

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 1 od 24		


## PRAVILNIK O OSOBNIM PODACIMA

Usvojio (datum)	22.5.2018	Uprava: Marko Filipović
Primjenjuje se od	25.5.2018	
Distribucijska lista	Odjel za procjenu rizika i ugovaranje usluge, Odjel prodaje, Odjel za usklađenost i pravne poslove, , Odjel obračuna i namirenja, Odjel informacijske tehnologije, Uprava	


PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 2 od 24		

## Sadržaj

1. Pregled pravilnika .....	4
1.1. Cilj .....	4
1.2. Područje primjene .....	4
1.3. Distribucija .....	4
2. Sukladnost .....	5
3. Definicije .....	5
4. ULOGE I ODGOVORNOSTI.....	6
4.1. Svi Suradnici GPN DATA-e .....	6
4.2. Suradnici zaduženi za odnose s Trećim stranama koje obrađuju EU osobne podatke u GPN DATA-ino ime ili na drugi način imaju pristup EU osobnim podacima.....	7
4.3. Uprava GPN DATA .....	7
4.4. Službenik za zaštitu podataka (“DPO”).....	7
4.4.1. Pozicija službenika za zaštitu podataka.....	7
4.4.2. Zadaće i odgovornosi službenika za zaštitu osobnih podataka .....	7
4.5. Odjel informacijske tehnologije. ....	8
5. GPN DATA-ina načela obrade EU osobnih podataka.....	8
5.1. Zakonitost, pravičnost i transparentnost .....	9
5.2. Ograničavanje svrhe .....	9
5.3. Minimizacija podataka.....	9
5.4. Točnost .....	9
5.5. Ograničavanje pohrane.....	9
5.6. Sigurnost podataka .....	9
5.7. Načela obrade u svojstvu Izvršitelja obrade. ....	9
6. GPN DATA-ini standardi privatnosti sukladno GDPR.....	10
6.1. Obavijesti .....	10
6.1.1. Oblik obavijesti .....	10
6.1.2. Sadržaj obavijesti .....	10
6.1.3. Obavijest nužna za svaku novu svrhu obrade .....	10
6.2. Zakoniti temelji za obradu, uključujući privolu.....	10
6.2.1. Temelji za obradu osobnih podataka .....	10
6.2.2. Privola .....	10
6.3. Prava ispitanika.....	12

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 3 od 24		

6.3.1. Djelovanje po zahtjevima ispitanika .....	12
6.3.2. Verifikacija ispitanika .....	15
6.4. Treće strane .....	16
6.4.1. Upravljanje odnosima s izvršiteljima obrade .....	16
6.4.2. Upravljanje odnosima zajedničkog voditelja obrade .....	16
6.5. Nastupanje u svojstvu Izvršitelja obrade .....	17
6.6. Zaštita podataka razvijena po mjeri .....	17
6.7. Zaštita podataka temeljem zadanih postavki.....	17
6.8. Sigurnost obrade.....	18
6.9. Prekogranični prijenos .....	18
6.10. Povrede EU osobnih podataka .....	19
6.10.1. Općenito o povredama .....	19
6.10.2. Postupanje u slučaju povrede EU osobnih podataka .....	19
6.11. Procjena učinka na zaštitu podataka i prethodne konzultacije .....	19
6.11.1. Procjena je obvezna.....	19
6.11.2. DPIA postupak .....	20
6.11.3. Prethodno savjetovanje s Nadzornim tijelom .....	20
6.12. Vođenje evidencije .....	20
7. Edukacija Suradnika.....	20
8. Upotreba kolačića (cookies). .....	21
10. Mjere zaštite i suradnja .....	21
9. Usklađenost s nacionalnim propisima.....	21
11. Ništetnost pojedinih odredbi .....	21
12. Nadležnost i nadležni sud .....	21
13. Tumačenje .....	22
14. Revizije.....	22
15. Povezani pravilnici .....	22
16. Upit i kontakt podaci .....	22
17. Prethodno savjetovanje i stupanje na snagu .....	22
Dodatak 1 : Sadržaj obavijesti .....	23
Dodatak 2 : Odredbe u ugovorima s izvršiteljima obrade.....	24

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 4 od 24		

Na temelju Opće uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travanja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podakata te o stavljanju izan snage Direktivie 95/46/EZ, Uprava GPN DATA-e d.o.o. 22. svibnja 2018. godine donosi

## PRAVILNIK O OSOBNIM PODACIMA

### 1. Pregled pravilnika

#### 1.1. Cilj

Ovaj Pravilnik usvaja se na temelju Opće uredbe o zaštiti osobnih podataka (GDPR) osiguravanja sukladnosti djelovanja GPN DATA-a sa GDPR-om. Pravilnikom se utvrđuju obavezni opći standardi kojih se zaposlenici i suradnici GPN DATA-e moraju pridržavati pri obradi osobnih podataka ispitanika koji žive u Europskoj Uniji (“**EU osobni podaci**”).


#### 1.2. Područje primjene

Pravilnik se primjenjuje na GPN DATA kada GPN DATA prima, pristupa ili na drugi način obrađuje EU osobne podatke. GPN DATA je također dužan poduzeti korake kako bi osigurao da treće strane kojima GPN DATA dostavlja EU osobne podatke provode svoje aktivnosti u ime GPN DATA-a u skladu s ovim Pravilnikom. Konkretno, Pravilnik se primjenjuje na:

- Sve zaposlenike GPN DATA-a, uključujući stalne i povremene suradnike na osnovi ugovora o djelu ili sličnoj osnovi (zbirno: “**Suradnici**”) koji imaju pristup EU osobnim podacima koje obrađuje GPN DATA ili koji se obrađuju u ime GPN DATA-e; ili koji upravljaju ili na drugi način imaju bilo kakvu odgovornost za obradu EU osobnih podataka;
- Sve aktivnosti koje vodi GPN DATA ili se vode u njegovo ime, a koje uključuju EU osobne podatke, kada GPN DATA nastupa u svojstvu Voditelja obrade;
- Sve aktivnosti koje vodi GPN DATA ili se vode u njegovo ime, a koje uključuju EU osobne podatke, kada GPN DATA nastupa u svojstvu Izvršitelja obrade.

#### 1.3. Distribucija

Pravilnik je dostupan svim Suradnicima na mrežnom poslužitelju (javno dostupnim mapama) i Inetnet stranici GPN DATA-e.

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 5 od 24		

## 2. Sukladnost

Suradnici su odgovorni za poznavanje i postupanje sukladno ovom Pravilniku, kao i za informiranje svojih nadređenih, GPN DATA-e ili GPN DATA-inog službenika za zaštitu EU osobnih podataka o svakoj sumnji na kršenje Pravilnika.

Djelovanje u skladu s ovom Pravilnikom obavezno je za sve GPN DATA- ine Suradnike. Neusklađenost s Pravilnikom mogla bi izložiti GPN DATA-u i Suradnika/e značajnoj građanskoj i/ili kaznenoj odgovornosti, imovinskoj šteti i gubitku ugleda. GPN DATA može, u mjeri u kojoj je to dopušteno primjenjivim propisima, poduzeti disciplinske mjere sve do uključivo s otkazom ili raskidom suradnje zbog kršenja Pravilnika od strane bilo kojeg GPN DATA-inog Suradnika.

## 3. Definicije

**Privola:** Svako dobrovoljno, izričito, informirano i nedvosmisleno iskazivanje želje ispitanika kojom on/ona, bilo izričito ili nedvojbeno potvrdnom radnjom, daje pristanak za obradu osobnih podataka koji se na njega/nju odnose i to za određene svrhe.

**Voditelj obrade:** Fizička ili pravna osoba ili drugo tijelo koje, samo ili zajedno s drugima, određuje svrhe i sredstva obrade osobnih podataka.

