ESET Cloud Office Security

Používateľská príručka

Pre zobrazenie tohto dokumentu v online verzii kliknite sem

Digital Security
Progress. Protected.

Copyright ©2023 ESET, spol. s r. o.

ESET Cloud Office Security bol vyvinutý spoločnosťou ESET, spol. s r. o.

Viac informácií nájdete na webovej stránke www.eset.sk.

Všetky práva vyhradené. Žiadna časť tejto publikácie nesmie byť reprodukovaná žiadnym prostriedkom ani distribuovaná akýmkoľvek spôsobom bez predchádzajúceho písomného povolenia spoločnosti ESET, spol. s r. o.

ESET, spol. s r. o. si vyhradzuje právo zmeny programových produktov popísaných v tejto publikácii bez predchádzajúceho upozornenia.

Kontaktný formulár: https://www.eset.com/sk/podpora/kontakt/

REV. 20.12.2023

1 Prehľad ... 1
1.1 Hlavné funkcie ... 2
1.2 Čo je nové ... 5
1.3 Integrácia ... 6
2 Špecifikácie ... 7
2.1 Požiadavky ... 7
2.2 Podporované plány Microsoft 365 ... 7
2.3 Podporované plány služby Google Workspace ... 8
2.4 Podporované webové prehliadače ... 8
2.5 Obmedzenia a politika uchovávania údajov ... 9
3 Licencovanie ESET Cloud Office Security ... 10
3.1 ESET Business Account ... 11
3.1 Vytvorenie nového účtu ESET Business Account ... 11
3.1 Pridanie licencie pre ESET Cloud Office Security do portálu ESET Business Account ... 12
3.1 Správa účtu ESET Business Account ... 13
3.2 ESET MSP Administrator ... 13
4 Aktivácia ESET Cloud Office Security ... 14
4.1 Deaktivácia ESET Cloud Office Security ... 16
5 Správa nájomníkov cez Nastavenia ... 17
5.1 Pridanie nájomníka ... 19
5.2 Nájomník Microsoft 365 ... 22
5.3 Nájomník Google Workspace ... 25
5.4 Odstránenie nájomníka z konzoly ESET Cloud Office Security ... 31
5.5 Odstránenie ESET Cloud Office Security z portálu Azure ... 32
6 Orientácia v ESET Cloud Office Security ... 32
7 ESET LiveGuard Advanced ... 34
8 Riadiaci panel ... 35
9 Používatelia ... 37
10 Tímy a lokality ... 38
11 Detekcie ... 39
12 Reporty ... 40
13 Karanténa ... 43
14 Protokoly kontroly ... 44
15 Politiky ... 45
15.1 Nastavenia ochrany pre Exchange Online ... 48
15.2 Nastavenia ochrany pre Gmail ... 51
15.3 Nastavenia ochrany pre OneDrive ... 54
15.4 Nastavenia ochrany pre Disk Google ... 55
15.5 Nastavenia ochrany pre Tímové skupiny ... 55
15.6 Nastavenia ochrany pre Lokality SharePoint ... 56
15.7 Nastavenia ochrany pre ESET LiveGuard Advanced ... 57
15.8 Hlásenia a ochrana s využitím strojového učenia ... 58
16 Správa licencií ... 59
16.1 Prístup používateľa k ESET Cloud Office Security pre prezeranie dát konkrétnej spoločnosti ... 62
17 Protokol auditu ... 63
18 Odoslanie spätnej väzby ... 64
19 Technická podpora ... 64
20 Dostupnosť služieb ... 65

20.1 Zabezpečenie ESET Cloud Office Security 65
20.2 Podmienky používania 69
20.2 Licenčná dohoda s koncovým používateľom 73
20.2 Dohoda o spracúvaní údajov 79
20.2 Štandardné zmluvné doložky 82
20.3 Zásady ochrany osobných údajov 105

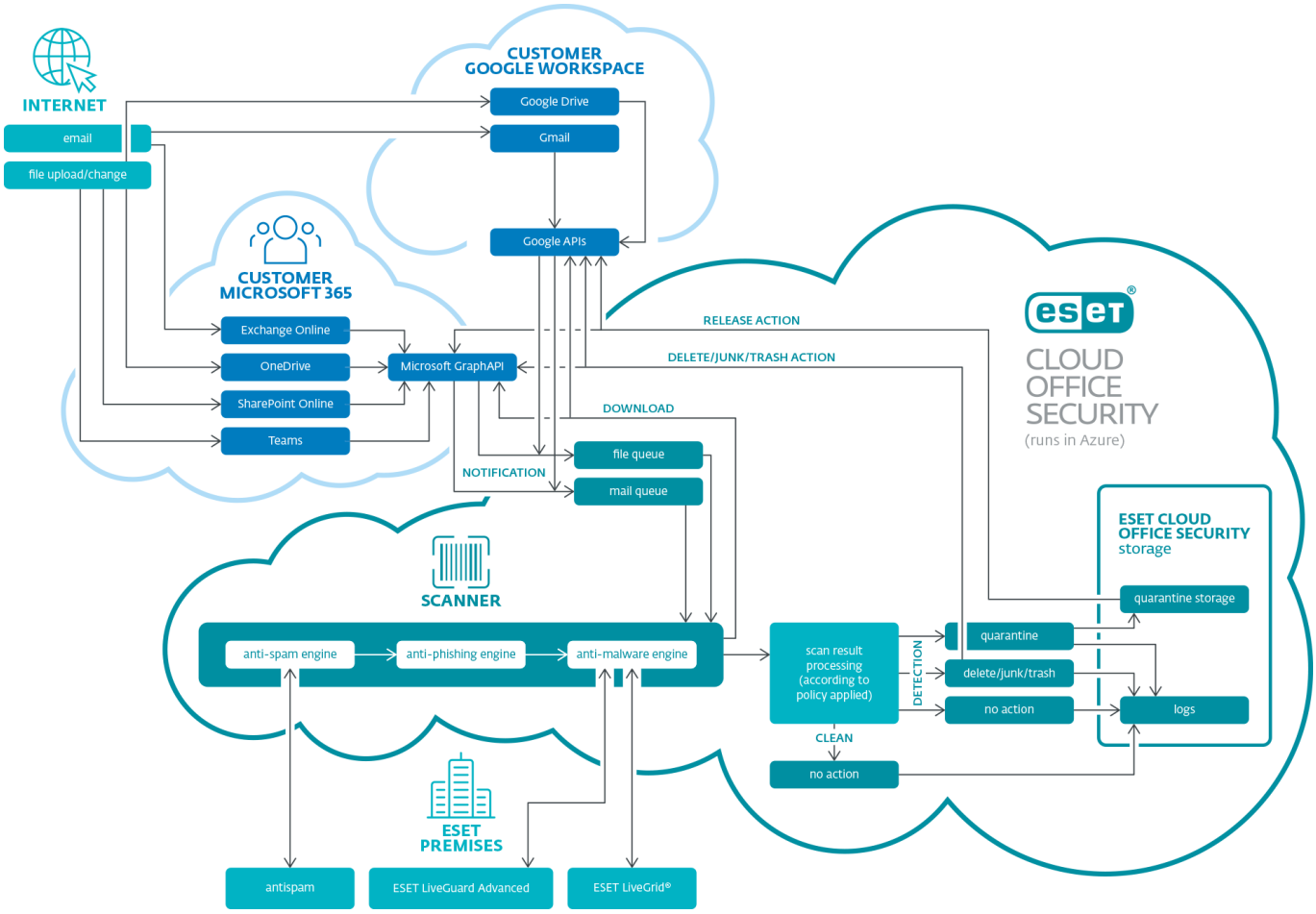
Prehľad

ESET Cloud Office Security je multitenantná škálovateľná cloudová služba v prostredí Microsoft Azure. Riešenie ESET Cloud Office Security je ponúkané ako Software-as-a-Service (SaaS) produkt, ktorý pracuje výhradne v cloude, takže na jeho prevádzku nepotrebujete vlastný hardvér. Ide o dokonalú kombináciu filtrovania spamu, antimalvérovej kontroly a antiphishingovej ochrany, ktorá pomáha chrániť vašu firemnú komunikáciu pred malvérom, minimalizuje nepriaznivý vplyv nevyžiadaných správ na produktivitu práce a predchádza tomu, aby sa prichádzajúce externé e□maily zneužívali ako kanál na cielené útoky.

Bezpečnostné služby ESET Cloud Office Security pokrývajú popredných poskytovateľov cloudových platforiem a poskytujú komplexnú e□mailovú ochranu vďaka špičkovým antimalvérovým jadrám a ESET LiveGuard Advanced. Toto riešenie ponúka pokročilú ochranu pred hrozbami prostredníctvom cloudového sandboxingu, ktorý analyzuje podozrivé vzorky v izolovanom prostredí.

Architektúra ESET Cloud Office Security umožňuje rýchle spustenie ochrany pripojením ku cloudovej platforme – Microsoft 365 a Google Workspace. Poskytuje vám možnosť spravovať ochranu prostredníctvom webovej konzoly dostupnej odkiaľkoľvek.

ESET Cloud Office Security ponúka pokročilú preventívnu ochranu na zabezpečenie firemných aplikácií Microsoft 365 – Exchange Online, OneDrive, SharePoint Online a Teams. Rovnaká ochrana sa vzťahuje aj na aplikácie Google Workspace – Gmail a Disk Google.



ESET Cloud Office Security chráni OneDrive a e-mailové schránky licencovaných používateľov, ako aj tímové skupiny a lokality SharePoint. Každé úložisko týchto aplikácií služby Microsoft 365 je chránené bez ohľadu na to, kto nahráva súbory alebo odosiela e-maily. Samotný obsah je chránený nezávisle od autora. V záujme čo najlepšej ochrany sa nerozlišuje, či je autor obsahu iba hosťom.

Hlavné funkcie

V nasledujúcej tabuľke nájdete zoznam funkcií dostupných v produkte ESET Cloud Office Security.

Podpora viacerých nájomníkov	Prostredníctvom jednej konzoly ESET Cloud Office Security môžete chrániť a spravovať viacerých nájomníkov Microsoft 365 a Google Workspace. Azure Active Directory (Azure AD) organizuje objekty, ako sú používatelia a aplikácie, do skupín, ktoré sa nazývajú nájomníci. Prostredníctvom nájomníkov môžete nastaviť politiky pre používateľov a aplikácie vo vašej organizácii s cieľom splniť bezpečnostné a prevádzkové požiadavky.

Antispam	Antispam je kľúčovým komponentom akéhokoľvek e-mailového servera. ESET Cloud Office Security využíva špičkové antispamové jadro, ktoré filtruje spam a phishing s vysokou mierou detekcie. ESET Cloud Office Security je niekoľkonásobným víťazom testu filtrovania a zachytávania spamu realizovaného poprednou testovacou organizáciou Virus Bulletin a niekoľkoročným držiteľom certifikácie VBSpam+. Naše antispamové jadro dosiahlo mieru detekcie spamu 99,99 % s nulovým výskytom falošných poplachov (false positive), vďaka čomu môžeme hovoriť o poprednej technológii v oblasti ochrany proti spamu. Antispam v produkte ESET Cloud Office Security je založený na dátach z cloudu, pričom väčšina využívaných cloudových databáz je umiestnená v datacentrách spoločnosti ESET. Antispamové cloudové služby umožňujú v prípade objavenia nového spamu pohotovo aktualizovať dáta v databázach a zabezpečiť tak rýchlejší reakčný čas.
Antiphishingová ochrana	Ide o funkciu, ktorá zabraňuje používateľom navštevovať phishingové webové stránky. E-mailové správy môžu obsahovať odkazy, ktoré smerujú na phishingové webové stránky. ESET Cloud Office Security využíva pokročilú a sofistikovanú metódu analýzy, pomocou ktorej sú telo a predmet prichádzajúcej správy prehľadávané s cieľom identifikovať takéto odkazy (URL). Odkazy sú porovnávané voči databáze s phishingovým obsahom, ktorá je neustále aktualizovaná.
Antimalvérová ochrana	Oceňovaná a inovatívna ochrana pred malvérom, ktorá využíva najmodernejšie technológie. Zabraňuje útokom a eliminuje všetky druhy hrozieb vrátane vírusov, ransomvéru, rootkitov, červov a spyvéru pomocou kontroly s podporou cloudu, vďaka ktorej je detekcia ešte účinnejšia. Navyše nezaťažuje systém, šetrí systémové prostriedky a nemá negatívny vplyv na výkon. Antimalvérová detekcia pracuje na viacerých vrstvách. Každá vrstva (fáza) pozostáva z niekoľkých technológií. Vo fáze pred spustením objektu (pre-execution) sa využívajú nasledujúce technológie: Kontrola UEFI (Unified Extensible Firmware Interface), Ochrana pred sieťovými útokmi, Reputácia a vyrovnávacia pamäť, Sandbox v rámci produktu a Detekcia na úrovni DNA. Medzi technológie, ktoré sa využívajú vo fáze execution, patrí Exploit Blocker, Ransomware Shield, Pokročilá kontrola pamäte a Kontrola skriptov (AMSI). Vo fáze post-execution sa využívajú technológie Ochrana pred botnetmi, Cloudový systém ochrany pred malvérom a Sandboxing. Kombinácia týchto kľúčových technológií vám poskytuje bezkonkurenčnú úroveň ochrany.
Politiky	Väčšie firmy majú zvyčajne viacero oddelení a v rámci každej organizačnej jednotky sa používajú rôzne nastavenia ochrany. ESET Cloud Office Security poskytuje nastavenia ochrany založené na politikách, ktoré môžete priradiť ku konkrétnym nájomníkom, používateľom, tímovým skupinám alebo lokalitám SharePoint. Každú politiku si môžete prispôsobiť podľa svojich potrieb.
Správca karantény	Správca karantény vám umožňuje kontrolovať objekty umiestnené v karanténe a vykonávať s nimi potrebné akcie (stiahnuť, odstrániť alebo uvoľniť). Táto funkcia ponúka jednoduchú správu e-mailov, príloh, ako aj súborov z Exchange Online/OneDrive/Tímových skupín/Lokalít SharePoint, ktoré boli umiestnené do karantény prostredníctvom ESET Cloud Office Security. Funkcia stiahnutia vám umožňuje analyzovať objekty v karanténe pomocou nástrojov tretích strán, ktoré môžu pomôcť pri rozhodovaní o tom, akú akciu je najvhodnejšie vykonať pre konkrétny objekt.
Riadiaci panel so štatistikami detekcie	Riadiaci panel poskytuje rýchly prehľad aktivít súvisiacich s bezpečnosťou v rámci Microsoft 365. Každá karta (Exchange Online/OneDrive/Tímové skupiny/Lokality SharePoint) obsahuje užitočné informácie. Karta Používateľ zobrazuje počet nájomníkov a využitie licencie, ako aj štatistické informácie o každom nájomníkovi – počet používateľov, najčastejších príjemcov spamu/phishingu/malvéru a najčastejšie podozrivé OneDrive účty/tímové skupiny/lokality SharePoint. Môžete si vybrať časové obdobie a nájomníka, pre ktorého budú zobrazené štatistické údaje. Ďalšie štatistiky detekcie a grafy sú zobrazené na kartách určených pre Exchange Online, OneDrive, Tímové skupiny a Lokality SharePoint. Ide o štatistické informácie, ako napr. počet skontrolovaných e-mailov a súborov alebo počet zachyteného spamu/phishingu/malvéru. Grafy zobrazujú frekvenciu výskytu pre každý typ detekcie – spam, malvér a phishing.

Detekcie s možnosťami filtrovania	Pomocou tejto funkcie si môžete zobraziť informácie o všetkých detekciách. Záznamy o každej detekcii zachytenej pomocou kontroly e-mailov sú dostupné na karte Exchange Online, kým záznamy detekcií zachytených pomocou kontroly súborov sú dostupné na kartách OneDrive/Tímové skupiny/Lokality SharePoint. To vám umožňuje efektívne filtrovať a jednoducho nájsť to, čo hľadáte, pomocou dodatočných informácií o konkrétnej detekcii (napr. názov infiltrácie, hash súboru).
Používatelia	Hlavným cieľom ochrany, ktorú ESET Cloud Office Security poskytuje, je používateľský účet. V podrobnostiach používateľa nájdete užitočné informácie, ako napr. prehľad, nastavenia definované politikami, zoznam politík priradených k používateľovi a detekcie súvisiace s Exchange Online a OneDrive. Táto funkcia pomáha preskúmať detekcie týkajúce sa konkrétneho používateľa. Môžete si tiež vybrať, ktorí používatelia budú chránení. Používatelia sú zoradení do skupín. Každá skupina predstavuje nájomníka Microsoft 365, ktorý obsahuje svojich používateľov. Na jednoduchšie vyhľadávanie konkrétnych používateľov v rámci skupiny môžete využiť filtrovanie s viacerými kritériami.
Hlásenia a ochrana s využitím strojového učenia	Súčasťou detekčného jadra je teraz aj pokročilé strojové učenie – pokročilá vrstva ochrany, ktorá zlepšuje detekciu na základe strojového učenia. Viac o tomto type ochrany sa môžete dočítať v slovníku pojmov. Môžete nakonfigurovať úrovne hlásenia pre tieto kategórie: malvér, potenciálne nechcené aplikácie (PUA), potenciálne podozrivé aplikácie a potenciálne nebezpečné aplikácie.
Reporty (štatistické reporty a reporty o e□mailovej karanténe)	Prostredníctvom tejto funkcie si môžete nechať na e□mail zasielať štatistické informácie o Exchange Online, OneDrive, tímových skupinách a lokalitách SharePoint, prípadne si kedykoľvek vygenerovať a stiahnuť report za vybrané obdobie. Môžete tiež naplánovať pravidelné generovanie reportov a ich zasielanie e□mailom na určené adresy príjemcov. Ako výstupný formát vyberte PDF alebo CSV. Reporty obsahujú údaje o počte skontrolovaných e-mailov, detegovanom malvéri, phishingu a spame. Ak si ako formát vyberiete PDF, reporty budú obsahovať aj údaje zobrazené v grafoch. Graf bude zobrazený samostatne pre skontrolované e-maily, detegovaný malvér, phishing a spam. K dispozícii budú aj štatistiky pre najčastejších príjemcov malvéru, phishingu a spamu. Viac informácií o možnostiach generovania reportov nájdete v kapitole Reporty. Okrem toho môžete vybraným príjemcom doručovať report o e□mailovej karanténe, ktorý obsahuje zoznam e□mailových správ premiestnených do karantény. Report o e□mailovej karanténe sa odošle v stanovenom dátume a čase, avšak len v prípade pridania nových položiek do karantény.
Tímy a lokality	ESET Cloud Office Security poskytuje ochranu pre tímové skupiny v službe Teams a lokality SharePoint. Táto funkcia rozširuje ochranu na riešenia Microsoft 365 určené na podporu spolupráce, keďže umožňuje chrániť SharePoint a Teams a zaisťuje bezpečné zdieľanie súborov. Ak už máte ESET Cloud Office Security, pred použitím funkcie Tímy a lokality môžete byť vyzvaný k obnoveniu súhlasu.
ESET LiveGuard Advanced	Dodatočná vrstva ochrany pred pokročilými zero-day hrozbami. ESET LiveGuard Advanced je riešenie cloudového sandboxingu, ktoré analyzuje zaslané súbory tak, že podozrivý kód spustí v izolovanom prostredí a následne vyhodnocuje jeho správanie. ESET Cloud Office Security odosiela na analýzu do ESET LiveGuard Advanced podozrivé e□mailové prílohy a súbory z Exchange Online, OneDrive, lokalít SharePoint a tímových skupín v službe Teams. Funkciu ESET LiveGuard Advanced môžete zapnúť a konfigurovať pomocou politík. Výsledky analýzy sa zobrazujú v protokoloch kontroly.
Protokol auditu	Protokol auditu umožňuje správcovi kontrolovať aktivity vykonané v rámci ESET Cloud Office Security. Táto funkcia môže byť užitočná najmä v prípade, že máte viacerých používateľov konzoly ESET Cloud Office Security. V protokole auditu sú zaznamenané všetky aktivity v tom poradí, v akom sa uskutočnili. Protokoly auditu uchovávajú informácie o konkrétnej operácii alebo udalosti. Protokoly auditu sa vytvárajú pri každej zmene alebo vytvorení objektu v rámci ESET Cloud Office Security (napríklad licenčného fondu, používateľa, politiky, reportu, položky v karanténe – e. g. prílohy).

Google Workspace (ochrana Gmailu a Disku Google)	ESET Cloud Office Security rozširuje pokrytie bezpečnostných služieb o ďalšieho popredného poskytovateľa cloudového e-mailu, Google Workspace. ESET Cloud Office Security poskytuje komplexnú ochranu používateľom Gmailu a Disku Google s využitím všetkých funkcií. Používateľov služby Google Workspace chráni pred malvérom, phishingom a spamom.

Čo je nové

V tejto kapitole nájdete informácie o nových funkciách a vylepšeniach, ktoré boli zavedené v jednotlivých verziách ESET Cloud Office Security:

Portál verzie 353 vydaný 23. novembra 2023

- Pridaná integrácia služby Google Workspace.
- Navigátor produktov na rýchly prístup k účtu ESET Business Account (ďalšie konzoly budú pridané v nasledujúcich mesiacoch).
- *Ďalšie opravy chýb a vylepšenia backendu.*

Portál verzie 342.3 vydaný 24. októbra 2023

- Pridané overenie účtu správcu pre Google Workspace.
- Pridaný typ stĺpca Používateľ.
- *Ďalšie opravy chýb a vylepšenia backendu.*

Portál verzie 311.2 vydaný 31. júla 2023

- Pridaná služba Google Workspace (ochrana Gmailu a Disku Google) – prístup k sekcii Ukážka funkcií v menu Rýchle odkazy.
- Pridaný tmavý režim.
- Pridaný navigátor produktov pre používateľov ESET HUB so skorým prístupom.
- *Ďalšie opravy chýb a vylepšenia backendu.*

Portál verzie 293.7 vydaný 13. júla 2023

- Pridané priradenie nájomníkov k lokalitám v rámci ESET Business Account (EBA). Táto zmena zabezpečuje kompatibilitu s budúcim zákazníckym portálom ESET PROTECT HUB, ktorý nahradí ESET MSP Administrator (EMA) a ESET Business Account (EBA). Týka sa to len niekoľkých zákazníkov, ktorí používajú licencie z viacerých lokalít na ochranu jedného nájomníka. Ak je to váš prípad, zobrazí sa vám výzva na priradenie nájomníkov k lokalitám v rámci EBA.
- Ďalšie drobné vylepšenia a opravy chýb.

Portál verzie 251.1 vydaný 21. marca 2023

- Zlepšenia v rámci oneskoreného načítania obrazoviek (tzv. lazy loading) na lepšiu podporu nájomníkov s desiatkami tisíc používateľov.
- Zmeny v sprievodcovi pre pridanie nájomníka.
- Aktualizovaná sekcia O aplikácii.
- Aktualizácie podmienok používania a zásad ochrany osobných údajov (Obmedzenia a politika uchovávania údajov).

Portál verzie 205 vydaný 9. novembra 2022

- Pridané okno „Čo je nové“ s popisom nových funkcií, ktoré sa zobrazí pri prvom prihlásení do konzoly ESET Cloud Office Security.
- Možnosť exportovať protokoly kontroly a protokoly auditu do súboru CSV.
- Pridané nové nastavenie pri zlučovaní politík so zoznamami a notifikačnými e-mailmi.

Portál verzie 180.2 vydaný 27. júla 2022

- Nová funkcia Protokol auditu.
- Zmena sekcie Protokoly na Protokoly kontroly.

Portál verzie 156.2 vydaný 26. apríla 2022

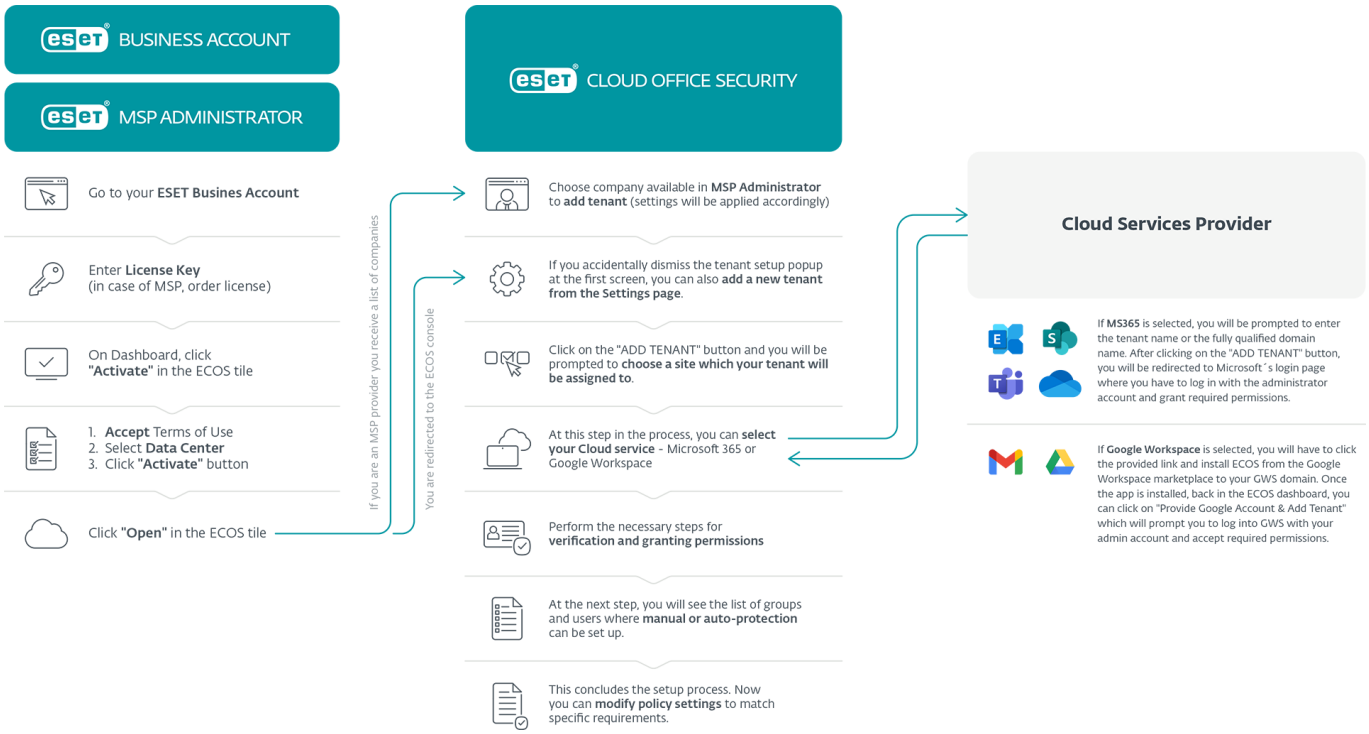
- Premenovanie Dynamic Threat Defense na ESET LiveGuard Advanced.
- Odosielanie falošne pozitívnych/falošne negatívnych vzoriek na analýzu.
- Import/export zoznamov povolených, blokovaných a ignorovaných adries/domén v rámci sekcie Politiky.
- Riadiaci panel zobrazujúci počet nechránených používateľov na karte Prehľad.
- Oprava chyby, ktorá umiestňovala notifikačné e□maily do karantény.

Portál verzie 140.6 vydaný 9. februára 2022

- Možnosť zahrnúť do reportov vlastnú značku (tzv. whitelabel) a rozhodnúť sa len pre zobrazenie vlastného loga alebo spoločné zobrazenie s logom ESET formou co□brandingu.
- Pridaná možnosť nastaviť preferovaný jazyk e□mailových oznámení zasielaných vlastníkom e□mailových schránok.
- Pridaná možnosť nastaviť preferovaný jazyk e□mailových oznámení zasielaných členom patriacim pod nájomníka.
- Filtrovanie e□mailov podľa ID správy.

Integrácia

Priebeh integrácie ESET Cloud Office Security s poskytovateľom cloudových služieb:



Špecifikácie

Referenčné technické špecifikácie pre ESET Cloud Office Security:

- Požiadavky
- Podporované plány Microsoft 365
- Podporované plány služby Google Workspace
- Podporované webové prehliadače
- Obmedzenia a politika uchovávania údajov

Požiadavky

Aby ste mohli využívať ESET Cloud Office Security na ochranu Microsoft 365, vyžaduje sa splnenie nasledujúcich požiadaviek:

- Podporovaný plán predplatného služby Microsoft 365
- Prístup správcu k službe Azure Active Directory (Azure AD)
- Azure Cloud Services – Exchange | OneDrive
- Účet na portáli ESET Business Account alebo ESET MSP Administrator

Podporované plány Microsoft 365

ESET Cloud Office Security podporuje nasledujúce plány Microsoft 365, Exchange Online a OneDrive.

Plány Microsoft 365 pre veľké podniky:

- Microsoft 365 Apps for enterprise
- Microsoft 365 E3
- Microsoft 365 E5
- Microsoft 365 F3
- Office 365 E1
- Office 365 E3
- Office 365 E5
- Office 365 F3

Plány Microsoft 365 pre firmy:

- Microsoft 365 Business Basic
- Microsoft 365 Business Standard
- Microsoft 365 Business Premium
- Microsoft 365 Apps

Plány Microsoft 365 pre vzdelávacie inštitúcie:

- Microsoft 365 A3
- Microsoft 365 A5

Plány Exchange Online:

- Exchange Online (Plan 1)
- Exchange Online (Plan 2)
- Microsoft 365 Business Standard

Plány OneDrive:

- OneDrive for Business (Plan 1)
- OneDrive for Business (Plan 2)
- Microsoft 365 Business Basic
- Microsoft 365 Business Standard

Podporované plány služby Google Workspace

ESET Cloud Office Security podporuje tieto plány služby Google Workspace:

- Business Starter
- Business Standard
- Business Plus
- Enterprise

Podporované webové prehliadače

> Pre optimálne fungovanie produktu ESET Cloud Office Security odporúčame používať najnovšie verzie webových prehliadačov.

Konzolu ESET Cloud Office Security môžete používať v nasledujúcich webových prehliadačoch:

- Mozilla Firefox 69 a novšie verzie
- Microsoft Edge 44 a novšie verzie
- Google Chrome 77 a novšie verzie
- Opera 63 a novšie verzie
- Safari 13.x a novšie verzie

Microsoft Internet Explorer nie je podporovaný.

Obmedzenia a politika uchovávania údajov

Za určitých okolností existujú isté obmedzenia pre ESET Cloud Office Security, pokiaľ ide o kontrolu. Súbor nebude skontrolovaný a zobrazí sa v protokoloch kontroly s príznakom **Neskontrolované** v prípade, že nastane niektorá z nasledujúcich situácií:

- Veľkosť súboru je viac ako 200 MB.
- Kontrola trvá dlhšie ako 2 minúty a vyprší platnosť relácie.
- Archív má 10 alebo viac úrovní vnorenia (zvyčajne ide o súbor, ktorý sa nazýva „archívna bomba“ alebo „zip bomba“).
- Archív je chránený heslom.
- Súbor je poškodený.

Obmedzenia vzťahujúce sa na karanténu (pri uvoľňovaní objektov z karantény):

- 15 MB pre jednu e-mailovú prílohu.
- 150 MB pre celý e-mail vrátane príloh.

Politika uchovávania údajov:

Objekt	Obdobie uchovávania	Poznámka
Objekty v karanténe	30 dní	Objekty staršie ako 30 dní budú natrvalo odstránené.
Detekcie	90 dní	Záznamy staršie ako 90 dní budú natrvalo odstránené.
Záznamy protokolov kontroly	90 dní	Záznamy staršie ako 90 dní budú natrvalo odstránené.
Záznamy protokolov kontroly s čistými výsledkami kontroly	3 dni	Ak sa uplatňuje politika zapisovania všetkých objektov do protokolu, čisté výsledky kontroly staršie ako 3 dni sa natrvalo odstránia.
Záloha databázy ESET Cloud Office Security	90 dní	Zálohy staršie ako 90 dní budú natrvalo zmazané.
Protokoly auditu	90 dní	Záznamy staršie ako 90 dní budú natrvalo odstránené.
Protokoly so štatistikami aplikácie	90 dní	Záznamy staršie ako 90 dní budú natrvalo odstránené.

Nájomník odstránený z konzoly ESET Cloud Office Security

Po odstránení nájomníka z konzoly ESET Cloud Office Security sa údaje nájomníka uchovávajú ešte 30 dní (karanténa, protokoly kontroly a štatistiky sa odstránia po 30 dňoch). Ak nájomníka do 30 dní znova pridáte, všetky údaje sa obnovia. Ostatné objekty (nájomníci, používatelia, skupiny, lokality, reporty, politiky) sa po 90 dňoch natrvalo odstránia.

ESET Cloud Office Security deaktivovaný v portáli ESET Business Account alebo ESET MSP Administrator

Ak deaktivujete ESET Cloud Office Security na portáli ESET Business Account alebo ESET MSP Administrator, tento proces odstráni aj nájomníkov z ESET Cloud Office Security. Odstránenie ESET Cloud Office Security je trvalé a vymazané údaje nie je možné obnoviť.

Antispamová kontrola

ESET Cloud Office Security kontroluje správy uložené v e□mailových schránkach na prítomnosť spamu. Z tohto dôvodu nemôže ESET Cloud Office Security zabrániť používateľovi v odoslaní spamovej správy na externú e□mailovú adresu. Ak by náhodou došlo k odcudzeniu prihlasovacích údajov používateľa služby Office 365, spamer môže tieto údaje použiť na hromadné rozosielanie spamových správ (v takomto prípade ide o odchádzajúcu e□mailovú komunikáciu).

Licencovanie ESET Cloud Office Security

Licencie ESET Cloud Office Security môžete spravovať prostredníctvom portálu ESET Business Account alebo ESET MSP Administrator. ESET Cloud Office Security si môžete vyskúšať zdarma využitím 30□dňovej skúšobnej licencie.

- Informácie o vytvorení účtu, pridaní licencie alebo správe licencie nájdete v kapitole ESET Business Account.
- Ak ste poskytovateľom spravovaných služieb (MSP), prečítajte si pokyny pre ESET MSP Administrator.

ESET Business Account a ESET MSP Administrator (hybridný licenčný účet)

Ak máte zaregistrovanú rovnakú e-mailovú adresu na portáli ESET MSP Administrator aj ESET Business Account (jednotné prihlásenie), môžete prepínať medzi zobrazením ESET Business Account a ESET MSP Administrator. Aktivujte ochranu pre používateľov alebo spoločnosti prostredníctvom správy licencií pre ESET Cloud Office Security.

Odkladacia lehota po uplynutí platnosti licencie v portáli ESET Business Account

Keď sa vaša licencia bude blížiť k vypršaniu, v rozhraní portálu ESET Business Account sa zobrazí upozornenie. Ak uplynie dátum platnosti licencie a licenciu ste si neobnovili ani ste si neaktivovali novú licenciu, v portáli ESET Business Account sa zobrazí upozornenie o uplynutí platnosti licencie. Ak nie je k dispozícii vhodná licencia, v portáli ESET Business Account sa zobrazí upozornenie, že vaša licencia bude o 14 dní pozastavená a zároveň vám bude doručený e-mail na adresu uvedenú vo vašom účte správcu.

K dispozícii máte 14-dňovú odkladaciu lehotu, počas ktorej si môžete po vypršaní svoju licenciu obnoviť. Po uplynutí polovice tejto lehoty budete upozornený v portáli ESET Business Account aj prostredníctvom e-mailu. Po 14 dňoch bude váš produkt ESET Cloud Office Security pozastavený. Váš účet bude nedostupný a nefunkčný. Pozastavený účet ESET Cloud Office Security však ostane uložený a po pridaní novej licencie ESET Cloud Office

Security do portálu ESET Business Account bude opäť dostupný. Váš účet ESET Cloud Office Security môže byť pozastavený maximálne 30 dní a po uplynutí tejto doby bude natrvalo odstránený.

Ak váš účet vstúpi do pozastaveného stavu a do jeho odstránenia zostáva 14 dní, budete upozornený v portáli ESET Business Account aj prostredníctvom e-mailu. Na obnovenie prístupu k svojmu účtu ESET Cloud Office Security si musíte aktivovať novú licenciu ESET Cloud Office Security.

Používatelia sú počas odkladacej lehoty naďalej plne chránení. Po uplynutí lehoty prídu používatelia o ochranu.

Pozastavená licencia

Ak v portáli ESET Business Account nie je k dispozícii žiadna platná licencia pre ESET Cloud Office Security, vaša inštancia ESET Cloud Office Security bude pozastavená. Inštancia bude nedostupná a nefunkčná. Vaša inštancia ESET Cloud Office Security môže byť pozastavená maximálne 30 dní a po uplynutí tejto doby bude natrvalo odstránená. Na obnovenie prístupu k svojej inštancii ESET Cloud Office Security si musíte aktivovať novú licenciu pre ESET Cloud Office Security.

ESET Business Account

Portál ESET Business Account slúži ako jednotný prístupový bod pre ESET Business Account aj ESET Cloud Office Security. Na prístup k svojmu produktu ESET Cloud Office Security môžete použiť prihlasovaciu stránku ESET Business Account alebo ESET Cloud Office Security. V oboch prípadoch však budete presmerovaný na portál ESET Business Account, kde dôjde k overeniu prihlásenia.

- Ak nemáte zaregistrovaný účet v portáli ESET Business Account, vytvorte si ho.
- Ak účet ESET Business Account máte, pridajte licenciu pre ESET Cloud Office Security.
- Spravujte účet ESET Business Account.

Vytvorenie nového účtu ESET Business Account

1. Otvorte prihlasovaciu stránku ESET Business Account a kliknite na **Bezplatne sa zaregistrujte**. Dôkladne vyplňte registračný formulár. Zadaná e-mailová adresa bude použitá ako prihlasovacie meno.

2. Heslo musí obsahovať aspoň 10 znakov. Zadajte svoje **Meno** a **Podrobnosti o spoločnosti** a kliknite na **Pokračovať**. Prečítajte si **Podmienky používania spoločnosti ESET** a potvrďte, že s nimi súhlasíte. Vyplňte formulár reCAPTCHA a kliknite na **Registrovať**.

3. Po úspešnej registrácii dostanete e-mail s potvrdením (môže to trvať až 15 minút). Kliknite na odkaz v e-maile s potvrdením, čím otvoríte nové okno **Aktivovať účet**.

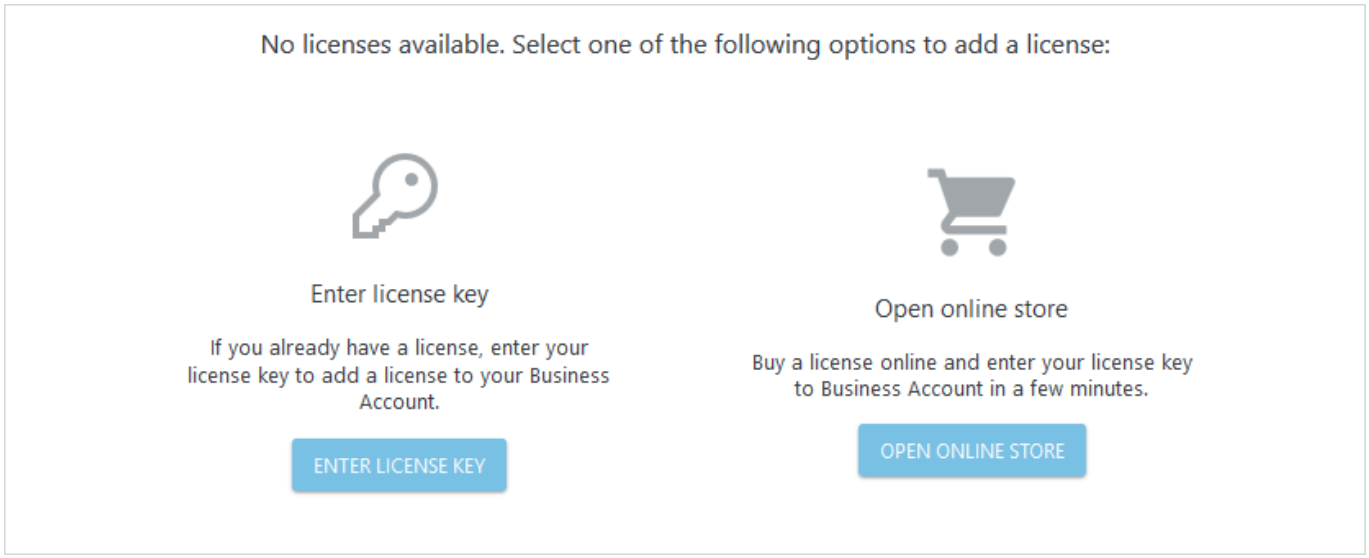
4. Zadajte svoje heslo a kliknite na **Aktivovať** pre aktiváciu svojho účtu ESET Business Account. Bude vám doručený ďalší e-mail pre potvrdenie, že váš účet ESET Business Account bol úspešne vytvorený. Teraz sa už môžete prihlásiť do účtu ESET Business Account.

Po aktivácii účtu ESET Business Account pridajte svoju licenciu pre ESET Cloud Office Security.

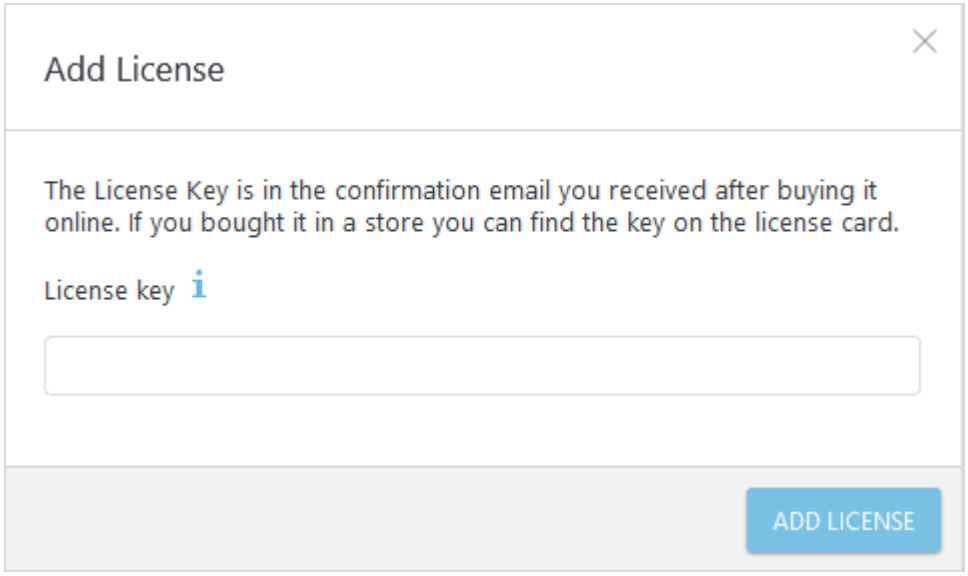
Pridanie licencie pre ESET Cloud Office Security do portálu ESET Business Account

Ak sa prihlasujete po prvýkrát, po úspešnom prihlásení do portálu ESET Business Account uvidíte úvodnú obrazovku pre ESET Business Account.

1. Kliknutím na **Pridať licenciu** otvoríte licenčné okno. Ak ste bežný ESET Business Account používateľ, prejdite na kartu **Licencia** a kliknite na **Pridať licenciu**.



2. Zadajte svoj **Licenčný kľúč** a kliknite na **Pridať licenciu**.



3. Dostanete e-mail s overovacím odkazom. Kliknite na odkaz a zadajte svoje prihlasovacie údaje do portálu ESET Business Account. Viac informácií o správe licencií, používateľoch a lokalitách nájdete v príručke pre ESET Business Account.

Správa účtu ESET Business Account

Bežné činnosti súvisiace s licencovaním:

Lokality a licenčný fond

Licencie a licenčné fondy sa načítavajú z portálu ESET Business Account. Licenčné fondy sú dostupné len v prípade, že máte existujúce lokality v rámci portálu ESET Business Account.

Vytvorenie nového používateľa na portáli ESET Business Account

Môžete vytvoriť používateľa, ktorý vám pomôže spravovať časť vašich licencií.

1. Otvorte ESET Business Account a prihláste sa.
2. Vyberte sekciu **Správa používateľov**, kliknite na položku **Nový používateľ** a zadajte požadované informácie.
3. Pre používateľa nastavte **prístupové práva** k ESET Cloud Office Security:
   - **Čítanie** – používateľ má prístup k ESET Cloud Office Security a vidí používateľov, protokoly a detekcie, ale nemôže spravovať politiky, chrániť používateľov ani uvoľňovať objekty z karantény.
   - **Zapisovanie** – používateľ má úplný prístup k ESET Cloud Office Security, vidí a môže spravovať používateľov a karanténu, ako aj vytvárať politiky.
   - **Bez prístupu** – používateľ nemá prístup k ESET Cloud Office Security.
4. Pre konzolu ESET Cloud Office Security vyberte jazyk cez používateľské **Nastavenia**.
5. Kliknite na **Vytvoriť**, čím vytvoríte nového používateľa.

Vytvorenie novej lokality na portáli ESET Business Account

Lokality vám umožňujú rozdeľovať alebo zlučovať licencie do licenčných fondov. Lokality sú samostatné skupiny, ktoré môžu mať svoje vlastné umiestnenie a správcov.

1. Otvorte ESET Business Account a prihláste sa.
2. Vyberte **Podrobnosti**, kliknite na **Vytvoriť lokalitu** a zadajte požadované osobné údaje.
3. Kliknite na **Pridať používateľa**, vyberte používateľa a kliknite na **Potvrdiť**.
4. V licenčnom fonde kliknite na **Pridať jednotky** a vyberte licenciu pre ESET Cloud Office Security. V prípade potreby môžete zmeniť **Podjednotky**. Kliknite na **Potvrdiť**.
5. Kliknite na **Vytvoriť**, čím vytvoríte lokalitu.

ESET MSP Administrator

ESET MSP Administrator je systém určený na správu licencií, ktorý umožňuje MSP používateľom vytvárať viacerých MSP zákazníkov a generovať licencie s konkrétnym počtom jednotiek. Licenčný portál ESET MSP

Administrator pracuje s cenotvorbou a fakturáciou podľa denného objemu jednotiek.

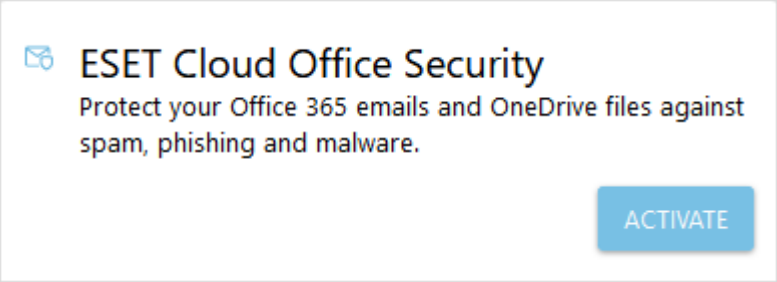
Riešenie ESET Cloud Office Security je dostupné pre všetkých MSP manažérov, MSP a spravovaných MSP. ESET MSP Administrator môžu aktivovať používatelia ESET Cloud Office Security, ktorí majú oprávnenia na zápis.
K riešeniu ESET Cloud Office Security majú prístup používatelia s oprávneniami na zápis alebo čítanie, prípadne tí, ktorí majú definované vlastné prístupové práva.

- Vytvorenie nového MSP zákazníka (na aktiváciu konzoly ESET Cloud Office Security sa vyžaduje e-mailová adresa zákazníka)
- Aktivácia produktu ESET Cloud Office Security prostredníctvom portálu ESET MSP Administrator

Aktivácia ESET Cloud Office Security

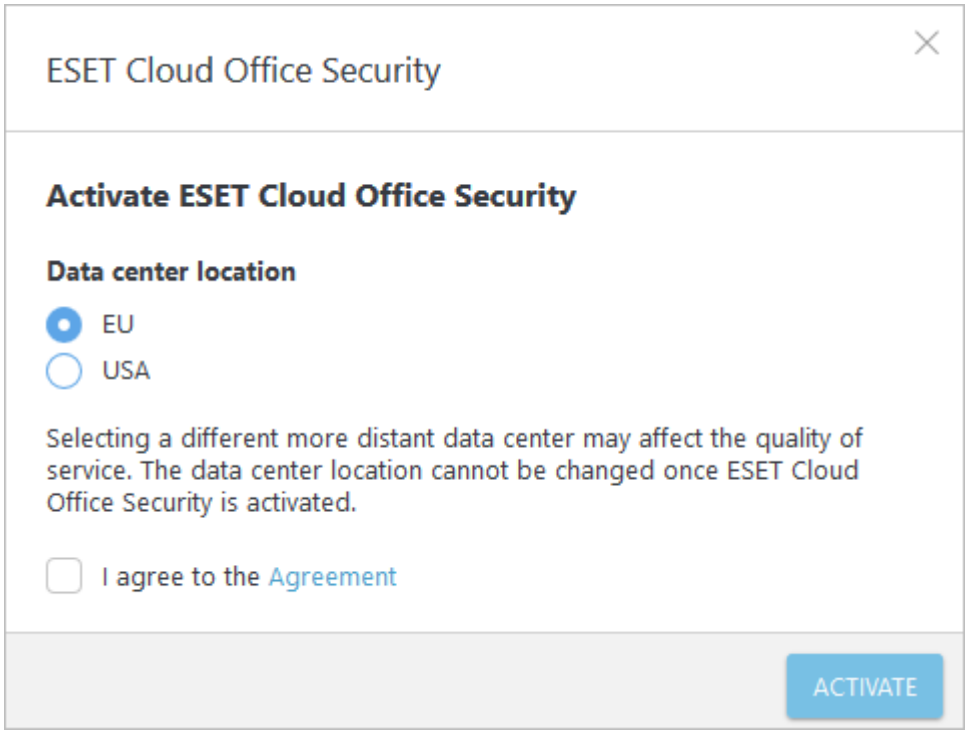
1. Prihláste sa do portálu ESET Business Account alebo ESET MSP Administrator a v **Riadiacom paneli** nájdite dlaždicu pre ESET Cloud Office Security.

2. Kliknite na **Aktivovať** v pravom dolnom rohu sekcie ESET Cloud Office Security.

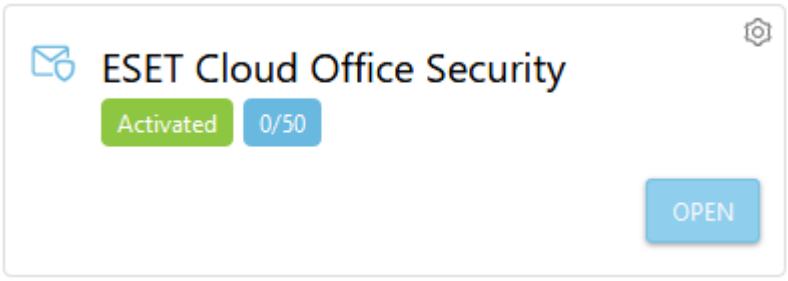


3. Sprievodca aktiváciou vás vyzve prečítať si Podmienky používania ESET Cloud Office Security a zobrazí optimálnu lokalitu dátového centra na základe vašej aktuálnej polohy. Vyberte možnosť **Súhlasím s podmienkami používania** a kliknite na **Aktivovať**. Neodporúčame meniť lokalitu dátového centra. Ak však potrebujete použiť inú lokalitu, použite príslušnú možnosť.

