ESET Cloud Office Security

Podręcznik użytkownika

Kliknij tutaj aby wyświetlić ten dokument jako Pomoc.

Digital Security
Progress. Protected.

Prawa autorskie ©2023 ESET, spol. s r.o.

Produkt ESET Cloud Office Security został opracowany przez ESET, spol. s r.o.

Aby uzyskać więcej informacji, odwiedź stronę https://www.eset.com.

Wszelkie prawa zastrzeżone. Żadna część tej dokumentacji nie może być powielana, przechowywana w systemie wyszukiwania lub przesyłana w jakiejkolwiek formie lub za pomocą jakichkolwiek środków elektronicznych, mechanicznych, fotokopiowania, nagrywania, skanowania lub w inny sposób bez pisemnej zgody autora.

Firma ESET, spol. s r.o. zastrzega sobie prawo do zmiany dowolnej z opisanych aplikacji bez uprzedniego powiadomienia.

Pomoc techniczna: https://support.eset.com

WER. 20.12.2023

1 Omówienie ... 1
1.1 Główne funkcje ... 2
1.2 Nowości ... 5
1.3 Integracja ... 6
2 Specyfikacje ... 7
2.1 Wymagania ... 7
2.2 Obsługiwane plany usługi Microsoft 365 ... 8
2.3 Obsługiwane pakiety Google Workspace ... 9
2.4 Obsługiwane przeglądarki internetowe ... 9
2.5 Ograniczenia i polityka przechowywania danych ... 9
3 Licencjonowanie dla ESET Cloud Office Security ... 11
3.1 ESET Business Account ... 12
3.1 Utwórz nowe konto ESET Business Account ... 12
3.1 Dodaj licencję ESET Cloud Office Security w ESET Business Account ... 12
3.1 Zarządzaj ESET Business Account ... 13
3.2 ESET MSP Administrator ... 14
4 Aktywacja usługi ESET Cloud Office Security ... 15
4.1 Zdezaktywuj ESET Cloud Office Security ... 17
5 Zarządzanie dzierżawami w Ustawieniach ... 18
5.1 Dodaj swoją pierwszą dzierżawę ... 20
5.2 Dzierżawa Microsoft 365 ... 22
5.3 Dzierżawa Google Workspace ... 25
5.4 Usuń dzierżawcę z ESET Cloud Office Security ... 31
5.5 Usuń ESET Cloud Office Security z portalu Azure ... 32
6 Poruszanie się po ESET Cloud Office Security ... 32
7 ESET LiveGuard Advanced ... 34
8 Panel kontrolny ... 34
9 Użytkownicy ... 36
10 Zespoły i lokacje ... 38
11 Wykrycia ... 39
12 Raporty ... 40
13 Kwarantanna ... 43
14 Dzienniki skanowania ... 44
15 Stosowane polityki ... 45
15.1 Ustawienia ochrony dla usługi Exchange Online ... 48
15.2 Ustawienia ochrony dla Gmail ... 51
15.3 Ustawienia ochrony dla usługi OneDrive ... 54
15.4 Ustawienia ochrony dla usługi Google Drive ... 55
15.5 Ustawienia ochrony dla grup zespołu ... 56
15.6 Ustawienia ochrony dla witryn programu SharePoint ... 57
15.7 Ustawienia ochrony dla ESET LiveGuard Advanced ... 58
15.8 Ochrona raportowania i uczenia maszynowego ... 59
16 Zarządzanie licencjami ... 61
16.1 Dostęp użytkownika ESET Cloud Office Security do konkretnej firmy ... 63
17 Dziennik audytu ... 64
18 Prześlij opinię ... 65
19 Pomoc techniczna ... 65
20 Dostępność usług ... 66

20.1 Zabezpieczenia dla ESET Cloud Office Security 66
20.2 Warunki korzystania 70
20.2 Umowa licencyjna użytkownika końcowego 75
20.2 Umowa o przetwarzaniu danych 82
20.2 Standardowe klauzule umowne 84
20.3 Zasady ochrony prywatności 110

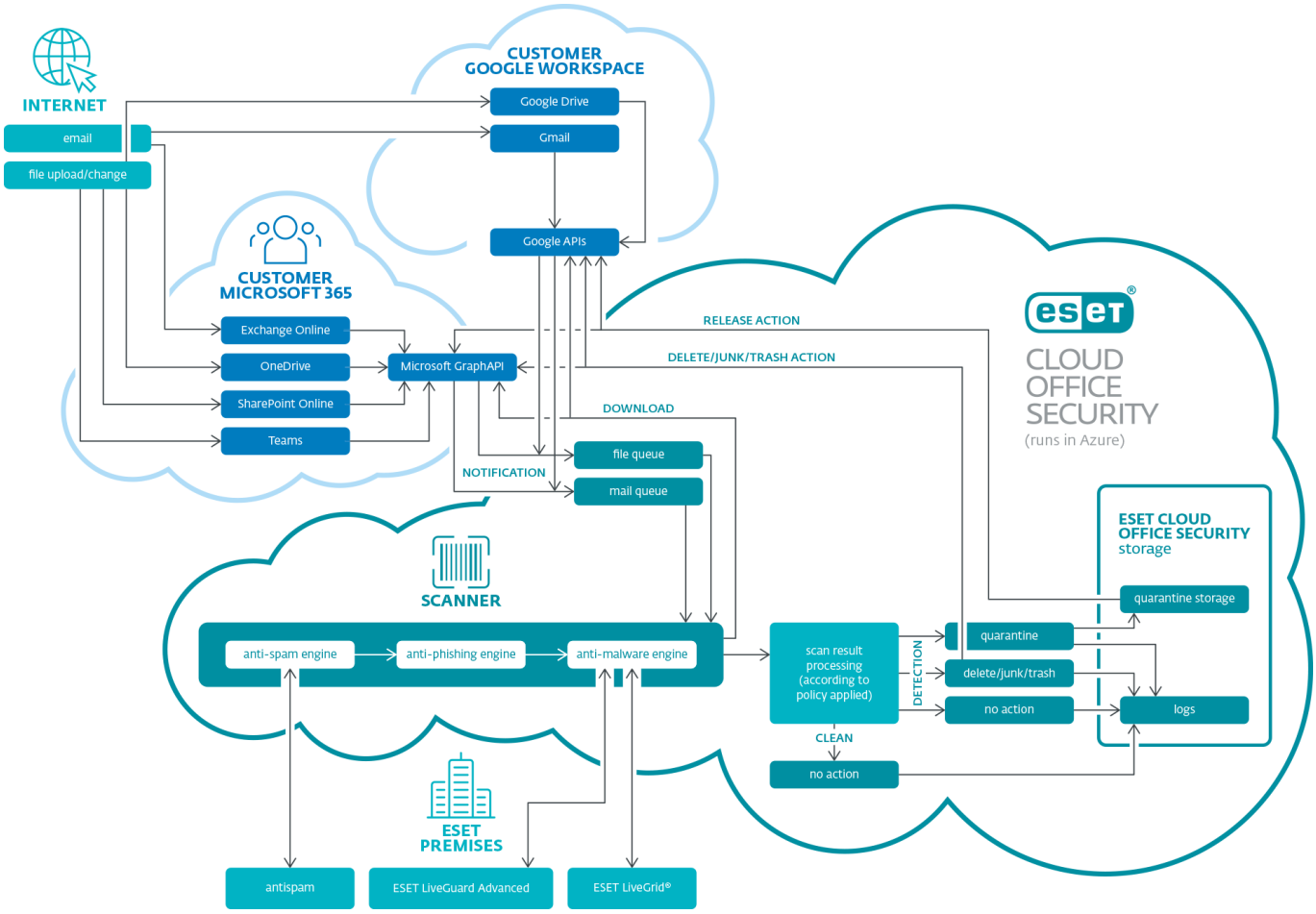
Omówienie

ESET Cloud Office Security to skalowalna usługa chmurowa z wieloma dzierżawami w chmurze na platformie Microsoft Azure. Usługa ESET Cloud Office Security oferowana jest w formie Software-as-a-Service (SaaS). Jest to najlepsze połączenie filtrowania spamu, skanowania szkodliwego oprogramowania i ochrony przed atakami typu phishing, które pomaga chronić komunikację firmy przed szkodliwym oprogramowaniem, minimalizuje negatywny wpływ niezamówionych wiadomości na codzienną produktywność i zapobiega wykorzystywaniu przychodzących zewnętrznych wiadomości e-mail jako kanału ukierunkowanych ataków.

Usługi bezpieczeństwa ESET Cloud Office Security obejmują wiodących dostawców platform chmurowych i zapewniają kompleksową ochronę poczty e-mail dzięki najnowocześniejszym silnikom zabezpieczającym przed złośliwym oprogramowaniem i ESET LiveGuard Advanced. To rozwiązanie oferuje zaawansowaną ochronę przed zagrożeniami za pośrednictwem piaskownicy bazującej na chmurze, analizując podejrzane próbki w odizolowanym środowisku.

Architektura ESET Cloud Office Security umożliwia szybkie inicjowanie ochrony poprzez nawiązanie połączenia z platformą chmurową — Microsoft 365 i Google Workspace. Daje możliwość zarządzania ochroną za pośrednictwem konsoli internetowej dostępnej z dowolnego miejsca.

ESET Cloud Office Security zapewnia zaawansowaną ochronę zapobiegawczą w celu zabezpieczenia firmowych aplikacji platformy Microsoft 365 — Exchange Online, OneDrive, SharePoint Online i Teams. Taką samą ochronę zapewniają aplikacje Google Workspace — Gmail i Dysk Google.



ESET Cloud Office Security zapewnia ochronę usługi OneDrive i skrzynek pocztowych licencjonowanych użytkowników, a także stronom grup zespołu i SharePoint. Każdy magazyn tych aplikacji platformy Microsoft 365 jest chroniony niezależnie od tego, kto przekazał plik lub wysłał wiadomość e-mail. Sama treść jest chroniona niezależnie od tego, kto jest autorem. Autor może być również gościem, aby zapewnić jak najlepszą ochronę.

Główne funkcje

Poniższa tabela zawiera listę funkcji dostępnych w ESET Cloud Office Security.

Wiele dzierżaw	Możesz chronić wiele dzierżaw usługi Microsoft 365 i Google Workspace zarządzać nimi z jednej konsoli ESET Cloud Office Security. Usługa Azure Active Directory (Azure AD) organizuje obiekty takie jak użytkownicy i aplikacje w grupy nazywane dzierżawami. Dzierżawy umożliwiają ustawianie zasad dotyczących użytkowników i aplikacji organizacji w celu spełnienia zasad zabezpieczeń i operacyjnych.

Antispam	Ochrona przed spamem stanowi niezbędny element na każdym serwerze poczty e-mail. Program ESET Cloud Office Security korzysta z doskonałego silnika niezwykle skutecznej ochrony przed spamem i atakami typu „phishing”. Program ESET Cloud Office Security kilka razy z rzędu wygrał w testach filtrowania spamu przeprowadzonych przez Virus Bulletin, lidera w zakresie testowania zabezpieczeń, i od lat otrzymuje certyfikat VBSpam+. Moduł antyspamowy oferuje wykrywalność spamu na poziomie 99,9% bez wyników fałszywie pozytywnych, co czyni go jednym z wiodących rozwiązań antyspamowych w branży. Ochrona przed spamem w programie ESET Cloud Office Security jest rozwiązaniem opartym na chmurze. Większość baz danych chmury znajduje się w centrach danych firmy ESET. Usługi ochrony przed spamem w chmurze umożliwiają szybką aktualizację danych, co zapewnia szybszą reakcję w przypadku pojawienia się nowego spamu.
Ochrona przed atakami typu „phishing”	Chroni on użytkowników przed odwiedzaniem stron wyłudzających informacje. Wiadomości e-mail mogą zawierać łącza prowadzące do stron internetowych typu „phishing”. Program ESET Cloud Office Security identyfikuje takie łącza (adresy URL) przy użyciu zaawansowanego parsera, który przeszukuje treść i temat nadchodzących wiadomości. Łącza są porównywane z bazą stron wyłudzających informacje, która jest stale aktualizowana.
Ochrona przed szkodliwym oprogramowaniem	Wielokrotnie nagradzana innowacyjna ochrona przed szkodliwym oprogramowaniem. Jest to wiodąca technologia zapobiegania atakom. Eliminuje ona wszelkie rodzaje zagrożeń, takie jak wirusy, oprogramowanie wymuszające okup, rootkity, robaki i spyware. Dzięki skanowaniu w chmurze wykrywanie zagrożeń jest niezwykle skuteczne. Małe wymagania tego rozwiązania przekładają się na niewielkie obciążenie zasobów systemowych, a więc nie wpływają na wydajność systemu. Ochrona przed szkodliwym oprogramowaniem, która bazuje na warstwowym modelu zabezpieczeń. Każda warstwa (faza) ma kilka kluczowych technologii. Faza przed uruchomieniem korzysta z następujących technologii: Skaner UEFI (Unified Extensible Firmware Interface), ochrona przed atakami z sieci, reputacja i pamięć podręczna, wbudowany sandbox, wykrywanie DNA. Technologie fazy uruchamiania to Blokada programów typu Exploit, Ochrona przed oprogramowaniem wymuszającym okup, zaawansowany skaner pamięci oraz Skaner skryptów (AMSI). Faza po uruchomieniu wykorzystuje ochronę przed botnetami, system ochrony przed szkodliwym oprogramowaniem w chmurze i sandboxing. Ten bogaty zestaw składający się z kluczowych technologii zapewnia niezrównany poziom ochrony.
Stosowane polityki	Większe organizacje mają zwykle wiele działów i chcą skonfigurować różne ustawienia ochrony dla każdej jednostki organizacyjnej. Usługa ESET Cloud Office Security oferuje oparte na politykach ustawienia zabezpieczeń, które można przypisać do wybranych dzierżaw, użytkowników, grup zespołu lub witryn programu SharePoint. Każdą politykę możesz dostosować do swoich potrzeb.
Menedżer kwarantanny	Sprawdź obiekty poddane kwarantannie i wykonaj odpowiednie działanie (pobierz, usuń lub zwolnij). Ta funkcja oferuje proste zarządzanie wiadomościami e-mail, załącznikami, a także plikami z usług Exchange Online / OneDrive / grup zespołu / witryn programu SharePoint, które zostały poddane kwarantannie przez ESET Cloud Office Security. Jeśli wymagane jest analizowanie obiektów poddanych kwarantannie za pomocą dodatkowych narzędzi, to pobieranie udostępnia taką możliwość, co może być pomocne przy podejmowaniu decyzji, jakie działania należy podjąć.

