CDT
Centar za digitalnu transformaciju
E-Mail: cdt@pks.rs
Web: cdt.org.rs
Adresa: Kneza Miloša 12/I,
Beograd - Stari Grad, 11000, Srbija

JAVNI POZIV

Program podrške malim i srednjim preduzećima u Republici Srbiji za unapređenje sajber bezbednosti

1 O CENTRU ZA DIGITALNU TRANSFORMACIJU

Centar za digitalnu transformaciju (CDT) predstavlja organizaciju fokusiranu na unapređenje konkurentnosti mikro, malih i srednjih preduzeća (MMSP) u Republici Srbiji kroz sistemsku podršku digitalnoj transformaciji i implementaciji modernih softverskih i sajber-fizičkih rešenja za unapređenje i optimizaciju poslovnih i proizvodnih procesa, prikupljanje i analizu digitalnih mašinski čitljivih podataka kao preduslova za primenu veštačke inteligencije i dalja unapređenja u sferi poslovnih performansi, smanjenja troškova i povećanja produktivnosti rada. Kao implementacioni partner Ministarstva privrede Republike Srbije, CDT ima ključnu ulogu u sprovođenju mera definisanih Strategijom industrijske politike Republike Srbije za period 2021–2030, posebno u delu koji se odnosi na unapređenje digitalizacije poslovnih modela i industrijske proizvodnje.

U proteklom periodu, CDT je razvio sveobuhvatan i metodološki utemeljen model podrške digitalnoj transformaciji MMSP, zasnovan na kombinaciji strateškog savetovanja, razvoja kompetencija i finansijskih podsticaja za implementaciju digitalnih rešenja. Model je rezultat višegodišnjeg iskustva u radu sa domaćim preduzećima, kao i saradnje sa relevantnim nacionalnim i međunarodnim institucijama i partnerima, čime je obezbeđena njegova usklađenost sa savremenim evropskim praksama i standardima .

Od pokretanja pilot programa 2018. godine, CDT je kontinuirano unapređivao svoj pristup, razvijajući strukturiran okvir koji obuhvata sve ključne faze procesa digitalne transformacije. Tokom ovog perioda, sprovedena su opsežna istraživanja i analize digitalne zrelosti domaćih preduzeća, razvijena metodologija rada sa kompanijama, kao i sistem obuke i sertifikacije konsultanata u skladu sa međunarodnim standardom ISO 17024.

Kroz pomenute programe, CDT je:

- uspostavio bazu sertifikovanih konsultanata sa relevantnim iskustvom u oblasti digitalne transformacije,
- omogućio velikom broju preduzeća da sagledaju sopstveni nivo digitalne zrelosti i identifikuju razvojne potencijale,
- podržao izradu strateških dokumenata za digitalnu transformaciju prilagođenih konkretnim potrebama kompanija,
- omogućio implementaciju konkretnih digitalnih rešenja koja doprinose unapređenju poslovanja.

Programi CDT-a privukli su značajan interes privrede, te je više hiljada preduzeća učestvovalo u različitim fazama programa, dok je više stotina njih uspešno realizovalo projekte digitalne transformacije i implementiralo inovativna tehnološka rešenja.

Jedna od ključnih vrednosti CDT modela ogleda se u njegovom integrisanom i faznom pristupu. Podrška preduzećima organizovana je kroz jasno definisan proces koji obuhvata:

- inicijalnu procenu digitalne zrelosti putem onlajn samoprocene,
- pripremnu fazu i razumevanje poslovnog konteksta preduzeća,
- ekspertsku analizu koja identifikuje snage, slabosti i razvojne prilike,
- razvoj strategije digitalne transformacije,
- implementaciju prioritetnih rešenja,
- verifikaciju rezultata i ostvarenih efekata .

Navedeni pristup omogućava preduzećima da digitalnoj transformaciji pristupe sistematično, uz jasno definisane ciljeve, merljive rezultate i kontinuiranu stručnu podršku. Poseban kvalitet ovog modela ogleda se u činjenici da su rezultati procesa (uključujući analize, strategije i implementirana rešenja) u potpunosti u vlasništvu preduzeća, čime se obezbeđuje dugoročna održivost i primenljivost postignutih rezultata na način da preduzeća mogu nastaviti proces digitalne transformacije i nakon okončanja programa

CDT je kroz Digitalnu akademiju razvio i edukativnu komponentu programa, koja omogućava vlasnicima i menadžerima MMSP da unaprede svoja znanja iz oblasti digitalne transformacije, poslovnih modela, marketinga, poslovnih procesa i primene savremenih tehnologija, čime se dodatno jačaju interni kapaciteti preduzeća za upravljanje promenama.

Zahvaljujući ovakvom sistemskom pristupu, CDT je uspostavio održiv i skalabilan model podrške koji doprinosi modernizaciji poslovanja MMSP, jačanju njihove konkurentnosti i boljoj integraciji u savremene, digitalno vođene lance vrednosti.

1.1 Razvoj novih modela podrške mikro, malim i srednjim preduzećima u procesu digitalne transformacije

Polazeći od dosadašnjih rezultata i iskustava u sprovođenju programa podrške digitalnoj transformaciji MMSP, kao i od uočenih trendova u razvoju digitalne ekonomije, Centar za digitalnu transformaciju (CDT) identifikovao je sajber bezbednost kao jedan od ključnih prioriteta za narednu fazu unapređenja konkurentnosti privrede. Sajber bezbednost je kao oblast bila zanemarena u prethodnim programima, dok stepen sajber rizika rastao eksponencijalno srazmerno stepenu digitalizacije i digitalne transformacije svake pojedinačne kompanije - MMSP. Svaki MMSP koji svoje celokupno poslovanje i proizvodnju bazira na digitalnim podacima i alatima utoliko je od istih i zavisan i svaki slučajni ili zlonamerni poremećaj može u potpunosti zaustavili ili značajno usporiti rad ostavljajući malo prostora za rezervne opcije vraćanja na tradicionalni manuelni i “papirni” rad.