Dátové centrá sú úplne oddelené. Keď vyberiete lokalitu dátového centra, už ju nebude možné zmeniť. Ak chcete zmeniť dátové centrum, spustite aktivačný proces od začiatku.

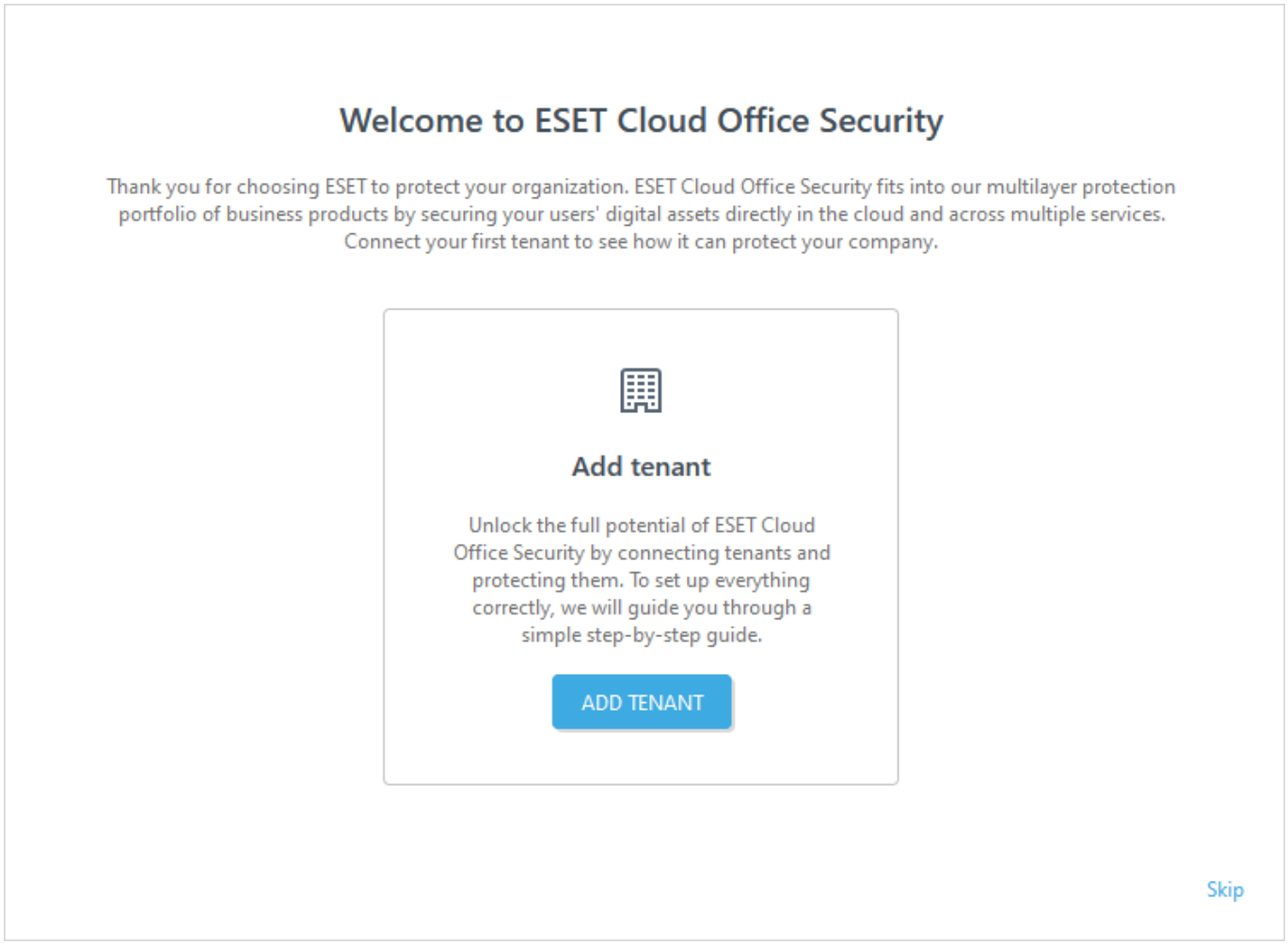


4. Kliknite na **Otvoriť** v sekcii ESET Cloud Office Security. V novom okne prehliadača sa otvorí Riadiaci panel ESET Cloud Office Security.

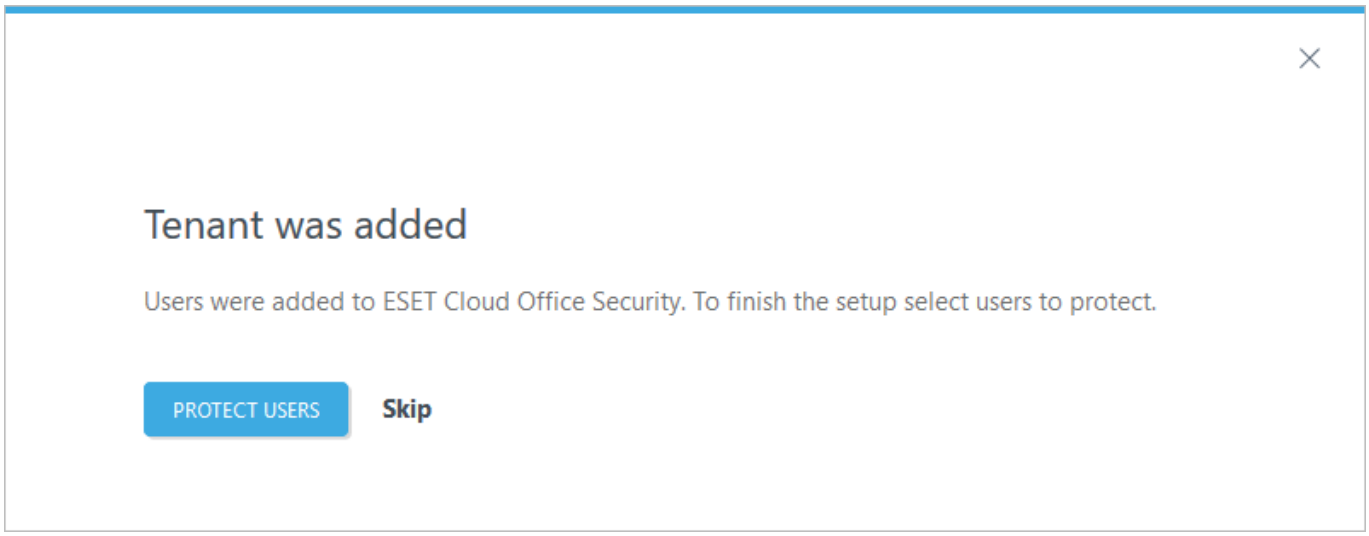


Keď sa po prvýkrát prihlásite do ESET Cloud Office Security, zobrazí sa **Sprievodca spustením**. Tento sprievodca vás prevedie procesom prvotného nasadenia.

1. Pridajte svojho nájomníka (Microsoft 365 alebo Google Workspace).



2. Ochráňte používateľov. Ak sa rozhodnete tento proces **preskočiť**, pre používateľov alebo spoločnosť môžete aktivovať ochranu neskôr prostredníctvom správy licencií pre ESET Cloud Office Security.

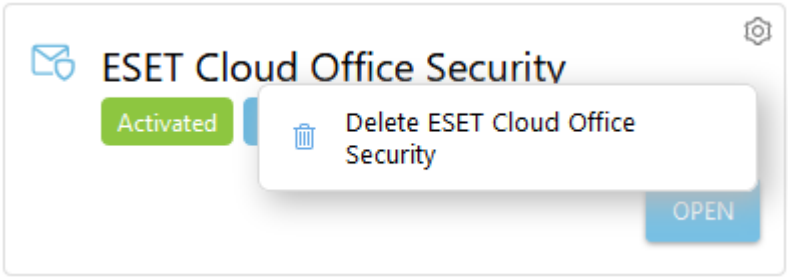


Deaktivácia ESET Cloud Office Security

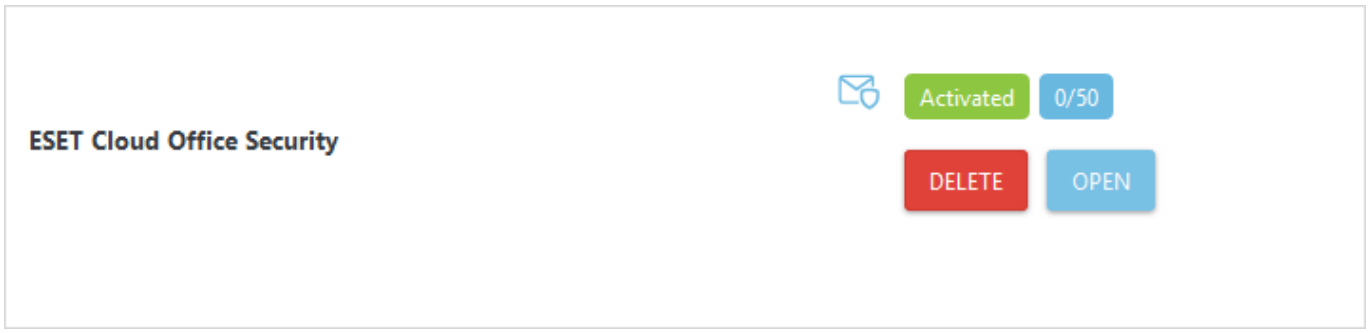
1. Prihláste sa do portálu ESET Business Account alebo ESET MSP Administrator a v **Riadiacom paneli** nájdite dlaždicu pre ESET Cloud Office Security.

2. Kliknite na ikonu v pravom hornom rohu sekcie ESET Cloud Office Security a vyberte možnosť **Odstrániť**

ESET Cloud Office Security.

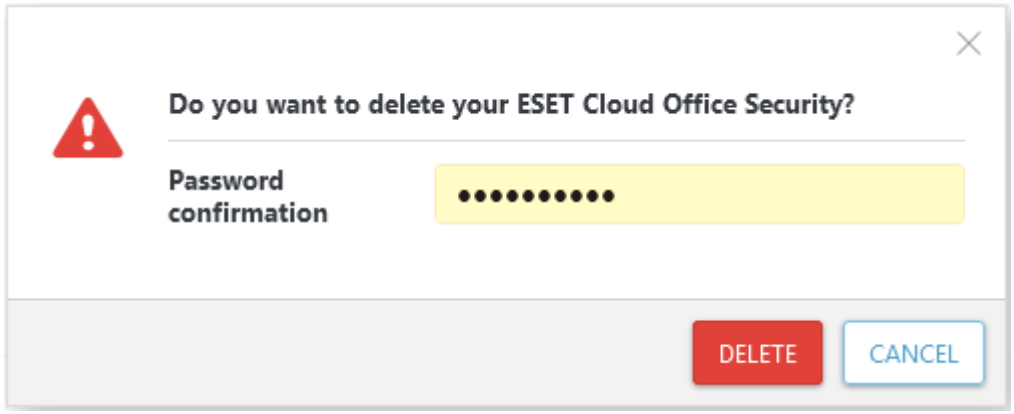


3. Môžete tiež prejsť do sekcie **Podrobnosti** a kliknúť na **Odstrániť**.



4. Následne sa zobrazí okno s upozornením, že dôjde k odstráneniu všetkých dát. Akciu potvrďte zadaním hesla k svojmu účtu na portáli ESET Business Account a kliknite na **Odstrániť**.

Odstránenie inštancie ESET Cloud Office Security je trvalé. Vymazané údaje nie je možné obnoviť.



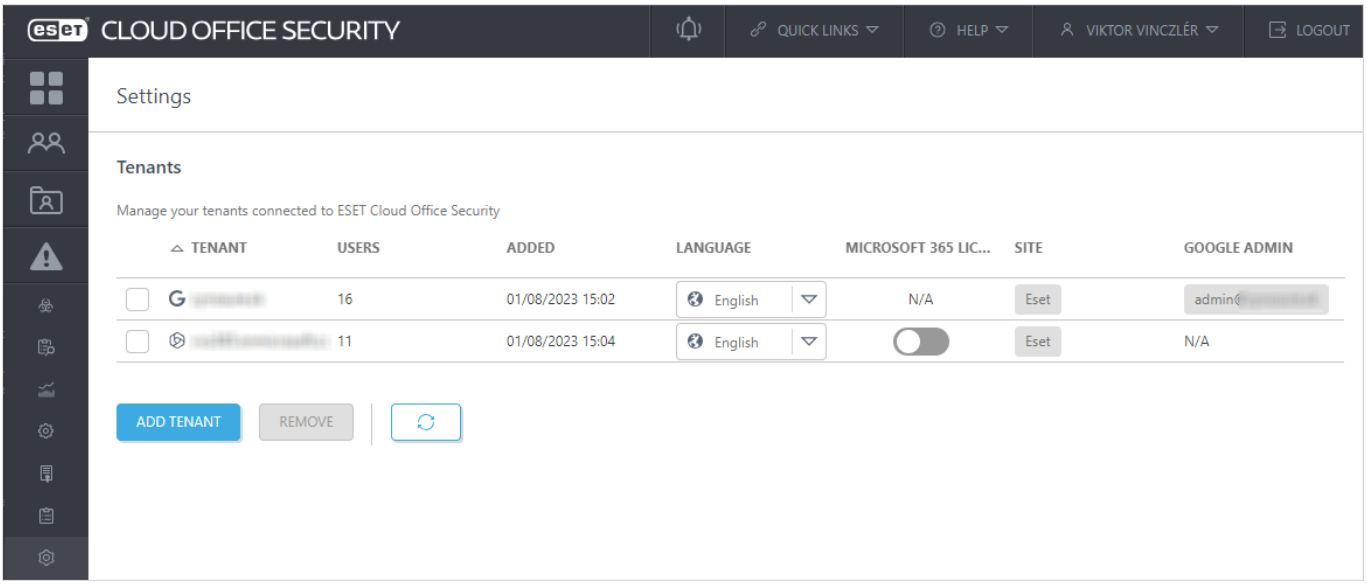
Vaša inštancia ESET Cloud Office Security bola odstránená a dlaždica produktu ESET Cloud Office Security sa vráti do stavu **Neaktivované**. Dostanete tiež potvrdzujúci e-mail z účtu ESET Business Account.

Správa nájomníkov cez Nastavenia

V tejto časti môžete spravovať nájomníkov pripojených k ESET Cloud Office Security. Všetci zaregistrovaní nájomníci sú zobrazení v tabuľke spolu s podrobnými informáciami. Pre opätovné načítanie tabuľky obsahujúcej nájomníkov kliknite na tlačidlo obnovenia.

Ak chcete pridať nového nájomníka, kliknite na Pridať nájomníka a vyberte Microsoft 365 alebo Google Workspace podľa toho, ktorú cloudovú službu chcete chrániť. Po dokončení procesu registrácie nájomníka bude vaša služba Microsoft 365 alebo Google Workspace chránená prostredníctvom produktu ESET Cloud Office Security.

Po pridaní nájomníka sa obrazovka zmení a zobrazí sa zoznam nájomníkov priradených k lokalite. Môžete spravovať existujúceho nájomníka alebo pridať ďalších. V tabuľke sa zobrazuje názov nájomníka, počet používateľov, kedy bol nájomník pridaný, nastavenie jazyka, používatelia s licenciou Microsoft 365, názov lokality a správca Google.



Jazyk

Toto nastavenie určuje jazyk, v ktorom sa budú členom patriacim pod nájomníka zasielať e-mailové oznámenia. Jazyk môžete nastaviť pre každého nájomníka zvlášť, čo môžete využiť, ak ste MSP a spravujete viacero spoločností.

Ak chcete odstrániť nájomníka z konzoly ESET Cloud Office Security, označte požadovaného nájomníka a kliknite na Odstrániť. Zobrazí sa potvrdzujúce okno, ktoré vám umožní vykonať konečné rozhodnutie. Po odstránení nájomníka dôjde po 30 dňoch k zmazaniu všetkých používateľských dát.

Licencovaní používatelia služby Microsoft 365

Táto možnosť je v predvolených nastaveniach zapnutá. Ide o ekvivalent zoznamu používateľov, ktorý nájdete v Centre spravovania služby Microsoft 365 v sekcii **Používatelia** > **Aktívni používatelia** > Filter: **Používatelia s licenciou**.

Po vypnutí tejto možnosti sa v ESET Cloud Office Security zobrazia všetci používatelia vrátane tých bez platnej licencie Microsoft 365 (napríklad zdieľané e-mailové schránky). Ak používate automatickú ochranu a v rámci nájomníka alebo skupiny sú používatelia bez platnej licencie Microsoft 365, dôjde k zobrazeniu týchto používateľov a zabezpečeniu ich ochrany, na ktorú sa využije potrebný počet licenčných jednotiek ESET Cloud Office Security. Do jednej hodiny od zobrazenia takýchto nových používateľov môže byť pri ich stave ochrany uvedené **Čaká sa**. Po dokončení procesu automatickej ochrany sa stav ochrany zmení na **Chránené** alebo na iný zodpovedajúci stav v sekcii Používatelia.

> Ak nájomník alebo skupina využívajúca automatickú ochranu obsahuje používateľa bez e-mailovej schránky a služby OneDrive, tento používateľ spotrebuje jednu licenčnú jednotku ESET Cloud Office Security. Pre takéhoto používateľa sa v rámci stavu ochrany zobrazí **Upozornenie**.

Ak opätovne zapnete možnosť Licencovaní používatelia služby Microsoft 365, zobrazení zostanú iba používatelia s licenciou Microsoft 365. Ak používate automatickú ochranu, používatelia bez licencie Microsoft 365 zmiznú zo sekcie Používatelia a uvoľní sa príslušný počet licenčných jednotiek ESET Cloud Office Security. Môže trvať až 1

hodinu, kým sa zmena prejaví.

> Ak ste manuálne aktivovali ochranu pre používateľov bez licencie Microsoft 365 (a súčasne bola vypnutá možnosť **Licencovaní používatelia služby Microsoft 365**), títo používatelia zostanú zobrazení a chránení aj po zapnutí možnosti **Licencovaní používatelia služby Microsoft 365** (až kým sa nedostanú do stavu nechránení).

Lokalita

Ak chcete zmeniť lokalitu, ku ktorej je nájomník priradený, kliknutím na názov lokality otvorte okno **Vyberte lokalitu, ktorú chcete chrániť** a vykonajte požadované zmeny.

Správca Google

Správca Google by mal byť aktívny e-mail vášho správcu služby Google Workspace.

> Ak sa má zmeniť rola alebo e-mailová adresa správcu, kliknite na danú informáciu správcu Google a aktualizujte ju. Urobte tak v predstihu, aby ste zaistili funkcionalitu nájomníkov a ochranu svojej lokality.

Obnoviť súhlas

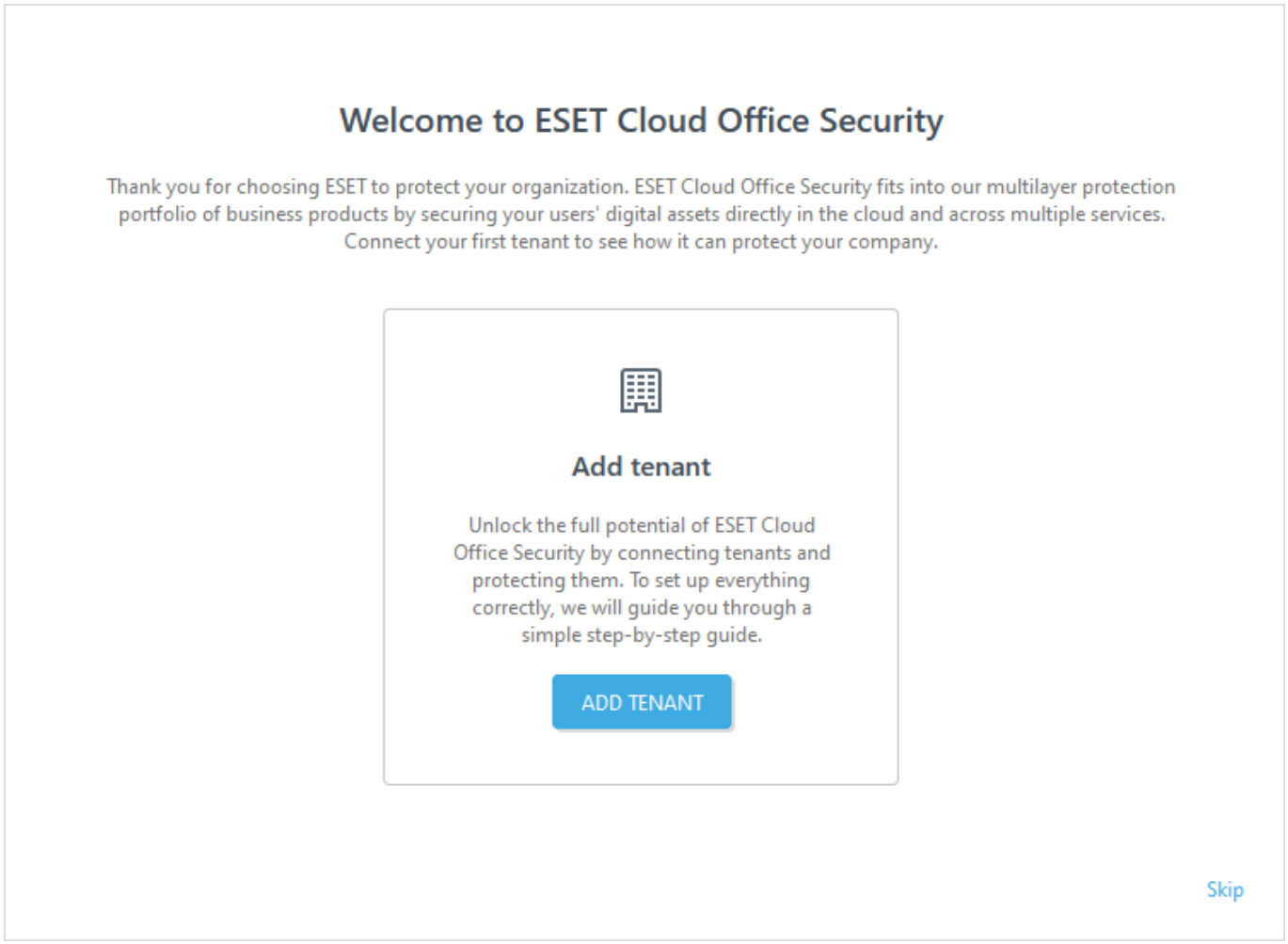
Ak sa zobrazuje žlté tlačidlo, môžete svoj súhlas obnoviť. Obnovenie súhlasu pre existujúceho nájomníka rozširuje oprávnenia ESET Cloud Office Security na váš účet Microsoft 365 a umožňuje funkciu, ktorá poskytuje informácie o type používateľa. Typ používateľa je definovaný v Azure Active Directory a zobrazí sa v časti Používatelia v príslušnom stĺpci. Ak chcete napríklad zobraziť len zdieľané e-mailové schránky, môžete používateľov Microsoft 365 filtrovať na základe ich typu.

Kliknite na tlačidlo **Obnoviť** pre každého nájomníka, ktorému chcete túto funkciu zapnúť. Aktualizácia typu používateľa z Azure AD môže trvať až 24 hodín.

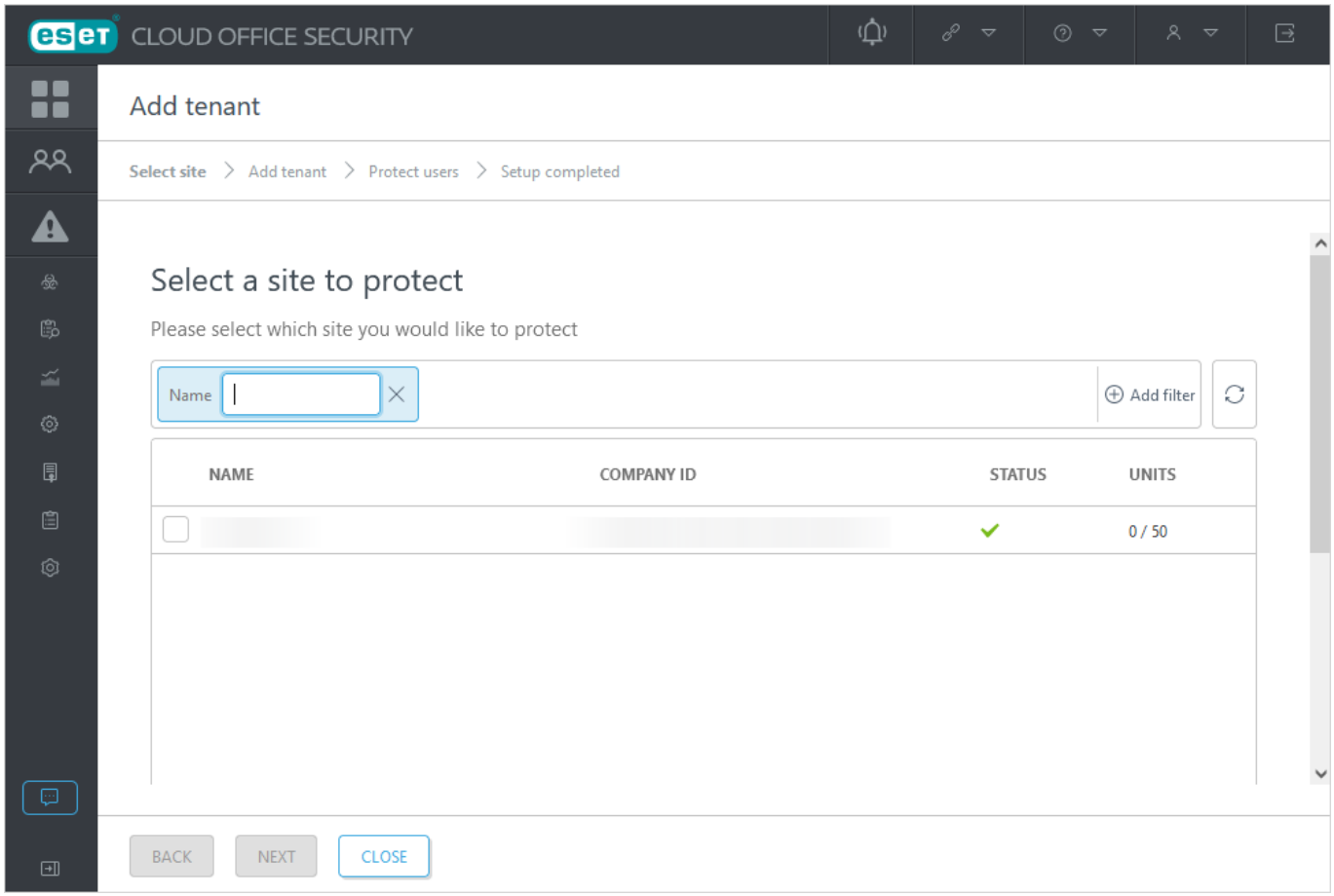
Ak sa zobrazuje červené tlačidlo, súhlas bol odvolaný alebo bola vykonaná iná zmena, ktorá ovplyvnila integráciu nájomníka s produktom ESET Cloud Office Security. Ak chcete aj naďalej chrániť používateľov, kliknite na tlačidlo **Aktualizovať**.

Pridanie nájomníka

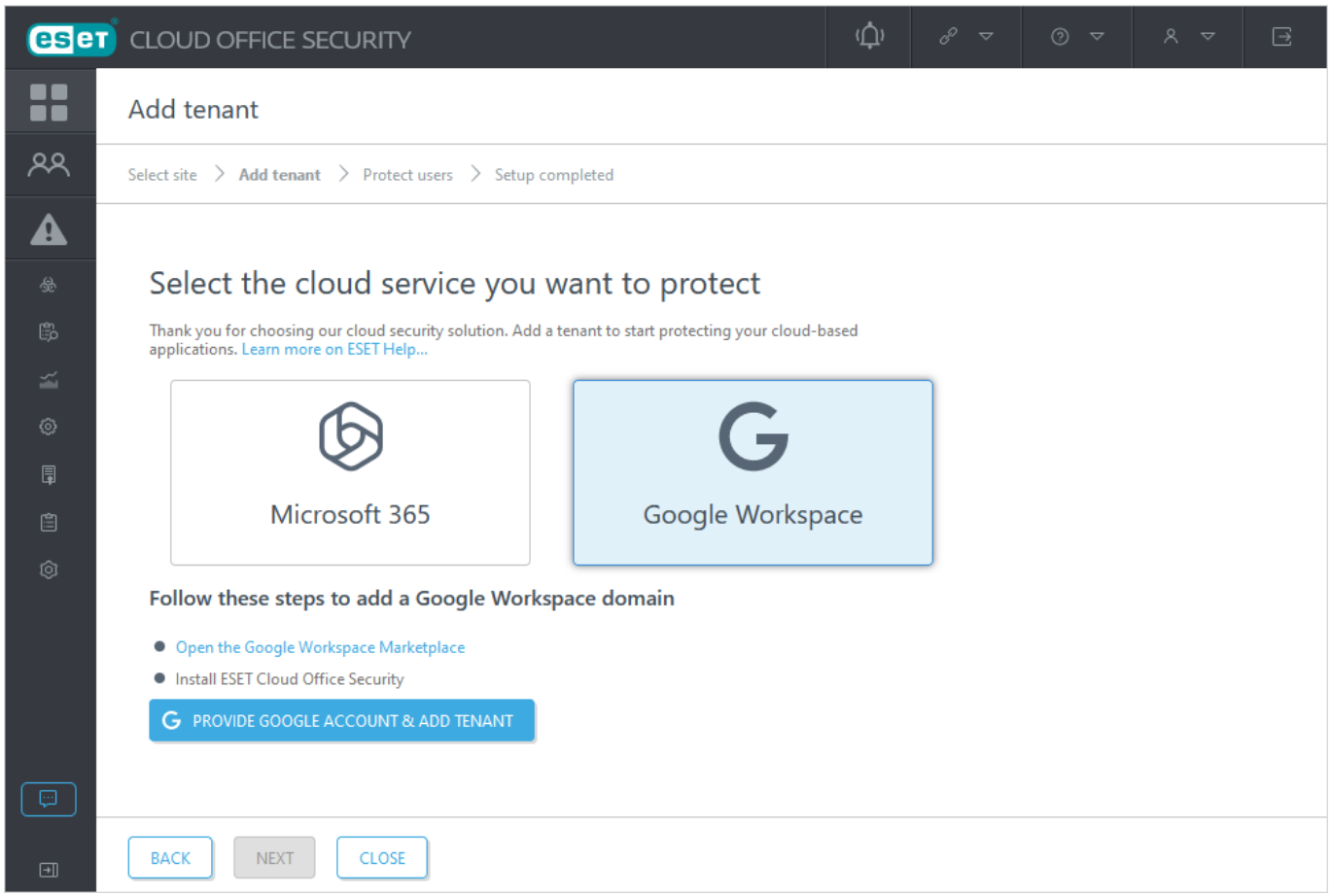
Na ochranu svojej cloudovej platformy kliknite na **Pridať nájomníka** a pripojte Microsoft 365 alebo Google Workspace k produktu ESET Cloud Office Security.



V okne **Vyberte lokalitu, ktorú chcete chrániť** by sa mal zobraziť zoznam dostupných lokalít. Označte políčko pri lokalite, ktorú chcete priradiť k nájomníkovi, a kliknite na tlačidlo **Ďalej**.



V okne **Vyberte cloudovú službu, ktorú chcete chrániť** kliknite na dlaždicu Microsoft 365 alebo Google Workspace a postupujte podľa uvedených bodov:



Nájomník Microsoft 365

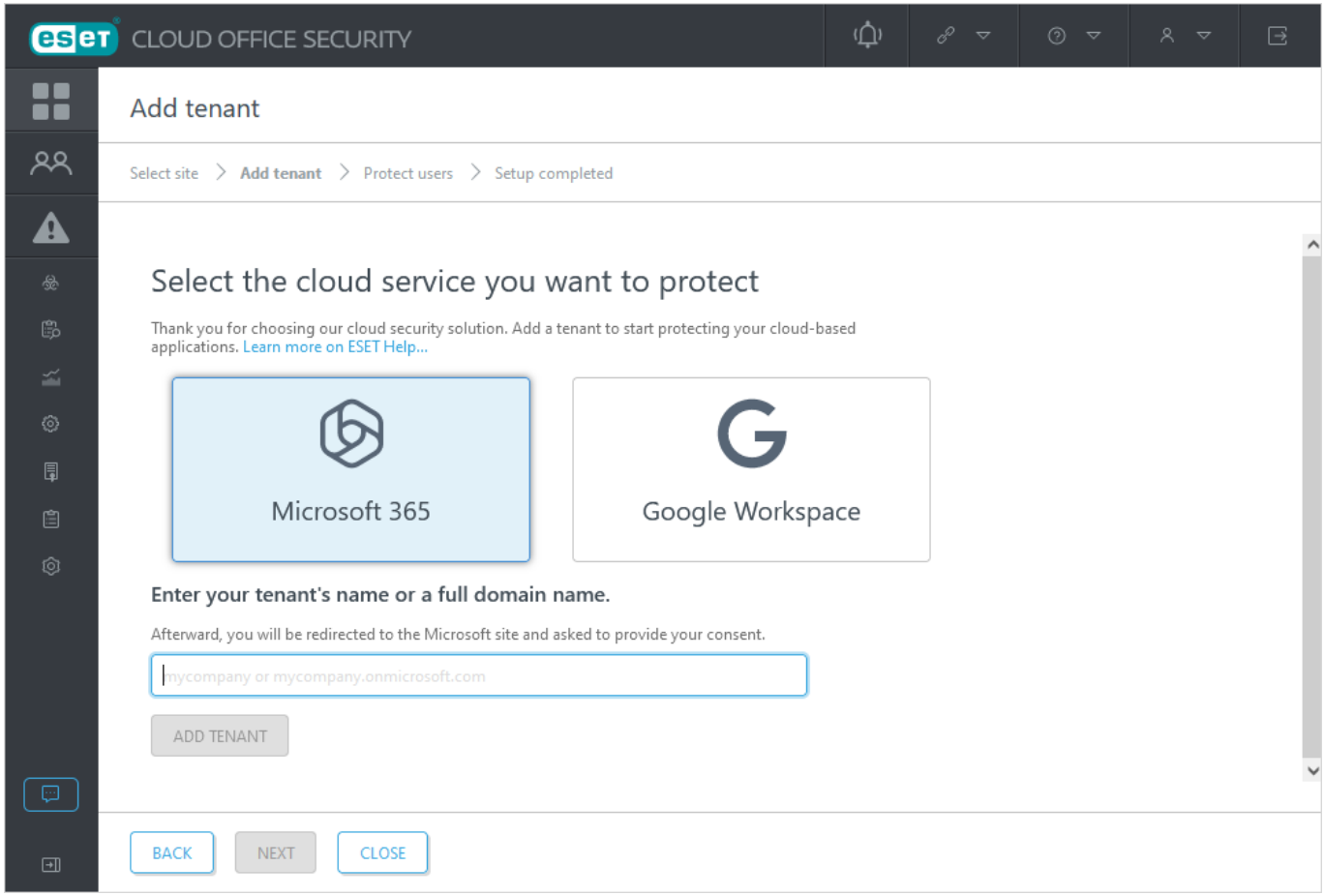
Active Directory (Azure AD) organizuje objekty, ako sú používatelia a aplikácie, do skupín, ktoré sa nazývajú nájomníci. Bežný spôsob identifikácie nájomníka je použitie názvu domény. Ak viacerí používatelia majú spoločný názov domény, títo používatelia patria pod rovnakého nájomníka. Prostredníctvom nájomníkov môžete nastaviť politiky pre používateľov a aplikácie vo vašej organizácii s cieľom splniť bezpečnostné a prevádzkové požiadavky. Prostredníctvom jednej konzoly ESET Cloud Office Security môžete chrániť a spravovať viacerých nájomníkov Microsoft 365.

Viac informácií o nájomníkoch v prostredí Azure Active Directory nájdete v článku spoločnosti Microsoft.

Pridanie nájomníka

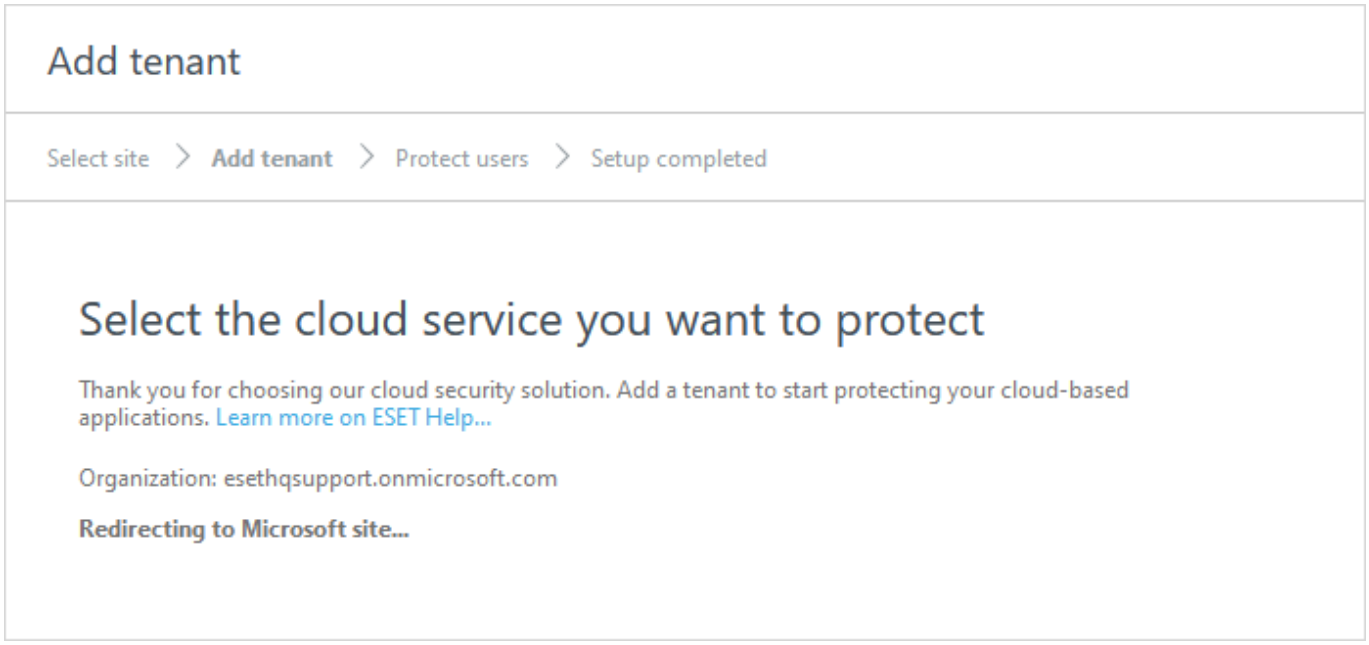
1. Prejdite do časti **Nastavenia** a kliknite na **Pridať nájomníka** (alebo kdekoľvek uvidíte tlačidlo **Pridať nájomníka**).

2. Kliknite na dlaždicu **Microsoft 365**.

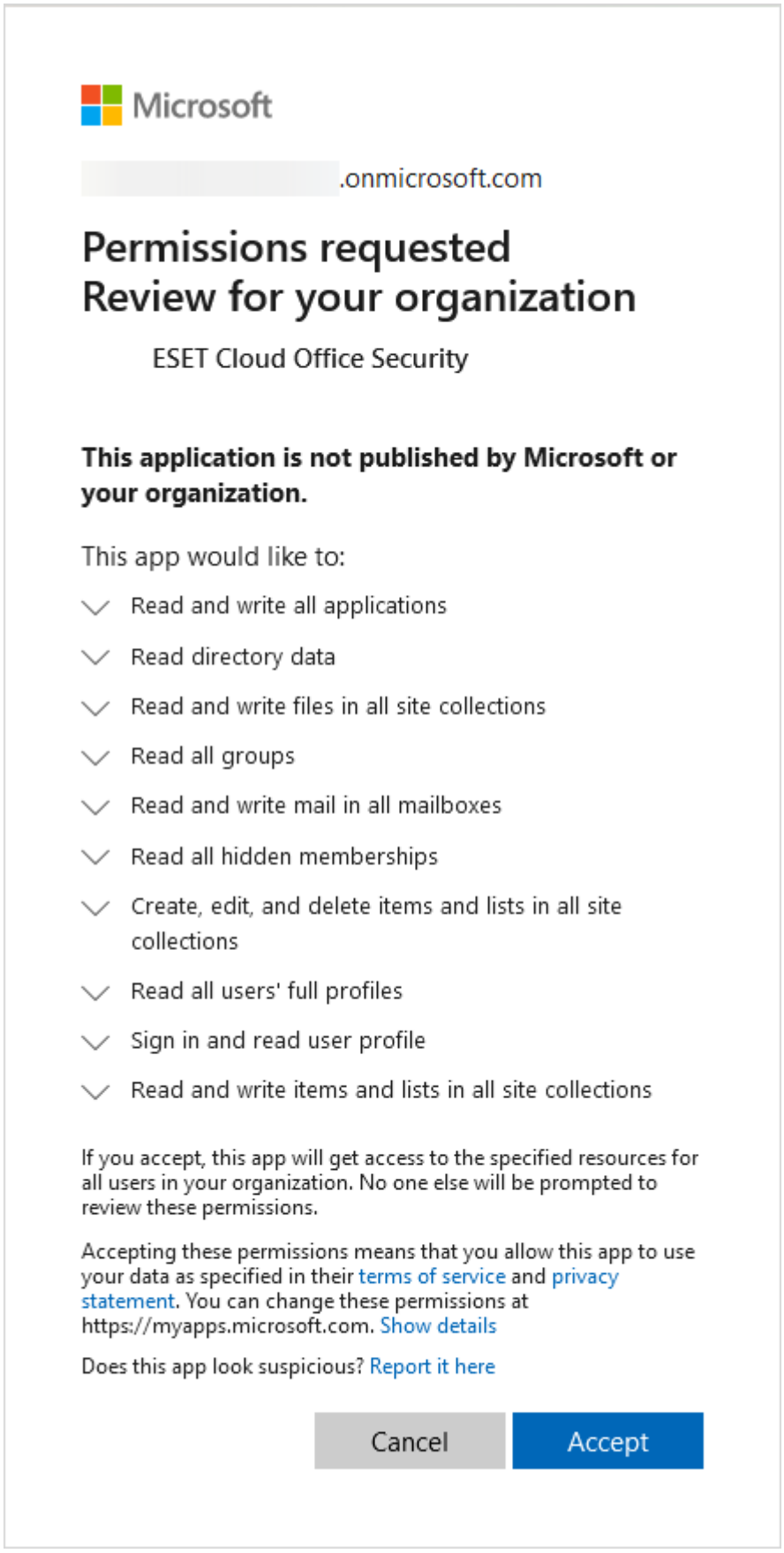


3. Zadajte meno nájomníka Microsoft 365 alebo úplný názov domény a kliknite na **Pridať nájomníka**.

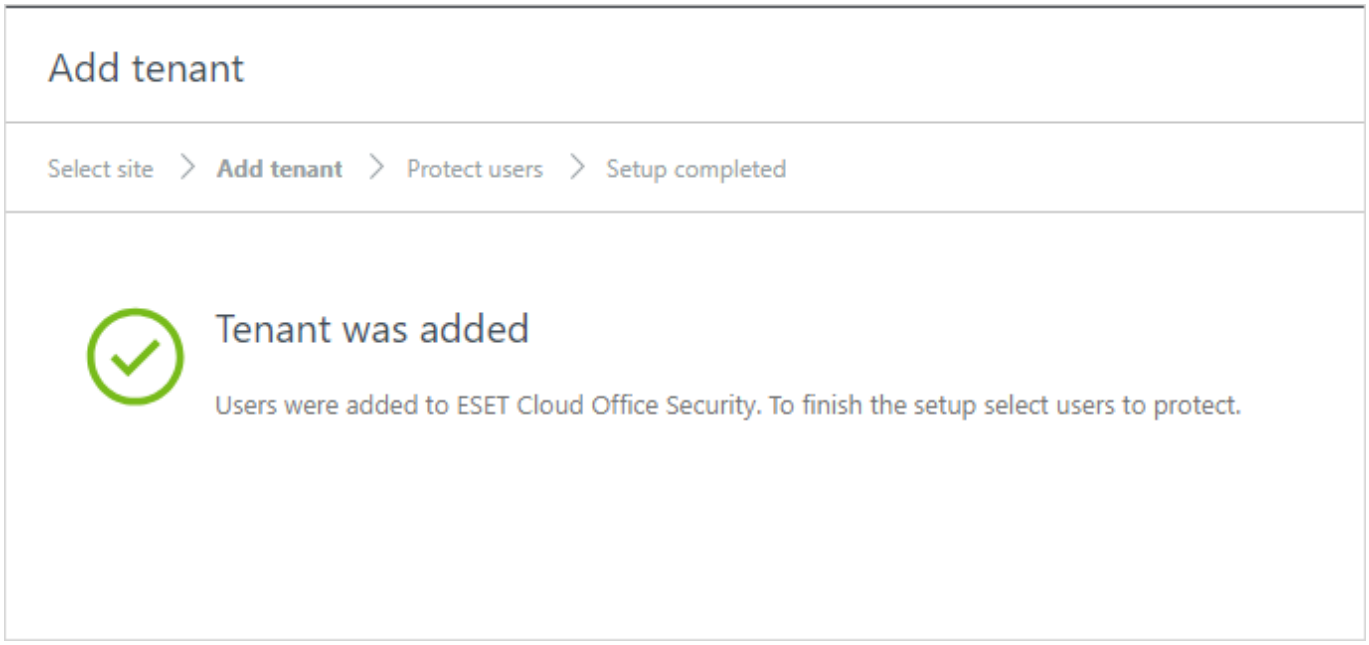
4. Budete presmerovaný na stránku spoločnosti Microsoft, kde nájdete zoznam povolení, ktoré vyžaduje ESET Cloud Office Security.



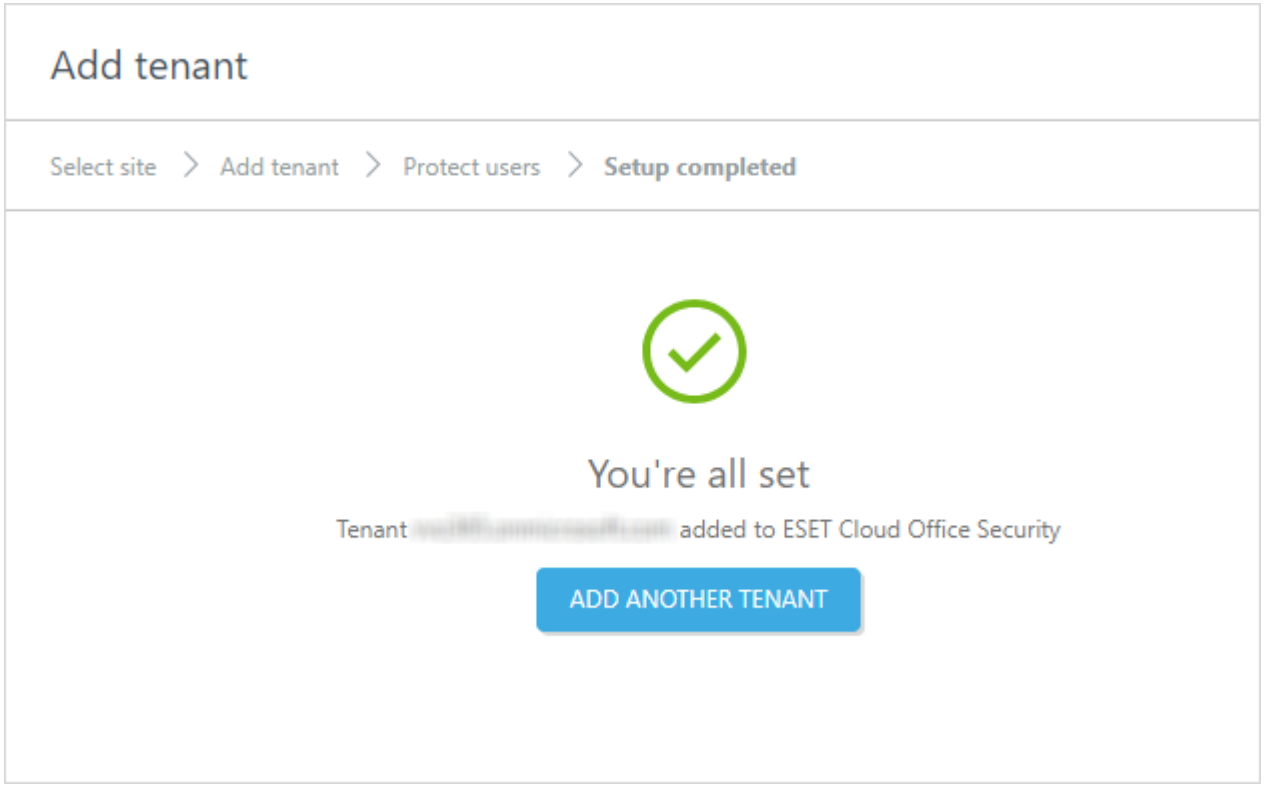
5. Ak chcete udeliť aplikácii ESET Cloud Office Security prístup k údajom nachádzajúcim sa vo vašom účte Microsoft, zadajte prihlasovacie údaje k svojmu správcovskému účtu Microsoft 365 a kliknite na **Prijať**.