Panel kontrolny ze statystykami wykryć	W łatwy sposób przeglądaj działania związane z bezpieczeństwem w usłudze Microsoft 365. Panel kontrolny zawiera podstawowe informacje na każdej z kart przeglądu (Exchange Online / OneDrive / grup zespołu / witryn programu SharePoint). Przegląd użytkowników pokazuje liczbę dzierżaw i używanych licencji, a także statystyki dla każdej z dzierżaw — liczbę użytkowników, odbiorców największej ilości spamu/prób wyłudzeń informacji/szkodliwego oprogramowania, najbardziej podejrzanych kont OneDrive, najbardziej podejrzanych grup zespołu oraz najbardziej podejrzanych witryn programu SharePoint. Możesz wyświetlić statystyki dla określonej dzierżawy w wybranym okresie czasu. Dodatkowe statystyki i wykresy wykryć są widoczne na kartach przeglądu usług Exchange Online i OneDrive, grup zespołu oraz witryn programu SharePoint. Są to statystyki przedstawiające liczbę zeskanowanych wiadomości e-mail i plików oraz ilość wykrytego spamu/prób wyłudzenia informacji/szkodliwego oprogramowania. Wykresy przedstawiają ruch dla każdego typu wykrywania — spamu, szkodliwego oprogramowania i wyłudzania informacji.
Opcja filtrowania wykryć	Ta funkcja zawiera wszystkie rekordy dotyczące wykryć. Zapisy obejmują dzienniki dotyczące każdego wykrycia w wyniku skanowania poczty e-mail w zakładce Exchange Online, a także skanowania plików na kartach OneDrive / grupach zespołu / witrynach programu SharePoint. Umożliwiają one skuteczne filtrowanie i odnajdywanie tego, czego szukasz, korzystając z dodatkowych informacji o konkretnym wykryciu (na przykład nazwy infekcji, skrótu plików itp.).
Użytkownicy	Centralnym elementem chronionym przez ESET Cloud Office Security jest konto użytkownika. Znajdź przydatne informacje otwierając szczegóły użytkownika, takie jak Przegląd, Ustawienia zdefiniowane przez polityki, Lista zasad przypisanych do użytkownika oraz Wykrycia w usługach Exchange Online i OneDrive. Funkcja ta jest pomocna, gdy wymagane jest zbadanie wykryć związanych z wybranym użytkownikiem. Można również określić, którzy użytkownicy będą chronieni. Użytkownicy są sortowani w grupy. Każda grupa jest dzierżawą usługi Microsoft 365 zawierającą jej użytkowników. Aby ułatwić sobie wyszukiwanie określonego użytkownika w grupie, możesz użyć filtrowania z wieloma kryteriami.
Ochrona raportowania i uczenia maszynowego	Zaawansowane uczenie maszynowe jest teraz częścią silnika detekcji jako zaawansowana warstwa ochrony, która poprawia wykrywanie w oparciu o uczenie maszynowe. Przeczytaj więcej o tego typu zabezpieczeniach w słowniczku. Można skonfigurować poziomy raportowania dla następujących kategorii: szkodliwe oprogramowanie, potencjalnie niepożądane aplikacje (PUA), potencjalnie podejrzane aplikacje i potencjalnie niebezpieczne aplikacje.
Raporty (statystyczne i kwarantanny poczty)	Otrzymuj dane statystyczne dla usług Exchange Online i OneDrive oraz dla grup zespołu i witryn SharePoint za pośrednictwem poczty e-mail lub wygeneruj i pobierz raport za wybrany okres. Można zaplanować regularne generowanie raportów i ich dystrybucję do określonych adresatów za pośrednictwem poczty e-mail. Wybierz format wyjściowy PDF lub CSV. Raporty zawierają takie dane, jak liczba zeskanowanych wiadomości e-mail, wykryte szkodliwe oprogramowanie, wyłudzanie informacji i spam. Format PDF zawiera dane wyświetlane na wykresach. Istnieje wykres dla każdego elementu — zeskanowanych wiadomości e-mail, ruchu szkodliwego oprogramowania, ruchu phishingowego i ruchu spamowego. Zawiera on również oddzielne statystyki dotyczące odbiorców najczęściej otrzymujących wiadomości z poszczególnych kategorii: szkodliwe oprogramowanie, phishing oraz spam. Istnieje kilka dostępnych opcji generowania raportów. Ponadto raport kwarantanny poczty — lista wiadomości e-mail poddanych kwarantannie — może być dostarczany do wybranych odbiorców. Raport kwarantanny poczty jest wysyłany w określonym dniu i o określonej godzinie, ale tylko wtedy, gdy istnieją nowe elementy do zgłoszenia.
Zespoły i lokacje	ESET Cloud Office Security zapewnia ochronę grup zespołu oraz witryn programu SharePoint. Rozszerza to ochronę na rozwiązania usługi Microsoft 365 do współpracy, chroniąc program SharePoint i grupy zespołu oraz umożliwiając bezpieczne udostępnianie plików. Jeśli korzystasz z programu ESET Cloud Office Security, przed rozpoczęciem korzystania z funkcji Zespoły i witryny możesz zostać poproszony o zaktualizowanie zgody.

ESET LiveGuard Advanced	Dodatkowa warstwa ochrony przed zaawansowanymi zagrożeniami typu zero-day. ESET LiveGuard Advanced to oparte na chmurze rozwiązanie piaskownicy, które analizuje przesłane pliki, wykonując podejrzany kod w izolowanym środowisku w celu oceny jego zachowania. Program ESET Cloud Office Security przesyła podejrzane załączniki i pliki wiadomości e-mail z usług Exchange Online, OneDrive, grup zespołu i witryn programu SharePoint do usługi ESET LiveGuard Advanced w celu analizy. Włączanie i konfigurowanie funkcji ESET LiveGuard Advanced przy użyciu polityk. Wyniki analizy są pokazane w Dziennikach skanowania.
Dziennik audytu	Dziennik audytu umożliwia Administratorowi wgląd w działania wykonywane w pliku ESET Cloud Office Security. Ta funkcja może być przydatna, zwłaszcza przy obecności wielu użytkowników konsoli ESET Cloud Office Security. Rekordy dziennika audytu są dowodem działań i pokazują sekwencję, w jakiej wystąpiły. Dzienniki audytu przechowują informacje o określonej operacji lub zdarzeniu. Dzienniki audytu są tworzone za każdym razem, gdy obiekt ESET Cloud Office Security (pula licencji, użytkownik, polityka, raport, element kwarantanny, taki jak załącznik) jest tworzony lub modyfikowany.
Google Workspace (ochrona usługi Gmail i Dysku Google)	ESET Cloud Office Security rozszerza zakres usług bezpieczeństwa na innego czołowego dostawcę poczty e-mail w chmurze, Google Workspace. ESET Cloud Office Security zapewnia kompleksową ochronę użytkownikom Gmaila i Dysku Google, wykorzystując wszystkie jego funkcje. Chroni użytkowników Google Workspace przed szkodliwym oprogramowaniem, phishingiem i spamem.

Nowości

Informacje o nowych funkcjach i ulepszeniach zaimplementowanych w poszczególnych wersjach ESET Cloud Office Security:

Wersja portalu 353 wydana 23 listopada 2023 r.

- Dodano integrację z Google Workspace.
- Nawigator produktu do szybkiego dostępu ESET Business Account (więcej konsol pojawi się w nadchodzących miesiącach).
- *Inne poprawki błędów i ulepszenia zaplecza.*

Wersja portalu 342.3 wydana 24 października 2023 r.

- Dodano weryfikację konta administratora w Google Workspace.
- Dodano kolumnę typu Użytkownik.
- *Inne poprawki błędów i ulepszenia zaplecza.*

Wersja portalu 311.2 wydana 31 lipca 2023 r.

- Dodano Google Workspace (ochrona Gmaila i Dysku Google) — dostęp do funkcji podglądu z szybkich łączy.
- Dodano motyw Dark mode (Tryb ciemny).
- Dodano funkcję Nawigator produktu dla użytkowników programu ESET HUB Early Access.
- *Inne poprawki błędów i ulepszenia zaplecza.*

Wersja portalu 293.7 wydana 13 lipca 2023 r.

- Dodano funkcję kojarzenia dzierżawców z witrynami ESET Business Account (EBA). Ta zmiana zapewnia zgodność z przyszłym portalem dla klientów ESET PROTECT HUB, który zastąpi ESET MSP Administrator (EMA) i ESET Business Account (EBA). Dotyczy to tylko garstki klientów korzystających z licencji z wielu witryn w celu ochrony jednego dzierżawcy. W takim przypadku zostanie wyświetlony monit o powiązanie dzierżawców z witrynami EBA.
- Inne drobne ulepszenia i poprawki błędów.

Wersja portalu 251.1 wydana 21 marca 2023 r.

- Ulepszenia związane z powolnym wczytywaniem ekranów w celu lepszej obsługi dzierżawców posiadających dziesiątki tysięcy użytkowników.
- Zmiany w kreatorze dodawania dzierżawcy.
- Aktualizacje na stronie Informacje.
- Aktualizacje Warunków korzystania i Polityki prywatności (Polityka dotycząca ograniczeń i przechowywania danych).

Wersja portalu 205 wydana 9 listopada 2022 r.

- Dodano okno „Co nowego”, które ma być wyświetlane po pierwszym zalogowaniu się do konsoli ESET Cloud Office Security, opisujące nowo dodane funkcje.
- Opcja eksportu Dzienników skanowania i Dziennika audytu do pliku CSV.
- Dodano nowe ustawienie podczas Scalania polityk z listami i wiadomościami e-mail z powiadomieniami.

Wersja portalu 180.2 wydana 27 lipca 2022 r.

- Nowa funkcja dziennika audytu.
- Zmień sekcję Dzienniki na Dzienniki skanowania.

Wersja portalu 156.2 wydana 26 kwietnia 2022 r.

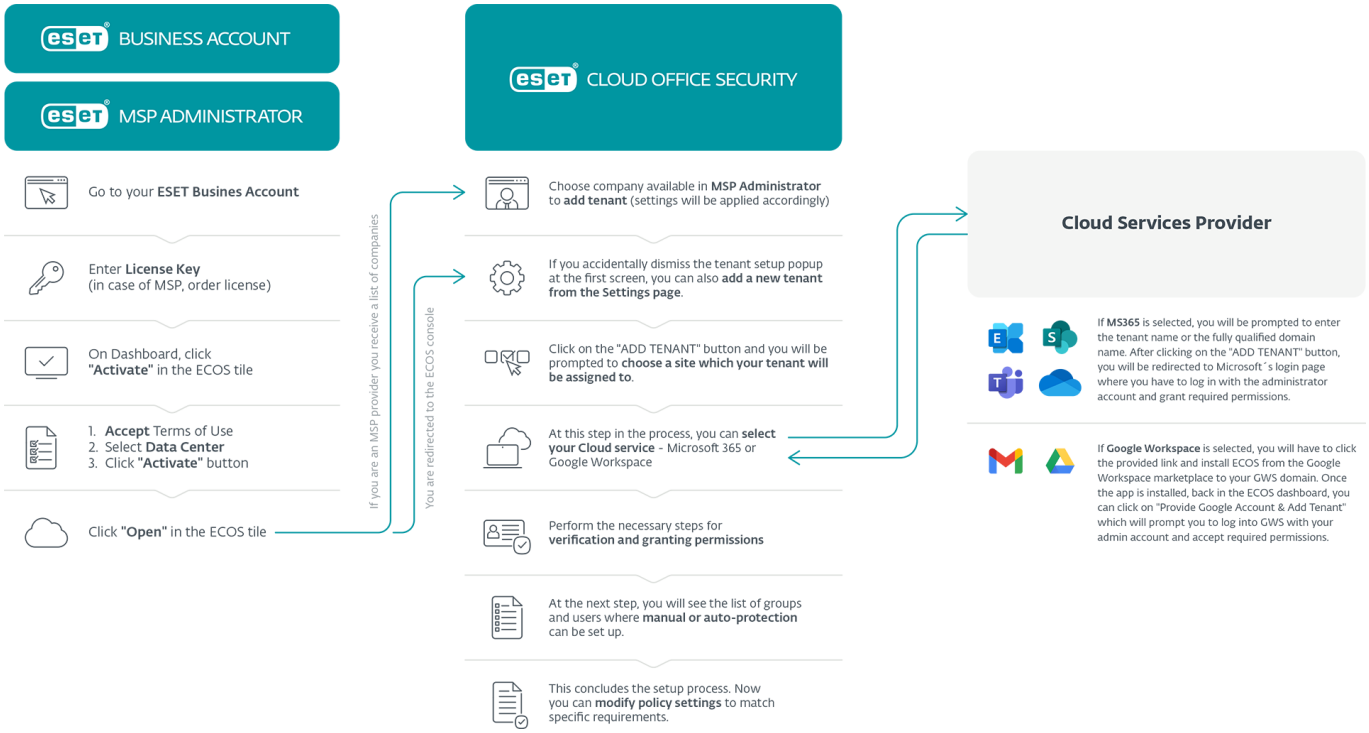
- Nazwa Dynamic Threat Defense została zmieniona na ESET LiveGuard Advanced.
- Przesłanie próbek fałszywie dodatnich / fałszywie ujemnych do analizy.
- Importowanie/eksportowanie list zatwierdzonych, zablokowanych i ignorowanych w Politykach.
- Panel kontrolny pokazuje liczbę niechronionych użytkowników na karcie Przegląd
- Naprawiono błąd, który powodował umieszczanie wiadomości e-mail z powiadomieniami w kwarantannie.

Wersja portalu 140.6 wydana 9 lutego 2022 r.

- Możliwość tworzenia raportów dotyczących produktów sprzedawanych pod marką dystrybutora (tylko co-branding lub niestandardowe logo).
- Opcja zdefiniowania preferowanego języka wiadomości e-mail z powiadomieniami (powiadomienia właściciela skrzynki pocztowej).
- Opcja definiowania preferowanego języka wiadomości e-mail z powiadomieniami dla członków dzierżawy.
- Filtrowanie wiadomości e-mail według identyfikatora wiadomości.

Integracja

Przebieg integracji ESET Cloud Office Security z dostawcą usług w chmurze:



Specyfikacje

Referencyjne specyfikacje techniczne dla ESET Cloud Office Security:

- Wymagania
- Obsługiwane plany usługi Microsoft 365
- Obsługiwane pakiety Google Workspace
- Obsługiwane przeglądarki internetowe
- Ograniczenia i polityka przechowywania danych

Wymagania

Aby korzystać z usługi ESET Cloud Office Security, chroniącej usługę Microsoft 365, należy posiadać:

- Obsługiwany plan subskrypcji usługi Microsoft 365
- Dostęp administratora do usługi Azure Active Directory (Azure AD)
- Azure Cloud Services – Exchange | OneDrive

- Konto w portalu ESET Business Account lub ESET MSP Administrator

Obsługiwane plany usługi Microsoft 365

ESET Cloud Office Security obsługuje następujące plany usług Microsoft 365, Exchange Online i OneDrive.

Plany usługi Microsoft 365 dla przedsiębiorstw:

- 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

Plany usługi Microsoft 365 dla firm:

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

Plany usługi Microsoft 365 Education:

- Microsoft 365 A3
- Microsoft 365 A5

Plany usługi Exchange Online:

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

Plany usługi OneDrive:

- OneDrive for Business (Plan 1)
- OneDrive for Business (Plan 2)

- Microsoft 365 Business Basic
- Microsoft 365 Business Standard

Obsługiwane pakiety Google Workspace

ESET Cloud Office Security obsługuje te pakiety Google Workspace.

- Business Starter
- Business Standard
- Business Plus
- Enterprise

Obsługiwane przeglądarki internetowe

> Aby jak najlepiej korzystać z konsoli internetowej ESET Cloud Office Security, zalecamy regularną aktualizację przeglądarek internetowych.

Z konsoli ESET Cloud Office Security można korzystać w następujących przeglądarkach internetowych:

- Mozilla Firefox 69 i nowsze
- Microsoft Edge 44 i nowsze
- Google Chrome 77 i nowsze
- Opera 63 i nowsze
- Safari 13.x i nowsze

> Przeglądarka Microsoft Internet Explorer nie jest obsługiwana.