Digitalna transformacija poslovanja, kao ključni pokretač rasta i konkurentnosti, neminovno podrazumeva sve intenzivnije oslanjanje preduzeća na digitalne tehnologije, informacione sisteme i obradu podataka. U takvom okruženju, sajber bezbednost postaje neodvojivi element digitalne transformacije i mora biti uvažena "po definiciji" (princip *Cybersecurity-by-Default*), jer nivo zaštite informacionih sistema direktno utiče na kontinuitet poslovanja, pouzdanost procesa i očuvanje poverenja svih stejkholdera (korisnika i partnera). Osim toga, negativna iskustva zbog sajber napada može napraviti i reputacionu štetu kompanijama, ugroziti poslovanje, konkurentnost, a menadžment obeshrabriti da nastavi proces promena i modernizacije u kompaniji.

Uspešna integracija sajber bezbednosti, ili i šire, informacione bezbednosti kao deo poslovne kulture unutar jedne kompanije predstavlja temelj da se na uspešne priče digitalizacije i digitalne transformacije dalje razvijaju bez prepreka. Razvoj kulture sajber higijene jednako je važan i uporedo neophodan koliko i implementacija softverskih i hardverskih i hibridnih rešenja za sajber bezbednost, te redovni auditi trenutnog stanja sajber bezbednosti.

Postizanje navedenih ciljeva ogleda se kroz nekoliko strateških slojeva koje je neophodno razvijati posebno ali sagledavati integralno, a to su:

- Prevencija
- Detekcija
- Otpornost
- Oporavak

Regulatorni i strateški okvir Republike Srbije u oblasti sajber bezbednosti definisan je Zakonom o informacionoj bezbednosti (Službeni glasnik Republike Srbije, br. 91/2025), te podzakonskim aktima kroz pravilnike predviđene Zakonom, kojima će biti uspostavljen sistem obaveza i smernica za unapređenja bezbednosti digitalnih sistema, načina procene, izbegavanja i upravljanja rizicima, jačanje otpornosti privrede i institucija. Strategijom razvoja informacionog društva i informacione bezbednosti za period 2021–2026 (Službeni glasnik Republike Srbije, br. 86/2021) dat je sistemski i institucionalni okvir o zadacima i zaduženjima svih institucija i pravnih subjekata u smislu postizanja sveobuhvatnog nivoa zaštite sajber prostora i informacione bezbednosti uporedo sa razvojem informacionog društva i digitalnom transformacijom privrede. U navedenom okviru, CDT prepoznaje svoju ulogu u domenu razvoja informacione bezbednosti privrede sa fokusom na MMSP u Republici Srbiji. U tom kontekstu, digitalna transformacija više ne podrazumeva isključivo uvođenje novih tehnologija i unapređenje poslovnih modela, već i integraciju principa sajber bezbednosti, upravljanja rizicima i organizacione otpornosti kao sastavnih elemenata savremenog i održivog poslovanja.

1.2 Program podrške MMSP sa fokusom na sajber bezbednost

Na osnovu **Ugovora o saradnji u sprovođenju mera u okviru *Posebnog cilja 1: Unapređena digitalizacija poslovnih modela industrijske proizvodnje* Akcionog plana za sprovođenje Strategije industrijske politike Republike Srbije od 2021. do 2030. godine, za period od 2024. godine do 2025. godine, za 2025. godinu** sa Ministarstvom privrede Republike Srbije (u daljem tekstu: Ugovor), kojim se uređuje sprovođenje programa podrške unapređenju digitalne transformacije privrede, a imajući u vidu dosadašnje rezultate, identifikovane potrebe mikro, malih i srednjih preduzeća, kao i savremene izazove u oblasti digitalnog poslovanja i sajber bezbednosti, Centar za digitalnu transformaciju (CDT) raspisuje Javni poziv za pružanje podrške mikro, malim i srednjim preduzećima u procesu digitalne transformacije sa fokusom na unapređenje sajber bezbednosti (u daljem tekstu Program).

Javnim pozivom CDT nastavlja sa daljim razvojem i unapređenjem postojećeg modela podrške, proširujući njegov obuhvat kroz integraciju aspekata upravljanja informacionom i sajber bezbednošću, zaštite podataka i jačanja otpornosti poslovanja, u cilju stvaranja sigurnog, pouzdanog i održivog digitalnog okruženja za poslovanje MMSP u Republici Srbiji.

Program podrške koji je predmet ovog javnog poziva omogućiće preduzećima (MMSP) pristup stručnoj i metodološki utemeljenoj podršci, kao i finansijskim podsticajima za razvoj i implementaciju digitalnih i bezbednosnih rešenja, čime se doprinosi njihovoj dugoročnoj konkurentnosti, usklađenosti sa relevantnim regulatornim okvirom i otpornosti na savremene digitalne i sajber rizike.

2 UVOD I OBRAZLOŽENJE PROGRAMA

2.1 Kontekst sajber pretnji u Republici Srbiji

Republika Srbija se suočava sa rastućim izazovima u domenu informacione bezbednosti. Prema podacima kompanije Kaspersky objavljenim u decembru 2024. godine, korisnici u Srbiji su prema stepenu rizika od sajber pretnji rangirani na 9. mestu[1] u svetu. Posebno zabrinjavaju trendovi u oblasti malicioznog softvera: broj ransomware detekcija uvećan je za više od 70% u odnosu na prethodnu godinu, dok je finansijski i bankarski malver zabeležio višestruki porast.

Broj neprijavljenih napada je značajno veći od onoga što zvanična statistika pokazuje, a u delu privrede posebno malih i srednjih preduzeća, koji nemaju ili imaju ograničene kapacitete internih IT službi, mnogi od tih napada ostaju i neprimećeni ugrožavajući interne podatke o ličnosti zaposlenih, poslovne podatke sa različitim kvalifikacijama tajnosti i u konačnom kreirajući reputacioni rizik za samu kompaniju.

2.2 Mala i srednja preduzeća kao prioritetna ciljna grupa

Sektor mikro, malih i srednjih preduzeća i preduzetnika (MSPP) predstavlja okosnicu srpske privrede. Prema podacima Republičkog zavoda za statistiku[2], ovaj sektor čini ključnu strukturu privrede Republike Srbije sa značajnim učešćem u broju privrednih subjekata i zaposlenosti.

