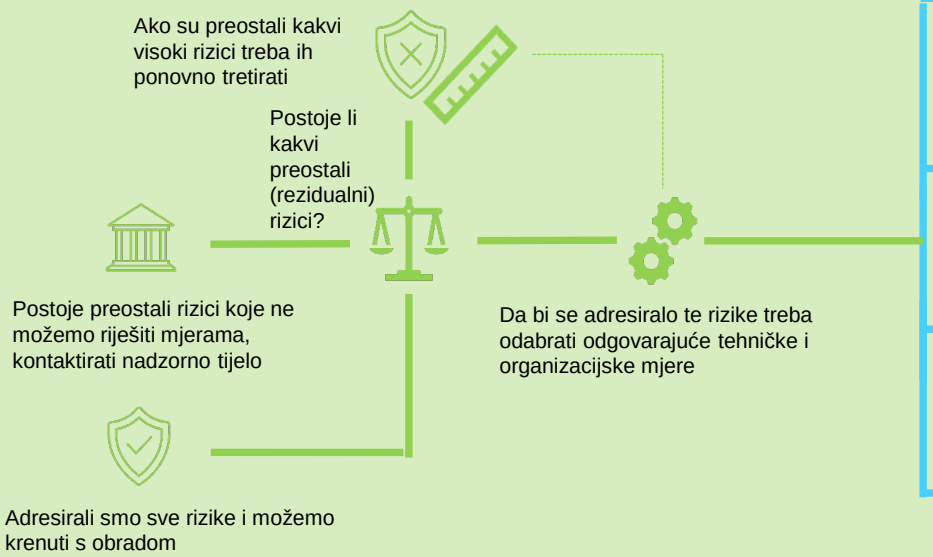


3. Procjena rizika

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.



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.

MTKDOO 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

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 [4] 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

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 potiče razvoj sektorski specifičnih metodologija za određene tipove obrada i setova osobnih podataka
  - Primjerice, u financijskoj industriji, zdravstvu, prometu, turizmu itd.
- Smjernice WP29 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

Koju metodologiju odabrati?

- ISO 31000:2009, ISO 29100:2011
- UK Treasury Orange Book: Management of Risk
- NIST SP 800-39, NIST SP 800-122
- CNIL Privacy Risk Management
- PMBOK, Prince2
- COBIT, ENISA, ISACA

Primjeri metoda procjena učinka u europskoj praksi

- DE: Standard Data Protection Model
- ES: Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española de protección de datos (AGPD)
- FR: Privacy Impact Assessment (PIA), Commission nationale de l’informatique et des libertés (CNIL)
- UK: Conducting privacy impact assessments code of practice, Information Commissioner’s Office (ICO)

Zaključno o DPIA

- DPIA/Procjena učinka je važan mehanizam osiguranja sukladnosti s Uredbom
- 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!

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

- Pregleda razvoja i razlozi nastanka instituta SZOP/DPO
- Kvalifikacije i uloga službenika, službenik kao profesija
- Imenovanje i radno mjesto SZOP
- Modeli uspostavljanja funkcije SZOP
- Obveze, odgovornosti i potrebni resursi
- Kako prepoznati izbjeći sukob interesa
- Kada i zašto grupa poduzetnika može imenovati jednog službenika za zaštitu podataka i pod kojim uvjetima
- Kako održavati i unaprijediti kompetencije SZOP

Uloga službenika za zaštitu podataka

- Još WP29 zauzela stajalište da praksa pokazuje kako DPO može pripomoći odgovornom/pouzdanom ponašanju voditelja, kasnije preuzeto od EDPB
- Službenici:
  - Olakšavaju usklađivanje provodeći mehanizme za osiguranje sukladnosti
    - Procjene učinka na zaštitu podataka
    - Revizija postupaka zaštite podataka
    - Savjetuju kod razvoja i puštanja u rad novih proizvoda i usluga (PBD)
  - Djeluju kao posrednici u odnosu na nadzorna tijela, ispitanike i poslovne jedinice unutar organizacija
  - Savjetuju uprave oko potrebnih resursa za održavanje usklađenosti
  - Ne odgovaraju osobno u slučaju neusklađenosti

Službenik kao profesija/poziv

- Odlikuje ga visoka razina osobnog integriteta, poštenja i visoka razina profesionalne etike
  - Djelovanje u skladu s načelima obrade podataka
  - Instrumentalan u ostvarivanju prava ispitanika
  - Sudjeluje u odabiru i implementaciji adekvatne razine tehničke i integrirane zaštite podataka
  - Pomaže u prepoznavanju obrada i ispunjavanju dokumenata kojima se jamči pouzdanost/odgovornost poput evidencije aktivnosti obrade
  - Izvješćuje i obavještava o povredama podataka

Malo povijesti

- Prvi put uveden u Njemačkoj prije gotovo trideset godina
- Od 2010. uveden u nacionalne zakone Poljske, Švedske, Francuske i RH, u ZZOP uveden izmjenama i dopunama 41/08 i 130/11
- Podsjećao na ZIS – savjetnik za informacijsku sigurnost
- U okviru razvoja GDPR korištena i poredbena iskustva iz industrijske samoregulacije te regulacije financijskih institucija

Službenik nekad... (čl.18.a ZZOP)

- Do 20 zaposlenih – voditelj može imenovati
- Više od 20 zaposlenih – obvezan imenovati
- Kontakt podaci službenika javno dostupni
- Imenovanje u pismenom obliku
- Registar službenika

Službenik nekad... (čl. 18.a ZZOP)

- Samo zaposlenik/član organizacije
- Ne može biti osoba:
  - Protiv koje se vodi postupak zbog povrede službene dužnosti/radne obveze
  - Izrečena mjera povrede etičkog kodeksa i dr.

Opća uredba o zaštiti podataka

- Čl. 37 Imenovanje službenika
- Čl. 38 Radno mjesto
- Čl. 39 Zadaće službenika
- Recital 97
- WP29 Smjernice o službeniku za zaštitu podataka WP243 rev. 01
- ICO DPO Guidance

Imenovanje službenika

- Čl. 37 Imenovanje DPO
  - Obradu provodi tijelo javne vlasti ili javno tijelo
  - Osnovna djelatnost voditelja
    - postupci koji iziskuju redovito i sustavno praćenje
    - opsežna obrada posebnih kategorija ili podataka u vezi s kaznenim osudama (čl. 9 i 10)
- Grupa poduzetnika može imenovati zajedničkog DPO – pod uvjetom da je lako dostupan
- Udruženje i druga tijela mogu imenovati zajedničkog DPO

Tijela javne vlasti u nacionalnom zakonodavstvu

- Termin tijela javne vlasti nalazimo u Zakonu o pravu na pristup informacijama čl.5:
  - »Tijela javne vlasti«, u smislu ovoga Zakona, su tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave, pravne osobe i druga tijela koja imaju javne ovlasti, pravne osobe čiji je osnivač Republika Hrvatska ili jedinica lokalne ili područne (regionalne) samouprave, pravne osobe koje obavljaju javnu službu, pravne osobe koje se temeljem posebnog propisa financiraju pretežito ili u cijelosti iz državnog proračuna ili iz proračuna jedinica lokalne i područne (regionalne) samouprave odnosno iz javnih sredstava (nameta, davanja, i sl.), kao i trgovačka društva u kojima Republika Hrvatska i jedinice lokalne i područne (regionalne) samouprave imaju zasebno ili zajedno većinsko vlasništvo;
- Zakon o provedbi Opće uredbe o zaštiti podataka u čl.3.st.2:
  - „Tijela javne vlasti u smislu ovoga Zakona su: tijela državne uprave i druga državna tijela, jedinice lokalne i područne (regionalne) samouprave.”
  - Definicija u svrhu (ne)izdavanja novčanih upravnih kazni

Osnovna djelatnost

- Recital 97: „ Osnovne djelatnosti voditelja obrade odnose se na njegove primarne djelatnosti i ne odnose se na obradu osobnih podataka kao dodatne djelatnosti”
- Osnovne djelatnosti - ključni postupci nužni za ostvarenje ciljeva voditelja obrade ili izvršitelja obrade
  - Bolnica – obrada zdravstvenih podataka
  - Privatno zaštitarsko poduzeće – videonadzor

Opsežna obrada

- Nije pobliže definirana Uredbom
- Najbliži Recital 91 (o procjeni učinka):
  - Obrada velikog opsega kojom se nastoji obraditi znatna količina osobnih podataka na regionalnoj, nacionalnoj ili nadnacionalnoj razini i...
  - Obrada koja bi mogla utjecati na veliki broj ispitanika i koja će dovesti do visokog rizika
  - Ne odnosi se na liječnike pojedince i druge zdravstvene djelatnike, odvjetnike

Opsežna obrada

- WP 29 preporučuje kriterije poput:
  - Broj predmetnih ispitanika, njihov konkretan broj ili udio u relevantnom stanovništvu
  - Obujam podataka i/ili opseg različitih podatkovnih stavki koje se obrađuju
  - Trajanje aktivnosti obrade podataka
  - Zemljopisni razmjer aktivnosti obrade

Redovito i sustavno praćenje

- Također nije definirano Uredbom
- WP29 „redovito” tumači kao:
  - Praćenje koje je trajno ili se provodi u određenim intervalima u određenom razdoblju
  - Praćenje koje se opetovano provodi ili ponavlja u točno određeno vrijeme
  - Praćenje koje se provodi stalno ili periodično
- WP29 „sustavno” tumači kao:
  - Praćenje koje se provodi u skladu s određenim sustavom
  - Praćenje prethodno dogovoreno, organizirano, metodično
  - Praćenje koje je dio općeg plana za prikupljanje podataka
  - Praćenje koje je dio strategije

Primjeri redovitog i sustavnog praćenja

- Upravljanje telekomunikacijskom mrežom, pružanje telekomunikacijskih usluga
- Praćenje podataka o općem stanju organizma, podataka tjelesnoj kondiciji i zdravlju putem uređaja koji se nose na tijelu
- Izrada profila i ocjena radi procjene rizika
  - Kreditni bonitet
  - Određivanje premije osiguranja
  - Sprečavanje prijevara
  - Otkrivanje pranja novca
- Marketinške aktivnosti temeljene na podacima – programi vjernosti, bihevioralno oglašavanje,
- Pametna brojila, pametni automobili, automatizacija doma

Imenovanje službenika za više organizacija

- Pod uvjetom da”... je lako dostupan iz svakog poslovnog nastana.”
  - Zadaće ispitanika kao točke za kontakt za ispitanike
  - Točka za kontakt s nadzornim tijelom
    - Komunikacija na jeziku predmetnog nadzornog tijela i ispitanika
  - Na raspolaganju organizaciji
    - Informiranje i savjetovanje voditelja/izvršitelja i zaposlenika o njihovim obvezama iz Uredbe
    - Preporuča se da je smješten u EU

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 poslovnog sektora i organizacije voditelja obrade
    - Dobro razumijevanje postupaka, informacijskih sustava voditelja i informacijske sigurnosti
  - Sposobnost izvršavanja zadaća iz članka 39. Uredbe
    - Poštenje, profesionalna etika

Radno mjesto 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

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

Radno mjesto 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

Službenik kao zaposlenik organizacije	Eksternalizirani (out-sourceani) službenik
Bolji uvid u poslovne procese organizacije	Predvidljivo, odabrat će se stručnjak i profesionalac s odgovarajućim iskustvom
Posljedično, bit će efikasniji u postavljanju vlastitog data protection management system (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

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 (CEO, COO, CFO itd)
  - 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

Prevencija sukoba interesa i dokazivanje da ne postoji

- Identificirati pozicije unutar organizacije nespojive s pozicijom službenika
- Pravilnikom o unutarnjem ustrojstvu ili drugim unutarnjim pravilima urediti poziciju službenika
- Prilikom imenovanja službenika pripremiti izjavu kojom odabrani djelatnik, svjestan svojih obveza, deklarira da nije u sukobu interesa
- O specifičnostima pozicije službenika obavijestiti kandidate u okviru natječaja za poziciju ili natječaja za pružanje takve usluge
- Osigurati upoznatost upravljačkih struktura s pravilima o prevenciji sukoba interesa

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
    - Kontaktna točka
    - Prethodno savjetovanje
  - Vodi računa o riziku (!) povezanom s postupcima obrade

Sankcije i odgovornost

- Službenik ne odgovara za povrede osobnih podataka koje počini voditelj obrade
- Uredba ne sadrži posebne odredbe o odgovornosti službenika
  - Uloga službenika je savjetnička
  - Službenik bi potencijalno odgovarao za neizvršavanje i posljedice neizvršavanja svojih zadaća
  - Ovisno o nacionalnom zakonodavstvu, primjenjuju se nacionalne odredbe iz područja kaznenog, upravnog ili trgovačkog prava

Razrješenje dužnosti ili kazna zbog izvršavanja zadaća službenika

- Čl.38.st.3 Uredbe: voditelj/izvršitelj ne smije službenika razriješiti dužnosti ili kazniti zbog izvršavanja zadaća
- Primjerice, službenika se ne može kazniti ili razriješiti dužnosti zašto što je ponudio savjet (npr. da će određena obrada izazvati visok stupanj rizika i da se treba provesti DPIA, a voditelj se ne slaže)
- Kazne mogu biti i neizravne, samo zaprijećene itd. Službenik
- Službenik naravno može biti razriješen zbog razloga koji nisu povezani s njegovim izvršavanjem zadaća (primjerice, krađa, fizičko, psihičko i spolno uznemiravanje, slične grube povrede dužnosti itd.)

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

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

Informacijska sigurnost, procjena rizika, poslovni informacijski sustavi

- 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
- PCI DSS standard sigurnosti kartičarskih transakcija
- Razne metodologije procjene rizika
  - Proučiti DPIA smjernice!

Koju metodologiju odabrati?

- ISO 31000:2009, ISO 29100:2011
- UK Treasury Orange Book: Management of Risk
- NIST SP 800-39, NIST SP 800-122
- CNIL Privacy Risk Management
- PMBOK, Prince2
- COBIT, ENISA, ISACA

Primjeri metoda procjena učinka u europskoj praksi

- DE: Standard Data Protection Model, V.1.0 – Trial version, studeni 2016.
- ES: Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española de protección de datos (AGPD), 2014.
- FR: Privacy Impact Assessment (PIA), Commission nationale de l’informatique et des libertés (CNIL), 2015.
- UK: Conducting privacy impact assessments code of practice, Information Commissioner’s Office (ICO), 2014.

Ponovimo: Uloge i odgovornosti

- **Službenik za zaštitu podataka**
  - savjetuje i educira
  - osigurava 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 unutar organizacije**
  - 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
  - implementiraju tehničke kontrole

Kodeksi, certifikacije i samoregulacija

Kodeksi ponašanja

- Uredba predlaže usvajanje kodeksa ponašanja kako bi se postigla viša razina efikasnosti i ujednačenosti primjene

- Kodeksi ponašanja trebaju reflektirati potrebe sektora gospodarstva i društva, potrebe mikro, malih i srednjih poduzeća itd.

Kodeksi ponašanja

- Svrha kodeksa je jednostavna i efikasna primjena Uredbe i dokazivanje sukladnosti
- Kodekse usvajaju komore, strukovna udruženja i druga tijela koja predstavljaju voditelje ili izvršitelje obrade
- Postupak usvajanja kodeksa treba okupiti sve uključene strane, po potrebi i predstavnike javnosti, potrošača itd.
- O prihvaćanju i mehanizmima praćenja odlučuje nadzorno tijelo u postupku odobravanja kodeksa

Postupak odobrenja kodeksa

- **AZOP**
  - Provjerava sadrži li kodeks ponašanja odgovarajuće mjere zaštite osobnih podataka
  - Provjerava koji su i kakvi kriteriji za odabir i akreditaciju tijela zaduženog za praćenje poštivanja kodeksa
  - Akreditira tijela zadužena za praćenje poštivanja kodeksa
  - Odobrava i objavljuje kodekse ponašanja
  - Vodi evidenciju o odobrenim i objavljenim kodeksima

Što bi kodeks trebao pokrivati?