Ograniczenia i polityka przechowywania danych

W pewnych okolicznościach istnieją ograniczenia skanowania przeprowadzanego przez ESET Cloud Office Security. Plik nie jest skanowany i pojawi się w Dziennikach skanowania jako **Nieskanowany**, jeśli zostaną spełnione następujące wymagania:

- Rozmiar pliku wynosi ponad 200 MB
- Skanowanie trwa dłużej niż 2 minuty i przekracza limit czasu
- Plik archiwum ma poziom zagnieżdżenia 10 lub wyższy (zwykle plik, który jest znany jako bomba dekompresyjna)
- Plik archiwum jest chroniony hasłem

- Plik jest uszkodzony

Limity kwarantanny (po zwolnieniu z kwarantanny):

- 15 MB na jeden załącznik wiadomości e-mail
- 150 MB dla całej wiadomości e-mail, w tym załączników

Polityka przechowywania danych:

Jednostka	Okres przechowywania	Komentarz
Obiekty poddane kwarantannie	30 dni	Obiekty starsze niż 30 dni zostaną usunięte na stałe.
Wykrycia	90 dni	Wykrycia starsze niż 90 dni zostaną usunięte na stałe.
Rekordy dzienników skanowania	90 dni	Wykrycia starsze niż 90 dni zostaną usunięte na stałe.
Rekordy dzienników skanowania z wynikiem czystego skanowania	3 dni	Jeśli masz politykę, która wykorzystuje funkcję Zapisz wszystkie obiekty, to wyniki czystych skanowań starsze niż 3 dni zostaną trwale usunięte.
kopia zapasowa bazy danych ESET Cloud Office Security	90 dni	Kopie zapasowe starsze niż 90 dni zostaną trwale usunięte.
Dzienniki audytu	90 dni	Wykrycia starsze niż 90 dni zostaną usunięte na stałe.
Dzienniki usługi Application Insights	90 dni	Wykrycia starsze niż 90 dni zostaną usunięte na stałe.

Dzierżawca usunięty z konsoli ESET Cloud Office Security

Po usunięciu dzierżawcy z ESET Cloud Office Security konsoli okres przechowywania danych dzierżawy wynosi 30 dni (Kwarantanna, Dzienniki skanowania i Statystyki są usuwane po 30 dniach). Jeśli dodasz dzierżawcę ponownie w ciągu 30 dni, wszystkie dane zostaną przywrócone. Inne obiekty (dzierżawcy, użytkownicy, grupy, witryny, raporty, zasady) są trwale usuwane po 90 dniach.

ESET Cloud Office Security dezaktywowany w ESET Business Account lub ESET MSP Administrator

Jeśli dezaktywujesz ESET Cloud Office Security w ESET Business Account lub ESET MSP Administrator, ten proces usuwa również dzierżawców z ESET Cloud Office Security. Usunięcie ESET Cloud Office Security jest trwałe i usuniętych danych nie można przywrócić.

Skaner ochrony przed spamem:

ESET Cloud Office Security skanuje wiadomości e-mail przechowywane w skrzynkach pocztowych w poszukiwaniu spamu. Z tego powodu ESET Cloud Office Security nie może uniemożliwić użytkownikowi wysyłania wiadomości spam na zewnętrzny adres e-mail. W mało prawdopodobnym scenariuszu, gdy poświadczenia użytkownika usługi Office 365 zostaną skradzione, mogą zostać użyte przez spamera do wysyłania zbiorczych wiadomości spam (wychodzący ruch e-mail).

Licencjonowanie dla ESET Cloud Office Security

Licencjami ESET Cloud Office Security można zarządzać za pośrednictwem konta ESET Business Account lub ESET MSP Administrator. ESET Cloud Office Security możesz wypróbować 30-dniową licencję próbną.

- Skorzystaj z sekcji ESET Business Account, aby utworzyć konto, dodać licencję lub zarządzać licencją.
- Skorzystaj z ESET MSP Administrator, jeśli jesteś dostawcą usług zarządzanych.

ESET Business Account oraz ESET MSP Administrator (hybrydowe konto licencyjne)

Jeśli masz ten sam adres e-mail zarejestrowany dla kont ESET MSP Administrator i ESET Business Account (logowanie jednokrotne), możesz przełączać się między widokami kont ESET Business Account i ESET MSP Administrator. Chroń użytkowników lub firmy za pomocą zarządzania licencjami dla produktu ESET Cloud Office Security.

Okres prolongaty wygasającej licencji w ESET Business Account

Kiedy zbliża się termin wygaśnięcia licencji, w interfejsie portalu ESET Business Account zostanie wyświetlony alert. Jeśli data wygaśnięcia minie, a licencja nie zostanie odnowiona ani nie zostanie aktywowana nowa licencja, w portalu ESET Business Account zostanie wyświetlony alert o wygaśnięciu. Jeśli odpowiednia licencja nie zostanie zapewniona, w portalu ESET Business Account zostanie wyświetlone powiadomienie o tym, że licencja zostanie zawieszona za 14 dni. Otrzymasz też wiadomość e-mail wysłaną na adres podany w danych swojego konta administratora.

Po wygaśnięciu licencji masz jeszcze 14 dni na jej odnowienie. W połowie tego okresu otrzymasz jeszcze powiadomienie w portalu ESET Business Account i w wiadomości e-mail. Po upływie 14 dni możliwość korzystania z programu ESET Cloud Office Security zostanie zawieszona. Konto stanie się niedostępne i niefunkcjonalne. Zawieszone konto ESET Cloud Office Security zostanie zachowane i będzie można odzyskać do niego dostęp poprzez dodanie nowej licencji ESET Cloud Office Security do konta ESET Business Account. Twoje konto programu ESET Cloud Office Security może pozostać zawieszone przez 30 dni. Po tym czasie zostanie trwale usunięte.

Jeśli Twoje konto zostanie zawieszone, zostaniesz o tym powiadomiony w ESET Business Account oraz w wiadomości e-mail 14 dni przed usunięciem konta. Aby odzyskać dostęp do konta ESET Cloud Office Security, musisz aktywować swoją licencję ESET Cloud Office Security.

> Użytkownicy są nadal w pełni chronieni w okresie prolongaty. Po zakończeniu okresu prolongaty użytkownicy utracą ochronę.

Zawieszona licencja

Jeśli nie posiadasz aktywnej licencji ESET Cloud Office Security na koncie ESET Business Account, Twoja instancja ESET Cloud Office Security zostanie zawieszona. Nie będzie można otworzyć instancji programu ani z niej korzystać. Twoja instancja programu ESET Cloud Office Security może być zawieszona przez 30 dni. Po tym czasie zostanie trwale usunięta. Aby odzyskać dostęp do swojej instancji programu ESET Cloud Office Security, musisz aktywować nową licencję obsługiwaną w programie ESET Cloud Office Security.

ESET Business Account

ESET Business Account działa jako ujednolicony punkt dostępu dla ESET Business Account i ESET Cloud Office Security. Dostęp do ESET Cloud Office Security możesz uzyskać poprzez stronę logowania do ESET Business Account lub ESET Cloud Office Security. Obie strony przekierowują Cię do uwierzytelniania ESET Business Account, aby Cię zweryfikować.

- Utwórz nowe konto, jeśli nie masz zarejestrowanego konta w ESET Business Account.
- Jeśli masz konto ESET Business Account, dodaj swoją licencję ESET Cloud Office Security.
- Zarządzaj ESET Business Account.

Utwórz nowe konto ESET Business Account

1. Otwórz stronę logowania ESET Business Account i kliknij **Zarejestruj się za darmo**. Dokładnie wypełnij formularz rejestracyjny. Wprowadzony adres e-mail będzie używany jako login.

2. Hasło musi zawierać co najmniej 10 znaków. Wpisz swoje **imię i nazwisko** oraz **dane firmy**, a następnie kliknij przycisk **Kontynuuj**. Przeczytaj **warunki korzystania z produktu firmy ESET** i zaznacz, że je akceptujesz. Wypełnij formularz reCAPTCHA i kliknij opcję **Rejestracja**.

3. Po pomyślnej rejestracji otrzymasz wiadomość e-mail (może to potrwać do 15 minut). Kliknij łącze w wiadomości e-mail z potwierdzeniem, aby otworzyć nowe okno **Aktywowanie konta**.

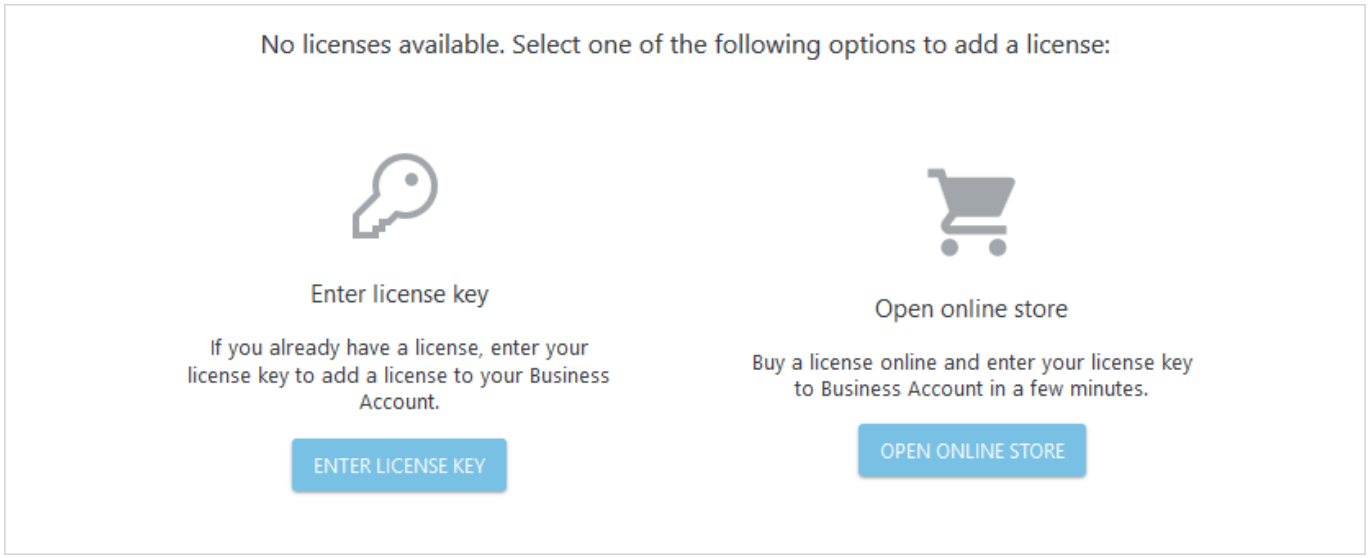
4. Wpisz swoje hasło i kliknij opcję **Aktywuj**, aby aktywować swoje konto ESET Business Account. Otrzymasz kolejną wiadomość e-mail mającą na celu zweryfikowanie, czy konto ESET Business Account zostało pomyślnie utworzone. Teraz możesz zalogować się w ESET Business Account.

Po aktywacji ESET Business Account dodaj swoją licencję ESET Cloud Office Security.

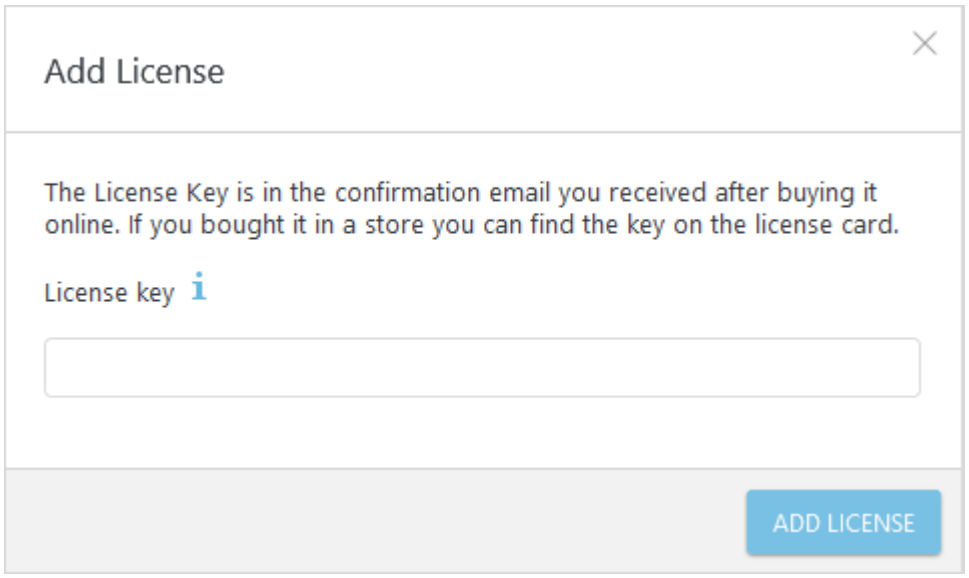
Dodaj licencję ESET Cloud Office Security w ESET Business Account

Jeśli jesteś nowym użytkownikiem, po pomyślnym zalogowaniu się do konta ESET Business Account zostanie wyświetlony ekran powitalny ESET Business Account.

1. Kliknij **Dodaj licencję**, aby otworzyć okno licencji. Jeśli jesteś zwykłym użytkownikiem ESET Business Account, przejdź do karty **Licencja** i kliknij pozycję **Dodaj licencję**.



2. Wprowadź swój **klucz licencyjny** i kliknij **Dodaj licencję**.



3. Otrzymasz wiadomość e-mail z linkiem weryfikacyjnym. Kliknij łącze i wprowadź wymagane dane logowania do portalu ESET Business Account. Aby uzyskać więcej informacji na temat zarządzania licencjami, użytkowników i witryn odwołaj się do przewodnika po ESET Business Account.

Zarządzaj ESET Business Account

Wspólne działania związane z licencjonowaniem:

Witryny i pula licencji

Licencje i pule licencji są ładowane z ESET Business Account. Pule licencji są dostępne tylko wtedy, gdy masz istniejące witryny w obrębie ESET Business Account.

Stwórz nowego użytkownika w ESET Business Account

Możesz utworzyć konto użytkownika, który będzie pomagał Ci w zarządzaniu Twoją pulą licencji.

1. Otwórz ESET Business Account i zaloguj się.

2. Wybierz **Zarządzanie użytkownikami**, kliknij **Nowy użytkownik** i wpisz wymagane informacje.

3. Wybierz **Uprawnienia dostępu** dla użytkownika ESET Cloud Office Security:

   • **Odczyt** — użytkownik ma dostęp do ESET Cloud Office Security, listy użytkowników, dzienników, wykryć, ale nie może zarządzać politykami, chronić użytkowników ani zwolnić niczego z kwarantanny.

   • **Zapisz** — użytkownik ma pełny dostęp do ESET Cloud Office Security, może przeglądać i zarządzać użytkownikami, kwarantanną, a także tworzyć polityki.

   • **Brak dostępu** — użytkownik nie może uzyskać dostępu do ESET Cloud Office Security

4. Ustaw język w **Preferencjach** użytkownika konsoli ESET Cloud Office Security.

5. Kliknij przycisk **Utwórz**, który utworzy użytkownika.

Tworzenie nowej witryny w ESET Business Account

Lokacje umożliwiają dzielenie i scalanie licencji w postaci pul licencji. Lokacje to pojedyncze grupy, które mają własną lokalizację i własnych administratorów.

1. Otwórz ESET Business Account i zaloguj się.

2. Wybierz pozycję **Szczegóły**, kliknij przycisk **Utwórz lokalizację** i wpisz wymagane dane osobowe.

3. Kliknij pozycję **Dodaj użytkownika**, wybierz użytkownika i kliknij przycisk **Potwierdź**.

4. W puli licencji kliknij pozycję **Dodaj jednostki** i wybierz licencję ESET Cloud Office Security. Możesz zmienić **podjednostki** i kliknąć przycisk **Potwierdź**.