Istraživanje kompanije Kaspersky[3] sprovedeno na uzorku od 880 ispitanika iz MSP sektora u Srbiji i 15 zemalja Evrope i Severne Afrike ukazuje na značajne izazove:

- 70% MSP kompanija u Srbiji nema jasnu, primenljivu strategiju sajber bezbednosti
- Manje od 30% poseduje specijalizovani tim zadužen za sajber bezbednost
- Trećina menadžmenta nema dovoljno razumevanja za značaj sajber bezbednosti
- 40% nije sigurno da li su njihove trenutne mere zaštite dovoljne
- Trećina ne razume zakonske obaveze u oblasti sajber bezbednosti

2.3 Regulatorni okvir

Republika Srbija je u oktobru 2025. godine usvojila novi Zakon o informacionoj bezbednosti (Sl. glasnik RS br. 91/2025) koji je stupio na snagu 31. oktobra 2025. godine. Ovaj zakon uvodi sistemske promene usklađene sa Direktivom EU 2022/2555 (NIS2), uključujući:

- Formiranje Kancelarije za informacionu bezbednost (operativna od 1. januara 2027)

---

[1] *Izvor: Kaspersky istraživanje, decembar 2024; objavljeno na Nova Ekonomija, 5.12.2024*

[2] *RZS publikacija 'Preduzeca po velicini i preduzetnici u Republici Srbiji, 2021-2023', jul 2025*

[3] *Kaspersky globalno istraživanje MSP sektora, objavljeno decembar 2025*

- Kategorije prioritetnih i važnih operatora IKT sistema
- Obaveze prijavljivanja incidenata u roku od 24 sata
- Proširene zahteve u oblasti upravljanja rizicima, kontinuiteta poslovanja i bezbednosti lanca snabdevanja

Zakon o informacionoj bezbednosti ne primenjuje se automatski na sva mikro, mala i srednja preduzeća, već uvodi pristup zasnovan na značaju IKT sistema za društvo i ekonomiju. MSP postaju obveznici zakona samo ukoliko upravljaju IKT sistemima od posebnog značaja, odnosno ukoliko njihove usluge imaju sistemski uticaj ili predstavljaju deo lanca vrednosti kritične infrastrukture. Međutim, u praksi se očekuje da će i MSP koja nisu direktno obuhvaćena zakonom biti pod sve većim pritiskom da usklade svoje poslovanje sa zahtevima informacione bezbednosti, usled zahteva partnera i regulatornog okruženja.

2.4 Opšti cilj programa

Opšti cilj Programa je unapređenje konkurentnosti i održivosti mikro, malih i srednjih preduzeća u Republici Srbiji kroz podršku digitalnoj transformaciji poslovanja, uz integraciju principa sajber bezbednosti, upravljanja rizicima i jačanja otpornosti na savremene digitalne pretnje, a što obuhvata:

1. Podizanje nivoa zrelosti sajber bezbednosti – Strukturiran pristup proceni trenutnog stanja i definisanju prioriteta za unapređenje

2. Priprema za regulatorne obaveze – Usklađivanje sa zahtevima Zakona 91/2025 pre potpune primene u 2027. godini

3. Smanjenje ranjivosti – Implementacija prioritetnih tehničkih i organizacionih mera zaštite

4. Jačanje svesti i kompetencija – Edukacija zaposlenih i menadžmenta o savremenim sajber pretnjama

5. Podrška konkurentnosti – Omogućavanje MSP sektoru da ispuni uslove partnera i klijenata u EU lancima vrednosti

2.5 Posebni ciljevi programa

Posebni ciljevi Programa su:

1. Unapređenje digitalne zrelosti MMSP kroz razvoj i implementaciju digitalnih rešenja u poslovnim procesima, proizvodima i uslugama;
2. Jačanje kapaciteta MMSP u oblasti sajber bezbednosti, uključujući identifikaciju rizika, uspostavljanje odgovarajućih organizacionih, tehničkih i proceduralnih mera zaštite;
3. Podrška usklađivanju poslovanja MMSP sa relevantnim regulatornim okvirom, uključujući Zakon o informacionoj bezbednosti i prateće podzakonske akte, kao i praksu usklađenu sa evropskim standardima;
4. Razvoj otpornosti poslovanja MMSP kroz unapređenje sposobnosti prevencije, detekcije i odgovora na sajber incidente, kao i obezbeđivanje kontinuiteta poslovanja;
5. Podsticanje sistemskog pristupa digitalnoj transformaciji, kroz povezivanje strateškog planiranja, implementacije i praćenja efekata digitalnih i bezbednosnih rešenja;
6. Jačanje kompetencija zaposlenih i menadžmenta MMSP u oblasti digitalnih tehnologija i informacione bezbednosti;
7. Podrška integraciji MMSP u savremene digitalne lance vrednosti, uz obezbeđivanje sigurnog i pouzdanog poslovnog okruženja.

3 FORMALNI USLOVI ZA PRIJAVU MALIH I SREDNJIH PREDUZEĆA I NAČIN REALIZACIJE PROGRAMA

3.1 Formalni uslovi za učešće kompanija u Programu

Pravo učešća u Programu imaju mikro, mala i srednja preduzeća koja ispunjavaju sledeće formalne uslove:

- da su registrovana u Agenciji za privredne registre Republike Srbije najkasnije do 01.01.2025. godine;
- da su u većinskom privatnom vlasništvu;
- da nad preduzećem nije pokrenut stečajni postupak ili postupak likvidacije;
- da imaju najmanje 5, a najviše 249 zaposlenih na dan prijave na Javni poziv;
- da su izmirila sve obaveze po osnovu poreza i doprinosa u skladu sa važećim propisima;
- da im nije izrečena mera zabrane obavljanja delatnosti u 2025. godini;
- da su podaci navedeni u Izjavi o korišćenju državne pomoći male vrednosti („de minimis“ pomoć) tačni, te da preduzeće realizacijom Programa ne prelazi dozvoljeni iznos državne pomoći male vrednosti u skladu sa važećim propisima.

Ispunjenost navedenih uslova proverava se na osnovu podataka dostavljenih kroz proces prijave, uključujući onlajn upitnik i prateću dokumentaciju.