- **Kodeks pomaže voditeljima obrade da budu sukladni uređujući ponašanje koje ispunjava zahtjeve Uredbe, osobito:**
  - Poštene i transparentne obrade podataka
  - Definicije legitimnog interesa voditelja obrade u konkretnim slučajevima
  - Definira postupke prikupljanja i obrade podataka
  - Postupke pseudonimizacije osobnih podataka i druge tehničke i organizacijske mjere
  - Pružanje podataka o obradi i ostvarivanje drugih podataka ispitanika
  - Propisuje postupke prijave povreda
  - Propisuje modele izvoza podataka izvan EU
  - Naznačuje postupke rješavanja sporova

Kodeksi ponašanja

- Prihvaćanje kodeksa poručuje ispitanicima i partnerima da voditelj obrade razumije i prati obveze prema Uredbi
- Pokazuje razumijevanje prisutnih rizika i prihvaćanje standardiziranih pravila o uspješnom tretiranju rizika
- Čini voditelja odgovornijim i transparentnijim
  - Dobro za reputaciju
  - Postavlja standarde najbolje prakse
  - Ako ih se pridržava, voditelj smanjuje rizike uslijed nadzora i mogućih povreda

Praktične implikacije za voditelja obrade

- Voditelj obrade može odabrati koje će kodekse ponašanja prihvatiti
- Voditelj po prihvaćanju treba tijelu akreditiranom za praćenje dokazati da ispunjava zahtjeve kodeksa
- Voditelj će redovito trebati dokazati da se ponaša u skladu s kodeksom. Tijelo akreditirano za praćenje o nepridržavanju obavještava nadzorno tijelo
- Ispitanici – klijenti i partneri moći će putem nadzornih tijela i EDBP provjeriti je li voditelj obrade prihvatio i primijenio koji (ili koje) kodekse ponašanja
- Prihvaćanje i pravilno usklađivanje smanjuje rizik od kazne za voditelja obrade te olakšava prepoznavanje odgovornih poslovnih partnera

EDPB i kodeksi ponašanja

- Kodeksi ponašanja regulirani su čl. 40-43 Uredbe te recitalima 77, 98, 99 i 168
- EDPB trenutno izrađuje smjernice o kodeksima ponašanja i poziciji i odgvornostima tijela akreditiranih za praćenje sukladnosti s kodeksom

Certifikacija

- Dobrovoljna, pokazuje sukladnost regulatorima, javnosti i poslovnim partnerima
- Certificira se postupanje s osobnim podacima – postupanje koje pokazuje sustavno i plansko ostvarivanje sukladnosti
- Uredba, Europska komisija, EDPB i nadzorna tijela će promicati certifkaciju
- Certifikacijski sustavi će olakšati sukladnost s Uredbom, povećati efikasnost i transparentnost
  - Posebno opet privlačno za mikro, male i srednje organizacije

Tko će biti uključen u certifikaciju

- Na europskoj razini, certifikaciju promiču EK, EDPB te nadzorna tijela
  - Postoji ideja da se uvede Europski pečat zaštite podataka / European Data Protection Seal
  - Trenutno ne postoje GDPR certifikacije (?)
  - EDPB će voditi upisnik svih certifikacija
- Na nacionalnoj razini u certifikaciji sudjeluju
  - Nadzorno tijelo
  - Nacionalno akreditacijsko tijelo
  - Akreditirana certifikacijska tijela
  - Voditelji i izvršitelji obrade koji će tražiti i održavati certifikate

Smisao i ciljevi certifikacije

- Pokazati da se obrada podataka vrši u skladu s Uredbom, osobito načelom odgovornosti
- Pokazuje sukladnost sa zahtjevima tehničke i integrirane zaštite (by design and by default) i adekvatnu primjenu tehničkih i organizacijskih mjera
- Pojednostaviti izvoz podataka u treće zemlje i međunarodne organizacije
- Pokazati da voditelj pristupa zaštiti podataka na sustavan način
  - Nadzornom tijelu
  - Ispitanicima
  - Poslovnim partnerima

Praktične implikacije certifikacije za voditelje i izvršitelje obrade

- Voditelji i izvršitelji mogu zatražiti certifikaciju za svoje poslovne procese, proizvode i usluge
  - Certifikacijska tijela će dati neovisan, vanjski i stručni input u pitanjima zaštite podataka
  - Voditelj treba pružiti puni pristup i sve relevantne podatke kako bi se adekvatno proveo certifikacijski postupak
- Certifikacija će trajati do tri godine i biti podložna povremenoj procjeni od strane neovisnog certifikacijskog tijela
- Certifikacija može bit povučena ukoliko voditelj/izvršitelj ne ispunjava zahtjeve, a certifikacijsko tijelo o tome izvještava nadzorno tijelo
- Ispitanici će certifikaciju moći provjeriti u javnim registrima certifikacijskih tijela i kod nadzornog tijela
- Certifikacija može pomoći s dokazivanjem sukladnosti, ali ne utječe na odgovornost. Može biti faktor za smanjenje kazne, ali nepridržavanje može biti i uzrok nadzora i kazne

EDPB i certifikacija

- Certifikacija je regulirana u Uredbi čl. 42, 43 i 83 te recitalima 81 i 100
- EDPB je ranije ove godine objavio draft smjernica o certifikaciji
- Draft je dostupan na stranicama EDPB
- Također, EDPB trenutno izrađuje smjernice o certifikaciji pri izvozu podataka u treće zemlje

Zakon o provedbi Opće uredbe o zaštiti podataka

(NN 42/2018)

Zakon o provedbi OUZP

- Zbog čega uz Uredbu usvajamo i provedbeni zakon
- Neka pitanja na koja Zakon daje odgovor
- Neka pitanja na koja Zakon ne daje odgovor
- Položaj i ovlasti Agencije
- Kome se na kraju i za što može izreći novčana upravna kazna
- Videonadzor
- Često postavljana pitanja

Predmet zakona

- Provedba Uredbe (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
- ne odnosi na obradu osobnih podataka koju obavljaju nadležna tijela u svrhu:
  - sprečavanja, istrage, otkrivanja ili progona kaznenih djela i izvršavanja kaznenih sankcija
  - zaštite od prijetnja javnoj sigurnosti i područja nacionalne sigurnosti i obrane

Pojmovi

- Pojmovi u smislu provedbenog Zakona imaju jednako značenje kao pojmovi korišteni u Općoj uredbi
- Mnogo konfuzije oko pojma „**tijela javne vlasti**”
  - Preko 40 komentara u javnoj raspravi
  - Specifičan termin za upotrebu u europskoj regulativi
  - Tijela javne vlasti« u smislu zakona su:
    - **tijela državne uprave i druga državna tijela**
      - DA – državne upravne organizacije i agencije
      - NE – javne ustanove?
    - jedinice lokalne i područne (regionalne) samouprave

Nadzorno tijelo?

- I dalje Agencija za zaštitu osobnih podataka
- Neovisno državno tijelo
- Samostalna, neovisna, odgovara za svoj rad Saboru
- Sjedište u Zagrebu
- Nadzorna tijela u Uniji prilično se razlikuju u pogledu ustroja, dostupnih resursa (osobito broja zaposlenih) i intenzitetu regulatornih aktivnosti
- Model Povjerenika vs Model Agencije

Ovlasti Agencije?

- Pozicija i ovlasti uređene čl. 51 do 59. Uredbe, temeljeno na Povelji o temeljnim pravima i razrađeno Uredbom
- objavljuje pojedinačne odluke sukladno člancima 18. i 48. Zakona na mrežnim stranicama Agencije
- pokreće i vodi odgovarajuće postupke protiv odgovornih osoba zbog povrede Opće uredbe o zaštiti podataka i zakona
- obavlja poslove neovisnog nadzornog tijela za praćenje primjene Direktive (EU) 2016/680 osim ako posebnim propisima nije drugačije određeno
- obavlja druge zakonom propisane poslove poput suradnje s tijelima državne uprave i drugim tijelima povodom nacrta prijedloga zakona kojima se uređuju pitanja vezana uz obradu osobnih podataka i davanja stručnih mišljenja

Suradnja s nadzornim tijelima za zaštitu podataka iz drugih država

- Predstavnici gostujućeg nadzornog tijela imaju ovlasti za provođenje zajedničkih operacija, uključujući istrage i zajedničke mjere provedbe
- Sporazumom između Agencije i gostujućeg nadzornog tijela Agencija daje ovlast predstavnicima gostujućeg nadzornog tijela da prate i sudjeluju u provođenju nadzornih aktivnosti sukladno članku 62. OUZP
- Voditelj obrade, izvršitelj obrade i ispitanik te sve druge stranke koje su neposredno uključene u konkretnu radnju prije početka zajedničke operacije trebaju biti upoznate da u operaciji sudjeluju i predstavnici gostujućeg nadzornog tijela.

Posebni slučajevi obrade

- Privola djeteta u odnosu na usluge informacijskog društva
- Obrada genetskih podataka
- Obrada biometrijskih podataka
- Obrada osobnih podataka putem videonadzora
- Obrada osobnih podatak u statističke svrhe

Privola djeteta u odnosu na usluge informacijskog društva

- Kod primjene članka 6. stavka 1. točke (a) OUZP, u vezi s nuđenjem usluga informacijskog društva izravno djetetu, obrada osobnih podataka djeteta zakonita je ako dijete ima najmanje 16 godina.
  - Za dijete mlađe od 16 godina privolu treba dati zakonski zastupnik
  - Voditelji trebaju moći dokazati kome su i kako komunicirali uvjete privole i dokumentirati privolu
- Postupanje suprotno odredbama smatra se povredom članka 8. Opće uredbe o zaštiti podataka i podliježe sankcioniranju sukladno članku 83. Opće Uredbe o zaštiti podataka.

Obrada biometrijskih podataka - tijela javne vlasti

- U tijelima javne vlasti obrada biometrijskih podataka može se provoditi samo ako je određena zakonom i ako je:
  - nužna za zaštitu osoba, imovine, klasificiranih podataka ili poslovnih tajni,
  - ako ne prevladavaju interesi ispitanika koji su u suprotnosti s takvom obradom biometrijskih podataka
  - ukoliko je potrebna za ispunjenje obveza iz međunarodnih ugovora u vezi s identificiranjem pojedinca u prelasku državne granice smatrat će se da je u skladu sa zakonom

Primjer slučaja (10)

- Gradsko poglavarstvo zabrinuto je porastom vandalizma i nasilnog kriminaliteta na ulicama grada. Grad je pokriven video-nadzornom (CCTV) mrežom postavljenom u svrhu nadzora nad prometom na brojnim gradskim prometnicama.
- Grad želi upariti CCTV sustav sa sustavom biometrijskog prepoznavanja temeljenog na strojnom učenju i AI tehnologijama te konačno s evidencijama o prekršajima i kaznenim djelima preko sustava ministarstva unutarnjih poslova, policije i kaznenopravnih tijela. Kad sustav bude u pogonu, moglo bi se u realnom vremenu identificirati i pratiti počinitelje nasilnih kaznenih djela na gradskim prometnicama i javnim prostorima.
- Gradonačelnik pritišće gradske službe da se sustav što prije stavi u pogon obzirom da mu je nedavno ukraden bicikl kojim se vozi na posao s parkirališta ispred gradskog poglavarstva. Drski maskirani razbojnik je pritom gledao u kameru i vikao političke parole konkurentske političke opcije.
- Što bi bilo potrebno učiniti prije stavljanja takvog sustava u funkciju – je li uopće zakonito i dopušteno upogoniti takav sustav na području EU?

Obrada biometrijskih podataka u privatnom sektoru

- Obrada biometrijskih podataka u privatnom sektoru može se provoditi samo ako je propisana zakonom ili ako je nužna za zaštitu osoba, imovine, klasificiranih podataka, poslovnih tajni ili za pojedinačno i sigurno identificiranje korisnika usluga, uzimajući u obzir da ne prevladavaju interesi ispitanika koji su u suprotnosti s takvom obradom.
- Pravni temelj za obradu biometrijskih podataka ispitanika radi sigurnog identificiranja korisnika usluga **izričita je privola** takvog ispitanika dana u skladu s odredbama Opće uredbe o zaštiti podataka.

Biometrija u svrhu evidentiranja radnog vremena i prisutnosti

- Dopuštena je obrada biometrijskih podataka zaposlenika u svrhu evidentiranja radnog vremena i radi ulaska i izlaska iz službenih prostorija:
  - ako je propisano zakonom ili
  - ako se takva obrada provodi kao alternativa drugom rješenju za evidentiranje radnog vremena ili ulaska i izlaska iz službenih prostorija,
  - uz uvjet da je zaposlenik dao izričitu privolu za takvu obradu biometrijskih podataka u skladu s odredbama Opće uredbe o zaštiti podataka

Primjena odredaba o biometriji

- Odredbe ovoga Zakona o obradi biometrijskih podataka primjenjuju se na ispitanike u Republici Hrvatskoj ako obradu provodi:
  - voditelj obrade s poslovnim nastanom u Republici Hrvatskoj ili koji pruža usluge u Republici Hrvatskoj
  - tijelo javne vlasti.
- Odredbe Zakona o obradi biometrijskih podataka ne utječu na obvezu provođenja procjene učinka sukladno članku 35. OUZP
- Odredbe Zakona o obradi biometrijskih podataka ne primjenjuju se na područje obrane, nacionalne sigurnosti i sigurnosno-obavještajnog sustava.

Obrada podataka putem videonadzora

- Videonadzorom se smatra:
  - prikupljanje i daljnja obrada osobnih podataka koja obuhvaća stvaranje snimke koja čini ili je namijenjena da čini dio sustava pohrane.
  - Ne i nadzorne kamere bez sustava pohrane
- Obrada osobnih podataka putem videonadzora može se provoditi samo u svrhu koja je nužna i opravdana za zaštitu osoba i imovine, ako ne prevladavaju interesi ispitanika koji su u suprotnosti s obradom podataka putem videonadzora.
- Videonadzorom mogu biti obuhvaćene prostorije, dijelovi prostorija, vanjska površina objekta, kao i unutarnji prostor u sredstvima javnog prometa, a čiji je nadzor nužan radi postizanja svrhe zaštite osoba i imovine.

Obveze voditelja/izvršitelja obrade videonadzora

- Pravo pristupa osobnim podacima prikupljenim putem videonadzora ima odgovorna osoba voditelja obrade odnosno izvršitelja obrade i/ili osoba koju on ovlasti.
  - Ovlaštene osobe ne smiju koristiti snimke iz sustava videonadzora u svrhe različite od onih zaštite osoba i imovine
  - Sustav videonadzora treba biti zaštićen od neovlaštenog pristupa

Obveze voditelja/izvršitelja obrade videonadzora

- Voditelj obrade i izvršitelj obrade dužni su uspostaviti automatizirani sustav zapisa za evidentiranje pristupa snimkama videonadzora koji će sadržavati:
  - vrijeme i mjesto pristupa,
  - oznaku osoba koje su izvršile pristup podacima prikupljenim putem videonadzora.
- Pristup podacima iz sustava videonadzora imaju nadležna državna tijela u okviru obavljanja poslova iz svojeg zakonom utvrđenog djelokruga.
- Snimke dobivene putem videonadzora mogu se čuvati najviše šest mjeseci, osim ako je drugim zakonom propisan duži rok čuvanja ili ako su dokaz u sudskom, upravnom, arbitražnom postupku

Videonadzor radnih prostorija

- Obrada osobnih podataka zaposlenika putem sustava videonadzora može se provoditi samo ako su uz uvjete utvrđene Zakonom:
  - ispunjeni i uvjeti utvrđeni propisima kojima se regulira zaštita na radu i
  - ako su zaposlenici bili na primjeren način unaprijed obaviješteni o takvoj mjeri te
  - ako je poslodavac informirao zaposlenike prije donošenja odluke o postavljanju sustava videonadzora.
- Videonadzor radnih prostorija ne smije obuhvaćati prostorije za odmor, osobnu higijenu i presvlačenje.

Videonadzor stambenih zgrada

- Za uspostavu videonadzora u stambenim odnosno poslovno-stambenim zgradama potrebna je suglasnost suvlasnika koji čine najmanje 2/3 suvlasničkih dijelova.
- Videonadzorom može se obuhvatiti samo:
  - pristup ulascima i izlascima iz stambenih zgrada te
  - zajedničke prostorije u stambenim zgradama.
- Zabranjeno je korištenje videonadzora za praćenje radne učinkovitosti domara, spremačica i drugih osoba koje rade u stambenoj zgradi.

Videonadzor javnih površina

- Praćenje javnih površina putem videonadzora dozvoljeno je samo:
  - tijelima javne vlasti,
  - pravnim osobama s javnim ovlastima i pravnim osobama koje obavljaju javnu službu,
  - samo ako je propisano zakonom,
  - ako je nužno za izvršenje poslova i zadaća tijela javne vlasti ili radi zaštite života i zdravlja ljudi te imovine.
- Odredbe Zakona ne isključuju primjenu članka 35. OUZP na sustavno praćenje javno dostupnog područja u velikoj mjeri.

Postupak u nadležnosti AZOP

- Svatko tko smatra da mu je povrijeđeno neko pravo zajamčeno ovim Zakonom i Općom uredbom o zaštiti podataka, može Agenciji podnijeti **zahtjev za utvrđivanje povrede prava**.
- O povredi prava Agencija odlučuje **rješenjem**, rješenje Agencije je **upravni akt**.
- Protiv rješenja Agencije **žalba nije dopuštena**, ali se tužbom može pokrenuti **upravni spor** pred nadležnim upravnim sudom

Odgoda provedbe brisanja podataka

- Ako je rješenjem naloženo brisanje ili drugo nepovratno uklanjanje osobnih podataka, nezadovoljna stranka može zatražiti od nadležnog upravnog suda odgodu izvršenja brisanja ili drugog nepovratnog uklanjanja osobnih podataka
  - Pod uvjetom da dokaže da bi nerazmjernim naporima ponovno prikupila osobne podatke čije se brisanje odnosno nepovratno uklanjanje traži.
- Ako nadležni upravni sud prihvati takav zahtjev stranka kojoj je naloženo brisanje ili drugo nepovratno uklanjanje osobnih podataka dužna je blokirati svaku obradu spornih osobnih podataka, osim njihova čuvanja, do donošenja pravomoćne sudske odluke.