**Izvršitelj obrade:** Fizička ili pravna osoba ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.

**Ispitanik:** Fizička ili pravna osoba, identificirana ili čiji se identitet može utvrditi, čiji se osobni podaci obrađuju.

**DPIA:** definirano u članku 6.11.2.

**DPO:** definirano u članku 4.4


**EU osobni podaci:** definirani u članku 1.1.

**Izričita privola:** Privola dobivena po prijedlogu ispitaniku da se suglasi ili ne suglasi s određenom uporabom ili otkrivanjem osobnih podataka, a ispitanik aktivno odgovori na upit, usmeno ili u pisanom obliku (npr. vlastoručnim potpisom, elektronički označavajući okvir u kojem piše "Suglasan sam").

**GDPR:** definirana u članku 1.1.

**Osobni podaci:** Sve informacije koje se odnose na fizičke osobe čiji je identitet utvrđen ili se može utvrditi ("Ispitanik"). Pojedinač čiji se identitet može utvrditi jest pojedinac koji se može identificirati, izravno ili neizravno, prije svega uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili pomoću jedne ili više značajki svojstvenih za fizički, psihološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca.

**Povreda osobnih podataka:** Kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili obrađivani na drugi način.

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 6 od 24		

**Obrada:** Svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim ili neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje.

**Izrada profila:** Svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih značajki povezanih s ispitanikom, posebice za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog ispitanika.

**Rizik za prava i slobode ispitanika:** Obrada osobnih podataka predstavlja rizik za prava i slobode ispitanika gdje takva obrada može rezultirati fizičkom, materijalnom ili nematerijalnom štetom, uključivo:

- ako obrada osobnih podataka može dovesti do diskriminacije, krađe identiteta ili prijevare, financijskog gubitka, štete ugledu, gubitka povjerljivosti osobnih podataka zaštićenih poslovnim tajnom, neovlaštenog obrnutog postupka pseudonimizacije ili bilo koje druge znatne ekonomske ili socijalne štete
- ako ispitanici mogu biti uskraćeni za svoja prava i slobode ili onemogućeni u vršenju kontrole nad svojim osobnim podacima
- pri obradi osjetljivih osobnih podataka
- pri izradi profila tijekom obrade osobnih podataka; pri obradi osobnih podataka ranjivih ispitanika, osobito djece
- kad obrada uključuje veliku količinu osobnih podataka i utječe na velik broj ispitanika

**Osjetljivi osobni podaci:** Posebne kategorije osobnih podataka koji otkrivaju rasno ili etničko podrijetlo ispitanika, njegove/njezine političke stavove, njegova/njezina vjerska ili filozofska uvjerenja ili njegovo/njezino članstvo u sindikatu. Osjetljivi osobni podaci također uključuju genetske podatke, biometrijske podatke u svrhu jedinstvene identifikacije ispitanika, podatke koji se odnose na zdravlje i podatke koji se odnose na spolni život ili seksualnu orijentaciju ispitanika.


**Nadzorna tijela:** Agencija za zaštitu osobnih podataka, Hrvatska Narodna Banka (za potrebe izvješćivanja o značajnom incidentu koji uključuje osobne podatke).

Za potrebe ove Pravilnike "**Treća strana**" označava pojedinca ili tijelo izvan GPN DATA, GPN DATA-inih Suradnika i ispitanika, a kojima GPN DATA prenosi ili omogućava pristup osobnim podacima.

## 4. ULOGE I ODGOVORNOSTI

### 4.1. Svi Suradnici GPN DATA-e

Svi Suradnici GPN DATA-e čije odgovornosti uključuju obradu EU osobnih podataka moraju poznavati i djelovati u skladu s ovim Pravilnikom i odlukama, postupcima i smjernicama koje na polju zaštite osobnih podataka utvrdi Uprava GPN DATA-e te donositi razumne odluke radi zaštite EU osobnih podataka u skladu s navedenim.

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 7 od 24		

## 4.2. Suradnici zaduženi za odnose s Trećim stranama koje obrađuju EU osobne podatke u GPN DATA-ino ime ili na drugi način imaju pristup EU osobnim podacima.

Osim odgovornosti navedenih u članku 4.1 svaki Suradnik čija je primarna odgovornost upravljanje bilo kakvim sadašnjim ili budućim odnosom s izvršiteljem obrade ili bilo kojom drugom Trećom stranom koja ima pristup EU osobnim podacima GPN DATA-inih Suradnika ili klijenata, mora se konzultirati s GPN DATA-inim službenikom za zaštitu osobnih podataka („DPO“) kako bi osigurao da ugovori s takvim trećim stranama sadrže odgovarajuće odredbe o zaštiti podataka. Povrh toga, takvi suradnici odgovorni su za konzultacije s GPN DATA-inim Odjelom informacijske tehnologije radi procjene sigurnosnih mjera koje takve treće strane imaju uvedene za zaštitu EU osobnih podataka.

## 4.3. Uprava GPN DATA

Uprava GPN DATA-e odgovorna je za odluke koje se odnose na obradu EU osobnih podataka i usklađivanje tih odluka s primjenjivim europskim i nacionalnim propisima o zaštiti podataka.

## 4.4. Službenik za zaštitu podataka („DPO“).

Postupajući u svojstvu voditelja obrade, GPN DATA je dužna imenovati službenika za zaštitu osobnih podataka. GPN DATA javno objavljuje kontakt podatke službenik, te ih bez odgode priopćava i nadzornom tijelu.

Pri donošenju odluke o imenovanju službenika za zaštitu osobnih podataka, GPN DATA će voditi računa da imenovana osoba ima odgovarajuća stručna znanja za provedbu svih mjera i aktivnosti za zaštitu osobnih podataka. Službenik mora imati potrebne stručne kvalifikacije, a osobito stručna znanja o pravu i praksama iz područja zaštite osobnih podataka.

GPN DATA može eksternalizirati funkciju službenika za zaštitu podataka.

### 4.4.1. Pozicija službenika za zaštitu podataka

Službenik za zaštitu osobnih podataka samostalan je i neovisan u svome radu koji će sukladno ovlaštenjima poduzimati sve potrebne aktivnosti i mjere kako bi se osigurala usklađenost poslovanja GPN DATA s propisima o zaštiti osobnih podataka.

Službenik za zaštitu osobnih podataka za svoje rad odgovara Upavi GPN DATA-e.


GPN DATA osigurava da sve organizacijske jedinice budu upoznate s ulogom Službenika za zaštitu osobnih podataka, te s važnošću obavještanja službenika o zahtjevima za ostvarivanjem prava ispitanika, povredama osobnih podataka, novim vrstama obrade, namjeravanjoj upotrebi novih tehnologija i sl.

### 4.4.2. Zadaće i odgovornosti službenika za zaštitu osobnih podataka

Službenik za zaštitu osobnih podataka svoje dužnosti dužan je obavljati osobno, uredno i savjesno.

Službenik za zaštitu osobnih podataka odgovoran je za provođenje svih mjera i aktivnosti usmjerenih na ostvarivanje ciljeva politike zaštite privatnosti i osobnih podataka GPN DATA-e, provedbu zakonskih, podzakonskih i drugih obvezujućih akata na području zaštite osobnih podataka.