5. Kliknij przycisk **Utwórz**, który utworzy witrynę.

ESET MSP Administrator

ESET MSP Administrator to system zarządzania licencjonowaniem, który umożliwia użytkownikom MSP tworzenie wielu klientów MSP i generowanie określonej licencji z liczbą stanowisk. Portal licencjonowania ESET MSP Administrator obsługuje ceny zbiorcze i rozliczenia na podstawie dokładnej liczby zakupionych stanowisk.

Produkt ESET Cloud Office Security jest dostępny dla wszystkich MSP Managers, a użytkownik MSPs managed MSPs. Użytkownik ESET MSP Administrator z dostępem do zapisu jest uprawniony do aktywacji produktu ESET Cloud Office Security. Usługa ESET Cloud Office Security jest dostępna dla użytkowników z uprawnieniami do zapisu, odczytu lub niestandardowymi prawami dostępu.

   • Utwórz nowego klienta MSP (adres e-mail klienta jest wymagany do aktywacji konsoli ESET Cloud Office Security).

   • Aktywuj ESET Cloud Office Security z ESET MSP Administrator.

Aktywacja usługi ESET Cloud Office Security

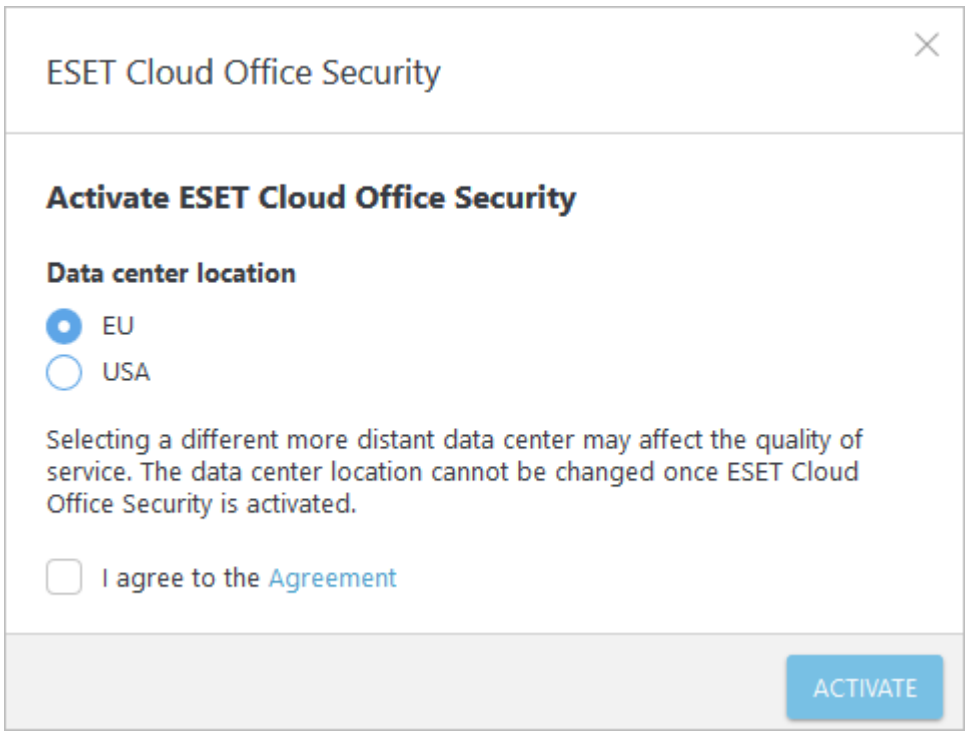
1. Zaloguj się do konta ESET Business Account lub ESET MSP Administrator i znajdź kafelek ESET Cloud Office Security na **panelu kontrolnym**.

2. Kliknij **Aktywuj** w prawym dolnym rogu kafelka ESET Cloud Office Security.

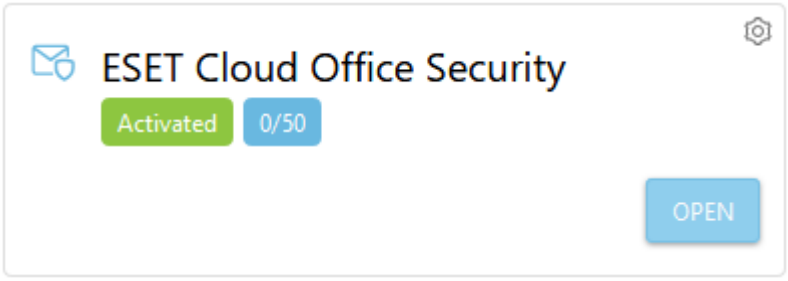


3. Kreator aktywacji odeśle Cię do ESET Cloud Office Security Warunków użytkowania i wyświetli optymalną lokalizację centrum danych na podstawie bieżącej lokalizacji. Wybierz opcję **Akceptuję Warunki użytkowania** i kliknij przycisk **Aktywuj**. Nie zaleca się zmiany lokalizacji centrum danych, jednak w razie potrzeby możesz ją zmienić.

Centra danych są całkowicie oddzielone. Po wybraniu lokalizacji centrum danych nie można jej zmienić i nie można przeprowadzić migracji do innej lokalizacji. Aby zmienić centrum danych, rozpocznij proces aktywacji od początku.

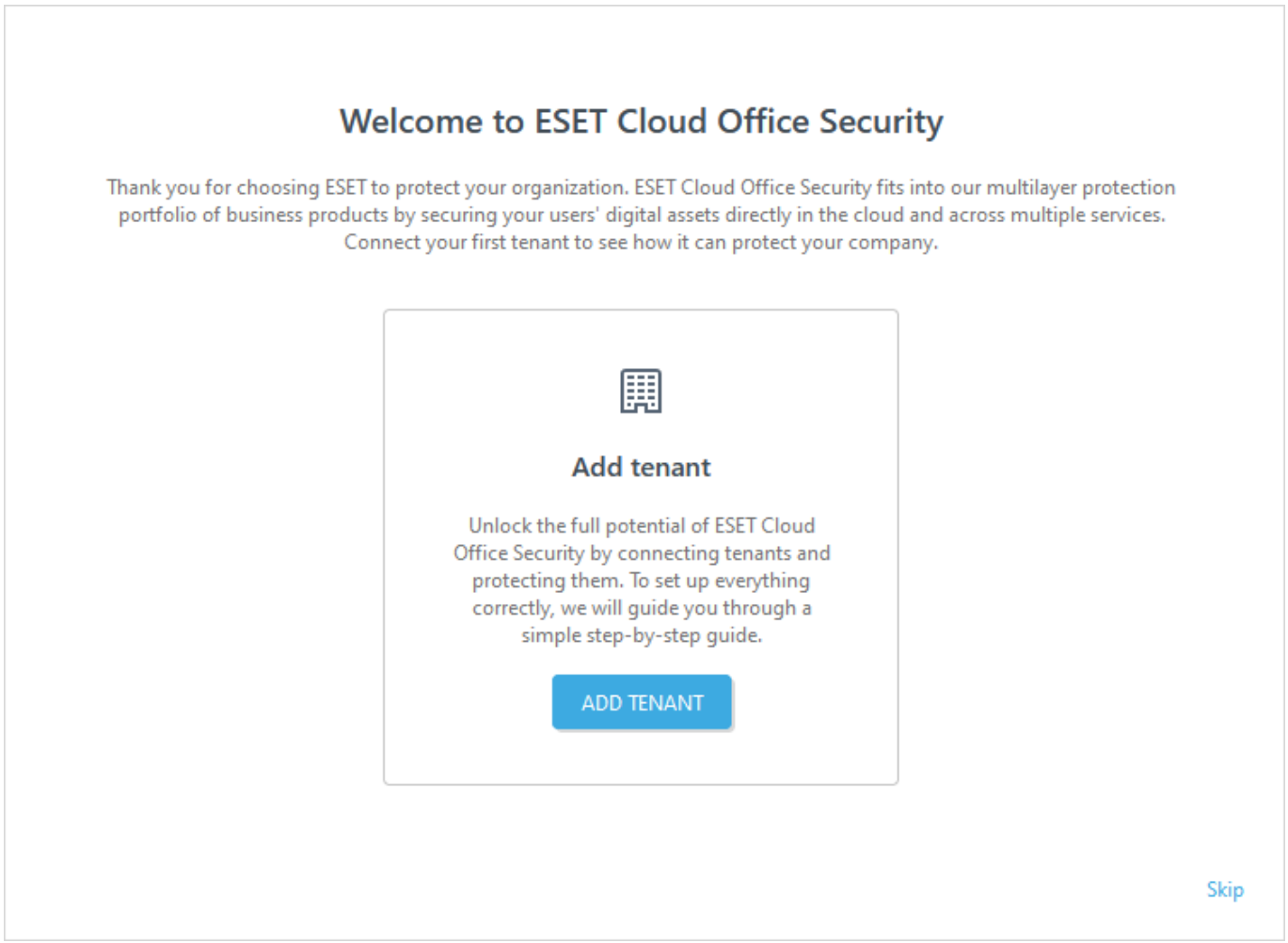


4. Kliknij **Otwórz** na kafelku ESET Cloud Office Security. Panel kontrolny ESET Cloud Office Security zostanie otwarty w nowej karcie przeglądarki.

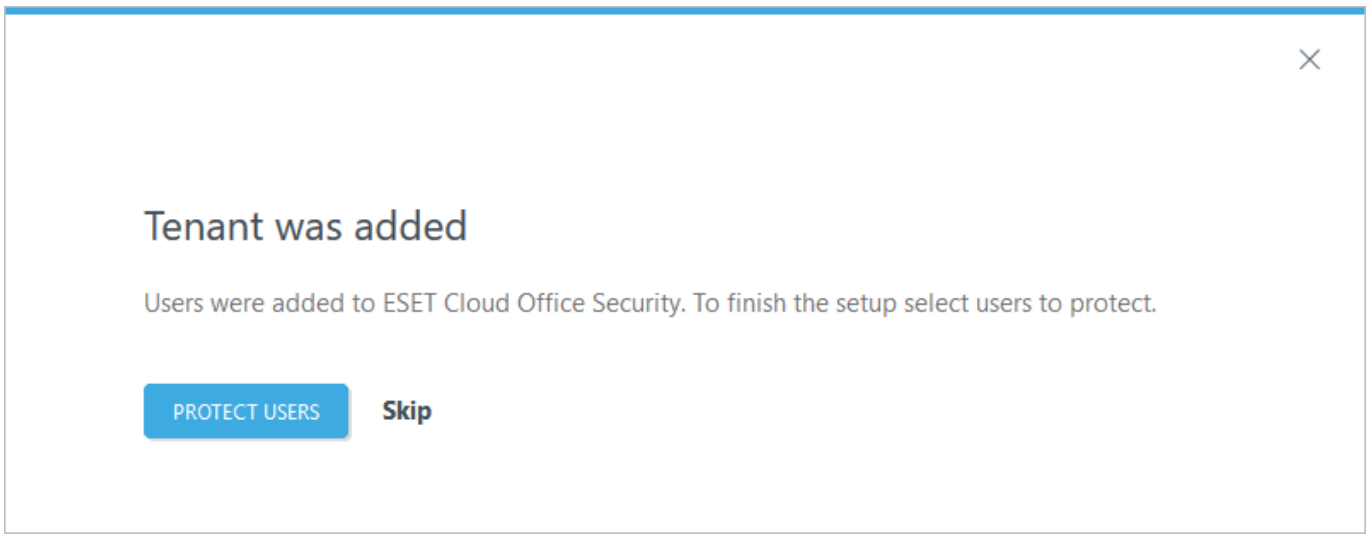


Przy pierwszym logowaniu do ESET Cloud Office Security pojawi się **Kreator uruchamiania**. Ten kreator przeprowadzi Cię przez proces wdrażania początkowego.

1. Dodaj dzierżawę (Microsoft 365 lub Google Workspace).



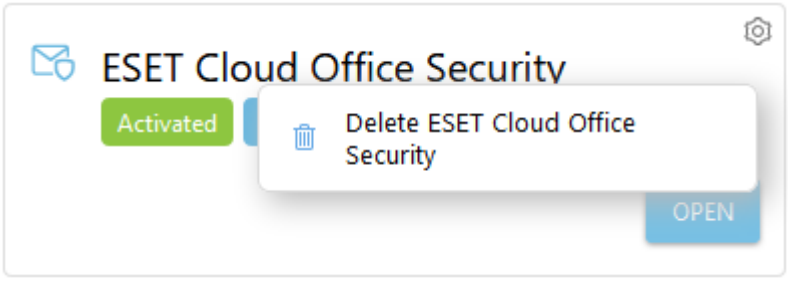
2. Chroń użytkowników. Jeśli **pominiesz** ten krok, możesz później zapewnić ochronę użytkownikom lub firmom za pomocą funkcji zarządzania licencją dla ESET Cloud Office Security.



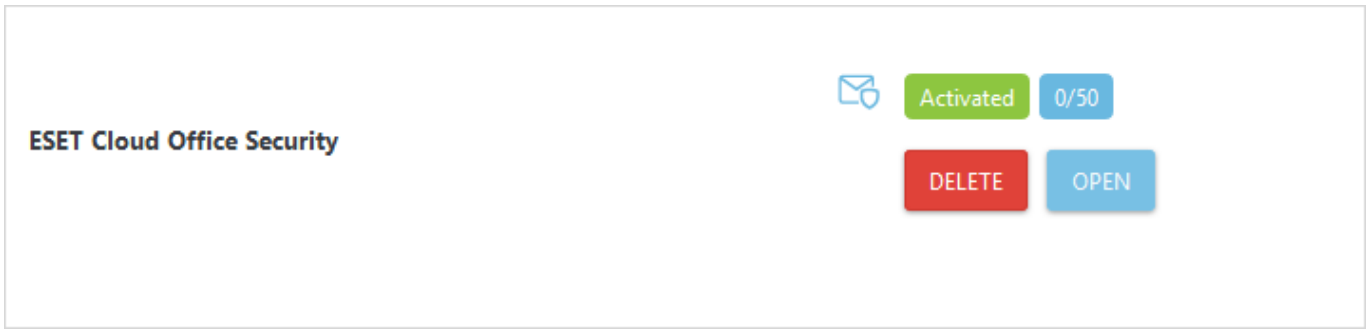
Zdezaktywuj ESET Cloud Office Security

1. Zaloguj się do konta ESET Business Account lub ESET MSP Administrator i znajdź kafelek ESET Cloud Office Security na **panelu kontrolnym**.

2. Kliknij ikonę koła zębatego w prawym górnym rogu kafelka ESET Cloud Office Security i wybierz **Usuń ESET Cloud Office Security**.