6. Nájomník Microsoft 365 bol pridaný, a to vrátane používateľov.



7. Na dokončenie nastavenia kliknite na tlačidlo **Ďalej** a vyberte používateľov, ktorých chcete **chrániť**.



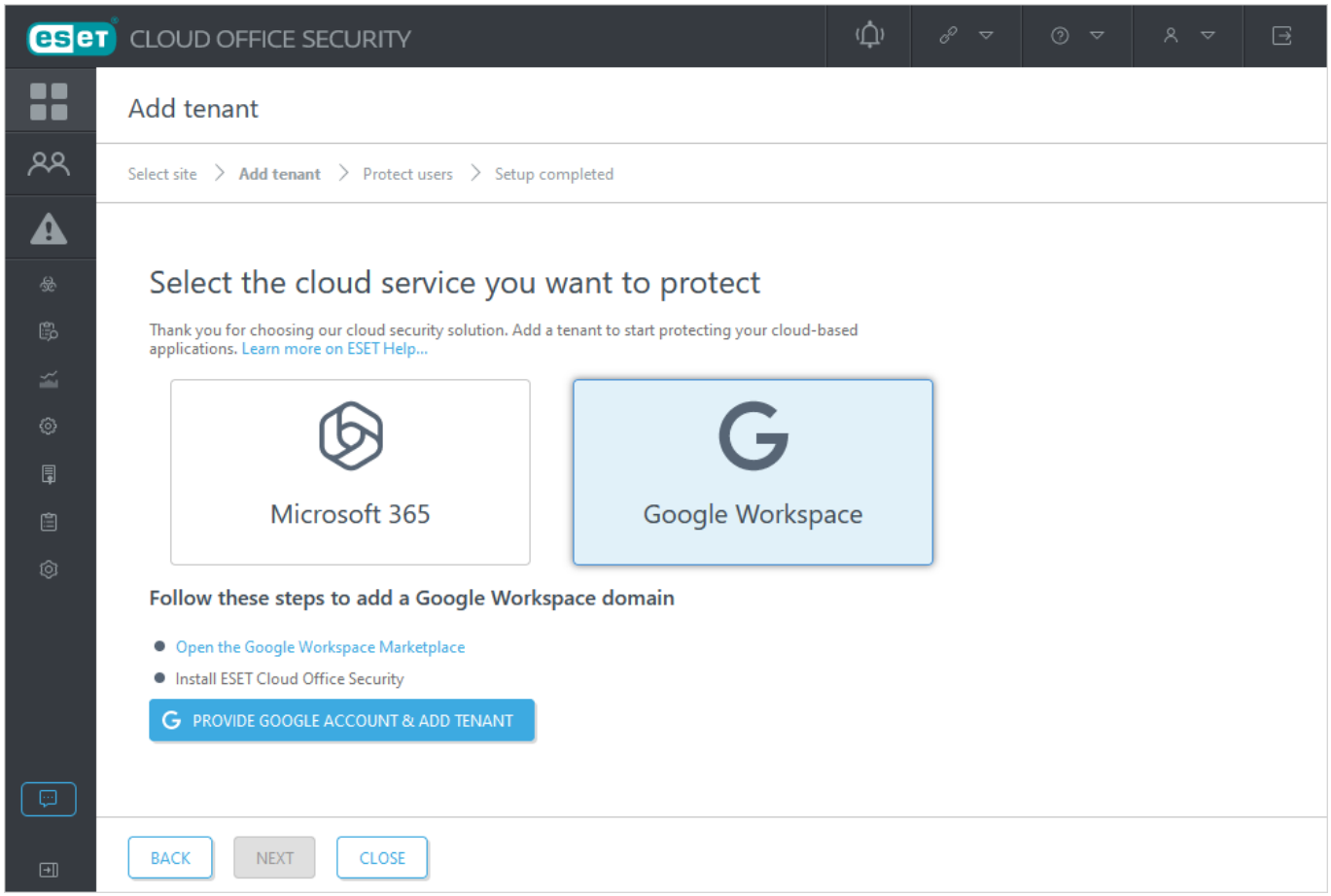
Nájomník Google Workspace

Integrujte nájomníka Google Workspace s produktom ESET Cloud Office Security s cieľom chrániť používateľov služby Google Workspace.

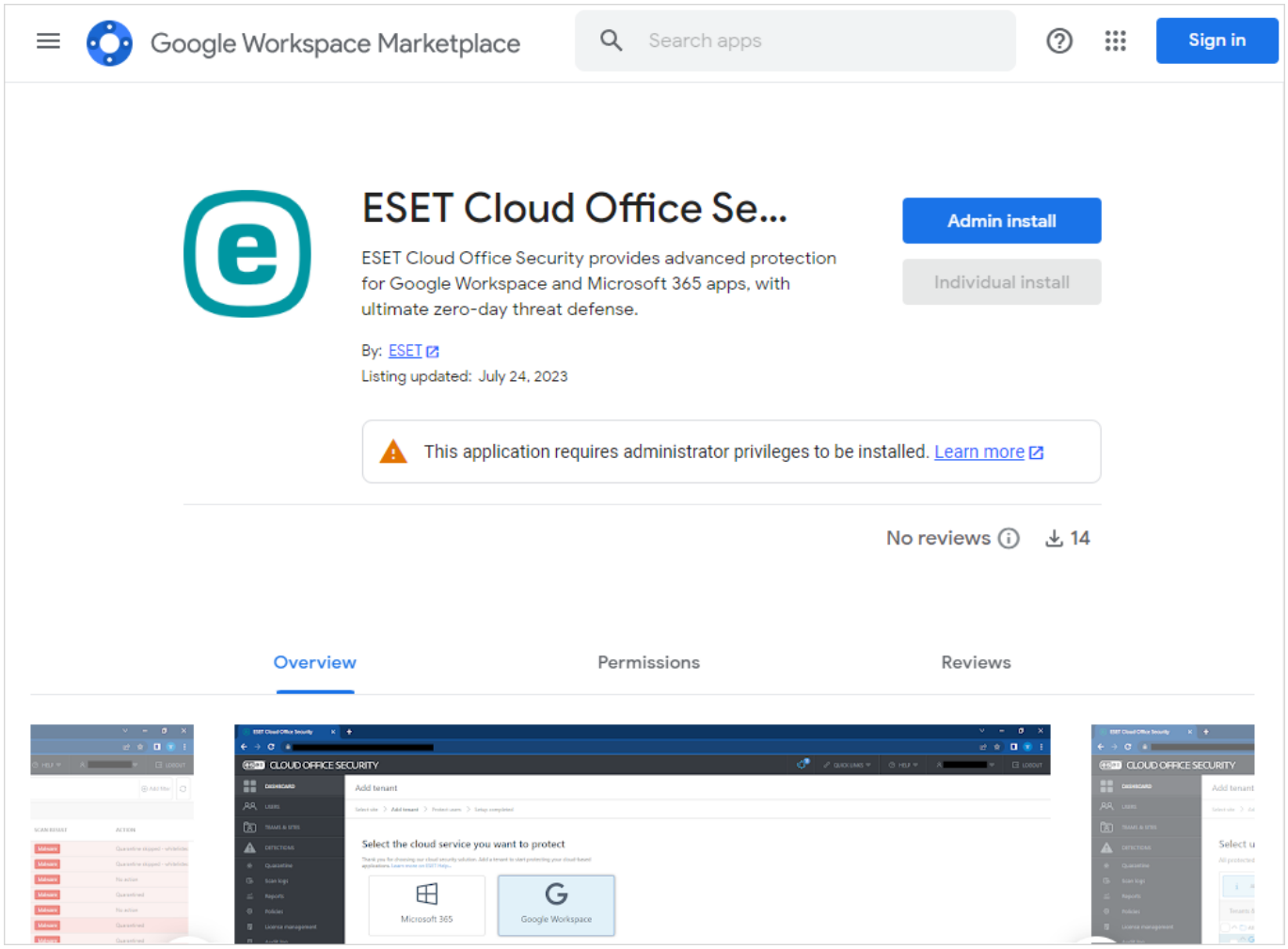
Pridanie nájomníka

1. Prejdite do časti **Nastavenia** a kliknite na **Pridať nájomníka** (alebo kdekoľvek uvidíte tlačidlo **Pridať nájomníka**).

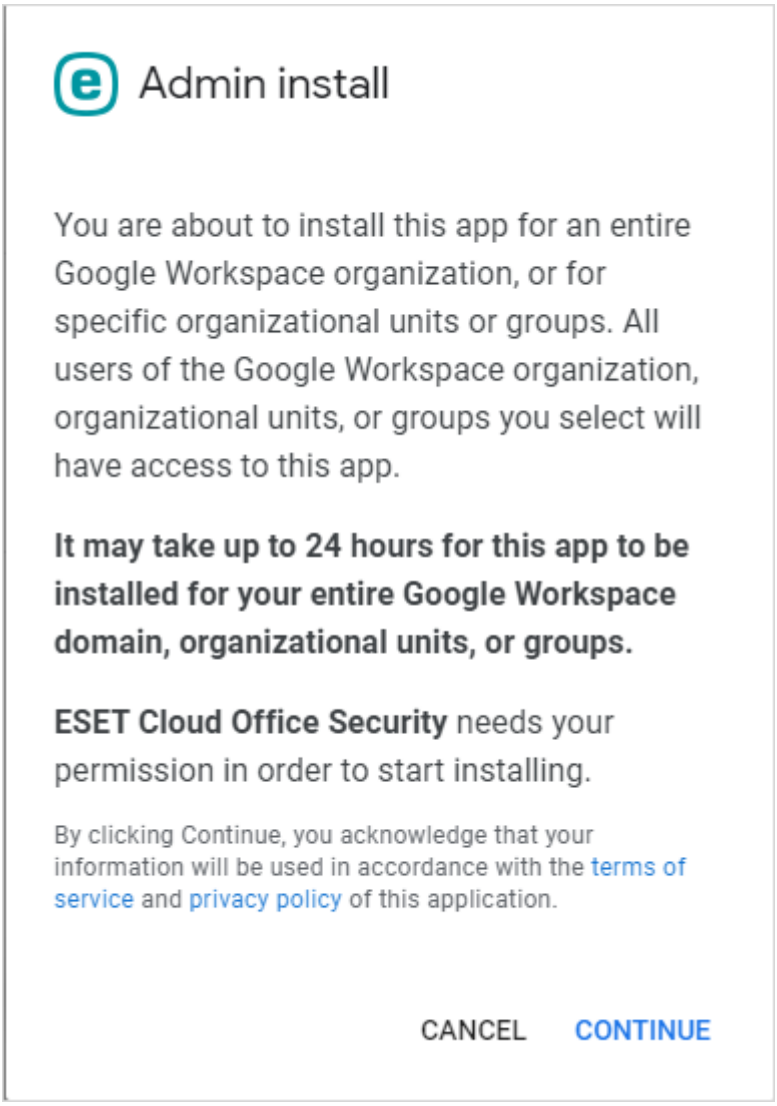
2. Kliknite na dlaždicu **Google Workspace**.



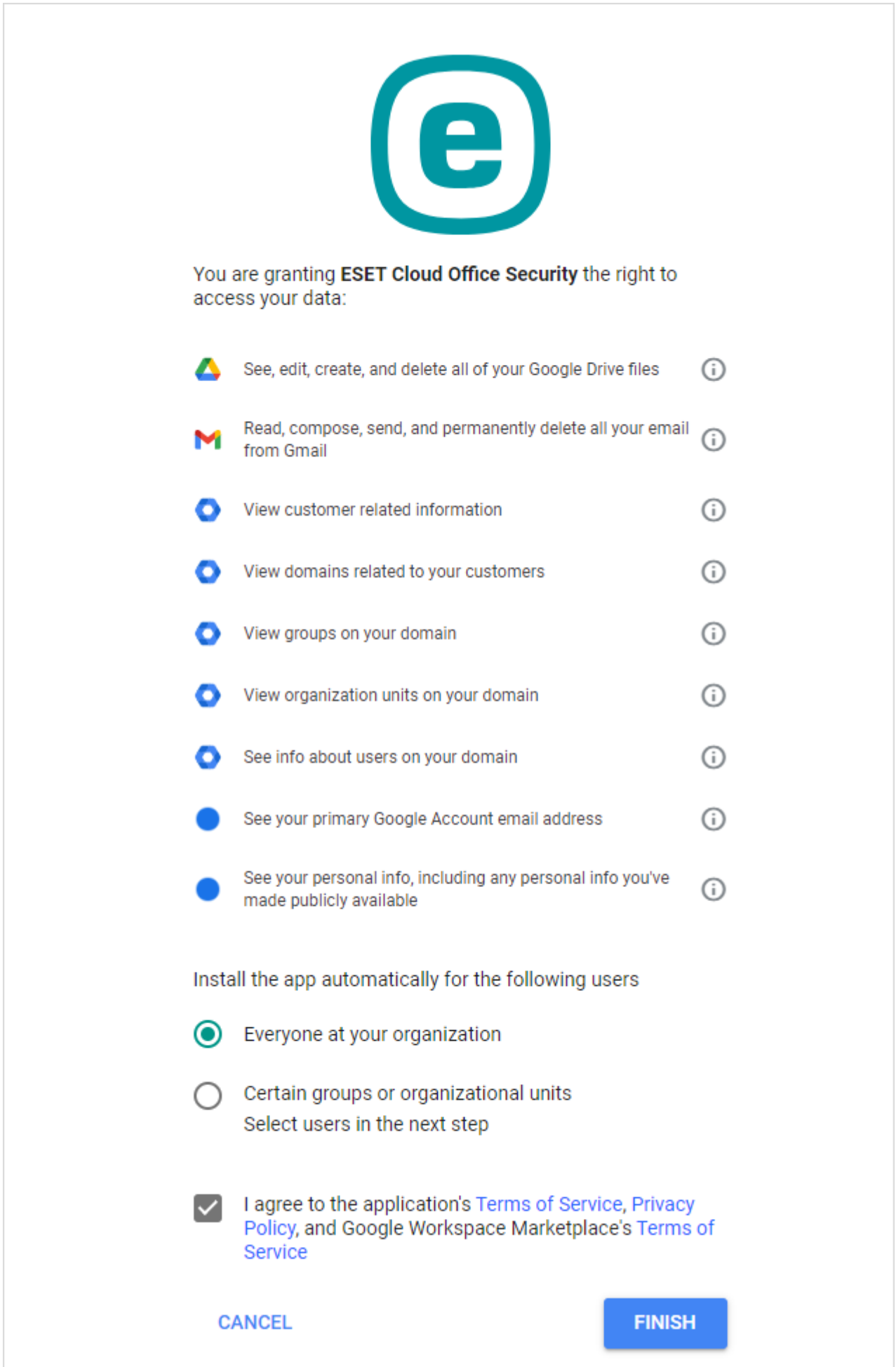
3. Otvorte Google Workspace Marketplace a nainštalujte aplikáciu ESET Cloud Office Security prostredníctvom účtu správcu. Aplikácia ESET Cloud Office Security je v súčasnosti dostupná len v obchode Google Workspace Marketplace cez priamy odkaz uvedený v tomto sprievodcovi.



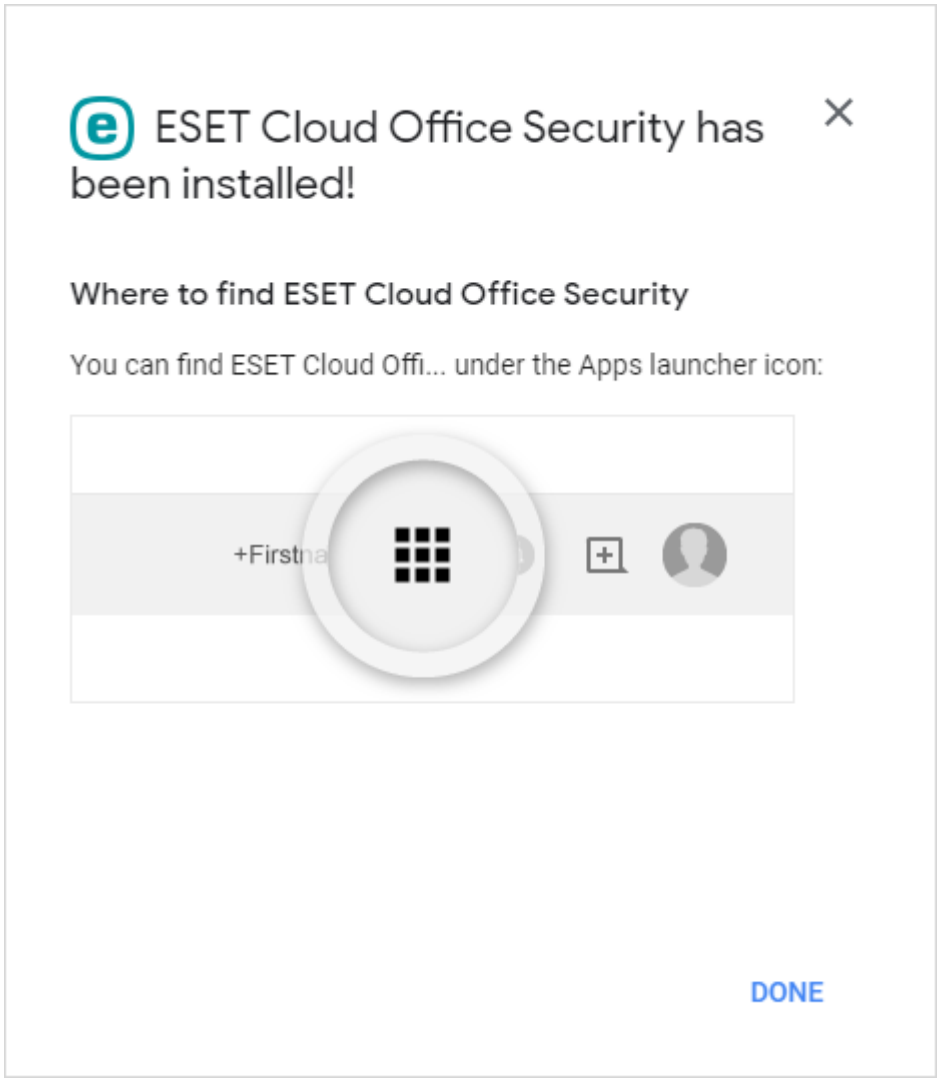
4. Na obrazovke **Admin install** (Inštalácia správcu) kliknite na tlačidlo **Continue** (Pokračovať).



5. Uistite sa, že na obrazovke s prístupovými právami je vybratá možnosť **Everyone at your organization** (Všetci vo vašej organizácii). Pred kliknutím na tlačidlo **Finish** (Dokončiť) by ste mali začiarknuť aj políčko s podmienkami poskytovania služieb a zásadami ochrany osobných údajov.

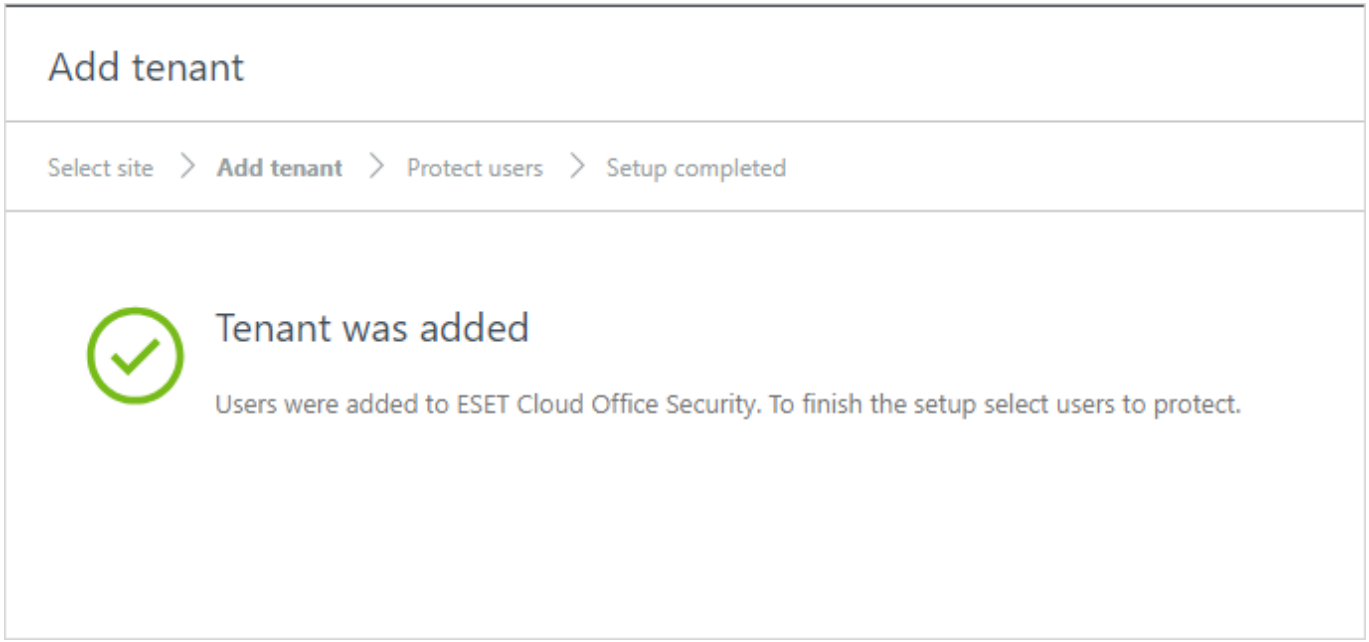

You are granting **ESET Cloud Office Security** the right to access your data:
See, edit, create, and delete all of your Google Drive files
Read, compose, send, and permanently delete all your email from Gmail
View customer related information
View domains related to your customers
View groups on your domain
View organization units on your domain
See info about users on your domain
See your primary Google Account email address
See your personal info, including any personal info you've made publicly available
Install the app automatically for the following users
Everyone at your organization
Certain groups or organizational units
Select users in the next step
I agree to the application's Terms of Service, Privacy Policy, and Google Workspace Marketplace's Terms of Service
CANCEL
FINISH

6. Aplikácia ESET Cloud Office Security je nainštalovaná, kliknite na tlačidlo **Done** (Hotovo).

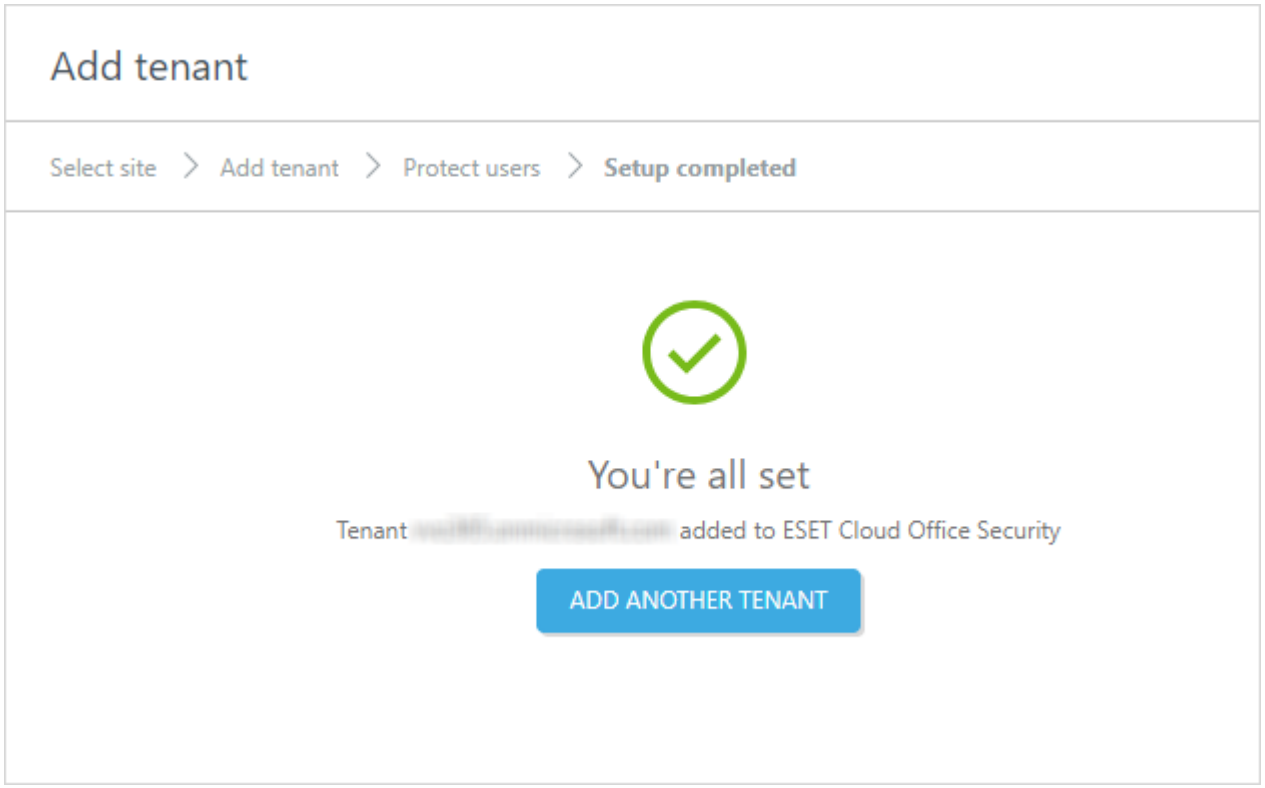


7. Po nainštalovaní aplikácie ESET Cloud Office Security prejdite späť do konzoly ESET Cloud Office Security. Kliknutím na možnosť **Poskytnúť účet Google a pridať nájomníka** overte vlastníctvo a pokračujte.

8. Nájomník Google Workspace bol pridaný, a to vrátane používateľov.



9. Na dokončenie nastavenia kliknite na tlačidlo **Ďalej** a vyberte používateľov, ktorých chcete **chrániť**. Potom už je všetko hotové.

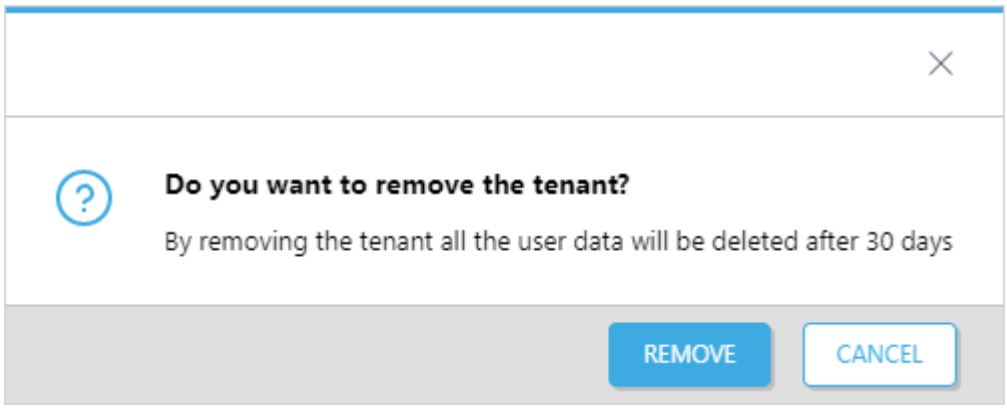


Odstránenie nájomníka z konzoly ESET Cloud Office Security

1. Vyberte **Nastavenia**.

2. Zvoľte požadovaného nájomníka a kliknite na **Odstrániť**.

3. Zobrazí sa okno s upozornením, že dôjde k odstráneniu údajov, ako je opísané v kapitole Obmedzenia a politika uchovávania údajov, a používatelia už nebudú chránení. Kliknutím na **Odstrániť** akciu potvrďte.



Po odstránení nájomníka z konzoly ESET Cloud Office Security sa údaje nájomníka uchovávajú ešte 30 dní (karanténa, protokoly kontroly a štatistiky sa odstránia po 30 dňoch). Ak nájomníka do 30 dní znova pridáte, všetky údaje sa obnovia. Ostatné objekty (nájomníci, používatelia, skupiny, lokality, reporty, politiky) sa po 90 dňoch natrvalo odstránia. Viac informácií nájdete v kapitole Obmedzenia a politika uchovávania údajov.

Odstránenie ESET Cloud Office Security z portálu Azure

1. Prihláste sa do portálu Azure pomocou správcovského účtu.

Na odstránenie aplikácie musíte byť uvedený ako vlastník aplikácie, prípadne mať oprávnenia správcu.

2. Prejdite na službu **Azure Active Directory** a vyberte možnosť **Enterprise applications**.

3. Vyhľadajte a kliknite na aplikáciu **ESET Cloud Office Security** na stránke Overview, prejdite do časti **Properties** a kliknite na **Delete**.

Orientácia v ESET Cloud Office Security

Pozrite sa, ako sa orientovať v rozhraní ESET Cloud Office Security. Zoznámte sa s navigačnými prvkami a nástrojmi produktu ESET Cloud Office Security, ktoré cielia na jednoduché, intuitívne a interaktívne používanie.

Navigačné menu na ľavej strane slúži na prepínanie medzi rôznymi časťami konzoly ESET Cloud Office Security:

- Používatelia
- Tímy a lokality
- Detekcie
- Karanténa
- Protokoly kontroly
- Reporty
- Politiky
- Správa licencií
- Protokol auditu
- Nastavenia

Zbaliť – táto funkcia slúži na rozbalenie a zbalenie navigačného menu. Zbalenie navigačného menu vám poskytne viac priestoru na obrazovke riadiaceho panela. Ak chcete rozbaliť navigačné menu, kliknite na ikonu .

Panel s nástrojmi v hornej časti produktu je vždy dostupný:



Navigátor produktov – poskytuje rýchly prístup ku konzolám ESET a ďalším užitočným odkazom. (Príslušné produkty môžete vidieť na základe svojej licencie a prístupových práv).

ESET Business Account a **ESET MSP Administrator** (hybridný licenčný účet) – ak máte zaregistrovanú rovnakú e-mailovú adresu na portáli ESET MSP Administrator aj ESET Business Account (jednotné prihlásenie), môžete prepínať medzi zobrazením ESET Business Account a ESET MSP Administrator.

Zobraziť oznámenia – kliknutím na ikonu zvončeka v pravom hornom rohu zobrazíte všetky oznámenia.

Rýchle odkazy – poskytujú jednoduchý prístup k nasledujúcim možnostiam: Pridať nájomníka, Nová politika, ESET Business Account alebo ESET MSP Administrator.

Pomoc – po kliknutí na prvý odkaz v tejto ponuke sa vždy zobrazí kapitola Online pomocníka, ktorá popisuje aktuálne prehliadanú časť produktu. V prípade, že problém neviete vyriešiť, vyhľadajte informácie o danom probléme v Databáze znalostí spoločnosti ESET alebo navštívte Fórum technickej podpory. Môžete tiež použiť možnosť Odoslať spätnú väzbu alebo **Poslať vzorku na analýzu**. Sekcia O aplikácii obsahuje podrobné informácie o verzii produktu ESET Cloud Office Security, ako aj odkazy na právne dokumenty.

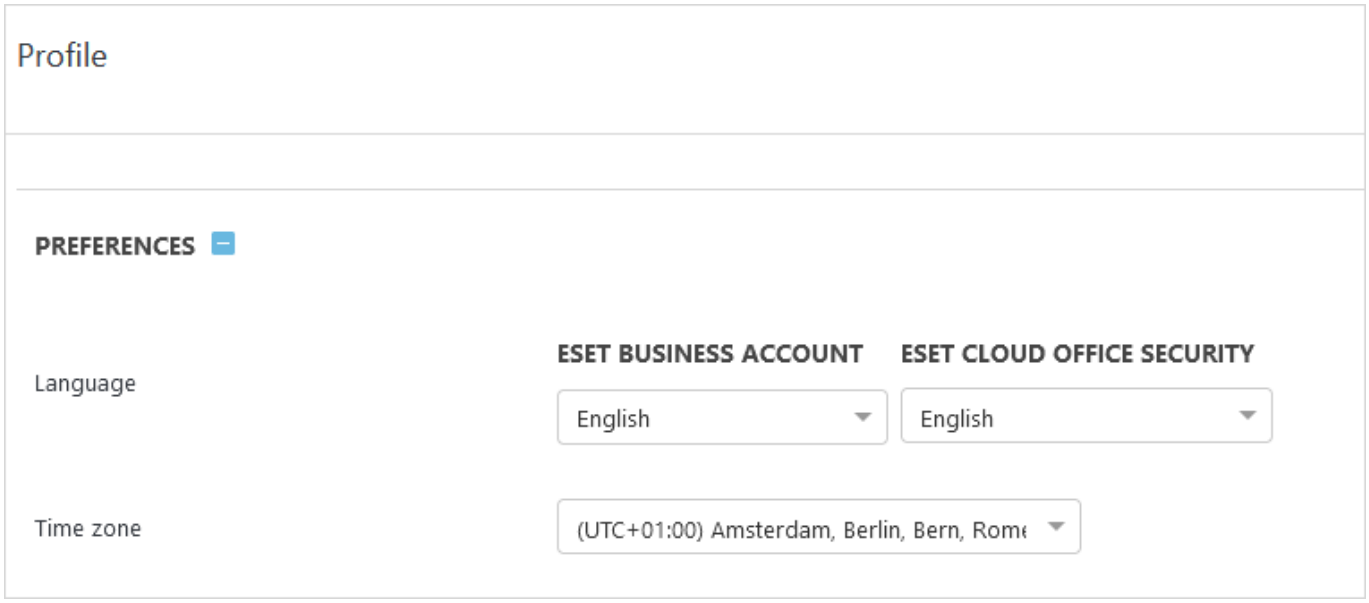
Používateľ (aktuálne prihlásený) – zobrazuje prihlasovacie meno používateľa. Kliknite na položku **Nastaviť motív** a vyberte požadovaný režim z roletového menu:

- **Predvolený (svetlý) motív** – ESET Cloud Office Security sa bude zobrazovať v svetlom motíve (predvolený režim).
- **Tmavý motív** – ESET Cloud Office Security sa bude zobrazovať v tmavom motíve (tmavý režim).
- **Motív operačného systému** – ESET Cloud Office Security sa bude zobrazovať v motíve nastavenom pre operačný systém.

Odhlásenie – kliknutím na túto ikonu sa odhlásite z konzoly ESET Cloud Office Security.

Zmena jazyka portálu ESET Cloud Office Security

Prihláste sa do portálu ESET Business Account alebo ESET MSP Administrator, prejdite do sekcie **Správa používateľov**, vyberte používateľa a kliknite na **Upraviť**. Vyhľadajte nastavenia jazyka pre ESET Cloud Office Security, zmeňte jazyk podľa potreby a pred opustením obrazovky **Profil** kliknite na **Uložiť**.



ESET LiveGuard Advanced

ESET LiveGuard Advanced poskytuje dodatočnú vrstvu zabezpečenia prostredníctvom pokročilej cloudovej technológie ESET umožňujúcej detekciu nových, dosiaľ neznámych druhov hrozieb. ESET LiveGuard Advanced sa postará o vašu ochranu pred novými typmi hrozieb a neblahými následkami, ktoré by mohli spôsobiť. V prípade, že ESET LiveGuard Advanced identifikuje podozrivý kód alebo správanie konkrétneho objektu, zabráni ďalšej nebezpečnej aktivite tým, že daný objekt dočasne presunie do karantény.

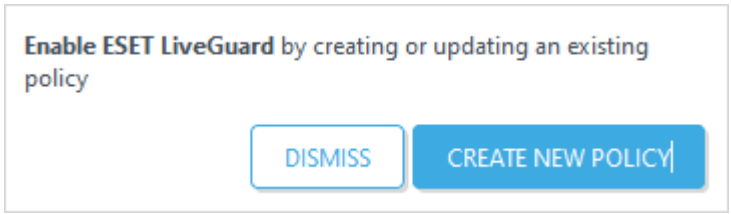
Podozrivá vzorka (súbor alebo e-mailová správa) je zároveň automaticky odoslaná do cloudu ESET, kde server ESET LiveGuard Advanced vykoná jej analýzu pomocou pokročilých techník detekcie. Kým sú podozrivé súbory alebo e-maily uložené v karanténe, ESET Cloud Office Security čaká na výsledky analýzy zo servera ESET LiveGuard Advanced.

Po vykonaní analýzy váš produkt ESET Cloud Office Security dostane správu obsahujúcu súhrn zistení o aktivite danej vzorky. Ak sa ukáže, že vzorka nie je nijakým spôsobom škodlivá, dôjde k jej uvoľneniu z karantény. V opačnom prípade bude v karanténe ponechaná.

Čo sa týka e-mailových správ, server ESET LiveGuard Advanced zvyčajne odošle výsledky analýzy vzoriek po niekoľkých minútach. Predvolená doba čakania je však nastavená na 5 minút. V ojedinelých prípadoch sa môže stať, že výsledky z ESET LiveGuard Advanced nie sú doručené v rámci stanoveného intervalu. V takomto prípade je správa uvoľnená z karantény. Predvolený interval je možné zmeniť podľa potreby v rozmedzí od 5 do 60 minút, pričom minimálna hodnota, s ktorou je možné pracovať, je 1 minúta.

V rámci licencie ESET Cloud Office Security môžete využívať funkciu ESET LiveGuard Advanced bez akýchkoľvek ďalších poplatkov. V sekcii Správa licencií budete vidieť označenie ELG vedľa ID licencie.

V malom dialógovom okne, ktoré sa zobrazí, máte možnosť aktivovať funkciu ESET LiveGuard Advanced vytvorením novej politiky alebo upravením už existujúcej politiky.



Podrobnejšie informácie o ESET LiveGuard Advanced nájdete v kapitole Ako fungujú detekčné vrstvy ESET LiveGuard Advanced.

Riadiaci panel

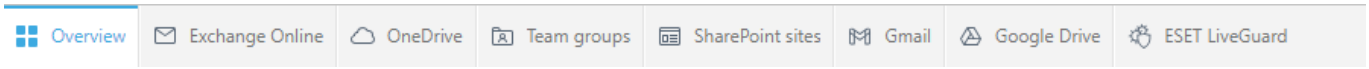
Riadiaci panel je súbor ovládacích prvkov, ktoré poskytujú prehľad o bezpečnostných činnostiach v rámci Microsoft 365. Každá karta riadiaceho panela (Prehľad, Exchange Online, OneDrive, Tímové skupiny, Lokality SharePoint, Gmail, Disk Google a ESET LiveGuard Advanced) obsahuje užitočné informácie. Sekcia **Prehľad** je hlavná obrazovka riadiaceho panela, ktorá sa zobrazí po každom prihlásení sa do konzoly ESET Cloud Office Security. Zobrazuje všeobecné a štatistické informácie.

> Dáta zobrazené v riadiacom paneli sa obnovujú každých 10 minút. Ak sa vám nezobrazujú najnovšie informácie, stlačením klávesu **F5** vynútite manuálne obnovenie.

Ak chcete zobraziť štatistiky, použite filtre v hornej časti riadiaceho panelu a vyberte príslušné **Časové obdobie** (posledných 24 hodín, posledných 7, 30 alebo 90 dní) a **Nájomníka**. Ďalšie štatistiky detekcie a grafy sú zobrazené na kartách určených pre **Exchange Online**, **OneDrive**, **Tímové skupiny**, **Lokality SharePoint**, **Gmail**, **Disk Google** a **ESET LiveGuard Advanced**. Ide o štatistické informácie, ako napr. počet skontrolovaných e-mailov a súborov alebo počet zachyteného spamu/phishingu/malvéru. Grafy zobrazujú frekvenciu výskytu pre každý typ detekcie – spam, malvér a phishing.

V niektorých situáciách sa môže zobraziť panel s oznámeniami. Farby označujú typ oznámenia (modrá = novinky, žltá = povedomie, červená = upozornenie).

Na prepínanie medzi jednotlivými zobrazeniami môžete použiť karty riadiaceho panela.



Prehľad

Zobrazuje:
- Počet nájomníkov a využitie licencie.
- Štatistiky pre každého nájomníka:
  - Celkový počet používateľov/Nechránení používatelia
  - Najčastejší príjemcovia spamu/phishingu/malvéru
  - Najčastejšie podozrivé OneDrive účty
  - Najčastejšie podozrivé tímové skupiny
  - Najčastejšie podozrivé lokality SharePoint

Zobrazenie podrobností:
- Kliknutím na dlaždicu Celkový počet používateľov otvoríte sekciu Používatelia.
- Kliknutím na používateľa v sekcii štatistík (spam/phishing/malvér/OneDrive) zobrazíte príslušné detekcie.

Kliknutím na skupinu alebo lokalitu zobrazíte detekcie a ďalšie podrobnosti o podozrivej tímovej skupine alebo lokalite SharePoint.

Exchange Online

Zobrazuje:
- Celkový počet skontrolovaných e-mailov.
- Štatistiky zachyteného spamu, malvéru a phishingových e-mailov.
- Grafy, z ktorých každý znázorňuje výskyt spamu, malvéru a phishingu.

Dlaždice sú interaktívne. Kliknite na požadovanú dlaždicu a prejdite na príslušnú sekciu v rámci konzoly ESET Cloud Office Security. Otvorí sa napríklad sekcia Protokoly kontroly s príslušnými záznamami.

OneDrive

Zobrazuje:
- Počet chránených používateľov.
- Celkový počet skontrolovaných súborov.
- Štatistiky zachyteného malvéru.
- Graf, ktorý znázorňuje výskyt malvéru.

Dlaždice sú interaktívne. Kliknite na požadovanú dlaždicu a prejdite na príslušnú sekciu v rámci konzoly ESET Cloud Office Security. Otvorí sa napríklad sekcia Protokoly kontroly s príslušnými záznamami.

Tímové skupiny

Zobrazuje:
- Počet chránených skupín.
- Celkový počet skontrolovaných súborov.
- Štatistiky zachyteného malvéru.
- Graf, ktorý znázorňuje výskyt malvéru.

Dlaždice sú interaktívne. Kliknite na požadovanú dlaždicu a prejdite na príslušnú sekciu v rámci konzoly ESET Cloud Office Security. Otvorí sa napríklad sekcia Protokoly kontroly s príslušnými záznamami.

Lokality SharePoint

Zobrazuje:
- Počet chránených lokalít.
- Celkový počet skontrolovaných súborov.
- Štatistiky zachyteného malvéru.
- Graf, ktorý znázorňuje výskyt malvéru.

Dlaždice sú interaktívne. Kliknite na požadovanú dlaždicu a prejdite na príslušnú sekciu v rámci konzoly ESET Cloud Office Security. Otvorí sa napríklad sekcia Protokoly kontroly s príslušnými záznamami.

Gmail

Zobrazuje:
- Celkový počet skontrolovaných e-mailov.
- Štatistiky zachyteného spamu, malvéru a phishingových e-mailov.
- Grafy, z ktorých každý znázorňuje výskyt spamu, malvéru a phishingu.

Dlaždice sú interaktívne. Kliknite na požadovanú dlaždicu a prejdite na príslušnú sekciu v rámci konzoly ESET Cloud Office Security. Otvorí sa napríklad sekcia Protokoly kontroly s príslušnými záznamami.

Google Drive

Zobrazuje:
- Počet chránených používateľov.
- Celkový počet skontrolovaných súborov.
- Štatistiky zachyteného malvéru.
- Graf, ktorý znázorňuje výskyt malvéru.

Dlaždice sú interaktívne. Kliknite na požadovanú dlaždicu a prejdite na príslušnú sekciu v rámci konzoly ESET Cloud Office Security. Otvorí sa napríklad sekcia Protokoly kontroly s príslušnými záznamami.

ESET LiveGuard Advanced

Zobrazuje:
- Odoslané súbory (počet zahŕňa duplikáty a počet môže byť vyšší ako počet jedinečných súborov).
- Počet detekcií.
- Priemerný čas analýzy.
- Graf, ktorý znázorňuje odoslané súbory.
- Najčastejší vlastníci odoslaných súborov.
- Typy odoslaných súborov.

Dlaždice sú interaktívne. Kliknite na požadovanú dlaždicu a prejdite na príslušnú sekciu v rámci konzoly ESET Cloud Office Security. Otvorí sa napríklad sekcia Protokoly kontroly s príslušnými záznamami.

Používatelia

Hlavným cieľom ochrany, ktorú ESET Cloud Office Security poskytuje, je používateľský účet. Dvojitým kliknutím na používateľa zobrazíte užitočné informácie, ako napr. prehľad, nastavenia definované politikami, zoznam politík priradených k používateľovi a detekcie súvisiace s Gmail, Google Drive, Exchange Online a OneDrive. Môžete si tiež vybrať, ktorí používatelia budú chránení alebo nechránení. Používatelia sú zoradení do skupín, pričom každá skupina je Microsoft 365 nájomník obsahujúci svojich používateľov. Na jednoduchšie vyhľadávanie konkrétnych používateľov v rámci skupiny môžete využiť filtrovanie s viacerými kritériami.

> Používatelia, ktorí nemajú licenciu Microsoft 365, nebudú predvolene zobrazení v konzole ESET Cloud Office Security. Toto sa vzťahuje aj na zdieľané e-mailové schránky bez licencie Microsoft 365.
> Ak chcete zobraziť a spravovať všetkých používateľov služieb Microsoft 365, prejdite do sekcie Nastavenia a vypnite možnosť Licencovaní používatelia služby Microsoft 365.

Stav ochrany:

Stav	Popis
Nechránené	Používateľ momentálne nie je chránený.
Automaticky chránené	Používateľ je chránený prostredníctvom automatickej ochrany.
Čaká sa	Prechodný stav, ktorý nastáva počas procesu ochrany používateľa. Po dokončení tohto procesu sa stav používateľa zmení na Chránené.
Chránené	E-mailová schránka a OneDrive používateľa sú chránené prednastavenou alebo vlastnou politikou.
Upozornenie	Proces ochrany používateľa bol neúspešný. Chyba sa môže týkať niektorého zo zdrojov – e-mailovej schránky alebo OneDrive. Pre používateľa pravdepodobne nie sú dostupné oba zdroje. Skontrolujte, či má používateľ pridelenú platnú licenciu Microsoft 365.

Na zobrazenie používateľov iba v rámci konkrétneho nájomníka alebo skupiny použite stromovú štruktúru. Ak chcete zobraziť všetkých používateľov pre každého nájomníka a skupinu, kliknite na **Všetko**.

Pre podrobnejšie informácie dvakrát kliknite na používateľa, kliknite na ikonu a vyberte príslušnú akciu (**Zobraziť podrobnosti**, **Ochrániť**, **Zrušiť ochranu**). Po kliknutí na používateľa môžete otvoriť okno **Zobraziť podrobnosti**, ktoré pozostáva zo štyroch častí:

Akcia	Použitie
Prehľad	Zobrazuje potrebné informácie o používateľovi, ktoré sú načítané z Microsoft 365 (e-mail, členstvo v skupine, pracovné zaradenie atď.). Zobrazený je tiež aktuálny stav ochrany pre e-mailovú schránku a OneDrive.

Akcia	Použitie
Konfigurácia	Obsahuje zoznam Nastavení s prístupom iba na čítanie a Politiky, ktoré sú priradené k danému používateľovi. Prepínaním medzi kartami si môžete zobraziť konfiguráciu alebo zoznam priradených politík. Ak chcete meniť nastavenia používateľov alebo k nim priraďovať politiky, je potrebné prejsť do sekcie Politiky.
Detekcie	Tu nájdete všetky detekcie pre daný používateľský účet (Gmail, Disk Google, Exchange Online alebo OneDrive).
Karanténa	Zobrazuje všetky e-maily a súbory, ktoré daný používateľ umiestnil do karantény. Pre objekty umiestnené v karanténe môžete vykonať nasledujúce akcie: Uvoľniť, Stiahnuť alebo Odstrániť.

Používateľov môžete filtrovať podľa niekoľkých kritérií. Kliknite na **Pridať filter** a z roletového menu vyberte typ filtra alebo zadajte reťazec, podľa ktorého chcete vyhľadávať (môžete tiež skombinovať viacero kritérií hľadania):

Pridať filter	Použitie
Stav ochrany	Vyberte niektorý z nasledujúcich stavov: Chránené, Nechránené, Upozornenie, Čaká sa.
Automaticky chránené	Zobraziť iba automaticky chránených používateľov.
Meno	Zadajte platné prihlasovacie meno.
E-mail	Zadajte platnú e-mailovú adresu používateľa.
Typ	Vyberte typ používateľa (Neznámy, Používateľ, Prepojený, Zdieľaná e-mailová schránka, Miestnosť, Zariadenie, Iné).

Ochrániť používateľov

1. Vyberte **používateľov**, ktorých chcete chrániť, a kliknite na **Ochrániť**.
2. Vyberte **licenčný fond** načítaný z portálu ESET Business Account a kliknite na **OK**. Vybraní používatelia sú teraz chránení prostredníctvom prednastavenej politiky.
3. V prípade potreby nastavte pre používateľov vlastnú politiku v sekcii Politiky.

Zrušiť ochranu používateľov

Vyberte **Používateľov**, ktorých nechcete chrániť, a kliknite na **Zrušiť ochranu**.

Tímy a lokality

ESET Cloud Office Security poskytuje ochranu pre tímové skupiny v službe Teams a lokality SharePoint.

Pomocou kariet môžete prepínať medzi Tímovými skupinami a Lokalitami SharePoint. Týmto si zobrazíte zoznam tímových skupín alebo lokalít SharePoint v rámci daného nájomníka.

Tímové skupiny

Na tejto karte sa zobrazujú objekty patriace danej skupine Microsoft 365 vrátane OneDrive a predvolenej tímovej lokality SharePoint:

- názov
- stav
- e-mail
- nájomník

Ak chcete chrániť tímové skupiny, uistite sa, že aspoň jeden člen je chránený produktom ESET Cloud Office Security. Každá skupina Microsoft 365 má predvolenú tímovú lokalitu SharePoint a OneDrive, ktoré sú tiež chránené:

Lokality SharePoint

Na tejto karte sa zobrazujú všetky koreňové lokality SharePoint, ktoré nie sú priradené k skupinám Microsoft 365:

- názov
- stav
- URL
- nájomník

Lokality SharePoint sú chránené automaticky vrátane podlokalít (tie sa tu preto nezobrazujú).

Kliknutím na tímovú skupinu alebo lokalitu SharePoint si môžete otvoriť okno **Zobraziť podrobnosti**, ktoré pozostáva zo štyroch častí:

Akcia	Použitie
Prehľad	Zobrazuje potrebné informácie o tímových skupinách alebo lokalitách SharePoint, ktoré sú načítané z Microsoft 365 (e-mail, vlastník, členovia, autor, URL atď.). Zobrazený je tiež aktuálny stav ochrany pre tímovú skupinu alebo lokalitu SharePoint.
Konfigurácia	V tejto časti nájdete v režime iba na čítanie zoznam Nastavení a priradených Politík. Prepínaním medzi kartami si môžete zobraziť konfiguráciu alebo zoznam priradených politík. Ak chcete meniť nastavenia alebo priraďovať politiky, je potrebné prejsť do sekcie Politiky.
Detekcie	V tejto časti nájdete zoznam všetkých detekcií v rámci tímových skupín alebo lokalít SharePoint.
Karanténa	V tejto časti nájdete všetky súbory, ktoré boli presunuté do karantény. Pre objekty umiestnené v karanténe môžete vykonať nasledujúce akcie: Uvoľniť, Stiahnuť alebo Odstrániť.

Kliknutím na **Pridať filter** si môžete vyfiltrovať tímové skupiny alebo lokality SharePoint.

Detekcie

V tejto sekcii nájdete zoznam všetkých detekcií zachytených prostredníctvom ESET Cloud Office Security. Pomocou kariet môžete prepínať medzi Gmailom, Diskom Google, Exchange Online, OneDrive, Tímovými skupinami a Lokalitami SharePoint. Na jednotlivých kartách nájdete detekcie aj s podrobnými informáciami. Napríklad zachytené súbory, ktoré boli nahrané do Tímovej skupiny, sa zobrazia na karte Tímové skupiny.

Kliknutím na ikonu otvoríte bočný panel so súhrnom konkrétneho záznamu protokolu (detekcie). Pre podrobnejšie informácie kliknite na ikonu a vyberte možnosť **Zobraziť podrobnosti**.

Na zobrazenie detekcií iba pre konkrétneho nájomníka alebo skupinu použite stromovú štruktúru. Ak chcete zobraziť všetky detekcie pre každého nájomníka a skupinu, kliknite na **Všetko**. Na jednoduchšie vyhľadávanie konkrétnych detekcií môžete využiť filtrovanie s viacerými kritériami. Kliknite na **Pridať filter** a z roletového menu vyberte typ filtra alebo zadajte reťazec (opakujte pri kombinovaní kritérií):

Pridať filter	Použitie
Výskyt od	Zadajte rozsah pre „dátum od“.

Pridať filter	Použitie
Výskyt do	Zadajte rozsah pre „dátum do“.
Predmet	Vzťahuje sa na správy, ktorých predmet obsahuje/neobsahuje konkrétny reťazec (alebo zadaný regulárny výraz).
ID správy	Filtrovanie správ podľa jedinečného identifikátora oceníte najmä vtedy, ak hľadáte konkrétnu správu v protokoloch obsahujúcich množstvo zaznamenaných správ alebo početné pokusy o doručenie správy.
Od	Filtrovanie správ podľa konkrétneho odosielateľa.
Komu	Filtrovanie správ podľa príjemcov.
E-mailová schránka	Vzťahuje sa na správy nachádzajúce sa v konkrétnej e-mailovej schránke.
Výsledok kontroly	Vyberte si jednu z nasledujúcich možností: Malvér, Malvér (zachytený pomocou ESET LiveGuard Advanced), Phishing alebo Spam.
Akcia	Vyberte si jednu z dostupných akcií.
Tím	Zadajte platný názov tímu.
Lokalita	Zadajte platný názov lokality.
Objekt	Zadajte platný názov objektu.
Detekcia	Zadajte platný názov detekcie.
Hash	Zadajte platný hash detekcie.

