

## Posebni pogoji za Storitve A1 Endpoint Protect

Družba A1 Slovenija, telekomunikacijske storitve, d. d., Ameriška ulica 4, 1000 Ljubljana, v okviru svojih dejavnosti in v skladu s svojimi Splošnimi pogoji, temi Posebnimi pogoji, Posebnimi pogoji uporabe Portala Cloud Market, Pogodbami in Veljavnimi predpisi, omogoča tudi uporabo Storitve A1 Endpoint Protect.

Ti Posebni pogoji vključujejo potrebne informacije o izvajanju, delovanju in uporabi Storitve A1 Endpoint Protect in zavezujejo vse Sopogodbenike, ki uporabljajo Storitve A1 Endpoint Protect.

Vsakokrat veljavni Splošni pogoji, Posebni pogoji, Posebni pogoji uporabe Portala Cloud Market, opis Storitve A1 Endpoint Protect, aktualna ponudba in cene, ter drugi pomembni dokumenti in informacije so dostopni na [www.A1.si](http://www.A1.si).

### I. Pomen izrazov

**I/1** Izrazi, ki se uporabljajo v teh Posebnih pogojih, imajo pomen, kot je zanje določen v (i) Splošnih pogojih, (ii) teh Posebnih pogojih in (iii) Posebnih pogojih uporabe Portala Cloud Market.

**I/2** Naslednji izrazi, uporabljeni v teh Posebnih pogojih, imajo naslednji pomen:

**Delovni čas:** je delovni čas Družbe A1 od 8:00 do 16:00 na Delovni dan, če ni v Pogodbi za posamezni primer dogovorjen drug delovni čas.

**Delovni dan:** je vsak delovni dan v tednu, to je od ponedeljka do petka, razen praznikov in dela prostih dni v Sloveniji.

**Drugi ponudnik:** je družba SentinelOne, Inc, 444 Castro Street, Suite 400 Mountain View, CA 94041 USA.

**Paket:** je posamezni paket Storitve A1 Endpoint Protect (npr. Core, Control, Complete).

**Posebni pogoji:** so ti Posebni pogoji za Storitve A1 Endpoint Protect, objavljeni na <https://www.a1.si/sodelovanje/splosni-pogoji/poslovne-resitve>.

**Programska oprema:** je SentinelOne Endpoint Security software, to je varnostna programska oprema za končne točke (končne naprave), katere opis je dostopen na [SentinelOne Singularity Core – Endpoint Security to Replace Legacy AV](#) in [Singularity Operating System Coverage - SentinelOne](#)

**Splošni pogoji:** so Splošni pogoji za izvajanje in posredovanje storitev, produktov in rešitev, ki niso Elektronske komunikacije storitve, za pravne osebe in podjetnike, objavljeni na <https://www.a1.si/sodelovanje/splosni-pogoji/poslovne-resitve>.

**Storitve A1 Endpoint Protect:** je storitev, v okviru katere Družba A1 Sopogodbniku omogoči uporabo Programske opreme in zanj izvaja Upravljanje storitev v vsebini in obsegu kot velja za posamezni Paket.

**Upravljanje storitev:** t.im. managed services, so storitve, ki jih v okviru posameznega Paketa Storitve A1 Endpoint Protect za Sopogodbenika izvaja Družba A1. Splošen opis Upravljanja storitev po posameznih Paketih je dostopen na <https://www.a1.si/upravljanje-storitve>

**I/3** Pomen posameznih izrazov, ki se uporabljajo v teh Posebnih pogojih, je lahko določen tudi v drugih točkah teh Posebnih pogojev.

## **II. Splošno**

**II/1** Družba A1 Sopogodbeniku zagotavlja Storitve A1 Endpoint Protect v vsebini in pod pogoji skladno s Pogodbeno dokumentacijo.

**II/2** Sopogodbenik potrjuje, da soglaša s temi Posebnimi pogoji in jih sprejema kot neločljivi sestavni del Pogodbe.

**II/3** Kakršni koli pogodbeni in drugi pogoji Sopogodbenika so izrecno izključeni in v nobenem primeru za Družbo A1 niso zavezujoči.

**II/4** Sopogodbenik se lahko za pridobitev informacij o Storitvi A1 Endpoint Protect obrne na svojega skrbnika pri Družbi A1, ali pošlje povpraševanje po elektronski pošti na naslov [A1endpointprotect@a1.si](mailto:A1endpointprotect@a1.si).

**II/5** Razmerja, ki nastanejo v zvezi z uporabo Storitve Endpoint Protect, urejajo naslednja Pogodbeno dokumentacija:

1. Pogodba (vključno z vsemi morebitnimi dodatki k Pogodbi (npr. za naročilo dodatnih Licenc));
2. Ti Posebni pogoji;
3. Posebni pogoji uporabe Portala Cloud Market, objavljeni na <https://www.a1.si/sodelovanje/splosni-pogoji/poslovne-resitve>;
4. Splošni pogoji.

**II/6** S sklenitvijo Pogodbe se Sopogodbenik strinja, da Družba A1 v njegovem imenu in za njegov račun lahko izvede vse potrebne aktivnosti za izvedbo njegovega Naročila, kar vključuje, a ni omejeno na:

- aktivacijo Storitve A1 Endpoint Protect,
- deaktivacijo Storitve A1 Endpoint Protect,
- spremembe Naročila Storitve A1 Endpoint Protect,
- potrditev morebitnih pogojev Drugega ponudnika ali tretjih oseb, ki jih je Sopogodbenik predhodno potrdil in sprejel v okviru Naročila, s sprejemom Ponudbe Družbe A1 in / ali sklenitvijo Pogodbe.

Sopogodbenik se nadalje tudi strinja, da lahko Družba A1 ob Naročilu Storitve A1 Endpoint Protect za Sopogodbenika ustvari Uporabniški račun na Portalu Cloud Market in Sopogodbeniku posreduje uporabniško ime in geslo za namen registracije in sprejema Posebnih pogojev uporabe Portala Cloud Market, kar bo Sopogodbeniku omogočilo, da z Naročili na Portalu Cloud Market upravlja tudi sam. Sopogodbenik se zaveda, da je sam odgovoren za uporabo in varstvo podatkov o Uporabniškem računu, ter izrecno pooblašča vsako osebo, ki bo Uporabniški račun uporabljala, da v imenu in za račun Sopogodbenika upravlja z Naročili Storitve A1 Endpoint Protect in Naročili drugih Storitvev, ki jih Sopogodbenik izvede na Portalu Cloud Market.