Provedba nadzora

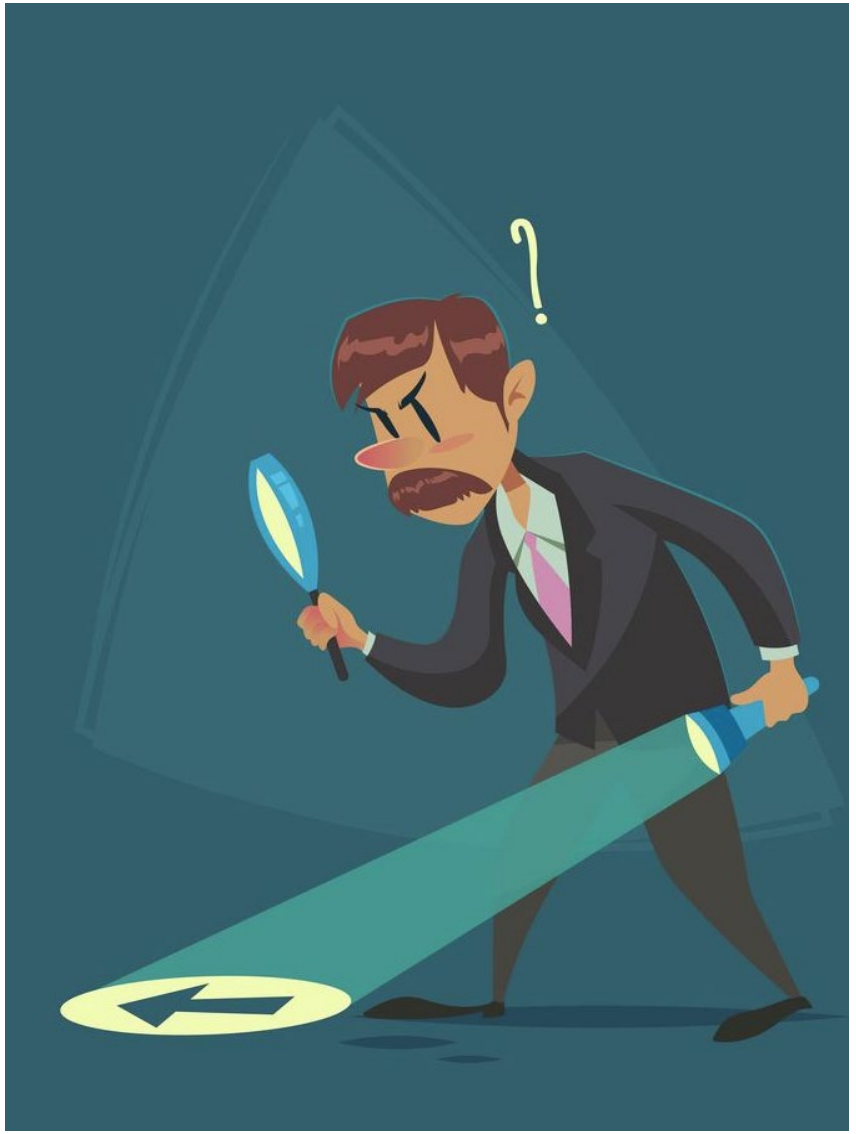
- Ovlašteni službenici Agencije samostalno, a u određenim slučajevima i uz sudjelovanje predstavnika gostujućeg nadzornog tijela (ovlaštene osobe), mogu provesti najavljeni ili nenajavljeni nadzor.
- O provedbi nenajavljenog nadzora nadzirana osoba odnosno voditelj obrade ili izvršitelj obrade bit će obaviješteni na mjestu i u trenutku provedbe nadzora.
- Prije početka obavljanja nadzora ovlaštene osobe dužne su predstaviti se predočenjem službene iskaznice i naloga za nadzor.
- Nalog za provedbu nadzora izdaje ravnatelj Agencije.

Preslike, pečaćenje i privremeno uzimanje sustava pohrane i opreme

- Ovlaštene osobe, prema potrebi, mogu napraviti preslike dostupnih dokumenata, presnimiti sve sadržaje sustava pohrane i prikupiti druge relevantne informacije.
- Ako iz tehničkih razloga nije moguće tijekom nadzora napraviti preslike potrebne dokumentacije, ovlaštene osobe će, prema potrebi, oduzeti potrebne sustave pohrane i opremu koja sadržava druge relevantne informacije i zadržati je koliko je potrebno za izradu preslika te dokumentacije, a najduže do 15 dana od dana oduzimanja sustava pohrane i opreme.
- Ovlaštene osobe mogu zapečatiti sustave pohrane ili opremu za vrijeme nadzora i u opsegu prijeko potrebnom za provedbu nadzornih aktivnosti ako postoji opasnost od uništenja ili izmjena dokaza, a najduže 15 dana od dana pečaćenja sustava pohrane ili opreme.

Provedba nadzora

- **O provedenom nadzoru sastavlja se zapisnik**.
- Zapisnik sadrži osobito:
  - mjesto i datum provedbe nadzora
  - naznaku je li nadzor bio najavljen ili nenajavljen
  - osobna imena i potpise ovlaštenih osoba koje su sudjelovale u nadzoru i predstavnika nadzirane osobe
  - opis tijeka i sadržaja svake provedene radnje tijekom nadzora i danih izjava
  - popis dokumenata i ostalih predmeta korištenih, kopiranih, zapečaćenih i/ili privremeno oduzetih tijekom nadzorne aktivnosti
  - pouku o pravu na ulaganje primjedbi na zapisnik



Naknada za postupanje po zahtjevu

- Obavljanje zadaća Agencije provodi se bez naplate u odnosu na ispitanike, službenike za zaštitu osobnih podataka, novinare i tijela javne vlasti.
- Agencija će naplatiti razumnu naknadu na temelju administrativnih troškova ili odbiti postupiti po zahtjevu ako su zahtjevi ispitanika očito neutemeljeni ili pretjerani, a osobito zbog njihove učestalosti.

Davanje stručnih mišljenja

- Na pisani zahtjev fizičke ili pravne osobe Agencija daje stručno mišljenje iz područja zaštite osobnih podataka, najkasnije u roku od 30 dana od dana podnošenja zahtjeva, ovisno o složenosti zahtjeva.
- Ako je pri davanju stručnog mišljenja potrebno uključiti i druga tijela u tuzemstvu ili u inozemstvu u svrhu dobivanja podataka ili informacija bitnih za stručno mišljenje, rok za davanje mišljenja može se produžiti za još 30 dana.

Davanje stručnih mišljenja

- Agencija će naplatiti naknadu za davanje mišljenja poslovnim subjektima (odvjetničkim društvima, konzultantima i dr.) koja su poslovni subjekti zatražili u svrhu obavljanja svoje redovite djelatnosti odnosno pružanja usluga.
  - Uključuje i pojedinačne odvjetnike, javne bilježnike.
- Kriterije za određivanje visine naknade utvrđuje Agencija. Kriteriji se objavljuju u »Narodnim novinama« te na mrežnim stranicama Agencije.
- Iznos naknade se uplaćuje u korist državnog proračuna.

Izricanje upravne novčane kazne

- Agencija izriče upravne novčane kazne za povrede odredaba zakona i Opće uredbe o zaštiti podataka, sukladno članku 83. Opće uredbe o zaštiti podataka.
  - Ako se upravna novčana kazna izriče protiv pravne osobe s javnim ovlastima ili protiv pravne osobe koja obavlja javnu službu, izrečena upravna novčana kazna ne smije ugroziti obavljanje takve javne ovlasti ili javne službe.
  - Izriču se odlukom koja utvrđuje iznos i način uplate, može i u obrocima
  - Protiv odluke nije dopuštena žalba, ali se može pokrenuti spor pred nadležnim upravnim sudom

Primjer slučaja (11)

- Banka sa sjedištem u Zagrebu zaprimila je nekoliko tisuća zahtjeva za pristupom podacima od strane ispitanika. Zahtjevi su bili motivirani sudjelovanjem ispitanika u drugom pravnom postupku protiv banke, za što su im trebali podaci koje banka posjeduje.
- Banka je višekratno odbila postupiti po zahtjevima ispitanika, smatrajući da ispitanici već imaju tražene podatke, a onda i navodeći troškove i kompleksnost zahtjeva kao razlog zašto ispitanici nisu dobili svoje podatke.
- Na zahtjev ispitanika nadzorno tijelo je provelo nadzor i naredilo banci dostavu podataka ispitanicima, no banka i dalje nije željela dati tražene podatke očito smatrajući da na taj način pomaže suprotnoj strani u postupku protiv sebe.
- Nadzorno tijelo je odredilo kaznu iznosa koji nije službeno objavljen. Iako se slučaj dogodio još 2020., podaci o okolnostima slučaja i dalje nisu službeno poznati javnosti. Razlozi za to su:

Isključenje primjene upravnih novčanih kazni na tijela javne vlasti

- U postupcima koji se provode protiv tijela javne vlasti, tijelu javne vlasti ne može se izreći upravna novčana kazna za povrede Zakona ili Opće uredbe o zaštiti podataka.
- Zakon definira tijela javne vlasti kao:
  - **tijela državne uprave**
  - **druga državna tijela**
  - **tijela lokalne i regionalne samouprave**

Upravne novčane kazne propisane Zakonom

- Upravnom novčanom kaznom u iznosu do 50.000,00 kuna kaznit će se:
  - voditelj obrade i izvršitelj obrade koji ne označe objekt, prostorije, dijelove prostorije te vanjsku površinu objekta na način propisan člankom 27. Zakona
  - voditelj obrade i izvršitelj obrade koji ne uspostave automatizirani sustav zapisa za evidentiranje pristupa snimkama videonadzora, sukladno članku 28. stavku 4. Zakona
  - osobe iz članka 28. stavka 1. Zakona koje snimke iz sustava videonadzora koriste suprotno članku 28. stavku 2. Zakona

Zastara izvršenja upravne novčane kazne

- Na zastaru prava na naplatu upravne novčane kazne primjenjuju se odredbe općeg zakona kojim se propisuje porezni postupak.
- Zastara počinje teći od dana pravomoćnosti odluke.
- Za vrijeme trajanja obročne otplate upravne novčane kazne zastara ne teče.

Prekršajne odredbe

- Novčanom kaznom za prekršaj u iznosu od 5000,00 do 50.000,00 kuna kaznit će se:
  - osoba koja obnaša dužnost ravnatelja i zamjenika ravnatelja Agencije ako neovlaštenoj osobi otkrije povjerljive podatke koje je saznala u obavljanju svoje dužnosti
  - službenik Agencije koji neovlaštenoj osobi otkrije povjerljive podatke koje je saznao u obavljanju poslova radnog mjesta
- Ovlašteni tužitelj za prekršaj je državni odvjetnik.

ODABRANA REGULATORNA I SUDSKA PRAKSA

- OUZP (GDPR) je **slojevita**, **opća** norma sa snagom **iznad nacionalnih zakona**
- Njena priroda opće norme podrazumijeva potrebu interpretacije i primjene na konkretne situacije u praksi
- Još od vremena Direktive o zaštiti podataka (1995) predviđen je institucionalan okvir za tumačenje (WP29). Direktive je svaka država članica samostalno transponirala u nacionalne propise (Zakon o zaštiti osobnih podataka, AZOP) = velike razlike u shvaćanju i primjeni.
- Uredbu se primjenjuje na jednak način. Zbog toga su potrebni mehanizmi kohezije – u prvom redu European Data Protection Board, među čije ovlasti se ubraja i usvajanje obvezujućih i neobvezujućih mišljenja i smjernica o primjeni OUZP
- Slična tijela predviđena su i drugim srodnim propisima (Cybersecurity Act, Digital Services Act, AI Regulation Act, Digital Governance Act)

Europski odbor za zaštitu podataka

- Tijelo Unije s pravnom osobnošću
- Čine ga voditelji nadzornog tijela te novi EU nadzornik za zaštitu osobnih podataka
- Neovisan, ne smije tražiti upute
- Izdaje smjernice, preporuke i primjere najbolje prakse
- Godišnje izvješće EP, EK i Vijeću

Opinions

We adopt **opinions in the context of legislative consultations** requested by the European Commission (**EDPB opinions under Art. 70 GDPR** or **EDPB/EDPS joint opinions** under Art. 42 of Regulation 2018/1725).

We also adopt **consistency opinions** addressed to national Supervisory Authorities (Art.64 GDPR). The national Supervisory Authorities can request EDPB opinions on any matter of general application of the GDPR, or any issue producing effects in more than one Member State. Where a national Supervisory Authority intends to adopt a measure on legal issues having cross-border effects, they must request an EDPB opinion on their draft decision (please see the full list of these measures under Art. 64(1) GDPR, e.g. codes of conduct, standard contractual clauses, ...).

Following our consistency opinions, the national Supervisory Authorities adopt their national decisions. Do not hesitate to visit our **Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism**

Opinion 14/2023 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Vestas Wind Systems Group
27 July 2023
Opinion of the Board (Art. 64) | Binding Corporate Rules | International Transfers of Data | Denmark
Download

Opinion 13/2023 on the draft decision of the competent supervisory authority of Croatia regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)
11 July 2023
Opinion of the Board (Art. 64) | Accreditation | Croatia
Download

Opinion 12/2023 on the draft decision of the competent supervisory authority of Cyprus regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)
11 July 2023
Opinion of the Board (Art. 64) | Accreditation | Cyprus
Download

Opinion 11/2023 on the draft decision of the competent supervisory authority of Sweden regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR
11 July 2023
Opinion of the Board (Art. 64) | Accreditation | Sweden
Download

Opinion 10/2023 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the PROSEGUR Group
30 June 2023
Opinion of the Board (Art. 64) | Binding Corporate Rules | International Transfers of Data | Spain
Download

Filters

Opinion types

- [ ] Opinion of the Board (Art. 64) (154)
- [ ] EDPB/EDPS Joint Opinion (10)
- [ ] Opinion (Art. 70) (7)
- [ ] Opinion (LED Directive (EU) 2016/680) (1)

Topics

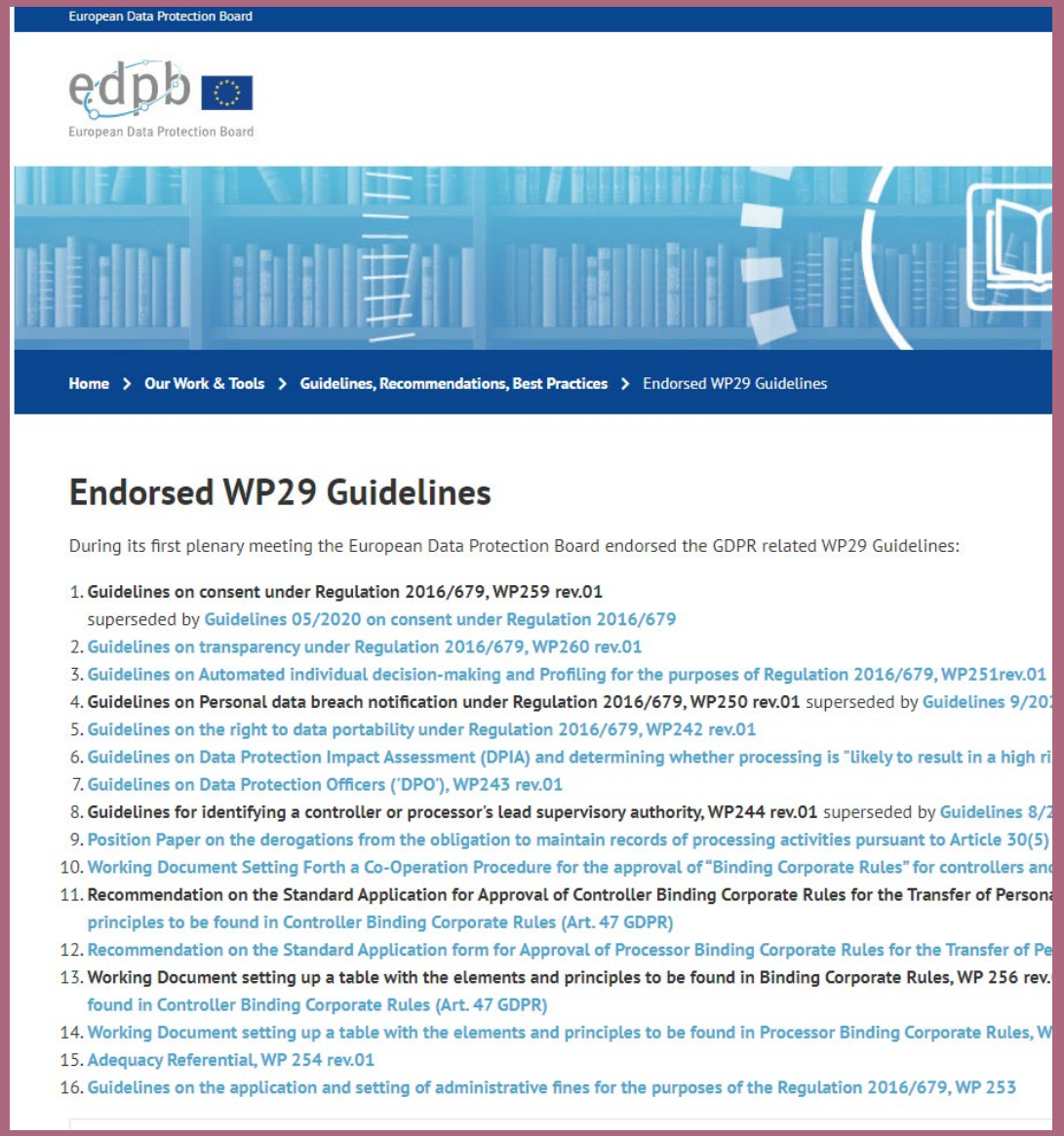
- [ ] International Transfers of Data (61)
- [ ] Binding Corporate Rules (58)
- [ ] Data Protection Impact Assessment (DPIA) (35)
- [ ] Accreditation (25)
- [ ] Code of conduct (25)
- [ ] EU Legislative proposal and strategy (11)
- [ ] Adequacy decision (5)
- [ ] Controller (5)
- [ ] Health (5)
- [ ] Standard contractual clauses (5)
- [ ] New Technology (4)
- [ ] Processor (4)
- [ ] Certification (3)
- [ ] Administrative arrangement (2)
- [ ] Law enforcement (2)
- [ ] Artificial intelligence (1)
- [ ] Children (1)
- [ ] Cooperation between authorities (1)
- [ ] Data subject rights (1)
- [ ] e-Evidence (1)
- [ ] e-Privacy (1)