Keď kliknete na ikonu , možnosť **Odstrániť z whitelistu** bude dostupná v prípade, že ste už v minulosti pre rovnakého používateľa pridali súbor na whitelist jeho uvoľnením z karantény. Táto možnosť slúži na odstránenie súboru z whitelistu. Všetky takéto súbory budú umiestnené do karantény.

Detekcie sú uchovávané 90 dní. Záznamy staršie ako 90 dní budú natrvalo odstránené.

Nahlásenie falošne pozitívnych (FP)/falošne negatívnych (FN) detekcií

Falošne pozitívne a falošne negatívne detekcie môžete manuálne nahlásiť pre spam, phishing alebo malvér, a to odoslaním vzorky do spoločnosti ESET, kde následne dôjde k vykonaniu potrebnej analýzy. E-mailové adresy pre odosielanie vzoriek:

Spam – pošlite e-mail na adresu nospam_ecos@eset.com v prípade e-mailov, ktoré sú nesprávne označené ako spam, alebo na adresu spam_ecos@eset.com v prípade nezachyteného spamu, spolu s pôvodnou správou v prílohe vo formáte *.eml* alebo *.msg*.

Phishing – ak chcete nahlásiť nesprávne detegovaný phishing, pošlite e-mail na adresu samples@eset.com s textom *'phishing email'* v predmete e-mailu a pripojte k nemu pôvodný phishingový e-mail ako prílohu vo formáte *.eml* alebo *.msg*.

Malvér – ak chcete nahlásiť nesprávne detegovaný malvér, pošlite e-mail na adresu samples@eset.com. Ak ide o falošne pozitívnu detekciu, uveďte do predmetu e-mailu *'False positive'*. Ak ide o nezachytený malvér, uveďte do predmetu e-mailu *'Suspected infection'*. Príslušné súbory vložte do archívu *.zip* alebo *.rar* a pripojte ho k e-mailu ako prílohu.

Reporty

Reporty v ESET Cloud Office Security vám poskytujú prehľadné štatistiky o fungovaní ochrany, ktorú zaisťuje produkt ESET Cloud Office Security. Na výber sú dva typy reportov: štatistické reporty a reporty o e-mailovej

karanténe.

Štatistické reporty obsahujú informácie o ochrane pre Gmail, Google Drive, Exchange Online, OneDrive, lokality SharePoint a tímové skupiny v službe Teams. Ide presnejšie o údaje o počte skontrolovaných e□mailov, súborov, detegovaného malvéru, phishingu a spamu za určité obdobie. Reporty je možné manuálne vygenerovať a stiahnuť vo formáte *CSV* alebo *PDF*, prípadne naplánovať a nechať doručiť vybraným príjemcom prostredníctvom e□mailu. Ak si ako výstupný formát zvolíte *PDF*, dáta budú zobrazené vo forme grafu, aj s porovnaním oproti dlhodobému priemeru. K dispozícii tiež budete mať štatistiky pre každý typ ochrany a informácie o najčastejších príjemcoch malvéru, phishingu a spamu.

Report o e□mailovej karanténe obsahuje zoznam nových objektov presunutých do karantény. Report sa zasiela vybraným príjemcom prostredníctvom e□mailu. Príjemcovia môžu z karantény uvoľniť nevyžiadané správy (ak ich považujú za bezpečné alebo legitímne) kliknutím na odkaz **Uvoľniť**. Toto platí len pre spam, iné typy objektov z karantény nie je možné uvoľniť.

Štatistiky si môžete nechať zasielať e□mailom a pre ich zobrazenie tak nebude nutné otvárať konzolu ESET Cloud Office Security. Naplánovať môžete pravidelné generovanie reportov a nastaviť ich posielanie na určené e-mailové adresy. Štatistiky si navyše môžete kedykoľvek vygenerovať a stiahnuť priamo z konzoly ESET Cloud Office Security. Stačí vybrať existujúci report (môže byť aj naplánovaný report) a kliknúť na **Vygenerovať a stiahnuť**. Táto akcia je rovnako dostupná cez kontextové menu po kliknutí pravým tlačidlom myši. Jednoducho si môžete vytvoriť aj novú šablónu reportu s vlastnými nastaveniami.

Nový report

Kliknutím na možnosť Nový report si otvoríte šablónu reportu, kde si môžete zvoliť preferované nastavenia pre nový report. Zadajte názov reportu a popis.

Jazyk

Z roletového menu vyberte požadovaný jazyk. Report sa vygeneruje v tomto jazyku.

Typ

Vyberte, aký typ dát chcete zahrnúť do štatistiky.

Štatistické reporty

Vytvorte naplánované reporty alebo manuálne generované reporty zahŕňajúce informácie na základe možností, ktoré si vyberiete.

Reporty o e□mailovej karanténe

Prostredníctvom e□mailových oznámení môžete vybraných používateľov informovať o ich nových e□mailových správach, ktoré boli presunuté do karantény. Priradiť môžete jedného alebo viacerých príjemcov, prípadne skupinu. Vyberte interval zasielania reportu a začiatočný dátum a čas. Ak ide o opakovaný report, vyberte, kedy sa má zasielanie skončiť (v určitý deň, po niekoľkých výskytoch alebo nikdy). Report sa vygeneruje len v prípade, ak sa v karanténe objavia nové objekty. Príjemcovia reportu môžu z karantény uvoľniť nevyžiadané správy (ak ich považujú za bezpečné alebo legitímne) kliknutím na odkaz Uvoľniť (vo webovom prehliadači sa otvorí potvrdzovacie okno). Spamová správa, ktorú príjemca takto uvoľní z karantény, sa doručuje v samostatnom e□maile ako príloha.

Nájomník

Táto možnosť je dostupná pre multitenantné prostredie. Môžete vybrať viacerých nájomníkov, pre ktorých sa budú generovať štatistiky. Report sa vygeneruje osobitne pre každého nájomníka a z ESET Cloud Office Security bude doručený jeden e-mail s viacerými prílohami.

Časové obdobie

Nastavte časové obdobie, za ktoré chcete zobraziť výsledky (posledných 24 hodín, týždeň, mesiac). Ak použijete možnosť Vlastný, môžete určiť vlastný rozsah (Dátum od a Dátum do).

Výstup

Vyberte si preferovaný formát súboru, k dispozícii je *PDF* alebo *CSV*. Ak si ako formát vyberiete *PDF*, reporty budú obsahovať aj údaje zobrazené v grafoch. Formát *CSV* je vhodný, ak potrebujete nespracované dáta. Údaje v reportoch budú zozbierané podľa zvolených nastavení. Ak si vyberiete viacero zdrojov údajov (Exchange Online, OneDrive, Tímové skupiny alebo Lokality SharePoint, Gmail či Disk Google), výstupom bude ZIP archív, v ktorom nájdete reporty v požadovanom formáte (*PDF* alebo *CSV*).

Whitelabel

Ak chcete mať v reporte zobrazené logo vašej spoločnosti, zapnite túto funkciu. Môžete si vybrať, či sa má v hlavičke reportu zobraziť vaše logo spolu s logom spoločnosti ESET formou co-brandingu alebo chcete zahrnúť len vlastné logo. Logo nahrajte vo formáte *JPEG* alebo *PNG*.

Naplánované

Plánovač použite na generovanie reportov v konkrétnom dátume a čase, prípadne si nastavte pravidelné generovanie a zasielanie reportov. Naplánované reporty budú určeným príjemcom doručené z ESET Cloud Office Security ako príloha e-mailu.

Opakovať

Vyberte, či má byť report vygenerovaný raz alebo opakovane:

- **Raz** – report sa vygeneruje iba raz v naplánovanom čase.
- **Denne** – report sa vygeneruje a odošle určeným príjemcom pravidelne každý deň (pokiaľ pomocou možnosti „skončí po výskytoch“ nenastavíte, dokedy sa má akcia opakovať).
- **Týždenne** – report sa vygeneruje a odošle určeným príjemcom pravidelne vo zvolených dňoch týždňa.
- **Mesačne** – report sa vygeneruje a odošle určeným príjemcom raz za mesiac v stanovený deň.

Začiatok

Vyberte dátum, odkedy sa má report generovať.

Skončí

Vyberte dátum, dokedy sa má report generovať.

Príjemcovia

Zadajte e-mailovú adresu príjemcu, ktorému má byť report doručený. Zadanie potvrďte stlačením klávesu Enter. Týmto spôsobom môžete postupne pridať viacero príjemcov.

Podrobné informácie alebo ďalšie akcie sú dostupné po kliknutí na ikonu . Zobrazia sa nasledujúce možnosti:

Akcia	Použitie
Zobraziť podrobnosti	Kliknutím si zobrazíte podrobné informácie o reporte.
Vygenerovať a stiahnuť	Po kliknutí na Vygenerovať a stiahnuť si vyberte preferovaný formát súboru. K dispozícii je formát *PDF* alebo *CSV*. Ak si ako formát vyberiete *PDF*, reporty budú obsahovať aj údaje zobrazené v grafoch. Formát *CSV* je vhodný, ak potrebujete nespracované dáta. Údaje v reportoch budú zozbierané podľa zvolených nastavení. Ak si ako zdroj údajov vyberiete Exchange Online, OneDrive, Tímové skupiny alebo Lokality SharePoint, výstupom bude *ZIP* archív, v ktorom nájdete reporty v požadovanom formáte (PDF alebo *CSV*).
Upraviť	Po kliknutí môžete upraviť konfiguráciu existujúceho reportu.
Odstrániť	Kliknutím kompletne odstránite vybraný report.

Ak chcete filtrovať reporty, kliknite na **Pridať filter** a z roletového menu vyberte typ filtra alebo zadajte reťazec, podľa ktorého chcete vyhľadávať (môžete tiež skombinovať viacero kritérií hľadania):

Pridať filter	Použitie
Názov	Zadajte časť alebo celý názov reportu.
Naplánované	K dispozícii sú tieto možnosti: Nenaplánované, Raz, Denne, Týždenne alebo Mesačne.
Údaje	Ak chcete filtrovať podľa zdroja údajov, vyberte Exchange Online, OneDrive, Tímové skupiny alebo Lokality SharePoint.

Karanténa

Karanténa poskytuje jednoduchú správu objektov (e-mailov a súborov), ktoré sem boli premiestnené prostredníctvom ESET Cloud Office Security. Pomocou kariet môžete prepínať medzi Gmailom, Diskom Google, Exchange Online, OneDrive, Tímovými skupinami a Lokalitami SharePoint. Pre každý objekt sú k dispozícii podrobné informácie.

Kliknutím na ikonu otvoríte bočný panel so súhrnnými informáciami o konkrétnom objekte. Pre podrobnejšie informácie kliknite na ikonu a vyberte možnosť **Zobraziť podrobnosti**.

Na zobrazenie objektov iba pre konkrétneho nájomníka alebo skupinu použite stromovú štruktúru. Ak chcete zobraziť všetky detekcie pre každého nájomníka a skupinu, kliknite na **Všetko**.

Môžete skontrolovať e-maily alebo súbory umiestnené v karanténe a vykonať príslušnú akciu (**Odstrániť** alebo **Uvoľniť**). Môžete si tiež **Stiahnuť** pôvodný súbor alebo archív chránený heslom vo formáte *.zip*.

> Ak detekciu vyhodnotíte ako neškodnú (falošný poplach), príslušný súbor môžete **uvoľniť** z karantény. Uvoľnený súbor bude automaticky pridaný na whitelist na základe hodnoty hash. Ďalšie výskyty rovnakého súboru (pre rovnakého používateľa) nebudú vyhodnotené ako podozrivé a nebudú umiestnené do karantény. Automatický whitelisting funguje pre každého používateľa osobitne. V prípade ostatných používateľov bude rovnaký súbor aj naďalej vyhodnotený ako podozrivý a uložený do karantény. Súbor môžete odstrániť z whitelistu v zozname detekcií pomocou možnosti **Odstrániť z whitelistu**.

Kliknite na ikonu a vyberte akciu:

Akcia	Použitie
Zobraziť podrobnosti	Zobrazia sa podrobnejšie informácie o e-maile umiestnenom v karanténe.

Akcia	Použitie
Uvoľniť (e-maily alebo súbory)	E-mail bude uvoľnený z karantény a odoslaný pôvodnému príjemcovi vo forme notifikačného e-mailu, pričom pôvodná správa bude pripojená ako príloha. V prípade OneDrive objektu bude súbor odovzdaný do pôvodného umiestnenia v úložisku OneDrive konkrétneho používateľa. V prípade súboru z tímovej skupiny alebo lokality SharePoint sa daný súbor po uvoľnení zobrazí späť v pôvodnom umiestnení. Uvoľnený súbor bude automaticky pridaný na whitelist na základe hodnoty hash. Týmto sa predíde opätovnému uloženiu súboru do karantény.
Odstrániť	Objekt bude odstránený z karantény.
Stiahnuť pôvodný súbor	Súbor sa stiahne v pôvodnej podobe bez ochrany heslom.
Stiahnuť archív chránený heslom	Stiahne sa súbor v archíve chránenom heslom.
Odoslať vzorku	Prostredníctvom okna Poslať vzorku na analýzu môžete odoslať podozrivý súbor alebo spam do spoločnosti ESET na analýzu. Z roletového menu vyberte Dôvod odoslania vzorky.

Na jednoduchšie vyhľadávanie konkrétnych objektov umiestnených v karanténe môžete využiť filtrovanie s viacerými kritériami. Kliknite na **Pridať filter** a z roletového menu vyberte typ filtra alebo zadajte reťazec (opakujte pri kombinovaní kritérií):

Pridať filter	Použitie
Výskyt od	Zadajte rozsah pre „dátum od“.
Výskyt do	Zadajte rozsah pre „dátum do“.
Predmet	Vzťahuje sa na správy, ktorých predmet obsahuje/neobsahuje konkrétny reťazec (alebo zadaný regulárny výraz).
ID správy	Filtrovanie správ podľa jedinečného identifikátora oceníte najmä vtedy, ak hľadáte konkrétnu správu v protokoloch obsahujúcich množstvo zaznamenaných správ alebo početné pokusy o doručenie správy.
Od	Filtrovanie správ podľa konkrétneho odosielateľa.
Komu	Filtrovanie správ podľa príjemcov.
E-mailová schránka	Vzťahuje sa na správy nachádzajúce sa v konkrétnej e-mailovej schránke.
Výsledok kontroly	Vyberte si jednu z nasledujúcich možností: Malvér, Malvér (zachytený pomocou ESET LiveGuard Advanced), Phishing alebo Spam.
Tím	Zadajte platný názov tímu.
Objekt	Zadajte platný názov objektu.
Lokalita	Zadajte platný názov lokality.

Obdobie uchovávania objektov v karanténe je stanovené na 30 dní. Objekty staršie ako 30 dní budú z karantény natrvalo odstránené.

Protokoly kontroly

V protokoloch nájdete výsledky všetkých kontrol vykonaných prostredníctvom ESET Cloud Office Security. Protokoly sú podobné detekciám, môže v nich však byť zahrnutý aj zoznam neinfikovaných objektov (v politikách je potrebné povoliť nastavenie Zapisovať všetky objekty do protokolu). Pomocou kariet môžete prepínať medzi Gmailom, Diskom Google, Exchange Online, OneDrive, Tímovými skupinami, Lokalitami SharePoint a Odoslanými súbormi. Pri každej detekcii sa zobrazuje značné množstvo informácií. Odoslané súbory obsahujú zoznam všetkých súborov, ktoré boli odoslané na analýzu do ESET LiveGuard Advanced.

Kliknutím na ikonu otvoríte bočný panel so súhrnom konkrétneho záznamu protokolu. Ak chcete získať podrobnejšie informácie, kliknite na trojbodkovú ikonu a vyberte možnosť **Zobraziť podrobnosti**.

Na zobrazenie záznamov iba pre konkrétneho nájomníka alebo skupinu použite stromovú štruktúru. Ak chcete zobraziť všetky detekcie pre každého nájomníka a skupinu, kliknite na **Všetko**.

> Ak je výsledok kontroly **Neskontrolované**, dôvody môžu byť rôzne. Viac informácií nájdete v kapitole Obmedzenia.

Keď v pravom hornom rohu kliknete na ikonu ozubeného kolesa a z kontextového menu vyberiete možnosť **Exportovať do súboru CSV**, tabuľku môžete exportovať do formátu *CSV* a s obsiahnutým zoznamom tak pracovať aj v iných aplikáciách.

Na jednoduchšie vyhľadávanie konkrétnych záznamov môžete využiť filtrovanie s viacerými kritériami. Kliknite na **Pridať filter** a z roletového menu vyberte typ filtra alebo zadajte reťazec (opakujte pri kombinovaní kritérií):

Pridať filter	Použitie
Výskyt od	Zadajte rozsah pre „dátum od“.
Výskyt do	Zadajte rozsah pre „dátum do“.
Zdroj dát	Vyberte si jednu z nasledujúcich možností: Exchange Online, OneDrive, Tímová skupina a Lokalita SharePoint.
E-mailová schránka	Vzťahuje sa na správy nachádzajúce sa v konkrétnej e-mailovej schránke.
Od	Filtrovanie správ podľa konkrétneho odosielateľa.
Komu	Filtrovanie správ podľa príjemcov.
Predmet	Vzťahuje sa na správy, ktorých predmet obsahuje/neobsahuje konkrétny reťazec.
ID správy	Filtrovanie správ podľa jedinečného identifikátora oceníte najmä vtedy, ak hľadáte konkrétnu správu v protokoloch obsahujúcich množstvo zaznamenaných správ alebo početné pokusy o doručenie správy.
Výsledok kontroly	Vyberte si jednu z nasledujúcich možností: Malvér, Malvér (zachytený pomocou ESET LiveGuard Advanced), Phishing, Spam, Čisté, Neskontrolované, Chyba, Vypnuté.
Akcia	Vyberte si jednu z dostupných akcií.
Vlastníci	Zadajte platný názov vlastníka.
Objekt	Zadajte platný názov objektu.
Detekcia	Zadajte platný názov detekcie.
Hash	Zadajte platný hash detekcie.
Tím	Zadajte platný názov tímu.
Lokalita	Zadajte platný názov lokality.

> Záznamy protokolov sa uchovávajú po dobu 90 dní. Záznamy staršie ako 90 dní budú natrvalo odstránené. Ak používate politiku, v rámci ktorej je nastavená možnosť **Zapisovať všetky objekty do protokolu**, záznamy protokolov s **čistým** výsledkom kontroly sú uchovávané 3 dni. Čisté výsledky kontroly staršie ako 3 dni budú natrvalo odstránené.

Politiky

Väčšie firmy majú zvyčajne viacero oddelení a v rámci každej organizačnej jednotky sa používajú rôzne nastavenia ochrany. ESET Cloud Office Security poskytuje nastavenia ochrany založené na politikách, ktoré môžete prispôsobiť svojim potrebám a priradiť ku konkrétnym používateľom, skupinám používateľov, nájomníkom,

tímovým skupinám alebo lokalitám SharePoint.

Ak chcete pridať kritériá filtrovania, kliknite na **Pridať filter**, vyberte príslušný **Názov** položky a zadajte názov politiky. V stromovej štruktúre politík sú zobrazení nájomníci a ich skupiny používateľov, tímové skupiny alebo lokality SharePoint, ako aj skupina **Nepriradené**, ktorá obsahuje vlastné politiky nepriradené k žiadnemu cieľu.

Môžete pridať novú politiku alebo zmeniť existujúcu politiku a jej nastavenia:

1. Kliknite na **Politiky** > **Nová politika**.

2. Zadajte **Názov** a **Popis** pre novú politiku.

3. Nakonfigurujte politiku pre vybraný cieľ:

   • **Nájomníci** – nastavte ochranu pre Gmail, Disk Google, Exchange Online, OneDrive, lokality SharePoint a tímové skupiny a priraďte ju vybraným nájomníkom.

   • **Používatelia** – nastavte ochranu pre Gmail, Disk Google, Exchange Online a OneDrive a priraďte ju vybraným používateľom alebo skupinám používateľov.

   • **Tímové skupiny** – nastavte ochranu tímových skupín a priraďte ju vybraným tímovým skupinám.

   • **Lokality SharePoint** – nastavte ochranu lokalít SharePoint a priraďte ju vybraným lokalitám.

4. V sekcii **Nastavenia** upravte nastavenia ochrany pre Exchange Online, Gmail, OneDrive, Disk Google, tímové skupiny, lokality SharePoint alebo ESET LiveGuard Advanced a kliknite na **Ďalej**.

5. Kliknite na **Priradiť** a vyberte cieľ, ktorému bude politika priradená.

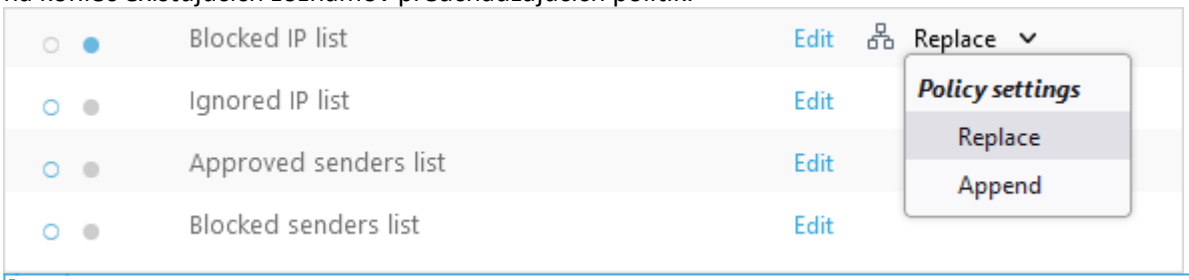
6. Kliknutím na **Uložiť zmeny** uložte nastavenia politiky.

Princípy politík

Predvolená politika: • Vzťahuje sa na všetkých používateľov (chránených aj nechránených). • Nie je možné ju zmeniť alebo odstrániť.
Vlastná politika môže byť priradená k: • **Používateľom** – politika sa vzťahuje na manuálne vybraných používateľov, • **Skupinám** – politika sa vzťahuje na všetkých členov skupiny používateľov, • **Nájomníkom** – politika sa vzťahuje na všetky objekty v rámci nájomníka, • **Tímovým skupinám** – politika sa vzťahuje na tímovú skupinu, • **Lokalitám SharePoint** – politika sa vzťahuje na lokalitu SharePoint.
Vlastná politika priradená k **nájomníkovi** alebo ku **skupine** je zlúčená s predvolenou politikou. Vlastná **politika nájomníka**, **skupinová politika**, **politika tímovej skupiny** alebo **politika lokality SharePoint** má vyššiu prioritu ako predvolená politika. Vlastná politika priradená k **používateľovi** je zlúčená s **politikou nájomníka/skupiny/tímovej skupiny/lokality SharePoint** a predvolenou politikou. Vlastná politika **používateľa** má vyššiu prioritu ako politika nájomníka/skupinová politika a predvolená politika. Politika tímovej skupiny/lokality SharePoint sa aplikuje vždy, keď používateľ nahráva súbor do služby Teams alebo na lokalitu SharePoint.
K používateľom a nájomníkom možno priradiť viacero **vlastných politík**, pričom výsledné nastavenie závisí od ich priority (poradia).

Nastavenie pre antispamové zoznamy pri zlučovaní politík

Možnosť zlúčenia sa vzťahuje na nastavenia antispamových zoznamov a možnosti Upozorniť správcu (ide o adresy, na ktoré sú zasielané notifikačné e-maily o detekciách pomocou funkcií Antimalvér a Anti‑Phishing). Ak existuje viacero politík s antispamovými zoznamami (zoznamami povolených, blokovaných a ignorovaných IP adries, domén alebo e-mailových adries) alebo s adresami správcu, na ktoré sú zasielané notifikačné e-maily, vyberte stratégiu zlučovania:
Nahradiť – ponechať len nové položky v zozname (predvolená možnosť). Všetky zoznamy z predchádzajúcich politík sa nahradia novými položkami aktuálnej politiky.
Pripojiť na koniec – rozšíriť zoznamy predchádzajúcich politík pripojením nových položiek. Zoznamy z predchádzajúcich politík sa zlúčia s novými položkami aktuálnej politiky. Nové položky budú umiestnené na koniec existujúcich zoznamov predchádzajúcich politík.



Predtým, ako bola k dispozícii možnosť zlúčenia, predvolená akcia bola **Nahradiť**. Ak už používate politiky s konkrétnymi antispamovými zoznamami, môžete ponechať predvolenú možnosť **Nahradiť**, v prípade potreby ju však môžete zmeniť na **Pripojiť na koniec**.

Vytvorte novú politiku s definovaným antispamovým zoznamom a vyberte možnosť zlúčenia (za predpokladu, že už sa používajú iné politiky s antispamovými zoznamami).
1. Kliknite na **Politiky** > **Nová politika**.
2. Zadajte **Názov** a **Popis** novej politiky, ako cieľ vyberte možnosť **Nájomníci** a kliknite na **Ďalej**.
3. Rozbaľte sekciu **Exchange Online: Antispam** a kliknite na **Upraviť** vedľa položky Zoznam blokovaných IP adries.
4. Kliknite na **Pridať**, zadajte IP adresu, stlačením klávesu **Enter** dokončite akciu (prípadne importujte zoznam zo súboru) a kliknite na **Uložiť zmeny**.
5. Z roletového menu vyberte ako možnosť zlúčenia **Pripojiť na koniec** a kliknite na tlačidlo **Ďalej**.
6. Kliknite na **Priradiť**, z roletového menu vyberte možnosť **Priradiť nájomníkom**, označte začiarkavacie políčko vedľa daného nájomníka a kliknite na **OK**.
7. Kliknite na **Uložiť zmeny** pre dokončenie procesu.

Ak chcete zmeniť prioritu politiky, kliknite na **Zmeniť poradie**. Vyberte politiku alebo viaceré politiky a kliknite na tlačidlo **Aplikovať skôr** alebo **Aplikovať neskôr**, čím dôjde k zmene ich priority. Politiky sú aplikované globálne (bez ohľadu na priradenie – nájomník, skupina alebo používateľ) v nastavenom poradí, a to odvrchu smerom nadol. Predvolená politika je vždy aplikovaná ako prvá.

Na vykonanie nasledujúcich akcií vyberte politiku a kliknite na trojbodkovú ikonu :

Akcia	Použitie
Zobraziť podrobnosti	Zobrazenie podrobných informácií o vytvorenej politike, nastaveniach a o tom, komu je politika priradená.
Upraviť	Po kliknutí môžete upraviť konfiguráciu existujúcej politiky.
Priradiť	Vyberte používateľov, nájomníkov, tímové skupiny alebo lokality SharePoint, na ktoré sa bude politika uplatňovať.
Duplikovať	Po kliknutí môžete vytvoriť novú politiku na základe zvolenej šablóny. Pre zduplikovanú politiku je potrebné zadať nový názov.
Odstrániť	Úplné odstránenie vybranej politiky.

Vytvorenie vlastnej politiky nájomníka s cieľom zobraziť všetky výsledky kontroly (vrátane čistých výsledkov) v protokoloch kontroly. Politika nájomníka sa vzťahuje na všetkých používateľov (chránených aj nechránených).

1. Kliknite na **Politiky** > **Nová politika**.
2. Zadajte **Názov** a **Popis** novej politiky, ako cieľ vyberte možnosť **Nájomníci** a kliknite na **Ďalej**.
3. Rozbaľte sekciu **Exchange Online: Všeobecné** a pomocou prepínacieho tlačidla povoľte možnosť **Zapisovať všetky objekty do protokolu**.
4. Rozbaľte sekciu **OneDrive: Všeobecné** a pomocou prepínacieho tlačidla povoľte možnosť **Zapisovať všetky objekty do protokolu**.
5. Rozbaľte sekciu **Tímové skupiny: Všeobecné** a pomocou prepínacieho tlačidla povoľte možnosť **Zapisovať všetky objekty do protokolu**.
6. Rozbaľte sekciu **Lokality SharePoint: Všeobecné**, pomocou prepínacieho tlačidla povoľte možnosť **Zapisovať všetky objekty do protokolu** a kliknite na **Ďalej**.
7. Kliknite na **Priradiť**, označte nájomníka a kliknite na **OK**.
8. Kliknite na **Uložiť zmeny** pre dokončenie procesu.

Vytvorenie vlastnej politiky pre konkrétnych používateľov s pokročilými nastaveniami, ktoré budú mať vplyv na riešenie malvéru, spamu a phishingu. Pomocou tejto politiky budú zmazané e-mailové prílohy, ktoré obsahujú malvér, spamové správy budú presunuté do priečinka s nevyžiadanou poštou, phishingové e-maily budú mať označený predmet správy a budú presunuté do karantény a obsah škodlivých súborov umiestnených v úložisku OneDrive bude nahradený obyčajným textom, aby sa predišlo akejkoľvek škode.

1. Kliknite na **Politiky** > **Nová politika**.
2. Zadajte **Názov** a **Popis** pre novú politiku, ako cieľ vyberte možnosť **Používatelia** a kliknite na **Ďalej**.
3. Rozbaľte sekciu **Exchange Online: Antimalvér** a pomocou roletového menu vedľa položky **Pri výskyte objektu** vyberte možnosť **Odstrániť prílohu**.
4. Rozbaľte sekciu **Exchange Online: Antispam** a pomocou roletového menu vedľa položky **Pri výskyte objektu** vyberte možnosť **Presunúť do nevyžiadanej pošty**.
5. Rozbaľte sekciu **Exchange Online: Anti-Phishing** a pomocou prepínacieho tlačidla povoľte možnosť **Označiť predmet správy**. V prípade potreby môžete zmeniť **Text pre označenie predmetu správy**.
6. Rozbaľte sekciu **OneDrive: Antimalvér**, z roletového menu vedľa položky **Pri výskyte objektu** vyberte možnosť **Nahradiť** a kliknite na **Ďalej**.
7. Kliknite na **Priradiť**, označte používateľov, na ktorých chcete politiku aplikovať, a kliknite na **OK**. Ak je už na používateľa aplikovaná existujúca vlastná politika, bude prepísaná novou politikou.
8. Kliknite na **Uložiť zmeny** pre dokončenie procesu.

Nastavenia ochrany pre Exchange Online

V tejto kapitole nájdete informácie o nastaveniach pre Exchange Online: Všeobecné, Antimalvér, Antispam a Antiphishing.

Exchange Online: Všeobecné

Systém spätnej väzby ESET LiveGrid®
Dáta budú odoslané do ESET Research Lab na ďalšiu analýzu. Viac informácií o ESET LiveGrid® nájdete v slovníku pojmov.

Zapisovať všetky objekty do protokolu
Ak je táto možnosť označená, všetky výsledky kontroly (vrátane čistých) budú zobrazené v protokoloch kontroly. Politika uchovávania údajov týkajúca sa čistých výsledkov kontroly predstavuje tri dni. Výsledky kontroly staršie ako 3 dni budú natrvalo odstránené.

Exchange Online: Antimalvér

Exchange Online: Antimalvér
Ak je táto možnosť povolená, daná funkcia je aktivovaná a môžete konfigurovať podrobné nastavenia.
Hlásenia a ochrana s využitím strojového učenia
Súčasťou detekčného jadra je teraz aj pokročilé strojové učenie – pokročilá vrstva ochrany, ktorá zlepšuje detekciu. Pred úpravou prahu (alebo úrovne) v rámci kategórie Hlásenia si prečítajte nižšie uvedené informácie.
Pri výskyte objektu
- **Žiadna akcia** – nevykoná sa žiadna akcia a e-mail bude doručený príjemcovi.
- **Presunúť do nevyžiadanej pošty** – e-mail bude presunutý medzi nevyžiadanú poštu.
- **Presunúť do koša** – e-mail bude presunutý do koša.
- **Odstrániť správu** – e mail bude zmazaný
- **Presunúť správu do karantény** – pôvodný e-mail bude zmazaný a jeho kópia bude uložená do karantény. Ak sa rozhodnete uvoľniť e-mail z karantény, príjemcovi bude doručený v podobe prílohy, ktorá bude pripojená k novému e-mailu.
- **Odstrániť prílohu** – príloha bude odstránená a správa bude doručená príjemcovi bez prílohy.
- **Nahradiť prílohu** – príloha bude nahradená textovým súborom obsahujúcim podrobné informácie o vykonanej akcii.
- **Presunúť prílohu do karantény** – príloha bude odstránená z e-mailu a uložená do súborovej karantény.

Text pre nahradenie prílohy
Nahradí prílohu textovým súborom obsahujúcim podrobné informácie o vykonanej akcii.
Označiť predmet správy
Ak je táto možnosť zapnutá, môžete upraviť šablóny pridávané do predmetu infikovaných správ.
Text pre označenie predmetu správy
Do predmetu infikovaných správ môžete pridať vlastné označenie.
Upozorniť vlastníka e-mailovej schránky
Ak je táto možnosť povolená, používateľ dostane v prípade zachytenia detekcie notifikačný e-mail.
Jazyk
Z roletového menu vyberte požadovaný jazyk. Pri uvoľnení objektu z karantény Exchange Online dostane vlastník e mailovej schránky oznámenie v tomto jazyku. Použitím tejto možnosti sa prepíše predvolený jazyk nájomníka v nastaveniach.
Upozorniť správcu
Zadajte e-mailovú adresu (pre pridanie viacerých adries stlačte Enter), na ktorú budú odoslané notifikačné e-maily vždy, keď sa nájde detekcia.

Exchange Online: Antispam

Exchange Online: Antispam
Ak je táto možnosť povolená, daná funkcia je aktivovaná a môžete konfigurovať podrobné nastavenia.
Pri výskyte objektu
- **Žiadna akcia** – nevykoná sa žiadna akcia a e-mail bude doručený príjemcovi.
- **Presunúť do nevyžiadanej pošty** – e-mail bude presunutý medzi nevyžiadanú poštu.
- **Presunúť do koša** – e-mail bude presunutý do koša.
- **Odstrániť správu** – e□mail bude zmazaný
- **Presunúť správu do karantény** – pôvodný e-mail bude zmazaný a jeho kópia bude uložená do karantény. Ak sa rozhodnete uvoľniť e-mail z karantény, príjemcovi bude doručený v podobe prílohy, ktorá bude pripojená k novému e-mailu.

Označiť predmet správy
Ak je táto možnosť zapnutá, môžete upraviť šablóny pridávané do predmetu infikovaných správ.
Text pre označenie predmetu správy
Do predmetu infikovaných správ môžete pridať vlastné označenie.
Môžete nastaviť **Povolené**, **Blokované** a **Ignorované** zoznamy zadaním kritérií, ako napr. IP adresa alebo rozsah IP adries, názov domény atď. Pre pridanie, úpravu alebo odstránenie kritérií použite tlačidlo **Upraviť**. Môžete prípadne importovať svoj vlastný zoznam zo súboru namiesto zadávania každej položky manuálne – kliknite na **Importovať** a vyhľadajte súbor (vo formáte *.txt*) obsahujúci položky, ktoré chcete pridať do zoznamu. Ak chcete exportovať existujúci zoznam do súboru (vo formáte *.txt*), vyberte z kontextového menu možnosť **Exportovať**.

Zoznam povolených IP adries	E-maily prichádzajúce z IP adries uvedených na tomto zozname budú automaticky doručené príjemcom. Obsah e□mailových správ nebude kontrolovaný.
Zoznam blokovaných IP adries	Automaticky zablokuje e-mailové správy prichádzajúce zo zadaných IP adries.
Zoznam ignorovaných IP adries	Zoznam IP adries, ktoré budú počas klasifikácie ignorované. Obsah e□mailových správ bude kontrolovaný.
Zoznam povolených odosielateľov	E-maily prichádzajúce od odosielateľov alebo z domén na tomto zozname budú doručené príjemcom. Pri vyhodnotení sa použije iba jeden odosielateľ alebo celá doména podľa nižšie uvedenej priority: 1.SMTP 'MAIL FROM' adresa 2.Hlavička "Return-Path:" 3.Hlavička "X-Env-Sender:" 4.Hlavička "From:" 5.Hlavička "Sender:" 6.Hlavička "X-Apparently-From:"
Zoznam blokovaných odosielateľov	Doručenie e-mailov od odosielateľov alebo z domén na tomto zozname bude blokované. Pri vyhodnotení sa použijú všetci zistení odosielatelia alebo celé domény: SMTP 'MAIL FROM' adresa Hlavička "Return-Path:" Hlavička "X-Env-Sender:" Hlavička "From:" Hlavička "Sender:" Hlavička "X-Apparently-From:"

Exchange Online: Antiphishing

Exchange Online: Antiphishing
Ak je táto možnosť povolená, daná funkcia je aktivovaná a môžete konfigurovať podrobné nastavenia.
Pri výskyte objektu
- **Žiadna akcia** – nevykoná sa žiadna akcia a e-mail so škodlivou prílohou bude doručený príjemcovi.
- **Presunúť do nevyžiadanej pošty** – e-mail bude presunutý medzi nevyžiadanú poštu.
- **Presunúť do koša** – e-mail bude presunutý do koša.
- **Odstrániť správu** – e□mail bude zmazaný
- **Presunúť správu do karantény** – pôvodný e-mail bude zmazaný a jeho kópia bude uložená do karantény. Ak sa rozhodnete uvoľniť e-mail z karantény, príjemcovi bude doručený v podobe prílohy, ktorá bude pripojená k novému e-mailu.

Označiť predmet správy
Ak je táto možnosť zapnutá, môžete upraviť šablóny pridávané do predmetu infikovaných správ.
Text pre označenie predmetu správy
Do predmetu infikovaných správ môžete pridať vlastné označenie.
Upozorniť vlastníka e-mailovej schránky
Ak je táto možnosť povolená, používateľ dostane v prípade zachytenia detekcie notifikačný e-mail.
Upozorniť správcu
Zadajte e-mailovú adresu (pre pridanie viacerých adries stlačte Enter), na ktorú budú odoslané notifikačné e-maily vždy, keď sa nájde detekcia pre ktoréhokoľvek používateľa Exchange Online.

Nastavenia ochrany pre Gmail

V tejto kapitole nájdete informácie o nastaveniach pre Gmail: Všeobecné, Antimalvér, Antispam a Antiphishing.

Gmail: Všeobecné

ESET LiveGrid®Systém spätnej väzby
Dáta budú odoslané do ESET Research Lab na ďalšiu analýzu. Viac informácií o ESET LiveGrid® nájdete v slovníku pojmov.
Zapisovať všetky objekty do protokolu
Ak je táto možnosť označená, všetky výsledky kontroly (vrátane čistých) budú zobrazené v protokoloch kontroly. Politika uchovávania údajov týkajúca sa čistých výsledkov kontroly predstavuje tri dni. Výsledky kontroly staršie ako 3 dni budú natrvalo odstránené.

Gmail: Antimalvér

Zapnúť Antimalvér pre Gmail
Ak je táto možnosť povolená, daná funkcia je aktivovaná a môžete konfigurovať podrobné nastavenia.
Hlásenia a ochrana s využitím strojového učenia
Súčasťou detekčného jadra je teraz aj pokročilé strojové učenie – pokročilá vrstva ochrany, ktorá zlepšuje detekciu. Pred úpravou prahu (alebo úrovne) v rámci kategórie Hlásenia si prečítajte nižšie uvedené informácie.
Pri výskyte objektu
- **Žiadna akcia** – nevykoná sa žiadna akcia a e-mail bude doručený príjemcovi.
- **Presunúť do nevyžiadanej pošty** – e-mail bude presunutý medzi nevyžiadanú poštu.
- **Presunúť do koša** – e-mail bude presunutý do koša.
- **Odstrániť správu** – e□mail bude zmazaný
- **Presunúť správu do karantény** – pôvodný e-mail bude zmazaný a jeho kópia bude uložená do karantény. Ak sa rozhodnete uvoľniť e-mail z karantény, príjemcovi bude doručený v podobe prílohy, ktorá bude pripojená k novému e-mailu.
- **Odstrániť prílohu** – príloha bude odstránená a správa bude doručená príjemcovi bez prílohy.
- **Nahradiť prílohu** – príloha bude nahradená textovým súborom obsahujúcim podrobné informácie o vykonanej akcii.
- **Presunúť prílohu do karantény** – príloha bude odstránená z e-mailu a uložená do súborovej karantény.

Text pre nahradenie prílohy
Nahradí prílohu textovým súborom obsahujúcim podrobné informácie o vykonanej akcii.
Označiť predmet správy
Ak je táto možnosť zapnutá, môžete upraviť šablóny pridávané do predmetu infikovaných správ.
Text pre označenie predmetu správy
Do predmetu infikovaných správ môžete pridať vlastné označenie.
Upozorniť vlastníka e-mailovej schránky
Ak je táto možnosť povolená, používateľ dostane v prípade zachytenia detekcie notifikačný e-mail.
Jazyk
Z roletového menu vyberte požadovaný jazyk. Pri uvoľnení objektu z karantény dostane vlastník e□mailovej schránky oznámenie v tomto jazyku. Použitím tejto možnosti sa prepíše predvolený jazyk nájomníka v nastaveniach.
Upozorniť správcu
Zadajte e-mailovú adresu (pre pridanie viacerých adries stlačte Enter), na ktorú budú odoslané notifikačné e-maily vždy, keď sa nájde detekcia.

Gmail: Antispam

Zapnúť Antispam pre Gmail
Ak je táto možnosť povolená, daná funkcia je aktivovaná a môžete konfigurovať podrobné nastavenia.
Pri výskyte objektu
- **Žiadna akcia** – nevykoná sa žiadna akcia a e-mail bude doručený príjemcovi.
- **Presunúť do nevyžiadanej pošty** – e-mail bude presunutý medzi nevyžiadanú poštu.
- **Presunúť do koša** – e-mail bude presunutý do koša.
- **Odstrániť správu** – e□mail bude zmazaný
- **Presunúť správu do karantény** – pôvodný e-mail bude zmazaný a jeho kópia bude uložená do karantény. Ak sa rozhodnete uvoľniť e-mail z karantény, príjemcovi bude doručený v podobe prílohy, ktorá bude pripojená k novému e-mailu.

Označiť predmet správy
Ak je táto možnosť zapnutá, môžete upraviť šablóny pridávané do predmetu infikovaných správ.
Text pre označenie predmetu správy
Do predmetu infikovaných správ môžete pridať vlastné označenie.
Môžete nastaviť **Povolené**, **Blokované** a **Ignorované** zoznamy zadaním kritérií, ako napr. IP adresa alebo rozsah IP adries, názov domény atď. Pre pridanie, úpravu alebo odstránenie kritérií použite tlačidlo **Upraviť**. Môžete prípadne importovať svoj vlastný zoznam zo súboru namiesto zadávania každej položky manuálne – kliknite na **Importovať** a vyhľadajte súbor (vo formáte *.txt*) obsahujúci položky, ktoré chcete pridať do zoznamu. Ak chcete exportovať existujúci zoznam do súboru (vo formáte *.txt*), vyberte z kontextového menu možnosť **Exportovať**.

Zoznam povolených IP adries	E-maily prichádzajúce z IP adries uvedených na tomto zozname budú automaticky doručené príjemcom. Obsah e□mailových správ nebude kontrolovaný.
Zoznam blokovaných IP adries	Automaticky zablokuje e-mailové správy prichádzajúce zo zadaných IP adries.
Zoznam ignorovaných IP adries	Zoznam IP adries, ktoré budú počas klasifikácie ignorované. Obsah e□mailových správ bude kontrolovaný.
Zoznam povolených odosielateľov	E-maily prichádzajúce od odosielateľov alebo z domén na tomto zozname budú doručené príjemcom. Pri vyhodnotení sa použije iba jeden odosielateľ alebo celá doména podľa nižšie uvedenej priority: 1.SMTP 'MAIL FROM' adresa 2.Hlavička "Return-Path:" 3.Hlavička "X-Env-Sender:" 4.Hlavička "From:" 5.Hlavička "Sender:" 6.Hlavička "X-Apparently-From:"
Zoznam blokovaných odosielateľov	Doručenie e-mailov od odosielateľov alebo z domén na tomto zozname bude blokované. Pri vyhodnotení sa použijú všetci zistení odosielatelia alebo celé domény: SMTP 'MAIL FROM' adresa Hlavička "Return-Path:" Hlavička "X-Env-Sender:" Hlavička "From:" Hlavička "Sender:" Hlavička "X-Apparently-From:"

Gmail: Anti□Phishing

Zapnúť Anti-Phishing pre Gmail
Ak je táto možnosť povolená, daná funkcia je aktivovaná a môžete konfigurovať podrobné nastavenia.
Pri výskyte objektu
- **Žiadna akcia** – nevykoná sa žiadna akcia a e-mail so škodlivou prílohou bude doručený príjemcovi.
- **Presunúť do nevyžiadanej pošty** – e-mail bude presunutý medzi nevyžiadanú poštu.
- **Presunúť do koša** – e-mail bude presunutý do koša.
- **Odstrániť správu** – e□mail bude zmazaný
- **Presunúť správu do karantény** – pôvodný e-mail bude zmazaný a jeho kópia bude uložená do karantény. Ak sa rozhodnete uvoľniť e-mail z karantény, príjemcovi bude doručený v podobe prílohy, ktorá bude pripojená k novému e-mailu.

Označiť predmet správy
Ak je táto možnosť zapnutá, môžete upraviť šablóny pridávané do predmetu infikovaných správ.
Text pre označenie predmetu správy
Do predmetu infikovaných správ môžete pridať vlastné označenie.
Upozorniť vlastníka e-mailovej schránky
Ak je táto možnosť povolená, používateľ dostane v prípade zachytenia detekcie notifikačný e-mail.
Upozorniť správcu
Zadajte e-mailovú adresu (pre pridanie viacerých adries stlačte Enter), na ktorú budú odoslané notifikačné e-maily vždy, keď sa nájde detekcia.

Nastavenia ochrany pre OneDrive

V tejto kapitole nájdete informácie o nastaveniach pre OneDrive: Všeobecné a OneDrive: Antimalvér.

OneDrive: Všeobecné

ESET LiveGrid®Systém spätnej väzby
Dáta budú odoslané do ESET Research Lab na ďalšiu analýzu. Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.
Zapisovať všetky objekty do protokolu
Ak je táto možnosť označená, všetky výsledky kontroly (vrátane čistých) budú zobrazené v protokoloch kontroly. Politika uchovávania údajov týkajúca sa čistých výsledkov kontroly predstavuje tri dni. Výsledky kontroly staršie ako 3 dni budú natrvalo odstránené.

OneDrive: Antimalvér

OneDrive: Antimalvér
Ak je táto možnosť povolená, daná funkcia je aktivovaná a môžete konfigurovať podrobné nastavenia.
Hlásenia a ochrana s využitím strojového učenia
Súčasťou detekčného jadra je teraz aj pokročilé strojové učenie – pokročilá vrstva ochrany, ktorá zlepšuje detekciu. Pred úpravou prahu (alebo úrovne) v rámci kategórie Hlásenia si prečítajte nižšie uvedené informácie.
Pri výskyte objektu
- **Žiadna akcia** – nevykoná sa žiadna akcia a súbor zostane vo OneDrive.
- **Presunúť do koša** – súbor bude presunutý do koša.
- **Nahradiť** – obsah pôvodného súboru bude nahradený textom definovaným v poli Text pre nahradenie súboru.
- **Presunúť do karantény** – pôvodný súbor bude presunutý do koša a zároveň skopírovaný do karantény Keď je súbor uvoľnený, súbor zmazaný v minulosti ostane v koši a nová kópia súboru bude odovzdaná do pôvodného priečinka OneDrive.

Text pre nahradenie súboru
Nahradí prílohu textovým súborom obsahujúcim podrobné informácie o vykonanej akcii.
Upozorniť vlastníka
Ak je táto možnosť povolená, používateľ dostane v prípade zachytenia detekcie notifikačný e-mail.
Upozorniť správcu
Zadajte e-mailovú adresu (pre pridanie viacerých adries stlačte Enter), na ktorú budú odoslané notifikačné e-maily vždy, keď sa nájde detekcia.

Nastavenia ochrany pre Disk Google

V tejto kapitole nájdete informácie o nastaveniach pre Disk Google: Všeobecné a Disk Google: Antimalvér.

Disk Google: Všeobecné

ESET LiveGrid®Systém spätnej väzby
Dáta budú odoslané do ESET Research Lab na ďalšiu analýzu. Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.
Zapisovať všetky objekty do protokolu
Ak je táto možnosť označená, všetky výsledky kontroly (vrátane čistých) budú zobrazené v protokoloch kontroly. Politika uchovávania údajov týkajúca sa čistých výsledkov kontroly predstavuje tri dni. Výsledky kontroly staršie ako 3 dni budú natrvalo odstránené.

Disk Google: Antimalvér

Disk Google: Antimalvér
Ak je táto možnosť povolená, daná funkcia je aktivovaná a môžete konfigurovať podrobné nastavenia.
Hlásenia a ochrana s využitím strojového učenia
Súčasťou detekčného jadra je teraz aj pokročilé strojové učenie – pokročilá vrstva ochrany, ktorá zlepšuje detekciu. Pred úpravou prahu (alebo úrovne) v rámci kategórie Hlásenia si prečítajte nižšie uvedené informácie.
Pri výskyte objektu
- **Žiadna akcia** – nevykoná sa žiadna akcia a súbor zostane na Disku Google
- **Presunúť do koša** – súbor bude presunutý do koša.
- **Nahradiť** – obsah pôvodného súboru bude nahradený textom definovaným v poli Text pre nahradenie súboru.
- **Presunúť do karantény** – pôvodný súbor bude presunutý do koša a zároveň skopírovaný do karantény
- **Odstrániť** – pôvodný súbor sa natrvalo odstráni z Disku Google.

Text pre nahradenie súboru
Nahradí prílohu textovým súborom obsahujúcim podrobné informácie o vykonanej akcii.
Upozorniť vlastníka
Ak je táto možnosť povolená, používateľ dostane v prípade zachytenia detekcie notifikačný e-mail.
Upozorniť správcu
Zadajte e-mailovú adresu (pre pridanie viacerých adries stlačte Enter), na ktorú budú odoslané notifikačné e-maily vždy, keď sa nájde detekcia.

Nastavenia ochrany pre Tímové skupiny

V tejto kapitole nájdete informácie o nastaveniach pre Tímové skupiny: Všeobecné a Tímové skupiny: Antimalvér.

Tímové skupiny: Všeobecné

ESET LiveGrid®Systém spätnej väzby
Dáta budú odoslané do ESET Research Lab na ďalšiu analýzu. Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.
Zapisovať všetky objekty do protokolu
Ak je táto možnosť označená, všetky výsledky kontroly (vrátane čistých) budú zobrazené v protokoloch kontroly. Obdobie uchovávania výsledkov kontroly je 3 dni. Výsledky kontroly staršie ako 3 dni budú natrvalo odstránené.