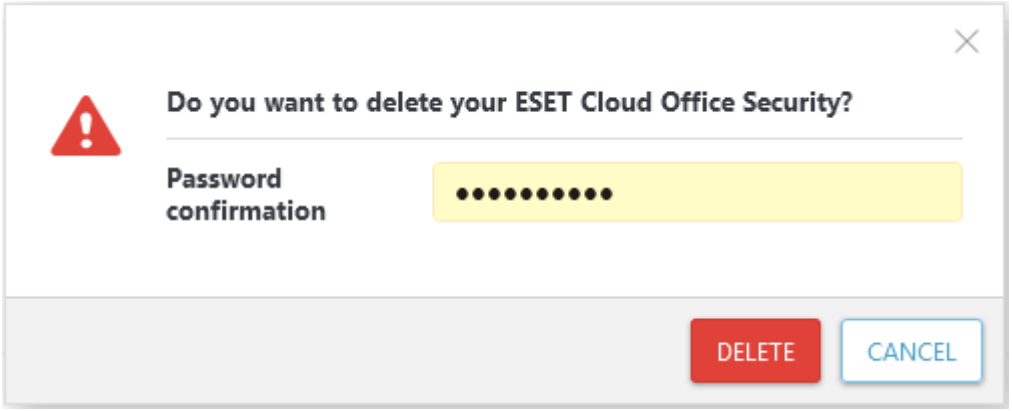


3. Możesz też przejść do sekcji **Szczegóły** i kliknąć przycisk **Usuń**.



4. Pojawi się okno z ostrzeżeniem, że wszystkie dane zostaną usunięte. Wprowadź hasło do konta ESET Business Account, aby potwierdzić wybór, a następnie kliknij **Usuń**.

Usunięcie ESET Cloud Office Security jest trwałe. Usuniętych danych nie można przywrócić.



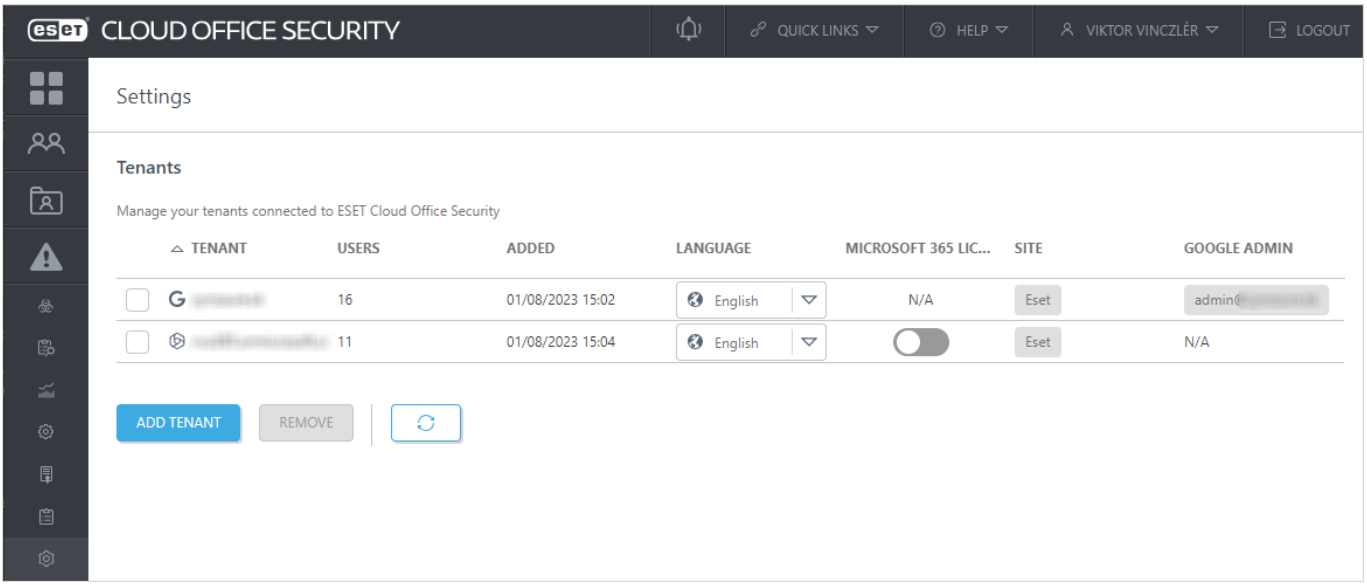
Instancja ESET Cloud Office Security zostanie usunięta, a kafelek produktu ESET Cloud Office Security zostanie zmieniony na **Nieaktywowany**. Otrzymasz również wiadomość e-mail z potwierdzeniem z ESET Business Account.

Zarządzanie dzierżawami w Ustawieniach

Zarządzanie dzierżawami połączonymi z ESET Cloud Office Security. Możesz zobaczyć wszystkie zarejestrowane dzierżawy w tabeli zawierającej szczegóły dotyczące każdej dzierżawy. Użyj przycisku Odśwież, aby ponownie załadować tabelę z dzierżawami.

Jeśli chcesz dodać nową dzierżawę, kliknij Add tenant (Dodaj dzierżawę) i wybierz Microsoft 365 lub Google Workspace w zależności od platformy w chmurze, którą chcesz chronić. Po zakończeniu procesu rejestracji dzierżawy Twoja platforma Microsoft 365 lub Google Workspace jest chroniona przez ESET Cloud Office Security.

Po dodaniu dzierżawy ekran zmienia się, pokazując listę dzierżaw skojarzonych z lokacją, można zarządzać istniejącą dzierżawą lub dodać więcej dzierżaw. W tabeli przedstawiono nazwę dzierżawy, liczbę użytkowników, datę dodania dzierżawy, ustawienie języka, licencjonowanych użytkowników platformy Microsoft 365, nazwę witryny i administratora Google.



Język

To ustawienie określa język wiadomości e-mail z powiadomieniami wysyłanych do członków dzierżawy. Język można zdefiniować dla każdej dzierżawy osobno, na przykład w przypadku MSP zarządzającego wieloma firmami.

Aby usunąć dzierżawę z ESET Cloud Office Security, wybierz odpowiednią dzierżawę i kliknij przycisk Usuń. Pojawi

się okno potwierdzenia, gdzie należy podjąć ostateczną decyzję. Po usunięciu wszystkie dane użytkownika zostaną wymazane po 30 dniach.

Użytkownicy posiadający licencję Microsoft 365

Opcja ta jest domyślnie włączona. Odpowiada ona liście użytkowników w centrum administracyjnym usługi Microsoft 365, którą można znaleźć w sekcji **Użytkownicy** > **Aktywni użytkownicy** > Filtruj: **Licencjonowani użytkownicy**

Wyłączenie tej opcji sprawi, że ESET Cloud Office Security wyświetli wszystkich użytkowników, w tym użytkowników bez licencji usługi Microsoft 365 (np. użytkowników skrzynek współużytkowanych). Jeśli używasz automatycznej ochrony dla grupy lub dzierżawy zawierającej użytkowników bez licencji usługi Microsoft 365, użytkownicy ci staną się widoczni, chronieni i będą korzystać z jednostek licencji ESET Cloud Office Security. Stan ochrony nowo widocznych użytkowników może być określony jako **Oczekujący** do 1 godziny. Gdy proces automatycznej ochrony dobiegnie końca, stan ochrony w sekcji **Użytkownicy** zmieni się na Pod ochroną lub inny możliwy stan.

> Jeśli dzierżawa lub grupa z automatyczną ochroną zawiera użytkownika bez skrzynki pocztowej i usługi OneDrive, ten użytkownik będzie korzystać z jednostki licencji ESET Cloud Office Security. Dla tego użytkownika zostanie wyświetlony stan ochrony **Ostrzeżenie**.

Po ponownym włączeniu opcji Użytkownicy posiadający licencję Microsoft 365 wyświetleni zostaną tylko użytkownicy z licencją usługi Microsoft 365. Użytkownicy z automatyczną ochroną, którzy nie posiadają licencji usługi Microsoft 365, znikną z sekcji Użytkownicy, a jednostki licencyjne ESET Cloud Office Security zostaną zwolnione. Zmiana może potrwać do 1 godziny.

> Jeśli masz ręcznie chronionych użytkowników bez licencji usługi Microsoft 365 (gdy wyłączono ustawienie **Użytkownicy posiadający licencję Microsoft 365**), użytkownicy ci pozostaną widoczni i chronieni nawet po włączeniu funkcji **Użytkownicy posiadający licencję Microsoft 365** (dopóki użytkownicy nie staną się niechronieni).

Lokacja

Jeśli chcesz zmienić lokację, z którą jest skojarzona dzierżawa, kliknij nazwę lokacji, aby otworzyć okno **Select a site to protect** (Wybierz witrynę, którą chcesz chronić) i wprowadzić wymagane zmiany.

Administrator Google

Administrator Google powinien być aktywnym adresem e-mail administratora Google Workspace.

> Jeśli rola lub adres e-mail administratora ma się zmienić, zaktualizuj informacje administratora Google, klikając je. Zrób to z wyprzedzeniem, aby zapewnić funkcjonalność dzierżawy i ochronę swojej witryny.

Zgoda na aktualizację

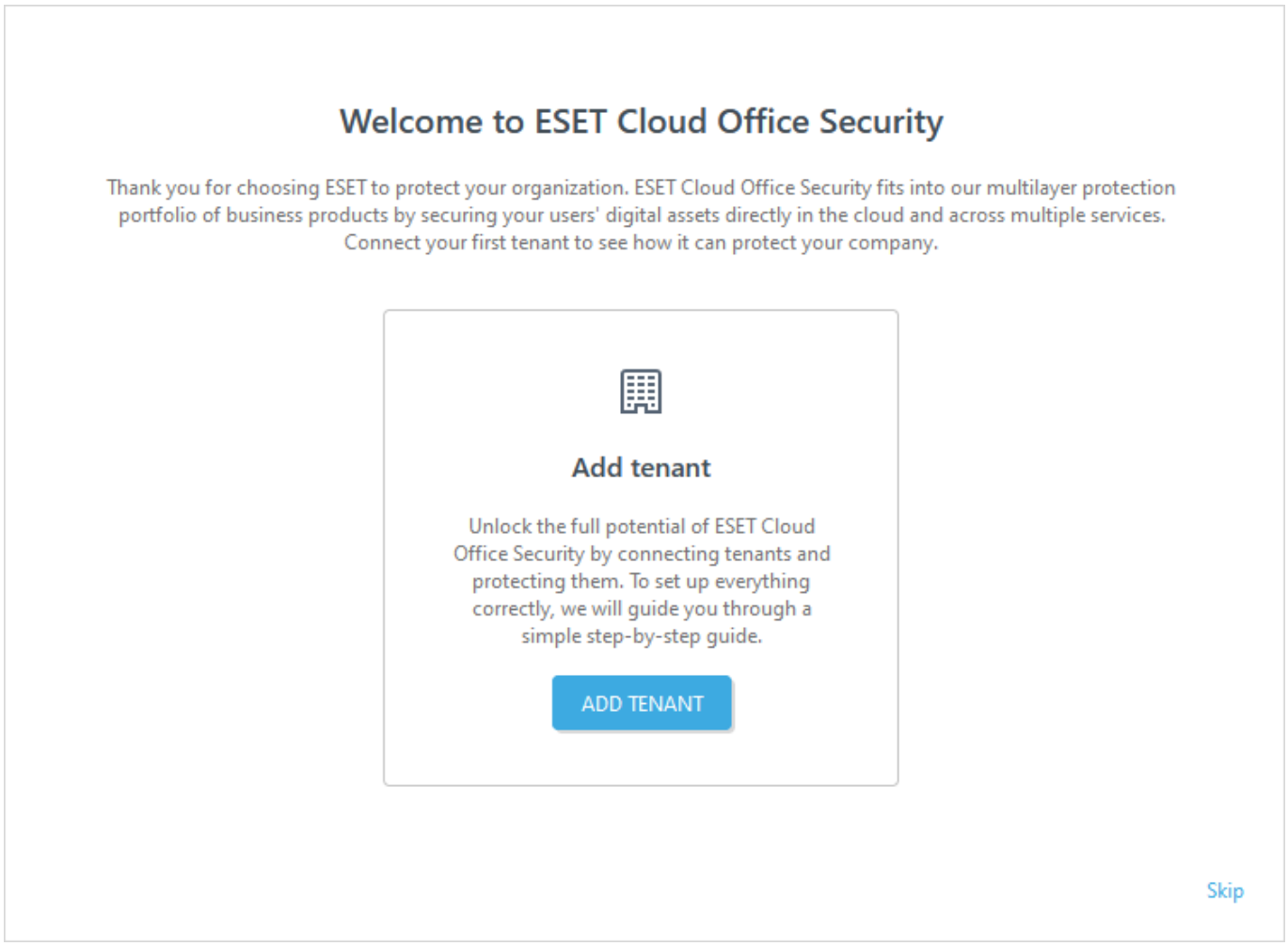
Jeśli widoczny jest żółty przycisk, możesz zaktualizować swoją zgodę. Aktualizowanie zgody dla istniejącej dzierżawy rozszerza uprawnienia ESET Cloud Office Security do konta platformy Microsoft 365, włączając funkcję, która zawiera informacje o typie użytkownika. Typ użytkownika jest zdefiniowany w usłudze Azure Active Directory i będzie wyświetlany w sekcji Użytkownicy w dedykowanej kolumnie. Na przykład możesz filtrować użytkowników Microsoft 365 na podstawie ich typu, jeśli chcesz wyświetlić listę tylko udostępnionych skrzynek pocztowych.

Kliknij przycisk **Aktualizuj** dla każdej dzierżawy, dla której chcesz włączyć tę funkcję. Aktualizacja typu użytkownika z usługi Azure AD może potrwać do 24 godzin.

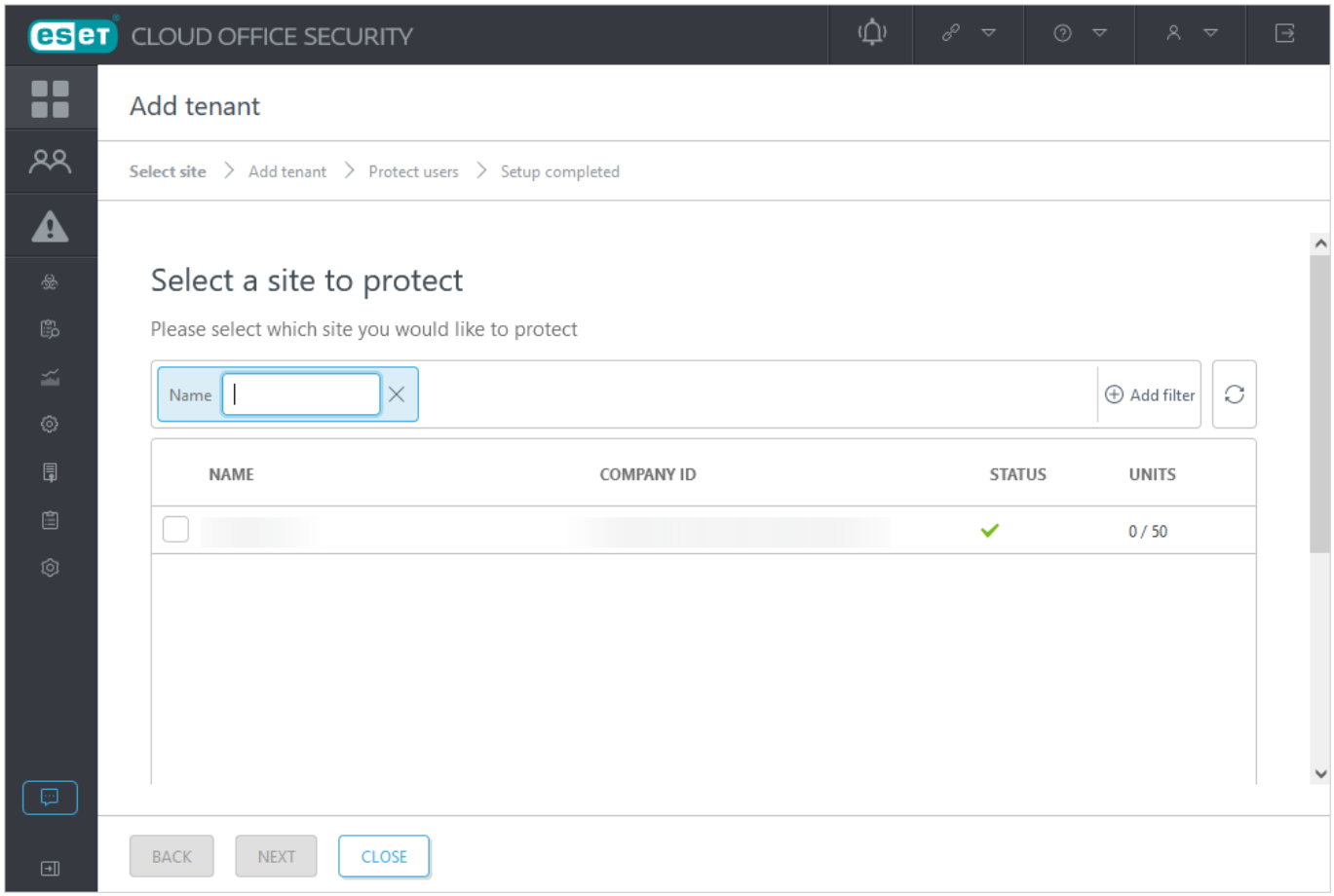
Jeśli wyświetlany jest czerwony przycisk, oznacza to, że zgoda została cofnięta lub wprowadzono inną zmianę, która wpłynęła na integrację dzierżawy z ESET Cloud Office Security. Kliknij przycisk **Aktualizuj**, jeśli chcesz nadal chronić użytkowników.

