Be cyber smart!



Kako zaštititi djecu na internetu — vodič za roditelje

KPMG Podgorica | kpmg.com/cyberday

Internet je nevjerovatno sredstvo za učenje, druženje i zabavu djece. Međutim, s obzirom na to da je svaki treći korisnik interneta mlađi od 18 godina, rizici povezani s onlajn aktivnostima su značajni i nastavljaju da rastu. Otprilike troje od četvoro djece širom svijeta iskusilo je bar jedan cyber rizik.[1] Kako biste zaštitili svoju djecu, ovaj vodič za internet bezbjednost pruža dragocjene savjete i preporuke. Kao roditelj ili staratelj, zaštita onlajn sigurnosti vašeg djeteta danas je važnija nego ikad.

[1] The Child onlajn Safety Index, DQ Institute, 2022

Razgovarajte o bezbjednosti na internetu na vrijeme i budite proaktivan roditelj

Počnite da razgovarate sa djecom o bezbjednosti na internetu u ranom uzrastu. Vođenjem ovih razgovora od malih nogu, možete im pomoći da donose pametne odluke i razviju zdrave navike u onlajn svijetu. Edukovanje o odgovornom korišćenju interneta, zaštiti privatnosti i potencijalnim opasnostima takođe će ih zaštititi od rizika. Zapamtite, nikada nije prerano da postavite temelje za sigurno korišćenje interneta.

- **Mladi su uvijek željni da uče.** Naučite ih kako da kreiraju sigurne lozinke, prepoznaju bezbjedne veb stranice, izbjegavaju prevare, praktikuju odgovorno ponašanje na internetu i usvoje druge vještine za sigurnu onlajn aktivnost.
- **Ne dijelite lične podatke.** Podsjetite djecu da nikada ne dijele lične informacije, poput punog imena, kućne adrese, lozinki ili broja telefona sa osobama koje ne poznaju.
- **Budite oprezni sa nepoznatim osobama.** Razgovarajte sa djecom o mogućim opasnostima komunikacije sa nepoznatim ljudima na internetu i objasnite im da nikada ne treba da se sastaju uživo sa osobama koje su upoznali onlajn bez vašeg znanja i saglasnosti.
- **Postavljajte pitanja.** Obavezno postavljajte svom djetetu pitanja o njihovim onlajn aktivnostima - koje sajtove posjećuju i s kim komuniciraju. Ohrabrite ga da iskreno razgovara o tome šta prati, gleda i dijeli na internetu.
- **Postavite jasna pravila.** Kontrolišite vrijeme provedeno pred ekranom tako što ćete definisati koliko dugo dijete može da bude onlajn i šta može da radi. Vrijeme provedeno ispred ekrana koje nije vezano za školu može biti dostupno nakon što završe domaći zadatak ili tokom vikenda. Računare i druge uređaje držite u zajedničkim prostorijama kako biste nadgledali sve aktivnosti..
- **Ograničite pristup internetu i pratite aktivnosti.** Ne morate da budete stručnjak za sajber bezbjednost da biste zaštitili svoju djecu na internetu. Aplikacije za roditeljsku kontrolu i opcije ugrađene u uređaje i Wi-Fi rutere su jednostavne za korišćenje. One vam omogućavaju da podesite vrijeme pristupa internetu, pratite aktivnosti i blokirate određene kategorije sajtova. Znanje o tome šta vaša djeca rade na internetu može pomoći u njihovoj zaštiti. Iskoristite ovu priliku da pokažete svojoj djeci koji su sajtovi prikladni za njihovu uzrasnu grupu
- **Budite dobar primjer.** Postavite dobar primjer svojim prisustvom na mreži. Demonstrirajte sigurno ponašanje i prakse.

© 2026 KPMG d.o.o. Podgorica, crnogorsko društvo s ograničenom odgovornošću i firma članica KPMG globalne organizacije nezavisnih firmi članica povezanih sa KPMG International Limited, privatnim engleskim društvom ograničenim garancijom. Sva prava zaštićena.

Onlajn igrice? Igrajte pametno!