## **III. Izvajanje Storitve A1 Endpoint Protect**

**III/1** Družba A1 ima pooblastilo Drugega ponudnika za nadaljnjo prodajo licenc za Programsko opremo na območju Slovenije in zagotavljanje Upravljanih storitev kot ponudnik upravljanih

varnostnih storitev (MSSP – Managed Security Services Provider). Družba A1 Sopogodbeniku omogoči uporabo Programske opreme in mu zagotavlja Upravljanje storitve za Sopogodbenikovo lastno uporabo, in sicer v vsebini in obsegu kot velja za posamezni Paket.

**III/2** Za uporabo in delovanje Programske opreme, kar vključuje tudi omejitve pri uporabi Programske opreme, jamstva in garancije ter ureditev varstva Pravic intelektualne lastnine, veljajo in Sopogodbenika zavezujejo licenčni in drugi pogoji Drugega ponudnika, dostopni na [Legal & Compliance - SentinelOne](#) in dodatno določeni v Prilogi I. teh Posebnih pogojev: Managed Services - Flow Down Terms (v nadaljevanju: **Pogoji Drugega ponudnika**).

**III/3** Družba A1 in Drugi ponudnik v okviru uporabe Storitve A1 Endpoint Protect ne dajeta nobenega jamstva ali garancije, da na sistemih, omrežju ali sredstvih Sopogodbenika ne more priti do kibernetске grožnje ali napada oziroma da bosta našla, locirala, odkrila ali identificirala vse grožnje, napake v konfiguraciji, ranljivosti ali zlonamerno programsko opremo oziroma da bosta ponovno vzpostavila nadzor nad sistemi v primerih, ko je prišlo do nepooblaščenega dostopa ali nadzora oziroma da so sistemi, omrežje ali sredstva Sopogodbenika popolnoma varni pred vsakršnimi tveganji. Vsakršna odgovornost Družbe A1 in Drugega ponudnika iz tega naslova je v celoti izključena. Šteje se, da Sopogodbenik s sprejemom teh Posebnih pogojev potrjuje, da se opisanega tveganja zaveda in to tveganje tudi v celoti prevzema.

**III/4** Pred začetkom izvajanja Storitve A1 Endpoint Protect je dolžan Sopogodbenik iz svojih sistemov in naprav odstraniti morebitno obstoječo protivirusno zaščito, nelegalno programsko opremo in vsako drugo programsko ali strojno opremo, ki kakor koli omejuje, preprečuje, onemogoča ali drugače vpliva na uporabo Storitve A1 Endpoint Protect. Vse morebitne negativne posledice opustitve te obveznosti nosi izključno Sopogodbenik in je vsaka obveznost in odgovornost Družbe A1 iz tega naslova v celoti izključena.

**III/5** Družba A1 lahko določi okno za vzdrževanje, v okviru katerega izvaja redno vzdrževanje svoje programske in strojne opreme ter druge morebitne opreme in omrežja, preko katerih oziroma s pomočjo katerih izvaja Storitve A1 Endpoint Protect. Sopogodbenik se strinja, da lahko med oknom za vzdrževanje prihaja do krajših motenj in prekinitev pri izvajanju Storitve A1 Endpoint Protect, pri čemer Sopogodbenik iz tega naslova nima pravice od Družbe A1 zahtevati povračila kakršnih koli stroškov in škode.

**III/6** Družba A1 bo Sopogodbeniku omogočila uporabo Storitve A1 Endpoint Protect v roku 20 (dvajsetih) delovnih dni od dneva sklenitve Pogodbe ali dodatka. V primeru objektivne nezmožnosti izvedbe se navedeni rok podaljša za čas trajanja objektivne nezmožnosti. Objektivna nezmožnost pomeni nezmožnost Družbe A1 za izpolnitev obveznosti zaradi okoliščin kot so npr. višja sila, ravnanje ali opustitev Sopogodbenika, ravnanje ali opustitev tretje osebe in/ali nezmožnost iz tehničnih razlogov.

**III/7** Družba A1 bo Sopogodbeniku v spletni nadzorni plošči SentinelOne za upravljanje storitev (v nadaljevanju: **Nadzorna plošča**) ustvarila uporabniški profil, v katerem mu bo dodelila naročene licence za uporabo Programske opreme (v nadaljevanju: **Licence**). Družba A1 Sopogodbeniku zagotovi dostop do programskih agentov, ki se namestijo na Sopogodbenikove končne točke (končne naprave), ki jih Sopogodbenik želi zaščititi, kot npr. prenosne računalnike, namizne računalnike, strežnike, ne pa tudi mobilne naprave (v nadaljevanju: **Naprave**). Za prenos in namestitev programskih agentov na Naprave je odgovoren Sopogodbenik. Naročniško obdobje za Storitve A1 Endpoint Protect začne teči z njeno aktivacijo v Portalu Cloud Market. Družba A1 bo Sopogodbeniku zagotovila tudi navodila za namestitev programskih agentov.