Za tačnost i istinitost podataka dostavljenih kroz online upitnik odgovorno je preduzeće – aplikant. U slučaju da u procesu provere tačnosti i istinitosti podataka Centar za digitalnu transformaciju utvrdi da su podaci svesno i namerno dostavljeni netačno ili neistinito sa ciljem da se Centar za digitalnu transformaciju dovede u zabludu u procesu odlučivanja i izbora, Centar za digitalnu transformaciju će poduzeti zakonom propisane mere.

Centar za digitalnu transformaciju zadržava pravo da, u cilju obezbeđenja kvaliteta i ostvarivanja ciljeva Programa, nakon sprovedene analize prijave i procene potencijala preduzeća, donese odluku o odbijanju prijave, čak i u slučaju kada su formalni uslovi ispunjeni.

3.2 Rok za podnošenje prijava i dinamika realizacije Programa

Rok za podnošenje prijava na Javni poziv iznosi 7 dana od dana objavljivanja Javnog poziva na zvaničnoj internet stranici Centra za digitalnu transformaciju.

Imajući u vidu da je broj preduzeća koja mogu biti obuhvaćena Programom ograničen raspoloživim sredstvima, CDT zadržava pravo da, nakon sprovedenog postupka selekcije, odabere preduzeća koja će učestvovati u Programu, kao i da formira listu rezervnih kandidata.

U slučaju da odabrana preduzeća ne ispune formalne uslove, odustanu od učešća u Programu ili ne pristupe potpisivanju ugovora u predviđenom roku, CDT zadržava pravo da uključi preduzeća sa liste rezervnih kandidata ili da ponovi Javni poziv, u celini ili delimično.

3.3 Obim i vrsta podrške u okviru Programa

Učešćem u Programu, mikro, mala i srednja preduzeća ostvaruju pristup stručnoj i finansijskoj podršci usmerenoj na unapređenje digitalne transformacije sa posebnim fokusom na sajber bezbednost.

Program omogućava preduzećima da:

- sagledaju sopstveni nivo zrelosti u oblasti sajber bezbednosti, kroz strukturiranu procenu postojećih kapaciteta, praksi i rizika u poslovanju;
- definišu jasne pravce daljeg razvoja, kroz izradu mape puta za unapređenje nivoa bezbednosti informacionih sistema, prilagođene specifičnostima i potrebama svakog pojedinačnog preduzeća;
- razviju konkretne projekte koji imaju za cilj unapređenje digitalne i bezbednosne infrastrukture, kroz definisanje projektnog zadatka;
- ostvare finansijsku podršku za implementaciju odabranih rešenja, u vidu subvencija za nabavku i uvođenje digitalnih i bezbednosnih tehnologija, u skladu sa definisanim projektnim zadatkom;
- ostvare pristup stručnoj konsultantskoj podršci bez direktnog finansijskog opterećenja za preduzeće, pri čemu troškove angažovanja sertifikovanih konsultanata u okviru Programa u celosti pokriva CDT;
- zadrže punu autonomiju u donošenju poslovnih odluka, uključujući izbor rešenja i dobavljača, kao i odgovornost za realizaciju projekta, uz obezbeđenu stručnu podršku u procesu donošenja odluka.

Finansijska podrška u okviru Programa realizuje se po principu refundacije dela troškova nakon uspešne implementacije projekta i izmirenja obaveza prema dobavljačima, čime se podstiče odgovorno planiranje i realizacija investicija.

3.4 Dodatne pogodnosti za učesnike Programa

Pored stručne i finansijske podrške za unapređenje digitalne transformacije i sajber bezbednosti, preduzećima koja učestvuju u Programu obezbeđuju se i dodatne pogodnosti usmerene na razvoj kompetencija i dugoročno jačanje kapaciteta:

- besplatan pristup Digitalnoj akademiji CDT-a, koja omogućava zaposlenima i menadžmentu da unaprede znanja iz oblasti digitalne transformacije, poslovnih modela, primene savremenih tehnologija i veštačke inteligencije;
- mogućnost pohađanja programa obuka CDT trening centra uz subvencionisanu cenu, odnosno uz popust od 50% na kurseve koji vode ka sticanju relevantnih stručnih i profesionalnih sertifikata.

Na ovaj način, Program ne doprinosi samo unapređenju tehnoloških rešenja u preduzećima, već i sistemskom razvoju znanja i veština, kao ključnog preduslova za održivu digitalnu transformaciju i efikasno upravljanje sajber rizicima.

3.5 Postupak prijave na Javni poziv

Prijava na Javni poziv vrši se elektronskim putem, popunjavanjem onlajn prijavnog formulara koji je dostupan na zvaničnoj internet stranici CDT-a na LINKU.

U okviru prijave, preduzeća su u obavezi da unesu osnovne podatke o poslovanju, nakon čega pristupaju popunjavanju strukturiranog upitnika za preliminarnu procenu nivoa zrelosti u oblasti sajber bezbednosti.

Upitnik je koncipiran na osnovu razvijene metodologije za procenu zrelosti sajber bezbednosti mikro, malih i srednjih preduzeća, koja je usklađena sa relevantnim međunarodnim standardima i regulatornim okvirom (uključujući NIS2 Direktivu, ISO/IEC 27001 i druge referentne okvire). Njegova svrha je da obezbedi inicijalni, objektivan uvid u postojeće kapacitete, prakse i izazove preduzeća u domenu sajber bezbednosti.

Popunjavanje upitnika ima isključivo dijagnostičku funkciju i ne predstavlja eliminatorni kriterijum za učešće u Programu. Cilj ovog instrumenta je da omogući adekvatno razumevanje početnog stanja preduzeća, kao i da posluži kao osnova za dalje prilagođavanje podrške u okviru Programa.

Na ovaj način obezbeđuje se da proces selekcije i daljeg rada sa preduzećima bude zasnovan na principima objektivnosti, transparentnosti i usklađenosti sa stvarnim potrebama korisnika.

3.6 Izbor kompanija za učešće u Programu

Izbor preduzeća za učešće u Programu vrši se na osnovu sveobuhvatne analize podnetih prijava, uzimajući u obzir više kriterijuma koji omogućavaju procenu spremnosti, potreba i potencijala preduzeća za uspešnu realizaciju aktivnosti u okviru Programa.