Tímové skupiny: Antimalvér

Tímové skupiny: Antimalvér
Ak je táto možnosť povolená, daná funkcia je aktivovaná a môžete konfigurovať podrobné nastavenia.
Hlásenia a ochrana s využitím strojového učenia
Súčasťou detekčného jadra je teraz aj pokročilé strojové učenie – pokročilá vrstva ochrany, ktorá zlepšuje detekciu. Pred úpravou prahu (alebo úrovne) v rámci kategórie Hlásenia si prečítajte nižšie uvedené informácie.
Pri výskyte objektu
- **Žiadna akcia** – nevykoná sa žiadna akcia, súbor zostane nezmenený.
- **Presunúť do koša** – súbor bude presunutý do koša služby Teams.
- **Nahradiť** – obsah pôvodného súboru bude nahradený textom definovaným v poli Text pre nahradenie súboru.
- **Presunúť do karantény** – pôvodný súbor bude presunutý do koša služby Teams a zároveň skopírovaný do karantény. Keď je súbor uvoľnený z karantény, zmazaný súbor ostane v koši a nová kópia súboru bude vrátená do pôvodného priečinka.

Text pre nahradenie súboru
Nahradí prílohu textovým súborom obsahujúcim podrobné informácie o vykonanej akcii.
Upozorniť vlastníka
Ak je táto možnosť povolená, používateľ dostane v prípade zachytenia detekcie notifikačný e-mail.
Upozorniť správcu
Zadajte e-mailovú adresu (pre pridanie viacerých adries stlačte Enter), na ktorú budú odoslané notifikačné e-maily vždy, keď sa nájde detekcia.

Nastavenia ochrany pre Lokality SharePoint

V tejto kapitole nájdete informácie o nastaveniach pre Lokality SharePoint: Všeobecné a Lokality SharePoint: Antimalvér.

Lokality SharePoint: Všeobecné

ESET LiveGrid®Systém spätnej väzby
Dáta budú odoslané do ESET Research Lab na ďalšiu analýzu. Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.
Zapisovať všetky objekty do protokolu
Ak je táto možnosť označená, všetky výsledky kontroly (vrátane čistých) budú zobrazené v protokoloch kontroly. Obdobie uchovávania výsledkov kontroly je 3 dni. Výsledky kontroly staršie ako 3 dni budú natrvalo odstránené.

Lokality SharePoint: Antimalvér

Lokality SharePoint: Antimalvér
Ak je táto možnosť povolená, daná funkcia je aktivovaná a môžete konfigurovať podrobné nastavenia.
Hlásenia a ochrana s využitím strojového učenia
Súčasťou detekčného jadra je teraz aj pokročilé strojové učenie – pokročilá vrstva ochrany, ktorá zlepšuje detekciu. Pred úpravou prahu (alebo úrovne) v rámci kategórie Hlásenia si prečítajte nižšie uvedené informácie.
Pri výskyte objektu
- **Žiadna akcia** – nevykoná sa žiadna akcia, súbor zostane nezmenený.
- **Presunúť do koša** – súbor bude presunutý do koša SharePoint.
- **Nahradiť** – obsah pôvodného súboru bude nahradený textom definovaným v poli Text pre nahradenie súboru.
- **Presunúť do karantény** – pôvodný súbor bude presunutý do koša SharePoint a zároveň skopírovaný do karantény. Keď je súbor uvoľnený z karantény, zmazaný súbor ostane v koši a nová kópia súboru bude vrátená do pôvodného priečinka.

Text pre nahradenie súboru
Nahradí prílohu textovým súborom obsahujúcim podrobné informácie o vykonanej akcii.
Upozorniť vlastníka
Ak je táto možnosť povolená, používateľ dostane v prípade zachytenia detekcie notifikačný e-mail.
Upozorniť správcu
Zadajte e-mailovú adresu (pre pridanie viacerých adries stlačte Enter), na ktorú budú odoslané notifikačné e-maily vždy, keď sa nájde detekcia.

Nastavenia ochrany pre ESET LiveGuard Advanced

Ak chcete používať funkciu ESET LiveGuard Advanced, nakonfigurujte politiku, ktorá povolí zasielanie vzoriek na analýzu do ESET LiveGuard Advanced. Používatelia alebo skupiny, ktorým túto politiku priradíte, budú zabezpečení dodatočnou ochranou. Súbory, ktoré boli odoslané na analýzu do ESET LiveGuard Advanced, sú uvedené na karte Odoslané súbory. Zasielajú sa len nové, doposiaľ neznáme podozrivé vzorky. Súbory, ktoré sa na základe hashu identifikujú ako škodlivé, už nie sú posielané na analýzu do ESET LiveGuard Advanced.

Výsledky z ESET LiveGuard Advanced si môžete pozrieť v Protokoloch kontroly (Exchange Online, OneDrive, Tímové skupiny alebo Lokality SharePoint) pod označením Malvér.

ESET LiveGuard Advanced

Ak je táto možnosť povolená, daná funkcia je aktivovaná a môžete konfigurovať podrobné nastavenia.

> Spolu s funkciou ESET LiveGuard Advanced sa automaticky zapne aj systém spätnej väzby ESET LiveGrid®. Dáta budú odoslané do ESET Research Lab na ďalšiu analýzu. Viac informácií o ESET LiveGrid® nájdete v slovníku pojmov.

Prah detekcie

Položky s výslednou úrovňou zodpovedajúcou alebo prevyšujúcou zvolený prah detekcie sa budú považovať za hrozby.

Automatické odosielanie podozrivých vzoriek (roletové menu)

Toto nastavenie sa týka systému ESET LiveGrid® a na výber sú nasledujúce možnosti: Všetko, Všetko okrem dokumentov, Žiadny.

Automatické odosielanie podozrivých vzoriek (prepínače)

Vyberte, aké typy súborov sa budú odosielať do ESET LiveGuard Advanced v prípade, že obsahujú podozrivý kód pripomínajúci hrozby alebo vykazujú nezvyčajné správanie či charakteristiky:

- **Spustiteľné súbory** – .exe, .dll, .sys
- **Archívy** – .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- **Skripty** – .bat, .cmd, .hta, .js, .vbs, .js, .ps1
- **Iné** – .jar, .reg, .msi, .swf, .lnk

Odstrániť podozrivé vzorky zo serverov spoločnosti ESET

Vyberte, kedy sa majú odstrániť vzorky, ktoré boli zaslané na analýzu. Vzorky sa vymažú z cloudu ESET LiveGuard Advanced: Nikdy, Po 30 dňoch, Okamžite po analýze.

Dokumenty

Pomocou prepínača môžete povoliť odosielanie dokumentov balíka Microsoft Office, PDF a iných typov dokumentov na analýzu do ESET LiveGuard Advanced.

Odstrániť dokumenty zo serverov spoločnosti ESET

Zaslané súbory vo formáte dokumentu sa vymažú z cloudu ESET LiveGuard Advanced: Nikdy, Po 30 dňoch, Okamžite po analýze.

Hlásenia a ochrana s využitím strojového učenia

Detekčné jadro zabezpečuje ochranu pred nebezpečnými útokmi ohrozujúcimi systém. Zahŕňa kontrolu súborov, e□mailov a sieťovej komunikácie. V prípade zachytenia škodlivého objektu sa začne okamžitá oprava. Detekčné jadro dokáže infiltráciu eliminovať zablokovaním a následným vyliečením, odstránením alebo presunutím do karantény.

Rezidentná ochrana s využitím strojového učenia

Súčasťou detekčného jadra je teraz aj pokročilé strojové učenie – pokročilá vrstva ochrany, ktorá zlepšuje detekciu. Viac o tomto type ochrany sa môžete dočítať v slovníku pojmov. Môžete nakonfigurovať úrovne hlásenia pre tieto kategórie:

Malvér

Počítačový vírus je škodlivý kód pripojený k existujúcim súborom v počítači. Termín „vírus“ sa však často používa nesprávne. Presnejším výrazom je „malvér“ (škodlivý softvér). Detekciu malvéru zabezpečuje modul detekčného jadra v kombinácii s komponentom strojového učenia. Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.

Potenciálne nechcené aplikácie

Potenciálne nechcená aplikácia je softvér, ktorého cieľ nie je jednoznačne škodlivý. Môže však nainštalovať ďalší neželaný softvér, zmeniť správanie zariadenia, vykonávať neschválené alebo neočakávané operácie bez vedomia používateľa, prípadne mať iné nejasné ciele.
Táto kategória zahŕňa softvér zobrazujúci reklamu, softvér sťahujúci ďalší softvér, rôzne dodatočné panely s nástrojmi pre prehliadače, softvér so zavádzajúcim správaním, softvér, ktorý inštaluje ďalší softvér, softvér na sledovanie atď.
Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.

Potenciálne podozrivé aplikácie

Podozrivá aplikácia je softvér, ktorý je skomprimovaný pomocou komprimačného nástroja alebo chrániacich nástrojov. Tieto aplikácie sú často používané na zabránenie reverznému inžinierstvu alebo na skrytie obsahu spustiteľných súborov (napr. malvéru), a to špeciálnymi metódami kompresie a/alebo šifrovania.
Táto kategória zahŕňa: všetky neznáme aplikácie skomprimované komprimačnými nástrojmi alebo chrániacimi nástrojmi používanými na kompromáciu malvéru.

Potenciálne nebezpečné aplikácie

Toto označenie sa používa pre legitímny komerčný softvér, ktorý môže byť zneužitý. Potenciálne nebezpečné aplikácie predstavujú v prevažnej miere komerčný a legitímny softvér, avšak v nesprávnych rukách môže dôjsť k ich zneužitiu na nekalé účely.
Táto kategória predstavuje programy, akými sú napr. nástroje určené na prelomenie ochrany softvéru, generátory licenčných kľúčov, nástroje vzdialeného prístupu, aplikácie určené na prelomenie hesiel a keyloggery (program, ktorý zaznamenáva každé stlačenie klávesu používateľom). Táto možnosť je v predvolených nastaveniach

zakázaná.
Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.

Hlásenia

Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia. Prah hlásení môžete nastaviť tak, aby lepšie vyhovoval vášmu prostrediu a vašim potrebám. Neexistuje len jedna správna konfigurácia. Preto vám odporúčame, aby ste monitorovali správanie vo svojom prostredí a rozhodli sa, či nie je pre vás vhodnejšie iné nastavenie Hlásení.

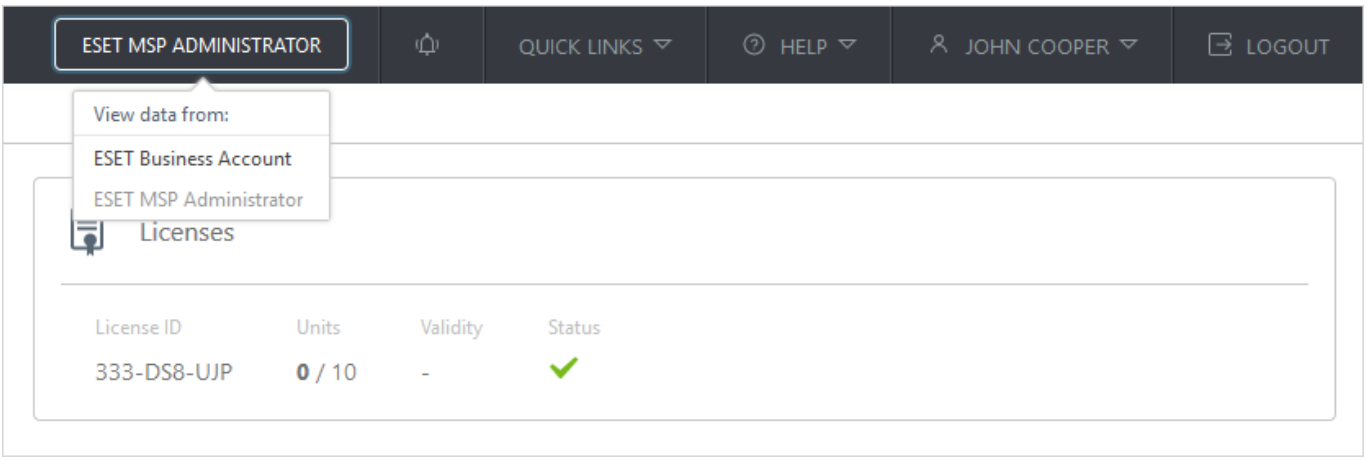
Hlásenia neovplyvňujú, čo sa stane so zachytenými objektmi. Hlásenia len posunú informáciu príslušnej vrstve ochrany, ktorá primeraným spôsobom zakročí.

Prísne	**Hlásenia nastavené na maximálnu citlivosť. Hlásené sú viaceré detekcie. Hoci sa toto nastavenie môže javiť ako najbezpečnejšie, často býva príliš citlivé, čo môže mať presne opačný účinok.** Prísne nastavenie môže nesprávne identifikovať objekty ako škodlivé, pričom bude s týmito objektmi vykonaná príslušná akcia (podľa nastavení Ochrany).
Vyvážené	Toto nastavenie predstavuje optimálnu rovnováhu medzi výkonom a presnosťou detekcie a počtom nesprávne identifikovaných objektov.
Mierne	Hlásenia sú nakonfigurované tak, aby sa minimalizovali nesprávne identifikované objekty pri súčasnom zachovaní dostatočnej úrovne ochrany. Objekty sú hlásené iba v prípade vysokej pravdepodobnosti a zhody s malvérovým správaním.
Vypnuté	Hlásenia nie sú aktívne. Detekcie nie sú nájdené, nahlásené ani vyliečené. Hlásenia malvéru nie je možné deaktivovať, a preto nie je pri malvéri k dispozícii možnosť Vypnuté.

Správa licencií

Hlavné okno vám poskytuje prehľad o licenciách, ktoré sa načítavajú z portálu ESET Business Account alebo ESET MSP Administrator. Sú tu zobrazené všetky licenčné fondy, lokality a spoločnosti, ktoré sú dostupné v portáli ESET Business Account alebo ESET MSP Administrator. Správa licencií vám umožňuje chrániť alebo zrušiť ochranu používateľov.

Ak máte zaregistrovanú rovnakú e-mailovú adresu na portáli ESET MSP Administrator aj ESET Business Account (jednotné prihlásenie), môžete prepínať medzi zobrazením ESET Business Account a ESET MSP Administrator (hybridný licenčný účet).



Licencia ESET Cloud Office Security vám umožňuje používať funkciu ESET LiveGuard Advanced bez ďalších

poplatkov. Vedľa ID licencie budete vidieť označenie ELG.

Správa licencií cez ESET Business Account

V tejto časti nájdete informácie o licencii a jej využití (názov licenčného fondu, ID licencie, jednotky, platnosť a stav). Licencie a licenčné fondy sa načítavajú z portálu ESET Business Account. Licenčné fondy sú dostupné len v prípade, že máte existujúce lokality v portáli ESET Business Account (lokality sú užitočné v rámci kategorizácie). Jedna jednotka predstavuje ochranu ESET Cloud Office Security pre jedného používateľa v rámci Exchange Online a OneDrive.

> Na každého chráneného používateľa sa využíva jedna licenčná jednotka. Nezáleží pritom na tom, aké služby Microsoft 365 sa používajú. Používateľ so službou Exchange Online alebo OneDrive (alebo oboma) vždy spotrebuje jednu licenčnú jednotku.
> Licenčnú jednotku nevyužívajú tímové skupiny ani lokality SharePoint.

Každý nový používateľ bude zobrazený v sekcii Používatelia pod Nechránené. Ak používate automatickú ochranu podľa nájomníka alebo skupiny, noví používatelia budú chránení automaticky a zobrazia sa pod Chránené.
V rámci ochrany používateľov máte dve možnosti:

- **Automatická ochrana podľa nájomníka alebo skupiny (odporúča sa)** – bez potreby údržby, každý nový používateľ, ktorý je členom Azure AD skupiny alebo patrí pod nájomníka, bude automaticky chránený. Podrobnosti nájdete nižšie.
- **Ochrana individuálnych používateľov** – vyžaduje si správu a ochranu budete musieť aktivovať manuálne pre každého nového používateľa.

Ochrana používateľov (bez licenčného fondu)

1. Kliknite na **Ochrániť**.
2. Vyberte nájomníka alebo skupinu, v rámci ktorej budú používatelia chránení automaticky, a kliknite na **Ochrániť**. Ak chcete ochrániť konkrétnych používateľov samostatne, vyberte príslušných používateľov a kliknite na tlačidlo **Ochrániť**. Používatelia sú teraz chránení prostredníctvom prednastavenej politiky.
3. V prípade potreby nastavte pre používateľov vlastnú politiku v sekcii Politiky.

Ochrana používateľov (s použitím licenčného fondu)

1. Vyberte licenčný fond a kliknite na ikonu troch bodiek > **Zobraziť podrobnosti** vedľa licenčného fondu.
2. Kliknite na **Ochrániť**.
3. Vyberte nájomníka alebo skupinu, v rámci ktorej budú používatelia chránení automaticky, a kliknite na **Ochrániť**. Ak chcete ochrániť konkrétnych používateľov samostatne, vyberte príslušných používateľov a kliknite na tlačidlo **Ochrániť**. Používatelia sú teraz chránení prostredníctvom prednastavenej politiky.
4. V prípade potreby nastavte pre používateľov vlastnú politiku v sekcii Politiky.

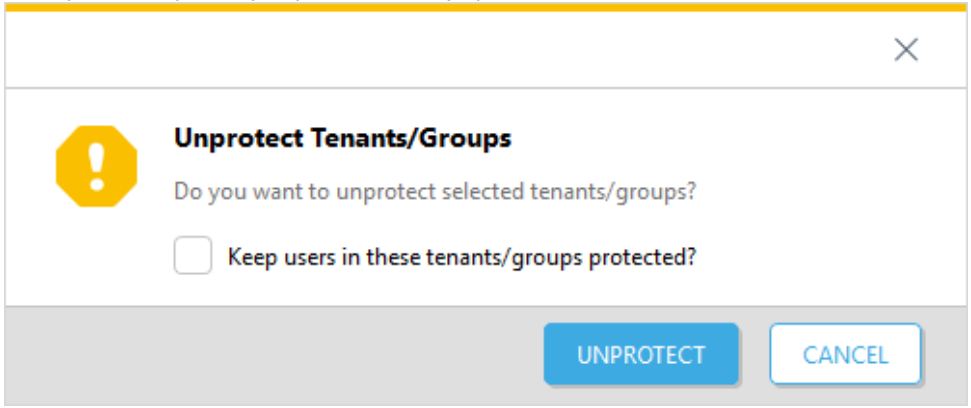
> Uistite sa, že máte dostatok licenčných jednotiek, najmä pri používaní automatickej ochrany, keď počet používateľov narastá. Po spotrebovaní všetkých licenčných jednotiek nebude môcť byť poskytnutá ochrana žiadnemu novému používateľovi, ktorý sa stane členom skupiny alebo pripadne pod nájomníka. Ochrana existujúcich používateľov zostane bez zmeny.
> Ak máte dočasne málo licenčných jednotiek a chcete chrániť konkrétnych používateľov, vypnite automatickú ochranu a manuálne aktivujte ochranu vybraným používateľom z nechránenej skupiny. Keď licenčné fondy navýšite o viac jednotiek, môžete sa vrátiť k automatickej ochrane pre jednoduchšiu správu.

Presunúť

Ak chcete presúvať používateľov medzi licenčnými fondmi a vykonávať pokročilejšie operácie s licenciami, prejdite na portál ESET Business Account.

Zrušiť ochranu

1. Vyberte jednotlivých používateľov, nájomníka alebo skupinu a kliknite na tlačidlo **Zrušiť ochranu**.
2. Ak sa rozhodnete zrušiť automatickú ochranu nájomníka alebo skupiny, zobrazí sa otázka **Chcete ponechať používateľov patriacich pod týchto nájomníkov/skupiny chránených?**. Ak sa rozhodnete nepoužiť túto možnosť, používatelia už nebudú naďalej chránení. Ak túto možnosť označíte, automatická ochrana nájomníka alebo skupiny bude deaktivovaná a zmení sa na ochranu individuálnych používateľov. Existujúci používatelia budú stále chránení, ale všetkých novo pridaných používateľov je potrebné chrániť manuálne.



V tejto časti nájdete informácie o licencii a jej využití (spoločnosť zákazníka, ID licencie, jednotky a stav).

> Na každého chráneného používateľa sa využíva jedna licenčná jednotka. Nezáleží pritom na tom, aké služby Microsoft 365 sa používajú. Používateľ so službou Exchange Online alebo OneDrive (alebo oboma) vždy spotrebuje jednu licenčnú jednotku.
> Licenčnú jednotku nevyužívajú tímové skupiny ani lokality SharePoint.

Každý nový používateľ bude zobrazený v sekcii Používatelia pod **Nechránené**. Ak používate automatickú ochranu podľa nájomníka alebo skupiny, noví používatelia budú chránení automaticky a zobrazia sa pod **Chránené**.
V rámci ochrany používateľov máte dve možnosti:

- **Automatická ochrana podľa nájomníka alebo skupiny (odporúča sa)** – bez potreby údržby, každý nový používateľ, ktorý je členom Azure AD skupiny alebo patrí pod nájomníka, bude automaticky chránený. Podrobnosti nájdete nižšie.
- **Ochrana individuálnych používateľov** – vyžaduje si správu a ochranu budete musieť aktivovať manuálne pre každého nového používateľa.

Ochrániť používateľov

1. Kliknite na **Ochrániť**.
2. Vyberte nájomníka alebo skupinu, v rámci ktorej budú používatelia chránení automaticky, a kliknite na **Ochrániť**. Ak chcete ochrániť konkrétnych používateľov samostatne, vyberte príslušných používateľov a kliknite na tlačidlo **Ochrániť**. Používatelia sú teraz chránení prostredníctvom prednastavenej politiky.
3. V prípade potreby nastavte pre používateľov vlastnú politiku v sekcii Politiky.

> Uistite sa, že máte dostatok licenčných jednotiek, najmä pri používaní automatickej ochrany, keď počet používateľov narastá. Po spotrebovaní všetkých licenčných jednotiek nebude môcť byť poskytnutá ochrana žiadnemu novému používateľovi, ktorý sa stane členom skupiny alebo pripadne pod nájomníka. Ochrana existujúcich používateľov zostane bez zmeny.
> Ak máte dočasne málo licenčných jednotiek a chcete chrániť konkrétnych používateľov, vypnite automatickú ochranu a manuálne aktivujte ochranu vybraným používateľom z nechránenej skupiny. Keď licenčné fondy navýšite o viac jednotiek, môžete sa vrátiť k automatickej ochrane pre jednoduchšiu správu.

Zrušiť ochranu

1. Vyberte jednotlivých používateľov, nájomníka alebo skupinu a kliknite na tlačidlo **Zrušiť ochranu**.
2. Ak sa rozhodnete zrušiť automatickú ochranu nájomníka alebo skupiny, zobrazí sa otázka **Chcete ponechať používateľov patriacich pod týchto nájomníkov/skupiny chránených?**. Ak sa rozhodnete nepoužiť túto možnosť, používatelia už nebudú naďalej chránení. Ak túto možnosť označíte, automatická ochrana nájomníka alebo skupiny bude deaktivovaná a zmení sa na ochranu individuálnych používateľov. Existujúci používatelia budú stále chránení, ale všetkých novo pridaných používateľov je potrebné chrániť manuálne.

Prístup používateľa k ESET Cloud Office Security pre prezeranie dát konkrétnej spoločnosti

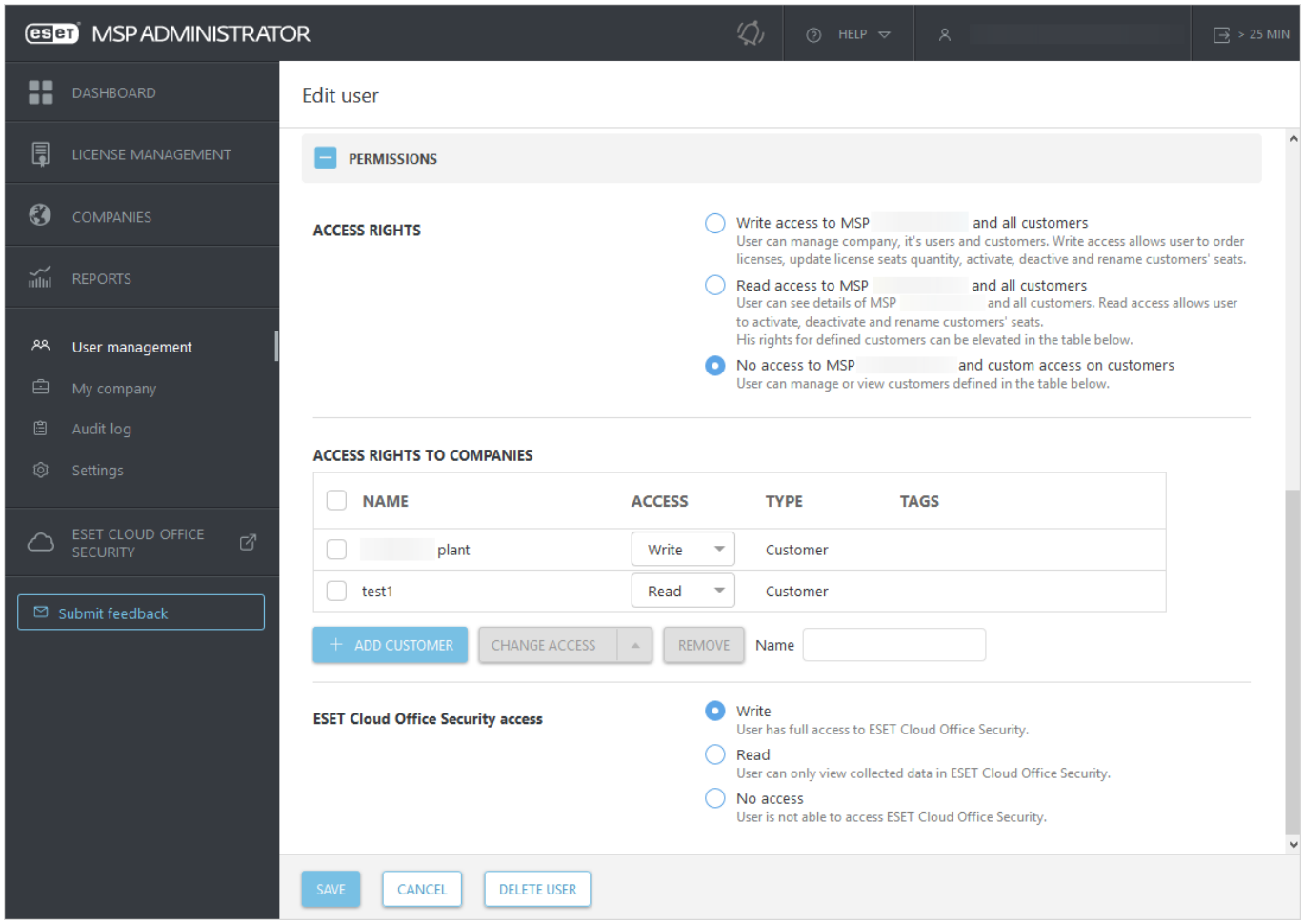
V multitenantnom prostredí môžete poskytnúť používateľovi prístup k ESET Cloud Office Security a umožniť mu prehliadať iba dáta konkrétnej spoločnosti (s právami na čítanie alebo zápis). Túto možnosť zvyčajne využívajú MSP.

Na portáli ESET MSP Administrator nakonfigurujte prístupové práva pre používateľa tak, že mu priradíte povolenie na prístup k spoločnosti na úrovni **Zápis** a rovnako mu pridelíte prístupové práva na **Zápis** do ESET Cloud Office Security:

1. Do ESET MSP Administrator sa prihláste ako správca.

2. Upravte vybraného používateľa a v sekcii Oprávnenia > **Prístup ku spoločnosti** vyberte možnosť **Zápis**. Používateľ uvidí iba priradenú spoločnosť s jej licenčným fondom.

3. Nastavte prístup na **Zápis** do ESET Cloud Office Security, aby používateľ mohol chrániť spoločnosť pridaním nájomníka. Používateľ s prístupom na Čítanie nemôže pridať ani odstrániť nájomníka.



Ako globálne nastavenie môžete nakonfigurovať len jeden typ prístupu do ESET Cloud Office Security, ktorý bude platiť pre všetky spoločnosti (ak má používateľ priradených viacero spoločností).

Protokol auditu

Zaznamenáva zmeny v konfigurácii produktu ESET Cloud Office Security alebo v stave ochrany. V protokole auditu sú zaznamenané všetky aktivity v tom poradí, v akom sa uskutočnili. Protokoly auditu uchovávajú informácie o konkrétnej operácii alebo udalosti. Protokoly auditu sa vytvárajú pri každej zmene alebo vytvorení objektu v rámci konzoly ESET Cloud Office Security (napríklad licenčného fondu, používateľa, politiky, reportu alebo položky v karanténe, ako sú prílohy).

Keď v pravom hornom rohu kliknete na ikonu ozubeného kolesa a z kontextového menu vyberiete možnosť **Exportovať do súboru CSV**, tabuľku môžete exportovať do formátu *CSV* a pracovať s ňou aj v iných aplikáciách.

Kliknutím na ikonu otvoríte bočný panel so súhrnom konkrétneho záznamu protokolu auditu. Ak chcete získať podrobnejšie informácie, kliknite na trojbodkovú ikonu a vyberte možnosť **Zobraziť podrobnosti**.

Sekcia	Podrobnosti
Základné informácie	Zobrazuje všeobecné údaje z protokolu auditu (Výskyt, Akcia, Závažnosť, Výsledok, Sekcia).
Používateľ	Zobrazuje informácie o používateľovi, ktorý vykonal akciu alebo zmenu, vrátane e□mailovej adresy a IP adresy používateľa.

Sekcia	Podrobnosti
Zmeny	Podrobnosti o vykonaných zmenách.
Pôvodné nastavenia	Zobrazuje pôvodné nastavenie/a politiky.
Nové nastavenia	Zobrazuje aktuálne nastavenie/a politiky.
Objekty	Zobrazuje objekty ovplyvnené zmenou alebo akciou (používateľ, politika, príloha atď.).

Používateľov môžete filtrovať podľa niekoľkých kritérií. Kliknite na **Pridať filter** a z roletového menu vyberte typ filtra alebo zadajte reťazec, podľa ktorého chcete vyhľadávať (môžete tiež skombinovať viacero kritérií hľadania):

Pridať filter	Použitie
Akcia	Vyberte si jednu z dostupných akcií.
Objekt	Zadajte platný názov objektu.
Stav	Vyberte si jednu z nasledujúcich možností: Úspešné, Neúspešné, Spustené alebo Čiastočne úspešné.
Používateľ	Zadajte používateľa, ktorý vykonal zmeny.
Závažnosť	Vyberte úroveň závažnosti: Nízka, Stredná alebo Vysoká.
Výskyt od/Výskyt do	Filtrovanie podľa času výskytu. Použite filter Výskyt od a kliknite na dátum, ak chcete zobraziť len záznamy novšie ako zvolený dátum. Použite filter Výskyt do na zobrazenie záznamov, ktoré vznikli pred zvoleným dátumom, alebo použite oba filtre a nastavte požadovaný časový rozsah.
Iniciované systémom	Filtrovanie záznamov vytvorených systémom.

Odoslanie spätnej väzby

Ak chcete odoslať spätnú väzbu, v konzole ESET Cloud Office Security použite panel s nástrojmi v pravom hornom rohu, prejdite kurzorom myši nad **Pomocníka** a kliknite na **Odoslať spätnú väzbu**. Následne vyberte možnosť **Podeľte sa s nami o svoj názor** alebo **Nahlásiť problém alebo chybu**.

Technická podpora

Použite nasledujúce odkazy poskytujúce pomoc pri riešení známych problémov:

Hľadanie v Databáze znalostí spoločnosti ESET

Databáza znalostí spoločnosti ESET Obsahuje odpovede na najčastejšie kladené otázky, ako aj odporúčané riešenia rozličných problémov. Pravidelná aktualizácia databázy znalostí pracovníkmi spoločnosti ESET z nej robí najrýchlejší nástroj na riešenie rozličných druhov problémov.

Návšteva ESET Security Forum

Fórum technickej podpory ESET Fórum umožňuje používateľom produktov ESET jednoducho získať hľadané riešenia problémov, ako aj pomôcť iným. Do fóra môžete pridať akýkoľvek problém alebo otázku týkajúcu sa vašich produktov ESET.

Kontaktovanie technickej podpory

Kontaktný formulár technickej podpory ESET Vyplňte formulár s uvedením podrobností vrátane popisu problému.

Kontaktovanie lokálneho partnera ESET

Obráťte sa na lokálneho partnera spoločnosti ESET Vyhľadajte kontaktné údaje na partnera vo vašom regióne v licenčnom e-maile, ktorý sme vám odoslali.

Odoslanie spätnej väzby

Odošlite spätnú väzbu Podeľte sa s nami o svoj názor, prípadne nahláste problém alebo chybu.

Návrh zlepšenia Online pomocníka

Svoje hodnotenie a spätnú väzbu ku konkrétnej téme spracovanej v Online pomocníkovi môžete zverejniť kliknutím na odkaz **Boli tieto informácie užitočné?** uvedený pod príslušnou stránkou pomocníka. Dajte nám vedieť, či vám obsah pomohol alebo ako ho podľa vás môže dokumentarista zlepšiť.

Dostupnosť služieb

ESET Status Portal zobrazuje aktuálny stav cloudových služieb ESET, plánované odstávky a minulé incidenty. Ak máte problém s podporovanou službou ESET a nevidíte ju uvedenú na portáli ESET Status Portal, kontaktujte technickú podporu spoločnosti ESET.

Monitorovacie tímy interne overujú potenciálne problémy a potvrdené incidenty manuálne zverejňujú a aktualizujú s cieľom zachovať dôveryhodnosť a presnosť. Na portáli ESET Status Portal sa preto zobrazujú s miernym oneskorením. Incidenty s krátkym trvaním nemusia byť zverejnené, ak sa vyriešia ešte pred ich manuálnym potvrdením.

Security for ESET Cloud Office Security

Úvod

Účelom tohto dokumentu je zhrnúť bezpečnostné postupy a bezpečnostné kontroly uplatňované v rámci ESET Cloud Office Security. Bezpečnostné postupy a kontroly sú navrhnuté tak, aby chránili dôvernosť, integritu a dostupnosť informácií o zákazníkoch. Upozorňujeme, že bezpečnostné postupy a kontroly sa môžu meniť.

Rozsah

Tento dokument popisuje bezpečnostné postupy a bezpečnostné kontroly týkajúce sa infraštruktúry ESET Cloud Office Security, ako aj infraštruktúry, organizácie, personálu a prevádzkových procesov spojených s ESET Business Account (ďalej iba „EBA“), ESET Data Framework, ESET LiveGrid, aktualizáciou, Antispamom a ESET Dynamic Threat Defense. Bezpečnostné postupy a kontroly zahŕňajú:

1. Politiky informačnej bezpečnosti
2. Organizácia informačnej bezpečnosti
3. Ľudské zdroje a bezpečnosť
4. Správa aktív
5. Kontrola prístupu
6. Kryptografia
7. Fyzické zabezpečenie a ochrana prostredia
8. Bezpečnosť operácií

9. Bezpečnosť sieťovej komunikácie
10. Akvizícia, vývoj a údržba systému
11. Dodávateľský vzťah
12. Správa incidentov v oblasti informačnej bezpečnosti
13. Aspekty informačnej bezpečnosti v rámci správy kontinuity prevádzky
14. Súlad s požiadavkami

Bezpečnostný koncept

Spoločnosť ESET, spol. s r. o., je držiteľom certifikátu ISO 27001:2013 s integrovaným systémom správy, ktorý pokrýva služby ESET Cloud Office Security, EBA a ďalšie.

Preto koncept informačnej bezpečnosti používa štandard ISO 27001 na implementáciu bezpečnostnej stratégie viacvrstvovej ochrany pri aplikovaní bezpečnostných kontrol na vrstve siete, operačných systémov, databáz, aplikácií, personálu a operačných procesov. Použité bezpečnostné postupy a bezpečnostné kontroly sa majú navzájom prekrývať a dopĺňať.

Bezpečnostné postupy a kontroly

1. Politiky informačnej bezpečnosti

Spoločnosť ESET uplatňuje politiky informačnej bezpečnosti, ktoré pokrývajú všetky aspekty štandardu ISO 27001 vrátane riadenia informačnej bezpečnosti a bezpečnostných kontrol a postupov. Politiky sa každoročne prehodnocujú a po výrazných zmenách aj aktualizujú, čo vedie k ich kontinuálnej vhodnosti, primeranosti a účinnosti.

Spoločnosť ESET vykonáva každoročnú revíziu týchto politík a interné bezpečnostné kontroly s cieľom zaistiť s nimi súlad. V prípade nedodržiavania politík informačnej bezpečnosti sú zamestnanci spoločnosti ESET vystavení disciplinárnemu konaniu a dodávatelia zmluvným sankciám alebo až výpoveďou zmluvy.

2. Organizácia informačnej bezpečnosti

Organizácia informačnej bezpečnosti služby ESET Cloud Office Security pozostáva z viacerých tímov a jednotlivcov zaoberajúcich sa informačnou bezpečnosťou a oblasťou IT vrátane:

- výkonného manažmentu spoločnosti ESET,
- interných bezpečnostných tímov spoločnosti ESET,
- IT tímov zaoberajúcich sa firemnými aplikáciami,
- ostatných podporných tímov.

Záväzky a úlohy v oblasti informačnej bezpečnosti sa prideľujú v súlade so zavedenými politikami informačnej bezpečnosti. Interné procesy sú identifikované a posudzované z hľadiska rizík vyplývajúcich z neoprávnenej alebo neúmyselnej modifikácie či zneužitia aktív spoločnosti ESET. Pri rizikových alebo citlivých činnostiach v spojení s internými procesmi sa na zmiernenie rizika uplatňuje zásada rozdelenia povinností.

Právny tím spoločnosti ESET je zodpovedný za kontakt so štátnymi orgánmi vrátane slovenských regulačných orgánov v oblasti kybernetickej bezpečnosti a ochrany osobných údajov. Interný bezpečnostný tím spoločnosti ESET je zodpovedný za kontakt so záujmovými skupinami, ako napríklad ISACA. Tím výskumníkov spoločnosti ESET je zodpovedný za komunikáciu s ostatnými spoločnosťami zameranými na bezpečnosť a so širšou komunitou z oblasti kybernetickej bezpečnosti.

Informačná bezpečnosť sa pri riadení projektov zohľadňuje pomocou aplikovaného rámca riadenia projektov

od koncepcie až po dokončenie projektu.

Práca na diaľku a práca z domu sú kryté politikou implementovanou na mobilných zariadeniach, ktorá zahŕňa používanie silnej kryptografickej ochrany údajov na mobilných zariadeniach počas prenosu cez nedôveryhodné siete. Bezpečnostné kontroly na mobilných zariadeniach sú navrhnuté tak, aby fungovali nezávisle od interných sietí a interných systémov spoločnosti ESET.

3. Ľudské zdroje a bezpečnosť

Spoločnosť ESET používa štandardné postupy v oblasti ľudských zdrojov vrátane politík určených na dodržiavanie informačnej bezpečnosti. Tieto postupy sa vzťahujú na celý životný cyklus zamestnanca a platia pre všetky tímy, ktoré majú prístup k prostrediu ESET Cloud Office Security.

4. Správa aktív

Infraštruktúra ESET Cloud Office Security je zahrnutá v inventároch aktív spoločnosti ESET s výhradným vlastníctvom a pravidlami uplatňovanými podľa typu a citlivosti aktív. Spoločnosť ESET má definovanú internú klasifikačnú schému. Všetky údaje a konfigurácie spojené s ESET Cloud Office Security sú klasifikované ako dôverné.

5. Kontrola prístupu

Politika kontroly prístupu spoločnosti ESET upravuje každý prístup v rámci ESET Cloud Office Security. Kontrola prístupu sa nastavuje na úrovni infraštruktúry, sieťových služieb, operačného systému, databázy a aplikácie. Správa úplného prístupu používateľov na úrovni aplikácie je autonómna. Prihlásenie jedným vstupom v rámci služieb ESET Cloud Office Security a ESET Business Account je riadené centrálnym poskytovateľom identity, ktorý zabezpečuje, že používateľ má prístup len k oprávnenému nájomníkovi. Aplikácia používa štandardné povolenia ESET Cloud Office Security s cieľom presadiť pre nájomníka kontrolu prístupu na základe rolí.

Prístup k backendu je obmedzený výlučne na oprávnené osoby a roly. Na správu prístupu zamestnancov spoločnosti ESET k infraštruktúre a sieťam služby ESET Cloud Office Security sa používajú štandardné procesy ESET pre (de)registráciu používateľov, ich pridávanie alebo odoberanie, správu oprávnení a kontrolu prístupových práv používateľov.

Na ochranu prístupu ku všetkým údajom týkajúcim sa služby ESET Cloud Office Security sa používa silné overovanie.

6. Kryptografia

Silná kryptografia slúži na šifrovanie uložených a prenášaných údajov s cieľom ochrániť údaje v rámci služby ESET Cloud Office Security. Certifikáty pre verejné služby vydáva všeobecne uznávaná a dôveryhodná certifikačná autorita. Kľúče v rámci infraštruktúry ESET Cloud Office Security sa spravujú prostredníctvom internej infraštruktúry verejných kľúčov spoločnosti ESET. Údaje uložené v databáze sú chránené šifrovacími kľúčmi generovanými cloudom. Všetky zálohované údaje sú chránené spravovanými kľúčmi ESET.

7. Fyzické zabezpečenie a ochrana prostredia

Keďže ESET Cloud Office Security a ESET Business Account sú cloudové služby, spoliehame sa na cloudovú platformu Microsoft Azure, ktorá zaisťuje fyzické zabezpečenie a ochranu prostredia. Microsoft Azure používa certifikované dátové centrá a spoľahlivo chráni uložené údaje. Fyzické umiestnenie dátového centra závisí od výberu oblasti zákazníka.

8. Bezpečnosť operácií

Služba ESET Cloud Office Security je prevádzkovaná automatizovanými prostriedkami na základe prísnych prevádzkových postupov a konfiguračných šablón. Všetky zmeny vrátane zmien konfigurácie a nasadzovania nových balíkov sa pred nasadením do produkcie schvaľujú a testujú v špecializovanom testovacom prostredí. Vývojové, testovacie a produkčné prostredia sú navzájom oddelené. Údaje služby ESET Cloud Office Security sú dostupné len v produkčnom prostredí.

Prostredie služby ESET Cloud Office Security je sledované pomocou prevádzkového monitorovania s cieľom rýchlo identifikovať problémy a zabezpečiť dostatočnú kapacitu všetkých služieb na úrovni siete a hostiteľa.

Všetky konfiguračné údaje sú uložené v našich pravidelne zálohovaných úložiskách, aby bolo možné automaticky obnoviť konfiguráciu prostredia. Zálohované údaje služby ESET Cloud Office Security sa ukladajú lokálne aj externe.

Zálohy sú šifrované a pravidelne testované na obnoviteľnosť v rámci testovania kontinuity prevádzky.

Audit systémov sa vykonáva podľa interných noriem a usmernení. Záznamy a udalosti z infraštruktúry, operačného systému, databázy, aplikačných serverov a bezpečnostných kontrol sa zhromažďujú nepretržite. IT a interné bezpečnostné tímy následne tieto záznamy spracúvajú s cieľom identifikovať prevádzkové a bezpečnostné anomálie a incidenty týkajúce sa informačnej bezpečnosti.

Spoločnosť ESET sa riadi všeobecným technickým procesom správy zraniteľností na riešenie výskytu zraniteľností v infraštruktúre spoločnosti ESET vrátane ESET Cloud Office Security a ďalších produktov ESET. Tento proces zahŕňa proaktívnu kontrolu zraniteľností a opakované penetračné testovanie infraštruktúry, produktov a aplikácií.

Spoločnosť ESET má zavedené interné smernice pre bezpečnosť internej infraštruktúry, sietí, operačných systémov, databáz, aplikačných serverov a aplikácií. Ich dodržiavanie sa kontroluje prostredníctvom technického monitorovania súladu a nášho interného bezpečnostného auditu.

9. Bezpečnosť sieťovej komunikácie

Prostredie ESET Cloud Office Security je segmentované prostredníctvom natívnej cloudovej segmentácie, pričom prístup k sieti je obmedzený len na nevyhnutné služby v rámci sieťových segmentov. Dostupnosť sieťových služieb je zabezpečená pomocou natívnych cloudových kontrol, ako sú zóny dostupnosti, vyrovnávanie zaťaženia a redundancia. Nasadia sa špeciálne komponenty na vyrovnávanie zaťaženia a overovanie sieťovej komunikácie medzi koncovými zariadeniami a inštanciou služby ESET Cloud Office Security. Sieťová komunikácia je nepretržite monitorovaná z hľadiska prevádzkových a bezpečnostných anomálií. Potenciálne útoky je možné vyriešiť pomocou natívnych cloudových kontrol alebo nasadených bezpečnostných riešení. Všetka sieťová komunikácia je šifrovaná prostredníctvom všeobecne dostupných techník vrátane protokolu IPsec a TLS.

10. Akvizícia, vývoj a údržba systému

Vývoj systémov služby ESET Cloud Office Security prebieha v súlade s politikou vývoja bezpečnostného softvéru spoločnosti ESET. Interné bezpečnostné tímy sú súčasťou projektu vývoja služby ESET Cloud Office Security od počiatočnej fázy a dohliadajú na všetky aspekty vývoja a údržby. Interný bezpečnostný tím stanovuje a kontroluje plnenie bezpečnostných požiadaviek v rôznych fázach vývoja softvéru. Bezpečnosť všetkých služieb, vrátane tých novo vyvinutých, sa od ich vydania nepretržite testuje.

11. Dodávateľský vzťah

Príslušný dodávateľský vzťah prebieha podľa platných smerníc spoločnosti ESET, ktoré upravujú celú správu vzťahov a zmluvné požiadavky z hľadiska informačnej bezpečnosti a ochrany osobných údajov. Kvalita

a bezpečnosť služieb poskytovaných poskytovateľom kritických služieb sa pravidelne vyhodnocuje.

12. Správa incidentov v oblasti informačnej bezpečnosti

Správa incidentov v oblasti informačnej bezpečnosti pre službu ESET Cloud Office Security je podobná riadeniu ostatných infraštruktúr ESET a opiera sa o definované postupy riešenia incidentov. Úlohy v rámci riešenia incidentov sú zadefinované a rozdelené medzi viaceré tímy z oblasti IT, bezpečnosti, právnych služieb, ľudských zdrojov, vzťahov s verejnosťou a výkonného manažmentu. Priradenie tímu na riešenie incidentu závisí od roztriedenia incidentov interným bezpečnostným tímom. Tento tím zabezpečí koordináciu ostatných tímov, ktoré incident riešia. Interný bezpečnostný tím je tiež zodpovedný za zhromažďovanie dôkazov k incidentu a získaných poznatkov. Vznik incidentu a jeho riešenie sa oznamuje dotknutým stranám. Právny tím spoločnosti ESET je v prípade potreby zodpovedný za nahlásenie incidentu regulačným orgánom v súlade so všeobecným nariadením o ochrane údajov (GDPR) a aktom EÚ o kybernetickej bezpečnosti transponujúcim smernicu o bezpečnosti sietí a informačných systémov (NIS).

13. Aspekty informačnej bezpečnosti v rámci správy kontinuity prevádzky

Kontinuita prevádzky služby ESET Cloud Office Security je zakódovaná v robustnej architektúre, ktorá maximalizuje dostupnosť poskytovaných služieb. V prípade úplného zlyhania všetkých redundantných uzlov pre súčasti ESET Cloud Office Security alebo službu ESET Cloud Office Security je možná kompletná obnova zo zálohovaných a konfiguračných údajov. Proces obnovy sa pravidelne testuje.

14. Súlad s požiadavkami

Dodržiavanie zmluvných požiadaviek a požiadaviek vychádzajúcich z právnych predpisov pre službu ESET Cloud Office Security sa pravidelne vyhodnocuje a kontroluje podobne ako iné infraštruktúry a procesy spoločnosti ESET, pričom sa tiež neustále prijímajú nevyhnutné kroky pre zabezpečenie súladu s požiadavkami. Spoločnosť ESET je registrovaná ako poskytovateľ digitálnych služieb v oblasti cloud computingu, kam spadajú viaceré služby spoločnosti ESET vrátane ESET Cloud Office Security. Upozorňujeme, že aktivity spoločnosti ESET zamerané na dodržiavanie požiadaviek nemusia nevyhnutne znamenať, že požiadavky zákazníkov v tejto oblasti sú kompletne splnené.

Podmienky používania

S účinnosťou od 23. októbra 2023 | Zobraziť predchádzajúcu verziu podmienok používania | Porovnať zmeny

Táto zmluva o službe ESET Cloud Office Security (ďalej iba „podmienky“) predstavujú špeciálnu zmluvu medzi spoločnosťou ESET, spol. s r. o. so sídlom na adrese Einsteinova 24, 85101 Bratislava, Slovak Republic, zapísanou v Obchodnom registri Okresného súdu Bratislava I, oddiel Sro, vložka číslo 3586/B, IČO: 31333532 (ďalej len „ESET“ alebo „poskytovateľ“) a vami, fyzickou alebo právnickou osobou (ďalej len „vy“ alebo „používateľ“ alebo formulácie vyjadrené v druhej osobe množného čísla), ktorá pristupuje k účtu na správu, k službe ESET Cloud Office Security a ktorá získava prístup k webovému portálu spravovanému spoločnosťou ESET (ďalej iba „účet“), aby ste mohli používať službu ESET Cloud Office Security. Ak používate účet a službu ESET Cloud Office Security (ďalej len spoločne označované ako „produkt“) v mene organizácie, potom s podmienkami súhlasíte v mene danej organizácie a zaručujete sa, že máte právomoc zaviazať ju týmito podmienkami. Označenie „používateľ“ a „vy“ alebo formulácie vyjadrené v druhej osobe množného čísla sa v takomto prípade budú vzťahovať na danú organizáciu. Pozorne si tieto podmienky prečítajte, vzťahujú sa aj na služby poskytované spoločnosťou ESET prostredníctvom produktu alebo vo vzťahu k nemu. Špecifické podmienky používania jednotlivých služieb mimo týchto podmienok sú uvedené pri každej službe a ich prijatie je súčasťou procesu aktivácie služby. Priložené prílohy dopĺňajú tieto podmienky.

Bezpečnosť a ochrana údajov

Účet poskytuje prístup k službám poskytovaným spoločnosťou ESET. Na zaregistrovanie a používanie účtu a na účely poskytovania a údržby služieb, ktoré sa prostredníctvom neho používajú, sa vyžaduje úplné meno používateľa, názov spoločnosti, krajina, platná e-mailová adresa, telefónne číslo, licenčné a štatistické údaje. Týmto súhlasíte so zhromažďovaním údajov a ich prenosom na servery poskytovateľa alebo jeho partnerov na účely zabezpečenia funkčnosti a overenia oprávnenia používať softvér a ochranu práv poskytovateľa. Po uzavretí dohody o týchto podmienkach získajú poskytovateľ alebo jeho partneri oprávnenie prenášať, spracovávať a uchovávať dôležité údaje, ktoré umožnia vašu identifikáciu, na účely poskytovania podpory a plnenia týchto podmienok. Máte oprávnenie používať účet výhradne na účely a spôsobom určeným v týchto podmienkach, individuálnych podmienkach poskytovania služby a dokumentácii.