**III/8** V okviru začetne nastavitve Storitve A1 Endpoint Protect bo Družba A1 Sopogodbeniku za vse programske agente aktivirala Standardno politiko varovanja, ki je opredeljena v nadaljevanju te točke, s čimer se Sopogodbenik izrecno strinja:

<b>Type of Protection</b>		
<b>Threat</b>	<b>Description</b>	<b>Option</b>
Malicious Threat	Actions, that are undertaken by the agent when a malicious threat is detected	Protect
Suspicious Threat	Actions, that are undertaken by the agent when a suspicious threat is detected	Detect
<b>Protection Level</b>	<b>Description</b>	<b>Option</b>
Kill & Quarantine	When a threat is detected, processes are "killed" and files associated with the threat are quarantined	Enabled
Remediate	Deletion of the files related to the threat and reverting the changes of the operating system to the state before the attack	Enabled
Rollback	On Windows OS, VSS is used to restore the operating system to its last stable state (Windows)	Enabled
Containment	The device on which a threat is detected shall be "disconnected from the network", i.e. the agent blocks all network traffic except for the access of the agent to the console and vice versa	Disabled
<b>Agent</b>		
<b>Security Settings</b>	<b>Description</b>	<b>Option</b>
Anti Tamper	It does not allow the user to make changes locally on the agent	Enabled
Snapshots	VSS technology of Windows is used for creation of the system backup. It is used with the Rollback option	Enabled
Logging	Logs are saved locally to the system for provision of better support	Enabled
Scan New Agents	Full scanning of the operating system when installing the agent	Enabled
<b>Agent UI</b>		
<b>Agent UI Settings</b>	<b>Description</b>	<b>Option</b>
Show Agent UI & tray icon on endpoints	Showing the agent in the taskbar of the respective operating system	Enabled
Show pop-up notifications for Threats and Mitigation	Showing of pop-up messages when blocking threats (Windows, MacOS)	Enabled
Show pop-up notifications for Blocked Devices	Showing of pop-up messages when blocking external devices (Windows, MacOS)	Enabled
Show suspicious events in the UI	Showing of suspicious threats in the UI of the agent	Enabled
Show warning in case of Agent errors	Functional warnings are displayed as messages for the operating system (Windows, MacOS)	Disabled
Show in the UI events from the last N days	Threats older than the specified number of days are not displayed in the UI of the agent (Windows, MacOS)	30 days

Show these menu items in the UI	Showing the following elements in the UI /User Interface/ of the Agent	
- Blocked Devices	Showing blocked devices in UI of the agent	Disabled
- Quarantined Files	Showing quarantined files in UI of the agent	Enabled
- Contact Support	Showing contact information with the support	Disabled
Support Contact Information	Support information	
- Free Text Message	Text Message	Disabled
- Company or Org	Company	Disabled
- Phone Number	Telephone number	Disabled
- Direct Message	Direct message	Disabled
- Support Website	Website	Disabled
- Other	Additional text	Disabled
<b>Deep Visibility</b>		
<b>Configuration</b>	<b>Description</b>	<b>Option</b>
Enable Deep Visibility	Enable Deep Visibility capabilities for the agent	Disabled
<b>More Options</b>		
<b>Option</b>	<b>Description</b>	<b>Option</b>
Decommissioning	Remove the agent from the control console after the specified number of days	Enabled - 21 days
Remote Shell	Possibility to provide remote powershell access to the workstation or server on which the agent is installed	Disabled

Sprememba Standardne politike varovanja v okviru Paketov »Control« in »Complete« je dovoljena na podlagi pisne zahteve Sopogodbnika, poslana po e-pošti na: A1endpointprotect@a1.si. Spremembo Standardne politike varovanja Družba A1 izvede v 5 (petih) delovnih dneh od datuma prejema zahteve za spremembo.

**III/9** Družba A1 ne odgovarja za:

- nepooblaščen dostop do Sopogodbnikovih podatkov s strani tretje osebe (npr. če Sopogodbnik podatke o svojem uporabniškem računu razkrije kateri koli tretji osebi);
- uničenje ali izgubo Sopogodbnikovih podatkov;
- škodo, ki jo Sopogodbnik povzroči tretjim osebam v zvezi s Storitvijo A1 Endpoint Protect, vključno zaradi kršitve Veljavnih predpisov;
- škodo, ki nastane zaradi Sopogodbnikove kršitve obveznosti po Pogodbi;
- terjatve tretjih oseb do Sopogodbnika;
- katero koli spremembo politike varovanja, ki jo izvede Sopogodbnik sam preko skrbniškega dostopa ali je izvedena na zahtevo Sopogodbnika.

**III/10** Za namestitev in uporabo Programske opreme mora Sopogodbnik izpolnjevati oziroma zagotoviti določene tehnične in sistemske zahteve, ki lahko vključujejo razpoložljivost internetne povezave, zahtevane Naprave, operacijski sistem itd. Veljavne tehnične in sistemske zahteve lahko Sopogodbnik preveri na [Singularity Operating System Coverage - SentinelOne](#)

**III/11** Ob identifikaciji programske opreme, ki je bila začasno ustavljena (status »v karanteni«) kot posledica ustreznega delovanja in implementacije politik zaščite, konfiguriranih v Nadzorni plošči, je Sopogodbnik upravičen do izvzema programske opreme iz karantene šele po pisni odobritvi

Družbe A1. Pisno zahtevo za odobritev mora Sopogodbenuk poslati Družbi A1 po e-pošti: [A1endpointprotect@a1.si](mailto:A1endpointprotect@a1.si)

#### IV. Plačilo Storitve A1 Endpoint Protect

**IV/1** Sopogodbenuk za Storitve A1 Endpoint Protect plačuje mesečno naročnino v višini skladno s Pogodbo, pri čemer se prva mesečna naročnina obračuna za mesec, v katerem je Storitve A1 Endpoint Protect aktivirana v Portalu Cloud Market.

V mesečno naročnino je vključena izvedba Upravljanih storitev v vsebini in obsegu kot veljajo za posamezni Paket in so opredeljene v Pogodbi, kar vključuje tudi naslednje aktivnosti:

- ustvarjanje uporabniškega profila Sopogodbenuka v Nadzorni plošči;
- dodelitev dogovorjenega števila Licenc ustrezne vrste v uporabniškem profilu Sopogodbenuka;
- generiranje in zagotavljanje programskega agenta za Sopogodbenuka, ki ga je treba aktivirati na vsaki zaščiteni Napravi;
- uvedba Standardne politike varovanja;
- spremembe konfiguracije in nastavitvev za Paketa »Control« in »Complete« ter aktivnosti za dodajanje novih Uporabnikov v naročniškem obdobju:
  - do 2 človek/uri na mesec na ravni podjetja za Paket »Control«
  - do 4 človek/ure na mesec na ravni podjetja za Paket »Complete«.