Show less

Member states

MIŠLJENJA I SMJERNICE EDPB

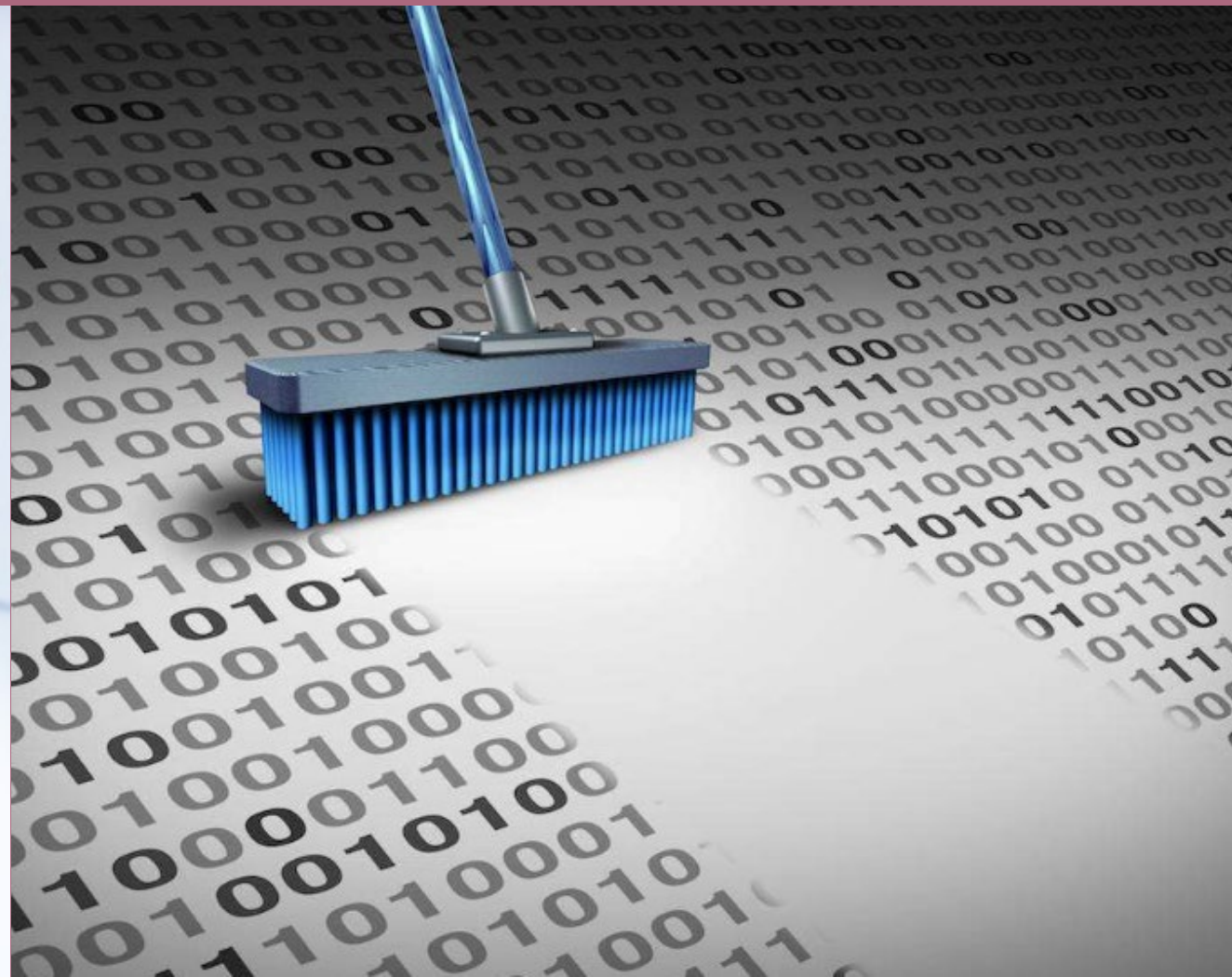
- Iako u ovlasti i obveze nadzornih tijela poput AZOP ulazi i davanje mišljenja i uputa, resursi nadzornih tijela često su napregnuti do razine da se na takve upute čeka jako dugo
- EDPB redovito objavljuje mišljenja i smjernice oko praktične primjene, kako sektorski, tako i u pogledu temeljnih instituta i pojmova iz Uredbe
- SZOP trebaju aktivno pratiti, sukladno polju aktivnosti svojeg voditelja obrade, mišljenja, smjernice i praksu koja može biti značajna za njihove aktivnosti
- Osim specifičnih smjernica važnih za konkretni sektor poput smjernica o zaštiti podataka u autonomnim vozilima, cloud uslugama, umjetnoj inteligenciji itd., treba istaknuti i važnost smjernica koje razrađuju temeljne koncepte poput načela zaštite podataka, prava ispitanika ili praktične primjene instituta poput procjene učinka na zaštitu podataka, standardnih ugovornih klauzula itd.
- https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en



Praksa Europskog suda (EU Court of Justice)

- Europski sud (ECJ) donio je niz presuda koje su oblikovale i definirale pravni okvir zaštite osobnih podataka u Europi, uključujući pravne interpretacije ključnih pojmova iz Opće uredbe o zaštiti podataka. Evo nekih:
  - Google Spain SL, Google Inc. protiv Agencia Española de Protección de Datos (AEPD), Mario Costeja González (C-131/12, 2014):
  - Maximillian Schrems protiv Data Protection Commissioner (C-362/14, 2015):
  - Tele2 Sverige AB protiv Post- och telestyrelsen (C-203/15, 2016)
  - Data Protection Commissioner protiv Facebook Ireland Limited, Maximillian Schrems (C-311/18, 2020)
  - Fashion ID GmbH & Co. KG protiv Verbraucherzentrale NRW eV (C-40/17, 2019):
  - Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV protiv Planet49 GmbH (C-673/17, 2019)
  - Breyer protiv Bundesrepublik Deutschland (C-582/14, 2016)
  - Wirtschaftsakademie Schleswig-Holstein GmbH protiv Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (C-210/16, 2018)

Google Spain SL, Google Inc. protiv Agencia Española de Protección de Datos (AEPD), Mario Costeja González (C-131/12, 2014



Tele2 Sverige AB vs Post- och telestyrelsen (C-203/15, 2016)

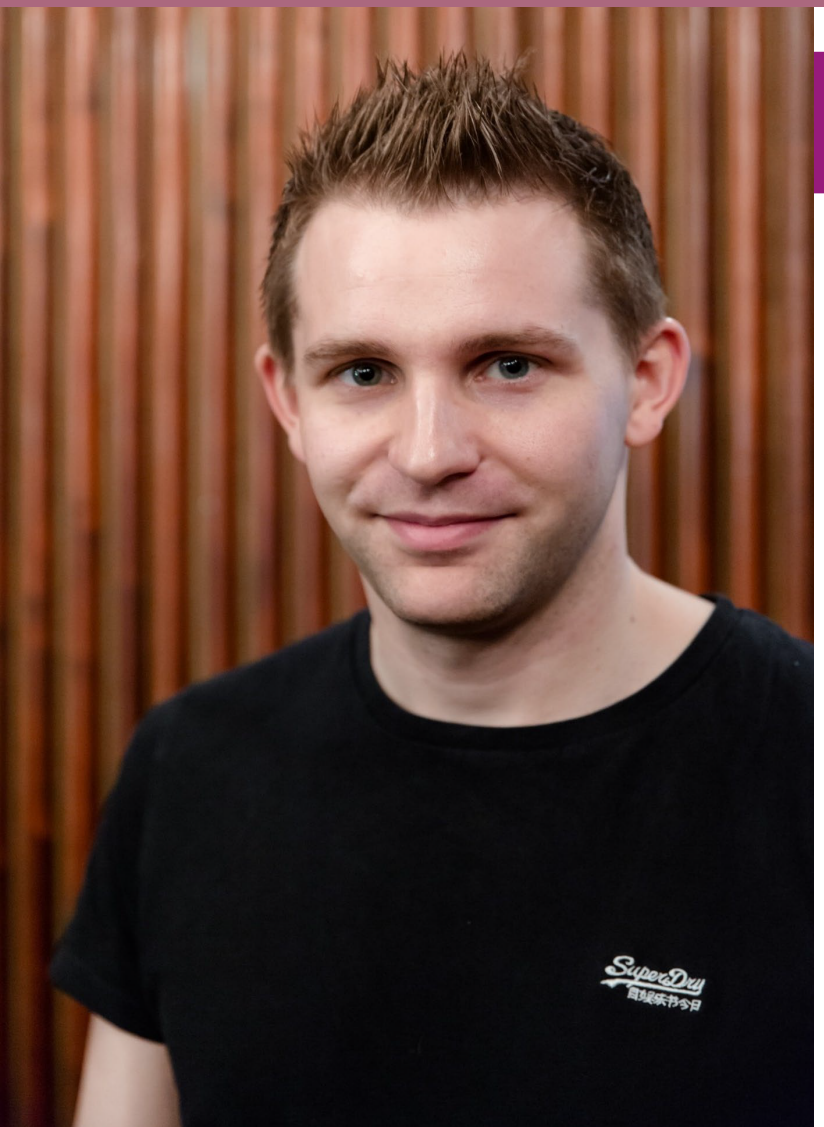
TELE2

PTS

POST & TELESTYRELSEN

PTS

Maximillian Schrems protiv Data Protection Commissioner (C-362/14, 2015):



noyb

NOYB enforces your right to privacy everyda

My Privacy is None of Your Business

News

How mobile apps illegally share your personal data

Sep 14, 2023

Some mobile apps share your personal data immediately after they're opened. This isn't compliant with EU privacy laws

Read more

Your Fitbit is useless – unless you consent to unlawful data sharing

Aug 31, 2023

noyb filed three complaints against Fitbit. The health and fitness company forces new app users to consent to data transfers

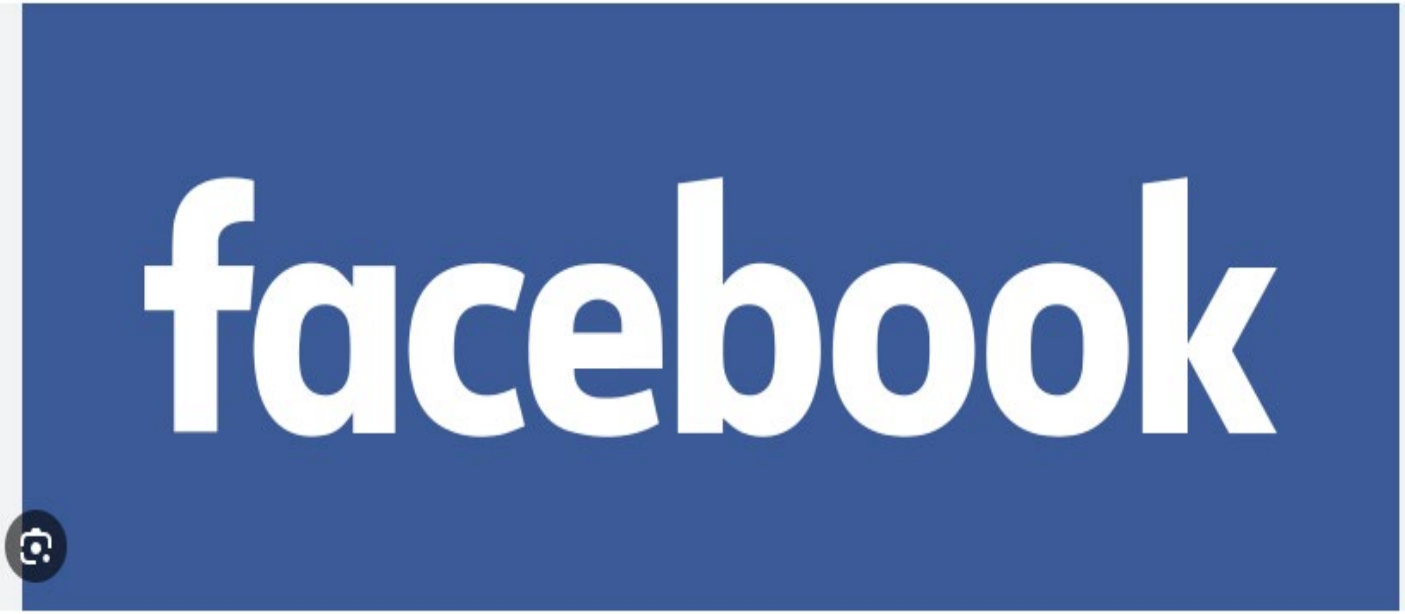
Read more

Annual Report 2022 out now!

Aug 23, 2023

23 years of illegal data transfers due to inactive DPAs and new EU-US deals

Fashion ID GmbH & Co. KG protiv Verbraucherzentrale NRW eV (C-40/17, 2019):

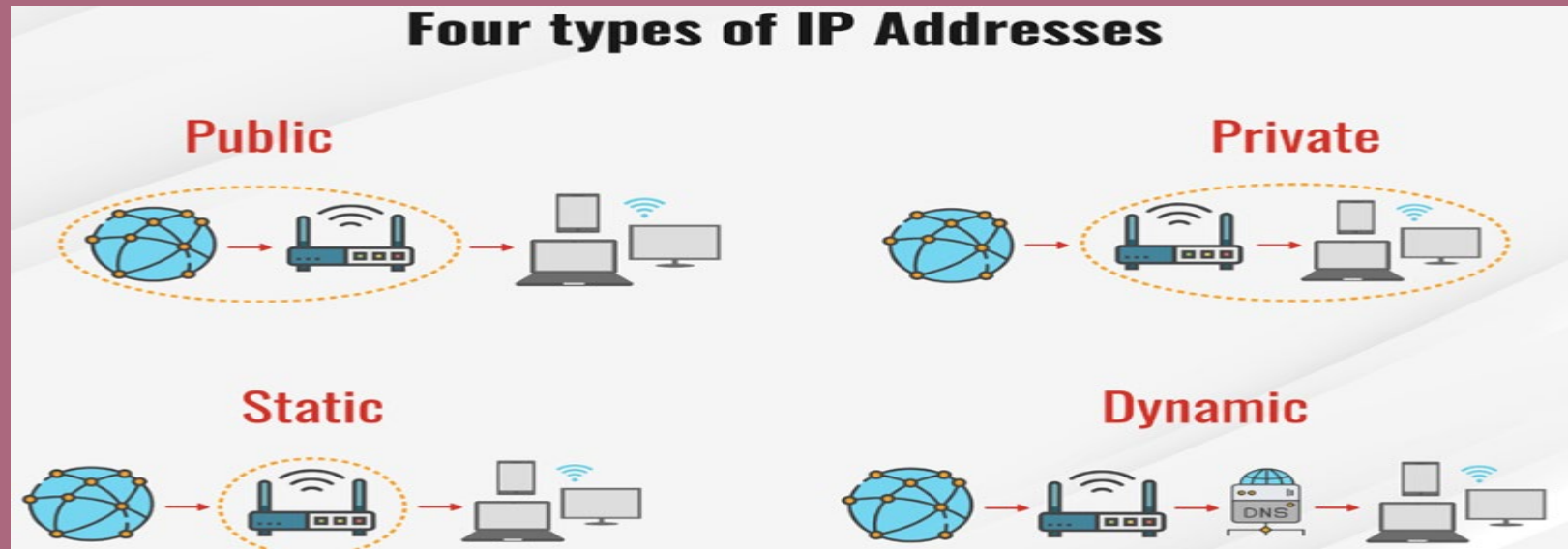


- Europski sud se bavio pitanjem odgovornosti za obradu podataka u okviru ugrađivanja Facebookovog gumba "Like" (sviđa mi se) na web stranicu.
- Postupak je pokrenut od strane njemačke organizacije za zaštitu potrošača, koja je podnijela tužbu protiv online modnog trgovca Fashion ID zbog navodnog kršenja odredbi o zaštiti podataka.
- Tvrdili su da Fashion ID, kroz integraciju Facebookovog gumba "Like" na svoje web mjesto, omogućuje prikupljanje i prijenos osobnih podataka korisnika Facebooku bez njihove prethodne informiranosti ili suglasnosti.
- Fashion ID je isticao da nisu odgovorni za obradu podataka koji se dalje obavlja od strane Facebooka nakon prijenosa.

