

OGRANIČENJE SVRHE · MINIMIZACIJA PODATAKA · ODGOVORNOST

Vođeno svrhom. Omogućeno tehnologijom.

Načela odgovorne obrade podataka u softveru za javni sektor i sustave kritične važnosti.

ID DOKUMENTA	VERZIJA	KLASIFIKACIJA	VLASNIK DOKUMENTA	CIKLUS REVIZIJE	OBJAVLJENO
ITO-TRUST-PRV-001	1.0	JAVNO	Privatnost i informacijska sigurnost	Godišnje	Listopad 2026.

Odgovorno upravljanje podacima od samog dizajna

ITO razvija digitalne platforme koje koriste državne institucije, organizacije javne sigurnosti i druge organizacije koje provode složene procese kritične važnosti.

Ti sustavi mogu obrađivati osobne, operativne ili na drugi način osjetljive informacije. Odgovorno upravljanje podacima stoga treba razmatrati tijekom dizajna, izrade, rada i održavanja sustava.

Ovaj dokument opisuje načela kojima se ITO vodi pri dizajnu tehnologije koja obrađuje institucionalne podatke ili omogućuje pristup njima.

ITO PRISTUPA PRIVATNOSTI I UPRAVLJANJU PODACIMA KROZ ŠEST NAČELA

01

Ograničenje svrhe
Obrađa za definirane i legitimne svrhe.

02

Minimizacija podataka
Bez nepotrebnog prikupljanja ili umnožavanja.

03

Kontrolirani pristup
Pristup samo ovlaštenim korisnicima i sustavima.

04

Odgovornost
Relevantne aktivnosti bilježe se gdje je potrebno.

05

Sigurnost
Zaštita kroz cijeli životni ciklus informacija.

06

Transparentnost
Jasne uloge i dokumentirano upravljanje.



Ovaj dokument ne zamjenjuje pravne, regulatorne ni upravljačke odgovornosti institucije koja upravlja sustavom.

SADRŽAJ

01	Svrha	02
02	Upravljanje pod kontrolom institucije	03
03	Privatnost od dizajna	04
04	Minimizacija i mjerodavni izvori	05
05	Pristup i odgovornost	06
06	Životni ciklus podataka	06
07	Dijeljenje podataka i integracije	07
08	Uloge i odgovornosti	08
09	Privatnost i sigurnost	09
10	Standardi i regulatorni kontekst	09
11	Jamstva privatnosti	10
12	Naše načelo	10

KONTROLA DOKUMENTA

ID DOKUMENTA

ITO-TRUST-PRV-001

VERZIJA

1.0

KLASIFIKACIJA

JAVNO

VLASNIK

Privatnost i informacijska sigurnost

CIKLUS REVIZIJE

Godišnje

OBJAVLJENO

Listopad 2026.

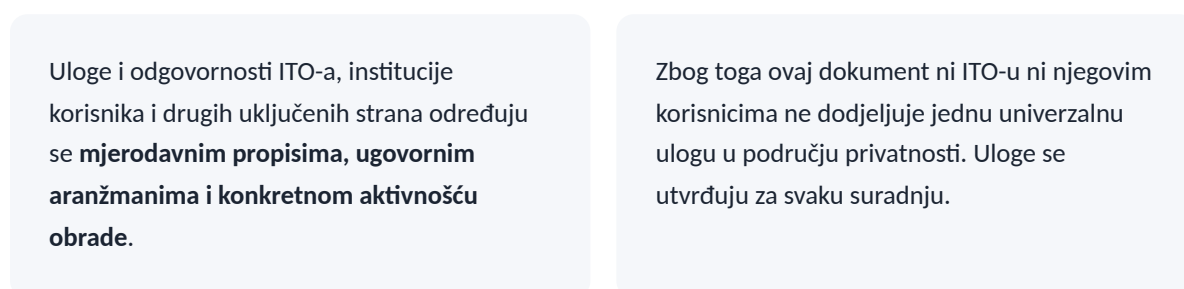
Tehnologija omogućuje upravljanje. Institucije ga definiraju.