Dodaj swoją pierwszą dzierżawę

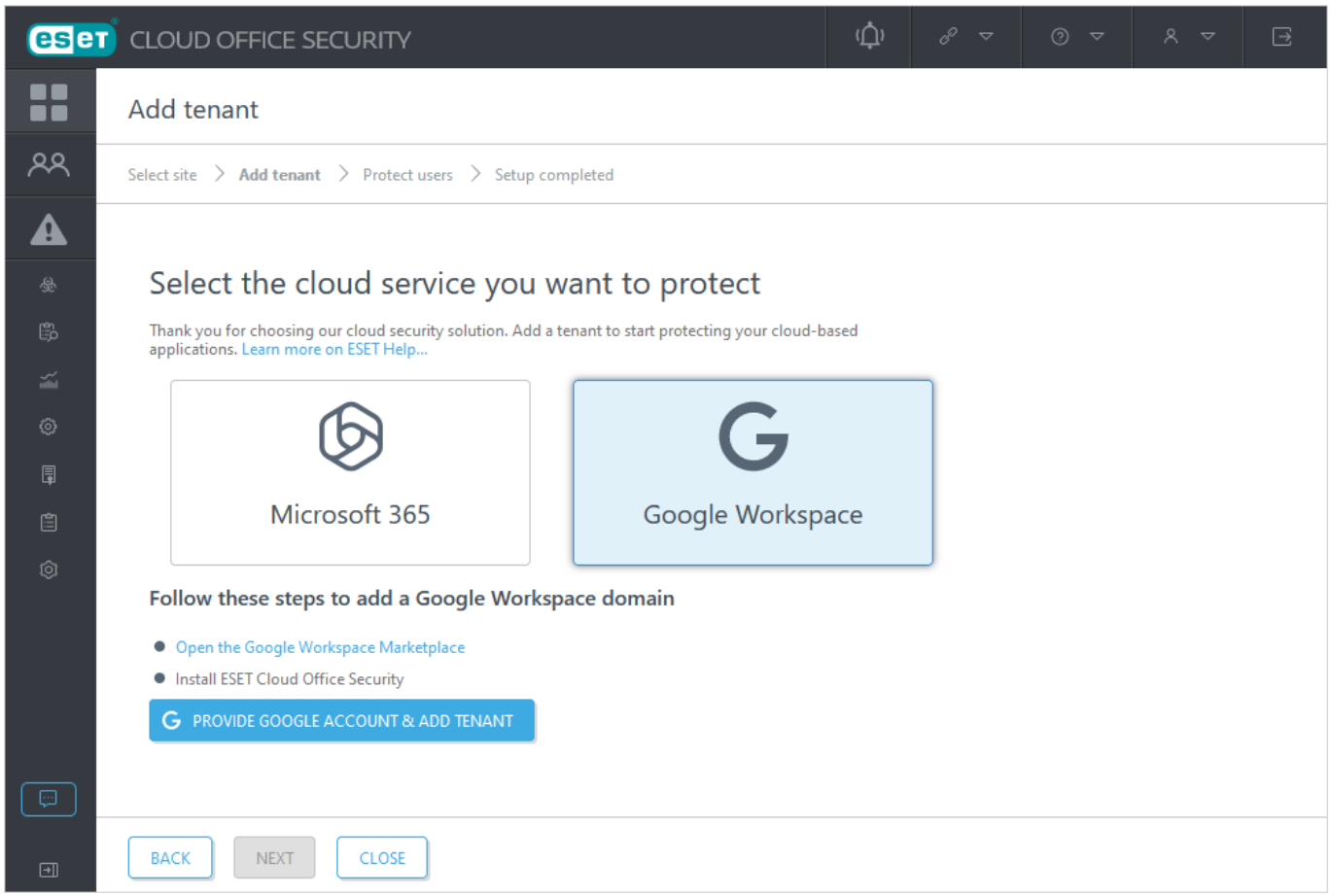
Aby chronić swoją platformę w chmurze, kliknij **Dodaj dzierżawę**, aby połączyć platformę Microsoft 365 lub Google Workspace z ESET Cloud Office Security.



Powinna zostać pokazana lista dostępnych witryn w oknie **Wybierz witrynę do ochrony**. Użyj pola wyboru, aby wybrać witrynę, którą chcesz skojarzyć z dzierżawą, a następnie kliknij przycisk **Dalej**.



Kliknij kafelek Microsoft 365 lub Google Workspace w oknie **Wybierz usługę w chmurze, którą chcesz chronić,** i postępuj zgodnie z instrukcjami podanymi w punktach:



Dzierżawa Microsoft 365

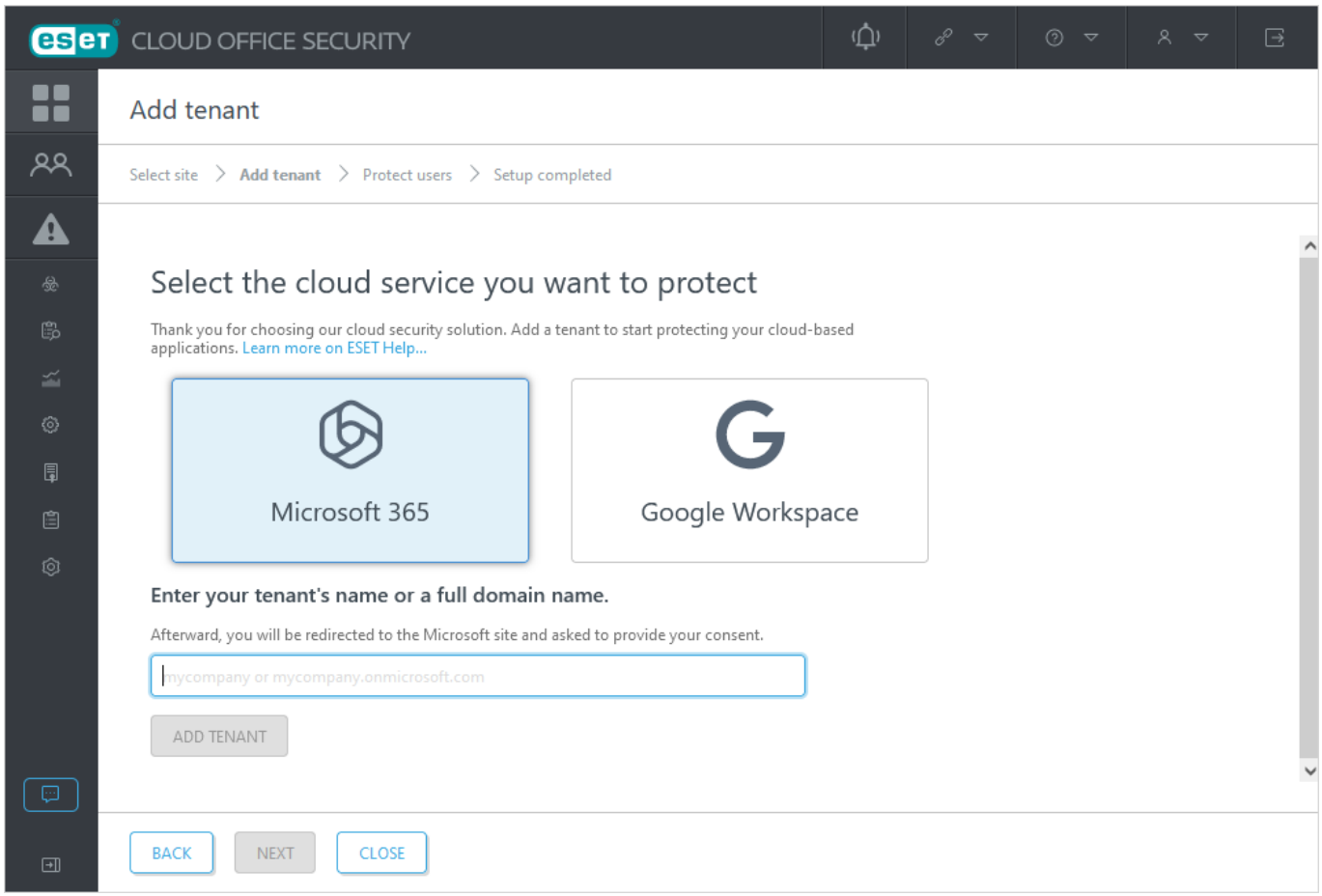
Usługa Azure Active Directory (Azure AD) organizuje obiekty takie jak użytkownicy i aplikacje w grupy nazywane dzierżawami. Typowym sposobem identyfikowania dzierżawy jest użycie nazwy domeny. Użytkownicy współużytkujący nazwę domeny są częścią tej samej dzierżawy. Dzierżawy umożliwiają ustawianie zasad dotyczących użytkowników i aplikacji organizacji w celu spełnienia zasad zabezpieczeń i operacyjnych. Możesz chronić wiele dzierżaw usługi Microsoft 365 i zarządzać nimi z jednej konsoli ESET Cloud Office Security.

Aby uzyskać więcej informacji, zobacz artykuł firmy Microsoft Dzierżawa w usłudze Azure Active Directory.

Dodaj dzierżawę

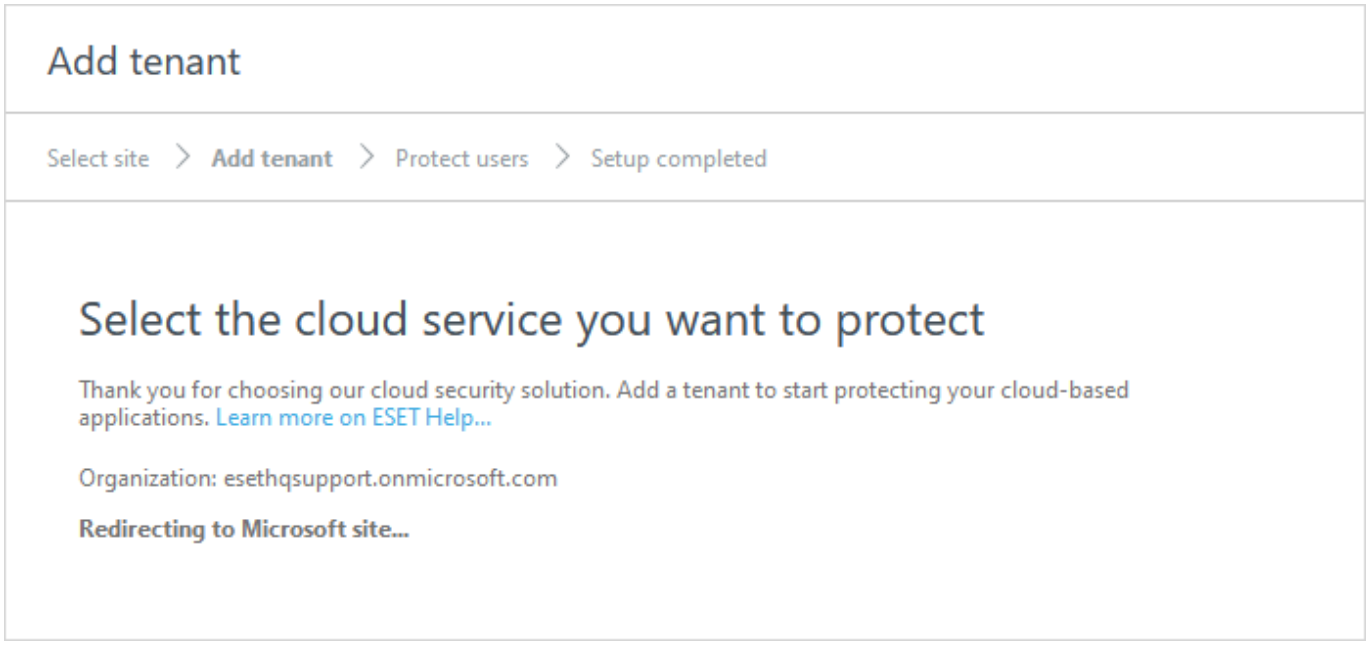
1. Przejdź do pozycji **Settings** (Ustawienia) i kliknij **Add tenant** (Dodaj dzierżawę) (lub w dowolnym miejscu, w którym widoczny jest przycisk **Add tenant** [Dodaj dzierżawę]).