U procesu selekcije posebno se vrednuju sledeći kriterijumi:

- nivo spremnosti preduzeća za aktivno učešće u Programu, uključujući angažovanost menadžmenta i raspoloživost resursa za realizaciju planiranih aktivnosti;
- kapacitet preduzeća za uspešnu implementaciju projekata, uključujući organizacione, tehničke i operativne kapacitete;
- identifikovani nivo rizika i potreba za unapređenjem sajber bezbednosti, u skladu sa rezultatima preliminarne procene sprovedene kroz prijavni upitnik;
- potencijal predloženih aktivnosti da doprinesu unapređenju bezbednosti informacionih sistema, kontinuiteta poslovanja i ukupne digitalne otpornosti preduzeća;
- doprinos uravnoteženoj zastupljenosti različitih sektora, veličina i tipova preduzeća, kao i geografsku diversifikaciju, u okviru Programa.

Gore pobrojani parametri se prikupljaju kroz prijavnu formu na već objavljenom linku.

3.7 Pripremna faza

Nakon sprovedenog postupka selekcije i izbora preduzeća za učešće u Programu, započinje pripremna faza, koja traje do 10 dana od dana obaveštavanja preduzeća o izboru.

U okviru ove faze, odabranom preduzeću se dodeljuje konsultant, čime se uspostavlja osnov za dalju realizaciju aktivnosti u okviru Programa.

Tokom pripremne faze, preduzeće je u obavezi da dostavi sledeću dokumentaciju:

- dokaz o izmirenim obavezama po osnovu poreza i doprinosa (poresko uverenje);
- potpisan ugovor o učešću u Programu;
- izjavu o korišćenju državne pomoći male vrednosti („de minimis“ pomoć) u prethodne tri fiskalne godine.

Dostavljanje kompletne i validne dokumentacije predstavlja uslov za uključivanje preduzeća u dalju realizaciju Programa.

Po prijemu i verifikaciji dokumentacije od strane CDT-a, stiču se uslovi za početak rada sa preduzećem, u skladu sa definisanom metodologijom i planiranim aktivnostima.

U slučaju da preduzeće ne dostavi traženu dokumentaciju u predviđenom roku ili odustane od učešća, CDT zadržava pravo da njegovo mesto dodeli drugom preduzeću, u skladu sa utvrđenom procedurom.

Potpisivanjem ugovora preduzeće se obavezuje na aktivno učešće u Programu, to jest aktivno angažovanje preduzeća u svim fazama njegove realizacije, uključujući saradnju sa dodeljenim konsultantom, pravovremeno dostavljanje potrebnih informacija i dokumentacije, kao i donošenje odluka neophodnih za sprovođenje aktivnosti.

U slučaju da preduzeće ne ispunjava navedene obaveze, ne učestvuje aktivno u realizaciji Programa ili neopravdano odustane od daljih aktivnosti, CDT zadržava pravo da obustavi njegovo učešće u Programu i uključi drugo preduzeće u skladu sa utvrđenom procedurom.

3.8 Rad sa mikro, malim i srednjim preduzećima

Rad sa mikro, malim i srednjim preduzećima u okviru Programa zasniva se na unapred definisanom, strukturiranom i metodološki utemeljenom pristupu, razvijenom sa ciljem da omogući objektivnu procenu postojećeg stanja, jasno definisanje prioriteta i usmeravanje preduzeća ka konkretnim merama za unapređenje sajber bezbednosti.

Polaznu osnovu za rad sa preduzećima predstavlja Metodologija za procenu zrelosti sajber bezbednosti za mala i srednja preduzeća, razvijena kao sveobuhvatan dijagnostički okvir za procenu spremnosti organizacija za sajber pretnje i bezbednu digitalnu transformaciju. Metodologija izrađena je u skladu sa relevantnim međunarodnim i nacionalnim referentnim okvirima, uključujući NIS2 Direktivu, ISO/IEC 27001:2022, NIST Cybersecurity Framework 2.0 i Zakon o informacionoj bezbednosti Republike Srbije. Pored toga, metodologija je inspirisana pristupom World Bank Digital Government Readiness Assessment (DGRA), uz prilagođavanje specifičnostima poslovanja mikro, malih i srednjih preduzeća.

Metodologija procene zasniva se na petostepenom modelu zrelosti, koji omogućava sagledavanje razvoja organizacije od početnog, ad-hoc pristupa sajber bezbednosti do nivoa optimizovanog i kontinuirano unapređivanog sistema upravljanja sajber rizicima. Procena obuhvata deset ključnih domena, među kojima su upravljanje i rizik, upravljanje imovinom, identitet i pristup, mrežna bezbednost, endpoint bezbednost, aplikativna bezbednost, zaštita podataka, bezbednosne operacije, upravljanje incidentima i kontinuitet poslovanja, kao i svest i obuka zaposlenih. Bodovanje se vrši na osnovu unapred definisanih kriterijuma i dokaza, a ne isključivo na osnovu izjava predstavnika preduzeća, čime se obezbeđuje objektivnost i uporedivost rezultata.

Na osnovama ove metodologije procene razvijena je i metodologija rada sa preduzećima u okviru Programa. Takav pristup omogućava da se rezultati procene neposredno prevedu u preporuke, prioritete, mapu puta unapređenja i definisanje konkretnih projekata za podršku. Time se obezbeđuje da Program ne ostane na nivou dijagnostike, već da procena predstavlja početnu tačku za planirano, ciljano i merljivo unapređenje nivoa sajber bezbednosti svakog uključenog preduzeća. U skladu sa principima same metodologije, rad sa preduzećima zasniva se na kolaborativnom pristupu, prilagođenosti specifičnostima svakog korisnika, akcionoj orijentisanosti i kontinuiranom unapređenju.

Rad sa preduzećima u okviru Programa može se realizovati neposredno, u prostorijama preduzeća, putem onlajn komunikacionih alata ili kombinovano, u zavisnosti od specifičnosti aktivnosti i organizacionih potreba učesnika. Izbor modaliteta realizacije ne utiče na sadržaj i kvalitet pružene podrške, već ima za cilj obezbeđenje efikasnog i fleksibilnog sprovođenja Programa.

Rad sa preduzećima odvija se kroz sledeće faze kako je navedeno u nastavku.