**IV/2** Sopogodbenuk lahko pri Družbi A1 naroči namestitev programskih agentov, za kar mora plačati enkratno nadomestilo v višini skladno s Ponudbo. Namestitev programskih agentov Družba A1 izvede na odgovornost Sopogodbenuka preko oddaljenega dostopa do Sopogodbenukovih Naprav.

**IV/3** Na zahtevo Sopogodbenuka Družba A1 pripravi zasnovo rešitve in predloži kot ločen projekt, vključno s ceno in plačilnimi pogoji, kar pogodbeni stranki uredita v Pogodbi.

**IV/4** Cene morebitnih drugih storitev, ki jih Družba A1 izvede za Sopogodbenuka (npr. urna postavka v primeru dodatnih aktivnosti), so določene v vsakokrat veljavnem Ceniku A1 ali dogovorjene s Pogodbo.

**IV/5** V pogodbeno ceno niso vključeni stroški, ki lahko Družbi A1 nastanejo pri izvajanju Storitve A1 Endpoint Protect na lokaciji Sopogodbenuka na podlagi naročila (npr. potni stroški, stroški namestitve, porabljen čas). Navedene stroške je dolžan Sopogodbenuk plačati Družbi A1 dodatno poleg pogodbene cene, in sicer v višini in skladno s plačilnimi pogoji, določenimi v Pogodbi.

**IV/6** Sopogodbenuk je dolžan vse svoje plačilne obveznosti poravnati v roku 15 dni od datuma računa, če ni s Pogodbo dogovorjen drugačen rok.

#### V. Pravila za izvajanje sprememb preko Portala Cloud Market

<b>Naročniško obdobje</b>	<ul style="list-style-type: none"><li>• 1 mesec</li><li>• 1 leto</li><li>• 2 leti</li></ul>
<b>Plačilo</b>	<ul style="list-style-type: none"><li>• mesečno</li></ul>
<b>Zamenjava Paketa</b>	<ul style="list-style-type: none"><li>• Zamenjava Paketa je možna samo za namen nadgradnje funkcionalnosti v Paketu</li></ul>

<p><b>Odpoved</b></p>	<ul style="list-style-type: none"> <li>• V primeru odpovedi pred iztekom naročniškega obdobja je dolžan Sopogodbenik v enkratnem znesku plačati vse preostale mesečne naročnine, obračunane od odpovedi do izteka naročniškega obdobja.</li> </ul> <p>Posledice odpovedi:</p> <ul style="list-style-type: none"> <li>• Sopogodbenik izgubi dostop do Licenc in podatkov, povezanih z Licencami;</li> <li>• Skrbnik Sopogodbenika, ki ima na Nadzorni plošči vlogo administratorja, izgubi dostop do podatkov na Nadzorni plošči ter s tem možnost uporabe Storitve A1 Endpoint Protect;</li> <li>• Licenc ni mogoče ponovno aktivirati, temveč je potrebno novo naročilo Storitve A1 Endpoint Protect.</li> </ul>
<p><b>Začasna ukinitvev (suspenz) aktivnih Licenc</b></p>	<ul style="list-style-type: none"> <li>• Družba A1 lahko Sopogodbeniku začasno ukine Storitvev A1 Endpoint Protect, če Sopogodbenik ne plača mesečne naročnine oziroma katere koli svoje druge plačilne obveznosti iz naslova Pogodbe oziroma v primeru katere koli druge kršitve Pogodbe, pri čemer pa je dolžan mesečno naročnino plačevati tudi ves čas trajanja suspenza.</li> <li>• Sopogodbenik je dolžan plačevati mesečno naročnino v celoten dogovorjenem naročniškem obdobju.</li> <li>• Med suspenzom Sopogodbenik nima dostopa do Storitve A1 Endpoint Protect.</li> </ul>
<p><b>Status za samodejno obnavljanje naročniškega obdobja</b></p>	<ul style="list-style-type: none"> <li>• Vključena opcija za samodejno obnavljanje (Auto-Renew ON): <ul style="list-style-type: none"> <li>• Auto-Renew ON je privzet status, ki ga lahko Sopogodbenik izklopi (Auto-Renew OFF)</li> <li>• Licenca se avtomatično podaljša ob izeku naročniškega obdobja</li> </ul> </li> <li>• Izključena opcija za samodejno obnavljanje (Auto-Renew OFF): <ul style="list-style-type: none"> <li>• Licenca se ob izeku naročniškega obdobja ne podaljša</li> <li>• Status Licence se spremeni v »suspenz«</li> </ul> </li> </ul>
<p><b>Skrbniški dostop do Nadzorne plošče</b></p>	<ul style="list-style-type: none"> <li>• Sopogodbenik mora Družbi A1 predložiti pisno zahtevo za skrbniški dostop do Nadzorne plošče, v kateri mora navesti tudi osebo, ki ji bo dostop dodeljen. Za skrbniški dostop je potrebna odobritev Družbe A1. Če je Sopogodbeniku odobren skrbniški dostop, Sopogodbenik v celoti sam odgovarja za vse posledice uvedbe oziroma spremembe politik varovanja, vsaka odgovornost Družbe A1 iz tega naslova pa je v celoti izključena in Sopogodbenik do Družbe A1 nima nobenega zahtevka</li> </ul>

## VI. Paketi

VI/1 Storitve A1 Endpoint Protect je Sopogodbenikom na voljo preko treh različnih Paketov: Core, Control in Complete. Podroben opis paketov je dostopen na:

<https://www.sentinelone.com/>

### VI/2 Funkcionalnosti Paketov

Paketi	Core	Control	Complete
Zaščita naprav za operacijske sisteme Windows in macOS	✓	✓	✓
Napredna zaščita naprav s protivirusnim sistemom naslednje generacije, ki uporablja statično in vedenjsko analizo umetne inteligence	✓	✓	✓
Možnost samodejne vrnitve naprave v stanje pred napadom z enim klikom	✓	✓	✓
Saniranje naprave in vrnitev v stanje pred napadom, hitra in enostavna možnost obnovitve šifriranih ali z virusi izbrisanih datotek.	✓	✓	✓
Funkcije za upravljanje paketa: Upravljanje naprav, upravljanje požarnega zidu, oddaljen dostop do nadzorovanih naprav		✓	✓
Analiza dokumentov /odkrivanje groženj v njih/, priloženih datotek, datotek, prenesenih z interneta	✓	✓	✓
Odkrivanje in zaščita pred napadi 0-day, online in offline /informacije o napadu so v agentu, nameščenem v napravi/	✓	✓	✓
Identifikacija in analiza odstopanj od standardnega vedenja uporabnika	✓	✓	✓
Uvedba izolacije in karantene okužene naprave v omrežju, da ne bi mogla okužiti celotnega omrežja	✓	✓	✓
Odkrivanje in upravljanje ranljivosti v programski opremi, s katero delujejo naprave	✓	✓	✓
Seznam aplikacij in pogostih ranljivosti		✓	✓
Nadzor EDR in celotna zgodovina napada z identifikacijo vzroka		✓	✓
Nadzor EDR tudi v šifriranem prometu		✓	✓
Analitika EDR, ki zbira in analizira informacije o varnostnih grožnjah z računalniških delovnih postaj		✓	✓
Začetna konfiguracija in namestitve storitve na podlagi vnaprej določenih politik varovanja	✓	✓	✓
XDR zaščita			✓
Celovit pristop k varnosti z integracijo in korelacijo podatkov prek več varnostnih plasti, vključno s končnimi točkami, omrežji, oblakom in e-pošto.			✓
Celosten pogled na varnost organizacije z nadzorovanjem sistemskih aktivnosti in vedenj prek različnih domen in virov.			✓
Napredna analitika in algoritmi strojnega učenja za prepoznavanje in določanje prednosti groženj.			✓
Podpora v času trajanja pogodbe	✓	✓	✓
Upravljanje storitve (spremembe in posodobitve politik varovanja)		✓ 2MH	✓ 4MH



## **VII. Pravice in obveznosti**

**VII/1** Družba A1 ima pravico do začasne ukinitve (suspenza) Storitve A1 Endpoint Protect, če Sopogodbenik prekrši katero koli svojo obveznost po Pogodbi (vključno z obveznostjo plačila). Družba A1 lahko (ni pa dolžna) Sopogodbenika pred suspenzom opozoriti na kršitev in mu omogočiti rok za odpravo kršitve. Družba A1 lahko Sopogodbeniku ponovno omogoči Storitve A1 Endpoint Protect, če je kršitev odpravil oziroma če Sopogodbenik kršitve ne odpravi, ima Družba A1 pravico do odstopa od Pogodbe.

**VII/2** Družba A1 ima pravico od Sopogodbenika zahtevati identifikacijo, ki je potrebna glede na okoliščine, ko od njega sprejema navodila v zvezi z uporabo ali upravljanjem Storitve A1 Endpoint Protect.

**VII/3** Sopogodbenik se zavezuje:

- da bo zagotovil skladnost z vsemi sistemskimi zahtevami za normalno delovanje Programske opreme, ki so na voljo v vmesniku Nadzorne plošče;
- da bo storitve, ki so predmet Pogodbe, potrdil in prevzel, če so za prevzem izpolnjene dogovorjene zahteve;
- da bo Družbi A1 v dogovorjenih rokih zagotovil vse pogoje, ki so potrebni za izvajanje Pogodbe (npr. tehnične informacije in pomoč v zvezi z vzpostavitvijo in konfiguracijo Storitve A1 Endpoint Protect, dostop do Naprav).

Sopogodbenik ne sme spreminjati, razstavljati, dekonstruirati, dekompilirati, prilagajati, nepooblaščen dostopati do nje, kopirati, uporabljati obratnega inženiringa, obratno prevajati ali odstraniti njenih delov ali na kakršen koli drug način reproducirati ali spreminjati Programske opreme.

## **VIII. Osebni podatki**

**VIII/1** Izrazi, ki se v teh Posebnih pogojih uporabljajo v zvezi z obdelavo osebnih podatkov, imajo enak pomen kot v Splošni uredbi o varstvu podatkov - Uredba (EU) 2016/679.

**VIII/2** Pri obdelavi osebnih podatkov v okviru izvajanja Storitve A1 Endpoint Protect, ima Sopogodbenik vlogo upravljavca osebnih podatkov, Družba A1 nastopa v vlogi Sopogodbenikovega obdelovalca, Drugi ponudnik pa v vlogi pod-obdelovalca Družbe A1. Kot pod-obdelovalec Družbe A1 za izvajanje druge stopnje tehnične podpore nastopa tudi družba A1 Digital International GmbH, ki je z Družbo A1 povezana družba znotraj skupine A1 Telekom Austria Group.

Seznam nadaljnjih pod-obdelovalcev Drugega ponudnika je dostopen na: <https://www.sentinelone.com/legal/sentinelone-sub-processors/>.

Za prenos osebnih podatkov v tretje države veljajo Standardne pogodbene klavzule, ki so dostopne na: [eu-c2p - SentinelOne](#).

**VIII/3** Podrobnosti obdelave osebnih podatkov

Namen in trajanje obdelave

Osebni podatki se obdelujejo za namen zagotavljanja Storitve A1 EP Protect skladno s Pogodbo.

Trajanje obdelave: Osebni podatki se obdelujejo za čas sklenjene Pogodbe ter do 60 dni od datuma prenehanja Pogodbe, razen če je daljše trajanje obdelave potrebno skladno z veljavnimi predpisi.

Vrsta in namen obdelave

Osebnih podatki se obdelujejo le v obsegu, ki je razumno potreben za zagotavljanje Storitve A1 EP Protect in z njo povezane podpore.

