



2

GDPR

MASTERCLASS

Privacy friendly oznaka za web

Bernat Gužvanj, konzultant za informacijsku sigurnost



I Agree



Privacy friendly oznaka je dokaz



- Neovisno i objektivno uvjerenje:
 - da je vašu web stranicu pregledao tim nezavisnih stručnjaka za zaštitu osobnih podataka
 - da vaša web stranica zadovoljava zahtjeve EU regulative iz područja zaštite privatnosti
 - da vaša web stranica primjenjuje najbolje svjetske prakse i standarde u zaštiti osobnih podataka
 - Vaše predanosti zaštiti osobnih podataka, ispitanika koji koriste Vaše stranice i njihovih prava



Metodologija



- metodologija razvijena od strane stručnjaka Ostendo Consulting grupe
- web stranica mora ispunjavati preko 30 kriterija iz područja EU regulative, kibernetičke sigurnosti, međunarodnih standarda i najboljih svjetskih praksi u zaštiti podataka kako bi dobila Privacy friendly web oznaku





Provjera sigurnosnih postavki web stranice



- Rating sigurnosti implementacije SSL i TLS protokola za enkripciju komunikacije između posjetitelja i stranice
- analiza certifikata (valjanost, izdavač itd.)
- konfiguracija podržanih protokola (backward compatibility, downgrade)
- analiza podržanih šifranata
- detekcija loših sigurnosnih postavki (kroz simulaciju handshakea)



Provjera usklađenosti privacy noticea sa GDPR zahtjevima



- Sadržaj privacy noticea, tj. informacija koje se trebaju pružiti ispitanicima je uređen:
 - odredbama čl. 12, 13 i 14 GDPR-a
 - Smjernice o transparentnosti na temelju Uredbe 2016/679 (WP260 rev.01)
- certificiranje stranice obuhvaća provjeru da li Vaša stranica udovoljava zahtjevima tih dvaju dokumenata

	OSOBNİ PODACI PRIKUPLJENI IZRAVNO OD ISPITANİKA	OSOBNİ PODACI NISU DOBIVENI OD ISPITANİKA
Trenutak pružanja informacija	Trenutak prikupljanja osobnih podataka	1. unutar razumnog roka nakon dobivanja osobnih podataka, a najkasnije u roku od jednog mjeseca. 2. ako se osobni podaci trebaju upotrebljavati za komunikaciju s ispitanikom, najkasnije u trenutku prve komunikacije ostvarene s tim ispitanikom; ili 3. ako je predviđeno otkrivanje podataka drugom primatelju, najkasnije u trenutku kada su osobni podaci prvi put otkriveni
Način pružanja informacija	sažeto i transparentno (kako bi se izbjeglo zamaranje zbog prekomjernih informacija)	
	Razumljivo (prosječnom pripadniku određene ciljane skupine ispitanika)	
	lako dostupno (ispitanik ju ne mora aktivno tražiti)	
	uporaba jasnog i jednostavnog jezika (osobito informacije koje su posebno namijenjene djetetu)	
	Izjava/obavijest o privatnosti je samostalno pružena (npr., nije obuhvaćena općim uvjetima korištenja web stranice/aplikacije)	
	Izjava/obavijest o privatnosti dostupna je na jednom mjestu ili u jednom cjelovitom dokumentu kojem ispitaniku mogu lako pristupiti	
	Koristi se slojevita izjava/obavijest o privatnosti koja ispitaniku omogućuje da izravno pristupi dijelu izjave/obavijesti koji želi pročitati	
	Prvi sloj izjave/obavijesti daje sadržaj informacije o (1) svrhama obrade, (2) identitetu voditelja obrade, (3) opisu prava ispitanika te (4) o obradi koja ima najveći učinak na ispitanika i obradi koja bi ga mogla iznenaditi	
Izmjene informacija koje se pružaju	Redovito pregledavamo i po potrebi ažuriramo izjavu/obavijest o privatnosti	
	Ako voditelj namjerava dodatno obrađivati osobne podatke u svrhu koja je različita od one za koju su osobni podaci prikupljeni, prije započinjanja nove obrade iskomunicirao je to ispitaniku i ažurirao izjavu/obavijest o privatnosti	



Cookie banner



- provjera kakve kolačiće stranica prikuplja o korisniku
 - obavezni
 - funkcionalni
 - marketinški
- jesu li informacije u cookie banneru točne (reflektiraju li realno stanje na stranici i cookie engineu?)



Privacy friendly web stranica



- Prikuplja podatke o posjetiteljima na transparentan način usklađen sa primjenjivom regulativom
- upravlja kolačićima u skladu sa zahtjevima GDPR i ePrivacy regulativa
- ima privacy notice usklađen sa GDPR zahtjevima
- osobne podatke štiti ispravnom primjenom enkripcije
- primjenjuje najbolje svjetske prakse za zaštitu od kibernetičkih napada

Za više informacija



pošaljite e-mail na: info@ostendogroup.com

HVALA VAM NA PAŽNJI!