Obveze i zadaće službenika za zaštitu osobnih podataka uključuje sljedeće „DPO“:

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 8 od 24		

- obavještanje i savjetovanje Uprave GPN DATA i GPN DATA-inih Suradnika koji provode aktivnosti obrade EU osobnih podataka o njihovim obvezama prema GDPR
- nadzire usklađenost s GDPR i drugim primjenjivim propisima o zaštiti podataka i ovom Pravilnikom
- jača svijest o GDPR, drugim primjenjivim regulativama EU i država članica EU o zaštiti podataka i ovom Pravilniku te savjetuje i educira GPN DATA-ine Suradnike koji sudjeluju u obradi EU osobnih podataka
- daje preporuke za izmjene i dopune Pravilnika i svih drugih povezanih akata ili postupaka kada je to prikladno
- odgovara na upite Suradnika, klijenata i trećih strana o GDPR i Pravilniku te surađuje s nadzornim tijelima
- pruža savjete u odnosu na procjene učinaka zaštite podataka (DPIA) i obavlja prethodne konzultacije
- vodi propisane evidencije koje se odnose na obradu EU osobnih podataka od strane GPN DATA-e
- savjetuje o odgovarajućim odredbama u vezi zaštite podataka koje treba uključiti u ugovore s trećim stranama koje obrađuju EU osobne podatke u ime GPN DATA-a
- vrši svaku drugu ulogu službenika za zaštitu podataka zahtijevanu po GDPR ili drugim propisima o zaštiti podataka odnosno, kada je to prikladno, uz suglasnost Uprave imenuje drugog GPN DATA-inog Suradnika da vrši neke od zahtijevanih poslova.

O svim uočenim neusklađenostima na području zaštite osobnih podataka Službenik za zaštitu osobnih podataka upozorava Upravu GPN DATA-e. Uprava GPN DATA-e odlučuje o mjerama koje će se poduzeti kako bi se otklonile eventualne neusklađenosti.

Službenik je dužan trajno čuvati povjerljivost svih informacija i osobnih podataka koje je saznao vezano uz obnašanje svoje funkcije.

Kontakt podaci Službenika za zaštitu osobnih podataka dostupni su na internet stranici GPN DATA.

#### **4.5. Odjel informacijske tehnologije.**


Odjel informacijske tehnologije odgovoran je za praćenje stanja informacijske sigurnosti GPN DATA-e, izvještavanje Uprave i DPO o stanju informacijske sigurnosti, odrednicama informacijske sigurnosti, mogućim poboljšanjima informacijske sigurnosti, savjetuje i, po odobrenju Uprave i uz savjetovanje sa DPO provodi implementaciju novih sigurnosnih rješenja kojima se osigurava odgovarajuća razina sigurnosti s obzirom na rizik, uključujući prema potrebi 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 i proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti sigurnosnih mjera za osiguravanje sigurnosti obrade.

Odjel Informacijskih tehnologija u svom radu koristi se sukladno propisanim internim pravilnicima i procedurama, a u svrhu ispunjavanja prijašnje navedenog.

### **5. GPN DATA-ina načela obrade EU osobnih podataka**

GPN DATA je predan provedbi svih aktivnosti obrade EU osobnih podataka u skladu s GDPR, uključivo sa sljedećim načelima obrade EU osobnih podataka:



PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 9 od 24		

## 5.1. Zakonitost, pravičnost i transparentnost

GPN DATA će obrađivati EU osobne podatke na zakonit i pravičan način koji je transparentan za ispitanika.

## 5.2. Ograničavanje svrhe

GPN DATA će prikupljati EU osobne podatke u određene, jasne i zakonite svrhe. GPN DATA neće dalje obrađivati EU osobne podatke na bilo koji način koji nije u skladu s takvim svrhama.

## 5.3. Minimizacija podataka

GPN DATA će prikupljati i zadržavati samo one EU osobne podatke koji su dostatni, relevantni i ograničeni samo na ono što je neophodno za ispunjavanje svrhe u koju se takvi podaci obrađuju.

## 5.4. Točnost

GPN DATA će osigurati da su EU osobni podaci točni i, kada je to potrebno, ažurirani. GPN DATA će poduzeti svaki razuman korak kako bi osigurao ispravak te brisanje sukladno točki 5.5., bez odgode, EU osobnih podataka koji su netočni, vodeći računa o svrsi u koju se takvi podaci obrađuju.

## 5.5. Ograničavanje pohrane

GPN DATA će zadržati EU osobne podatke u obliku koji omogućava identificiranje ispitanika ne duže no što je to potrebno za ispunjavanje svrhe u koju GPN DATA obrađuje takve podatke, uključujući ne samo poslovne svrhe, već i svrhe koje se odnose na ispunjavanje GPN DATA-inih zakonskih obveza kao što su zakonska dužnost držanja podataka koji se odnose na:


- sudske postupke u tijeku ili one koji se razumno mogu očekivati
- postupanje u skladu sa sudskim nalogom ili sudskim pozivom

## 5.6. Sigurnost podataka

GPN DATA će EU osobne podatke obrađivati na siguran način. Tijekom trajanja obrade i/ili pohrane zaštitit će EU osobne podatke od neovlaštene ili nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja, koristeći odgovarajuće razumne tehničke, te organizacijske mjere.

## 5.7. Načela obrade u svojstvu Izvršitelja obrade.

Kada GPN DATA nastupa u svojstvu Izvršitelja obrade osobnih podataka, GPN DATA će načela ovog članka 5. Pravilnika provoditi sukladno obvezama propisanim GDPR-om za Izvršitelja obrade i sukladno zakonitim uputama odnosno voditelja obrade.

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 10 od 24		

## 6. GPN DATA-ini standardi privatnosti sukladno GDPR

U cilju osiguravanja sukladnosti s načelima obrade EU osobnih podataka, GPN DATA je usvojio sljedeće standarde koji uređuju njegovu obradu EU osobnih podataka:

### 6.1. Obavijesti

Tijekom ili uoči prikupljanja EU osobnih podataka GPN DATA će obavijestiti ispitanike o GPN DATA-inom prikupljanju i obradi EU osobnih podataka.

#### 6.1.1. Oblik obavijesti

GPN DATA će osigurati da obavijesti budu sažete, transparentne, razumljive (tj. jasnog i jednostavnog izričaja), i lako dostupne putem Internet stranice GPN DATA-e.

#### 6.1.2. Sadržaj obavijesti

GPN DATA će u obavijestima osigurati u najmanju ruku informacije koje se odnose na GPN DATA-inu obradu EU osobnih podataka kako je to navedeno u [Dodatku 1](#) ovog Pravilnika.

#### 6.1.3. Obavijest nužna za svaku novu svrhu obrade

Prije svake obrade EU osobnih podataka u bilo koju svrhu, a koja se ne spominje u prethodnim GPN DATA-inim obavijestima, Suradnici GPN DATA-e moraju se savjetovati sa Službenikom za zaštitu osobnih podataka koji će im pomoći pri izradi i davanju ažurirane obavijesti ispitanicima zahtijevane po GDPR-u prije svake obrade EU osobnih podataka u nove svrhe.

## 6.2. Zakoniti temelji za obradu, uključujući privolu

### 6.2.1. Temelji za obradu osobnih podataka

Prije svake obrade EU osobnih podataka GPN DATA će utvrditi postojanje zakonitog temelja za obradu EU osobnih podataka prema GDPR-u.


DPO je odgovoran za potvrđivanje da se takav zakonski temelj utvrdio prije no što GPN DATA pokrene predložene aktivnosti obrade EU osobnih podataka.

### 6.2.2. Privola

#### 6.2.2.1. Metode dobivanje privole

##### 6.2.2.1.1. Općenito

Kada se oslanja na privolu kao zakonitu osnovu za obradu, GPN DATA će ishoditi pristanak koji je dan:

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 11 od 24		

- dobrovoljno (tj. ispitanik ima istinski slobodan izbor i ne postoji “očigledna neravnoteža” između GPN DATA-e i ispitanika)
- koji je određen, informiran, nedvosmislen (tj. izražen izjavom ili jasnom potvrdnom radnjom, poput označavanja odgovarajućeg okvira na web stranici)
- dobiven od ispitanika prije no što obrada započne
- koji je moguće razlikovati od drugih informacija

#### **6.2.2.1.2. Izričita privola**

Kada se GPN DATA oslanja na privolu kako bi legitimizirao obradu osjetljivih EU osobnih podataka, GPN DATA će od ispitanika ishoditi izričitu privolu.