Breyer protiv Bundesrepublik Deutschland (C-582/14, 2016)

- Presuda Europskog suda u slučaju Patrick Breyer protiv Bundesrepublik Deutschland (C-582/14, 2016) značajna je za definiciju što se smatra "osobnim podacima" u okviru EU zakonodavstva o zaštiti podataka.
- Slučaj se usredotočuje na pitanje da li dinamičke IP adrese mogu biti smatrane osobnim podacima.
- Patrick Breyer, član Piratske stranke Njemačke, pokrenuo je parnicu protiv Njemačke oko prakse pohrane dinamičkih IP adresa od strane javnih tijela.
- S druge strane, njemačka Vlada je tvrdila da IP adrese ne predstavljaju osobne podatke jer, prema njihovom mišljenju, identifikacija korisnika nije moguća bez dodatnih informacija od internetskog pružatelja usluga.

PIRATENPARTEI Deutschland



Opći uvjeti za izricanje upravnih novčanih kazni

- Kazne trebaju biti:
  - učinkovite
  - proporcionalne
  - odvraćajuće
- Visina kazne ovisit će o brojnim kriterijima poput: prirode, težine i trajanja povrede,
  - opsega i svrhe obrade
  - broja ispitanika,
  - kategorijama osobnih podataka
  - postojanja namjere ili nepažnje,
  - aktivnostima za ublažavanje štete,
  - prijašnjim povredama itd.

Neke od istaknutijih kazni izrečenih od europskih nadzornih tijela

1. **British Airways (2019)** : Ovo je jedan od najvećih slučajeva povrede podataka u smislu financijske kazne (oko 183 milijuna GBP). Odluka se odnosi na obvezu implementacije adekvatnih sigurnosnih mjera za zaštitu osobnih podataka korisnika od neovlaštenog pristupa i manipulacije
2. **Marriott International (2019**: Kazna izrečena Marriottu (oko 99 milijuna GBP) odnosi se na obvezu voditelja obrade u provjeri i osiguranju da su osobni podaci koji su preuzeti kroz akvizicije zaštićeni u skladu s OUZP
3. **Google (2019, Francuska, 2021 Francuska i Irska)** : Prvo je francuski CNIL kaznio je Google s 50 milijuna EUR, naglašavajući važnost jasnoće i transparentnosti u informiranju korisnika o obradi njihovih podataka, kao i važnost valjane privole, a onda opet s 60 i 90 milijuna eura zbog nedostatne pravne osnove obrade
4. **Vodafone España (2020, Španjolska)** : Poštivanje prava ispitanika, uključujući pravo na prigovor marketinškim komunikacijama.
5. **H&M (2020, Njemačka)**: Kazna od 35,3 milijuna EUR odnosi se na povredu prava zaposlenika, kao i potrebu za uspostavljanjem jasnih granica između profesionalnih i osobnih informacija u radnom okruženju.
6. **TikTok (2023, Nizozemska)**: Jedna od najviših izrečenih kazni (350 milijuna eura) naglašava pitanje zaštite osobnih podataka djece, ukazujući na potencijalnu ozbiljnost povreda koje se odnose na obradu podataka maloljetnika
7. **Amazon (2021, Luksemburg):** Vodeći svjetski e-trgovac kažnjen sa 750 milijuna eura zbog povrede načela zaštite osobnih podataka

Praksa europskih nadzornih tijela – odabrani slučajevi

	Voditelj obrade	Država	Iznos (€)	Povreda	Datum
1	**Meta Platforms Ireland Limited**	IRSKA	1200000000	Neodgovarajuća pravna osnova obrade	12.5.2023
2	**Amazon Europe Core S.à.r.l.**	LUXEMBOURG	746000000	Povreda načela obrade osobnih podataka	16.7.2021
3	**Meta Platforms, Inc.**	RSKA	405000000	Povreda načela obrade osobnih podataka	5.9.2022
4	**Meta Platforms Ireland Limited**	RSKA	390000000	Povreda načela obrade osobnih podataka	4.1.2023
5	**Meta Platforms Ireland Limited**	RSKA	265000000	Neodgovarajuće tehničke i organizacijske mjere	#######
6	**WhatsApp Ireland Ltd.**	RSKA	225000000	Povreda prava na informiranje o obradi	2.9.2021
7	**Google LLC**	FRANCUSKA	90000000	Neodgovarajuća pravna osnova obrade	#######
8	**Facebook Ireland Ltd.**	FRANCUSKA	60000000	Neodgovarajuća pravna osnova obrade	#######
9	**Google Ireland Ltd.**	FRANCUSKA	60000000	Neodgovarajuća pravna osnova obrade	#######
10	**Google LLC**	FRANCUSKA	50000000	Neodgovarajuća pravna osnova obrade	21.1.2019

1. mjesto – top negativac

Privacy no longer a social norm, says Facebook founder

People have become more comfortable sharing private information online, says Facebook founder Mark Zuckerberg. Photograph: Eric Risberg/AP

The rise of social networking online means that people no longer have an expectation of privacy, according to Facebook founder Mark Zuckerberg.

Talking at the Crunchie awards in San Francisco this weekend, the 25-year-old chief executive of the world's most popular social network said that privacy was no longer a "social norm".

"People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people," he said. "That social norm is just something that has evolved over time."

Zuckerberg said that the rise of social media reflected changing attitudes among ordinary people, adding that this radical change has happened in just a few years.

Statistics: Highest individual fines (Top 10)

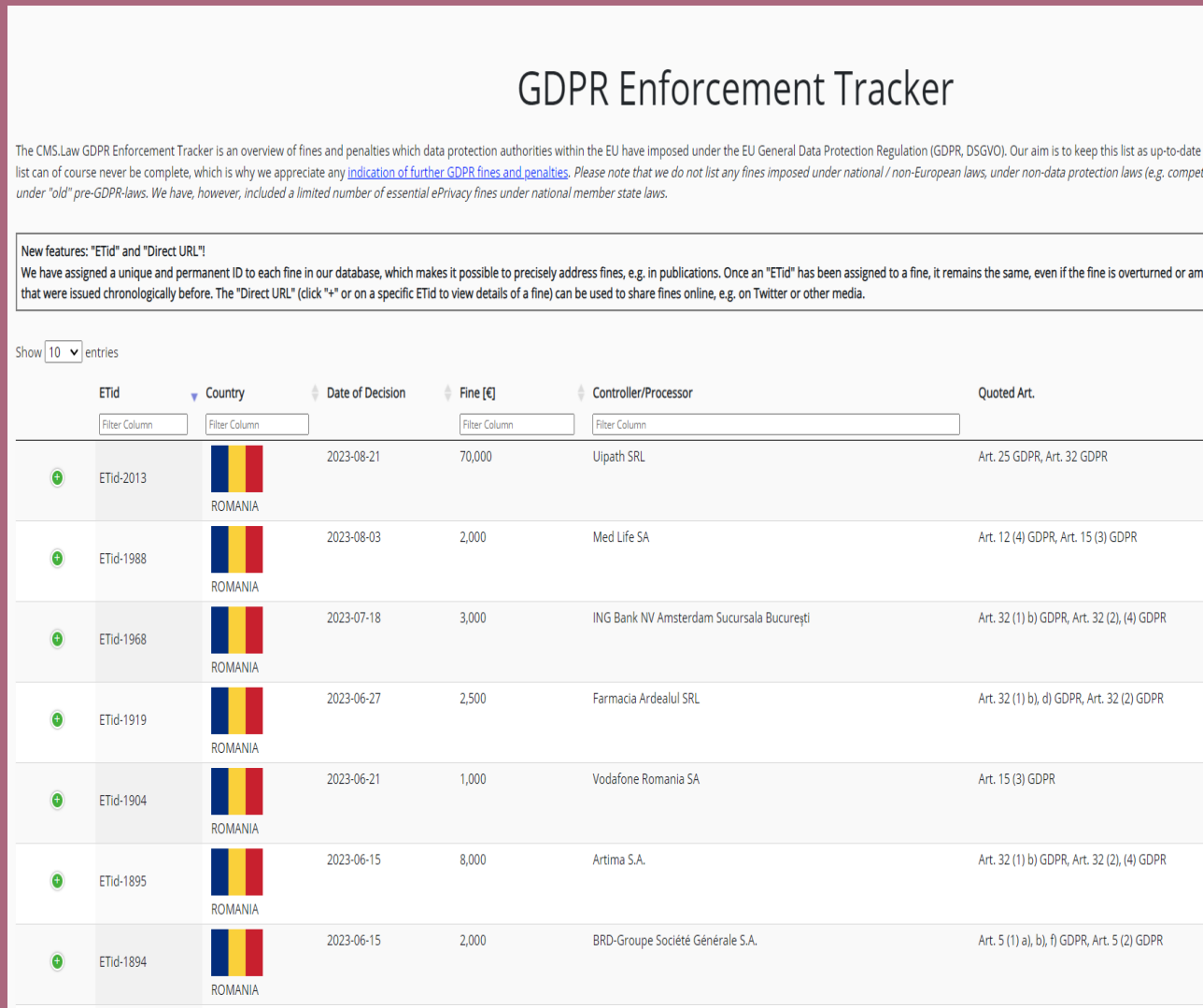
The following statistics shows the highest individual fines imposed to date per data controller (only top 10 fines).

	Controller	Sector	Country	Fine [€]
1	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	1200000000
2	Amazon Europe Core S.à.r.l.	Industry and Commerce	LUXEMBOURG	746000000
3	Meta Platforms, Inc.	Media, Telecoms and Broadcasting	IRELAND	405000000
4	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	390000000
5	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	265000000
6	WhatsApp Ireland Ltd.	Media, Telecoms and Broadcasting	IRELAND	225000000
7	Google LLC	Media, Telecoms and Broadcasting	FRANCE	90000000
8	Facebook Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60000000
9	Google Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60000000
10	Google LLC	Media, Telecoms and Broadcasting	FRANCE	50000000

- **Facebook/Meta je vodeći prekršitelj među velikim internetskim platformama**
- **Ukupan iznos izrečenih kazni prelazi 2.5 milijardi eura**
- **U tijeku su postupci protiv Instagrama i drugih organizacija iz Meta grupe**
- **Također je pod istragom zbog povreda tržišnog natjecanja i drugih europskih propisa**

Statistike izrečenih kazni prema Enforcementtracker.com (GDPRTRACKER)

- Izvor: GDPR Enforcement Tracker – enforcementtracker.com
- Ukupno izrečeno 1801 kazna u razdoblju 2018-2023 (rujan 2023)
- Ukupan iznos izrečenih kazni prelazi 4.051 milijardi eura
- Najveći iznosi kazni izrečeni su u: Luksemburgu, Irskoj, Francuskoj, Italiji, Španjolskoj, UK, Njemačkoj, Grčkoj, Austriji i Švedskoj
- U Nizozemskoj je nadzorno tijelo prijavilo i kaznilo samo sebe
- U Hrvatskoj je do sad izrečena 21 kazna u ukupnom iznosu preko 4 milijuna eura.