2. Kliknij kafelek **Microsoft 365**.

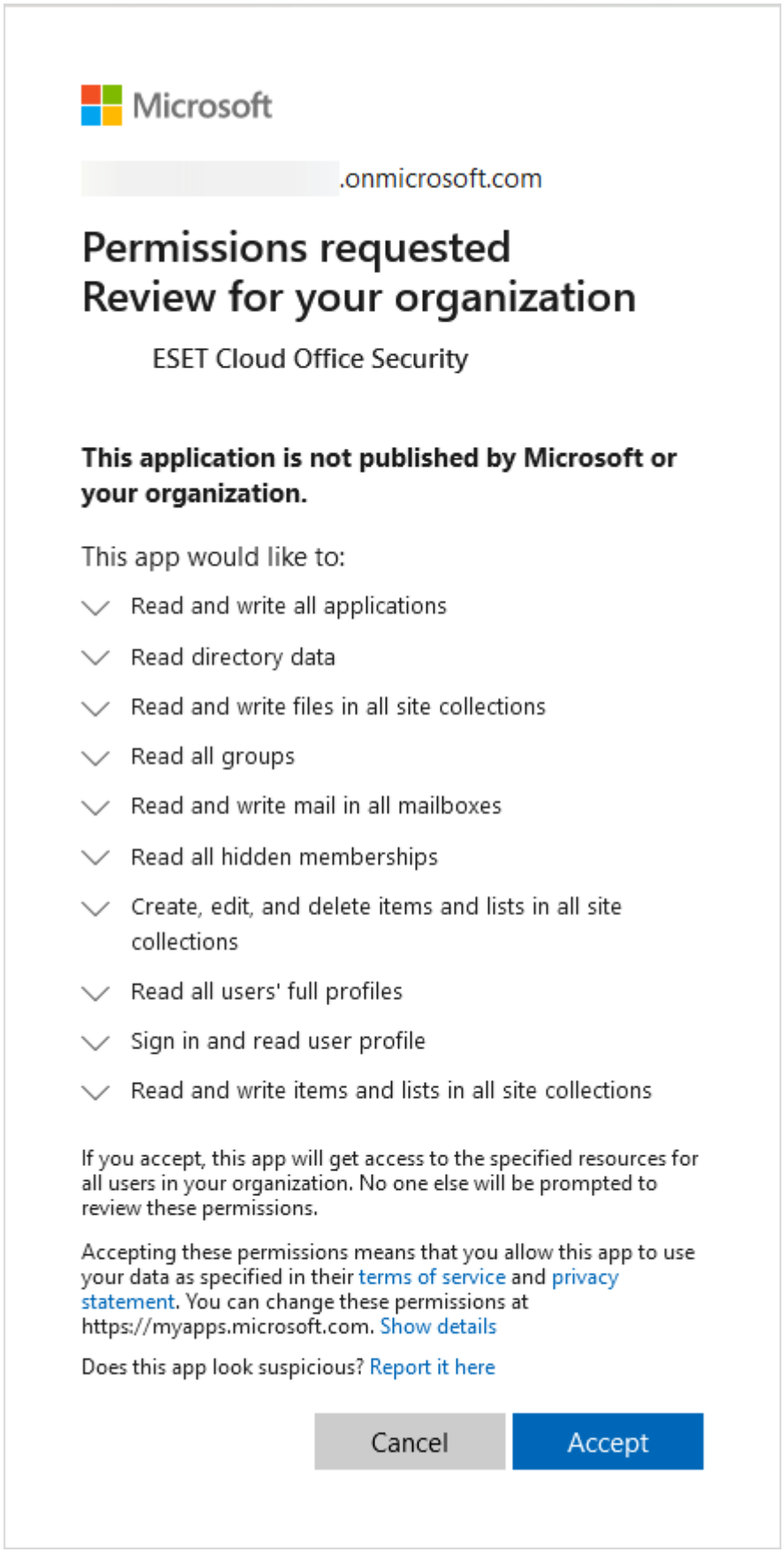


3. Wpisz nazwę dzierżawy usługi Microsoft 365 lub pełną nazwę domeny i kliknij pozycję **Dodaj dzierżawę**.

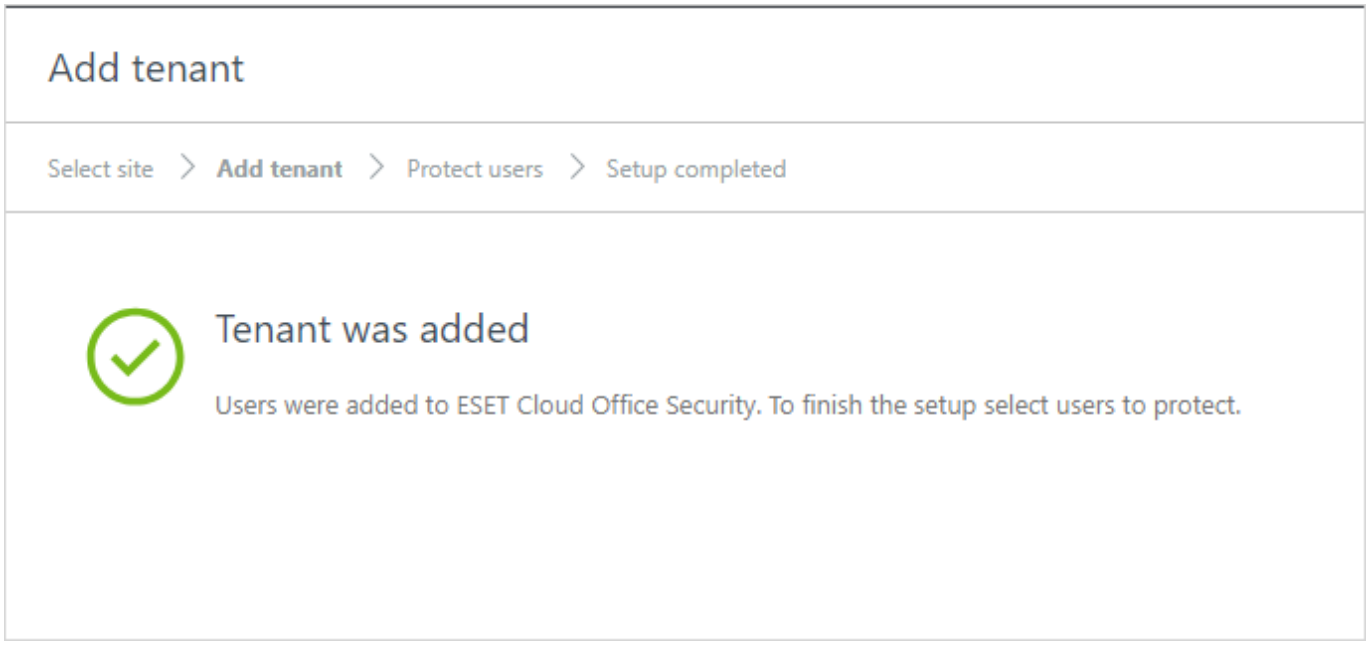
4. Użytkownik zostanie przekierowany na stronę usługi Microsoft Online zawierającą zgody dotyczące listy uprawnień wymaganych przez program ESET Cloud Office Security.



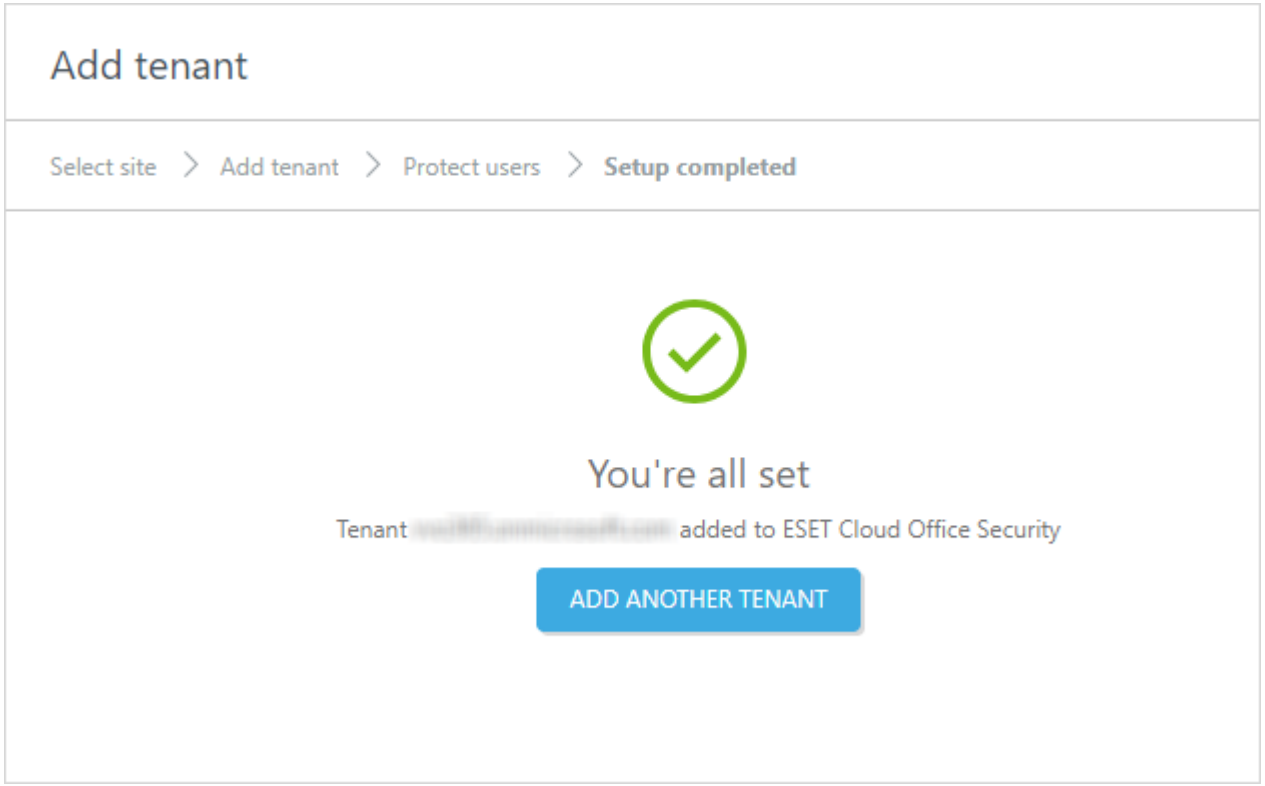
5. Wprowadź dane logowania do konta administratora usługi Microsoft 365, a następnie kliknij **Akceptuj**, aby zezwolić ESET Cloud Office Security na dostęp do danych znajdujących się na koncie Microsoft.



6. Twoja dzierżawa platformy Microsoft 365, w tym użytkownicy, została dodana.



7. Aby zakończyć konfigurację, kliknij przycisk **Dalej** i wybierz użytkowników do **ochrony**.



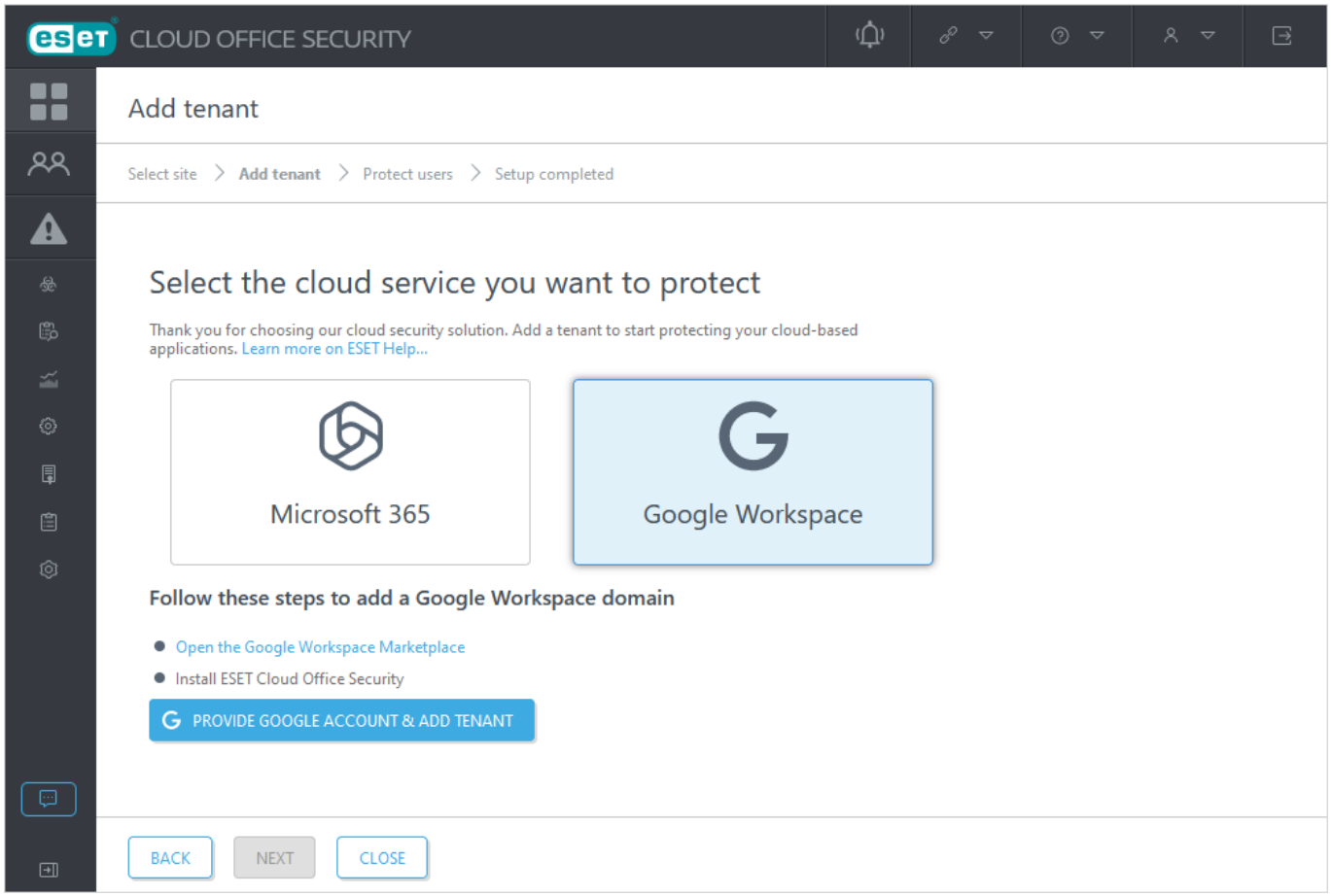
Dzierżawa Google Workspace

Zintegruj dzierżawę Google Workspace z ESET Cloud Office Security, aby włączyć ochronę dla użytkowników Google Workspace.

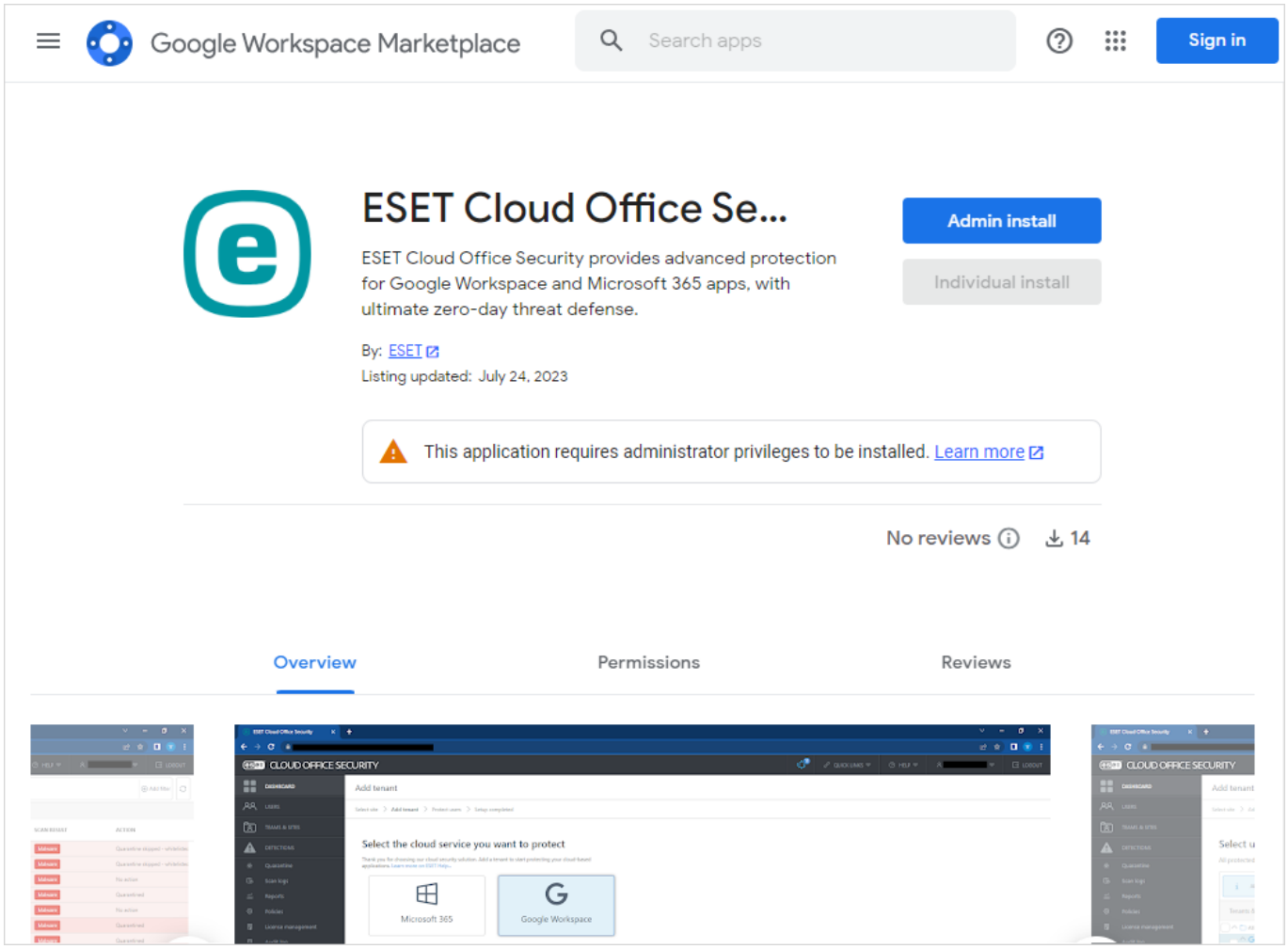
Dodaj dzierżawę

1. Przejdź do pozycji **Settings** (Ustawienia) i kliknij **Add tenant** (Dodaj dzierżawę) (lub w dowolnym miejscu, w którym widoczny jest przycisk **Add tenant** [Dodaj dzierżawę]).