ITO platforme dizajnirane su za rad unutar okvira upravljanja koje definiraju organizacije koje ih koriste.

OVISNO O MJERODAVNOM PRAVNOM I UGOVORNOM MODELU, INSTITUCIJA KORISNIK ODREĐUJE PITANJA KAO ŠTO SU



ULOGE I ODGOVORNOSTI



Privatnost počinje u fazi dizajna

Razmatranja privatnosti trebaju započeti tijekom dizajna sustava, a ne uvoditi se tek nakon implementacije.

Ovisno o prirodi rješenja, relevantna razmatranja pri dizajnu mogu uključivati:

Ograničenje svrhe

01

Informacije treba obrađivati za definirane i legitimne operativne svrhe.

Minimizacija podataka

02

Sustavi trebaju izbjegavati nepotrebno prikupljanje ili umnožavanje informacija.

Ograničenje pristupa

03

Informacije trebaju biti dostupne samo primjereno ovlaštenim korisnicima i sustavima.

Sljedivost

04

Relevantne aktivnosti treba bilježiti gdje je to potrebno radi odgovornosti.

Čuvanje

05

Informacije se ne bi smjele čuvati dulje nego što to zahtijevaju mjerodavna pravila i operativni zahtjevi.

Sigurnost

06

Odgovarajuće tehničke i organizacijske mjere trebaju štititi informacije kroz cijeli njihov životni ciklus.

Ova se razmatranja primjenjuju razmjerno prirodi svakog rješenja, informacijama koje obrađuje i okviru upravljanja koji definira institucija.

Integracija bez umnožavanja

Jedno od temeljnih arhitektonskih načela ITO-a jest izbjegavanje nepotrebnog umnožavanja institucionalnih informacija.

Gdje je to tehnički i operativno prikladno, ITO platforme mogu se integrirati s mjerodavnim izvorima informacija umjesto stvaranja dodatnih neovisnih kopija istih informacija.



Pristup odražava odgovornost

Pristup informacijama treba odražavati organizacijsku odgovornost i operativnu potrebu.

OVISNO O RJEŠENJU, ITO PLATFORME MOGU PODRŽAVATI

Autentificirane identitete

Kontrolu pristupa temeljenu na ulogama

Organizacijsku hijerarhiju

Ograničene administrativne funkcije

Revizijsko bilježenje

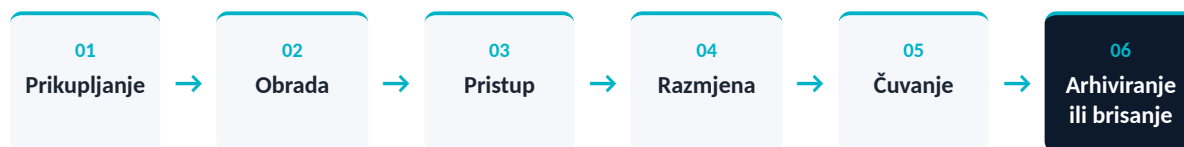
Gdje rješenje to podržava, revizijske informacije mogu ovlaštenom osoblju pružiti uvid u relevantne aktivnosti sustava i korisnika.

INSTITUCIJA ODLUČUJE

Institucija određuje tko treba imati pristup određenim informacijama i funkcionalnostima, u skladu sa svojim mjerodavnim modelom upravljanja.

Upravljanje kroz životni ciklus informacija

Upravljanje podacima obuhvaća cijeli životni ciklus informacija.



ITO PLATFORME

Mogu pružati tehničke mehanizme koji podržavaju politike životnog ciklusa.