#### **6.2.2.3. Povlačenje privole**

GPN DATA će dozvoliti ispitanicima da u svakom trenutku povuku privolu. Pri tome će ispitaniku povlačenje privole učiniti jednako jednostavnim kao i njezino davanje.

GPN DATA će se oslanjati na privolu samo ako ne postoji druga, prikladnija pravna osnova za obradu EU osobnih podataka. Privola može predstavljati pravni temelj za obradu EU osobnih podataka jedino ako je njezino davanje uistinu dobrovoljno i ako je ispitanik može uskratiti bez snošenja štetnih posljedica.

#### **6.2.2.4. Izražavanje privole**

Kada se oslanja na privolu kao zakoniti temelj za obradu GPN DATA će zadržati dokaz da je ispitanik dao privolu za obradu njegovih/njezinih EU osobnih podataka kako je to bilo prethodno navedeno.

#### **6.2.2.5. Osobni podaci djece**

GPN DATA djeci mlađoj od 16 godina trenutačno ne nudi nikakve online usluge niti svjesno prikuplja bilo kakve EU osobne podatke od bilo kojeg djeteta mlađeg od 16 godina. Ukoliko GPN DATA ponudi bilo kakvu online uslugu djeci mlađoj od 16 godina ili svjesno prikupi bilo kakve EU osobne podatke od djece mlađe od 16 godina, GPN DATA će to učiniti uz pristanak roditelja u skladu s uvjetima navedenima u GDPR.


#### **6.2.2.6. Obrada osobnih podataka u svrhu izravnog marketinga**

Može se smatrati da postoji legitimni interes GPN DATA-e za obradu osobnih podataka za svrhu izravnog marketinga. Pritom se treba raditi o osobnim podacima koje je GPN DATA prije toga zakonito prikupila, a upotreba podataka u svrhu izravnog marketinga mora biti u okvirima onoga što ispitanik razumno može očekivati temeljem svoga odnosa s GPN DATA-om kao voditeljem obrade.

U protivnom, obrada osobnih podataka može se temeljiti samo na privoli ispitanika.

Ako se za potrebe izravnog marketinga, osobni podaci obrađuju temeljem legitimnog interesa GPN DATA-e, ispitanik u svakom trenutku ima pravo prigovoriti takvoj obradi osobnih podataka, što uključuje izradu profila. Najkasnije u trenutku prve komunikacije s ispitanikom, ispitanika se na ovo pravo upozorava na jasan i transparentan način, odvojeno od bilo koje druge informacije.

Ako se ispitanik usprostavi obradi za potrebe izravnog marketinga, GPN DATA više ne smije obrađivati njegove osobne podatke u takve svrhe.

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 12 od 24		

## 6.3. Prava ispitanika

### 6.3.1. Djelovanje po zahtjevima ispitanika

GPN DATA će omogućiti ostvarivanje sljedećih prava ispitanika:

#### 6.3.1.1. Pravo ispitanika na pristup njihovim EU osobnim podacima

Ispitanik ima pravo od GPN DATA-e dobiti potvrdu obrađuju li se EU osobni podaci koje se odnose na njega te, ako se takvi podaci obrađuju, ima pravo na pristup EU osobnim podacima i sljedeće informacije:

- svrsi obrade
- kategorijama njihovih EU osobnih podataka koji se obrađuju
- primateljima ili kategorijama primatelja kojima je GPN DATA otkrio ili će otkriti njihove EU osobne podatke, uključivo s primateljima u trećim zemljama ili međunarodnim organizacijama
- predviđeno razdoblje tijekom kojeg će GPN DATA čuvati njihove EU osobne podatke (ili kriterije korištene za utvrđivanje tog razdoblja)
- postojanje prava da zatraže brisanje ili ispravak;
- da zatraže ograničavanje obrade njihovih EU osobnih podataka
- te da izjave prigovor na obradu
- pravo ispitanika na podnošenje prigovora Agenciji za zaštitu osobnih podataka
- izvor njihovih podataka (ukoliko GPN DATA nije prikupio podatke izravno od ispitanika);
- i
- postojanje svakog automatskog odlučivanja, uključujući izradu profila, koje ima značajan utjecaj na ispitanika, i objašnjavanje logike kao i značenja i mogućih posljedica takve izrade profila za ispitanika.

Nakon primitka zahtjeva za pristup osobnim podacima, GPN DATA će ispitaniku u pisanom obliku dati gore navedene informacije, odnosno informacije koje je ispitanik tražio.

GPN DATA će osigurati kopiju osobnih podataka koji se obrađuju, te pravo na dobivanje predmetnih kopija ne smije negativno utjecati na prava i slobode drugih.


#### 6.3.1.2. Pravo ispitanika na ispravljanje netočnih EU osobnih podataka

Ispitanik ima pravo bez nepotrebnog odgađanja ishoditi od GPN DATA-e ispravak netočnih osobnih podataka koji se na njega odnose. Uzimajući u obzir svrhu obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke.

Kad je primjereno okolnostima, GPN DATA će od ispitanika tražiti da dokaže utemeljenost svog zahtjeva predloženjem vjerodostojnog dokaza.

#### 6.3.1.3. Pravo ispitanika na brisanje EU osobnih podataka

Ispitanik ima pravo od GPN DATA ishoditi brisanje osobnih podataka koji se na njega ne odnose bez nepotrebnog odgađanja, te GPN DATA ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako je ispunjen jedan od sljedećih uvjeta:

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 13 od 24		

- njihovi EU osobni podaci više nisu potrebni u svrhe za koje su takvi podaci prikupljeni ili obrađeni na drugi način
- zakoniti temelj za obradu jest privola - ukoliko ispitanik povuče takvu privolu, a ne postoji drugi zakoniti temelj
- ispitanik iskoristi svoje pravo na prigovor, a GPN DATA nema važnije legitimne temelje za nastavak obrade
- su njihovi EU osobni podaci nezakoniti obrađeni
- su njihovi EU osobni podaci prikupljeni u vezi s ponudom usluga informacijskog društva (tj. *online usluga*)
- brisanje je nužno radi postupanja u skladu s zakonskim propisima EU ili država članica

Pravo na brisanje ne primjenjuje ukoliko GPN DATA mora nastaviti s obradom EU osobnih podataka ispitanika radi postupanja sukladno zakonima EU ili država članica ili da bi utvrdio, koristio ili branio zakonska prava GPN DATA-e.

#### 6.3.1.4. Pravo ispitanika na ograničavanje obrade EU osobnih podataka

Ispitanika ima pravo ishoditi ograničenje obrade EU osobnih podataka u slučaju da:

- ispitanik osporava točnost EU osobnih podataka (u tom će slučaju obrada biti ograničena na razdoblje potrebno da se GPN DATA-i omogući provjera točnosti EU osobnih podataka)
- obrada je nezakonita, pa ispitanik umjesto brisanja zahtijeva ograničavanje uporabe njegovih/njezinih podataka
- GPN DATA više ne treba podatke u izvorne svrhe, no podaci su i dalje potrebni kako bi utvrdio, koristio ili branio svoja zakonska prava
- ispitanik je uložio prigovor na obradu i GPN DATA provjerava jesu li njegovi zakonski temelji za obradu podataka nadređeni interesima, pravima i slobodama na koje se ispitanik poziva.

GPN DATA će ispitanika koji je ishodio ograničenje obrade obavijestiti prije nego što ograničenje obrade bude ukinuto.


GPN DATA priopćava svaki ispravak ili brisanje osobnih podataka ili ograničavanje obrade svakom primatelju kojem su otkriveni osobni podaci, osim ako se to pokaže nemogućim ili zahtijeva nerazmjern npr. GPN DATA će obavijestiti ispitanika o tim primateljima ako to ispitanik zatraži.