Za zabezpečenie svojho účtu a prihlasovacích poverení zodpovedáte sami. Spoločnosť ESET nezodpovedá za žiadnu stratu alebo škodu spôsobenú vaším zanedbaním povinnosti udržiavať zabezpečenie. Používateľ je zodpovedný aj za všetky činnosti súvisiace s používaním účtu bez ohľadu na to, či sú oprávnené. V prípade neoprávneného použitia účtu na to poskytovateľa okamžite upozornite.

Na účely poskytovania služby spravovania účtu sa vyžaduje zhromažďovanie údajov o spravovaných zariadeniach, ako aj informácií týkajúcich sa správy (ďalej iba „údaje“). Údaje poskytujete spoločnosti ESET výhradne na účely poskytovania služby spravovania účtu. Údaje sa budú spracovávať a ukladať v súlade s politikami a postupmi zabezpečenia spoločnosti ESET a tiež v súlade so zásadami ochrany osobných údajov.

Podrobné informácie o ochrane súkromia, ochrane osobných údajov a právach ako dotknutej osoby sú uvedené v zásadách ochrany osobných údajov.

Zásady férového používania

Máte povinnosť dodržiavať technické obmedzenia uvedené v dokumentácii. Súhlasíte s tým, že účet a jeho funkcie budete používať výlučne spôsobom, ktorý neobmedzí možnosti iných používateľov na prístup k týmto službám. Poskytovateľ si vyhradzuje právo obmedziť rozsah služieb poskytovaných jednotlivým používateľom tak, aby umožnil využívanie týchto služieb čo najväčšiemu počtu používateľov. Obmedzenie rozsahu služieb môže tiež znamenať úplné ukončenie možnosti používať všetky funkcie účtu a odstránenie údajov a informácií.

Podrobnosti o technických obmedzeniach sú uvedené v sekcii Obmedzenia.

Poloha

Poskytovateľ vám môže umožniť vybrať si z dostupných umiestnení hostiteľa účtu vrátane odporúčaného umiestnenia vybratého poskytovateľom. Beriete na vedomie, že výber iného ako odporúčaného umiestnenia môže mať vplyv na vaše komfortné používanie produktu. Na základe vybratej polohy môžu platiť zmluva o ochrane údajov, ktorá je súčasťou prílohy č. 2 tejto zmluvy, a štandardné zmluvné doložky, ktoré sú súčasťou prílohy č. 3 tejto zmluvy. Spoločnosť ESET si vyhradzuje právo kedykoľvek zmeniť špecifické umiestnenie bez predchádzajúceho upozornenia v záujme zlepšenia služieb poskytovaných spoločnosťou ESET v súlade s vašimi preferenciami umiestnenia (napr. Európska únia).

Softvér

Spoločnosť ESET alebo jej jednotliví dodávatelia vlastnia alebo si uplatňujú autorské práva k softvéru dostupnému ako súčasť produktu (ďalej iba „softvér“). Softvér možno používať iba v súlade s licenčnou dohodou s koncovým používateľom, ktorá je súčasťou prílohy č. 1 tejto dohody. Ďalšie informácie týkajúce sa licencovania, autorských práv, dokumentácie a ochranných známok sú uvedené v dokumente obsahujúcom právne informácie.

Obmedzenia

Účet nesmiete kopírovať, šíriť, oddeľovať jeho časti ani vytvárať od účtu odvodené diela. Pri používaní účtu máte povinnosť dodržiavať tieto obmedzenia:

(a) Účet nesmiete používať, upravovať, prekladať, reprodukovať ani prevádzať práva na používanie účtu alebo jeho častí inak, než je výslovne uvedené v týchto podmienkach.

(b) Účet nesmiete predať, sublicencovať, prenajať ani prenajať si, vypožičať si ho alebo používať na poskytovanie komerčných služieb.

(c) Účet nesmiete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu ani sa iným spôsobom pokúsiť získať zdrojový kód účtu s výnimkou rozsahu, v ktorom je takéto obmedzenie výslovne zakázané zákonom.

(d) Súhlasíte s tým, že budete účet používať iba spôsobom, ktorý je v súlade so všetkými platnými právnymi predpismi v právnom systéme, v ktorom účet používate, najmä v súlade s platnými obmedzeniami vyplývajúcimi z autorského práva a ďalších práv duševného vlastníctva.

Vyhlásenia

AKO POUŽÍVATEĽ TÝMTO UZNÁVATE, ŽE ÚČET, AKO AJ SLUŽBY, SÚ POSKYTOVANÉ „AKO STOJA A LEŽIA“, BEZ VÝSLOVNEJ ALEBO IMPLIKOVANEJ ZÁRUKY AKÉHOKOĽVEK DRUHU A V MAXIMÁLNEJ MIERE DOVOLENEJ APLIKOVATEĽNÝMI ZÁKONMI. ANI POSKYTOVATEĽ, ANI JEHO POSKYTOVATELIA LICENCIÍ ALEBO PRIDRUŽENÉ SPOLOČNOSTI ANI DRŽITELIA AUTORSKÝCH PRÁV NEPOSKYTUJÚ ŽIADNE VÝSLOVNÉ ALEBO IMPLIKOVANÉ PREHLÁSENIA ALEBO ZÁRUKY VRÁTANE, NIE VŠAK VÝHRADNE, ZÁRUKY PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL ALEBO ZÁRUKY, ŽE ÚČET ALEBO SLUŽBY NEPORUŠUJÚ ŽIADNE PATENTY, AUTORSKÉ PRÁVA, OCHRANNÉ ZNÁMKY ALEBO INÉ PRÁVA TRETÍCH STRÁN. POSKYTOVATEĽ ANI ŽIADNA ĎALŠIA STRANA NEZARUČUJÚ, ŽE ÚČET ALEBO SLUŽBY BUDÚ VYHOVOVAŤ VAŠIM POŽIADAVKÁM ALEBO ŽE PREVÁDZKA ÚČTU ALEBO SLUŽIEB BUDE NEPRERUŠENÁ A BEZCHYBNÁ. PREBERÁTE ÚPLNÚ ZODPOVEDNOSŤ A RIZIKO ZA VÝBER A POUŽÍVANIE ÚČTU A SLUŽIEB NA DOSIAHNUTIE VAMI ZAMÝŠĽANÝCH VÝSLEDKOV, KTORÉ S ÚČTOM DOSIAHNETE.

Tieto podmienky nezakladajú na strane poskytovateľa a jeho prípadných poskytovateľov licencií okrem záväzkov konkrétne tu uvedených žiadne iné záväzky.

Obmedzenie zodpovednosti

V MAXIMÁLNEJ MIERE, AKÚ DOVOĽUJE APLIKOVATEĽNÉ PRÁVO, NEBUDE POSKYTOVATEĽ, JEHO ZAMESTNANCI ALEBO JEHO DODÁVATELIA V ŽIADNOM PRÍPADE ZODPOVEDAŤ ZA ŽIADNY UŠLÝ ZISK, PRÍJEM, PREDAJ ALEBO ZA ŽIADNU STRATU ÚDAJOV, ANI ZA NÁKLADY VYNALOŽENÉ NA OBSTARANIE NÁHRADNÝCH TOVAROV ALEBO SLUŽIEB, ZA MAJETKOVÉ ŠKODY, ZA PORANENIA OSÔB, ZA PRERUŠENIE PODNIKANIA, ZA STRATU OBCHODNÝCH INFORMÁCIÍ ANI ZA ŽIADNE ŠPECIÁLNE, PRIAME, NEPRIAME, NÁHODNÉ, EKONOMICKÉ, KRYCIE, TRESTNÉ, ŠPECIÁLNE ALEBO NÁSLEDNÉ ŠKODY, AKOKOĽVEK ZAPRÍČINENÉ, ČI UŽ VYPLYNULI ZO ZMLUVY, ÚMYSELNÉHO KONANIA, NEDBALOSTI ALEBO INEJ SKUTOČNOSTI, ZAKLADAJÚCEJ VZNIK ZODPOVEDNOSTI, VZNIKNUTÉ POUŽÍVANÍM ALEBO NEMOŽNOSŤOU POUŽÍVAŤ ÚČET, A TO AJ V PRÍPADE, ŽE POSKYTOVATEĽ, JEHO DODÁVATELIA ALEBO PRIDRUŽENÉ SPOLOČNOSTI BOLI UPOZORNENÍ NA MOŽNOSŤ VZNIKU TAKÝCHTO ŠKÔD. KEĎŽE NIEKTORÉ ŠTÁTY A NIEKTORÉ PRÁVNE SYSTÉMY NEDOVOĽUJÚ VYLÚČENIE ZODPOVEDNOSTI, ALE MÔŽU DOVOĽOVAŤ OBMEDZENIE ZODPOVEDNOSTI, JE ZODPOVEDNOSŤ POSKYTOVATEĽA, JEHO ZAMESTNANCOV, DODÁVATEĽOV ALEBO PRIDRUŽENÝCH SPOLOČNOSTÍ OBMEDZENÁ DO VÝŠKY SUMY, KTORÚ STE ZAPLATILI ZA PRÍSLUŠNÚ SLUŽBU ALEBO ÚČET.

Súlad s kontrolou obchodu

(a) Zaväzujete sa, že Softvér nebudete priamo alebo nepriamo vyvážať, opätovne vyvážať ani ho inak nesprístupníte žiadnej osobe, ani ho nepoužijete akýmkoľvek spôsobom, ktorý by spôsobil, že spoločnosť ESET alebo jej holdingové spoločnosti, dcérske spoločnosti alebo dcérske spoločnosti jej holdingových spoločností spolu s osobami ovládanými jej holdingovými spoločnosťami („Pobočky“) porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu, ktoré zahŕňajú:

i. všetky zákony, ktoré kontrolujú, obmedzujú alebo vynucujú licenčné podmienky vývozu, opätovného vývozu alebo prenosu výrobkov, softvéru, technológií alebo služieb vydaných alebo prijatých akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej majú byť naplnené tieto Podmienky alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje a

ii. všetky ekonomické, finančné, obchodné alebo iné sankcie, obmedzenia, embargá, zákazy dovozu alebo vývozu, zákazy prevodu prostriedkov alebo aktív alebo poskytovania služieb alebo iné porovnateľné opatrenie prijaté akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej majú byť naplnené tieto Podmienky alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje (právne predpisy, na ktoré sa odkazuje v bodoch i. a ii. vyššie, ďalej spoločne „Zákony na kontrolu obchodu“).

(b) Spoločnosť ESET si vyhradzuje právo s okamžitou platnosťou pozastaviť alebo ukončiť plnenie svojich povinností vyplývajúcich z tejto dohody v prípade, že:

i. Spoločnosť ESET rozhodne podľa svojho najlepšieho vedomia a svedomia, že Používateľ porušil alebo pravdepodobne poruší ustanovenia sekcie (a) tejto doložky Súlad s kontrolou obchodu týchto Podmienok; alebo

ii. Koncový používateľ a/alebo Softvér sa stanú predmetom zákonov na kontrolu obchodu, následkom čoho spoločnosť ESET podľa svojho najlepšieho vedomia a svedomia rozhodne, že ďalšie plnenie jej povinností vyplývajúcich z týchto Podmienok by mohlo mať za následok, že spoločnosť ESET a jej Pobočky porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu.

(c) Žiadna časť týchto Podmienok nie je zamýšľaná a nesmie byť interpretovaná tak, že podnecuje niektorú zo strán či od nej vyžaduje, aby konala alebo sa zdržala konania spôsobom (či s takýmto konaním či nekonaním súhlasila), ktorý akýmkoľvek spôsobom porušuje platné zákony na kontrolu obchodu alebo sa týmito zákonmi postihuje či zakazuje.

Rozhodujúce právo a jazyk

Tieto podmienky sa riadia zákonmi Slovenskej republiky a musia byť vykladané v súlade s nimi. Koncový používateľ a poskytovateľ sa dohodli, že kolízne ustanovenia rozhodujúceho práva a Dohovoru OSN o zmluvách pri medzinárodnej kúpe tovarov sa nepoužijú. Ak ste spotrebiteľom s obvyklým pobytom v krajine EÚ, máte tiež k dispozícii ďalšiu ochranu, ktorú vám poskytujú povinné ustanovenia právnych predpisov platných v krajine vášho pobytu.

Výslovne súhlasíte s tým, že o akýchkoľvek nárokoch voči poskytovateľovi alebo spory s poskytovateľom týkajúce sa akýmkoľvek spôsobom používania softvéru, účtu alebo služieb alebo vyplývajúce z týchto podmienok alebo osobitných podmienok (ak sa uplatňujú) bude výhradne rozhodovať Okresný súd Bratislava I., Slovensko a tiež v spojení s akýmikoľvek takýmito nárokmi alebo spormi výslovne súhlasíte s vykonávaním osobnej jurisdikcie na Okresnom súde Bratislava I. Ak ste spotrebiteľom s obvyklým pobytom v krajine EÚ, môžete tiež uplatniť nárok na

svoje práva spotrebiteľa, a to na mieste výhradnej jurisdikcie alebo v krajine EÚ, v ktorej žijete. Okrem toho môžete využiť platformu na riešenie sporov online, ku ktorej môžete získať prístup tu: https://ec.europa.eu/consumers/odr/. Žiadame vás však, aby ste pred uplatnením akéhokoľvek nároku úradnou cestou kontaktovali najskôr nás.

V prípade akýchkoľvek rozporov medzi jazykovými verziami týchto podmienok vždy platí verzia v angličtine dostupná tu.

Všeobecné ustanovenia

Spoločnosť ESET si vyhradzuje právo kedykoľvek zmeniť tieto podmienky a dokumentáciu alebo ich časť aktualizovaním príslušného dokumentu, aby odrážal zmeny zákona alebo účtu. O každej zmene týchto podmienok vás informujeme prostredníctvom účtu. Ak so zmenami podmienok nebudete súhlasiť, môžete svoj účet zrušiť. Ak po upozornení na zmeny účet nezrušíte, tak až do zrušenia účtu vás zaväzujú všetky podmienky používania, ich dodatky alebo zmeny. Mali by ste pravidelne navštevovať túto stránku a prejsť si aktuálne podmienky používania vzťahujúce sa na používanie účtu.

Oznámenia

Všetky oznámenia musia byť doručené na adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Príloha č. 1

Licenčná dohoda s koncovým používateľom

Príloha č. 2

Dohoda o spracúvaní údajov

Príloha č. 3

Štandardné zmluvné doložky

Licenčná dohoda s koncovým používateľom

DÔLEŽITÉ: Pred stiahnutím, inštaláciou, kopírovaním alebo použitím si pozorne prečítajte nižšie uvedené podmienky používania produktu. **INŠTALÁCIOU, STIAHNUTÍM, KOPÍROVANÍM ALEBO POUŽITÍM SOFTVÉRU VYJADRUJETE SVOJ SÚHLAS S TÝMITO PODMIENKAMI A BERIETE NA VEDOMIE ZÁSADY OCHRANY OSOBNÝCH ÚDAJOV.**

Licenčná dohoda s koncovým používateľom

Podľa podmienok tejto Dohody s koncovým používateľom (ďalej len „Dohoda“) uzatvorenej medzi spoločnosťou ESET, spol. s r. o., so sídlom Einsteinova 24, 851 01 Bratislava, Slovak Republic, zapísanej v Obchodnom registri okresného súdu Bratislava I, oddiel Sro, vložka č. 3586/B, IČO: 31333532(ďalej len „ESET“ alebo „Poskytovateľ“) a vami, fyzickou alebo právnickou osobou (ďalej len „Vy“ alebo „Koncový používateľ“) máte právo na používanie Softvéru uvedeného v článku 1 tejto Dohody. Softvér uvedený v článku 1 tejto Dohody môže byť v súlade so zmluvnými podmienkami uvedenými nižšie uložený na dátovom médiu, odoslaný elektronickou poštou, stiahnutý z internetu, stiahnutý zo serverov Poskytovateľa alebo získaný z iných zdrojov.

TOTO NIE JE KÚPNA ZMLUVA ALE DOHODA O PRÁVACH KONCOVÉHO POUŽÍVATEĽA. Poskytovateľ zostáva vlastníkom kópie Softvéru a prípadného fyzického média, na ktorom sa Softvér dodáva v obchodnom balení, ako aj všetkých kópií Softvéru, na ktoré má Koncový používateľ právo podľa tejto Dohody.

Kliknutím na položku „Súhlasím“ alebo „Súhlasím…“ pri inštalácii, sťahovaní, kopírovaní alebo používaní Softvéru vyjadrujete svoj súhlas s podmienkami a požiadavkami tejto Dohody. Ak s niektorými podmienkami a požiadavkami tejto Dohody nesúhlasíte, bezodkladne kliknite na možnosť zrušenia, zrušte inštaláciu alebo sťahovanie, prípadne zničte alebo vráťte Softvér, inštalačné médium, priloženú dokumentáciu a potvrdenie o platbe späť Poskytovateľovi alebo v obchode, kde ste Softvér získali.

SÚHLASÍTE S TÝM, ŽE VAŠE POUŽÍVANIE SOFTVÉRU JE ZNAKOM TOHO, ŽE STE SI PREČÍTALI TÚTO DOHODU, ROZUMIETE JEJ, A SÚHLASÍTE S TÝM, ŽE STE VIAZANÝ JEJ USTANOVENIAMI.

1. **Softvér**. Pojem „Softvér“ v tejto zmluve označuje (i) počítačový program, ku ktorému je priložená táto Zmluva, vrátane všetkých jeho súčastí, (ii) celý obsah diskov, CD-ROM, DVD médií, e-mailov a ich všetkých prípadných príloh alebo iných médií, ku ktorým je priložená táto Zmluva, vrátane Softvéru dodaného vo forme objektového kódu na dátovom nosiči, elektronickou poštou alebo stiahnutého cez internet, (iii) so Softvérom súvisiace vysvetľujúce písomné materiály a akúkoľvek dokumentáciu, najmä akýkoľvek popis Softvéru, jeho špecifikácie, popis vlastností, popis ovládania, popis operačného prostredia, v ktorom sa Softvér používa, pokyny na použitie alebo inštaláciu Softvéru alebo akýkoľvek popis používania Softvéru (ďalej len „Dokumentácia“), (iv) kópie Softvéru, opravy prípadných chýb Softvéru, dodatky k Softvéru, rozšírenia Softvéru, modifikované verzie Softvéru a aktualizácie súčastí Softvéru, ak sú dodané, na ktoré vám Poskytovateľ udeľuje licenciu v zmysle článku 3. tejto Zmluvy. Softvér sa dodáva výlučne vo forme spustiteľného objektového kódu.

2. **Inštalácia, počítač a licenčný kľúč**. Softvér dodaný na pamäťovom médiu, odoslaný elektronickou poštou, stiahnutý z internetu, stiahnutý zo serverov Poskytovateľa alebo získaný z iných zdrojov je nutné inštalovať. Softvér je potrebné inštalovať do správne nakonfigurovaného počítača, ktorý spĺňa minimálne požiadavky uvedené v Dokumentácii. Spôsob inštalácie je popísaný v Dokumentácii. Do počítača, do ktorého inštalujete Softvér, sa nesmú inštalovať žiadne počítačové programy ani hardvér, ktorý by mohol mať na Softvér negatívny vplyv. Počítač znamená hardvér vrátane, okrem iného, osobných počítačov, notebookov, pracovných staníc, vreckových počítačov, smartfónov, ručných elektronických zariadení a ďalších elektronických zariadení, pre ktoré je Softvér určený a v ktorých sa bude inštalovať a/alebo používať. Licenčný kľúč znamená jedinečnú postupnosť symbolov, písmen, číslic alebo špeciálnych znakov poskytnutú Koncovému používateľovi a umožňujúcu legálne používanie Softvéru, jeho konkrétnej verzie alebo predĺženie obdobia licencie v súlade s touto Dohodou.

3. **Licencia**. Za predpokladu, že ste súhlasili s podmienkami tejto Dohody a dodržiavate všetky jej zmluvné podmienky, Poskytovateľ vám udeľuje nasledujúce práva (ďalej len „Licencia“):

a) **Inštalácia a používanie**. Máte nevýhradné a neprevoditeľné, časovo obmedzené právo inštalovať Softvér na pevný disk počítača alebo na iné podobné médium slúžiace na trvalé ukladanie dát, inštaláciu a na ukladanie Softvéru do pamäte počítačového systému, na vykonávanie, na ukladanie a na zobrazovanie Softvéru.

b) **Stanovenie počtu licencií**. Právo na použitie Softvéru sa viaže na počet Koncových používateľov. Jedným Koncovým používateľom sa pritom rozumie: (i) inštalácia Softvéru na jednom počítačovom systéme, alebo (ii) ak sa rozsah licencie viaže na počet poštových schránok, potom sa rozumie jedným Koncovým používateľom užívateľ počítača, ktorý si pomocou Mail User Agent (ďalej len „MUA“) preberá elektronickú poštu. Ak MUA preberá elektronickú poštu a následne ju automaticky rozdeľuje viacerým používateľom potom sa počet Koncových používateľov stanovuje podľa skutočného počtu užívateľov, pre ktorých je elektronická pošta rozdeľovaná. V prípade, že poštový server vykonáva funkciu poštovej brány, je počet Koncových používateľov zhodný s počtom užívateľov poštových serverov, pre ktoré poskytuje táto brána služby. Pokiaľ je jednému používateľovi smerovaný ľubovoľný počet adries elektronickej pošty (napríklad pomocou aliasov) a preberá si ich jeden používateľ, a správy nie sú automaticky na strane klienta rozdeľované pre viac používateľov, je potrebná licencia pre jeden počítač.

Jednu licenciu nesmiete súčasne používať na viacerých počítačoch. Koncový používateľ smie zadať licenčný kľúč v Softvéri len v rozsahu, v ktorom má právo používať Softvér v súlade s obmedzením vyplývajúcim z počtu Licencií pridelených Poskytovateľom. Licenčný kľúč sa považuje za dôverný – Licenciu nesmiete zdieľať s tretími stranami a ani nesmiete tretím stranám umožniť používať licenčný kľúč, ak to nie je povolené v tejto Dohode alebo Poskytovateľom. Ak dôjde k neoprávnenému použitiu vášho licenčného kľúča, okamžite informujte Poskytovateľa.

c) **Business Edition**. Pre použitie Softvéru na mailových serveroch, mail relay serveroch, mailových bránach alebo internetových bránach musíte získať Softvér vo verzii Business Edition.

d) **Trvanie Licencie**. Vaše právo používať Softvér je časovo obmedzené.

e) **OEM Softvér**. OEM Softvér sa viaže na počítač, s ktorým ste ho získali. Nie je ho možné preniesť na iný počítač.

f) **NFR, TRIAL Softvér**. Softvér označený ako „Not-for-resale“, NFR alebo TRIAL nemôžete previesť za protihodnotu alebo používať na iný účel, ako na predvádzanie, testovanie jeho vlastností alebo vyskúšanie.

g) **Zánik Licencie**. Licencia zaniká automaticky uplynutím obdobia, na ktoré bola udelená. Ak nedodržíte ktorékoľvek ustanovenie tejto Dohody má Poskytovateľ právo odstúpiť od Dohody bez toho, aby bol dotknutý akýkoľvek nárok alebo prostriedok, ktorý má Poskytovateľ pre takýto prípad k dispozícii. V prípade zániku Licencie musíte Softvér a všetky jeho záložné kópie okamžite zničiť alebo na vlastné náklady vrátiť spoločnosti ESET alebo na miesto, kde ste Softvér získali. Zánikom Licencie je tiež Poskytovateľ oprávnený ukončiť možnosť Koncového používateľa používať funkcie Softvéru, ktoré vyžadujú pripojenie k serverom Poskytovateľa alebo serverom tretích strán.

4.**Funkcie so zhromažďovaním údajov a požiadavky na pripojenie na internet.** Softvér na svoje správne fungovanie vyžaduje pripojenie na internet a musí sa v pravidelných intervaloch pripájať na servery Poskytovateľa alebo servery tretích strán. Takisto vyžaduje zhromažďovanie príslušných údajov v súlade so Zásadami ochrany osobných údajov. Pripojenie na internet a zhromažďovanie údajov je nevyhnutné na tieto funkcie Softvéru:

a) **Aktualizácia Softvéru**. Poskytovateľ môže z času na čas vydať aktualizáciu Softvéru ("Update"), avšak nie je povinný poskytovať Update. Táto funkcia je pri štandardnom nastavení Softvéru zapnutá, preto sa Update nainštaluje automaticky, okrem prípadov, keď Koncový používateľ automatickú inštaláciu Update zakázal. Na účely poskytovania aktualizácii sa vyžaduje overenie pravosti Licencie vrátane informácií o počítači a/alebo platforme, na ktorej je Softvér nainštalovaný, v súlade so Zásadami ochrany osobných údajov.

b) Preposielanie infiltrácií a informácií Poskytovateľovi. Softvér obsahuje funkcie, ktoré zhromažďujú vzorky počítačových vírusov a iných škodlivých počítačových programov, ako aj podozrivých, problémových, potenciálne nechcených alebo potenciálne nebezpečných objektov, ako sú napríklad súbory, URL adresy, IP pakety a ethernetové rámce (ďalej len „Infiltrácie“), a potom ich odosiela Poskytovateľovi vrátane, nie však výhradne, informácií o procese inštalácie, počítači a/alebo platforme, na ktorej je Softvér nainštalovaný, a/alebo informácií o prevádzke a fungovaní Softvéru (ďalej len „Informácie“.) Informácie a Infiltrácie môžu obsahovať údaje (vrátane náhodne alebo neúmyselne získaných osobných údajov) o Koncovom používateľovi alebo iných používateľoch počítača, v ktorom je Softvér nainštalovaný, a súboroch postihnutých Infiltráciami spolu so súvisiacimi metaúdajmi. Informácie a Infiltrácie sa môžu zhromažďovať prostredníctvom nasledujúcich funkcií Softvéru:

i. Súčasťou funkcie LiveGrid Reputation System je zhromažďovanie a odosielanie jednosmerných hodnôt hash súvisiacich s infiltráciami Poskytovateľovi. Táto funkcia sa zapína v štandardných nastaveniach Softvéru.

ii. Súčasťou funkcie LiveGrid Feedback System je zhromažďovanie a odosielanie Infiltrácií spolu so súvisiacimi metaúdajmi a Informáciami Poskytovateľovi.

Poskytovateľ použije získané Informácie a Infiltrácie iba na účely analýzy a preskúmania Infiltrácií, vylepšenia Softvéru a overenia pravosti Licencie, pričom vykoná primerané opatrenia na zachovanie zabezpečenia získaných

Infiltrácií a Informácií. Aktivovaním tejto funkcie Softvéru môže Poskytovateľ zhromažďovať a spracúvať Infiltrácie a Informácie v súlade so zásadami ochrany osobných údajov a príslušnými právnymi predpismi. Tieto funkcie môžete kedykoľvek deaktivovať.

Na účely tejto Dohody je potrebné zhromažďovať, spracúvať a ukladať údaje umožňujúce Poskytovateľovi identifikovať vás v súlade so Zásadami ochrany osobných údajov. Týmto beriete na vedomie, že Poskytovateľ kontroluje s využitím vlastných prostriedkov, či Softvér používate v súlade s ustanoveniami tejto Dohody. Zároveň týmto beriete na vedomie, že na účely tejto Dohody je počas komunikácie medzi Softvérom a počítačovými systémami Poskytovateľa alebo jeho obchodných partnerov v rámci distribučnej a podpornej siete Poskytovateľa potrebný prenos údajov na zabezpečenie funkčnosti Softvéru a oprávnenia na používanie Softvéru a na ochranu práv Poskytovateľa.

Po uzavretí tejto Dohody je Poskytovateľ alebo ľubovoľný jeho obchodný partner v rámci distribučnej a podpornej siete Poskytovateľa oprávnený na účely fakturácie, plnenia tejto Dohody a prenosu oznámení do vášho počítača v nevyhnutnom rozsahu prenášať, spracovávať a uchovávať dôležité údaje, ktoré vás umožnia identifikovať. Týmto súhlasíte s prijímaním oznámení a správ vrátane, okrem iného, marketingových informácií.

Podrobné informácie o ochrane súkromia, ochrane osobných údajov a vašich právach ako dotknutej osoby sú uvedené v zásadách ochrany osobných údajov dostupných na webových stránkach Poskytovateľa a prístupných priamo počas procesu inštalácie. Prístup k nim môžete získať aj v pomocníkovi softvéru.

5. **Výkon práv Koncového používateľa**. Práva Koncového používateľa musíte vykonávať osobne alebo prostredníctvom svojich prípadných zamestnancov. Softvér môžete použiť výlučne na zabezpečenie svojej činnosti a na ochranu len tých počítačových systémov, pre ktoré ste získali Licenciu.

6. **Obmedzenie práv.** Nesmiete Softvér kopírovať, šíriť, oddeľovať jeho časti alebo vytvárať od Softvéru odvodené diela. Pri používaní Softvéru ste povinný dodržiavať nasledovné obmedzenia:

a) Môžete pre seba vytvoriť jedinú kópiu Softvéru na médiu určenom na trvalé ukladanie dát ako záložnú kópiu, za predpokladu, že vaša archívna záložná kópia sa nebude inštalovať alebo používať na inom počítači. Vytvorenie akejkoľvek ďalšej kópie Softvéru je porušením tejto Dohody.

b) Softvér nesmiete používať, upravovať, prekladať, reprodukovať, alebo prevádzať práva na používanie Softvéru alebo kópií Softvéru inak, než je výslovne uvedené v tejto Dohode.

c) Softvér nesmiete predať, sublicencovať, prenajať alebo prenajať si, vypožičať si ho alebo používať na poskytovanie komerčných služieb.

d) Softvér nesmiete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu alebo sa iným spôsobom pokúsiť získať zdrojový kód Softvéru s výnimkou rozsahu, v ktorom je takéto obmedzenie výslovne zakázané zákonom.

e) Súhlasíte s tým, že budete používať Softvér iba spôsobom, ktorý je v súlade so všetkými platnými právnymi predpismi v právnom systéme, v ktorom Softvér používate, najmä v súlade s platnými obmedzeniami vyplývajúcimi z autorského práva a ďalších práv duševného vlastníctva.

f) Súhlasíte s tým, že budete používať Softvér a jeho funkcie výlučne spôsobom, ktorý neobmedzí možnosti iných Koncových používateľov na prístup k týmto službám. Poskytovateľ si vyhradzuje právo obmedziť rozsah služieb poskytovaných jednotlivým Koncovým používateľom tak, aby umožnil ich využívanie čo najväčšiemu počtu Koncových používateľov. Obmedzenie rozsahu služieb môže znamenať aj úplné zrušenie možnosti používať niektorú z funkcií Softvéru a likvidáciu Údajov a informácií na serveroch Poskytovateľa alebo serveroch tretích strán spojených danou funkciou Softvéru.

g) Súhlasíte s tým, že nebudete vykonávať žiadne činnosti zahŕňajúce použitie licenčného kľúča v rozpore s podmienkami tejto Dohody alebo vedúce k poskytnutiu licenčného kľúča akejkoľvek osobe, ktorá nie je oprávnená používať Softvér, ako napríklad prenos použitého alebo nepoužitého licenčného kľúča v akejkoľvek forme, ako aj neoprávnená reprodukcia alebo distribúcia duplikovaných alebo generovaných licenčných kľúčov alebo používanie Softvéru v dôsledku použitia licenčného kľúča získaného od iného zdroja ako od Poskytovateľa.

7. **Autorské práva**. Softvér a všetky práva, najmä vlastnícke práva a práva duševného vlastníctva k nemu, sú vlastníctvom spoločnosti ESET a/alebo jej poskytovateľov licencií. Tieto sú chránené ustanoveniami medzinárodných dohôd a všetkými ďalšími aplikovateľnými zákonmi krajiny, v ktorej sa Softvér používa. Štruktúra, organizácia a kód Softvéru sú obchodnými tajomstvami a dôvernými informáciami spoločnosti ESET a/alebo jej poskytovateľov licencií. Softvér nesmiete kopírovať, s výnimkou uvedenou v ustanovení článku 6 písmeno a). Akékoľvek kópie, ktoré smiete vytvoriť podľa tejto Zmluvy, musia obsahovať rovnaké upozornenia na autorské a vlastnícke práva, aké sú uvedené na Softvéri. V prípade, že v rozpore s ustanoveniami tejto Zmluvy budete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu alebo sa iným spôsobom pokúsite získať zdrojový kód, súhlasíte s tým, že takto získané informácie sa budú automaticky a neodvolateľne považovať za prevedené na Poskytovateľa a vlastnené v plnom rozsahu Poskytovateľom od okamihu ich vzniku, čím nie sú dotknuté práva Poskytovateľa spojené s porušením tejto Zmluvy.

8. **Výhrada práv**. Všetky práva k Softvéru, okrem práv ktoré Vám ako Koncovému používateľovi Softvéru boli výslovne udelené v tejto Dohode, si Poskytovateľ vyhradzuje pre seba.

9. **Viaceré jazykové verzie, verzie pre viac operačných systémov, viaceré kópie**. V prípade ak Softvér podporuje viaceré platformy alebo jazyky, alebo ak ste získali viac kópii Softvéru, môžete Softvér používať len na takom počte počítačových systémov a v takých verziách, na ktoré ste získali Licenciu. Verzie alebo kópie Softvéru, ktoré nepoužívate nesmiete predať, prenajať, sublicencovať, zapožičať alebo previesť na iné osoby.

10. **Začiatok a trvanie Dohody.** Táto Dohoda je platná a účinná odo dňa, kedy ste odsúhlasili túto Dohodu. Dohodu môžete kedykoľvek ukončiť tak, že natrvalo odinštalujete zničíte alebo na svoje vlastné náklady vrátite Softvér, všetky prípadné záložné kópie a všetok súvisiaci materiál, ktorý ste získali od Poskytovateľa alebo jeho obchodných partnerov. Bez ohľadu na spôsob zániku tejto Dohody, ustanovenia jej článkov 7, 8, 11, 13, 19 a 21 zostávajú v platnosti bez časového obmedzenia.

11. **VYHLÁSENIA KONCOVÉHO POUŽÍVATEĽA**. AKO KONCOVÝ POUŽÍVATEĽ UZNÁVATE, ŽE SOFTVÉR JE POSKYTOVANÝ "AKO STOJÍ A LEŽÍ", BEZ VÝSLOVNEJ ALEBO IMPLIKOVANEJ ZÁRUKY AKÉHOKOĽVEK DRUHU A V MAXIMÁLNEJ MIERE DOVOLENEJ APLIKOVATEĽNÝMI ZÁKONMI. ANI POSKYTOVATEĽ, ANI JEHO POSKYTOVATELIA LICENCIÍ, ANI DRŽITELIA AUTORSKÝCH PRÁV NEPOSKYTUJÚ AKÉKOĽVEK VÝSLOVNÉ ALEBO IMPLIKOVANÉ PREHLÁSENIA ALEBO ZÁRUKY, NAJMÄ NIE ZÁRUKY PREDAJNOSTI ALEBO VHODNOSTI PRE KONKRÉTNY ÚČEL ALEBO ZÁRUKY, ŽE SOFTVÉR NEPORUŠUJE ŽIADNE PATENTY, AUTORSKÉ PRÁVA, OCHRANNÉ ZNÁMKY ALEBO INÉ PRÁVA TRETÍCH STRÁN. NEEXISTUJE ŽIADNA ZÁRUKA ZO STRANY POSKYTOVATEĽA ANI ŽIADNEJ ĎALŠEJ STRANY, ŽE FUNKCIE, KTORÉ OBSAHUJE SOFTVÉR, BUDÚ VYHOVOVAŤ VAŠÍM POŽIADAVKÁM, ALEBO ŽE PREVÁDZKA SOFTVÉRU BUDE NERUŠENÁ A BEZCHYBNÁ. PREBERÁTE ÚPLNÚ ZODPOVEDNOSŤ A RIZIKO ZA VÝBER SOFTVÉRU PRE DOSIAHNUTIE VAMI ZAMÝŠĽANÝCH VÝSLEDKOV A ZA INŠTALÁCIU, POUŽÍVANIE A VÝSLEDKY, KTORÉ SO SOFTVÉROM DOSIAHNETE.

12. **Žiadne ďalšie záväzky.** Táto Dohoda nezakladá na strane Poskytovateľa a jeho prípadných poskytovateľov licencií okrem záväzkov konkrétne uvedených v tejto Dohode žiadne iné záväzky.

13. **OBMEDZENIE ZODPOVEDNOSTI**. V MAXIMÁLNEJ MIERE, AKÚ DOVOĽUJE APLIKOVATEĽNÉ PRÁVO, V ŽIADNOM PRÍPADE NEBUDE POSKYTOVATEĽ, JEHO ZAMESTNANCI ALEBO JEHO POSKYTOVATELIA LICENCIÍ ZODPOVEDAŤ ZA AKÝKOĽVEK UŠLÝ ZISK, PRÍJEM ALEBO PREDAJ, ALEBO ZA AKÚKOĽVEK STRATU DÁT, ALEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARANIE NÁHRADNÝCH TOVAROV ALEBO SLUŽIEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÚ UJMU, ZA PRERUŠENIE PODNIKANIA, ZA STRATU OBCHODNÝCH INFORMÁCIÍ, ANI ZA AKÉKOĽVEK ŠPECIÁLNE,

PRIAME, NEPRIAME, NÁHODNÉ, EKONOMICKÉ, KRYCIE, TRESTNÉ, ŠPECIÁLNE ALEBO NÁSLEDNÉ ŠKODY, AKOKOĽVEK ZAPRÍČINENÉ, ČI UŽ VYPLYNULI ZO ZMLUVY, ÚMYSELNÉHO KONANIA, NEDBALOSTI ALEBO INEJ SKUTOČNOSTI, ZAKLADAJÚCEJ VZNIK ZODPOVEDNOSTI, VZNIKNUTÉ POUŽÍVANÍM ALEBO NEMOŽNOSŤOU POUŽÍVAŤ SOFTVÉR, A TO AJ V PRÍPADE, ŽE POSKYTOVATEĽ ALEBO JEHO POSKYTOVATELIA LICENCIÍ BOLI UVEDOMENÍ O MOŽNOSTI TAKÝCHTO ŠKÔD. NAKOĽKO NIEKTORÉ ŠTÁTY A NIEKTORÉ PRÁVNE SYSTÉMY NEDOVOĽUJÚ VYLÚČENIE ZODPOVEDNOSTI, ALE MÔŽU DOVOĽOVAŤ OBMEDZENIE ZODPOVEDNOSTI, JE ZODPOVEDNOSŤ POSKYTOVATEĽA, JEHO ZAMESTNANCOV ALEBO POSKYTOVATEĽOV LICENCIÍ OBMEDZENÁ DO VÝŠKY CENY, KTORÚ STE ZAPLATILI ZA LICENCIU.

14. Žiadne ustanovenie tejto Dohody sa nedotýka práv strany, ktorej zákon priznáva práva a postavenie spotrebiteľa, pokiaľ je s nimi v rozpore.

15. **Technická podpora**. Technickú podporu poskytuje ESET alebo ním poverená tretia strana na základe vlastného uváženia bez akýchkoľvek záruk alebo prehlásení. Koncový používateľ je povinný pred poskytnutím technickej podpory zálohovať všetky jeho existujúce dáta, softvér a programové vybavenie. ESET a/alebo ním poverená tretia strana nepreberajú zodpovednosť za poškodenie alebo stratu dát, majetku, softvéru alebo hardvéru alebo ušlý zisk pri poskytovaní technickej podpory. ESET a/alebo ním poverená tretia strana si vyhradzuje právo na rozhodnutie, že riešený problém presahuje rozsah technickej podpory. ESET si vyhradzuje právo odmietnuť, pozastaviť alebo ukončiť poskytovanie technickej podpory na základe vlastného uváženia. Informácie o Licencii, Informácie a ďalšie údaje v súlade so Zásadami ochrany osobných údajov sa môžu vyžadovať na účely poskytovania technickej pomoci.

16. **Prevod Licencie**. Softvér môžete preniesť z jedného počítačového systému na iný počítačový systém, pokiaľ to nie je v rozpore s Dohodou. Pokiaľ to nie je v rozpore s Dohodou, Koncový používateľ môže jednorazovo trvalo previesť Licenciu a všetky práva z tejto Dohody na iného Koncového používateľa iba so súhlasom Poskytovateľa za podmienky, že (i) pôvodný Koncový používateľ si neponechá žiadnu kópiu Softvéru, (ii) prevod práv musí byť priamy, teda z pôvodného Koncového používateľa na nového Koncového používateľa, (iii) nový Koncový používateľ musí prebrať všetky práva a povinnosti, ktoré má podľa tejto Dohody pôvodný Koncový používateľa (iv) pôvodný Koncový používateľ musí odovzdať novému Koncovému používateľovi doklady umožňujúce overenie legality Softvéru ako je uvedené v článku 17.

17. **Overenie pravosti softvéru**. Koncový používateľ musí preukázať právo na používanie Softvéru jedným z týchto spôsobov: (i) prostredníctvom osvedčenia o licencii vydaného Poskytovateľom alebo treťou stranou určenou Poskytovateľom, (ii) prostredníctvom písomnej licenčnej zmluvy, ak takáto zmluva bola uzavretá, (iii) predložením e-mailu odoslaného Poskytovateľom, ktorý obsahuje podrobnosti o licencii (meno používateľa a heslo). Informácie o Licencii a identifikačné údaje Koncového používateľa v súlade so Zásadami ochrany osobných údajov sa môžu vyžadovať na účely overenia pravosti Softvéru.

18. **Licencovanie pre štátne orgány a vládu USA**. Softvér sa poskytuje štátnym orgánom vrátane vlády Spojených štátov amerických s licenčnými právami a obmedzeniami popísanými v tejto Dohode.

19. **Súlad s kontrolou obchodu**

a) Zaväzujete sa, že Softvér nebudete priamo alebo nepriamo vyvážať, opätovne vyvážať ani ho inak nesprístupníte žiadnej osobe, ani ho nepoužijete akýmkoľvek spôsobom, ktorý by spôsobil, že spoločnosť ESET alebo jej holdingové spoločnosti, dcérske spoločnosti alebo dcérske spoločnosti jej holdingových spoločností spolu s osobami ovládanými jej holdingovými spoločnosťami (ďalej iba Pobočky) porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu, ktoré zahŕňajú:

i. všetky zákony, ktoré kontrolujú, obmedzujú alebo vynucujú licenčné podmienky vývozu, opätovného vývozu alebo prenosu výrobkov, softvéru, technológií alebo služieb vydaných alebo prijatých akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej má byť naplnená Dohoda alebo

v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje (ďalej iba Zákony na kontrolu vývozu); a

ii. všetky ekonomické, finančné, obchodné alebo iné sankcie, obmedzenia, embargá, zákazy dovozu alebo vývozu, zákazy prevodu prostriedkov alebo aktív alebo poskytovania služieb alebo iné porovnateľné opatrenie prijaté akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej má byť naplnená Dohoda alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje (ďalej iba Sankčné zákony).

b) Spoločnosť ESET si vyhradzuje právo s okamžitou platnosťou pozastaviť alebo ukončiť plnenie svojich povinností vyplývajúcich z tejto dohody v prípade, že:

i. Spoločnosť ESET rozhodne podľa svojho najlepšieho vedomia a svedomia, že Používateľ porušil alebo pravdepodobne poruší ustanovenia článku 19 bodu (a) Dohody; alebo

ii. Koncový používateľ a/alebo Softvér sa stanú predmetom zákonov na kontrolu obchodu, následkom čoho spoločnosť ESET podľa svojho najlepšieho vedomia a svedomia rozhodne, že ďalšie plnenie jej povinností vyplývajúcich z Dohody by mohlo mať za následok, že spoločnosť ESET a jej Pobočky porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu.

c) Žiadna časť Dohody nie je zamýšľaná a nesmie byť interpretovaná tak, že podnecuje niektorú zo strán či od nej vyžaduje, aby konala alebo sa zdržala konania spôsobom (či s takýmto konaním či nekonaním súhlasila), ktorý akýmkoľvek spôsobom porušuje platné zákony na kontrolu obchodu alebo sa týmito zákonmi postihuje či zakazuje.

20. **Oznámenia**. Všetky oznámenia, vrátený Softvér a Dokumentáciu je potrebné doručiť na adresu: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

21. **Rozhodujúce právo**. Táto Dohoda sa riadi a musí byť vykladaná v súlade so zákonmi Slovenskej republiky. Koncový používateľ a Poskytovateľ sa dohodli, že kolízne ustanovenia rozhodujúceho právneho poriadku a Dohovor OSN o zmluvách pri medzinárodnej kúpe tovarov sa nepoužijú. Výslovne súhlasíte, že riešenie akýkoľvek sporov alebo nárokov z tejto Dohody voči Poskytovateľovi alebo spory a nároky súvisiace s používaním softvéru je príslušný Okresný súd Bratislava I a výslovne súhlasíte s výkonom jurisdikcie týmto súdom.

22. **Všeobecné ustanovenia**. V prípade, že akákoľvek ustanovenie tejto Dohody je neplatné alebo nevykonateľné, neovplyvní to platnosť ostatných ustanovení Dohody. Tie zostanú platné a vykonateľné podľa podmienok v nej stanovených. V prípade akýchkoľvek nezrovnalostí medzi jazykovými verziami tejto Dohody platí anglická verzia. Zmeny tejto Dohody sú možné iba v písomnej forme, pričom za Poskytovateľa musí takúto zmenu podpísať štatutárny zástupca alebo osoba k tomuto úkonu výslovne splnomocnená.

Táto Zmluva medzi Vami a Poskytovateľom predstavuje jedinú a úplnú Zmluvu vzťahujúcu sa na Softvér, a plne nahrádza akékoľvek predchádzajúce vyhlásenia, rokovania, záväzky, správy alebo reklamné informácie, týkajúce sa Softvéru.

EULA ID: BUS-ECOS-20-01

Data Processing Agreement

V súlade s požiadavkami nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), poskytovateľ (ďalej len „sprostredkovateľ“) a vy (ďalej len

„prevádzkovateľ“) vstupujete do zmluvného vzťahu týkajúceho sa spracúvania údajov s cieľom vymedziť podmienky pre spracúvanie osobných údajov a spôsob ich ochrany, ako aj stanoviť ďalšie práva a povinnosti obidvoch strán pri spracúvaní osobných údajov dotknutých osôb v mene prevádzkovateľa v priebehu vykonávania predmetu týchto podmienok ako hlavnej zmluvy.

1. **Spracúvanie osobných údajov.** Služby poskytované v súlade s týmito podmienkami zahŕňajú spracúvanie informácií týkajúcich sa identifikovanej alebo identifikovateľnej fyzickej osoby, ktoré sú uvedené v zásadách ochrany osobných údajov (ďalej len „osobné údaje“).

2. **Poverenie.** Prevádzkovateľ poveruje sprostredkovateľa spracúvaním osobných údajov, pričom

(i) „účel spracúvania“ znamená poskytovanie služieb v súlade s týmito podmienkami, sprostredkovateľ môže spracúvať osobné údaje v mene prevádzkovateľa len v súvislosti s poskytovaním služieb vyžiadaných prevádzkovateľom, všetky informácie zhromaždené na dodatočné účely sa spracúvajú mimo zmluvného vzťahu medzi prevádzkovateľom a sprostredkovateľom,

(ii) doba spracúvania znamená obdobie od začatia spolupráce podľa týchto podmienok do ukončenia služieb,

(iii) rozsah a kategórie osobných údajov. Tieto služby sú určené na spracúvanie iba všeobecných osobných údajov. Prevádzkovateľ však nesie výhradnú zodpovednosť za určenie rozsahu osobných údajov,

(iv) dotknutá osoba je fyzická osoba ako oprávnený používateľ zariadení prevádzkovateľa,

(v) spracovateľské činnosti predstavujú všetky operácie potrebné na spracúvanie,

(vi) „zdokumentované pokyny” znamenajú pokyny uvedené v týchto podmienkach, ich prílohách, zásadách ochrany osobných údajov a v dokumentácii k službe. Prevádzkovateľ je zodpovedný za právnu prípustnosť spracúvania osobných údajov sprostredkovateľom s ohľadom na príslušné platné ustanovenia zákona o ochrane osobných údajov.

3. **Povinnosti sprostredkovateľa.** Sprostredkovateľ je povinný:

(i) spracúvať osobné údaje len na základe zdokumentovaných pokynov a na účely definované v podmienkach, ich prílohách, zásadách ochrany osobných údajov a v dokumentácii k službe,

(ii) poučiť osoby oprávnené spracúvať osobné údaje (ďalej len „oprávnené osoby“) o ich právach a povinnostiach podľa všeobecného nariadenia o ochrane údajov, o ich zodpovednosti v prípade porušenia a zabezpečiť, aby sa oprávnené osoby zaviazali zachovávať dôvernosť informácií a dodržiavali zdokumentované pokyny,

(iii) implementovať a dodržiavať opatrenia opísané v podmienkach, ich prílohách, zásadách ochrany osobných údajov a v dokumentácii k službe,

(iv) pomáhať prevádzkovateľovi reagovať na žiadosti dotknutých osôb súvisiace s ich právami. Sprostredkovateľ nesmie opraviť, odstrániť ani obmedziť spracúvanie osobných údajov bez pokynu prevádzkovateľa. Všetky žiadosti dotknutej osoby týkajúce sa osobných údajov spracúvaných v mene prevádzkovateľa sa bezodkladne prepošlú prevádzkovateľovi,

(v) pomáhať prevádzkovateľovi s oznámením porušenia ochrany osobných údajov dozornému orgánu a dotknutej osobe. Sprostredkovateľ oznámi prevádzkovateľovi každé porušenie spracúvania osobných údajov alebo bezpečnosti osobných údajov okamžite po jeho zistení. Sprostredkovateľ bude v primeranom rozsahu spolupracovať pri vyšetrovaní a náprave takéhoto porušenia a prijme primerané opatrenia, aby obmedzil ďalšie negatívne dôsledky.

(vi) podľa rozhodnutia prevádzkovateľa vymazať alebo vrátiť všetky osobné údaje prevádzkovateľovi po skončení

doby spracúvania. Prevádzkovateľ sa zaväzuje informovať sprostredkovateľa o svojom rozhodnutí do desiatich (10) dní po skončení doby spracúvania. Toto ustanovenie nemá vplyv na právo sprostredkovateľa uchovávať osobné údaje v nevyhnutnom rozsahu na účely archivácie vo verejnom záujme, na účely vedeckého výskumu, na štatistické účely alebo na účely preukazovania, uplatňovania alebo ochrany právnych nárokov,

(vii) viesť aktuálny register všetkých kategórií spracovateľských činností, ktoré vykonal v mene prevádzkovateľa,

(viii) sprístupniť prevádzkovateľovi všetky informácie potrebné na preukázanie súladu v rámci podmienok, ich príloh, zásad ochrany osobných údajov a dokumentácie k službe. V prípade auditu alebo kontroly spracúvania osobných údajov zo strany prevádzkovateľa je prevádzkovateľ povinný písomne informovať sprostredkovateľa najmenej tridsať (30) dní pred plánovaným auditom alebo kontrolou.