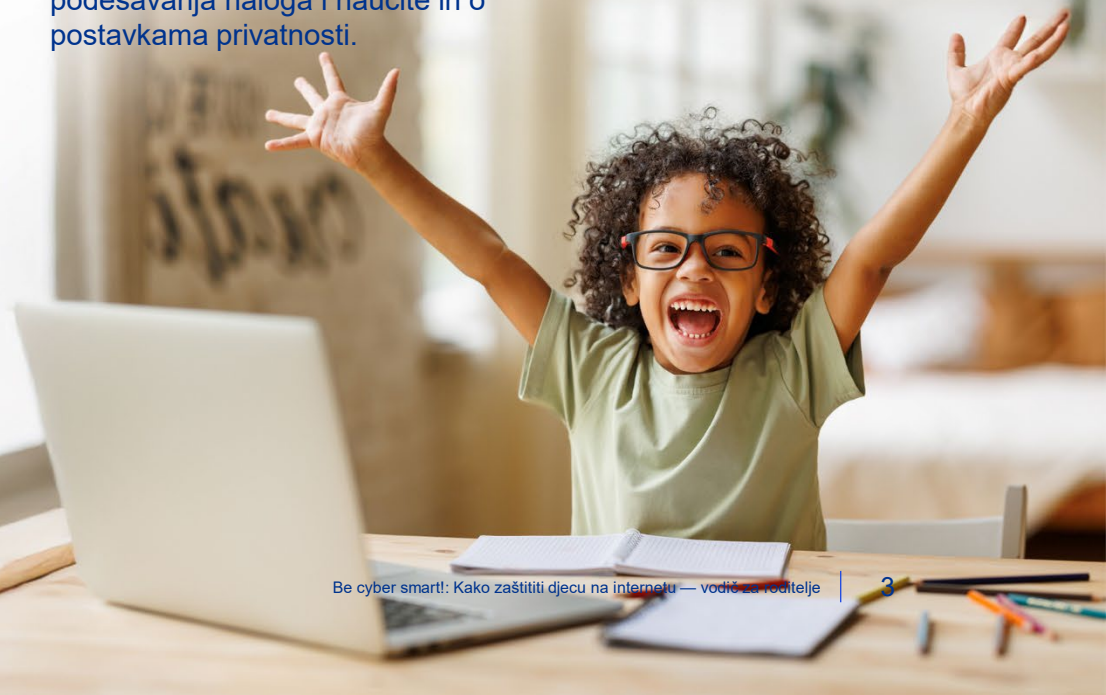
Onlajn igre mogu biti zabavna društvena aktivnost, ali takođe nose određene rizike. Sajber nasilje, onlajn predatori i skriveni troškovi su neki od problema kojih bi roditelji trebalo da budu svjesni. Da biste osigurali sigurnost svoje djece, evo nekoliko savjeta koje možete pratiti:

- Koristite dostupne roditeljske kontrole kako biste spriječili preuzimanje neprimjerenih aplikacija i igara.
- Postavite lozinke kako biste spriječili kupovine unutar igre.
- Ustanovite jasna očekivanja i pravila o vremenskim ograničenjima i vrstama igara koje su dozvoljene.
- Ograničite dopisivanje u okviru igre na razgovore koji su povezani sa samom igrom.
- Uvjerite se da vaše dijete razumije važnost čuvanja ličnih informacija privatnim i da ih nikada ne dijeli onlajn.
- Recite im da odmah prijave odrasloj osobi bilo kakvo nasilje.

Bezbjednost na društvenim mrežama

Društvene mreže su postale sastavni dio naših svakodnevnih života i dragocjeni alati za komunikaciju i zabavu. Međutim, postoje i značajni rizici povezani s ovim platformama, posebno za djecu. Ukoliko djeca neodgovorno koriste društvene mreže, to ih može ih izložiti raznim opasnostima, uključujući sajber nasilje i onlajn predatore. Da biste zaštitili svoju djecu, evo nekoliko savjeta koje treba imati na umu:

- **Starosna ograničenja.** Većina društvenih mreža ima ograničenja prema uzrastu. Vodite računa da se ta pravila poštuju i pratite njihovo korišćenje.
- **Razmislite pre objavljivanja.** Naučite svoju djecu da budu svjesna komentara i slika koje objavljuju i naglasite im da nikada ne dijele lične informacije kao što su njihova starost, škola, adresa ili puno ime. Objasnite im da, jednom kada nešto postane onlajn, ostaje na internetu. Ovo je posebno važno kako djeca odrastu i počinju da traže prve ljetnje poslove, jer poslodavci često provjeravaju prisustvo kandidata na internetu.
- **Pratite svoje dijete.** Nadgledajte aktivnosti na društvenim mrežama tako što ćete pratiti svoje dijete onlajn. Ne morate učestvovati, samo redovno pregledajte profile i objave.
- **Pregledajte stranice za roditeljsku podršku na društvenim mrežama.** Da biste saznali više o zaštiti naloga vašeg djeteta na društvenim mrežama, pregledajte stranice za podršku roditeljima. Osigurajte da je profil vašeg djeteta uvijek podešen na „privatni“ režim putem podešavanja naloga i naučite ih o postavkama privatnosti.



© 2026 KPMG d.o.o. Podgorica, crnogorsko društvo s ograničenom odgovornošću i firma članica KPMG globalne organizacije nezavisnih firmi članica povezanih sa KPMG International Limited, privatnim engleskim društvom ograničenim garancijom. Sva prava zaštićena.

Sajber nasilje

Sajber nasilje je vrsta nasilja koja se odvija putem elektronskih sredstava komunikacije i nažalost je postalo veoma rasprostranjeno. Iako ima sličnosti sa tradicionalnim nasiljem, sajber nasilje može nanijeti još veću štetu jer napadač može nastaviti da uznemirava žrtvu bez obzira na to gdje se ona nalazi. Sa internetom i mobilnim telefonima, svako može postati sajber nasilnik u bilo kojem trenutku i sa bilo koje lokacije. Evo kako možete pomoći:

Pričajte sa djecom

Važno je danas razgovarati s djecom o sajber nasilju. Potičite otvorenu komunikaciju kako bi se osjećali prijatno da vam prijave takve situacije. Edukujte ih da:

• Odmah prijavite uvredljive ili bolne komentare, bez obzira na to da li su oni meta ili ne.

• Budite oprezni sa onim što govore, šalju, objavljuju ili bloguju o drugima — nenamjerna povreda je takođe nasilje.

Prepoznajte

Znakovi da je neko žrtva sajber nasilja:

• Pokazivanje iznenadne ljutnje, depresije ili frustracije nakon korišćenja bilo kog uređaja ili izbjegavanje korišćenja uređaja uopšte.

• Nelagodnost oko odlaska u školu ili učestvovanja u grupnim ili timskim aktivnostima.

• Neuobičajeno se povlači od prijatelja i članova porodice.

Reagujte

Roditelji i djeca treba da preduzmu akciju na sljedeće načine:

• Čuvanje uvredljivih poruka, objava i e-mailova.

• Ne odgovarati na njih i ne brisati ih.

• Prijavljivanje ID-ja onlajn i blokiranje korisnika kako bi se spriječila dalja interakcija.

• Prijavljivanje problema školi vašeg djeteta ili policiji, ako je to potrebno.

© 2026 KPMG d.o.o. Podgorica, crnogorsko društvo s ograničenom odgovornošću i firma članica KPMG globalne organizacije nezavisnih firmi članica povezanih sa KPMG International Limited, privatnim engleskim društvom ograničenim garancijom. Sva prava zaštićena.

Bezbjedno prijavljivanje i odjavljivanje

Upravljanje velikim brojem lozinki može biti izazov, naročito za djecu koja ih teško pamte. Međutim, važno je razumjeti da su lozinke osnovna zaštita od moguće zloupotrebe ličnih podataka, koja može ugroziti njihovu bezbjednost kako na internetu, tako i van mreže. Da biste obezbijedili bezbjedno prijavljivanje i odjavljivanje, evo nekoliko ključnih savjeta koji će pomoći djeci da bolje zaštite svoje lične informacije:

Pažljivo birajte korisnička imena

- Izbjegavajte korišćenje punog imena, starosti, adrese, datuma rođenja, pola ili drugih ličnih informacija.
- Savjetujte djeci da se konsultuju s odraslom osobom prilikom kreiranja korisničkih imena ako imaju nedoumica.