Faza 1: Procena zrelosti kompanije u domenu sajber bezbednosti

Prvi korak podrazumeva sprovođenje detaljne procene trenutnog nivoa zrelosti kompanije u oblasti sajber bezbednosti. Procena se vrši korišćenjem razvijene metodologije, kroz strukturiran pristup koji obuhvata organizacione, tehničke i procesne aspekte poslovanja. Cilj ove faze je da se utvrdi početna pozicija kompanije, identifikuju ključni rizici, postojeći kapaciteti i najznačajniji nedostaci u domenu sajber bezbednosti. Procena se ne posmatra kao izolovani administrativni korak, već kao stručna dijagnostika koja predstavlja osnov za sve dalje aktivnosti u okviru Programa. Metodologija posebno polazi od principa da se procena zasniva na dokazima i

proverljivim elementima, uz sagledavanje ljudi, procesa i tehnologije kao tri međusobno povezana stuba sajber bezbednosti.

Po završetku procesa procene zrelosti, angažovani konsultant izrađuje izveštaj o proceni zrelosti sajber bezbednosti kompanije, koji sadrži pregled utvrđenog stanja, identifikovane ključne rizike i nedostatke, kao i inicijalne preporuke za unapređenje. Izveštaj se dostavlja kompaniji na uvid, a potom i Centru za digitalnu transformaciju radi razmatranja i davanja saglasnosti, čime se obezbeđuje jedinstven kvalitet i usklađenost daljih aktivnosti u okviru Programa.

Faza 2: Definisanje mape puta unapređenja zrelosti kompanije u domenu sajber bezbednosti

Na osnovu nalaza procene izrađuje se mapa puta unapređenja, kao planski dokument koji definiše preporučene pravce razvoja kompanije u oblasti sajber bezbednosti. Mapa puta omogućava prevođenje nalaza procene u skup prioritetnih mera i aktivnosti koje su usklađene sa nivoom rizika, regulatornim zahtevima, poslovnim potrebama i raspoloživim resursima kompanije. Stoga se Mapa puta može smatrati instrumentom za postepeno i realno unapređenje zrelosti, budući da omogućava sagledavanje prioriteta u vremenskom, organizacionom i investicionom smislu. Time se kompaniji daje jasan okvir za donošenje odluka o tome koje korake treba preduzeti najpre, a koje u srednjem roku, radi postizanja višeg nivoa sajber otpornosti. Sama metodologija predviđa prioritetizaciju remedijacije upravo na osnovu procene rizika, regulatorne relevantnosti i poslovne kritičnosti.

Faza 3: Izbor i definisanje prioritetnog projekta

Nakon definisanja mape puta, pristupa se identifikaciji i razradi prioritetnog projekta koji će biti predmet podrške u okviru Programa. Prioritetni projekat predstavlja konkretan skup mera ili rešenje koje ima najveći potencijal da unapredi bezbednosni položaj kompanije, smanji ključne rizike i doprinese jačanju otpornosti poslovanja. U ovoj fazi se, na osnovu rezultata procene i mape puta, definišu ciljevi projekta, njegov obim, očekivani rezultati, osnovni tehnički i funkcionalni zahtevi, kao i povezanost projekta sa identifikovanim prioritetima kompanije. Navedeni pristup obezbeđuje da izbor projekta ne bude zasnovan na parcijalnim ili ad hoc odlukama, već na prethodno sprovedenoj stručnoj analizi i objektivno utvrđenim potrebama.

Po završetku izrade mape puta unapređenja i definisanja prioritetnog projekta, konsultant izrađuje objedinjeni izveštaj koji obuhvata detaljan plan aktivnosti, prioritetizaciju mera i razrađen projektni zadatak. Izveštaj se dostavlja kompaniji kao osnova za donošenje poslovnih odluka, a zatim i Centru za digitalnu transformaciju na saglasnost, čime se obezbeđuje da predložene aktivnosti i projekat budu u skladu sa ciljevima Programa i rezultatima sprovedene procene.

Faza 4: Nabavka definisanog rešenja od strane kompanije

Nakon definisanja prioritetnog projekta, kompanija pristupa nabavci odgovarajućeg rešenja u skladu sa projektnim zadatkom i sopstvenim poslovnim potrebama. U Fazi 4 posebno je važno naglasiti da kompanija zadržava punu autonomiju u donošenju poslovnih odluka, uključujući izbor dobavljača i konačnog rešenja. Uloga Programa u ovom koraku jeste da obezbedi da je odluka kompanije zasnovana na prethodno sprovedenoj proceni, jasno definisanim prioritetima i stručno oblikovanom projektnom zadatku, čime se smanjuje rizik od neadekvatnih investicija i povećava verovatnoća da odabrano rešenje zaista odgovori na identifikovane bezbednosne izazove.

Faza 5: Verifikacija nabavke i implementacije rešenja

Po sprovedenoj nabavci i implementaciji, vrši se verifikacija realizovanog projekta. Cilj ovog koraka je da se potvrdi da je nabavljeno i implementirano rešenje u skladu sa definisanim projektnim zadatkom, prioritetima utvrđenim kroz procenu i mapom puta unapređenja. Verifikacija predstavlja važan mehanizam obezbeđenja kvaliteta i usklađenosti,

jer omogućava da se utvrdi da li je podrška ostvarila svoju svrhu i da li je kompanija realizovala projekat na način koji odgovara ciljevima Programa. Istovremeno, ovaj korak predstavlja osnov za dalje administrativno-finansijske aktivnosti u okviru Programa.

Faza 6: Refundacija subvencionisanog iznosa

U okviru Programa, odabranim preduzećima obezbeđuje se finansijska podrška za realizaciju prioritetnog projekta unapređenja sajber bezbednosti.

Finansijska podrška se dodeljuje u formi subvencije u maksimalnom iznosu do 8.500,00 EUR u dinarskoj protivvrednosti bez PDV, po pojedinačnom preduzeću.

Podrška se odnosi na projekte čija je ukupna vrednost najmanje 10.000,00 EUR bez PDV, pri čemu preduzeće snosi razliku između ukupne vrednosti investicije i iznosa odobrene subvencije. U slučaju projekata veće vrednosti, iznos subvencije ostaje nepromenjen.

Isplata subvencionisanih sredstava vrši se po principu refundacije, nakon što preduzeće u potpunosti realizuje projekat i izmiri obaveze prema dobavljaču.

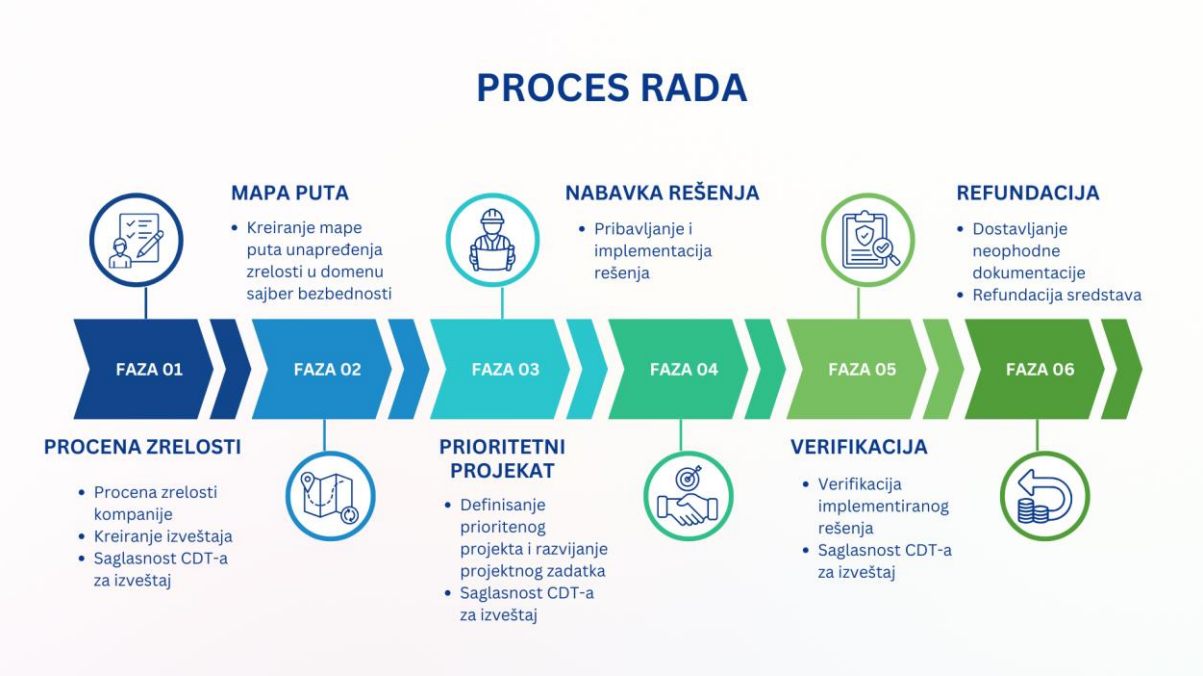
Da bi ostvarilo pravo na refundaciju, preduzeće je u obavezi da dostavi:

- fakturu dobavljača za nabavljeno i implementirano rešenje;
- dokaz o izvršenom plaćanju u celosti;
- zahtev za isplatu subvencionisanih sredstava;
- pozitivan izveštaj o verifikaciji projekta, sačinjen od strane angažovanog konsultanta, kojim se potvrđuje da je rešenje implementirano u skladu sa definisanim projektnim zadatkom i ciljevima Programa.

Refundacija se vrši isključivo za projekte koji su uspešno implementirani i verifikovani, čime se obezbeđuje namensko korišćenje sredstava i ostvarenje planiranih efekata Programa.

CDT zadržava pravo da odbije zahtev za refundaciju u celosti ili delimično, ukoliko se utvrdi da realizovani projekat nije u skladu sa definisanim projektnim zadatkom, ciljevima Programa ili rezultatima procene i mape puta unapređenja.

Takođe, zahtev za refundaciju može biti odbijen ukoliko dostavljena dokumentacija nije potpuna, verodostojna ili u skladu sa zahtevima Programa, kao i u slučajevima kada implementirano rešenje nije funkcionalno ili nije adekvatno integrisano u poslovne procese preduzeća.



3.9 Vrste prihvatljivih rešenja

U okviru Programa, podrška se odnosi na nabavku i implementaciju rešenja iz oblasti sajber bezbednosti koja doprinose unapređenju nivoa zrelosti preduzeća i jačanju njegove digitalne otpornosti.

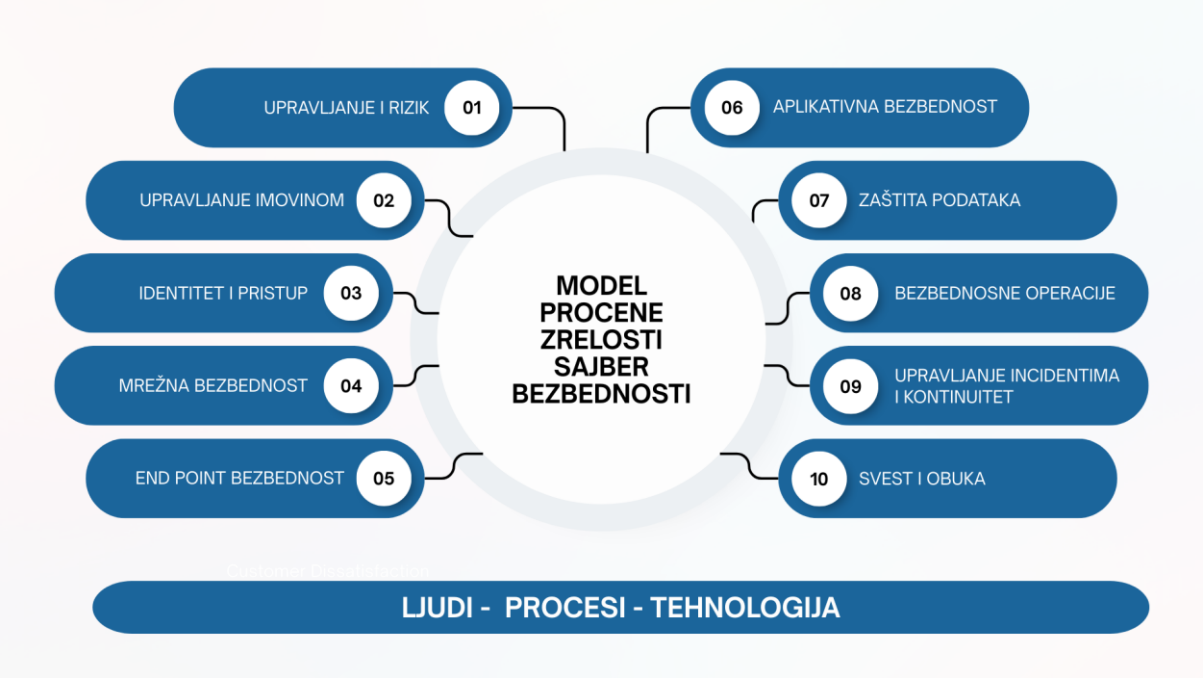
Prihvatljivim se smatraju rešenja koja podrazumevaju uspostavljanje ili unapređenje funkcionalnog sistema sajber bezbednosti, uključujući tehničke, organizacione i operativne komponente, a ne isključivo pojedinačne alate ili parcijalne intervencije.