#### 6.3.1.5. Pravo ispitanika na prenosivost podataka

Ispitanika ima pravo na prenosivost podataka (odnosno pravo na dobivanje primjerka EU osobnih podataka u uobičajenom, elektronički čitljivom obliku te na prijenos njihovih EU osobnih podataka s jednog voditelja obrade na drugog ili vršenje prijenosa podataka izravno između voditelja obrade) ukoliko se obrada vrši na automatizirani način, te ukoliko pravni temelj za obradu čini ili privola ili ispunjenje ugovora u kojem je ispitanik ugovorna strana ili ukoliko se obrada vrši u svrhu poduzimanja mjera na zahtjev ispitanika prije sklapanja ugovora.

#### 6.3.1.6. Pravo ispitanika na prigovor na obradu EU osobnih podataka

Ispitanika ima pravo na prigovor na obradu EU osobnih podataka koji se odnose na njega, uključivo s izradom profila, na temelju legitimnih interesa GPN DATA-a ili treće strane ili za izvršenje zadaće koja se vrši u javnom interesu.

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 14 od 24		

GPN DATA nakon takovog prigovora ispitanika više ne smije obrađivati osobne podatke. Iznimno, GPN DATA može i dalje obrađivati osobne podatke ako dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika, i/ili radi postavljanja, ostvarivanja, te obrane pravnih zahtjeva. Dokazivanje okolnosti koje GPN DATA-i omogućuju daljnju obradu mora biti dokumentirano u pisanom obliku.

### **6.3.1.7. Pravo ispitanika na prigovor na obradu njihovih EU osobnih podataka u svrhu izravnog marketinga**

Ako se EU osobni podaci obrađuju za potrebe izravnog marketinga, ispitanik u svakom trenutku ima pravo uložiti prigovor na obradu osobnih podataka za potrebe izravnog marketinga, kao i na izradu profila u mjeri koja je povezana s takvim izravnim marketingom. Uloži li ispitanik prigovor, GPN DATA više ne smije obrađivati osobne podatke u svrhu izravnog marketinga.

### **6.3.1.8. Pravo ispitanika na prigovor na obradu njihovih EU osobnih podataka u znanstvene i u statističke svrhe**

Ispitanika ima pravo na prigovor na obradu njihovih EU osobnih podataka u znanstvene i u statističke svrhe, osim ako je obrada potrebna za izvršenje zadaće koja se vrši iz razloga javnog interesa.

### **6.3.1.9. Pravo ispitanika da ne bude podvrgnut odluci koja na njega značajno utječe utemeljene isključivo na automatiziranoj obradi (uključivo s izradom profila)**

Ispitanika ima pravo da ne bude podvrgnut odluci koja na njega značajno utječe utemeljena isključivo na automatiziranoj obradi (uključivo s izradom profila), osim ako je takva obrada:


- neophodna za sklapanje ili izvršavanje ugovora s ispitanikom i postoje odgovarajuće zaštitne mjere
- obrada je dopuštena prema zakonskim propisima EU ili države članice koji se primjenjuju na GPN DATA i koji propisuju odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa ispitanika
- ispitanik dao izričitu privolu za takvu obradu i postoje odgovarajuće zaštitne mjere.

### **6.3.1.10. Pravo ispitanika na podnošenje prigovora Agenciji za zaštitu osobnih podataka**

Ispitanik u svako doba ima pravo podnijeti prigovor nadzornom tijelu vezano za obradu osobnih podataka.

Nadzorno tijelo je Agencija za zaštitu osobnih podataka

Martićeve ulica 14  
10 000 Zagreb, Hrvatska  
[www.azop.hr](http://www.azop.hr)

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 15 od 24		

### 6.3.1.11. Ostvarivanje prava

Ispitanik ima pravo u svakom trenutku zahtijevati realizaciju bilo kojeg od gore navednih prava. Komunikacija s ispitanikom treba biti u skladu s zahtjevima ispitanika kad god je to moguće (npr. putem e-maila, faksa ili u pisanom obliku putem pošte).

Suradnici moraju odmah obavijestiti DPO ukoliko zaprime neki zahtjev ispitanika putem bilo kojeg kanala, te se savjetovati o odgovarajućem postupanju.

U situacijama kada ostvarivanje prava podnosi osoba koja nije fizički pristuna, GPN DATA može prije postupanja po zahtjevu od podnositelja tražiti pružanje dodatnih informacija radi provjere njegovog identiteta.

GPN DATA ne smije odbiti dostaviti odgovor na zahtjev ispitanik za ostvarivanje njegovih prava.

GPN DATA će ispitaniku pružiti odgovor na poneseni zahtjev, bez odgađanja, a najkasnije u roku od mjesec dana od primanja zahtjeva.

Ovaj rok se može produžiti za još dva mjeseca, uzimajući u obzir složenost i broj zahtjeva.

U slučaju produljenja roka, GPN DATA će obavijestiti ispitanika u roku od mjesec dana od primanja zahtjeva, te će navesti razloge za produženje.

Ako GPN DATA ne postupi po zahtjevima ispitanika, bez odgađanja, a najkasnije jedan mjesec od primitka zahtjeva, izvješćuje ispitanika o razlozima zbog kojih nije postupila po zahtjevu, te o mogućnosti podnošenja prigovora nadzornom tijelu i traženja pravnog lijeka.

GPN DATA navedne informacije pruža bez naknade, ali ako su zahtjevi ispitanika očito neutemeljeni ili pretjerani, osobito zbog njihovog učestalog ponavljanja, GPN DATA može:

- naplatiti razumnu naknadu uzimajući u obzir administrativne troškove pružanja informacija ili obavijesti ili postupanja po zahtjevu, u kojem će slučaju GPN DATA iznos troška pripočiti ispitaniku, te postupiti po zahtjevu tek nakon što ispitanik pristane snositi trošak ili
- odbiti postupiti po zahtjevu

### 6.3.1.12. Evidencija primljenih zahtjeva

Službenik za zaštitu osobnih podataka vodi evidenciju u kojoj će biti sadržani svi primljeni zahtjevi ispitanika, odgovori na zahtjeve, po potrebi, interna izvješća o provedenim istragama i slična dokumentacija vezana uz pojedini zahtjev ispitanika.


Ova evidencija vodi se u elektroničkom obliku. Evidencija se vodi kronološki, na način da se svakom primljenom zahtjevu ispitanika može pružiti odgovor na njega i ostala prateća dokumentacija.

Iz evidencije mora biti vidljivo da se poštuju rokovi za postupanje po zahtjevu, te ova evidencija mora biti dostupna nadzornom tijelu na zahtjev.

## 6.3.2. Verifikacija ispitanika

GPN DATA će uložiti sve razumne napore kako bi provjerio identitet ispitanika prije no što ispitanicima osigura pristup EU osobnim podacima ili udovolji drugim zahtjevima ispitanika.

Ukoliko GPN DATA ima razumne dvojbe u pogledu identiteta osobe koja podnosi bilo kakav zahtjev kao ispitanik, GPN DATA može zatražiti dodatne informacije u vidu važećeg identifikacijskog dokumenta, sukladno zakonu o sprječavanju pranja novca i drugim pozitivnim propisima kako bi potvrdio identitet, te osobe.

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 16 od 24		

Ukoliko GPN DATA ne može potvrditi identitet osobe koja podnosi zahtjev kao ispitanik, GPN DATA neće odgovoriti na takav zahtjev ispitanika.

## 6.4. Treće strane

### 6.4.1. Upravljanje odnosima s izvršiteljima obrade

GPN DATA će koristiti samo one izvršitelje obrade koji jamče primjenu odgovarajućih tehničkih i organizacijskih mjera potrebnih za usklađivanje s GDPR i osiguravanje zaštite prava ispitanika.

GPN DATA će sklopiti ugovore u pisanom obliku s izvršiteljima obrade u kojima će se utvrditi predmet i trajanje obrade, prirodu i svrhu obrade, vrstu EU osobnih podataka koji se obrađuju, kategorije ispitanika, te obveze i prava GPN DATA-e kao voditelja obrade.

Ovisno o okolnostima slučaja, GPN DATA može prije angažiranja određenog izvršitelja obrade izvršiti provjere koje smatra razumnim i prikladnim, kao na primjer:

- tražiti informacije je li izvršitelj obrade imenovao službenika za zaštitu osobnih podataka
- tražiti informacije o tome angažira li izvršitelj obrade pod-izvršitelje, koga sve i u kojim se zemljama nalaze
- provjeriti s izvršiteljem vodi li se evidencija o aktivnostima obrade
- provjeriti s izvršiteljima postojanje internih politika, pravilnika, te procedura glede zaštite osobnih podataka
- obaviti razgovore o načinu na koji su organizirani relevantni podaci izvršitelja obrade
- tražiti informacije ima li izvršitelj obrade certifikat da je usklađen s GDPR-om (certifikacija nije obvezna, ali je korisno navesti ako je ima)
- tražiti informacije ima li izvršitelj kakve ISO certifikate na području IT sigurnosti
- posjetiti poslovne prostorije izvršitelja obrade
- ako se radi o izvršitelju obrade s kojim GPN DATA surađuje već duži niz godina, u obzir se može uzeti njihova savjesnost i urednost u dosadašnjem izvršavanju ugovornih obveza
- druge razumne provjere

GPN DATA će u pravilu izbjegavati suradnju s izvršiteljima obrade kod kojih bi trebalo doći do prijenosa osobnih podataka u treće zemlje (izvan EU). Do suradnje s takvim izvršiteljima može doći ako su primijenjene odgovarajuće zaštite mjere sukladno poglavlju V. Opće uredbe o zaštiti osobnih podataka.


GPN DATA-ini ugovori s izvršiteljima obrade uključivat će najmanje odredbe koje su navedene u Dodatku 2 ovog Pravilnika.

### 6.4.2. Upravljanje odnosima zajedničkog voditelja obrade

Kada GPN DATA i jedna ili više osoba zajednički odrede svrhe i načine obrade, GPN DATA će s takvim zajedničkim voditeljima obrade zaključiti ugovor kojim se raspoređuju odgovornosti za postupanje sukladno pravilima o zaštiti podatka između voditelja obrade.

GPN DATA će ili pripremiti sažetak obavijesti za ispitanike ili će ugovorom utvrditi da je jedan od voditelja s kojim zajednički vodi obradu pripremio takav sažetak.



PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 17 od 24		

## 6.5. Nastupanje u svojstvu Izvršitelja obrade

Kada nastupa u svojstvu Izvršitelja obrade, GPN DATA će postupati sukladno odredbama GDPR-a i nacionalnog zakonodavstva u mjeri u kojem su istim propisane obveze za Izvršitelja obrade i sukladno dokumentiranim uputama odnosno voditelja obrade.

Prije početka ili prilikom pružanja usluga koje uključuju obradu EU osobnih podataka za odnosnog voditelja obrade, GPN DATA će provjeriti, potvrditi i prema potrebi pružiti odgovarajuće dokaze ispunjenja tehničkih i organizacijskih mjera zaštite potrebnih radi osiguranja odgovarajuće razine zaštite prava ispitanika.

Prije početka pružanja usluga obrade za odnosnog voditelja obrade, GPN DATA će zaposlenike uključene u odnosnu obradu upozoriti na činjenicu da se obrada vrši za odnosnog voditelja obrade i isključivo u skladu s njegovim dokumentiranim uputama, te osigurati odgovarajuće evidentiranje dokumentacije o uputama i poslovima obrade.

Sa svakim voditeljem obrade kojem GPN DATA pruža usluge koje uključuju obradu EU osobnih podataka, GPN DATA će sklopiti ugovor koji će sadržavati odredbe o:

- predmetu i trajanju obrade, prirodi i svrsi obrade
- vrsti EU osobnih podataka koji se obrađuju
- kategoriji ispitanika
- obveze i prava GPN DATA-e kao voditelja obrade sukladne GDPR-u i pobliže navedene u Dodatku 2 ovom Pravilniku, koji se primjenjuje na odgovarajući način.

## 6.6. Zaštita podataka razvijena po mjeri

GPN DATA će provoditi zaštitu podataka razvijenu po mjeri pri razvoju i provedbi novih aktivnosti obrade, uključivo s novim proizvodima ili uslugama koji će obrađivati EU osobne podatke.

GPN DATA će primijeniti odgovarajuće tehničke i organizacijske mjere razvijene u svrhu provedbe načela zaštite podataka (npr. minimizacija podataka) na djelotvoran način.


GPN DATA će također u svoje aktivnosti obrade uključiti potrebne zaštitne mjere kako bi ispunio zahtjeve po GDPR i zaštitio prava ispitanika.

Pri primjeni zaštite podataka razvijene po mjeri GPN DATA će u cilju osiguravanja razine sigurnosti koja odgovara riziku uzeti u obzir sljedeće:

- tehničke mogućnosti
- troškove primjene
- prirodu, područje primjene, kontekst i svrhu obrade, te
- rizik da obrada ima negativan utjecaj na prava i slobode pojedinaca, vodeći računa i o izglednosti nastale štete i o njezinoj mogućoj ozbiljnosti.

## 6.7. Zaštita podataka temeljem zadanih postavki

GPN DATA će primijeniti odgovarajuće tehničke i organizacijske mjere kako bi osigurao da, na temelju zadanih postavki, obrađuje samo one EU osobne podatke koji su potrebni za svaku pojedinu svrhu

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 18 od 24		

obrade.

GPN DATA će provoditi zaštitu podataka po zadanim načelima uz primjenu tehnike minimiziranja podataka kako bi pomogao osigurati da:

- GPN DATA prikuplja samo one EU osobne podatke koji su potrebni da bi se ispunile pojedine svrhe obrade
- EU osobne podatke obrađuje samo u te svrhe
- zadržava EU osobne podatke samo onoliko dugo koliko je potrebno za ispunjavanje pojedine svrhe obrade ili kako bi se ispunile druge zakonske obveze u EU ili državama članicama EU
- pristup EU osobnim podacima dopusti samo osobama kojima je takav pristup potreban radi ispunjavanja specifičnih svrha obrade

## 6.8. Sigurnost obrade

Za svaku svoju aktivnost obrade EU osobnih podataka GPN DATA će primijeniti odgovarajuće i razumne tehničke i organizacijske mjere potrebne za osiguravanje odgovarajuće razine sigurnosti, vodeći računa o sljedećim čimbenicima:


- tehničkim mogućnostima
- troškovima primjene
- prirodi, opsegu, kontekstu i svrsi obrade
- riziku da obrada negativno utječe na prava i slobode pojedinaca, vodeći računa kako o izglednosti nastanka štete tako i o njezinoj mogućoj ozbiljnosti

## 6.9. Prekogranični prijenos

GPN DATA će dozvoliti prekogranični prijenos EU osobnih podataka pojedincu ili tijelu u zemlji koja je izvan EU samo ako je:

- Europska Komisija ocijenila da treća zemlja, teritorij unutar treće zemlje, područje unutar treće zemlje ili međunarodna organizacija kamo GPN DATA prenosi EU osobne podatke osigurava odgovarajuću razinu zaštite (npr. Kanada, Švicarska, savezne države SAD koje sudjeluju u EU-SAD Štitu privatnosti)
- GPN DATA primijenio zakonom dopušten mehanizam prijenosa podataka (npr. standardne ugovorne odredbe usvojene od strane Europske Komisije; obvezujuća korporativna pravila; odobreni kodeks ponašanja, zajedno s obvezujućim i izvršivim obvezama za osiguravanje odgovarajućih zaštitnih mjera); ili
- Na temelju iznimaka ili odricanja (npr. izričita privola ispitanika dana nakon što su obaviješteni o mogućim rizicima prijenosa)

U slučaju postojanja sumnje na prijenos osobnih podataka u zemlju koja ne osigurava adekvatnu razinu zaštite, GPN DATA će prethodno tražiti savjet i mišljenje Službenika za zaštitu osobnih podataka.

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 19 od 24		

## 6.10. Povrede EU osobnih podataka

### 6.10.1. Općenito o povredama

Unatoč odgovarajućim mjerama zaštite osobnih podataka koje GPN DATA poduzima kako bi se spriječile povrede osobnih podataka, nije isključena mogućnost da ipak dođe do povrede osobnih podataka.

Pored mjera zaštite koje bi trebale osigurati da do povrede ne dođe, GPN DATA poduzima i tehničke mjere kojima je cilj otkriti je li do povrede došlo.

Pored osobnih podataka GPN DATA može imati niz štetnih posljedica za ispitanike, te stoga je od iznimne važnosti da GPN DATA na povrede što prije reagira.

Povreda osobnih podataka znači kršenje sigurnosti koje dovode do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

O uništenju osobnih podataka - riječ je kada osobni podaci više ne postoje ili ne postoje u obliku u kojem su GPN DATA-i potrebni za svrhu u koje ih se obrađuje.

O gubitku je riječ kada osobni podaci postoje, ali je GPN DATA izgubila kontrolu nad njima ili mogućnost pristupa, ili podaci na drugi način više nisu u posjedu GPN DATA-e. Gubitak može biti privremenog ili trajnog karaktera.

O izmjeni je riječ kada zbog promjena izvršenih na njima osobni podaci više nisu potpuni, točni ili ažurni.

O neovlaštenom otkrivanju ili pristupu osobnim podacima radi se kada je došlo do njihovog otkrivanja osobama koje za to nisu ovlaštene.

### 6.10.2. Postupanje u slučaju povrede EU osobnih podataka

GPN DATA će imenovati Tim za reakciju i postupanje u slučaju incidenata (*Incident Response Team*) koji će se sastojati od Člana uprave, Službenika za zaštitu podataka, voditelja IT odjela i Voditelja odjela u kojem se dogodio incident te će reagirati na povredu EU osobnih podataka u skladu sa svojim Planom postupanja u slučaju incidenata (u daljnjem tekstu: Plan) i svojim obvezama prema GDPR i drugim mjerodavnim propisima, uz odgovarajuće pravovremeno obavještanje Nadležnih tijela.


Tim za reakciju i postupanje u slučaju incidenta (*Incident Response Team*) utvrditi će sve potrebne činjenice i okolnosti te će donijeti potrebni Plan.

## 6.11. Procjena učinka na zaštitu podataka i prethodne konzultacije

### 6.11.1. Procjena je obvezna

U slučaju kad GPN DATA želi provesti novu aktivnost obrade, posebice aktivnost koja uključuje nove tehnologije i za koju je izgledno da može rezultirati visokim rizikom za prava i slobode pojedinaca, GPN DATA će prije takve aktivnosti obrade provesti procjenu učinka na zaštitu podataka ("DPIA").

GPN DATA će razmotriti narav, opseg, kontekst i svrhe obrade kako bi procijenio utjecaj mogućih novih aktivnosti obrade na zaštitu EU osobnih podataka.

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 20 od 24		

GPN DATA će provesti DPIA postupak ako njegove aktivnosti obrade uključuju bilo što od sljedećeg:

- sustavnu, opsežnu procjenu osobnih značajki ispitanika koja se temelji na automatiziranoj obradi, uključivo s izradom profila, na temelju koje GPN DATA donosi odluke koje proizvode pravne učinke u odnosu na takve ispitanike ili na drugi način značajno utječu na takve ispitanike
- opsežnu obradu osjetljivih EU osobnih podataka ili obradu EU osobnih podataka u vezi s kaznenim osudama ili kaznenim djelima
- sustavno praćenje velikih razmjera javno dostupnog područja
- druge obrade koje bi prouzročile visok rizik za prava i slobode pojedinaca
- svaku drugu aktivnost obrade za koju Agencija za zaštitu osobnih podataka zahtjeva provedbu DPIA.

U izradu procjene učinka aktivno sudjeluje Službenik za zaštitu osobnih podataka. Ako je u obradu uključen ili treba biti uključen Izvršitelj obrade i/ili zajednički Voditelj, GPN DATA može tražiti pomoć od potonjih pri izradi procjene učinika.

### 6.11.2. DPIA postupak

GPN DATA će provesti i primijeniti svoj DPIA postupak i preglede DPIA postupaka savjetujući se s DPO-om i koristeći smjernice za postupanje prilikom provedbe DPIA postupka koje je izradila Europska komisija, odnosno Nadležno tijelo.

### 6.11.3. Prethodno savjetovanje s Nadzornim tijelom

Ako provedeni DPIA postupak pokaže da bi obrada rezultirala visokim rizikom za prava i slobode ispitanika ukoliko voditelj obrade podataka ne poduzme mjere smanjenja rizika ili kada zakon propisuje prethodno savjetovanje s Nadzornim tijelom i njegovo odobrenje u odnosu na obradu, prije pokretanja takvih aktivnosti obrade GPN DATA-in DPO prethodno će se savjetovati s Nadzornim tijelom.

## 6.12. Vođenje evidencije


GPN DATA će sačiniti, ažurirati i čuvati evidenciju svojih aktivnosti obrade u skladu s zahtjevima GDPR koji se odnose na vođenje evidencija. Službenik za zaštitu osobnih podataka izrađuje i ažurira potrebne evidencije.

## 7. Edukacija Suradnika

Kako bi se Suradnike što bolje osvijestilo o važnosti zaštite osobnih podataka, GPN DATA je dužna obrazovati sve svoje Suradnike o značenju i načinu zaštite osobnih podataka unutar prvog mjeseca rada.

GPN DATA će provoditi najmanje jednom godišnje povremene edukacije Suradnika tijekom trajanja ugovora o radu s ciljem podizanja razine zaštite osobnih podataka i svijesti o potrebi zaštite njihove tajnosti. Provedena edukacija će se evdientirati u elektroničkom obliku.

Suradnike će se na edukacijama informirati o tome da sve uočene nedostatke i neusklađenosti na području zaštite osobnih podataka mogu i trebaju priopćiti službeniku ili nadređenoj osobi.

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 21 od 24		

Program obrazovanja utvrđuje i provodi Službenik za zaštitu osobnih podataka u dogovoru s Upravom GPN DATA-e, vodeći računa o razini rizika za pojedina radna mjesta tako da sadržaj programa bude prilagođen radnim zadacima radnika i opsegu u kojem oni dolaze u dodir s osobnim podacima.

## 8. Upotreba kolačića (cookies).

Internet stranica GPN DATA-e koristi kolačiće (*cookies*).

Kolačići su malene tekstualne datoteke koje Internet stranica pohranjuje na računalo posjetiteljima prilikom posjete Internet stranici.

GPN DATA koristi kolačiće koji ne identificiraju posjetitelja već pružaju podršku funkcionalnosti Internet stranice i prate depersoniziranu statistiku korištenja bez „pamćenja“ posjetiteljevih preferencija.

Radi izbjegavanja svake dvojbe, GPN DATA ne ide za time da pomoću svih vrsta kolačića utvrđuje identitet pojedinaca, već koristi kolačiće isključivo u gore navedene svrhe.

Prilikom posjete Internet stranice GPN DATA-e, posjetitelju se daju informacije o vrsti kolačića koje Internet stranica koristi, njihovoj svrsi i mogućnosti njihova isključivanja.

## 10. Mjere zaštite i suradnja

GPN DATA će poduzimati sve potrebne mjere za ispravljanje svih slabosti utvrđenih tijekom nadzora koja bi utjecala ili mogla utjecati na povredu obveze zaštite osobnih podataka.

GPN DATA je obvezna surađivati s AZOP-om, odnosno s drugim nadležnim tijelom.

GPN DATA će od svojih izvršitelja obrada tražiti da surađuju s nadzornim tijelima u slučajevima kada će to biti potrebno.

## 9. Usklađenost s nacionalnim propisima


GPN DATA će postupati sukladno svim dodatnim zahtjevima u odnosu na zaštitu podataka, privatnost i sigurnost koji su propisani mjerodavnim pravnim propisima EU ili nacionalnim zakonodavstvom Republike Hrvatske.

## 11. Ništetnost pojedinih odredbi

U slučaju da se utvrdi da je određena odredba ovog Pravilnika ništetna, smatra se da je takva odredba zamjenjana s odredbom koja u najvećoj mogućoj mjeri odgovara namjeri koju je GPN DATA htjela postići ništetnom odredbom.

## 12. Nadležnost i nadležni sud

Za sve eventualne sporeve proizašle iz povreda osobnih podataka primjenjuju se zakoni i drugi propisi primjenjivi u Republici Hrvatskoj, a sud nadležan za rješavanje u sporu je stvarno nadležni sud prema sjedištu GPN DATA-e.

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 22 od 24		

## 13. Tumačenje

Ovaj Pravilnik tumači se sukladno Općoj uredbi o zaštiti osobnih podataka i primjenjivom zakonodavstvu Republike Hrvatske na području zaštite osobnih podataka.

## 14. Revizije

GPN DATA će po potrebi revidirati ovaj Pravilnik kako bi uzeo u obzir promjene u pravnim, regulatornim ili operativnim zahtjevima za zaštitu EU osobnih podataka.

## 15. Povezani pravilnici

Ovaj Pravilnik treba se čitati zajedno sa svim GPN DATA-inim primjenjivim Pravilnicima, postupcima i smjernicama u odnosu na zaštitu podataka, informacijske tehnologije i evidencije u danom trenutku. U cilju izbjegavanja svake dvojbe, ovaj Pravilnik nema veću pravnu snagu niti zamjenjuje bilo koji mjerodavni zakonski propis, regulativu, pravila ili ugovore, kao niti bilo koju GPN DATA-inu politiku, proceduru ili odluku koje su strože od ovog Pravilnika.

## 16. Upit i kontakt podaci

Suradnici koji imaju pitanja u vezi ovog Pravilnika trebaju se obratiti Upravi ili DPO-u. Ime i kontakt podaci DPO nalaze se na mrežnom poslužitelju (javno dostupnim mapama – [Placu](#)). u mapi Organizacija i dužnosti.

## 17. Prethodno savjetovanje i stupanje na snagu

Ovaj Pravilnik o osobnim podacima donesen je na dan 25.05.2018.

Društvo će odredbe ovog Pravilnika učiniti dostupnim svim zaposlenicima na mrežnom poslužitelju (javno dostupnim mapama - [Placu](#)).

Pravilnik stupa na snagu dana 25.05.2018.


Ovaj Pravilnik GPN DATA će revidirati po potrebi.

U Zagrebu, 22. svibnja 2018. godine

**GPN DATA d.o.o.**

---


Marko Filipović, Član Uprave

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 23 od 24		

## Dodatak 1 : Sadržaj obavijesti

GPN DATA će u obavijestima ispitanicima koje se odnose na GPN DATA-ino prikupljanje i obradu EU osobnih podataka osigurati sljedeće informacije :

- identitet i kontakt podatke izvršitelja obrade podataka;
- kontakt podatke DPO;
- svrhu i pravni temelj za obradu;
- legitimne interese za obradu, kada one čine zakoniti temelj za obradu;
- primatelje ili kategorije primatelja EU osobnih podataka, ukoliko postoje;
- kategorije odnosnih EU osobnih podataka (ukoliko se EU osobni podaci ne prikupljaju od ispitanika);
- informacije o svakom prekograničnom prijenosu podataka i moguće rizike povezane s takvim prijenosima;
- razdoblje tijekom kojeg će GPN DATA pohranjivati EU osobne podatke (ili ako nije moguće odrediti točno razdoblje, kriterij za određivanje tog razdoblja);
- postojanje specifičnih prava ispitanika, uključujući pravo zahtijevati pristup, ispravak ili brisanje EU osobnih podataka; ograničavanje obrade koja se odnosi na ispitanika; pravo na prigovor u odnosu na obradu; te prenosivost podataka;
- kada privola ispitanika čini zakoniti temelj za obradu, postojanje prava na povlačenje privole u svakom trenutku (bez utjecaja na zakonitost obrade temeljene na privoli prije povlačenja);
- pravo podnošenja prigovora Agenciji za zaštitu osobnih podataka;
- je li davanje EU osobnih podataka zakonski ili ugovorni uvjet, ili preduvjet potreban za sklapanje ugovora; je li ispitanik dužan dati svoje EU osobne podatke; te moguće posljedice u slučaju nedavanja EU osobnih podataka;
- postojanje automatiziranog odlučivanja, uključivo s izradom profila (kad takve odluke imaju pravne učinke ili značajno utječu na ispitanika) i davanje smislene informacije u vezi logike i mogućih posljedica takve obrade za ispitanika; i
- informacije o izvorima EU osobnih podataka (ukoliko GPN DATA ne prikuplja takve podatke izravno od ispitanika) i, gdje je primjenjivo, dolaze li iz javno dostupnih izvora.

PRAVILNIK O OSOBNIM PODACIMA		
Pravilnik. Br. 1		
Verzija	v. 1	
Stranica 24 od 24		

## Dodatak 2 : Odredbe u ugovorima s izvršiteljima obrade

GPN DATA-ovi ugovori s izvršiteljima obrade podataka moraju sadržavati sljedeće odredbe kojima se utvrđuje da će izvršitelj obrade:

- obrađivati EU osobne podatke samo prema dokumentiranim uputama izdanim od GPN DATA-e (uključivo s uputama za prekogranični prijenos EU osobnih podataka), osim u ograničenim okolnostima u kojima je obrada propisana zakonom EU ili države članice mjerodavnim za izvršitelja obrade, u kojem slučaju izvršitelj obrade mora prije započinjanja obrade obavijestiti GPN DATA o takvom zakonskom zahtjevu, osim ako dijeljenje takvih informacija nije zabranjeno zakonom na temelju značajnog javnog interesa;
- nametnuti obveze čuvanja povjerljivosti za svo osoblje koje sudjeluje u obradi EU osobnih podataka;
- primijeniti odgovarajuće tehničke i organizacijske mjere u svrhu osiguravanja odgovarajuće razine sigurnosti u svjetlu izvjesnosti i razine rizika negativnog učinka na prava i slobode ispitanika u skladu s GDPR;
- poštivati sve zahtjeve sadržane u GDPR u vezi angažiranja podizvršitelja obrade;
- pružiti GPN DATA-u pomoć u ispunjavanju GPN DATA-ine obveze odgovaranja na zahtjeve ispitanika u vezi EU osobnih podataka koje izvršitelj obrade obrađuje;
- osigurati usklađenost sa sigurnosnim obvezama izvršitelja obrade, njegovim obvezama provođenja procjene utjecaja na zaštitu podataka i, gdje je to primjenjivo, obvezama da se prije obrade savjetuje s Nadzornim tijelom i obveze da izvijesti GPN DATA bez odgode nakon saznanja da je došlo do povrede EU osobnih podataka.
- izbrisati ili GPN DATA-u vratiti, po izboru GPN DATA-a, sve EU osobne podatke kada je cijela obrada gotova ili je poslovni odnos okončan na drugi način, te izbrisati bilo koju i sve kopije EU osobnih podataka, osim ako primjenjivi propisi EU ili države članice ne zahtijevaju njihovo daljnje čuvanje; i

dostaviti GPN DATAu sve informacije potrebne za uvjeravanje da izvršitelj obrade djeluje sukladno GDPR te dopustiti i surađivati u svim revizijama, uključivo s inspekcijama, koje provodi GPN DATA ili revizor angažiran od strane GPN DATA-a.