Vježbajte sigurnost lozinki:

- Pokažite djeci kako da kombinuju fraze, brojeve, simbole i velika i mala slova.
- Naglasite im da nikada ne ponavljaju ili ponovo koriste lozinke i da nikada ne dijele lozinku ili je ne daju ako ih neko zatraži.
- Izbjegavajte lozinke koje se lako pogađaju, poput datuma rođenja ili omiljenog sporta ili aktivnosti.
- Pokušajte da koristite menadžer lozinki i savjetujte svojoj djeci da zapamte samo tri lozinke: jednu za školu, jednu za svoj računar i jednu za menadžer lozinki — dok će sve ostale lozinke biti pohranjene tamo.
- Podstičite ih da koriste dvostruku autentifikaciju gdje god je to moguće.

Zaštita vaših ličnih podataka

Podsjetite svoje dijete da se uvijek odjavi kada napusti sajt ili platformu.

Izbjegavajte besplatan WI-FI i rizik od krađe podataka od strane hakera.

Nikada ne dijelite svoje pristupne podatke s drugima, uključujući prijatelje.

Savjetujte djeci da nikada ne daju lične informacije kao što su puno ime, kućna adresa ili broj telefona osobama koje ne poznaju.

Kada posjećujete veb sajtove na telefonima, ne unosite korisnička imena i lozinke.



© 2026 KPMG d.o.o. Podgorica, crnogorsko društvo s ograničenom odgovornošću i firma članica KPMG globalne organizacije nezavisnih firmi članica povezanih sa KPMG International Limited, privatnim engleskim društvom ograničenim garancijom. Sva prava zaštićena.

Bezbjedno i odgovorno korišćenje vještačke inteligencije

Kako alati zasnovani na vještačkoj inteligenciji (AI) postaju sve popularniji, prirodno je da i djeca pokazuju interesovanje za njih. Zato je važno razgovarati sa njima o odgovornom i prikladnom korišćenju tehnologije. Sljedeći savjeti mogu da pomognu vašoj porodici da zajedno istražujete i učite o vještačkoj inteligenciji.

Kako to funkcioniše? Objasnite svojoj djeci kako funkcioniše AI, kako bi mogla da cijene njene prednosti, razumiju potencijalna ograničenja i nauče kako da je efikasno koriste. Dajte im nekoliko primjera s kojima su možda već upoznati kako biste im pomogli da shvate o čemu se radi.

Kako je koristiti? AI alati mogu pomoći djeci da budu kreativna i nauče nove vještine. Razgovarajte sa njima o tehnologijama i alatima koji ih zanimaju. Pomozite im da razmisle na koje načine im ovi alati mogu pomoći u učenju i ličnom razvoju. Podstičite ih da budu kritični prema informacijama koje dobijaju iz nove tehnologije i da koriste svoju kreativnost kako bi dopunili vještačku inteligenciju.

Koji su rizici? Djeca treba da razumiju da vještačka inteligencija ima ograničenja koja mogu dovesti do netačnih i pristrasnih rezultata. Hakeri takođe mogu manipulisati vještačkom inteligencijom mijenjajući podatke, što može dovesti do pogrešnih predikcija. Ne zaboravite da podsjetite djecu da vještačka inteligencija nema emocionalno razumijevanje i ne može zamijeniti ljudske odnose i povezanosti.

Kako bezbjedno koristiti vještačku inteligenciju?

- **Budite svjesni ličnih informacija.**
Djeca ne bi trebalo da dijele osjetljive informacije, kao što su puno ime i prezime, adresa, broj telefona ili finansijski podaci, osim ako koriste pouzdanu platformu i razumiju na koji način se upravlja ličnim podacima.

- **Razumijevanje podešavanja privatnosti.**
Odvojite vrijeme da pregledate i prilagodite postavke privatnosti na AI platformama u skladu sa podešavanjima koja vam odgovaraju.

- **Ne pretjerujte s dijeljenjem.**
Ograničite količinu ličnih informacija koje su javno dostupne i obratite pažnju na to koje se informacije prikupljaju.