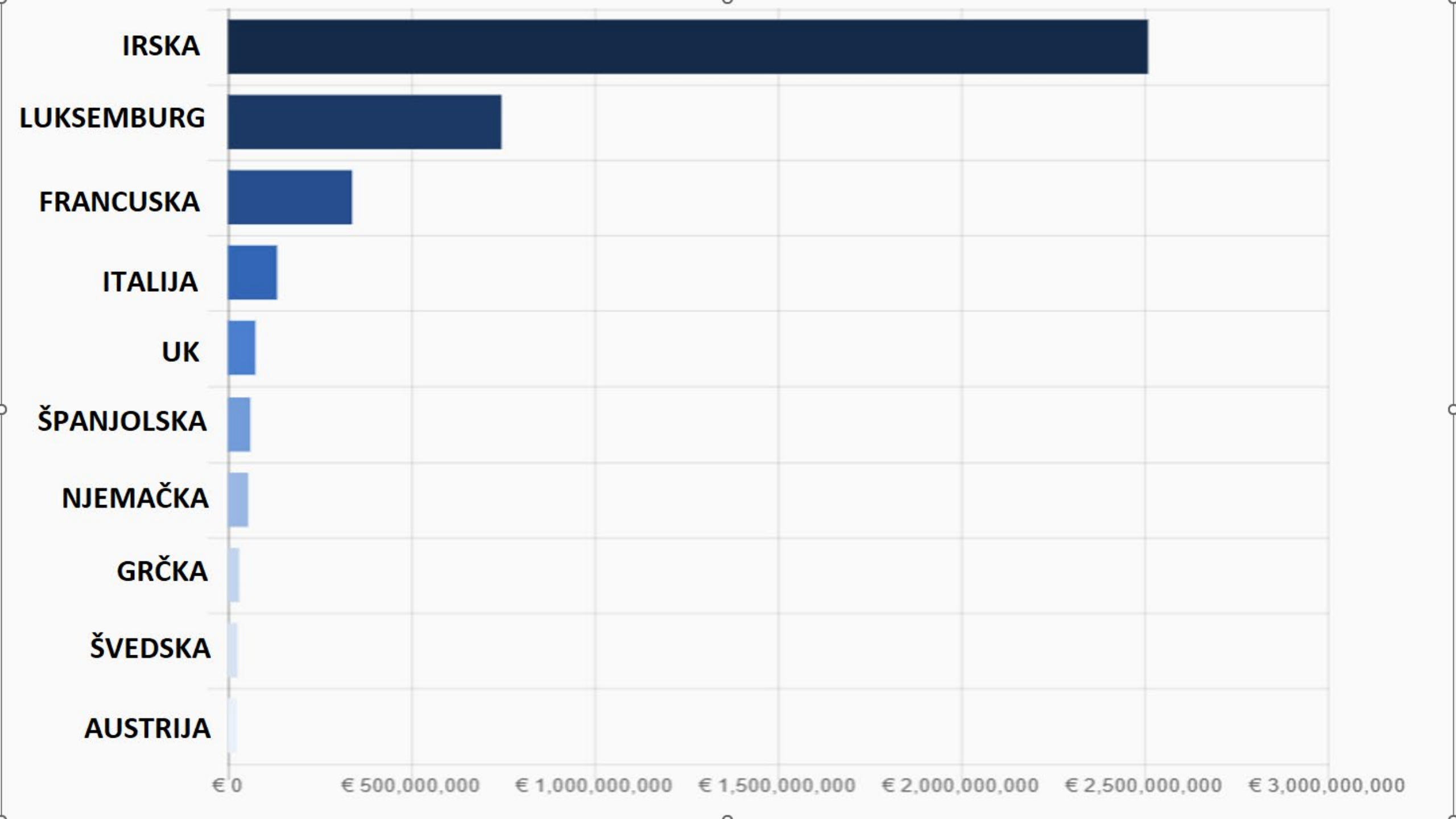
GDPR Enforcement Tracker

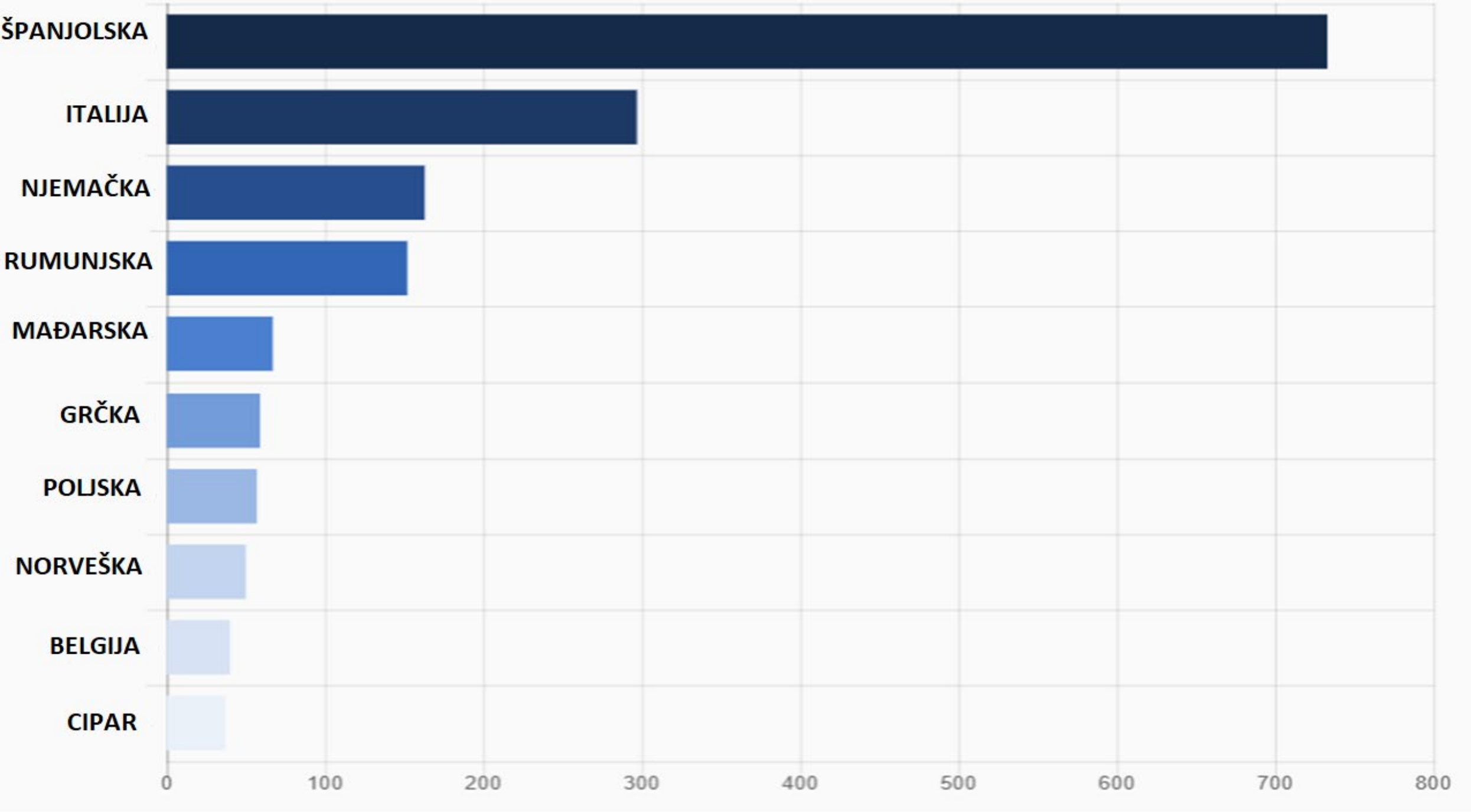
The CMS.Law GDPR Enforcement Tracker is an overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date list can of course never be complete, which is why we appreciate any indication of further GDPR fines and penalties. *Please note that we do not list any fines imposed under national / non-European laws, under non-data protection laws (e.g. compet under "old" pre-GDPR-laws. We have, however, included a limited number of essential ePrivacy fines under national member state laws.*

New features: "ETid" and "Direct URL"!
We have assigned a unique and permanent ID to each fine in our database, which makes it possible to precisely address fines, e.g. in publications. Once an "ETid" has been assigned to a fine, it remains the same, even if the fine is overturned or am that were issued chronologically before. The "Direct URL" (click "+" or on a specific ETid to view details of a fine) can be used to share fines online, e.g. on Twitter or other media.

Show 10 entries

ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.
ETid-2013	ROMANIA	2023-08-21	70,000	Uipath SRL	Art. 25 GDPR, Art. 32 GDPR
ETid-1988	ROMANIA	2023-08-03	2,000	Med Life SA	Art. 12 (4) GDPR, Art. 15 (3) GDPR
ETid-1968	ROMANIA	2023-07-18	3,000	ING Bank NV Amsterdam Sucursala București	Art. 32 (1) b) GDPR, Art. 32 (2), (4) GDPR
ETid-1919	ROMANIA	2023-06-27	2,500	Farmacia Ardealul SRL	Art. 32 (1) b), d) GDPR, Art. 32 (2) GDPR
ETid-1904	ROMANIA	2023-06-21	1,000	Vodafone Romania SA	Art. 15 (3) GDPR
ETid-1895	ROMANIA	2023-06-15	8,000	Artima S.A.	Art. 32 (1) b) GDPR, Art. 32 (2), (4) GDPR
ETid-1894	ROMANIA	2023-06-15	2,000	BRD-Groupe Société Générale S.A.	Art. 5 (1) a), b), f) GDPR, Art. 5 (2) GDPR

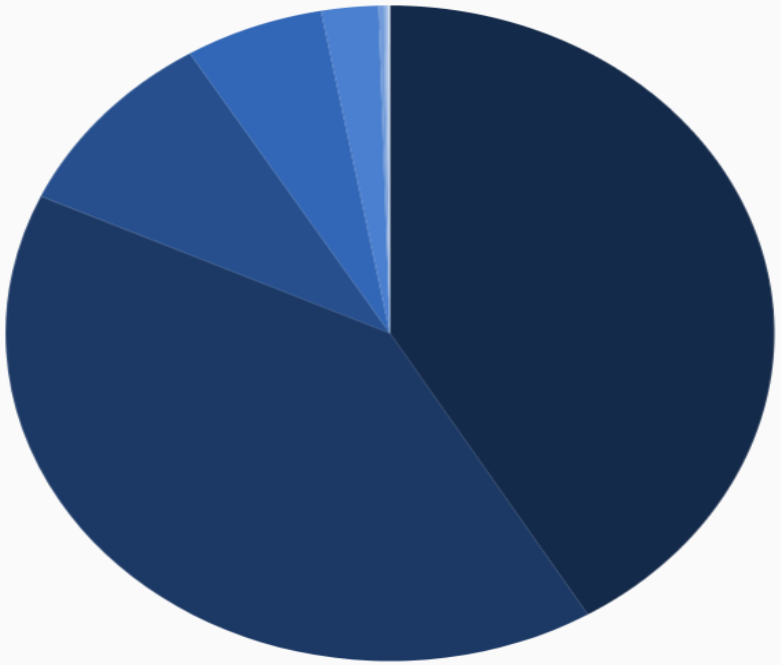

IRSKA
LUKSEMBURG
FRANCUSKA
ITALIJA
UK
ŠPANJOLSKA
NJEMAČKA
GRČKA
ŠVEDSKA
AUSTRIJA
€ 0
€ 500,000,000
€ 1,000,000,000
€ 1,500,000,000
€ 2,000,000,000
€ 2,500,000,000
€ 3,000,000,000


ŠPANJOLSKA
ITALIJA
NJEMAČKA
RUMUNJSKA
MAĐARSKA
GRČKA
POLJSKA
NORVEŠKA
BELGIJA
CIPAR
0
100
200
300
400
500
600
700
800

Statistics: Fines by type of violation
The following statistics show how many fines and what sum of fines have been imposed per type of GDPR violation to date.

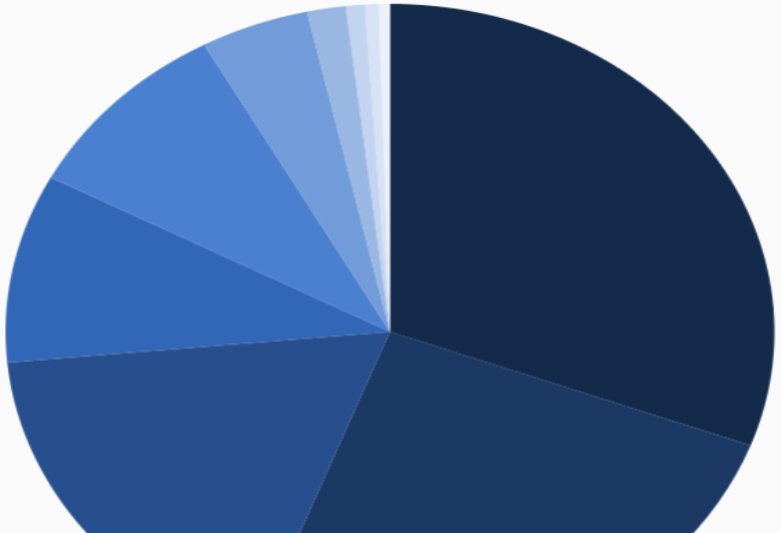
Note: Only fines with valid information on the amount of the fine and on the type of violation are taken into account.

1. By total sum of fines:



Violation	Sum of Fines
Non-compliance with general data processing principles	**€ 1,680,455,079** (at 480 fines)
Insufficient legal basis for data processing	**€ 1,642,666,672** (at 584 fines)
Insufficient technical and organisational measures to ensure information security	**€ 382,152,575** (at 337 fines)
Insufficient fulfilment of information obligations	**€ 237,264,180** (at 175 fines)
Insufficient fulfilment of data subjects rights	**€ 97,430,970** (at 177 fines)
Unknown	**€ 9,250,000** (at 9 fines)
Insufficient cooperation with supervisory authority	**€ 6,144,029** (at 87 fines)
Insufficient fulfilment of data breach notification obligations	**€ 1,778,582** (at 31 fines)
Insufficient data processing agreement	**€ 1,057,110** (at 11 fines)
Insufficient involvement of data protection officer	**€ 919,300** (at 15 fines)

2. By total number of fines:



Violation	Number of Fines
Insufficient legal basis for data processing	**584** (with total € 1,642,666,672)
Non-compliance with general data processing principles	**480** (with total € 1,680,455,079)
Insufficient technical and organisational measures to ensure information security	**337** (with total € 382,152,575)
Insufficient fulfilment of data subjects rights	**177** (with total € 97,430,970)
Insufficient fulfilment of information obligations	**175** (with total € 237,264,180)
Insufficient cooperation with supervisory authority	**87** (with total € 6,144,029)
Insufficient fulfilment of data breach notification obligations	**31** (with total € 1,778,582)
Insufficient involvement of data protection officer	**15** (with total € 919,300)
Insufficient data processing agreement	**11** (with total € 1,057,110)
Unknown	**9** (with total € 9,250,000)

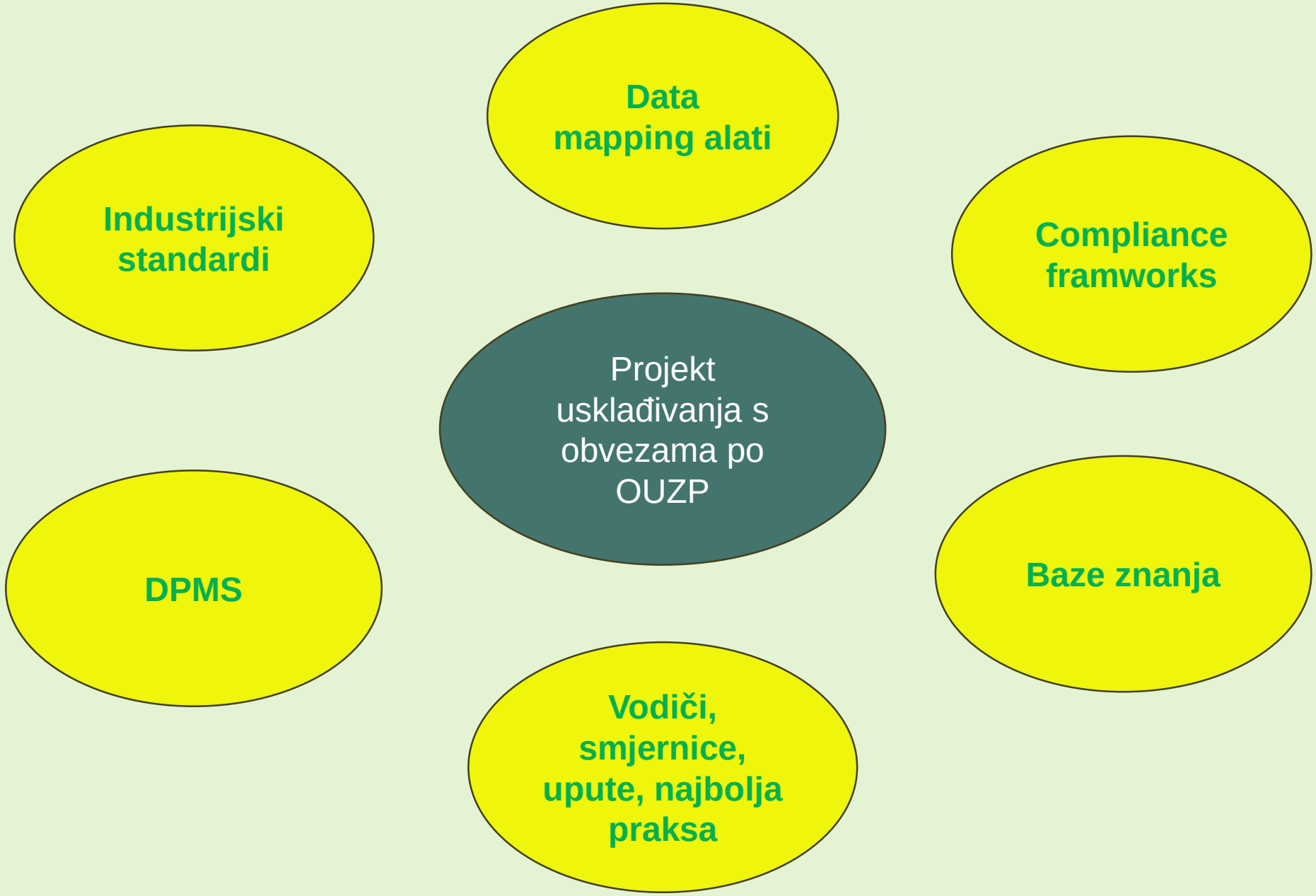
Kako se uskladiti sa zahtjevima OUZP?

Prepoznati informacijske sustave i usluge – MAPIRANJE PODATAKA
Provesti postupke procjene učinka – DPIA
Razviti internu politiku zaštite podataka – PRAVILNIK O ZAŠTITI PODATA
Pripremiti popis tehničkih i organizacijskih mjera za zaštitu osobnih podataka (TOMs)
Pripremiti obavijesti ispitanicima – OBAVIJESTI O OBRADI
Ustanoviti i pripremiti vođenje evidencija aktivnosti obrade – EAO
Pripremiti postupke za ispunjavanje zahtjeva ispitanika – ZAHTJEVI ISPITANIKA
Utvrditi postupak upravljanja incidentima povrede osobnih podataka – UPRAVLJANJE INCIDENTIMA
Definirati mehanizme za prijenos osobnih podataka izvan EU – TRANSFERI
Edukacija uprave i djelatnika te priprema programa podizanja svjesnosti – SVJESNOST

Kako se uskladiti sa zahtjevima OUZP?

Prepoznati informacijske sustave i usluge – MAPIRANJE
Provesti postupke procjene učinka – DPIA
Razviti internu politiku zaštite podataka – PRAVILNIK O ZAŠTITI PODATAKA
Pripremiti popis tehničkih i organizacijskih mjera za zaštitu osobnih podataka (TOMs)
Pripremiti obavijesti ispitanicima – OBAVIJESTI O OBRADI PODATAKA
Ustanoviti i pripremiti vođenje evidencija aktivnosti obrade – EAO
Pripremiti postupke za ispunjavanje zahtjeva ispitanika – ZAHTJEVI ISPITANIKA
Utvrditi postupak upravljanja incidentima povrede osobnih podataka – UPRAVLJANJE INCIDENTIMA
Definirati mehanizme za prijenos osobnih podataka izvan EU – TRANSFERI
Edukacija uprave i djelatnika te priprema programa podizanja svjesnosti? – SVJESNOST

Kako do usklađivanja?