4. **Zapojenie ďalšieho sprostredkovateľa.** Sprostredkovateľ je oprávnený zapojiť ďalšieho sprostredkovateľa na vykonávanie špecifických spracovateľských činností, ako je napríklad poskytovanie cloudového úložiska a infraštruktúry pre službu, v súlade s podmienkami, ich prílohami, zásadami ochrany osobných údajov a dokumentáciou k službe. V súčasnosti poskytuje cloudové úložisko a infraštruktúru spoločnosť Microsoft ako súčasť cloudovej služby Azure. Aj v tomto prípade zostane sprostredkovateľ jediným kontaktným miestom a stranou zodpovednou za zaistenie súladu s požiadavkami. Sprostredkovateľ sa týmto zaväzuje informovať Prevádzkovateľa o každom pridaní alebo nahradení iného sprostredkovateľa, čím mu umožní voči takejto zmene namietať.

5. **Územná pôsobnosť.** Sprostredkovateľ vynaloží maximálne úsilie s cieľom zabezpečiť, aby sa spracúvanie údajov uskutočňovalo v Európskom hospodárskom priestore alebo v krajine označenej Európskou komisiou za bezpečnú, a to na základe rozhodnutia Prevádzkovateľa. Štandardné zmluvné doložky sa uplatňujú v prípade prenosov údajov a spracúvania prebiehajúceho mimo Európskeho hospodárskeho priestoru alebo krajiny označenej Európskou komisiou za bezpečnú na žiadosť prevádzkovateľa.

6. **Bezpečnosť.** Sprostredkovateľ je držiteľom certifikátu ISO 27001:2013 a používa štandard ISO 27001 pre implementáciu bezpečnostnej stratégie viacvrstvovej ochrany pri aplikovaní bezpečnostných kontrol na vrstve siete, operačných systémov, databáz, aplikácií, personálu a operačných procesov. Dodržiavanie zmluvných požiadaviek a požiadaviek vychádzajúcich z právnych predpisov sa pravidelne vyhodnocuje a prehodnocuje podobne ako iné infraštruktúry a operácie sprostredkovateľa, pričom sa tiež neustále prijímajú nevyhnutné kroky na zabezpečenie súladu s požiadavkami. Sprostredkovateľ zaisťuje bezpečnosť údajov pomocou systému riadenia bezpečnosti informácií (ISMS) založenom na norme ISO 27001. Bezpečnostná dokumentácia obsahuje najmä dokumenty týkajúce sa politík pre bezpečnosť informácií, fyzickú bezpečnosť, zabezpečenie zariadení, správu incidentov, riešenie únikov údajov a bezpečnostných incidentov atď.

7. **Technické a organizačné opatrenia**. Sprostredkovateľ chráni osobné údaje pred náhodným a nezákonným poškodením a zničením, náhodnou stratou, zmenou, neoprávneným prístupom a zverejnením. Na tento účel sprostredkovateľ prijme primerané technické a organizačné opatrenia zodpovedajúce spôsobu spracúvania a riziku, ktoré spracúvanie predstavuje pre práva dotknutých osôb v súlade s požiadavkami všeobecného nariadenia o ochrane údajov. Detailný opis technických a organizačných opatrení je uvedený v bezpečnostnej politike.

8. **Kontaktné informácie sprostredkovateľa.** Všetky oznámenia, žiadosti, požiadavky a ďalšia komunikácia týkajúca sa ochrany osobných údajov sa adresujú spoločnosti ESET, spol. s.r.o., zodpovednej osobe: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.

Standard Contractual Clauses

ODDIEL I

Doložka 1 Účel a rozsah pôsobnosti

Účelom týchto štandardných zmluvných doložiek je zabezpečiť súlad s požiadavkami nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27.apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov) (1) pri prenose osobných údajov do tretej krajiny.

b) Zmluvné strany:

fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný orgán (ďalej len „subjekt“), ktoré uskutočňujú prenos osobných údajov, ako sa uvádza v prílohe I časti A (ďalej len „vývozca údajov“), a

subjekt v tretej krajine, ktorý prijíma osobné údaje od vývozcu údajov, a to priamo alebo nepriamo prostredníctvom iného subjektu, ktorý je tiež zmluvnou stranou týchto doložiek, ako sa uvádza v prílohe I časti A (ďalej len „dovozca údajov“),

sa dohodli na týchto štandardných zmluvných doložkách (ďalej len „doložky“).

Tieto doložky sa uplatňujú na prenos osobných údajov podľa prílohy I časti B.

Dodatok k týmto doložkám obsahujúci prílohy, na ktoré sa v týchto doložkách odkazuje, tvorí neoddeliteľnú súčasť týchto doložiek.

Doložka 2 Účinok a nemennosť doložiek

a) V týchto doložkách sa stanovujú primerané záruky vrátane vymáhateľných práv dotknutých osôb a účinných právnych prostriedkov nápravy podľa článku 46 ods.1 a článku 46 ods. 2 písm. c) nariadenia (EÚ) 2016/679, a pokiaľ ide o prenosy údajov od prevádzkovateľov sprostredkovateľom a/alebo od sprostredkovateľov sprostredkovateľom, štandardné zmluvné doložky podľa článku 28 ods. 7 nariadenia (EÚ) 2016/679, pokiaľ nie sú zmenené, okrem prípadu, keď sa vyberá vhodný modul/moduly, prípadne keď sa dopĺňajú alebo aktualizujú informácie v dodatku. To zmluvným stranám nebráni v tom, aby zahrnuli štandardné zmluvné doložky stanovené v týchto doložkách do širšej zmluvy a/alebo doplnili iné doložky či dodatočné záruky za predpokladu, že nie sú v priamom ani nepriamom rozpore s týmito doložkami ani neobmedzujú základné práva alebo slobody dotknutých osôb.

b) Týmito doložkami nie sú dotknuté povinnosti, ktoré sa vzťahujú na vývozcu údajov na základe nariadenia (EÚ) 2016/679.

Doložka 3 Oprávnenosť tretích strán

a) Dotknuté osoby sa môžu týchto doložiek dovolávať a vymáhať ich ako oprávnené tretie strany vo vzťahu k vývozcovi údajov a/alebo dovozcovi údajov s týmito výnimkami:

i) doložka 1, doložka 2, doložka 3, doložka 6, doložka 7;

ii) doložka 8 – modul č. 1: doložka 8 – modul č. 1: doložka 8.5 písm. e) a doložka 8.9 písm. b); modul č. 2: doložka

8.1 písm. b), doložka 8.9 písm. a), c), d) a e); modul č. 3: doložka 8.1 písm. a), c) a d), ako aj doložka 8.9 písm. a), c), d), e), f) a g); modul č. 4: doložka 8.1 písm. b) a doložka 8.3 písm. b);

iii) doložka 9 – modul č. 2: doložka 9 písm. a), c), d) a e); modul č. 3: doložka 9 písm. a), c), d) a e);

iv) doložka 12 – modul č. 1: doložka 12 písm. a) a d); moduly č. 2 a 3: doložka 12 písm. a), d) a f);

v) doložka 13;

vi) doložka 15.1 písm. c), d) a e);

vii) doložka 16 písm. e);

viii) doložka 18 – moduly č. 1, 2 a 3: doložka 18 písm. a) a b); modul č. 4: doložka 18.

b) Písmenom a) nie sú dotknuté práva dotknutých osôb podľa nariadenia (EÚ) 2016/679.

Doložka 4 Výklad

a) Ak sa v týchto doložkách používajú pojmy vymedzené v nariadení (EÚ) 2016/679, tieto pojmy majú rovnaký význam ako v uvedenom nariadení.

b) Tieto doložky sa vykladajú v zmysle ustanovení nariadenia (EÚ) 2016/679.

c) Tieto doložky sa nesmú vykladať spôsobom, ktorý je v rozpore správami a povinnosťami stanovenými v nariadení (EÚ) 2016/679.

Doložka 5 Hierarchia

V prípade rozporu medzi týmito doložkami a ustanoveniami súvisiacich dohôd medzi zmluvnými stranami, ktoré existovali v čase, keď sa dohodli tieto doložky, alebo ktoré sa uzavreli neskôr, majú prednosť tieto doložky.

Doložka 6 Opis prenosu

Informácie o prenose a najmä kategórie prenášaných osobných údajov a účel, na ktorý sa prenášajú, sú uvedené v prílohe I časti B.

Doložka 7 – nepovinná Doložka o pristúpení

a) Subjekt, ktorý nie je zmluvnou stranou týchto doložiek, môže so súhlasom zmluvných strán kedykoľvek pristúpiť k týmto doložkám ako vývozca alebo dovozca údajov vyplnením dodatku a podpísaním prílohy I časti A.

b) Po vyplnení dodatku a podpísaní prílohy I časti A sa pristupujúci subjekt stane zmluvnou stranou týchto doložiek a bude mať práva a povinnosti vývozcu alebo dovozcu údajov v súlade s označením v prílohe I časti A.

c) Pristupujúci subjekt nemá žiadne práva ani povinnosti vyplývajúce z týchto doložiek, pokiaľ ide o obdobie pred tým, ako sa stal zmluvnou stranou.

ODDIEL II – POVINNOSTI ZMLUVNÝCH STRÁN

Doložka 8 Záruky v oblasti ochrany údajov

Vývozca údajov vyhlasuje, že vynaložil primerané úsilie, na základe ktorého možno konštatovať, že dovozca údajov je vďaka prijatiu vhodných technických a organizačných opatrení schopný plniť svoje povinnosti podľa týchto doložiek.

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

8.1. Obmedzenie účelu

Dovozca údajov je oprávnený spracúvať osobné údaje len na osobitné účely prenosu stanovené v prílohe I časti B. Osobné údaje môže spracúvať na iný účel len vtedy, ak:

i) získal predchádzajúci súhlas dotknutej osoby;

ii) je to nevyhnutné na účely preukazovania, uplatňovania alebo ochrany právnych nárokov v kontexte konkrétneho správneho alebo súdneho konania, prípadne konania v oblasti regulácie; alebo

iii) je to nevyhnutné v záujme ochrany životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby.

8.2. Transparentnosť

a) S cieľom umožniť dotknutým osobám účinne uplatňovať práva podľa doložky 10 ich dovozca údajov priamo alebo prostredníctvom vývozcu údajov informuje:

i) o svojej totožnosti a kontaktných údajoch;

ii) o kategóriách spracúvaných osobných údajov;

iii) o práve získať kópiu týchto doložiek

iv) v prípade úmyslu uskutočniť následný prenos osobných údajov akejkoľvek tretej strane o príjemcovi alebo kategóriách príjemcov (podľa potreby s cieľom poskytnúť zmysluplné informácie), účele a dôvode tohto následného prenosu podľa doložky 8.7.

b) Písmeno a) sa neuplatňuje, ak po prvé dotknutá osoba už má informácie vrátane prípadu, keď takéto informácie už poskytol vývozca údajov, alebo ak sa po druhé poskytnutie informácií ukáže ako nemožné alebo by si vyžadovalo neprimerané úsilie dovozcu údajov. V druhom prípade dovozca údajov v čo najväčšej možnej miere sprístupní tieto informácie verejnosti.

c) Zmluvné strany sprístupnia dotknutej osobe na požiadanie a bezplatne kópiu týchto doložiek vrátane nimi vyplneného dodatku. V rozsahu potrebnom na ochranu obchodného tajomstva alebo iných dôverných informácií vrátane osobných údajov môžu zmluvné strany pred poskytnutím kópie dodatku odstrániť časť jeho textu, pričom však poskytnú zmysluplné zhrnutie, ak by dotknutá osoba inak nebola schopná pochopiť jeho obsah alebo uplatňovať svoje práva. Zmluvné strany na požiadanie oznámia dotknutej osobe dôvody odstránenia textu, pokiaľ možno bez toho, aby došlo k prezradeniu odstránených informácií.

d) Písmenami a) až c) nie sú dotknuté povinnosti vývozcu údajov podľa článkov 13 a14 nariadenia (EÚ) 2016/679.

8.3. Správnosť a minimalizácia údajov

a) Každá zmluvná strana zabezpečí, aby osobné údaje boli správne a v prípade potreby aktualizované. Dovozca údajov prijme všetky primerané opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov spracúvania, bezodkladne vymazali alebo opravili.

b) Ak jedna zo zmluvných strán zistí, že osobné údaje, ktoré preniesla alebo získala, sú nesprávne alebo neaktuálne, bez zbytočného odkladu o tom informuje druhú zmluvnú stranu.

c) Dovozca údajov zabezpečí, aby osobné údaje boli primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely spracúvania.

8.4. Minimalizácia uchovávania

Dovozca údajov nesmie uchovávať osobné údaje dlhšie než je nevyhnutné na účely, na ktoré sa spracúvajú. Na účely splnenia si tejto povinnosti zavedie vhodné technické alebo organizačné opatrenia vrátane výmazu alebo anonymizácie (2) údajov a všetkých záloh v momente uplynutia obdobia uchovávania.

8.5. Bezpečnosť spracúvania

a) Dovozca údajov a počas prenosu aj vývozca údajov prijmú vhodné technické a organizačné opatrenia na zaistenie bezpečnosti osobných údajov vrátane ochrany pred porušením bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu alebo prístupu (ďalej len „porušenie ochrany osobných údajov“). Pri posudzovaní primeranej úrovne bezpečnosti náležite zohľadnia najnovšie poznatky, náklady na vykonanie, povahu, rozsah, kontext a účely spracúvania, ako aj riziká pre dotknutú osobu, ktoré súvisia so spracúvaním. Zmluvné strany zvážia najmä použitie šifrovania alebo pseudonymizácie, a to aj počas prenosu, ak možno vďaka nim splniť účel spracúvania.

b) Zmluvné strany sa dohodli na technických a organizačných opatreniach uvedených v prílohe II. Dovozca údajov je povinný vykonávať pravidelné kontroly s cieľom zabezpečiť, aby tieto opatrenia nepretržite poskytovali primeranú úroveň bezpečnosti.

c) Zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú dôvernosť údajov, alebo aby sa na ne vzťahovala primeraná zákonná povinnosť zachovávať dôvernosť údajov.

d) V prípade porušenia ochrany osobných údajov týkajúceho sa osobných údajov spracúvaných dovozcom údajov podľa týchto doložiek prijme dovozca údajov primerané opatrenia na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho možných nepriaznivých účinkov.

e) V prípade porušenia ochrany osobných údajov, ktoré môže predstavovať riziko pre práva a slobody fyzických osôb, zašle o tom dovozca údajov bez zbytočného odkladu oznámenie vývozcovi údajov a príslušnému dozornému orgánu podľa doložky 13. Takéto oznámenie obsahuje i) opis povahy porušenia (podľa možnosti vrátane kategórií a približného počtu dotknutých osôb a záznamov o osobných údajoch); ii) pravdepodobné následky porušenia; iii) prijaté alebo navrhované opatrenia s cieľom napraviť porušenie a iv) údaje kontaktného miesta, kde možno získať viac informácií. V rozsahu, v akom nie je možné, aby dovozca údajov poskytol všetky informácie súčasne, možno ich poskytnúť vo viacerých etapách bez ďalšieho zbytočného odkladu.

f) V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, dovozca údajov bez zbytočného odkladu oznámi dotknutým osobám porušenie ochrany osobných údajov a povahu tohto porušenia, v prípade potreby v spolupráci s vývozcom údajov, spolu s informáciami uvedenými v písmene e) bodoch ii) až iv), okrem prípadov, ak dovozca údajov prijal opatrenia na výrazné zníženie rizika pre práva alebo slobody fyzických osôb, alebo ak by si oznámenie vyžadovalo neprimerané úsilie. Vtedy dovozca údajov namiesto toho uverejní oznámenie alebo prijme podobné opatrenie na informovanie verejnosti o porušení ochrany osobných údajov.

g) Dovozca údajov zdokumentuje všetky relevantné skutočnosti týkajúce sa porušenia ochrany osobných údajov vrátane jeho účinkov a všetkých prijatých opatrení na nápravu a vedie o nich záznamy.

8.6. Citlivé údaje

Ak prenos zahŕňa osobné údaje odhaľujúce rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, genetické alebo biometrické údaje na účely jedinečnej identifikácie fyzickej osoby, údaje týkajúce sa zdravia alebo sexuálneho života či sexuálnej orientácie osoby, alebo údaje týkajúce sa odsúdenia za trestné činy (ďalej len „citlivé údaje“), uplatňuje dovozca údajov osobitné obmedzenia a/alebo dodatočné záruky prispôsobené osobitnej povahe údajov a súvisiacim rizikám. Môže to zahŕňať obmedzenie okruhu zamestnancov, ktorí majú prístup k osobným údajom, dodatočné bezpečnostné opatrenia (napríklad pseudonymizácia) a/alebo dodatočné obmedzenia v súvislosti s ďalším poskytnutím.

8.7. Následné prenosy

Dovozca údajov poskytne osobné údaje tretej strane nachádzajúcej sa mimo Európskej únie (3) (v rovnakej krajine ako dovozca údajov alebo v inej tretej krajine, ďalej len „následný prenos“) len vtedy, ak je táto tretia strana viazaná týmito doložkami alebo súhlasí s tým, že bude týmito doložkami viazaná, a to v súlade s príslušným modulom. Inak môže dovozca údajov uskutočniť následný prenos len v týchto prípadoch:

i) uskutočňuje sa do krajiny, na ktorú sa vzťahuje rozhodnutie o primeranosti podľa článku 45 nariadenia (EÚ) 2016/679, ktorého predmetom je následný prenos;

ii) tretia strana inak zabezpečuje primerané záruky podľa článkov 46 alebo 47 nariadenia (EÚ) 2016/679 v súvislosti s predmetným spracúvaním;

iii) tretia strana uzavrie s dovozcom údajov dohodu o záväznom nástroji zabezpečujúcom rovnakú úroveň ochrany údajov ako podľa týchto doložiek a dovozca údajov poskytne kópiu týchto záruk vývozcovi údajov;

iv) je to nevyhnutné na účely preukazovania, uplatňovania alebo ochrany právnych nárokov v kontexte konkrétneho správneho alebo súdneho konania, prípadne konania v oblasti regulácie;

v) je to potrebné v záujme ochrany životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby; alebo

vi) ak sa neuplatňuje žiadna z uvedených podmienok, dovozca údajov získal výslovný súhlas dotknutej osoby s následným prenosom v konkrétnej situácii po tom, ako ju informoval o jeho účele, totožnosti príjemcu a možných rizikách takéhoto prenosu pre ňu z dôvodu nedostatku primeraných záruk v oblasti ochrany údajov. V tomto prípade dovozca údajov informuje vývozcu údajov a na jeho žiadosť mu odovzdá kópiu informácií poskytnutých dotknutej osobe.

Na účely akéhokoľvek následného prenosu sa vyžaduje, aby dovozca údajov dodržiaval všetky ostatné záruky podľa týchto doložiek, osobitne obmedzenie účelu.

8.8. Spracúvanie na základe poverenia dovozcu údajov

Dovozca údajov zabezpečí, aby akákoľvek osoba konajúca na základe jeho poverenia vrátane sprostredkovateľa spracúvala údaje výlučne podľa jeho pokynov.

8.9. Dokumentácia a splnenie povinností

a) Každá zmluvná strana musí byť schopná preukázať splnenie svojich povinností podľa týchto doložiek. Dovozca údajov uchováva najmä príslušnú dokumentáciu týkajúcu sa spracovateľských činností vykonávaných v rámci jeho zodpovednosti.

b) Dovozca údajov na požiadanie sprístupní túto dokumentáciu príslušnému dozornému orgánu.

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

8.1. Pokyny

a) Dovozca údajov spracúva osobné údaje len na základe zdokumentovaných pokynov vývozcu údajov. Vývozca údajov môže udeľovať takéto pokyny počas celého trvania zmluvy.

b) Dovozca údajov bezodkladne informuje vývozcu údajov, ak nie je schopný tieto pokyny dodržať.

8.2. Obmedzenie účelu

Dovozca údajov je oprávnený spracúvať osobné údaje len na osobitné účely prenosu stanovené v prílohe I časti B, ak vývozca údajov neudelí iné pokyny.

8.3. Transparentnosť

Vývozca údajov sprístupní dotknutej osobe na požiadanie a bezplatne kópiu týchto doložiek vrátane dodatku, ktorý vyplnili zmluvné strany. V rozsahu potrebnom na ochranu obchodného tajomstva alebo iných dôverných informácií vrátane opatrení uvedených v prílohe II a osobných údajov môže vývozca údajov pred poskytnutím kópie dodatku k týmto doložkám odstrániť časť jeho textu, pričom poskytne zmysluplné zhrnutie, ak by dotknutá osoba inak nebola schopná pochopiť jeho obsah alebo uplatňovať svoje práva. Zmluvné strany na požiadanie oznámia dotknutej osobe dôvody odstránenia textu, pokiaľ možno bez toho, aby došlo k prezradeniu odstránených informácií. Touto doložkou nie sú dotknuté povinnosti vývozcu údajov podľa článkov 13 a 14 nariadenia (EÚ) 2016/679.

8.4. Správnosť

Ak dovozca údajov zistí, že osobné údaje, ktoré získal, sú nesprávne alebo neaktuálne, bez zbytočného odkladu o tom informuje vývozcu údajov. V takom prípade je dovozca údajov povinný spolupracovať s vývozcom údajov na účely výmazu alebo opravy údajov.

8.5. Obdobie spracúvania, výmaz alebo vrátenie údajov

Dovozca údajov je oprávnený spracúvať údaje len počas obdobia uvedeného v prílohe I časti B. Po ukončení poskytovania spracovateľských služieb dovozca údajov vymaže všetky osobné údaje spracúvané v mene vývozcu údajov a vývozcovi údajov túto skutočnosť potvrdí, alebo vývozcovi údajov vráti všetky osobné údaje spracúvané v jeho mene a vymaže existujúce kópie, a to podľa toho, pre ktorú z možností sa vývozca údajov rozhodne. Dovozca údajov zabezpečuje dodržiavanie týchto doložiek dovtedy, kým nedôjde k vymazaniu alebo vráteniu údajov. Pokiaľ ide o miestne právne predpisy uplatniteľné na dovozcu údajov, ktorými sa zakazuje vrátenie alebo vymazanie osobných údajov, dovozca údajov vyhlasuje, že bude naďalej zabezpečovať súlad s týmito doložkami a bude ich spracúvať len v takom rozsahu a tak dlho, ako to vyžaduje uvedené miestne právo. Tým nie je dotknutá doložka 14, najmä povinnosť dovozcu údajov podľa doložky 14 písm. e) zasielať počas trvania zmluvy vývozcovi údajov oznámenia v prípade, keď má dôvod domnievať sa, že sa naň vzťahujú alebo začali vzťahovať právne predpisy alebo prax, ktoré nie sú v súlade s požiadavkami uvedenými v doložke 14 písm. a).

8.6. Bezpečnosť spracúvania

a) Dovozca údajov a počas prenosu aj vývozca údajov prijmú vhodné technické a organizačné opatrenia na zaistenie bezpečnosti údajov vrátane ochrany pred porušením bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu alebo prístupu k týmto údajom (ďalej len „porušenie ochrany osobných údajov“). Pri posudzovaní primeranej úrovne bezpečnosti zmluvné strany náležite zohľadnia najnovšie poznatky, náklady na vykonanie, povahu, rozsah, kontext a účely spracúvania, ako aj riziká pre dotknuté osoby, ktoré súvisia so spracúvaním. Zmluvné strany zvážia najmä použitie šifrovania alebo pseudonymizácie, a to aj počas prenosu, ak možno vďaka nim splniť účel spracúvania. V prípade pseudonymizácie zostávajú dodatočné informácie na priradenie osobných údajov ku konkrétnej dotknutej osobe, ak je to možné,

pod výlučnou kontrolou vývozcu údajov. Pri plnení si povinností podľa tohto písmena je dovozca údajov povinný prijať prinajmenšom technické a organizačné opatrenia uvedené v prílohe II. Dovozca údajov je povinný vykonávať pravidelné kontroly s cieľom zabezpečiť, aby tieto opatrenia nepretržite poskytovali primeranú úroveň bezpečnosti.

b) Dovozca údajov poskytne prístup k osobným údajom svojim zamestnancom len v rozsahu, ktorý je nevyhnutne potrebný na plnenie, riadenie a monitorovanie zmluvy. Zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú dôvernosť údajov, alebo aby sa na ne vzťahovala primeraná zákonná povinnosť zachovávať dôvernosť údajov.

c) V prípade porušenia ochrany osobných údajov týkajúceho sa osobných údajov spracúvaných dovozcom údajov podľa týchto doložiek prijme dovozca údajov primerané opatrenia na nápravu porušenia vrátane opatrení na zmiernenie jeho nepriaznivých účinkov. Dovozca údajov zašle vývozcovi údajov aj oznámenie o porušení bez zbytočného odkladu po tom, ako sa o tomto porušení dozvedel. Takéto oznámenie obsahuje údaje kontaktného miesta, kde možno získať viac informácií, opis povahy porušenia (podľa možnosti vrátane kategórií a približného počtu dotknutých osôb a záznamov o osobných údajoch), pravdepodobné následky porušenia, ako aj prijaté alebo navrhované opatrenia s cieľom napraviť porušenie, v prípade potreby vrátane opatrení na zmiernenie jeho možných nepriaznivých účinkov. Pokiaľ nemožno poskytnúť všetky informácie súčasne, pôvodné oznámenie musí obsahovať informácie, ktoré boli v danom čase dostupné, pričom ďalšie informácie sa poskytnú bez zbytočného odkladu po tom, ako budú k dispozícii.

d) Dovozca údajov spolupracuje s vývozcom údajov a poskytuje mu pomoc pri plnení si povinností podľa nariadenia (EÚ) 2016/679, najmä pokiaľ ide o podávanie oznámení príslušnému dozornému orgánu a dotknutým osobám, ktoré sú ovplyvnené, pričom zohľadní povahu spracúvania a informácie, ktoré má k dispozícii dovozca údajov.

8.7. Citlivé údaje

Ak prenos zahŕňa osobné údaje odhaľujúce rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, genetické alebo biometrické údaje na účely jedinečnej identifikácie fyzickej osoby, údaje týkajúce sa zdravia alebo sexuálneho života či sexuálnej orientácie osoby, alebo údaje týkajúce sa odsúdenia za trestné činy (ďalej len „citlivé údaje“), uplatňuje dovozca údajov osobitné obmedzenia a/alebo dodatočné záruky stanovené v prílohe I časti B.

8.8. Následné prenosy

Dovozca údajov poskytuje osobné údaje tretej strane len na základe zdokumentovaných pokynov vývozcu údajov. Údaje možno navyše poskytnúť tretej strane nachádzajúcej sa mimo Európskej únie (4) (v rovnakej krajine ako dovozca údajov alebo v inej tretej krajine, ďalej len „následný prenos“) len vtedy, ak je táto tretia strana viazaná týmito doložkami alebo súhlasí s tým, že bude týmito doložkami viazaná, a to v súlade s príslušným modulom, alebo ak:

i) následný prenos sa uskutočňuje do krajiny, na ktorú sa vzťahuje rozhodnutie o primeranosti podľa článku45 nariadenia (EÚ) 2016/679, ktorého predmetom je následný prenos;

ii) tretia strana inak zabezpečuje primerané záruky podľa článkov 46 alebo 47 nariadenia (EÚ) 2016/679 v súvislosti s predmetným spracúvaním;

iii) následný prenos je nevyhnutný na účely preukazovania, uplatňovania alebo ochrany právnych nárokov v kontexte konkrétneho správneho alebo súdneho konania, prípadne konania v oblasti regulácie; alebo

iv) následný prenos je potrebný v záujme ochrany životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby.

Na účely akéhokoľvek následného prenosu sa vyžaduje, aby dovozca údajov dodržiaval všetky ostatné záruky podľa týchto doložiek, osobitne obmedzenie účelu.

8.9. Dokumentácia a splnenie povinností

a) Dovozca údajov sa bezodkladne a primerane zaoberá žiadosťami vývozcu údajov, ktoré sa týkajú spracúvania podľa týchto doložiek.

b) Zmluvné strany musia byť schopné preukázať, že si splnili povinnosti podľa týchto doložiek. Dovozca údajov uchováva najmä príslušnú dokumentáciu týkajúcu sa spracovateľských činností vykonávaných v mene vývozcu údajov.

c) Dovozca údajov sprístupní vývozcovi údajov všetky informácie potrebné na preukázanie splnenia povinností stanovených v týchto doložkách a na žiadosť vývozcu údajov umožní audity spracovateľských činností, na ktoré sa vzťahujú tieto doložky, a poskytne pri nich potrebnú súčinnosť v primeraných intervaloch alebo ak existujú náznaky nesplnenia povinností. Pri rozhodovaní o preskúmaní alebo audite môže vývozca údajov zohľadniť relevantné certifikácie, ktorými disponuje dovozca údajov.

d) Vývozca údajov sa môže rozhodnúť, či vykoná audit sám alebo poverí nezávislého audítora. Audity môžu zahŕňať inšpekcie v priestoroch alebo fyzických zariadeniach dovozcu údajov a v prípade potreby sa vykonávajú po primeranom upovedomení.

e) Zmluvné strany sprístupnia príslušnému dozornému orgánu na požiadanie informácie uvedené v písmenách b) a c) vrátane výsledkov všetkých auditov.

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

8.1. Pokyny

a) Vývozca údajov informoval dovozcu údajov, že koná ako sprostredkovateľ podľa pokynov prevádzkovateľa, ktoré dá vývozca údajov pred spracúvaním k dispozícii dovozcovi údajov.

b) Dovozca údajov spracúva osobné údaje len na základe zdokumentovaných pokynov prevádzkovateľa, ktoré dovozcovi údajov oznámil vývozca údajov, a akýchkoľvek dodatočných zdokumentovaných pokynov vývozcu údajov. Takéto dodatočné pokyny nesmú byť v rozpore s pokynmi prevádzkovateľa. Prevádzkovateľ alebo vývozca údajov môže udeľovať ďalšie zdokumentované pokyny týkajúce sa spracúvania údajov počas celého trvania zmluvy.

c) Dovozca údajov bezodkladne informuje vývozcu údajov, ak nie je schopný tieto pokyny dodržať. Ak dovozca údajov nie je schopný dodržať pokyny prevádzkovateľa, vývozca údajov bezodkladne zašle oznámenie prevádzkovateľovi.

d) Vývozca údajov vyhlasuje, že dovozcovi údajov uložil rovnaké povinnosti v oblasti ochrany údajov, ako sú stanovené v zmluve alebo inom právnom akte podľa práva Únie alebo členského štátu, ktoré boli uzatvorené medzi prevádzkovateľom a vývozcom údajov (5).

8.2. Obmedzenie účelu

Dovozca údajov je oprávnený spracúvať osobné údaje len na osobitné účely prenosu stanovené v prílohe I časti B, ak neexistujú iné pokyny prevádzkovateľa, ktoré vývozca údajov oznámil dovozcovi údajov, ani iné pokyny vývozcu údajov.

8.3. Transparentnosť

Vývozca údajov sprístupní dotknutej osobe na požiadanie a bezplatne kópiu týchto doložiek vrátane dodatku, ktorý vyplnili zmluvné strany. V rozsahu potrebnom na ochranu obchodného tajomstva alebo iných dôverných informácií vrátane osobných údajov môže vývozca údajov pred poskytnutím kópie dodatku odstrániť časť jeho textu, pričom však poskytne zmysluplné zhrnutie, ak by dotknutá osoba inak nebola schopná pochopiť jeho obsah alebo uplatňovať svoje práva. Zmluvné strany na požiadanie oznámia dotknutej osobe dôvody odstránenia textu, pokiaľ možno bez toho, aby došlo k prezradeniu odstránených informácií.

8.4. Správnosť

Ak dovozca údajov zistí, že osobné údaje, ktoré získal, sú nesprávne alebo neaktuálne, bez zbytočného odkladu o tom informuje vývozcu údajov. V takom prípade je dovozca údajov povinný spolupracovať s vývozcom údajov na účely opravy alebo výmazu údajov.

8.5. Obdobie spracúvania, výmaz alebo vrátenie údajov

Dovozca údajov je oprávnený spracúvať údaje len počas obdobia uvedeného v prílohe I časti B. Po ukončení poskytovania spracovateľských služieb dovozca údajov vymaže všetky osobné údaje spracúvané v mene prevádzkovateľa a vývozcovi údajov túto skutočnosť potvrdí, alebo vývozcovi údajov vráti všetky osobné údaje spracúvané v jeho mene a vymaže existujúce kópie, a to podľa toho, pre ktorú z možností sa vývozca údajov rozhodne. Dovozca údajov zabezpečuje dodržiavanie týchto doložiek dovtedy, kým nedôjde k vymazaniu alebo vráteniu údajov. Pokiaľ ide o miestne právne predpisy uplatniteľné na dovozcu údajov, ktorými sa zakazuje vrátenie alebo vymazanie osobných údajov, dovozca údajov vyhlasuje, že bude naďalej zabezpečovať súlad s týmito doložkami a bude ich spracúvať len v takom rozsahu a tak dlho, ako to vyžaduje uvedené miestne právo. Tým nie je dotknutá doložka 14, najmä povinnosť dovozcu údajov podľa doložky 14 písm. e) zasielať počas trvania zmluvy vývozcovi údajov oznámenia v prípade, keď má dôvod domnievať sa, že sa naň vzťahujú alebo začali vzťahovať právne predpisy alebo prax, ktoré nie sú v súlade s požiadavkami uvedenými v doložke 14 písm. a).

8.6. Bezpečnosť spracúvania

a) Dovozca údajov a počas prenosu aj vývozca údajov prijmú vhodné technické a organizačné opatrenia na zaistenie bezpečnosti údajov vrátane ochrany pred porušením bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu alebo prístupu k týmto údajom (ďalej len „porušenie ochrany osobných údajov“). Pri posudzovaní primeranej úrovne bezpečnosti náležite zohľadnia najnovšie poznatky, náklady na vykonanie, povahu, rozsah, kontext a účely spracúvania, ako aj riziká pre dotknutú osobu, ktoré súvisia so spracúvaním. Zmluvné strany zvážia najmä použitie šifrovania alebo pseudonymizácie, a to aj počas prenosu, ak možno vďaka nim splniť účel spracúvania. V prípade pseudonymizácie zostávajú dodatočné informácie na priradenie osobných údajov ku konkrétnej dotknutej osobe, ak je to možné, pod výlučnou kontrolou vývozcu údajov alebo prevádzkovateľa. Pri plnení si povinností podľa tohto písmena je dovozca údajov povinný prijať prinajmenšom technické a organizačné opatrenia uvedené v prílohe II. Dovozca údajov je povinný vykonávať pravidelné kontroly s cieľom zabezpečiť, aby tieto opatrenia nepretržite poskytovali primeranú úroveň bezpečnosti.

b) Dovozca údajov poskytne prístup k údajom svojim zamestnancom len v rozsahu, ktorý je nevyhnutne potrebný na plnenie, riadenie a monitorovanie zmluvy. Zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú dôvernosť údajov, alebo aby sa na ne vzťahovala primeraná zákonná povinnosť zachovávať dôvernosť údajov.

c) V prípade porušenia ochrany osobných údajov týkajúceho sa osobných údajov spracúvaných dovozcom údajov podľa týchto doložiek prijme dovozca údajov primerané opatrenia na nápravu porušenia vrátane opatrení na zmiernenie jeho nepriaznivých účinkov. Dovozca údajov bez zbytočného odkladu zašle oznámenie vývozcovi údajov a v prípade potreby, ak je to možné, aj prevádzkovateľovi po tom, ako sa dozvedel o porušení. Takéto oznámenie obsahuje údaje kontaktného miesta, kde možno získať viac informácií, opis povahy porušenia (podľa možnosti vrátane kategórií a približného počtu dotknutých osôb a záznamov o osobných údajoch),

pravdepodobné následky porušenia, ako aj prijaté alebo navrhované opatrenia s cieľom napraviť porušenie ochrany údajov vrátane opatrení na zmiernenie jeho možných nepriaznivých účinkov. Pokiaľ nemožno poskytnúť všetky informácie súčasne, pôvodné oznámenie musí obsahovať informácie, ktoré boli v danom čase dostupné, pričom ďalšie informácie sa poskytnú bez zbytočného odkladu po tom, ako budú k dispozícii.

d) Dovozca údajov spolupracuje s vývozcom údajov a poskytuje mu pomoc pri plnení si povinností podľa nariadenia (EÚ) 2016/679, najmä pokiaľ ide o podávanie oznámení prevádzkovateľovi tak, aby mohol tento prevádzkovateľ následne zaslať oznámenie príslušnému dozornému orgánu a dotknutým osobám, ktoré sú ovplyvnené, pričom zohľadní povahu spracúvania a informácie, ktoré má k dispozícii dovozca údajov.

8.7. Citlivé údaje

Ak prenos zahŕňa osobné údaje odhaľujúce rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, genetické alebo biometrické údaje na účely jedinečnej identifikácie fyzickej osoby, údaje týkajúce sa zdravia alebo sexuálneho života či sexuálnej orientácie osoby, alebo údaje týkajúce sa odsúdenia za trestné činy (ďalej len „citlivé údaje“), uplatňuje dovozca údajov osobitné obmedzenia a/alebo dodatočné záruky stanovené v prílohe I časti B.

8.8. Následné prenosy

Dovozca údajov poskytuje osobné údaje tretej strane len na základe zdokumentovaných pokynov prevádzkovateľa, ktoré dovozcovi údajov oznámil vývozca údajov. Údaje možno navyše poskytnúť tretej strane nachádzajúcej sa mimo Európskej únie (6) (v rovnakej krajine ako dovozca údajov alebo v inej tretej krajine, ďalej len „následný prenos“) len vtedy, ak je táto tretia strana viazaná týmito doložkami alebo súhlasí s tým, že bude týmito doložkami viazaná, a to v súlade s príslušným modulom, alebo ak:

i) následný prenos sa uskutočňuje do krajiny, na ktorú sa vzťahuje rozhodnutie o primeranosti podľa článku45 nariadenia (EÚ) 2016/679, ktorého predmetom je následný prenos;

ii) tretia strana inak zabezpečuje primerané záruky podľa článkov 46 alebo 47 nariadenia (EÚ) 2016/679;

iii) následný prenos je nevyhnutný na účely preukazovania, uplatňovania alebo ochrany právnych nárokov v kontexte konkrétneho správneho alebo súdneho konania, prípadne konania v oblasti regulácie; alebo

iv) následný prenos je potrebný v záujme ochrany životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby.

Na účely akéhokoľvek následného prenosu sa vyžaduje, aby dovozca údajov dodržiaval všetky ostatné záruky podľa týchto doložiek, osobitne obmedzenie účelu.

8.9. Dokumentácia a splnenie povinností

a) Dovozca údajov sa bezodkladne a primerane zaoberá žiadosťami vývozcu údajov alebo prevádzkovateľa, ktoré sa týkajú spracúvania podľa týchto doložiek.

b) Zmluvné strany musia byť schopné preukázať, že si splnili povinnosti podľa týchto doložiek. Dovozca údajov uchováva najmä príslušnú dokumentáciu týkajúcu sa spracovateľských činností vykonávaných v mene prevádzkovateľa.

c) Dovozca údajov sprístupní vývozcovi údajov všetky informácie potrebné na preukázanie splnenia povinností stanovených v týchto doložkách, pričom vývozca údajov ich poskytne prevádzkovateľovi.

d) Dovozca údajov umožní vývozcovi údajov audity spracovateľských činností, na ktoré sa vzťahujú tieto doložky, a poskytne pri nich potrebnú súčinnosť v primeraných intervaloch alebo ak existujú náznaky nesplnenia povinností.

To isté platí aj v prípade, keď vývozca údajov žiada o audit na základe pokynov prevádzkovateľa. Pri rozhodovaní o audite môže vývozca údajov zohľadniť relevantné certifikácie, ktorými disponuje dovozca údajov.

e) Ak sa audit vykonáva na základe pokynov prevádzkovateľa, vývozca údajov sprístupní výsledky prevádzkovateľovi.

f) Vývozca údajov sa môže rozhodnúť, či vykoná audit sám alebo poverí nezávislého audítora. Audity môžu zahŕňať inšpekcie v priestoroch alebo fyzických zariadeniach dovozcu údajov a v prípade potreby sa vykonávajú po primeranom upovedomení.

g) Zmluvné strany sprístupnia príslušnému dozornému orgánu na požiadanie informácie uvedené v písmenách b) a c) vrátane výsledkov všetkých auditov.

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

8.1. Pokyny

a) Vývozca údajov spracúva osobné údaje len na základe zdokumentovaných pokynov dovozcu údajov v postavení prevádzkovateľa.

b) Vývozca údajov bezodkladne informuje dovozcu údajov, ak nie je schopný dodržať predmetné pokyny, a to aj v prípade, že dané pokyny porušujú nariadenie (EÚ) 2016/679 alebo iné právne predpisy Únie alebo členského štátu o ochrane údajov.

c) Dovozca údajov sa zdrží akéhokoľvek konania, ktoré by vývozcovi údajov bránilo v plnení povinností podľa nariadenia (EÚ) 2016/679, a to aj v kontexte ďalšieho sprostredkovania alebo pokiaľ ide o spoluprácu s príslušnými dozornými orgánmi.

d) Po ukončení poskytovania spracovateľských služieb vývozca údajov vymaže všetky osobné údaje spracúvané v mene dovozcu údajov a dovozcovi údajov túto skutočnosť potvrdí, alebo dovozcovi údajov vráti všetky osobné údaje spracúvané v jeho mene a vymaže existujúce kópie, a to podľa toho, pre ktorú z možností sa dovozca údajov rozhodne.

8.2. Bezpečnosť spracúvania

a) Zmluvné strany prijmú primerané technické a organizačné opatrenia na zaistenie bezpečnosti údajov, a to aj počas prenosu, ako aj ochrany pred porušením bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu alebo prístupu (ďalej len „porušenie ochrany osobných údajov“). Pri posudzovaní primeranej úrovne bezpečnosti náležite zohľadňujú najnovšie poznatky, náklady na vykonanie opatrení, povahu osobných údajov (7), povahu, rozsah, kontext a účel spracúvania a riziká spojené s spracúvaním pre dotknuté osoby, pričom najmä zvážia použitie šifrovania alebo pseudonymizácie, a to aj počas prenosu, ak možno vďaka nim splniť účel spracúvania.

b) Vývozca údajov pomáha dovozcovi údajov zabezpečiť primeranú bezpečnosť údajov v súlade s písmenom a). V prípade porušenia ochrany osobných údajov týkajúceho sa osobných údajov spracúvaných vývozcom údajov podľa týchto doložiek zašle vývozca údajov oznam dovozcovi údajov bez zbytočného odkladu po tom, ako sa o tejto skutočnosti dozvie, a dovozcovi údajov poskytne pomoc pri náprave porušenia.

c) Vývozca údajov zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú dôvernosť údajov, alebo aby sa na ne vzťahovala primeraná zákonná povinnosť zachovávať dôvernosť údajov.

8.3. Dokumentácia a splnenie povinností

a) Zmluvné strany musia byť schopné preukázať, že si splnili povinnosti podľa týchto doložiek.

b) Vývozca údajov sprístupní dovozcovi údajov všetky informácie potrebné na preukázanie, že si splnil povinnosti podľa týchto doložiek, umožní audity a poskytne pri nich potrebnú súčinnosť.

Doložka 9 Využívanie ďalších sprostredkovateľov

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

Dovozca údajov má všeobecné povolenie vývozcu údajov na zapojenie ďalších sprostredkovateľov z dohodnutého zoznamu. Dovozca údajov osobitne písomne informuje vývozcu údajov o všetkých zamýšľaných zmenách v tomto zozname, pokiaľ ide o pridanie alebo nahradenie ďalších sprostredkovateľov, a to najmenej [uveďte časové obdobie] vopred, čím poskytne vývozcovi údajov dostatočný čas na to, aby mohol proti takýmto zmenám vzniesť námietky pred zapojením ďalšieho sprostredkovateľa. Dovozca údajov poskytne vývozcovi údajov informácie, na základe ktorých môže uplatniť svoje právo namietať.

b) Ak dovozca údajov zapojí ďalšieho sprostredkovateľa do vykonávania konkrétnych spracovateľských činností (v mene vývozcu údajov), urobí to na základe písomnej zmluvy, v ktorej sa v podstate stanovujú rovnaké povinnosti v oblasti ochrany údajov ako sú tie, ktoré má dovozca údajov podľa týchto doložiek, a to aj pokiaľ ide o práva oprávnenej tretej strany v prípade dotknutých osôb. (8) Zmluvné strany vyhlasujú, že splnením povinností v zmysle tejto doložky si dovozca údajov zároveň splní aj povinnosti v zmysle doložky 8.8. Dovozca údajov zabezpečí, aby ďalší sprostredkovateľ dodržiaval povinnosti, ktoré sa podľa týchto doložiek vzťahujú na dovozcu údajov.

c) Dovozca údajov poskytne vývozcovi údajov na jeho žiadosť kópiu dohody s ďalším sprostredkovateľom, ako aj neskorších zmien tejto dohody. V rozsahu potrebnom na ochranu obchodného tajomstva alebo iných dôverných informácií vrátane osobných údajov môže dovozca údajov pred poskytnutím kópie tejto dohody odstrániť časti jej textu.

d) Dovozca údajov naďalej v plnom rozsahu zodpovedá vývozcovi údajov za plnenie povinností ďalšieho sprostredkovateľa podľa zmluvy, ktorú uzatvoril s dovozcom údajov. Dovozca údajov zašle vývozcovi údajov oznámenie o každom porušení povinností ďalšieho sprostredkovateľa v zmysle uvedenej zmluvy.

e) Dovozca údajov sa dohodne s ďalším sprostredkovateľom na doložke o oprávnenosti tretej strany, podľa ktorej má vývozca údajov v prípade, že dovozca údajov fakticky zanikol, prestal podľa práva existovať alebo sa stal insolventným, právo vypovedať zmluvu s ďalším sprostredkovateľom a ďalšiemu sprostredkovateľovi dať pokyn, aby osobné údaje vymazal alebo vrátil.

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

a) Dovozca údajov má všeobecné povolenie prevádzkovateľa na zapojenie ďalších sprostredkovateľov z dohodnutého zoznamu. Dovozca údajov osobitne písomne informuje prevádzkovateľa o všetkých zamýšľaných zmenách v tomto zozname, pokiaľ ide o pridanie alebo nahradenie ďalších sprostredkovateľov, a to najmenej [uveďte časové obdobie] vopred, čím poskytne prevádzkovateľovi dostatočný čas na to, aby mohol proti takýmto zmenám vzniesť námietky pred zapojením ďalšieho sprostredkovateľa. Dovozca údajov poskytne prevádzkovateľovi informácie, na základe ktorých môže uplatniť svoje právo namietať. Dovozca údajov informuje vývozcu údajov o zapojení ďalšieho sprostredkovateľa.

b) Ak dovozca údajov zapojí ďalšieho sprostredkovateľa do vykonávania konkrétnych spracovateľských činností (v mene prevádzkovateľa), urobí to na základe písomnej zmluvy, v ktorej sa v podstate stanovujú rovnaké povinnosti v oblasti ochrany údajov ako sú tie, ktoré má dovozca údajov podľa týchto doložiek, a to aj pokiaľ ide o práva oprávnenej tretej strany v prípade dotknutých osôb. (9) Zmluvné strany vyhlasujú, že splnením povinností v zmysle tejto doložky si dovozca údajov zároveň splní aj povinnosti v zmysle doložky 8.8. Dovozca údajov zabezpečí, aby ďalší sprostredkovateľ dodržiaval povinnosti, ktoré sa podľa týchto doložiek vzťahujú na dovozcu údajov.

c) Dovozca údajov poskytne vývozcovi údajov na jeho žiadosť alebo na žiadosť prevádzkovateľa kópiu dohody s ďalším sprostredkovateľom, ako aj neskorších zmien tejto dohody V rozsahu potrebnom na ochranu obchodného tajomstva alebo iných dôverných informácií vrátane osobných údajov môže dovozca údajov pred poskytnutím kópie tejto dohody odstrániť časti jej textu.

d) Dovozca údajov naďalej v plnom rozsahu zodpovedá vývozcovi údajov za plnenie povinností ďalšieho sprostredkovateľa podľa zmluvy, ktorú uzatvoril s dovozcom údajov. Dovozca údajov zašle vývozcovi údajov oznámenie o každom porušení povinností ďalšieho sprostredkovateľa v zmysle uvedenej zmluvy.

e) Dovozca údajov sa dohodne s ďalším sprostredkovateľom na doložke o oprávnenosti tretej strany, podľa ktorej má vývozca údajov v prípade, že dovozca údajov fakticky zanikol, prestal podľa práva existovať alebo sa stal insolventným, právo vypovedať zmluvu s ďalším sprostredkovateľom a ďalšiemu sprostredkovateľovi dať pokyn, aby osobné údaje vymazal alebo vrátil.

Doložka 10 Práva dotknutých osôb

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

a) Dovozca údajov sa prípadne s pomocou vývozcu údajov zaoberá všetkými otázkami a žiadosťami, ktoré dostane od dotknutej osoby a ktoré sa týkajú spracúvania jej osobných údajov a uplatňovania jej práv podľa týchto doložiek, a to bez zbytočného odkladu a najneskôr do jedného mesiaca od prijatia predmetnej otázky alebo žiadosti. (10) Dovozca údajov prijme vhodné opatrenia na uľahčenie týchto otázok, žiadostí a uplatňovania práv dotknutej osoby. Všetky informácie poskytnuté dotknutej osobe musia byť v zrozumiteľnej a ľahko dostupnej forme, pričom musia byť formulované jasne a jednoducho.

b) Na žiadosť dotknutej osoby dovozca údajov predovšetkým bezplatne:

i) poskytne dotknutej osobe potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú; ak áno, kópiu údajov, ktoré sa jej týkajú, a informácie v prílohe I; ak osobné údaje boli alebo budú následne prenášané, poskytne informácie o príjemcoch alebo kategóriách príjemcov (podľa potreby s cieľom poskytnúť zmysluplné informácie), ktorým osobné údaje boli alebo budú následne prenášané, účel takýchto následných prenosov a ich dôvod podľa doložky 8.7; a poskytne informácie o práve podať sťažnosť dozornému orgánu v súlade s doložkou 12 písm. c) bodom i);

ii) opraví nesprávne alebo neúplné údaje týkajúce sa dotknutej osoby;

iii) vymaže osobné údaje týkajúce sa dotknutej osoby, ak sa takéto údaje spracúvajú alebo spracúvali v rozpore s doložkami, ktorých cieľom je zabezpečiť práva oprávnenej tretej strany, alebo ak dotknutá osoba odvolá súhlas, na ktorom je spracúvanie založené.

c) Ak dovozca údajov spracúva osobné údaje na účely priameho marketingu, spracúvanie na tieto účely ukončí, ak dotknutá osoba proti tomu namieta.

d) Dovozca údajov nie je oprávnený založiť rozhodnutie len na automatizovanom spracúvaní prenášaných osobných údajov (ďalej len „automatizované rozhodnutie“), ktoré by vyvolávalo právne účinky týkajúce sa dotknutej osoby alebo by ju podobne významne ovplyvňovalo, okrem prípadu, že by s tým dotknutá osoba výslovne súhlasila alebo dovozca údajov má na to oprávnenie podľa právnych predpisov krajiny určenia, pokiaľ sa v týchto právnych predpisoch stanovujú vhodné opatrenia na zaručenie práv a oprávnených záujmov dotknutej osoby. V takom prípade je dovozca údajov samostatne alebo v spolupráci s vývozcom údajov povinný:

i) informovať dotknutú osobu o zamýšľanom automatizovanom rozhodnutí a dôsledkoch, ako aj o súvisiacej logike, a

ii) zaviesť vhodné záruky, a to aspoň tak, že sa dotknutej osobe umožní napadnúť predmetné rozhodnutie, vyjadriť svoj názor a dosiahnuť preskúmanie človekom.

e) Ak sú žiadosti dotknutej osoby neprimerané najmä z dôvodu ich opakujúcej sa povahy, dovozca údajov môže buď vyúčtovať primeraný poplatok zohľadňujúci administratívne náklady v súvislosti s vybavením žiadosti, alebo žiadosť odmietnuť.

f) Dovozca údajov môže žiadosť dotknutej osoby zamietnuť, ak takéto zamietnutie povoľujú právne predpisy krajiny určenia, pričom je to nevyhnutné a primerané v demokratickej spoločnosti na ochranu jedného z cieľov uvedených v článku 23 ods. 1 nariadenia (EÚ) 2016/679.

g) Ak má dovozca údajov v úmysle zamietnuť žiadosť dotknutej osoby, informuje dotknutú osobu o dôvodoch zamietnutia a možnosti podať sťažnosť príslušnému dozornému orgánu a/alebo domáhať sa nápravy na súde.