- **Razmišljajte kritički.**
Zapamtite da AI sistemi nijesu savršeni i mogu praviti greške. Zamolite djecu da provjeravaju činjenice, upoređuju informacije i razmatraju različite perspektive pre nego što donesu zaključke ili odluke isključivo na osnovu rezultata koje generiše AI.

- **Prijavite neprikladan sadržaj.**
Ako vaše dijete naiđe na uvredljiv ili štetan sadržaj ili doživi neprimjerenu interakciju, naučite ih da to prijave platformi, pružaocu usluga ili odrasloj osobi kojoj vjeruju.

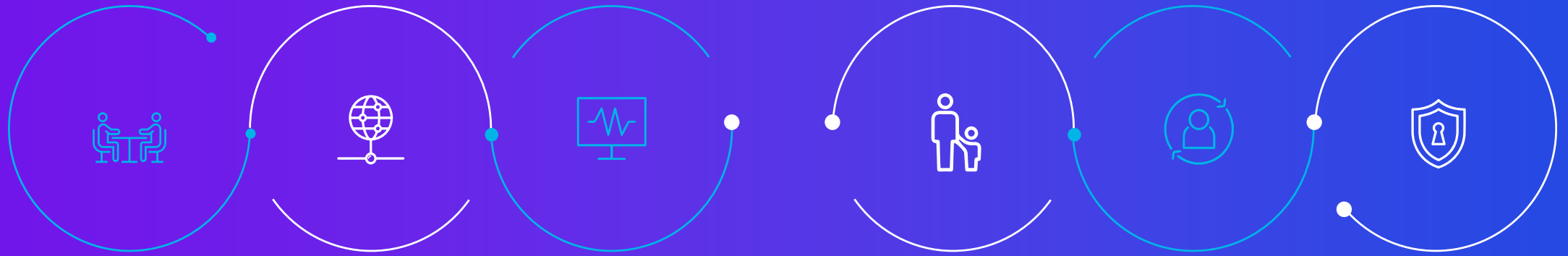
- **Budite oprezni sa porukama koje generiše AI.**
Ako prime neočekivane ili sumnjive poruke sa AI naloga ili čet botova, neka ne dijele lične informacije niti se upuštaju u razgovore koji ih čine nelagodnim.

- **Ne oslanjajte se isključivo na AI.**
Izbjegavajte prekomjerno oslanjanje na vještačku inteligenciju za donošenje odluka. Objasnite im da korišćenje AI za školski rad koji nijesu sami kreirali može biti smatrano plagiranjem ili prevarom. Umjesto toga, upoznajte ih sa obrazovnim AI alatima koji dopunjuju njihovo učenje.

- **Budite informisani.**
Pratite najnovija dostignuća i promjene u oblasti vještačke inteligencije kako biste bolje razumjeli njene mogućnosti, ograničenja i potencijalne rizike. Ovo znanje će omogućiti vašoj porodici da donosi dobro informisane odluke i odgovorno koristi vještačku inteligenciju.

© 2026 KPMG d.o.o. Podgorica, crnogorsko društvo s ograničenom odgovornošću i firma članica KPMG globalne organizacije nezavisnih firmi članica povezanih sa KPMG International Limited, privatnim engleskim društvom ograničenim garancijom. Sva prava zaštićena.

Šest koraka za bezbjednije onlajn okruženje za vašu djecu



01

Budite uključeni svaki dan.

Redovno razgovarajte sa djecom o značaju bezbjednosti na internetu. Pre nego što primijenite bilo kakve mjere zaštite, razgovarajte sa svojom djecom zašto planirate da to uradite, kako bi se osjećala poštovano u vezi s njihovom privatnošću.

02

Roditeljska kontrola.

Razmotrite korišćenje alata za roditeljsku kontrolu kako biste upravljali sve većim brojem uređaja koje vaša djeca koriste i kako biste ih zaštitili na internetu. Ovi alati mogu pomoći tako što blokiraju nepoželjni veb sadržaj, ograničavaju korišćenje rizičnih aplikacija i još mnogo toga. Važno je naučiti kako ih koristiti i redovno ih ažurirati.