Rešenja koja su predmet podrške treba da budu implementirana do nivoa pune tehničke i operativne funkcionalnosti, što podrazumeva da su adekvatno instalirana i konfigurisana, integrisana u postojeće poslovne i IT procese kompanije, aktivno korišćena u svakodnevnom radu, kao i praćena odgovarajućim procedurama, pravilima korišćenja i kapacitetima za upravljanje i održavanje.

U skladu sa rezultatima procene zrelosti i definisanom mapom puta unapređenja, podrška može obuhvatiti sledeće kategorije rešenja:

- Rešenja za upravljanje sajber bezbednošću, rizicima i IT imovinom, uključujući uspostavljanje politika i procedura, sistema upravljanja bezbednošću informacija (ISMS), procene rizika, kao i identifikaciju, klasifikaciju i upravljanje IT imovinom;
- Rešenja za upravljanje identitetima i pristupom (IAM), uključujući kontrolu pristupa, višefaktorsku autentifikaciju, upravljanje privilegovanim nalozima i centralizovano upravljanje korisnicima;
- Rešenja za zaštitu mreže, infrastrukture i krajnjih uređaja, uključujući zaštitu mrežnog saobraćaja, segmentaciju mreže, bezbedan udaljeni pristup, kao i zaštitu radnih stanica, servera i mobilnih uređaja;
- Rešenja za zaštitu podataka i poslovnih komunikacija, uključujući klasifikaciju i enkripciju podataka, backup i oporavak, kao i zaštitu elektronske pošte i drugih komunikacionih kanala;
- Rešenja za aplikativnu, cloud i DevSecOps bezbednost, uključujući zaštitu aplikacija, cloud okruženja, API servisa, kao i bezbednosne kontrole u razvoju i održavanju softvera;
- Rešenja za detekciju, praćenje i odgovor na bezbednosne incidente, uključujući sisteme za upravljanje logovima, detekciju pretnji, bezbednosne operacije i reagovanje na incidente;

- Rešenja za upravljanje incidentima i obezbeđenje kontinuiteta poslovanja, uključujući planove reagovanja, oporavka i kontinuiteta poslovanja u slučaju sajber incidenata;
- Rešenja za OT/industrijsku sajber bezbednost, uključujući zaštitu industrijskih sistema, segmentaciju i upravljanje rizicima u operativnim tehnologijama;
- Rešenja za podizanje svesti, obuku i specijalizovane usluge podrške, uključujući edukaciju zaposlenih, simulacije napada, kao i stručnu podršku u implementaciji i unapređenju bezbednosnih mera.



Navedene kategorije predstavljaju okvir za identifikaciju i strukturiranje projekata, dok se konkretna rešenja definišu u skladu sa potrebama preduzeća, rezultatima procene i prioritetima utvrđenim kroz mapu puta unapređenja.

Konačan izbor rešenja samostalno vrši preduzeće, u skladu sa definisanim projektnim zadatkom.

Prednost će imati integrisana rešenja koja obuhvataju više domena sajber bezbednosti i doprinose uspostavljanju celovitog i održivog sistema zaštite.

3.10 Etički kodeks CDT-a i upravljanje kvalitetom

Centar za digitalnu transformaciju (CDT) sprovodi Program u skladu sa principima profesionalnog i poslovnog integriteta, transparentnosti i odgovornosti, koji su definisani internim Etičkim kodeksom CDT-a i primenjuju se na sve učesnike u realizaciji Programa, uključujući sertifikovane konsultante.

Etički kodeks CDT-a uređuje osnovna pravila ponašanja i profesionalne standarde u radu sa preduzećima, sa posebnim fokusom na nepristrasnost, objektivnost, poverljivost informacija, izbegavanje sukoba interesa i poštovanje važećih zakona i propisa. Sertifikovani konsultanti angažovani u okviru Programa dužni su da svoje aktivnosti obavljaju u skladu sa navedenim principima, kao i da deluju u najboljem interesu korisnika Programa i ciljeva CDT-a.

U cilju obezbeđenja doslednog kvaliteta pruženih usluga, CDT primenjuje sistem upravljanja kvalitetom u skladu sa standardom ISO 9001. Ovaj sistem podrazumeva jasno definisane procedure rada, standardizovane metodologije i alate, kao i mehanizme za praćenje, kontrolu i unapređenje kvaliteta usluga.

Kvalitet realizacije Programa obezbeđuje se kroz:

- primenu standardizovane metodologije rada sa preduzećima;
- angažovanje sertifikovanih konsultanata sa relevantnim znanjima i iskustvom;
- internu kontrolu i verifikaciju ključnih faza rada i izrađenih izveštaja;
- kontinuirano unapređenje metodologije i alata na osnovu iskustava iz prakse;
- uspostavljene kanale komunikacije za prijavu nepravilnosti, nedoumica ili potencijalnih problema u realizaciji Programa.

Na ovaj način CDT obezbeđuje da se Program sprovodi u skladu sa najvišim profesionalnim i etičkim standardima, uz fokus na kvalitet, pouzdanost i dugoročnu vrednost za korisnike.

*Za više informacija kontaktirajte nas na **+381 60 4080 450** ili putem imejla **cdt@pks.rs***