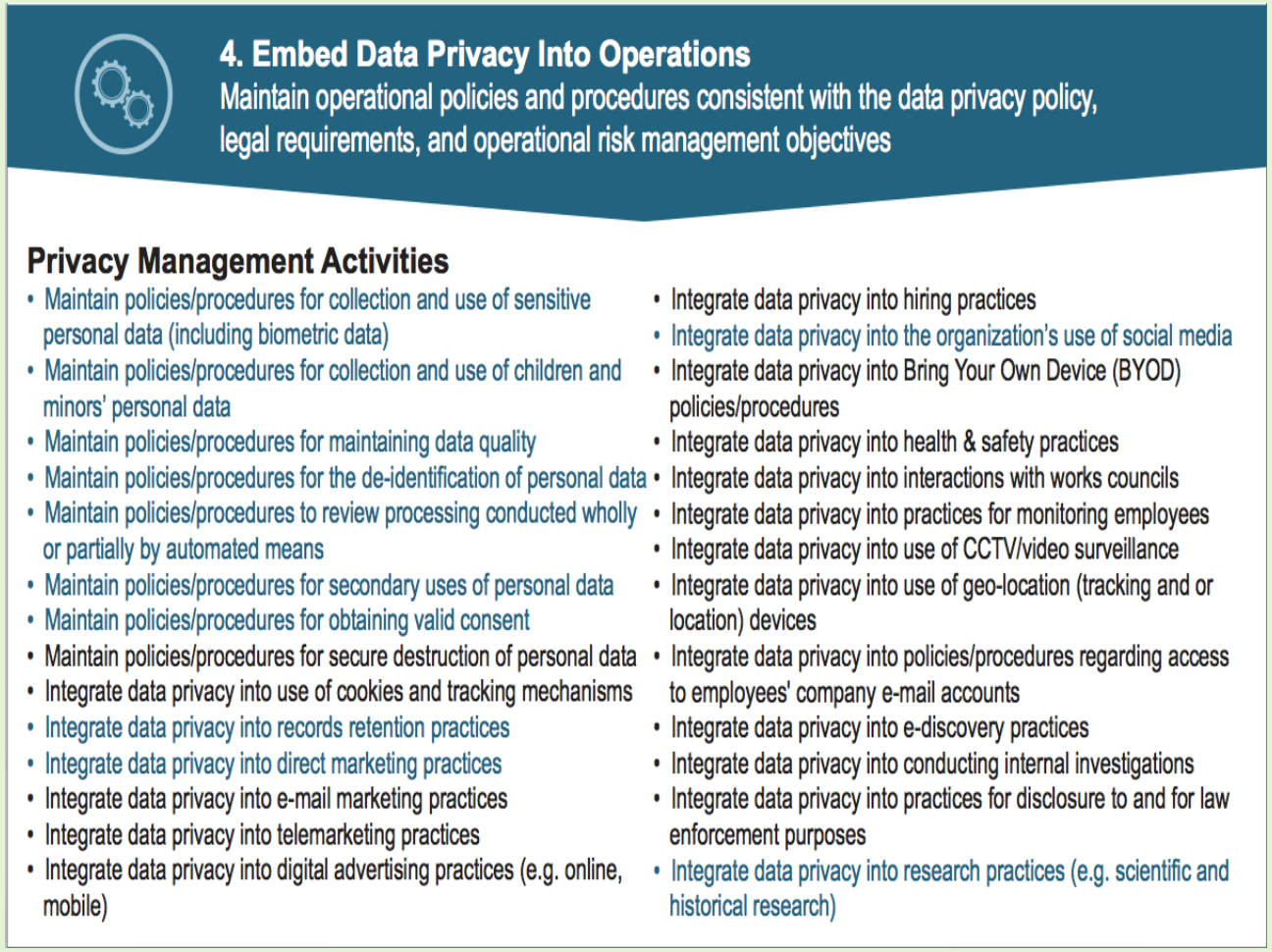
Data mapping alati

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

Okviri za usklađivanje (compliance frameworks)

- GDPR Compliance Frameworks, kao što je Nymity Framework, su strukturirani set alata, smjernica i najboljih praksi koje pomažu organizacijama da se usklade s zahtjevima Opće uredbe o zaštiti podataka
- Oni nude strukturiran pristup za upravljanje svim aspektima zaštite podataka, od identifikacije i klasifikacije podataka do izrade politika i procedura za zaštitu podataka
- Često osim interpretacije obveza iz Opće uredbe sadrže i tzv. kontrole iz standarda informacijske sigurnosti, kao što je ISO 27000 obitelj standarda informacijske sigurnosti



4. Embed Data Privacy Into Operations

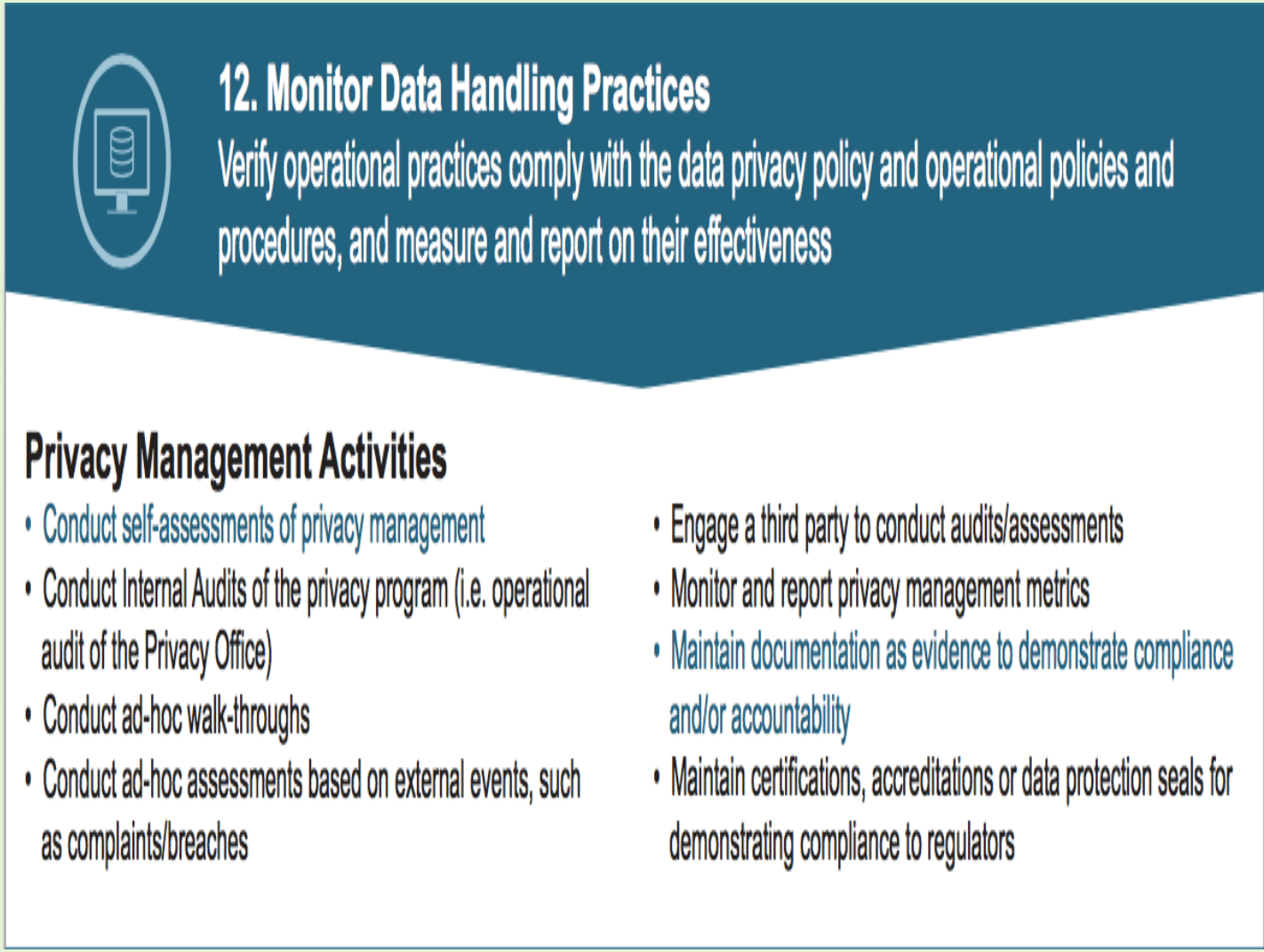
Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

Privacy Management Activities

- Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)
- Maintain policies/procedures for collection and use of children and minors' personal data
- Maintain policies/procedures for maintaining data quality
- Maintain policies/procedures for the de-identification of personal data
- Maintain policies/procedures to review processing conducted wholly or partially by automated means
- Maintain policies/procedures for secondary uses of personal data
- Maintain policies/procedures for obtaining valid consent
- Maintain policies/procedures for secure destruction of personal data
- Integrate data privacy into use of cookies and tracking mechanisms
- Integrate data privacy into records retention practices
- Integrate data privacy into direct marketing practices
- Integrate data privacy into e-mail marketing practices
- Integrate data privacy into telemarketing practices
- Integrate data privacy into digital advertising practices (e.g. online, mobile)
- Integrate data privacy into hiring practices
- Integrate data privacy into the organization's use of social media
- Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures
- Integrate data privacy into health & safety practices
- Integrate data privacy into interactions with works councils
- Integrate data privacy into practices for monitoring employees
- Integrate data privacy into use of CCTV/video surveillance
- Integrate data privacy into use of geo-location (tracking and or location) devices
- Integrate data privacy into policies/procedures regarding access to employees' company e-mail accounts
- Integrate data privacy into e-discovery practices
- Integrate data privacy into conducting internal investigations
- Integrate data privacy into practices for disclosure to and for law enforcement purposes
- Integrate data privacy into research practices (e.g. scientific and historical research)

Zašto koristiti komercijalne 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 (E-Health 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 uspostavi robustnih procedura za zaštitu podataka od samog početka
- Lakše je uvesti pravila o zaštiti podataka na novu, rastuću organizaciju nego na postojeću

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

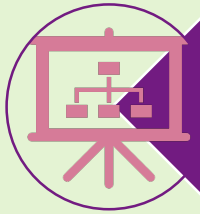
Sektorski specijalizirani industrijski samoregulacijski standardi

- **AICPA Privacy Management Framework**
  - Razvijen od strane American Institute of Certified Public Accountants (AICPA), ovaj okvir nudi smjernice za uspostavu i održavanje programa upravljanja privatnošću.
  - Sadrži kontrole prilagodbe pravnih i regulatornih obveze, upravljanje rizikom privatnosti, kontinuirano praćenje i testiranje politika privatnosti
- **TISAX (Trusted Information Security Assessment Exchange)**
  - **Osiguravanje sigurnosti informacija u automobilskoj industriji**: TISAX je standard koji je razvijen od strane automobilske industrije (primarno u Njemačkoj) da ocijeni i verificira adekvatnost mjera sigurnosti informacija unutar industrije.
  - TISAX omogućava tvrtkama unutar automobilske industrije da koriste rezultate međusobnih ocjena, što pomaže u smanjenju potrebe za višestrukim, odvojenim procjenama.
- **PCI DSS (Payment card industry data security standard)**
  - **Osiguravanje sigurnosti financijskih transakcija**: PCI DSS je globalni standard koji postavlja zahtjeve za sigurnosne mjere koje trebaju biti na mjestu za sve organizacije koje pohranjuju, obrađuju ili prenose podatke o kartičnim plaćanjima.
  - **Zaštita osjetljivih podataka o karticama**: Cilj ovog standarda je smanjiti rizik od curenja i zloupotrebe osjetljivih informacija o vlasnicima kartica.
  - **Usklađenost s regulatornim zahtjevima**: Pomaže organizacijama u ispunjavanju zakonskih i regulatornih zahtjeva u vezi s financijskim transakcijama.

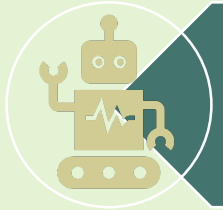
ISO 27001

- ISO 27001, službeno poznat kao ISO/IEC 27001, je međunarodni standard koji pruža okvir za uspostavu, implementaciju, upravljanje i kontinuirano poboljšanje sustava upravljanja sigurnošću informacija (Information Security Management System - ISMS) unutar organizacije
- **Čemu služi ISO 27001?**

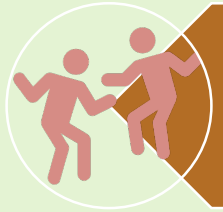
KLJUČNE KOMPONENTE ISO 27001 SUSTAVA



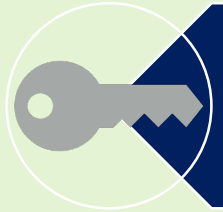
Organizacijske kontrole



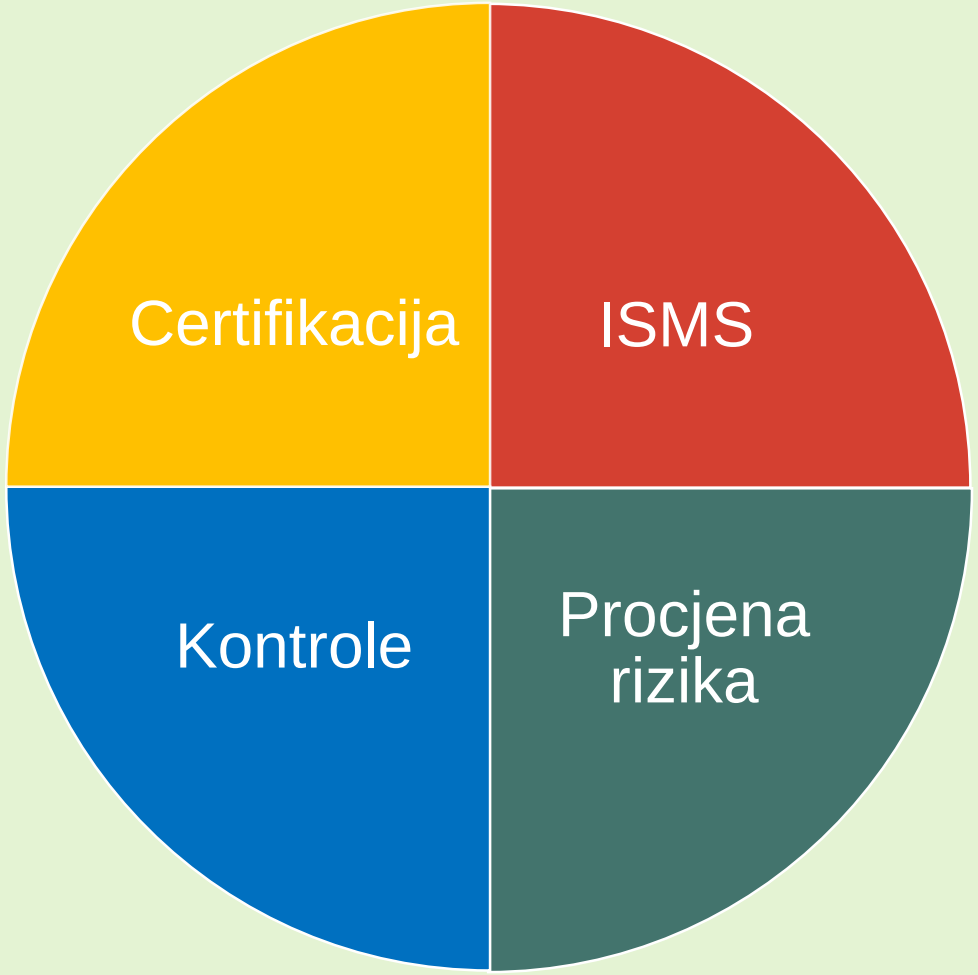
Tehničke kontrole



Kontrole ljudskih resursa



Fizičke kontrole



ISO 27001 kontrole

- Temeljne grupe kontrola su: **organizacijske, tehničke, kontrole ljudskih resursa i fizičke kontrole**
- ISO 27001 standard sadrži ukupno 114 kontrola, koje su podijeljene u ove četiri kategorije. Organizacije mogu izabrati koje kontrole će implementirati, ovisno o svojim specifičnim potrebama i rizicima.
- Primjeri implementacije kontrola ISO 27001 standarda u organizaciji:
  - Organizacija može implementirati politiku informacijske sigurnosti koja definira ciljeve i zahtjeve organizacije u vezi s informacijskom sigurnošću.
  - Organizacija može uspostaviti odjel za sigurnost informacija koji je odgovoran za implementaciju i održavanje programa informacijske sigurnosti.
  - Organizacija može zahtijevati od zaposlenika da prođu obuku o informacijskoj sigurnosti i da potpišu sporazum o tajnosti.
  - Organizacija može implementirati firewall i antivirusni softver za zaštitu svoje mreže i računala.
  - Organizacija može šifrirati svoje podatke kako bi ih zaštitila od nedozvoljenog pristupa i zloupotrebe
  - Organizacija može instalirati kamere i ostale fizičke kontrole za zaštitu svojih prostorija i opreme

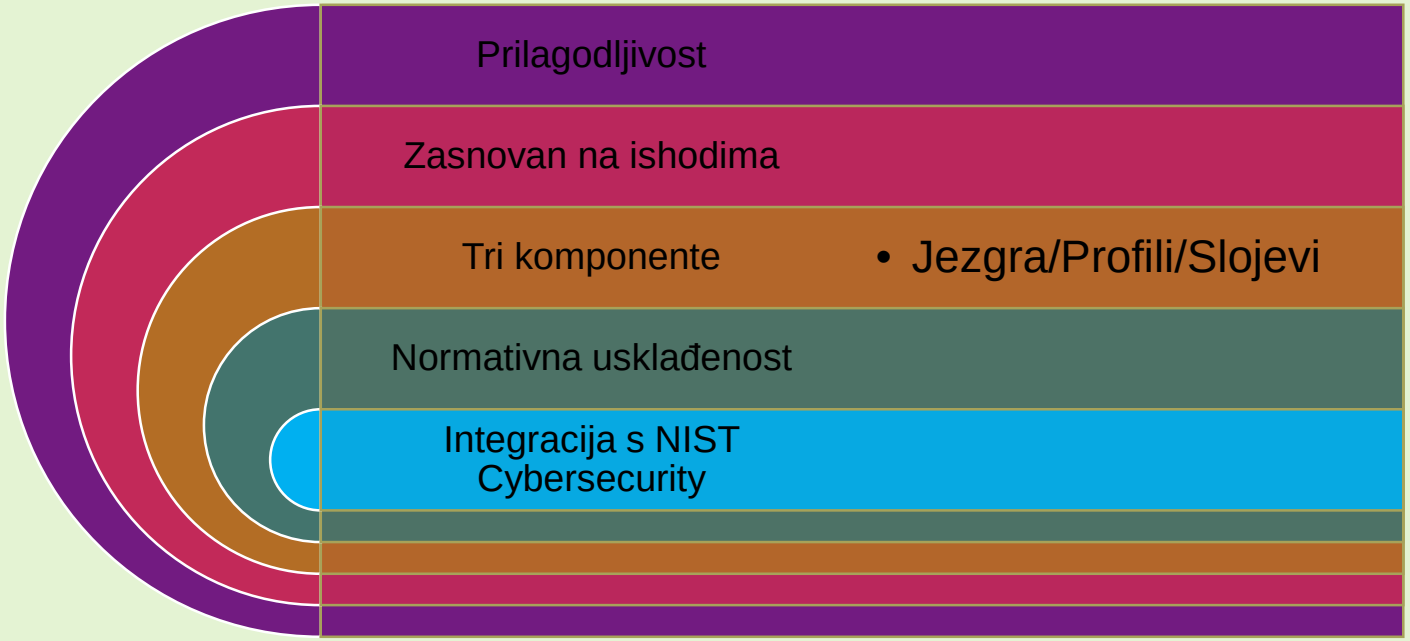
Ovo su samo neki primjeri implementacije kontrola ISO 27001 standarda. Organizacije mogu implementirati i druge kontrole, ovisno o svojim specifičnim potrebama i rizicima.

Što je i čemu služi ISO 27701

- Standard koji pruža smjernice za upravljanje informacijama o privatnosti, uključujući detalje o kako implementirati, održavati i poboljšavati sustav upravljanja informacijama o privatnosti (PIMS - Privacy Information Management System).
- Ovaj standard pomaže organizacijama da bolje zaštite privatnost podataka i usklade se s relevantnim zakonima o zaštiti privatnosti, uključujući OUZP
- ISO 27701 poznat je i kao dodatak već tržišno prepoznatim i široko raširenim ISO/IEC 27001 i ISO/IEC 27002 standardima

NIST Privacy Framework

- NIST Privacy Framework je alat koji je razvila američka Nacionalna agencija za standarde i tehnologiju (NIST) kako bi pomogla organizacijama u upravljanju rizicima povezanima s privatnošću i zaštitom podataka



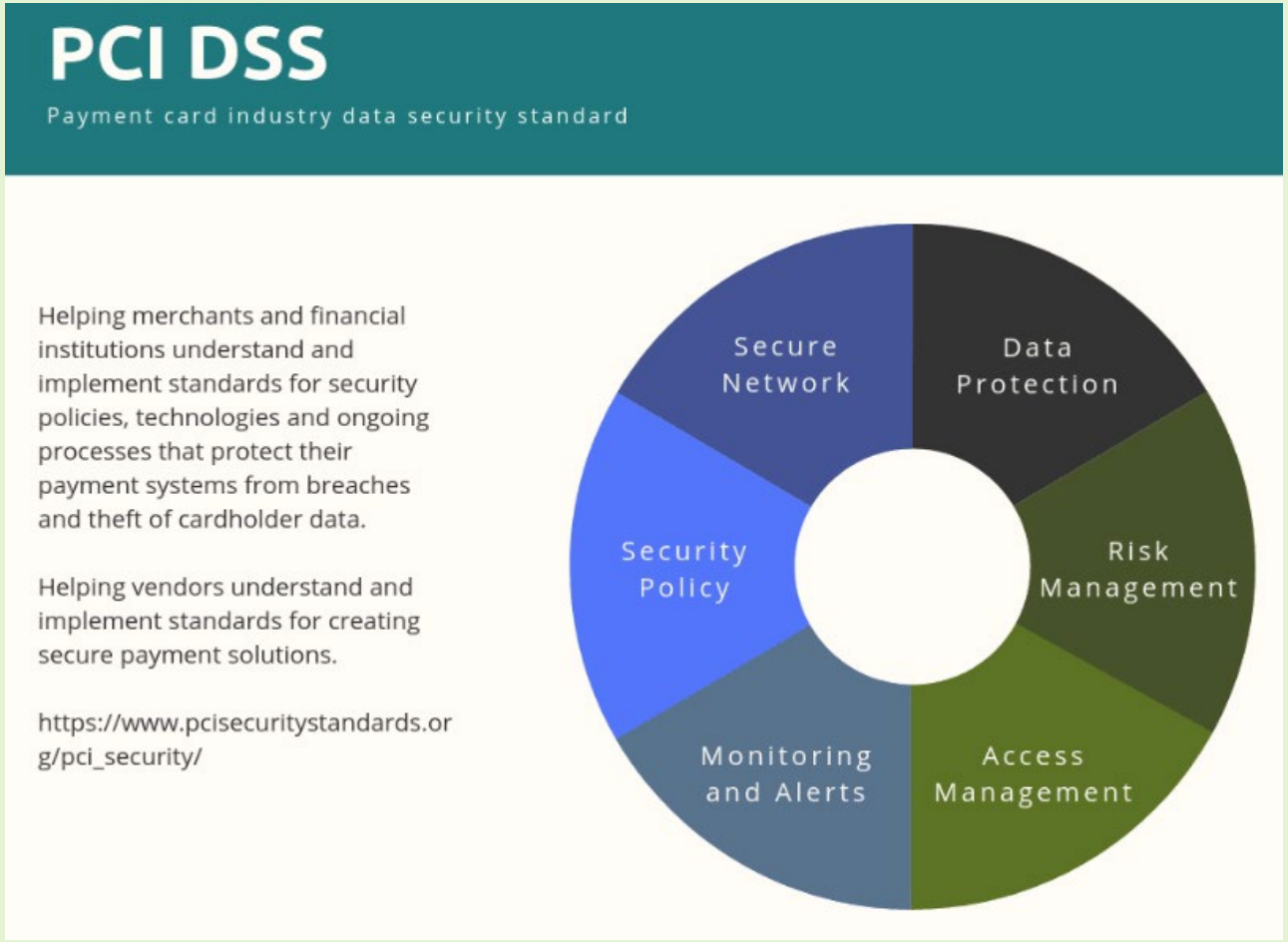
- Ovaj okvir, službeno objavljen u siječnju 2020, nudi pristup zasnovan na rizicima koji organizacijama pomaže u integraciji praksi zaštite privatnosti u njihovu poslovnu strategiju i tehničke sustave.

TISAX

- TISAX (Trusted Information Security Assessment Exchange) je standard za sigurnost informacija koji je usvojen u automobilskoj industriji.
- Usklađivanje s OUZP (Općom uredbom o zaštiti podataka) zahtijeva sveobuhvatno upravljanje i zaštitu osobnih podataka.
- Iako TISAX nije specifično dizajniran za usklađenost s Uredbom, njegova struktura i principi mogu poslužiti kao čvrsta osnova za razvoj i implementaciju potrebnih procesa i kontrola

PCI DSS

- PCI DSS (Payment Card Industry Data Security Standard) je globalni sigurnosni standard koji je uspostavljen kako bi se osigurala sigurnost transakcija s kreditnim karticama i zaštita podataka vlasnika kartica.
- Iako PCI DSS primarno cilja na zaštitu podataka vezanih uz plaćanja karticama, njegova implementacija može biti koristan korak prema usklađivanju s OUZP, jer promiče sigurnu obradu, prijenos, i pohranu osobnih podataka.
- Integriranjem PCI DSS standarda s OUZP obvezama organizacije mogu stvoriti sveobuhvatan i robusni sustav zaštite podataka.



Često postavljana pitanja (1)

1. **Koja je institucija EU-a ovlaštena na vlastitu inicijativu predlagati nove propise o zaštiti osobnih podataka?**

2. **Koji je glavni cilj koji su imale Smjernice OECD-a, Konvencija VE 108 i Direktiva o zaštiti podataka (Direktiva 95/46/EZ), ali koji su u velikoj mjeri propustili postići u Europi?**

3. **Je li točna tvrdnja da je prema Europskoj Konvenciji o ljudskim pravima pravo na privatnost apsolutno i neotuđivo pravo?**

4. **Koja je razlika u ulozi Europskog suda (ECJ) i Europskog suda za ljudska prava (ECHR) u pogledu judikature iz područja zaštite osobnih podataka?**

5. **Koje su europske institucije najviše involvirane u području regulacije i nadzora primjene pravila o zaštiti osobnih podataka?**

Često postavljana pitanja (2)

6. Koji aspekt OUZP vjerojatno ima najveći utjecaj na dosljednu provedbu zaštite podataka na području Europske unije?

7. Je li točna tvrdnja da su odredbe OUZP jedino relevantan pravni izvor u kontekstu regulacije zaštite osobnih podataka?

8. Objasnite kako na sadržaj pravila o zaštiti podataka može djelovati postojanje Uredbi konfliktne odredbe u specijalnom propisu, primjerice u budućem propisu o regulaciji umjetne inteligencije ili o ponovnoj upotrebi podataka?

9. Ukoliko bi nacionalno nadzorno tijelo usvojilo smjernice koje bi odudarale od smjernica Europskog odbora, voditelji obrade bili bi dužni primijeniti koje smjernice u svojoj praksi?

10. Iz perspektive ovlasti nacionalnog zakonodavstva, što možemo zaključiti o opcijama koje nacionalni zakonodavac ima ukoliko usvaja propise koji sadrže odredbe o zaštiti osobnih podataka u odnosu na standarde postavljene OUZP?

Često postavljanja pitanja (3)

11. Zbog čega odnosno temeljem kojeg propisa Europska unija ima pravnu obvezu zakonski razraditi zaštitu osobnih podataka?
12. Koji su razlozi zašto je došlo do razvoja i usvajanja Opće uredbe?
13. Odnosi li se GDPR na trgovačko društvo koje prikuplja i obrađuje osobne podatke europskih građana na području SAD?
14. Primjenjuje li se Opća uredba na obradu osobnih podataka preminulih osoba?
15. Koji pravni okvir Uredba zamjenjuje – koji se propisi više ne primjenjuju?
16. Koji sektorski propisi u zakonodavstvu Republike Hrvatske također sadrže odredbe vezane uz zaštitu osobnih podataka?
17. Odnosi li se Uredba na obradu podataka na materijalnom mediju (papirnatih dokumenata)?
18. Je li svaki korisnik mobitela koji ima telefonski imenik voditelj obrade u smislu primjene odredaba OUZP?

Često postavljana pitanja (4)

19. Koliko detaljno treba ići u raspisivanje aktivnosti obrade, obzirom da neki obrasci preporučaju da se slične obrade grupiraju, a neki ih raspisuju prema različitim kriterijima veće razine detalja (pojedini informacijski sustav, pojedina kategorija primatelja?)

20. Koliko često treba mijenjati sadržaj evidencije?

21. Čemu uopće služi evidencija ?

22. Kako je najučinkovitije pristupiti izradi i održavanju evidencije?

23. U našoj velikoj organizaciji ne postoji dobra komunikacija među odjelima. Službenik tako često ne zna što se događa, a to se reflektira i na sadržaj evidencije. Tko je u konačnici odgovoran za njen sadržaj?

24. Koji voditelji nisu dužni voditi evidenciju aktivnosti obrade?

25. U čemu je razlika između evidencije koju voditelj i one koju vodi izvršitelj?

Često postavljana pitanja (5)

26. Je li IP adresa uvijek osobni podatak?

27. Što su biometrijski, a što genetski podaci?

28. Je li sama mogućnost pristupa podacima prilikom tehničkog održavanja sustava obrada podataka?

29. Koja je razlika između pseudonimizacije i anonimizacije?

30. Kad možemo zaključiti da su podaci zaista anonimizirani?

31. Koje tehnologije ugrožavaju anonimiziranje osobnih podataka?

32. Jesu li netočni osobni podaci i dalje osobni podaci?

33. Jesu li podaci nerođene djece osobni podaci?

34. Jesu li osobni podaci izabranih javnih dužnosnika i osoba koje obavljaju javne funkcije osobni podaci? Postoje li tu neka ograničenja u kontekstu njihove zaštite?

35. Kako se iz perspektive OUZP štite podaci preminulih osoba?

Često postavljana pitanja (6)

36. Koje elemente treba imati ugovor o obradi podataka?

37. Kako trebaju biti raspisane tehničke i organizacijske mjere u ugovoru o obradi podataka?

38. Za što odgovara voditelj obrade, a za što izvršitelj obrade?

39. Što ukoliko voditelj ili izvršitelj nisu dužni imenovati SZOP?

40. Tvrtke A, B i C uspostavljaju zajedničku platformu za neku uslugu, tko je tu voditelj, a tko izvršitelj?

Često postavljana pitanja (7)

41. Je li istinita tvrdnja da većina europskih provedbenih propisa iz područja zaštite podataka konkretno navodi koje su tehničke kontrole nužne za određenu kategoriju obrade osobnih podataka?

42. Što treba sadržavati sporazum između zajedničkih voditelja?

43. Kako treba urediti odnose sa predstavnikom?

44. Tko je dužan odabrati predstavnika?

Često postavljena pitanja (8)

45. Je li hrvatsko regulatorno tijelo jedino nadležno za pružanje pomoći ispitanicima u pogledu povrede njihovih osobnih podataka u RH?

46. Kako se zovu regulatorna tijela u Francuskoj, Velikoj Britaniji, Italiji i Španjolskoj? Kakav je sustav nadzora u Njemačkoj i Švicarskoj? Gdje će najveći broj platformi imati sjedište – koje će nadzorno tijelo nadzirati najveće platforme?

47. Koje uvjete treba ispuniti prije obrade posebnih kategorija osobnih podataka?

47. Koje sve uvjete treba ispuniti privola? Treba li svaka obrada nužno biti temeljena na privoli? Koja je razlika između privole i izričite privole kao pravnih osnova?

48. Kada smo dužni prijaviti povredu osobnih podataka nadzornom tijelu, a kada ispitaniku/ispitanicima čije podatke obrađujemo?

49. Koje smo podatke i okolnosti dužni prijaviti u prijavi povrede?

50. Kako će teći postupak nakon naše prijave povrede?

Često postavljena pitanja (9)

54. Je li hrvatsko regulatorno tijelo jedino nadležno za pružanje pomoći ispitanicima u pogledu povrede njihovih osobnih podataka u RH?

55. Je li u EU moguće legalno prodavati osobne podatke?

56. Smije li banka obavijestiti drugu instituciju o transakcijama ispitanika, bez da o tome obavijesti samog ispitanika?

57. Treba li porezna uprava notificirati ispitanike da prima njihove osobne podatke od njihovog poslodavca?

Često postavljena pitanja (10)

58. Zbog čega mi voditelj obrade ne želi obrisati podatke koje obrađuje temeljem ugovora o radu, a više nisam njegov zaposlenik?

59. Vaša organizacija putem web stranice prikuplja osobne podatke korisnika. Podaci uključuju ip adrese. Na temelju podataka se kreiraju jedinstveni korisnički profili. Koja je pravna osnova takve obrade?

60. Trebate li privolu za obradu podataka vaših radnika u svrhu isplate plaća?

61. Napravite tablicu podataka koje vaša organizacija prikuplja – za svaku kategoriju podataka označite pravni temelj i rok čuvanja. Postoji li situacija da je primjenjiva više od jedne pravne osnove obrade?

62. Ukoliko je tehnički problem brisati podatke, da li je zadovoljavajuće podatke anonimizirati na primjeren način?

63. Koliko dugo se čuvaju podaci o zaposlenicima? Koliko se dugo čuvaju podaci o njihovim životopisima, o njihovoj naobrazbi?

ZAHVALJUJEMO NA PAŽNJI

PITANJA?

Kontakt:

OPĆA UREDBA O ZAŠTITI PODATAKA U PRAKSI

Praktikum za službenike za zaštitu osobnih podataka


edpb
European Data Protection Board