03

Podesite bezbjednosne opcije.

Bez obzira na uređaj, aplikaciju ili servis koji vaše dijete koristi, važno je da pravilno podesite bezbjednosne opcije kako biste obezbijedili sigurnije okruženje.

Koristite sajtove poput: internetmatters.org za korak-po-korak podešavanje bezbjednosnih opcija.

Obratite pažnju na privatnost profila, filtriranje neprimjerenog sadržaja, komunikaciju sa nepoznatim osobama i dijeljenje lokacije kako biste dodatno zaštitili svoje dijete na internetu.

04

Roditeljske kontrole.

Razmotrite korišćenje roditeljskih kontrola za ograničavanje vremena pred ekranom, blokiranje aplikacija i praćenje aktivnosti. Ove alate je potrebno podesiti i redovno ažurirati. Upoznajte se i sa njihovim ograničenjima, odnosno aplikacijama koje ne mogu da kontrolišu. Oni ne mogu da zamijene korake 1–3. Otvoreno razgovarajte sa djetetom o praćenju aktivnosti.

05

Pratite i prilagođavajte

Redovno preispitujte navike korišćenja tehnologije u porodici. Tehnologija može stvoriti osjećaj zavisnosti čak i kod odraslih, zato, ako nešto ne funkcioniše, preispitajte situaciju, razgovarajte i prilagodite pristup.

Kako dijete odrasta, razmotrite koje zaštitne mjere možete postepeno ublažiti.

06

Osnove sajber bezbjednosti.

Ne zaboravite na zaštitu od svakodnevnih internet prijetnji:

- Instalirajte antivirusni softver.
- Koristite duže lozinke koje se lako pamte, a teško pogađaju. Razmotrite korišćenje menadžera lozinki.
- Redovno pravite rezervne kopije važnih podataka.
- Vodite računa o digitalnom tragu svoje porodice.
- Pokažite djeci primjere fišing poruka i internet prevara kako bi ih lakše prepoznali.

© 2026 KPMG d.o.o. Podgorica, crnogorsko društvo s ograničenom odgovornošću i firma članica KPMG globalne organizacije nezavisnih firmi članica povezanih sa KPMG International Limited, privatnim engleskim društvom ograničenim garancijom. Sva prava zaštićena.

Dodatne informacije i resursi

Kako biste pomogli djeci i tinejdžerima da razviju bezbjedne navike na internetu, važno je da promovišete odgovorno ponašanje na mreži i ostanete uključeni u njihove digitalne aktivnosti. Za više informacija i savjeta o bezbjednom korišćenju interneta posjetite: kpmg.com/cyberday.



© 2026 KPMG d.o.o. Podgorica, crnogorsko društvo s ograničenom odgovornošću i firma članica KPMG globalne organizacije nezavisnih firmi članica povezanih sa KPMG International Limited, privatnim engleskim društvom ograničenim garancijom. Sva prava zaštićena.

kpmg.com

Informacije sadržane u ovom dokumentu su opšte prirode i nijesu namijenjene okolnostima određenog pojedinca ili pravnog lica. Iako nastojimo da pružimo tačne i pravovremene informacije, ne možemo garantovati da su te informacije tačne onda kada su primljene niti da će ostati tačne u budućnosti. Ne bi trebalo postupati na osnovu takvih informacija bez prethodnog odgovarajućeg stručnog savjeta datog nakon detaljnog ispitivanja određene situacije.

KPMG International Limited je privatno englesko društvo ograničeno garancijom. KPMG International Limited i njegova povezana pravna lica ne pružaju usluge klijentima. Za više informacija o našoj strukturi posjetite kpmg.com/governance.

© 2026 KPMG d.o.o. Podgorica, crnogorsko društvo s ograničenom odgovornošću i firma članica KPMG globalne organizacije nezavisnih firmi članica povezanih sa KPMG International Limited, privatnim engleskim društvom ograničenim garancijom. Sva prava zaštićena.

KPMG ime i logo su zaštitni znaci koje nezavisne firme članice KPMG globalne organizacije koriste u skladu sa licencom.