

GDPR Compliance Report

example-store.com

Good Compliance



COMPLIANCE SCORE

5

RECOMMENDED
ACTIONS

2

HIGH
PRIORITY

2

MEDIUM
PRIORITY

"Sejni piškotki se nastavijo pred privolitvijo; v politiki zasebnosti manjka pravica do pritožbe pri nadzornem organu"

Prednostni ukrepi

Spletno mesto ima dobro tehnično osnovo — sledenje je načeloma vezano na privolitev, HTTPS je omogočen in obrazci so pravilno nastavljeni — vendar politika zasebnosti vsebuje pomembne vrzeli, vključno z manjkajočimi informacijami o nadzornem organu, formulacijami implicirane privolitve in nepopolnim naborom pravic posameznika.

HIGH

Preprečite nalaganje piškotkov pred privolitvijo

Preglejte nastavitev upravljanja privolitev in zagotovite, da se pred aktivnim sprejemom prek pasice ne nastavijo nobeni piškotki, razen strogo nujnih sejnih piškotkov.

HIGH

Dodajte pravico do pritožbe pri nadzornem organu

V politiko zasebnosti jasno dodajte, da imajo uporabniki pravico vložiti pritožbo pri pristojnem nadzornem organu za varstvo podatkov — to je obvezno razkritje po členu 13(2)(d) GDPR.

MEDIUM

Jasno navedite vse pravice posameznika

Dodajte ločen razdelek s pravicami po GDPR: dostop, popravek, izbris, prenosljivost, omejitev obdelave in ugovor.

MEDIUM

Odstranite formulacije implicirane privolitve

Politika ne sme navajati, da se uporabniki samodejno strinjajo že z uporabo spletnega mesta. Privolitev mora biti aktivna in nedvoumna.

LOW

Razmislite o zasebnosti prijazni analitiki

Prehod na orodje, kot je Plausible ali samogostovani Matomo, lahko odpravi potrebo po privolitvi za analitiko in zmanjša kompleksnost skladnosti.

Detailed Findings

Piškotki in privolitev

- ✓ **Prisotna pasica za piškotke**
Obiskovalcem je prikazana pasica za privolitev v piškotke.
- ✓ **Piškotek za jezikovno nastavitev se nastavi pred privolitvijo**
Piškotki za jezikovne nastavitve so tehnično nujni za delovanje strani in ne zahtevajo predhodne privolitve.
- ✓ **Sejni piškotek se nastavi pred privolitvijo**
Sejni piškotki so nujni za osnovno delovanje strani (npr. košarica, prijava) in so izvzeti iz zahteve po predhodni privolitvi.
- ✗ **Sledilni ali funkcionalni piškotki se naložijo pred privolitvijo**
Kljub pasici je pregled zaznal nastavljanje piškotkov še pred interakcijo uporabnika z mehanizmom privolitve, kar je v nasprotju z GDPR zahtevo po predhodni in prostovoljni privolitvi.
- ! **Mehanizem privolitve obstaja in blokira sledilce**
Sledilci so po načelu blokirani z orodjem za privolitev, vendar predčasno nastavljanje piškotkov zmanjšuje učinkovitost tega mehanizma.

Sledenje in analitika

- ! **Zaznan sledilni piksel tretje osebe**
Prisoten je sledilni piksel tretje osebe; deluje kot vezan na privolitev, vendar je treba preveriti, da se sproži šele po izrecni privolitvi.
- ! **Naložen skript vedenjske analitike**
Na strani se nalaga analitični skript; aktivirati bi se moral šele po privolitvi uporabnika, ker spremlja vedenjske podatke.
- ✗ **Uporaba zasebnosti prijazne analitike**
Ni zaznano orodje zasebnosti prijazne analitike (npr. Plausible ali samogostovani Matomo); aktivne analitične storitve zahtevajo privolitev in prinašajo višje GDPR tveganje.
- ✓ **Blokiranje sledilcev tretjih oseb do privolitve**
Spletno mesto uporablja pristop upravljanja privolitev, ki naj bi blokiral sledilce tretjih oseb do privolitve — dobra praksa, ki jo je smiselno redno preverjati.

Zbiranje podatkov

- ✓ **Obrazec z nizko občutljivostjo (GET, brez osebnih podatkov)**
Iskalni ali filtrirni obrazec z metodo GET ne zbira e-pošte, telefona ali imena — nizko tveganje in potrditveno polje ni potrebno.
- ✓ **Obrazec z visoko občutljivostjo (POST, zbira ime in e-pošto)**
Kontaktni ali novičarski obrazec uporablja POST (pravilno za občutljivejše podatke) in zbira ime ter e-poštni naslov.
- ✓ **Potrditveno polje privolitve na občutljivem obrazcu**
Obrazec z višjo občutljivostjo vsebuje potrditveno polje za privolitev — dobra praksa za veljavno pravno podlago obdelave.

Politika zasebnosti

- ✓ **Politika zasebnosti obstaja in je dostopna**
Na spletni strani je javno dostopna politika zasebnosti.
- ✓ **Razkrita identiteta upravljavca in kontaktni podatki**
Politika navaja upravljavca podatkov in njegove kontaktne podatke.
- ✓ **Navedeni nameni obdelave in pravne podlage (člen 6 GDPR)**
Politika pojasni pravne podlage za obdelavo osebnih podatkov, vključno s privolitvijo in pogodbeno nujnostjo.
- ✓ **Navedeni prejemniki podatkov**
Politika navaja ponudnike plačil, gostovanja, analitike in operativnih storitev, vključene v obdelavo podatkov.
- ✓ **Navedena obdobja hrambe podatkov**
Za več kategorij osebnih podatkov so opredeljeni konkretni roki hrambe.
- ! **Pokrite pravice posameznika (členi 15-21 GDPR)**
Nekatere GDPR pravice so omenjene, vendar dostop, prenosljivost, popravek in izbris niso jasno navedeni posamično.
- ! **Omenjena pravica do preklica privolitve**
Politika omenja preklic privolitve, vendar ne pove jasno, da jo lahko uporabnik kadar koli prekliče.
- ✗ **Pravica do pritožbe pri nadzornem organu**
Politika ne omenja pravice uporabnika do vložitve pritožbe pri nadzornem organu za varstvo podatkov.
- ✗ **Jezik implicirane privolitve**
Politika nakazuje, da nadaljnja uporaba spletnega mesta pomeni strinjanje, kar ni veljavna privolitev po GDPR.
- ! **Razkriti mednarodni prenosi podatkov in varovalke**
Do mednarodnih prenosov podatkov lahko prihaja, vendar politika ne pojasni dovolj jasno uporabljenih zaščitnih ukrepov.

Tehnična varnost



HTTPS je omogočen

Celotno spletno mesto deluje prek HTTPS, zato so podatki med prenosom šifrirani.



Občutljiv obrazec uporablja metodo POST

Obrazec, ki zbira osebne podatke, uporablja POST, zato podatki niso vidni v URL-jih ali strežniških dnevnikih.