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

a) Dovozca údajov bezodkladne oznámi vývozcovi údajov každú žiadosť, ktorú dostal od dotknutej osoby. Na túto žiadosť nie je oprávnený sám reagovať, pokiaľ mu to vývozca údajov nepovolil.

b) Dovozca údajov pomáha vývozcovi údajov pri plnení povinnosti reagovať na žiadosti dotknutých osôb o výkon ich práv podľa nariadenia (EÚ) 2016/679. V tejto súvislosti zmluvné strany stanovia v prílohe II vhodné technické a organizačné opatrenia na poskytnutie pomoci, ako aj rozsah potrebnej pomoci, a to s ohľadom na povahu spracúvania.

c) Dovozca údajov dodržiava pri plnení svojich povinností podľa písmen a) a b) pokyny vývozcu údajov

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

a) Dovozca údajov bezodkladne oznámi vývozcovi údajov a v prípade potreby aj prevádzkovateľovi každú žiadosť, ktorú dostal od dotknutej osoby, a to bez toho, aby na ňu reagoval, pokiaľ na to nebol poverený prevádzkovateľom.

b) Dovozca údajov v prípade potreby v spolupráci s vývozcom údajov pomáha prevádzkovateľovi pri plnení povinnosti reagovať na žiadosti dotknutých osôb o výkon ich práv podľa nariadenia (EÚ) 2016/679, prípadne nariadenia (EÚ) 2018/1725. V tejto súvislosti zmluvné strany stanovia v prílohe II vhodné technické a organizačné opatrenia na poskytnutie pomoci, ako aj rozsah potrebnej pomoci, a to s ohľadom na povahu spracúvania.

c) Dovozca údajov dodržiava pri plnení svojich povinností podľa písmen a) a b) pokyny prevádzkovateľa, ktoré mu oznámil vývozca údajov.

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

Zmluvné strany si navzájom poskytujú pomoc pri reagovaní na otázky a žiadosti dotknutých osôb podľa miestneho práva uplatniteľného na dovozcu údajov alebo v prípade spracúvania údajov vývozcom údajov v EÚ podľa nariadenia (EÚ) 2016/679.

Doložka 11 Náprava

a) Dovozca údajov informuje dotknuté osoby v transparentnom a ľahko dostupnom formáte prostredníctvom individuálneho oznámenia alebo na svojom webovom sídle o kontaktnom mieste, ktoré je oprávnené vybavovať sťažnosti. Bezodkladne sa zaoberá všetkými sťažnosťami, ktoré dostane od dotknutej osoby.

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

b) V prípade sporu medzi dotknutou osobou a jednou zo zmluvných strán, ktorý sa týka dodržiavania ustanovení týchto doložiek, vynaloží táto zmluvná strana maximálne úsilie na rýchle vyriešenie sporu formou zmieru. Zmluvné strany sa navzájom informujú o takýchto sporoch a v prípade potreby spolupracujú na ich riešení.

c) Ak sa dotknutá osoba odvoláva na právo oprávnenej tretej strany podľa doložky 3, dovozca údajov akceptuje rozhodnutie dotknutej osoby:

i) podať sťažnosť dozornému orgánu v členskom štáte svojho obvyklého pobytu alebo miesta výkonu práce, alebo príslušnému dozornému orgánu podľa doložky 13;

ii) postúpiť spor príslušným súdom v zmysle doložky 18.

d) Zmluvné strany súhlasia s tým, aby dotknutú osobu zastupoval neziskový subjekt, organizácia alebo združenie za podmienok stanovených v článku 80 ods. 1 nariadenia (EÚ) 2016/679.

e) Dovozca údajov je povinný riadiť sa rozhodnutím, ktoré je záväzné podľa platných právnych predpisov EÚ alebo členského štátu.

f) Dovozca údajov vyjadruje súhlas s tým, že rozhodnutie dotknutej osoby nebude mať vplyv na jej hmotné a procesné práva domáhať sa nápravy v súlade s platnými právnymi predpismi.

Doložka 12 Zodpovednosť

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

a) Každá zmluvná strana je zodpovedná voči druhej zmluvnej strane za akúkoľvek ujmu, ktorú jej spôsobí v dôsledku porušenia týchto doložiek.

b) Každá zmluvná strana je zodpovedná voči dotknutej osobe za akúkoľvek majetkovú alebo nemajetkovú ujmu, ktorú spôsobí dotknutej osobe porušením práv oprávnenej tretej strany podľa týchto doložiek, pričom dotknutá osoba má nárok na náhradu uvedenej ujmy. Tým nie je dotknutá zodpovednosť vývozcu údajov podľa nariadenia (EÚ) 2016/679.

c) Ak je za ujmu spôsobenú dotknutej osobe v dôsledku porušenia týchto doložiek zodpovedná viac ako jedna zmluvná strana, tieto zmluvné strany zodpovedajú spoločne a nerozdielne, pričom dotknutá osoba je oprávnená podať žalobu na súd proti ktorejkoľvek z týchto zmluvných strán.

d) Zmluvné strany sa dohodli, že v prípade, keď nesie zodpovednosť podľa písmena c) jedna zmluvná strana, je oprávnená žiadať od druhej zmluvnej strany vrátenie časti náhrady vyjadrujúcej jej zodpovednosť za ujmu.

e) Dovozca údajov sa nemôže odvolávať na konanie sprostredkovateľa alebo ďalšieho sprostredkovateľa s cieľom zbaviť sa svojej vlastnej zodpovednosti.

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

a) Každá zmluvná strana je zodpovedná voči druhej zmluvnej strane za akúkoľvek ujmu, ktorú jej spôsobí v

dôsledku porušenia týchto doložiek.

b) Dovozca údajov je zodpovedný voči dotknutej osobe za akúkoľvek majetkovú alebo nemajetkovú ujmu, ktorú spôsobí on sám alebo ďalší sprostredkovateľ dotknutej osobe porušením práv oprávnenej tretej strany podľa týchto doložiek, pričom dotknutá osoba má nárok na náhradu uvedenej ujmy.

c) Bez ohľadu na písmeno b) je vývozca údajov zodpovedný voči dotknutej osobe za akúkoľvek majetkovú alebo nemajetkovú ujmu, ktorú on sám alebo dovozca údajov (prípadne ďalší sprostredkovateľ) spôsobí dotknutej osobe porušením práv oprávnenej tretej strany podľa týchto doložiek, pričom dotknutá osoba má nárok na náhradu uvedenej ujmy. Tým nie je dotknutá zodpovednosť vývozcu údajov a v prípade, že vývozca údajov je sprostredkovateľom konajúcim v mene prevádzkovateľa, ani zodpovednosť prevádzkovateľa podľa nariadenia (EÚ) 2016/679, prípadne nariadenia (EÚ) 2018/1725.

d) Zmluvné strany sa dohodli, že v prípade, keď nesie zodpovednosť za ujmu spôsobenú dovozcom údajov (alebo ďalším sprostredkovateľom) podľa písmena c) vývozca údajov, je oprávnený žiadať od dovozcu údajov vrátenie časti náhrady vyjadrujúcej jeho zodpovednosť za ujmu.

e) Ak je za ujmu spôsobenú dotknutej osobe v dôsledku porušenia týchto doložiek zodpovedná viac ako jedna zmluvná strana, tieto zmluvné strany zodpovedajú spoločne a nerozdielne, pričom dotknutá osoba je oprávnená podať žalobu na súd proti ktorejkoľvek z týchto zmluvných strán.

f) Zmluvné strany sa dohodli, že v prípade, keď nesie zodpovednosť jedna zmluvná strana podľa písmena e), je oprávnená žiadať od druhej zmluvnej strany vrátenie časti náhrady vyjadrujúcej jej zodpovednosť za ujmu.

g) Dovozca údajov sa nemôže odvolávať na konanie ďalšieho sprostredkovateľa s cieľom zbaviť sa svojej vlastnej zodpovednosti.

Doložka 13 Dohľad

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

a) [Ak je vývozca údajov usadený v členskom štáte EÚ:] Dozorný orgán zodpovedný za zabezpečenie toho, aby vývozca údajov dodržiaval ustanovenia nariadenia (EÚ) 2016/679 v oblasti prenosu údajov podľa prílohy I časti C, má postavenie príslušného dozorného orgánu.

[Ak vývozca údajov nie je usadený v členskom štáte EÚ, ale patrí do územnej pôsobnosti nariadenia (EÚ) 2016/679 v súlade s článkom 3 ods. 2, pričom určí zástupcu podľa článku 27 ods. 1 nariadenia (EÚ) 2016/679:] Dozorný orgán členského štátu, v ktorom je podľa prílohy I časti C usadený zástupca v zmysle článku 27 ods. 1 nariadenia (EÚ) 2016/679, má postavenie príslušného dozorného orgánu.

[Ak vývozca údajov nie je usadený v členskom štáte EÚ, ale patrí do územnej pôsobnosti nariadenia (EÚ) 2016/679 v súlade s článkom 3 ods. 2 bez toho, aby musel určiť zástupcu podľa článku 27 ods. 2 nariadenia (EÚ) 2016/679:] Dozorný orgán jedného z členských štátov, v ktorom sa nachádzajú dotknuté osoby, ktorých osobné údaje sa prenášajú v súlade s týmito doložkami v súvislosti s tovarom alebo službami, ktoré sa im ponúkajú, alebo ktorých správanie sa monitoruje, ako sa to uvádza v prílohe I časti C, má postavenie príslušného dozorného orgánu.

b) Dovozca údajov sa zaväzuje, že sa podriadi jurisdikcii príslušného dozorného orgánu a bude s ním spolupracovať v rámci akýchkoľvek konaní, ktorých cieľom je zabezpečiť dodržiavanie týchto doložiek. Dovozca údajov sa najmä zaväzuje reagovať na otázky, podriadiť sa auditom a konať v súlade s opatreniami prijatými

dozorným orgánom vrátane nápravných a kompenzačných opatrení. Dozornému orgánu poskytne písomné potvrdenie, že boli prijaté potrebné opatrenia.

ODDIEL III – MIESTNE PRÁVNE PREDPISY A POVINNOSTI V PRÍPADE PRÍSTUPU ORGÁNOV VEREJNEJ MOCI

Doložka 14 Miestne právne predpisy a prax, ktoré majú vplyv na dodržiavanie doložiek

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi (ak sprostredkovateľ v EÚ kombinuje osobné údaje prijaté od prevádzkovateľa z tretej krajiny s osobnými údajmi, ktoré získal sprostredkovateľ v EÚ)

a) Zmluvné strany vyhlasujú, že nemajú žiadny dôvod považovať právne predpisy a prax v tretej krajine určenia, pokiaľ ide o spracúvanie osobných údajov dovozcom údajov vrátane akýchkoľvek požiadaviek na poskytovanie osobných údajov alebo opatrení, ktorými sa povoľuje prístup orgánov verejnej moci, za prekážku, ktorá by bránila dovozcovi údajov v plnení jeho povinností vyplývajúcich z týchto doložiek. Uvedené vychádza z výkladu, podľa ktorého právne predpisy a prax, ktoré rešpektujú podstatu základných práv a slobôd a neprekračujú rámec toho, čo je nevyhnutné a primerané v demokratickej spoločnosti na zabezpečenie jedného z cieľov uvedených v článku 23 ods. 1 nariadenia (EÚ) 2016/679, nie sú v rozpore s týmito doložkami.

b) Zmluvné strany deklarujú, že v súvislosti s vyhlásením v písmene a) náležite zohľadnili najmä tieto prvky:

i) osobitné okolnosti prenosu vrátane dĺžky spracovateľského reťazca, počtu zapojených aktérov a použitých prenosových kanálov; zamýšľané následné prenosy; typ príjemcu; účel spracúvania; kategórie a formát prenášaných osobných údajov; odvetvie hospodárstva, v ktorom sa prevod uskutočňuje; miesto uchovávania prenášaných údajov;

ii) právne predpisy a prax tretej krajiny určenia – vrátane tých, podľa ktorých sa vyžaduje poskytovanie údajov orgánom verejnej moci alebo povoľuje prístup týchto orgánov, – ktoré sú relevantné vzhľadom na osobitné okolnosti prenosu, ako aj uplatniteľné obmedzenia a záruky (12);

iii) všetky príslušné zmluvné, technické alebo organizačné záruky zavedené na doplnenie záruk podľa týchto doložiek vrátane opatrení uplatňovaných počas prenosu a spracúvania osobných údajov v krajine určenia.

c) Dovozca údajov vyhlasuje, že pri vykonávaní posúdenia podľa písmena b) vynaložil maximálne úsilie na to, aby poskytol vývozcovi údajov relevantné informácie, a zaväzuje sa naďalej spolupracovať s vývozcom údajov tak, aby sa zabezpečilo dodržiavanie týchto doložiek.

d) Zmluvné strany sa zaväzujú zdokumentovať posúdenie podľa písmena b) a na požiadanie túto dokumentáciu sprístupniť príslušnému dozornému orgánu.

e) Dovozca údajov sa zaväzuje bezodkladne oznámiť vývozcovi údajov, či má po vyjadrení súhlasu s týmito doložkami počas trvania zmluvy dôvod domnievať sa, že sa na neho vzťahujú alebo začali vzťahovať právne predpisy alebo prax, ktoré nie sú v súlade s požiadavkami podľa písmena a), a to aj po zmene právnych predpisov tretej krajiny alebo prijatí opatrenia (ako je žiadosť o poskytnutie údajov) týkajúceho sa uplatnenia takýchto

právnych predpisov v praxi, ktoré nie je v súlade s požiadavkami podľa písmena a). [V prípade modulu č. 3: Vývozca údajov postúpi oznámenie prevádzkovateľovi.] Vývozca údajov postúpi oznámenie prevádzkovateľovi.]

f) V nadväznosti na oznámenie podľa písmena e) alebo ak má vývozca údajov inak dôvod domnievať sa, že dovozca údajov už nemôže plniť svoje povinnosti podľa týchto doložiek, vývozca údajov bezodkladne určí vhodné opatrenia (napríklad technické alebo organizačné opatrenia na zaistenie bezpečnosti a dôvernosti), ktoré má prijať vývozca údajov a/alebo dovozca údajov na riešenie situácie [v prípade modulu č. 3: v prípade potreby po konzultácii s prevádzkovateľom]. Vývozca údajov preruší prenos údajov, ak sa domnieva, že nie je možné zabezpečiť primerané záruky pre takýto prenos, alebo ak mu dá na to pokyn [v prípade modulu č. 3: prevádzkovateľ alebo] príslušný dozorný orgán. V takom prípade je vývozca údajov oprávnený vypovedať zmluvu, pokiaľ ide o spracúvanie osobných údajov podľa týchto doložiek. Ak má zmluva viac ako dve zmluvné strany, vývozca údajov ju môže vypovedať len vo vzťahu k príslušnej zmluvnej strane, pokiaľ sa zmluvné strany nedohodli inak. V prípade vypovedania zmluvy podľa tejto doložky sa uplatní doložka 16 písm. d) a e).

Doložka 15 Povinnosti dovozcu údajov v prípade prístupu orgánov verejnej moci

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi(ak sprostredkovateľ v EÚ kombinuje osobné údaje prijaté od prevádzkovateľa z tretej krajiny s osobnými údajmi, ktoré získal sprostredkovateľ v EÚ)

15.1. Oznámenie

a) Dovozca údajov sa zaväzuje bezodkladne zaslať oznámenie vývozcovi údajov a prípadne dotknutej osobe (v prípade potreby s pomocou vývozcu údajov), ak:

i) dostane právne záväznú žiadosť od orgánu verejnej moci vrátane súdnych orgánov podľa právnych predpisov krajiny určenia o poskytnutie osobných údajov prenášaných podľa týchto doložiek; takéto oznámenie obsahuje informácie o požadovaných osobných údajoch, žiadajúcom orgáne, právnom základe žiadosti a poskytnutej odpovedi; alebo

ii) sa dozvie o akomkoľvek priamom prístupe orgánov verejnej moci k osobným údajom prenášaným podľa týchto doložiek v súlade s právnymi predpismi krajiny určenia; takéto oznámenie obsahuje všetky informácie, ktoré má dovozca k dispozícii.

[V prípade modulu č. 3: Vývozca údajov postúpi oznámenie prevádzkovateľovi.]

b) Ak sa dovozcovi údajov zakazuje podľa právnych predpisov krajiny určenia zaslať oznámenie vývozcovi údajov a/alebo dotknutej osobe, dovozca údajov sa zaväzuje vynaložiť maximálne úsilie na získanie výnimky zo zákazu s cieľom oznámiť čo najviac informácií a čo najskôr. Dovozca údajov sa zaväzuje zdokumentovať svoje maximálne úsilie tak, aby ho mohol na žiadosť vývozcu údajov preukázať.

c) Ak to právne predpisy krajiny určenia umožňujú, dovozca údajov sa zaväzuje, že počas trvania zmluvy bude vývozcovi údajov v pravidelných intervaloch poskytovať čo najviac relevantných informácií o prijatých žiadostiach (najmä počet žiadostí, druh požadovaných údajov, žiadajúci orgán, či boli žiadosti napadnuté a výsledok súvisiacich konaní atď.). [V prípade modulu č. 3: Vývozca údajov postúpi informáciu prevádzkovateľovi.]

d) Dovozca údajov sa zaväzuje, že informácie podľa písmen a) až c) uchová počas trvania zmluvy a na požiadanie ich sprístupní príslušnému dozornému orgánu.

e) Písmená a) až c) sa uplatňujú bez toho, aby bola dotknutá povinnosť dovozcu údajov podľa doložky 14 písm. e) a doložky 16, a to bezodkladne informovať vývozcu údajov, ak nie je schopný konať v súlade s týmito doložkami.

15.2. Preskúmanie zákonnosti a minimalizácia údajov

a) Dovozca údajov sa zaväzuje preskúmať zákonnosť žiadosti o poskytnutie údajov, najmä či je zachovaná právomoc žiadajúceho orgánu verejnej moci, a žiadosť napadnúť, ak po dôkladnom posúdení dospeje k záveru, že existujú opodstatnené dôvody domnievať sa, že žiadosť je nezákonná podľa právnych predpisov krajiny určenia, platných záväzkov podľa medzinárodného práva a zásad ústretovosti v medzinárodných vzťahoch. Dovozca údajov je za rovnakých podmienok povinný využívať možnosti odvolania. Pri napadnutí žiadosti dovozca údajov navrhne nariadenie predbežných opatrení s cieľom pozastaviť účinky žiadosti dovtedy, kým príslušný súdny orgán nerozhodne vo veci samej. Požadované osobné údaje poskytne až vtedy, keď je na to povinný podľa platných procesných pravidiel. Týmito požiadavkami nie sú dotknuté povinnosti dovozcu údajov podľa doložky 14 písm. e).

b) Dovozca údajov sa zaväzuje zdokumentovať príslušné právne posúdenie, ako aj akékoľvek napadnutie žiadosti o poskytnutie údajov, a v rozsahu povolenom právnymi predpismi krajiny určenia sprístupní dokumentáciu vývozcovi údajov Na požiadanie sprístupní túto dokumentáciu aj príslušnému dozornému orgánu. [V prípade modulu č. 3: Vývozca údajov sprístupní posúdenie prevádzkovateľovi.]

c) Dovozca údajov sa zaväzuje, že v rámci odpovede na žiadosť o poskytnutie údajov poskytne minimálne dovolené množstvo informácií, a to na základe primeraného výkladu žiadosti.

ODDIEL IV – ZÁVEREČNÉ USTANOVENIA

Doložka 16 Nedodržanie doložiek a ukončenie platnosti

a) Dovozca údajov bezodkladne informuje vývozcu údajov, ak nie je schopný tieto pokyny z akéhokoľvek dôvodu dodržať.

b) V prípade, že dovozca údajov porušuje tieto doložky alebo nie je schopný plniť si povinnosti podľa týchto doložiek, vývozca údajov pozastaví prenos osobných údajov dovozcovi údajov, kým sa opäť nedosiahne súlad alebo nedôjde k ukončeniu platnosti zmluvy. Doložka 14 písm. f) tým nie je dotknutá.

c) Vývozca údajov je oprávnený vypovedať zmluvu v rozsahu, v akom sa týka spracúvania osobných údajov podľa týchto doložiek, ak:

i) vývozca údajov prerušil prenos osobných údajov dovozcovi údajov podľa písmena b) a dodržiavanie týchto doložiek sa neobnoví v primeranej lehote a v každom prípade do jedného mesiaca od prerušenia;

ii) dovozca údajov závažným alebo trvalým spôsobom porušuje tieto doložky; alebo

iii) dovozca údajov porušuje záväzné rozhodnutie príslušného súdu alebo dozorného orgánu, pokiaľ ide o jeho povinnosti podľa týchto doložiek.

V týchto prípadoch informuje o tomto porušení príslušný dozorný orgán [v prípade modulu č. 3: a prevádzkovateľa]. Ak má zmluva viac ako dve zmluvné strany, vývozca údajov ju môže vypovedať len vo vzťahu k príslušnej zmluvnej strane, pokiaľ sa zmluvné strany nedohodli inak.

d) [V prípade modulov č. 1, 2 a 3: Osobné údaje, ktoré boli prenesené pred vypovedaním zmluvy podľa písmena c), sa bezodkladne vrátia vývozcovi údajov alebo v celom rozsahu vymažú, a to podľa toho, pre ktorú z možností

sa vývozca údajov rozhodne. To isté platí v prípade kópií údajov.] [V prípade modulu č. 4: Osobné údaje získané vývozcom údajov v EÚ, ktoré boli prenesené pred vypovedaním zmluvy podľa písmena c), sa bezodkladne v celom rozsahu vymažú, vrátane ich kópií.] Dovozca údajov vydá vývozcovi údajov potvrdenie o tom, že údaje boli vymazané. Dovozca údajov zabezpečuje dodržiavanie týchto doložiek dovtedy, kým nedôjde k vymazaniu alebo vráteniu údajov. Pokiaľ ide o miestne právne predpisy uplatniteľné na dovozcu údajov, ktorými sa zakazuje vrátenie alebo vymazanie prenesených osobných údajov, dovozca údajov vyhlasuje, že bude naďalej zabezpečovať súlad s týmito doložkami a údaje bude spracúvať len v takom rozsahu a tak dlho, ako to vyžaduje uvedené miestne právo.

e) Ktorákoľvek zo zmluvných strán môže odvolať svoj súhlas s tým, že bude viazaná týmito doložkami, ak i) Európska komisia prijme rozhodnutie podľa článku 45 ods. 3 nariadenia (EÚ) 2016/679 týkajúce sa prenosu osobných údajov, na ktoré sa vzťahujú tieto doložky, alebo ii) nariadenie (EÚ) 2016/679 sa stane súčasťou právneho rámca krajiny, do ktorej sa osobné údaje prenášajú. Tým nie sú dotknuté ostatné povinnosti vzťahujúce sa na predmetné spracúvanie podľa nariadenia (EÚ) 2016/679.

Doložka 17 Rozhodné právo

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

Tieto doložky sa riadia právom členského štátu Európskej únie, ak toto právo priznáva účinok právam oprávnenej tretej strany. Zmluvné strany sa dohodli, že toto bude právny poriadok ako je to definované v Podmienkach.

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

Tieto doložky sa riadia právom krajiny, ktoré priznáva účinok právam oprávnenej tretej strany. Zmluvné strany sa dohodli, že toto bude právny poriadok ako je to definované v Podmienkach.

Doložka 18 Voľba súdu a právomoci

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

a) Na rozhodovanie sporov vyplývajúcich z týchto doložiek sú príslušné súdy členského štátu EÚ.

b) Zmluvné strany sa dohodli, že týmito súdmi sú súdy ako je definované v Podmienkach.

c) Dotknutá osoba môže podať návrh na začatie konania proti vývozcovi údajov a/alebo dovozcovi údajov aj na súdoch členského štátu, v ktorom má obvyklý pobyt.

d) Zmluvné strany sa dohodli, že sa podriadia právomoci týchto súdov.

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

Na rozhodovanie sporov vyplývajúcich z týchto doložiek sú príslušné súdy ako je definované v Podmienkach.

DODATOK

VYSVETLIVKA: Musí byť možné jasne rozlišovať informácie uplatniteľné na jednotlivé prenosy alebo kategórie prenosov a v tomto ohľade identifikovať úlohy jednotlivých zmluvných strán v postavení vývozcov údajov a/alebo dovozcov údajov. V tomto ohľade nie je nevyhnutné, aby došlo k vyplneniu a podpisu osobitných dodatkov pre každý prevod/kategóriu prevodov a/alebo zmluvný vzťah, ak túto transparentnosť možno dosiahnuť prostredníctvom jedného dodatku. Ak je však potrebné zabezpečiť dostatočnú jasnosť, mali by sa použiť samostatné dodatky.

PRÍLOHA I

A. ZOZNAM ZMLUVNÝCH STRÁN

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

Vývozca údajov: [Totožnosť a kontaktné údaje vývozcu údajov a prípadne jeho zodpovednej osoby a/alebo zástupcu v Európskej únii]

1. Prevádzkovateľ v zmysle Dohody o spracúvaní údajov

2. Sprostredkovateľ v zmysle Dohody o spracúvaní údajov

(na základe toku údajov)

Dovozca údajov: [Totožnosť a kontaktné údaje dovozcu údajov vrátane akejkoľvek kontaktnej osoby zodpovednej za ochranu údajov]

1. Prevádzkovateľ v zmysle Dohody o spracúvaní údajov

2. Sprostredkovateľ v zmysle Dohody o spracúvaní údajov

(na základe toku údajov)

B. OPIS PRENOSU

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

Kategórie dotknutých osôb, ktorých osobné údaje sa prenášajú: Ako je definované v Dohode o spracúvaní údajov.

Kategórie prenášaných osobných údajov: Ako je definované v Dohode o spracúvaní údajov a Zásadách ochrany osobných údajov.

Prenášané citlivé údaje (v relevantných prípadoch) a uplatňované obmedzenia alebo záruky, ktoré v plnej miere zohľadňujú povahu údajov a súvisiace riziká, ako napríklad prísne obmedzenie účelu, obmedzenia prístupu (vrátane prístupu len pre personál, ktorý absolvoval špecializovanú odbornú prípravu), vedenie záznamov o prístupe k údajom, obmedzenia následných prenosov alebo dodatočné bezpečnostné opatrenia: Ako je definované v Dohode o spracúvaní údajov a Zásadách ochrany osobných údajov.

Frekvencia prenosu (napríklad či sa údaje prenášajú jednorazovo alebo sústavne): Sústavný prenos.

Povaha spracúvania: Automatizovaná.

Účel prenosu a ďalšieho spracúvania údajov: Poskytovanie služby v zmysle Podmienok, ich príloh, Zásad ochrany osobných údajov a dokumentácie k službe.

Obdobie uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jeho určenie: Ako je definované v Dohode o spracúvaní údajov.

V prípade prevodov sprostredkovateľom alebo ďalším sprostredkovateľom uveďte aj predmet, povahu a trvanie spracúvania: Ako je definované v Dohode o spracúvaní údajov.

C. PRÍSLUŠNÝ DOZORNÝ ORGÁN

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

Uveďte príslušný dozorný orgán v súlade s doložkou 13: Ako je definované v Zásadách ochrany osobných údajov

PRÍLOHA II TECHNICKÉ A ORGANIZAČNÉ OPATRENIA VRÁTANE TECHNICKÝCH A ORGANIZAČNÝCH OPATRENÍ NA ZAISTENIE BEZPEČNOSTI ÚDAJOV

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

VYSVETLIVKA: Technické a organizačné opatrenia treba opísať konkrétne, nie všeobecne. Pozri aj všeobecnú poznámku na prvej strane dodatku, najmä pokiaľ ide o potrebu jasne uviesť, ktoré opatrenia sa vzťahujú na konkrétny prevod/súbor presunov.

Opis technických a organizačných opatrení prijatých dovozcom údajov (vrátane všetkých príslušných certifikácií) s cieľom zabezpečiť primeranú úroveň bezpečnosti, pričom sa zohľadní povaha, rozsah, kontext a účel spracúvania, ako aj riziká pre práva a slobody fyzických osôb: Ako je definované v bezpečnostnej politike

V prípade prenosov sprostredkovateľom alebo ďalším sprostredkovateľom opíšte aj osobitné technické a organizačné opatrenia, ktoré má prijať sprostredkovateľ alebo ďalší sprostredkovateľ, aby mohol poskytnúť pomoc prevádzkovateľovi, a v prípade prenosov od sprostredkovateľa k ďalšiemu sprostredkovateľovi vývozcovi údajov

PRÍLOHA III ZOZNAM ĎALŠÍCH SPROSTREDKOVATEĽOV

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

VYSVETLIVKA: Túto prílohu je potrebné vyplniť v prípade modulov č. 2 a 3, pokiaľ ide o osobitné povolenie pre ďalších sprostredkovateľov [doložka 9 písm. a) možnosť 1].

Prevádzkovateľ povolil využitie týchto ďalších sprostredkovateľov: Ako je definované v Dohode o spracúvaní údajov

Odkazy:

(1) Ak je vývozca údajov sprostredkovateľom, na ktorého sa vzťahuje nariadenie (EÚ) 2016/679 a ktorý koná v mene inštitúcie alebo orgánu Únie ako prevádzkovateľ, tak uplatňovaním týchto doložiek sa pri zapojení iného sprostredkovateľa (ďalšie sprostredkovanie), na ktorého sa nevzťahuje nariadenie (EÚ) 2016/679, zabezpečuje aj súlad s článkom 29 ods. 4 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39), pokiaľ sú tieto doložky a povinnosti v oblasti ochrany údajov, ktoré sú stanovené v zmluve alebo inom právnom akte uzavretom medzi prevádzkovateľom a sprostredkovateľom podľa článku 29 ods. 3 nariadenia (EÚ) 2018/1725, vo vzájomnom súlade. Platí to najmä v prípade, keď sa prevádzkovateľ a sprostredkovateľ odvolávajú na štandardné zmluvné doložky uvedené v rozhodnutí 2021/915.

(2) Je teda nevyhnutné, aby boli údaje anonymizované tak, aby nikto nemohol jednotlivca identifikovať, ako sa to uvádza v odôvodnení 26 nariadenia (EÚ) 2016/679, pričom tento postup musí byť nezvratný.

(3) Dohodou o Európskom hospodárskom priestore (ďalej len „Dohoda o EHP“) sa vnútorný trh Európskej únie rozširuje o tri štáty EHP – Island, Lichtenštajnsko a Nórsko. Na právne predpisy Únie v oblasti ochrany osobných údajov vrátane nariadenia (EÚ) 2016/679 sa vzťahuje Dohoda o EHP a tieto predpisy boli začlenené do prílohy XI k tejto dohode. Preto akékoľvek poskytnutie údajov zo strany dovozcu údajov tretej strane nachádzajúcej sa v EHP sa na účely týchto doložiek nepovažuje za následný prenos.

(4) Dohodou o Európskom hospodárskom priestore (ďalej len „Dohoda o EHP“) sa vnútorný trh Európskej únie rozširuje o tri štáty EHP – Island, Lichtenštajnsko a Nórsko. Na právne predpisy Únie v oblasti ochrany osobných údajov vrátane nariadenia (EÚ) 2016/679 sa vzťahuje Dohoda o EHP a tieto predpisy boli začlenené do prílohy XI k tejto dohode. Preto akékoľvek poskytnutie údajov zo strany dovozcu údajov tretej strane nachádzajúcej sa v EHP sa na účely týchto doložiek nepovažuje za následný prenos.

(5) Pozri článok 28 ods. 4 nariadenia (EÚ) 2016/679 a v prípade, že prevádzkovateľom je inštitúcia alebo orgán EÚ, článok 29 ods. 4 nariadenia (EÚ) 2018/1725.

(6) Dohodou o Európskom hospodárskom priestore (ďalej len „Dohoda o EHP“) sa vnútorný trh Európskej únie rozširuje o tri štáty EHP – Island, Lichtenštajnsko a Nórsko. Na právne predpisy Únie v oblasti ochrany osobných údajov vrátane nariadenia (EÚ) 2016/679 sa vzťahuje Dohoda o EHP a tieto predpisy boli začlenené do prílohy XI k tejto dohode. Preto akékoľvek poskytnutie údajov zo strany dovozcu údajov tretej strane nachádzajúcej sa v EHP sa na účely týchto doložiek nepovažuje za následný prenos.

(7) Vrátane toho, či prenos a ďalšie spracúvanie zahŕňajú osobné údaje odhaľujúce rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, genetické alebo biometrické údaje na účely jedinečnej identifikácie fyzickej osoby, údaje týkajúce sa zdravia alebo

sexuálneho života či sexuálnej orientácie osoby, alebo údaje týkajúce sa odsúdenia za trestné činy.

(8) Túto požiadavku môže ďalší sprostredkovateľ, ktorý pristupuje k týmto doložkám v súlade s príslušným modulom, splniť podľa doložky 7.

(9) Túto požiadavku môže ďalší sprostredkovateľ, ktorý pristupuje k týmto doložkám v súlade s príslušným modulom, splniť podľa doložky 7.

(10) Túto lehotu možno predĺžiť najviac o dva mesiace, a to v nevyhnutnom rozsahu a s ohľadom na zložitosť a počet žiadostí. Dovozca údajov náležite a bezodkladne informuje dotknutú osobu o každom takomto predĺžení.

(11) Dovozca údajov môže ponúknuť nezávislé riešenie sporov na rozhodcovskom orgáne len vtedy, ak je usadený v krajine, ktorá ratifikovala Newyorský dohovor o výkone rozhodcovských rozhodnutí.

(12) Pokiaľ ide o vplyv týchto právnych predpisov a praxe na dodržiavanie týchto doložiek, v rámci celkového posúdenia možno zohľadniť rôzne prvky. Medzi tieto prvky možno zahrnúť relevantné a zdokumentované praktické skúsenosti s predchádzajúcimi prípadmi žiadostí orgánov verejnej moci o poskytnutie údajov alebo neexistenciu takýchto žiadostí, ktoré sa vzťahujú na dostatočne reprezentatívny časový rámec. Ide najmä o interné záznamy alebo inú dokumentáciu, ktoré boli vypracúvané priebežne v súlade s náležitou starostlivosťou a certifikované na úrovni vyššieho manažmentu, ak možno tieto informácie zákonne poskytovať tretím stranám. Pokiaľ možno na základe týchto praktických skúseností dospieť k záveru, že dovozcovi údajov nič nebráni v dodržiavaní týchto doložiek, treba uviesť aj ďalšie relevantné objektívne prvky, pričom zmluvným stranám prináleží dôkladne posúdiť, či tieto prvky ako celok majú dostatočnú váhu na podporu tohto záveru, pokiaľ ide o ich spoľahlivosť a reprezentatívnosť. Zmluvné strany musia predovšetkým prihliadnuť na to, či sú ich praktické skúsenosti potvrdené, a teda nie v rozpore s verejnými alebo inak dostupnými a spoľahlivými informáciami o existencii alebo neexistencii žiadostí v rámci toho istého odvetvia a/alebo uplatňovaním právnych predpisov v praxi, ako je napríklad judikatúra a správy nezávislých orgánov dohľadu.

Zásady ochrany osobných údajov

Platné od 21. marca 2023 | Zobraziť predchádzajúcu verziu Zásad ochrany osobných údajov | Porovnať zmeny

Spoločnosť ESET, spol. s r. o. so sídlom na adrese Einsteinova 24, 851 01 Bratislava, Slovak Republic, zapísaná v Obchodnom registri Okresného súdu Bratislava I, oddiel Sro, vložka číslo 3586/B, IČO: 31333532, ako prevádzkovateľ údajov (ďalej len „ESET“ alebo „my“) kladie veľký dôraz na ochranu osobných údajov. Chceme splniť požiadavku transparentnosti, ktorá je právne štandardizovaná vo všeobecnom nariadení EÚ o ochrane údajov (ďalej len „GDPR“). S týmto cieľom zverejňujeme tieto zásady ochrany osobných údajov, ktorých jediným účelom je informovať nášho zákazníka (ďalej len „koncový používateľ“ alebo „vy“) ako dotknutú osobu o týchto témach ochrany osobných údajov:

- právny základ spracúvania osobných údajov;
- zdieľanie a dôvernosť údajov;
- bezpečnosť údajov;
- práva, ktoré máte ako dotknutá osoba;
- spracúvanie osobných údajov;
- Kontaktné informácie.

Právny základ spracúvania osobných údajov

Existuje len niekoľko právnych základov spracovania údajov, ktoré využívame v súlade s príslušným právnym rámcom týkajúcim sa ochrany osobných údajov. Spracúvanie osobných údajov spoločnosťou ESET je potrebné

najmä preto, aby sa mohla plniť Podmienky používania (ďalej len „podmienky“) pre koncového používateľa (článok 6 ods. 1 písm. b) nariadenia GDPR), ktorá sa vzťahuje na poskytovanie produktov alebo služieb spoločnosti ESET, pokiaľ nie je výslovne uvedené inak, napríklad:

- Právny základ oprávneného záujmu (článok 6 ods. 1 písm. f) nariadenia GDPR), ktorý nám umožňuje spracúvať údaje o tom, ako naši zákazníci používajú naše služby a ako sú s nimi spokojní, aby sme používateľom poskytli čo najlepšiu ochranu, podporu a skúsenosti. Príslušné právne predpisy uznávajú ako oprávnený záujem dokonca aj marketing, a preto sa naň spoliehame pri marketingovej komunikácii s našimi zákazníkmi.
- Súhlas (článok 6 ods. 1 písm. a) nariadenia GDPR), o ktorý vás môžeme požiadať v špecifických situáciách, keď tento právny základ považujeme za najvhodnejší, alebo ak to vyžaduje zákon.
- Splnenie zákonnej povinnosti (článok 6 ods. 1 písm. c) nariadenia GDPR), napríklad pokiaľ ide o stanovenie požiadaviek týkajúcich sa elektronickej komunikácie alebo uchovávania fakturačných a účtovných dokumentov.

Zdieľanie a dôvernosť údajov

Vaše údaje nezdieľame s tretími stranami. Spoločnosť ESET však pôsobí globálne prostredníctvom pridružených spoločností alebo partnerov v rámci svojej siete predaja, služieb a podpory. Informácie o správe licencií, účtovaní a technickej podpore spracúvané spoločnosťou ESET sa môžu prenášať medzi pridruženými subjektmi alebo partnermi na účely plnenia dohody EULA, ako je napríklad poskytovanie služieb alebo podpory.

Spoločnosť ESET uprednostňuje spracúvanie údajov v krajinách Európskej únie (EÚ). V závislosti od vašej polohy (používanie našich produktov a/alebo služieb mimo EÚ) a/alebo vami vybratej služby však môže byť nevyhnutné preniesť vaše údaje do krajiny mimo EÚ. Využívame napríklad služby tretích strán spojené s cloudovou výpočtovou technikou. V týchto prípadoch si dôkladne vyberáme poskytovateľov služieb a dbáme na ochranu údajov na primeranej úrovni prostredníctvom zmluvných, ale tiež technických a organizačných opatrení. V prípade potreby sa spravidla dohodneme na štandardných zmluvných doložkách EÚ s doplnkovými zmluvnými pravidlami.

Pri niektorých krajinách mimo EÚ, ako je napríklad Spojené kráľovstvo a Švajčiarsko, už EÚ určila porovnateľnú úroveň ochrany údajov. Z dôvodu porovnateľnej úrovne ochrany údajov sa pri prenose údajov do týchto krajín nevyžaduje žiadne osobitné oprávnenie ani dohoda.

Využívame služby tretej strany súvisiace s technológiou cloud computing. Poskytuje ich spoločnosť Microsoft ako poskytovateľom cloudových služieb.

Bezpečnosť údajov

Spoločnosť ESET realizuje vhodné technické a organizačné opatrenia na zabezpečenie úrovne bezpečnosti, ktorá zodpovedá potenciálnym rizikám. Čo najlepšie sa snažíme zabezpečiť neustálu dôvernosť, integritu, dostupnosť a odolnosť systémov a služieb spracovania údajov. V prípade úniku údajov, ktorý má za následok ohrozenie vašich práv a slobôd, sme však pripravení informovať príslušný dozorný orgán, ako aj koncových používateľov ako dotknuté osoby.

Práva dotknutej osoby

Práva každého koncového používateľa sú dôležité a chceme vás informovať, že všetci koncoví používatelia (z ktorejkoľvek krajiny EÚ aj mimo EÚ) majú práva uvedené nižšie zaručené spoločnosťou ESET. Ak chcete uplatniť svoje práva dotknutej osoby, môžete nás kontaktovať prostredníctvom formulára podpory alebo e-mailom na adrese dpo@eset.sk. Na účely identifikácie vás požiadame o tieto informácie: meno, e-mailovú adresu a (ak sú tieto informácie k dispozícii) licenčný kľúč alebo číslo zákazníka a pridruženú spoločnosť. Neodosielajte nám

žiadne iné osobné údaje, napríklad dátum narodenia. Chceme zdôrazniť, že na účely spracovania vašej žiadosti, ako aj na účely identifikácie, budeme spracúvať vaše osobné údaje.

Právo na odvolanie súhlasu. Právo na odvolanie súhlasu sa uplatňuje v prípade spracúvania, ktoré je založené len na súhlase. Ak vaše osobné údaje spracúvame na základe vášho súhlasu, máte právo súhlas kedykoľvek odvolať aj bez uvedenia dôvodu. Odvolanie súhlasu je účinné len pre budúcnosť a nemá vplyv na zákonnosť spracúvania údajov pred odvolaním.

Právo namietať. Právo namietať voči spracúvaniu sa uplatňuje v prípade spracúvania na základe oprávneného záujmu spoločnosti ESET alebo tretej strany. Ak vaše osobné údaje spracúvame na ochranu oprávneného záujmu, ako dotknutá osoba máte právo kedykoľvek namietať voči nami uvedenému oprávnenému záujmu a spracúvaniu vašich osobných údajov. Vaša námietka je účinná len pre budúcnosť a nemá vplyv na zákonnosť spracúvania údajov pred námietkou. Ak vaše osobné údaje spracúvame na účely priameho marketingu, nie je potrebné uvádzať dôvody námietky. Platí to aj pre profilovanie, pokiaľ je spojené s takýmto priamym marketingom. Vo všetkých ostatných prípadoch vás požiadame, aby ste nás stručne informovali o svojich sťažnostiach týkajúcich sa oprávneného záujmu spoločnosti ESET spracúvať vaše osobné údaje.

V niektorých prípadoch máme oprávnenie napriek vášmu odvolaniu súhlasu ďalej spracúvať vaše osobné údaje na inom právnom základe, napríklad na účely plnenia zmluvy.

Právo prístupu. Ako dotknutá osoba máte právo kedykoľvek bezplatne získať informácie o svojich údajoch, ktoré uchováva spoločnosť ESET.

Právo na opravu. Ak neúmyselne spracúvame vaše nesprávne osobné údaje, máte právo na ich opravu.

Právo na vymazanie a právo na obmedzenie spracúvania. Ako dotknutá osoba máte právo požiadať o vymazanie alebo obmedzenie spracúvania svojich osobných údajov. Ak napríklad vaše osobné údaje spracúvame s vaším súhlasom, odvoláte ho a neexistuje žiadny iný právny základ, ako je napríklad zmluva, vaše osobné údaje vymažeme okamžite. Vaše osobné údaje tiež budú vymazané, keď už nebudú potrebné na účely, ktoré sú pre ne uvedené, na konci nášho obdobia uchovávania.

Ak vaše osobné údaje používame výhradne na účely priameho marketingu a odvoláte súhlas alebo budete namietať voči existujúcemu oprávnenému záujmu spoločnosti ESET, spracúvanie vašich osobných údajov obmedzíme tak, že pridáme vaše kontaktné údaje do svojho interného blacklistu, aby nedošlo k nevyžiadanému kontaktu. V opačnom prípade sa vaše osobné údaje vymažú.

Upozorňujeme, že sa od nás môže žiadať, aby sme vaše údaje uchovávali až do uplynutia povinností a období uchovávania stanovených zákonodarcom alebo dozornými orgánmi. Povinnosti a obdobia uchovávania tiež môžu vyplývať z právnych predpisov Slovenskej republiky. Po ich uplynutí sa príslušné údaje vymažú zvyčajným spôsobom.

Právo na prenosnosť údajov. Ako dotknutej osobe vám radi poskytneme osobné údaje spracúvané spoločnosťou ESET vo formáte XLS.

Právo podať sťažnosť. Ako dotknutá osoba máte právo kedykoľvek podať sťažnosť dozornému orgánu. Spoločnosť ESET podlieha slovenským zákonom a je viazaná právnymi predpismi Európskej únie o ochrane údajov. Príslušným dozorným orgánom na ochranu údajov je Úrad na ochranu osobných údajov Slovenskej republiky so sídlom na adrese Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Spracúvanie osobných údajov

Služby poskytované spoločnosťou ESET a realizované v rámci nášho webového produktu sa poskytujú za

podmienok používania (ďalej len „ToU“), niektoré z nich však môžu vyžadovať osobitnú pozornosť. Chceme vám poskytnúť podrobnejšie informácie o spracovaní údajov, ktoré súvisí s poskytovaním našich produktov a služieb. Poskytujeme rôzne služby opísané v podmienky a produktovej dokumentácii. Nato, aby všetko fungovalo, ako má, musíme zhromažďovať tieto informácie:

Licenčné a účtovné údaje. Spoločnosť ESET zhromažďuje a spracúva meno, e-mailovú adresu, licenčný kľúč a (v prípade potreby) adresu, pridruženú spoločnosť a platobné údaje, aby mohla zabezpečiť aktiváciu licencie, poskytnutie licenčného kľúča, pripomenutia uplynutia platnosti, plnenie žiadostí o podporu, overenie pravosti licencií, poskytovanie svojej služby a iné upozornenia vrátane marketingových oznámení v súlade s príslušnými právnymi predpismi alebo vaším súhlasom. Spoločnosť ESET má zákonnú povinnosť uchovávať účtovné informácie počas obdobia 10 rokov, licenčné informácie sa však najneskôr 12 mesiacov od uplynutia platnosti licencie anonymizujú.

Informácie o aktualizáciách a ďalšie štatistické informácie. Spracúvané informácie zahŕňajú informácie týkajúce sa procesu inštalácie a počítača vrátane informácií o platforme, na ktorej je nainštalovaný náš produkt, a informácií o operáciách a funkčnosti našich produktov, napríklad informácií o operačnom systéme, hardvéri, identifikátoroch inštalácie, identifikátoroch licencie, IP adrese, MAC adrese a nastaveniach konfigurácie produktu. Spracúvajú sa na účely poskytovania služieb aktualizácie a inovácie a na účely údržby, zabezpečenia a vylepšenia našej infraštruktúry koncových serverov.

Tieto informácie sa uchovávajú oddelene od identifikačných informácií potrebných na účely správy licencií a účtovania, pretože nevyžadujú identifikáciu koncového používateľa. Obdobie uchovávania je najviac 4 roky.

Reputačný systém **ESET LiveGrid®.** Jednosmerné hashe súvisiace s infiltráciou sa spracúvajú na účely reputačného systému ESET LiveGrid®, ktorý zlepšuje účinnosť našich antimalvérových riešení na základe porovnávania kontrolovaných súborov s databázou položiek zaradených na whitelist a blacklist v cloude. Počas tohto procesu sa koncový používateľ neidentifikuje.

Systém spätnej väzby **ESET LiveGrid®.** Prijaté podozrivé vzorky a metadáta zhromažďované v rámci systému spätnej väzby ESET LiveGrid®, ktoré umožňujú spoločnosti ESET okamžite reagovať na potreby svojich koncových používateľov, ako aj na najnovšie hrozby. Spoliehame sa na to, že nám zašlete

- Infiltrácie, ako napríklad vzorky potenciálnych vírusov a iných škodlivých a podozrivých programov; problematické, potenciálne neželané alebo potenciálne nebezpečné objekty, ako napríklad spustiteľné súbory, e-mailové správy, ktoré ste nahlásili ako spam alebo ktoré takto označil váš produkt;
- Informácie o používaní internetu, ako napríklad IP adresu, geografické informácie, IP pakety, URL adresy a ethernetové rámce;
- Súbory výpisov pri zlyhaní a informácie, ktoré obsahujú.

Nemáme v úmysle zhromažďovať vaše údaje mimo tohto rozsahu, niekedy sa tomu však nedá zabrániť. Náhodne zhromaždené údaje môžu byť obsiahnuté v samotnom malvéri (zhromaždené bez vášho vedomia alebo súhlasu) alebo môžu byť súčasťou názvov súborov či URL adries a my nemáme v úmysle začleniť ich do našich systémov ani ich spracovať na účely uvedené v týchto zásadách ochrany osobných údajov.

Všetky informácie získané a spracúvané prostredníctvom systému spätnej väzby ESET LiveGrid® sú určené na používanie bez identifikácie koncového používateľa.

Technická podpora. Kontaktné a licenčné informácie a údaje obsiahnuté vo vašich žiadostiach o podporu sa môžu vyžadovať na poskytnutie podpory. Podľa toho, akým spôsobom sa nás rozhodnete kontaktovať, môžeme zhromažďovať informácie, ako sú napríklad vaša e-mailová adresa, telefónne číslo, licenčné informácie, podrobnosti o produkte a popis vášho konkrétneho prípadu podpory. Na zjednodušenie poskytnutia služby podpory vás môžeme požiadať o poskytnutie ďalších informácií. Údaje spracúvané na účely technickej podpory sa uchovávajú 4 roky.

Ak osoba, ktorá používa naše produkty a služby, nie je koncovým používateľom, ktorý si príslušný produkt alebo službu zakúpil a vyjadril súhlas s našimi podmienkami (napríklad zamestnanec koncového používateľa, jeho rodinný príslušník alebo osoba inak oprávnená koncovým používateľom používať produkt alebo službu v súlade s podmienkami), spracúvanie údajov sa uskutočňuje v oprávnenom záujme spoločnosti ESET v zmysle článku 6 ods. 1 písm. f) nariadenia GDPR, aby používateľ oprávnený koncovým používateľom mohol používať nami poskytované produkty a služby v súlade s podmienkami.

Kontaktné informácie

Ak chcete využiť svoje právo dotknutej osoby alebo chcete položiť otázku či vyjadriť obavu, obráťte sa na nás na adrese:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk