



REPUBLIKA HRVATSKA  
Središnji državni ured za  
razvoj digitalnog društva

# Opća Uredba o zaštiti osobnih podataka

GDPR – General Data Protection Regulation

# GDPR

- Opća uredba o zaštiti podataka
- Usvojena od strane europskog parlamenta **14. travnja 2016.**
- Počinje se primjenjivati **25. svibnja 2018.**
- Stavlja izvan snage Direktivu 95/46/EC
- Ciljevi:
  - usklađivanje zakona o zaštiti podataka u cijeloj Europi,
  - zaštita i osnaživanje osobnih podataka svih građana EU,
  - promjena načina pristupa zaštiti podataka u organizacijama.
- **Uvode se učinkovite odvraćajuće mjere za nepoštivanje Uredbe (izuzetno visoke kazne, odštete)**

# Načela obrade osobnih podataka

- Zakonitost, poštenost i transparentnost
- Ograničavanje svrhe
- Smanjenje količine podataka
- Točnost
- Ograničenje pohrane
  - Osobni podaci moraju biti čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju
- Cjelovitost i povjerljivost
- Pouzdanost
  - Voditelj obrade odgovoran je za usklađenost sa načelima te mora biti u mogućnosti dokazati usklađenost

# GDPR i prava ispitanika

- Pravo na informiranje
- Pravo pristupa
- Pravo na ispravak
- Pravo na brisanje
- Pravo na ograničavanje obrade
- Pravo na prijenos podataka
- Pravo na prigovor
- Prava vezana uz automatsko donošenje odluka i profiliranje

# Što je u opsegu?

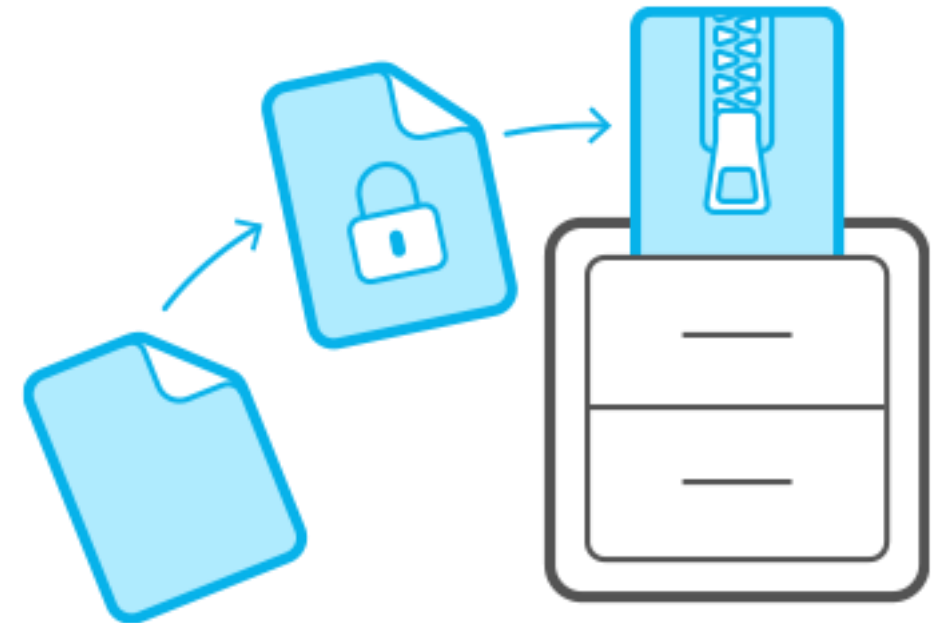
## Članak 2.

### Glavno područje primjene

1. Ova se Uredba primjenjuje na obradu osobnih podataka koja se u cijelosti obavlja automatizirano te na neautomatiziranu obradu osobnih podataka koji čine dio sustava pohrane ili su namijenjeni biti dio sustava pohrane.

## Članak 4.

6. „**sustav pohrane**” znači svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi;



# Zakonitost obrade

Obrada je zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećega:

- (a) ispitanik je dao **privolu** za obradu svojih osobnih podataka u jednu ili više posebnih svrha;
- (b) obrada je **nužna za izvršavanje ugovora** u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;
- (c) obrada je nužna radi **poštovanja pravnih obveza** voditelja obrade;
- (d) obrada je nužna kako bi se **zaštili ključni interesi ispitanika** ili druge fizičke osobe;
- (e) obrada je nužna za **izvršavanje zadaće od javnog interesa** ili pri izvršavanju **službene ovlasti** voditelja obrade;
- (f) obrada je nužna za potrebe **legitimnih interesa** voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

Točka (f) prvog podstavka ne odnosi se na obradu koju provode tijela javne vlasti pri izvršavanju svojih zadaća.

# Obrada temeljem privole

Privola bi trebala obuhvatiti sve aktivnosti obrade koje se obavljaju u istu svrhu ili svrhe.

Kada obrada ima višestruke svrhe, privolu bi trebalo dati za sve njih.

**Kada se obrada temelji na privoli, voditelj obrade mora moći dokazati da je ispitanik dao privolu za obradu svojih osobnih podataka.**

# Privola

Privola bi se trebala davati **jasnom potvrdnom radnjom** kojom se izražava dobrovoljan, poseban, **informiran i nedvosmislen pristanak** ispitanika na obradu osobnih podataka koji se odnose na njega, poput pisane izjave, uključujući elektroničku, ili usmene izjave.

**Šutnja, unaprijed kvačicom označeno polje ili manjak aktivnosti stoga se ne bi smjeli smatrati privolom.**



# Službenik za zaštitu podataka

Imenuje se ukoliko:

- (a) obradu provodi tijelo javne vlasti ili javno tijelo, osim za sudove koji djeluju u okviru svoje sudske nadležnosti,
- (b) osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od postupaka obrade koji zbog svoje prirode, opsega i/ili svrha iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri, ili
- (c) osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od opsežne obrade posebnih kategorija podataka na temelju članka 9. i osobnih podataka u vezi s kaznenim osudama i kažnjivim djelima iz članka 10.

# Procjena učinka na zaštitu podataka

- Fokus na procjenu i upravljanje rizicima u cilju smanjenja negativnog učinka na privatnost, prava i slobode pojedinaca
- Informacijska sigurnost – upravljanje rizicima u cilju smanjenja negativnog učinka za organizaciju

**Pristup: Integracija procesa upravljanja rizicima informacijske sigurnosti i rizicima vezanima uz privatnost i zaštitu osobnih podataka, te upravljanja projektima i promjenama**

# Prethodno savjetovanje

1. Voditelj obrade savjetuje se s nadzornim tijelom prije obrade ako se procjenom učinka na zaštitu podataka pokazalo da bi, u slučaju da voditelj obrade ne donese mjere za ublažavanje rizika, obrada dovela do **visokog rizika**.
2. Ako nadzorno tijelo smatra da bi se namjeravanom obradom kršila Uredba, osobito ako voditelj obrade nije u dovoljnoj mjeri utvrdio ili umanjio rizik, nadzorno tijelo u roku od najviše osam tjedana od zaprimanja zahtjeva za savjetovanje pisanim putem savjetuje voditelja obrade i, prema potrebi, izvršitelja obrade

# Povreda osobnih podataka

Ako se povreda osobnih podataka ne rješava na odgovarajući način i pravodobno, ona može prouzročiti fizičku, materijalnu ili nematerijalnu štetu pojedincima, kao što su **gubitak nadzora nad osobnim podacima ili ograničavanje njihovih prava, diskriminacija, krađa identiteta ili prijevara, financijski gubici, neovlašteni obrnuti postupak pseudonimizacije, šteta za ugled, gubitak povjerljivosti osobnih podataka** zaštićenih poslovnom tajnom ili bilo koju drugu ekonomsku ili društvenu štetu za dotičnog pojedinca.

# Rok za izvještavanje o povredi

Čim voditelj obrade primijeti da je došlo do povrede osobnih podataka, trebao bi o tome izvijestiti nadležno nadzorno tijelo bez nepotrebnog odgađanja i to, ako je izvedivo, **najkasnije 72 sata nakon saznanja o toj povredi** osobnih podataka, osim ako voditelj obrade može dokazati, u skladu s načelom odgovornosti, da povreda osobnih podataka vjerojatno neće prouzročiti rizik za prava i slobode pojedinaca.