Kategorije podatkov:

V zvezi s Singularity se lahko obdelujejo naslednje kategorije osebnih podatkov:

- podatki o uporabniku in končni točki: ID agenta, ime končne točke, ID uporabnika aktivnega imenika stranke, uporabniško ime, nameščene aplikacije – čas namestitve, velikost, izdajatelj in različica, uporabniško ime SMTP, konfiguracijski podatki, povezani z integracijo aktivnega imenika;
- polna pot do datoteke: vključuje osebne podatke samo, če ime datoteke vključuje osebne podatke;
- v primeru suma grožnje agent za vsak proces zbere metapodatke o datoteki, hash, vrsto datoteke, certifikat, argumente ukazne vrstice, metapodatke o omrežnem dostopu (naslov IP, protokol), register (ustvarjeni ključi, izbrisani ključi, spremenjena imena ključev);
- omrežne podatke (naslov IP notranjega omrežja, javni naslov IP (če je nameščena konzola za upravljanje v oblaku);
- podatki o grožnjah (pot do datoteke, identifikatorji agentov, vsebina sporočil SMS (ki lahko vključujejo uporabniška imena, naslove IP, imena datotek);
- spremljanje omrežja v živo (naslovi URL, glave URL, časovni žigi) in
- v primeru uporabe funkcije SentinelOne za pridobivanje datotek: vsi podatki, ki jih vsebujejo datoteke, ki jih pridobijo skrbniki.

V zvezi z Datasetom in/ali XDR Ingestom se lahko obdelujejo naslednje kategorije osebnih podatkov:

- podatki v zvezi s posamezniki, ki so vključeni v podatkih prenesenih v Dataset in/ali XDR Ingest.

Posebne vrste podatkov

- Osebnih podatki ne vključujejo posebnih vrst osebnih podatkov ali podatkov v zvezi s kazenskimi obsodbami ali prekrški, razen kadar Sopogodbenu take podatke naloži v povezavi s storitvami Dataset ali XDR Ingest ali kadar do njih dostopa z uporabo funkcije File Fetching v rešitvah SentinelOne.

Posamezniki, na katere se nanašajo podatki

- Posamezniki, na katere se nanašajo osebni podatki, vključujejo posameznike, o katerih podatke prek Storitve A1 EP Protect zagotovi Sopogodbenu (ali druga oseba po njegovem navodilu).

Obveznost informiranja posameznikov o obdelavi osebnih podatkov pri uporabi Storitve A1 Endpoint Protect, kot jo zahtevata 13. in 14. člen Splošne uredbe o varstvu podatkov, je izključno na strani Sopogodbenu - upravljavca.

**VIII/4** Za pisni dogovor med Družbo A1 in Sopogodbenukom z vsebino iz 28. člena Splošne uredbe o varstvu podatkov se štejejo ti Posebni pogoji in Pogodba.

**VIII/5** Družba A1 se kot obdelovalec osebnih podatkov zaveda, da brez izrecnih in dokumentiranih navodil Sopogodbenuka kot upravljavca, npr. odobritve Sopogodbenuka (oziroma sprejem teh Pogojev) ali specifične zahteve po pravu Unije ali države članice, ki velja za Družbo A1, v okviru Pogodbe ne sme:

- prenašati osebnih podatkov upravljavcu ali obdelovalcu v tretji državi ali mednarodni organizaciji;
- prenašati osebnih podatkov podobdelovalcu v tretji državi ali mednarodni organizaciji;

- omogočiti obdelave osebnih podatkov obdelovalcu v tretji državi ali mednarodni organizaciji.

**VIII/6** Družba A1 bo obdelovala osebne podatke samo na podlagi dokumentiranih navodil Sopogodbnika, razen, če odstopanje od tega od nje zahteva pravo Unije ali države članice, ki velja za Družbo A1. Sopogodbnik navodila, poleg teh, ki so že vsebovana v teh Posebnih pogojih in Pogodbi ter njenih prilogah, Družbi A1 posreduje pisno, praviloma v elektronski obliki na elektronski naslov Sopogodbnikovega skrbnika pri Družbi A1. Če bi Družba A1 menila, da so navodila Sopogodbnika v nasprotju s predpisi o varstvu osebnih podatkov, bo Sopogodbnika o tem nemudoma obvestila.

**VIII/7** Družba A1 mora pri izvrševanju določil Pogodbe z organizacijskimi, tehničnimi in logično-tehničnimi postopki in ukrepi zagotoviti tako varnost osebnih podatkov, da se preprečuje slučajno ali namerno nepooblaščen uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščen obdelava, in sicer:

- z varovanjem prostorov, v katerih se nahajajo osebni podatki, ter strojne in programske opreme, ki omogoča dostop do teh podatkov:
  - prostori in strojna ter programska oprema morajo biti varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov,
  - prostori morajo biti fizično varovani, npr. s kontrolo vstopa z vstopno kartico, videonadzorom vstopa, alarmom gibanja po prostorih, fizičnim varovanjem varnostnika itd.,
  - dostop v prostore je dovoljen le tistim zaposlenim, katerih pravica do vstopa v posamezni prostor izhaja iz notranjega akta Družbe A1;
- z varovanjem sistemske in aplikativne programske opreme, s katero se obdelujejo osebni podatki:
  - dostop do programske opreme mora biti varovan s sistemom gesel za avtorizacijo in identifikacijo uporabnikov, ki omogoča dostop samo določenim pooblaščenim delavcem,
  - program oziroma aplikacija mora biti sestavljen tako, da je obdelava podatkov ponovljiva ter da ob prekinitvi obdelav ne pride do izgube, uničenja ali sprememb podatkov,
  - vsak nov program ali spremembo pri obstoječih programih je treba pred redno uporabo testirati na testnem vzorcu - razvojni programi in testne podatkovne zbirke morajo biti ločene od produkcijskega okolja;
- z varovanjem podatkovnih nosilcev:
  - osebni podatki morajo biti hranjeni v varovanih prostorih, izven varovanih prostorov (hodniki, skupni prostori ipd.) pa morajo biti vedno zaklenjeni v ognjevarni in protivlomno zaščiteni omari;
- z varovanjem pri prenosu po telekomunikacijskih omrežjih:
  - osebni podatki morajo biti pri prenosu po telekomunikacijskih sredstvih in omrežjih zaščiteni;
- da se zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;
- da se omogoča poznejše ugotavljanje, kdaj so bili posamezni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil (za čas petih letih let od posamične aktivnosti obdelave osebnih podatkov).

**VIII/8** Vsi ukrepi se izvajajo z namenom, da se zagotovi stalna zaupnost, celovitost, nespremenljivost (integriteta), razpoložljivost podatkov (v primeru fizičnega ali tehničnega incidenta) in odpornost sistemov za obdelavo osebnih podatkov.

**VIII/9** Skladno z določbami člena 32 Splošne uredbe o varstvu podatkov bo tudi Družba A1 - neodvisno od Sopogodbjenika - ocenila tveganja za pravice in svoboščine posameznikov, ki izhajajo iz obdelave osebnih podatkov, ki ji jo je poveril Sopogodbjenik, in uveljavila ukrepe za njihovo ublažitev. Med drugim bo tudi redno ocenjevala in vrednotila učinkovitost tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave.

**VIII/10** Družba A1 mora, kadar to izhaja iz narave obdelave, pomagati Sopogodbjeniku pri izpolnjevanju njegovih obveznosti, da odgovori na zahteve za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki kot je na primer posredovanje informacij, ki jih je potrebno zagotoviti posamezniku, pravice do izbrisa, pravice do popravka, pravice do omejitve obdelave, obveznost obveščanja v zvezi s popravkom ali izbrisom osebnih podatkov ali omejitvijo obdelave ter pravice do prenosljivosti obdelave. Po splošnem ali posamičnem navodilu Sopogodbjenika mora Družba A1 vse obveznosti do posameznika izvajati v skladu z navodili neposredno v odnosu do posameznika.

**VIII/11** Družba A1 je dolžna voditi evidenco dejavnosti obdelave, ki jih izvaja v imenu Sopogodbjenika, in vsebuje: naziv in kontaktne podatke podobdelovalca in pooblaščen osebe za varstvo podatkov, vrste obdelave, ki se izvajajo v imenu Sopogodbjenika, prenose osebnih podatkov v tretjo državo ali mednarodno organizacijo, vključno z identifikacijo te tretje države ali mednarodne organizacije in dokumentacijo o ustreznih zaščitnih ukrepih ter splošni opis tehničnih in organizacijskih varnostnih ukrepov pri podobdelovalcu.

**VIII/12** Družba A1 je dolžna v primeru seznanitve s kršitvijo varstva osebnih podatkov, brez nepotrebnega odlašanja, najkasneje v 24-ih urah potem, ko se je seznanila s kršitvijo, pisno o tem obvestiti Sopogodbjenika. Pisno obvestilo mora vsebovati:

- naravo kršitve varnosti osebnih podatkov, po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število zadevnih evidenc osebnih podatkov;
- verjetne posledice kršitve varnosti osebnih podatkov;
- ukrepe, ki naj jih Sopogodbjenik sprejme ali katerih sprejetje Družba A1 predlaga Sopogodbjeniku za obravnavanje kršitve varnosti osebnih podatkov, pa tudi, kadar je smiselno, ukrepe za ublažitev morebitnih škodljivih učinkov kršitve.

**VIII/13** Družba A1 mora dati Sopogodbjeniku na voljo vse informacije, ki dokazujejo izpolnjevanje obveznosti iz Pogodbe ter mora Sopogodbjeniku ali drugemu revizorju, ki ga pooblasti Sopogodbjenik, omogočiti izvajanje revizij, tudi drugih pregledov skladnosti obdelave s predpisi in navodili Sopogodbjenika ter pri njih sodelovati.

**VIII/14** Družba A1 lahko samo po predhodnem pisnem soglasju Sopogodbjenika poveri posamezna opravila v zvezi z obdelavo osebnih podatkov podobdelovalcu, ki je registriran za opravljanje takšne dejavnosti in zagotavlja ustrezne postopke in ukrepe za varovanje osebnih podatkov.

**VIII/15** Družba A1 je dolžna pri izpolnjevanju predmeta Pogodbe ravnati s skrbnostjo dobrega strokovnjaka. Družba A1 ne odgovarja za škodo, ki je pri izpolnjevanju Pogodbe povzročena s strani Sopogodbjenika. Če je za nastalo škodo ali otežitev položaja Družbe A1 kriv tudi Sopogodbjenik oziroma kdo drug, za katerega je Sopogodbjenik odgovoren, se odškodninska odgovornost Družbe A1 temu ustrezno zmanjša (v obsegu, kot je višino škode mogoče pripisati Sopogodbjeniku oziroma osebi, za katero je Sopogodbjenik odgovoren). Družba A1 ne odgovarja za izgubo, poškodbo, ali drugo obliko spremembe osebnih podatkov, do katere je prišlo zaradi višje sile, kot je opredeljena v Pogodbi.

**VIII/16** Družba A1 je dolžna skrbeti, da bodo zaposleni in drugi posamezniki, ki opravljajo dela ali naloge obdelave osebnih podatkov, varovali vse podatke, s katerimi se seznanijo pri opravljanju njihovih del in nalog, kot poslovno skrivnost (kot zaupne/tajne). Dolžnost varovanja tajnosti

osebnih podatkov te osebe obvezuje tudi po prenehanju zaposlitve oziroma opravljanja del ali nalog pogodbene obdelave.

**VIII/17** Družba A1 lahko razkrije podatke, ki jih za Sopogodbenika obdeluje po Pogodbi samo tistim osebam, ki neposredno sodelujejo pri izvrševanju Pogodbe, in ki so se zavezale k zaupnosti ali so ustrezno statusno-pravno zavezane glede zaupnosti in samo glede na izkazano potrebo po dostopu do podatkov. Seznam oseb, katerim je omogočen dostop do osebnih podatkov vodi Družba A1 in je lahko predmet pregleda s strani Sopogodbenika. Na podlagi pregledov bo dostop do osebnih podatkov ukinjen, če ni več potreben, s čimer osebni podatki zadevnim osebam ne bodo več dostopni.

**VIII/18** V primeru prenehanja oziroma odpovedi Pogodbe mora Družba A1 nemudoma prenehati obdelovati osebne podatke Sopogodbenika. Izjemoma jih lahko obdeluje le še zaradi dokončanja začelih poslov po Pogodbi, ki jih je dolžna zagotoviti. V primeru prenehanja oziroma odpovedi Pogodbe mora Družba A1 vse osebne podatke takoj vrniti Sopogodbeniku, morebitne kopije teh podatkov pa mora takoj uničiti razen, če da Sopogodbenik drugačna pisna navodila.

## **IX. Trajanje Pogodbe in odpoved**

**IX/1** Pogodba se sklepa za čas trajanja naročniškega obdobja, ki ga izbere Sopogodbenik (mesečno, letno ali dvoletno). Naročniško obdobje se vsakokrat samodejno podaljša za enako obdobje, če posamezna pogodbeni stranka druge pogodbeni stranke pisno ne obvesti najmanj trideset (30) dni pred zaključkom tekočega naročniškega obdobja, da naročniškega obdobja ne bo podaljšala. Sopogodbenik lahko v Portalu Cloud Market tudi izklopi opcijo za samodejno podaljševanje, kar pomeni, da se naročniško obdobje ob izteku ne podaljša in Pogodba preneha veljati.

**IX/2** Pogodba preneha veljati tudi v drugih primerih, ki so določeni v Splošnih pogojih. Pogodba preneha veljati tudi v primeru, če preneha pogodba med Družbo A1 in Drugim ponudnikom, na podlagi katere je Družba A1 pooblaščen za nadaljnjo prodajo Licenc za Programsko opremo in zagotavljanje Upravljanih storitev, o čemer bo Družba A1 Sopogodbenika obvestila takoj, ko bo to mogoče.

**IX/3** Ob prenehanju veljavnosti Pogodbe: (i) Sopogodbeniku prenehajo vse pravice in Licence, ki so mu bile podeljene na podlagi Pogodbe; (ii) prenehajo vse obveznosti Družbe A1; (iii) bo pogodbeni stranka na podlagi prejete zahteve drugi pogodbeni stranki nemudoma vrnila vse zaupne podatke, ki je od nje prejela, ali uničila vse kopije takšnih zaupnih podatkov; (iv) bo Sopogodbenik nemudoma prenehal uporabljati Programsko opremo in bo uničil in/ali trajno izbrisal vse kopije vseh komponent Programske opreme, ki jih ima shranjene pri sebi in bo na zahtevo Družbe A1 zagotovil pisno potrditev take odstranitve.

**IX/4** Če Pogodba preneha veljati pred iztekom naročniškega obdobja iz razlogov na strani Sopogodbenika, je dolžan Sopogodbenik v enkratnem znesku plačati mesečno naročnino za celotno preostalo naročniško obdobje, in sicer v roku 15 dni od datuma računa. Prav tako Družba A1 Sopogodbeniku v tem primeru ni dolžna vračati morebitne vnaprej plačane in neporabljene mesečne naročnine.

## **X. Spremembe Pogodbene dokumentacije in Storitve**

**X./1.** Družba A1 ima pravico do spremembe Pogodbene dokumentacije in Storitve A1 EP Protect. O vsaki spremembi bo Družba A1 Sopogodbenike obvestila skladno s Splošnimi pogoji.

## **XI. Končna določba**

**XI/1** Ti Posebni pogoji začnejo veljati z dnem 1. 11. 2023

A1 Slovenija, d. d.

## Priloga 1

### Managed Services - Flow Down Terms

Customer ("Sopogodbenik") and MSSP ("Družba A1") have entered an agreement ("Solution Terms") where MSSP is providing managed security services for the Customer ("Services"). This Managed Services – Flow Down Terms, ("Attachment") shall be made part of the Solution Terms between MSSP and Customer, and where this Attachment and Solution Terms conflict, this Attachment shall control. MSSP has licensed SentinelOne's platform including its malware protection, detection and remediation solutions, endpoint detection and response solutions, device discovery and control solutions, and other solutions and enhancements thereto offered by SentinelOne over time, ("Solutions") from SentinelOne, Inc. and is using the Solutions in its provision of Services.

1. All Claims between MSSP and Customer. Customer agrees that it will bring all claims under this Agreement as well as any claims arising out of its related use of Solution against MSSP and will not make claim directly against SentinelOne. Customer agrees that SentinelOne has no obligation or liability to Customer under this agreement and to the maximum extent allowable by law, Customer shall hold indemnify and hold harmless SentinelOne Inc. for any cause of action arising out of Services.
2. Solution Use. Customer may only use Solutions for its internal business security and operations, in accordance with the Documentation in conjunction with the Services.
3. Restrictions on Use. Customer may not do any of the following: (i) modify, disclose, alter, translate or create derivative works of the Solutions (or any components thereof) or any accompanying Documentation; (ii) license, sublicense, resell, distribute, lease, rent, lend, transfer, assign or otherwise dispose of the Solutions (or any components thereof) or any Documentation; (iii) use the Solutions for commercial or business uses not contemplated in Services such as offering Solutions to the benefit of other third-parties, Solution may only be used as directly related to Customer's internal business operations and in conformity with the Documentation; (iv) use the Solutions in violation of any laws or regulations, including, without limitation, to store or transmit infringing, libelous or otherwise unlawful or tortious material, or material in violation of third-party privacy rights; (v) use the Solutions to store, transmit or test for any viruses, software routines or other code designed to permit unauthorized access, disable, erase or otherwise harm software, hardware or data, or to perform any other harmful actions; (vi) probe, scan or test the efficacy or vulnerability of the Solutions, or take any action in an effort to circumvent or undermine the Solutions, except for the legitimate testing of the Solutions in coordination with MSSP and SentinelOne, in connection with considering a subscription to the Solutions as licensed herein; (vii) attempt or actually disassemble, decompile or reverse engineer, copy, frame or mirror any part or content of the Solutions, or otherwise derive any of the Solutions' source code; (viii) access, test, and/or use the Solutions in any way to build a competitive product or service, or copy any features or functions of the Solutions; (ix) interfere with or disrupt the integrity or performance of the Solutions; (x) attempt to gain unauthorized access to the Solutions or their related systems or networks; (xi) disclose to any third party or publish in any media any performance information or analysis relating to the Solutions; (xii) fail to maintain all copyright, trademark and proprietary notices on the Solutions and any permitted copy thereof; or (xiii) cause or permit any Solutions user or third party to do any of the foregoing.