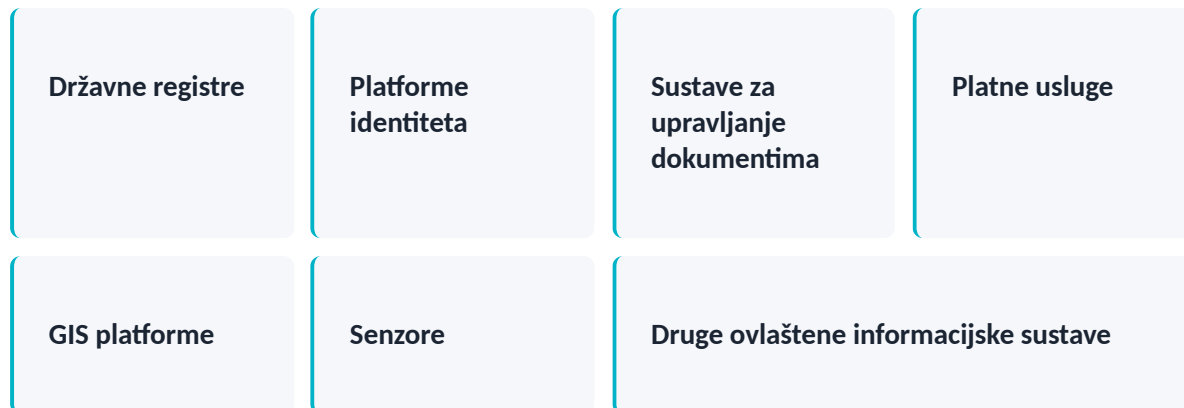
PROPISI, INSTITUCIONALNE PROCEDURE I UGOVORI

Određuju mjerodavne zahtjeve za čuvanje, arhiviranje i brisanje.

Kontrolirana razmjena između sustava

Razmjena informacija između sustava treba se odvijati putem kontroliranih i dokumentiranih integracijskih mehanizama.

OVISNO O ARHITEKTURI, INTEGRACIJE MOGU UKLJUČIVATI



Pristup vanjskim izvorima informacija ostaje podložan ovlastima, politikama i tehničkim kontrolama odgovornih organizacija.

NAŠE STAJALIŠTE

Integracija ne stvara ovlast za pristup podacima.

Ovlast mora postojati **neovisno** o tehnologiji koja omogućuje integraciju.

Jasne uloge za svaku stranu

Svaka je strana odgovorna za svoj dio obrade, u skladu s mjerodavnim propisima i ugovornim aranžmanima.



Institucija korisnik

Definira zakonite svrhe, ovlaštene korisnike, operativne procedure, zahtjeve za čuvanje i institucionalne politike upravljanja podacima u skladu s mjerodavnim propisima.

DEFINIRA



ITO

Osigurava sigurnu tehnologiju, provodi dogovorene kontrole, podržava konfiguraciju sustava i obavlja dogovorene aktivnosti obrade u skladu s mjerodavnim ugovornim i pravnim okvirom.

OMOGUĆUJE



Treće strane

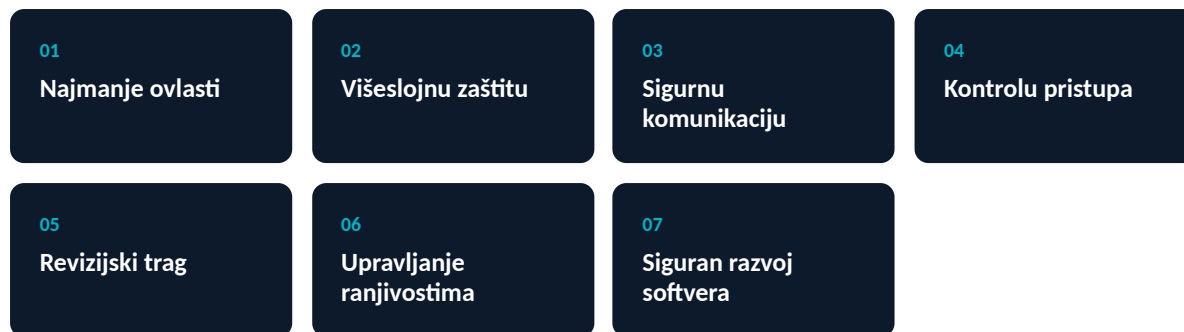
Ostaju odgovorne za svoje sustave, usluge i aktivnosti obrade, u skladu sa svojom ulogom i mjerodavnim obvezama.

ODGOVORNE ZA SVOJ
DIO

Točna raspodjela uloga određuje se mjerodavnim propisima, ugovornim aranžmanima i konkretnom aktivnošću obrade.

Nema privatnosti bez sigurnosti

ITO-ov pristup privatnosti stoga je potkrijepljen sigurnosnim načelima koja uključuju:



Za dodatne informacije

ITO sigurnosni whitepaper

ITO-TRUST-SEC-001 · ito.dev/en/trust-center

[Povezani dokument →](#)

Dizajnirano za podršku mjerodavnim zahtjevima

ITO dizajnira svoj pristup upravljanju privatnošću pozivajući se na mjerodavne zahtjeve zaštite podataka i priznata načela upravljanja privatnošću.

ISO/IEC 27701

UPRAVLJANJE PRIVATNOŠĆU INFORMACIJA

ISO/IEC 27001

UPRAVLJANJE INFORMACIJSKOM SIGURNOŠĆU

ITO-ovi sustavi upravljanja potkrijepljeni su certifikatima ISO/IEC 27701 i ISO/IEC 27001 unutar njihova certificiranog opsega.

NAŠA PREDANOST

ITO dizajnira svoju tehnologiju kako bi korisnicima pomogao ispuniti mjerodavne zahtjeve privatnosti i zaštite podataka.

Konkretna pravna obveza ovisi o jurisdikciji, vrsti organizacije, svrsi obrade i prirodi uključenih informacija.

Informacije za dubinsku analizu

Korisnici i partneri kojima su potrebne dodatne informacije mogu zatražiti odgovarajuću dokumentaciju o privatnosti i upravljanju podacima u sklopu nabave, implementacije ili aktivnosti procjene dobavljača.

OVISNO O SURADNJI, TO MOŽE UKLJUČIVATI INFORMACIJE O

01 Tokovima podataka	02 Arhitekturi obrade	03 Sigurnosnim kontrolama	04 Upravljanju pristupom
05 Mogućnostima čuvanja	06 Integracijama	07 Relevantnim certifikatima	08 Ugovornim aranžmanima o zaštiti podataka

Osjetljive informacije mogu se pružiti uz odgovarajuće zahtjeve povjerljivosti.

ZATRAŽITE DOKUMENTACIJU

Kontaktirajte ITO putem Trust Centra ili određenog sigurnosnog kanala.

security@ito.dev
ito.dev/en/trust-center

Podatke treba obrađivati zato što postoji **legitimna institucionalna svrha** — a ne samo zato što tehnologija obradu čini mogućom.

ITO razvija tehnologiju koja institucijama omogućuje učinkovito korištenje podataka uz održavanje odgovarajućeg upravljanja, sigurnosti, odgovornosti i kontrole.



ITO TRUST DOKUMENTI

Engineering Digital Trust.

POVEZANI DOKUMENTI

ITO-TRUST-SEC-001

ITO sigurnosni whitepaper

ITO-TRUST-AI-001

ITO Načela odgovorne umjetne
inteligencije

ITO-TRUST-SDL-001

ITO Pregled sigurnog razvoja softvera

DOKUMENT

ITO Privatnost i upravljanje podacima

ID • VERZIJA • KLASIFIKACIJA

ITO-TRUST-PRV-001 • 1.0 • JAVNO

VLASNIK • REVIZIJA

Privatnost i informacijska sigurnost • Godišnje • Listopad 2026.

KONTAKT

security@ito.dev • ito.dev/en/trust-center

TVRKA

IT Odjel Mostar d.o.o., Mostar, Bosna i Hercegovina