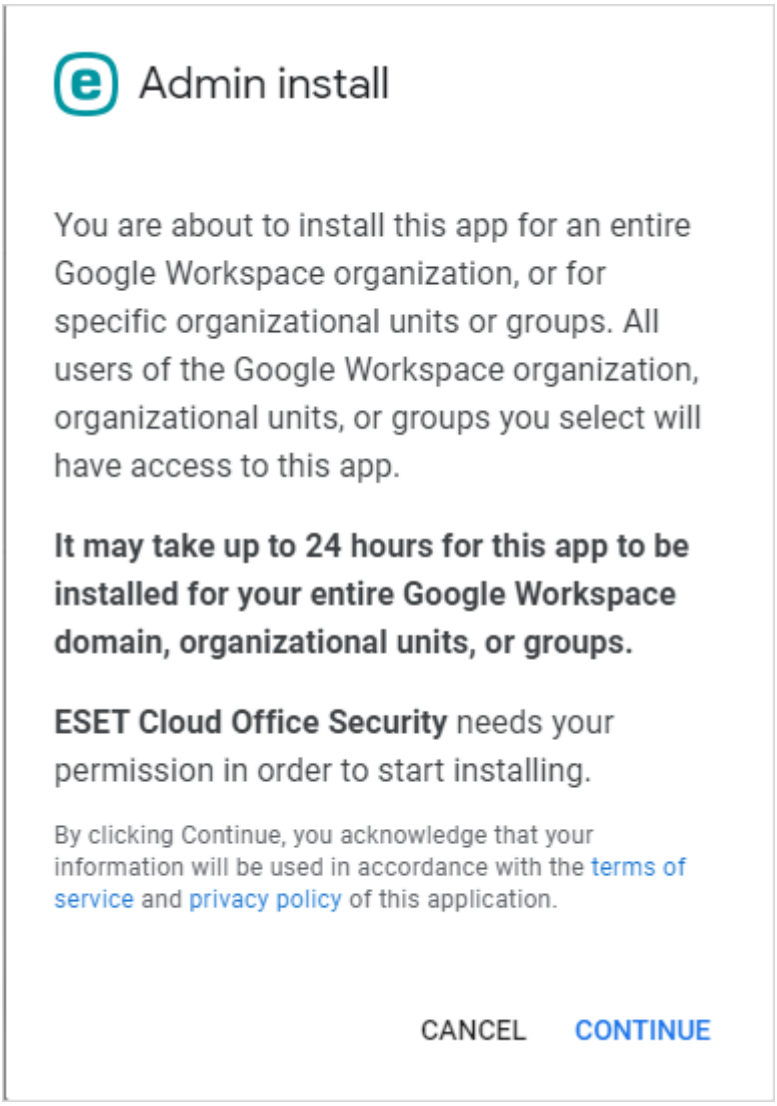
2. Kliknij kafelek **Google Workspace**.



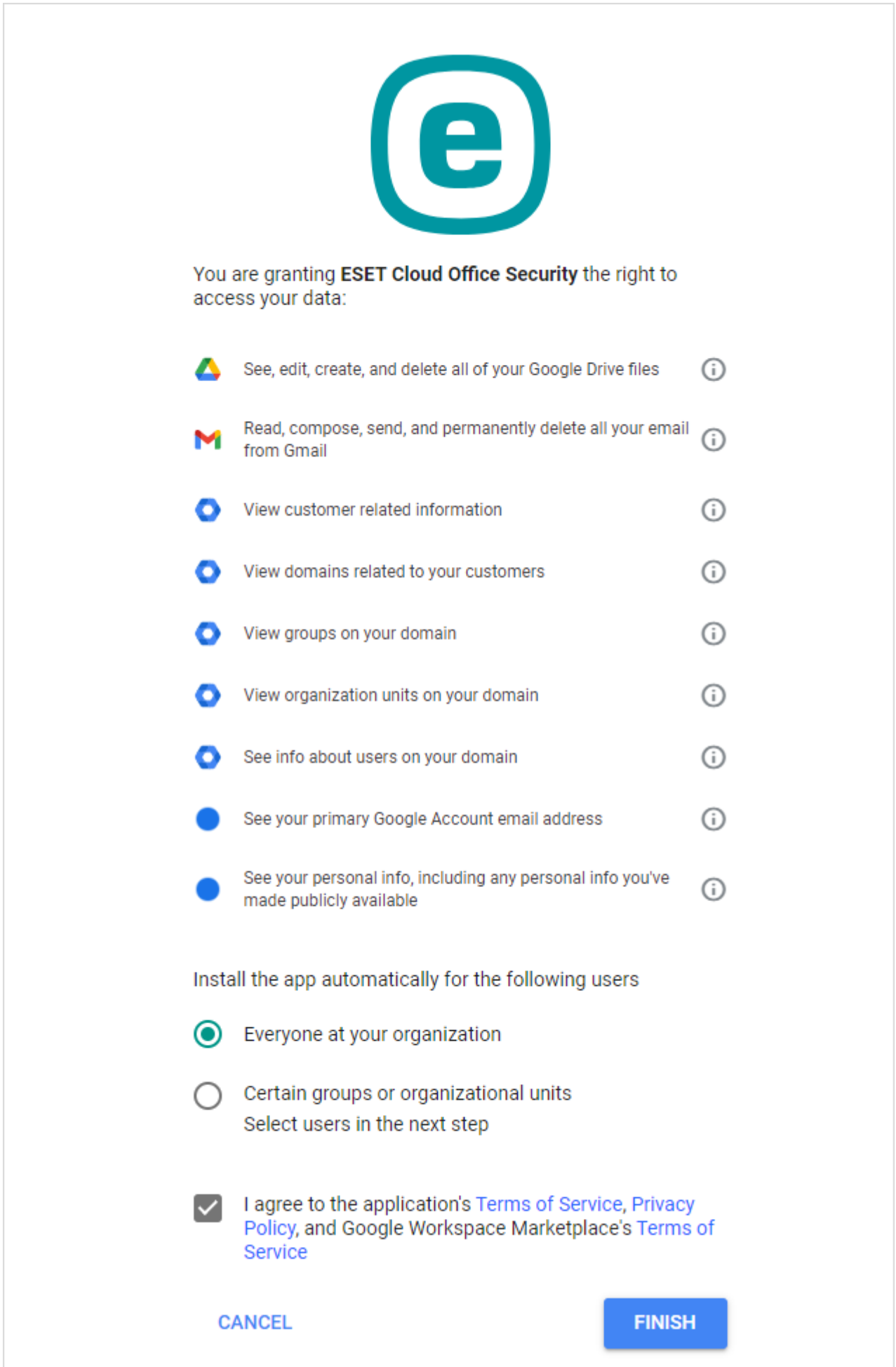
3. Kliknij Open the Google Workspace Marketplace (Otwórz Google Workspace Marketplace) i zainstaluj aplikację ESET Cloud Office Security przy użyciu konta administratora. Aplikacja ESET Cloud Office Security jest obecnie dostępna w Google Workspace Marketplace tylko za pośrednictwem bezpośredniego łącza w tym kreatorze.



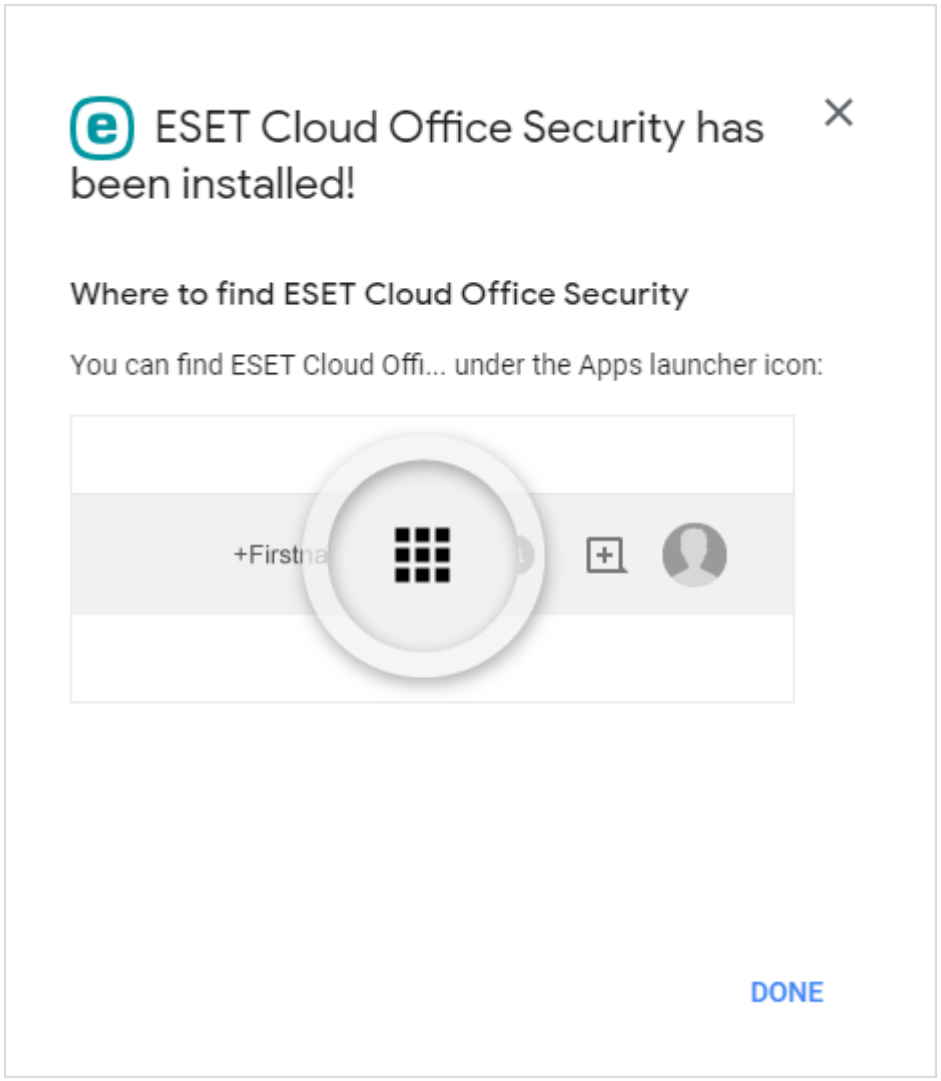
4. Kliknij przycisk **Continue** (Kontynuuj) na ekranie **Admin install** (Instalacja przez administratora).



5. Upewnij się, że na ekranie praw dostępu jest zaznaczona opcja **Everyone at your organization** (Wszyscy w organizacji). Ponadto pole wyboru Warunki korzystania z usługi i Polityka prywatności powinno być zaznaczone przed kliknięciem przycisku **Finish** (Zakończ).

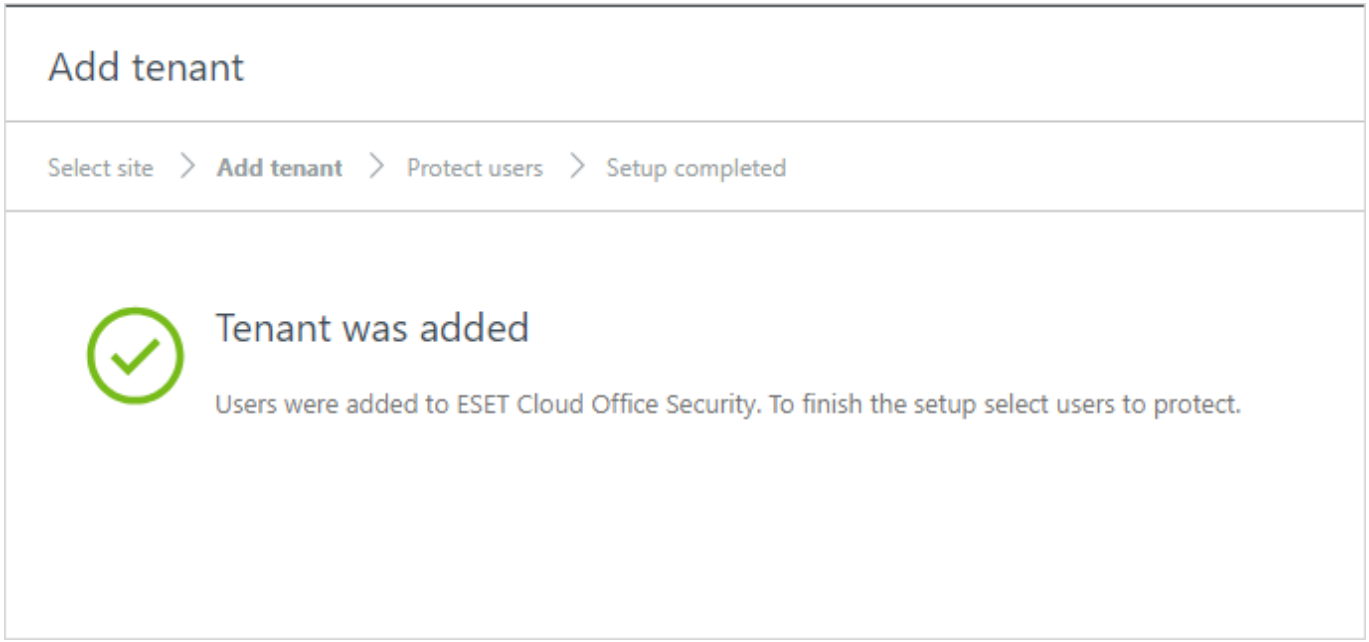

You are granting **ESET Cloud Office Security** the right to access your data:
See, edit, create, and delete all of your Google Drive files
Read, compose, send, and permanently delete all your email from Gmail
View customer related information
View domains related to your customers
View groups on your 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. Aplikacja ESET Cloud Office Security jest zainstalowana, kliknij **Done** (Gotowe).

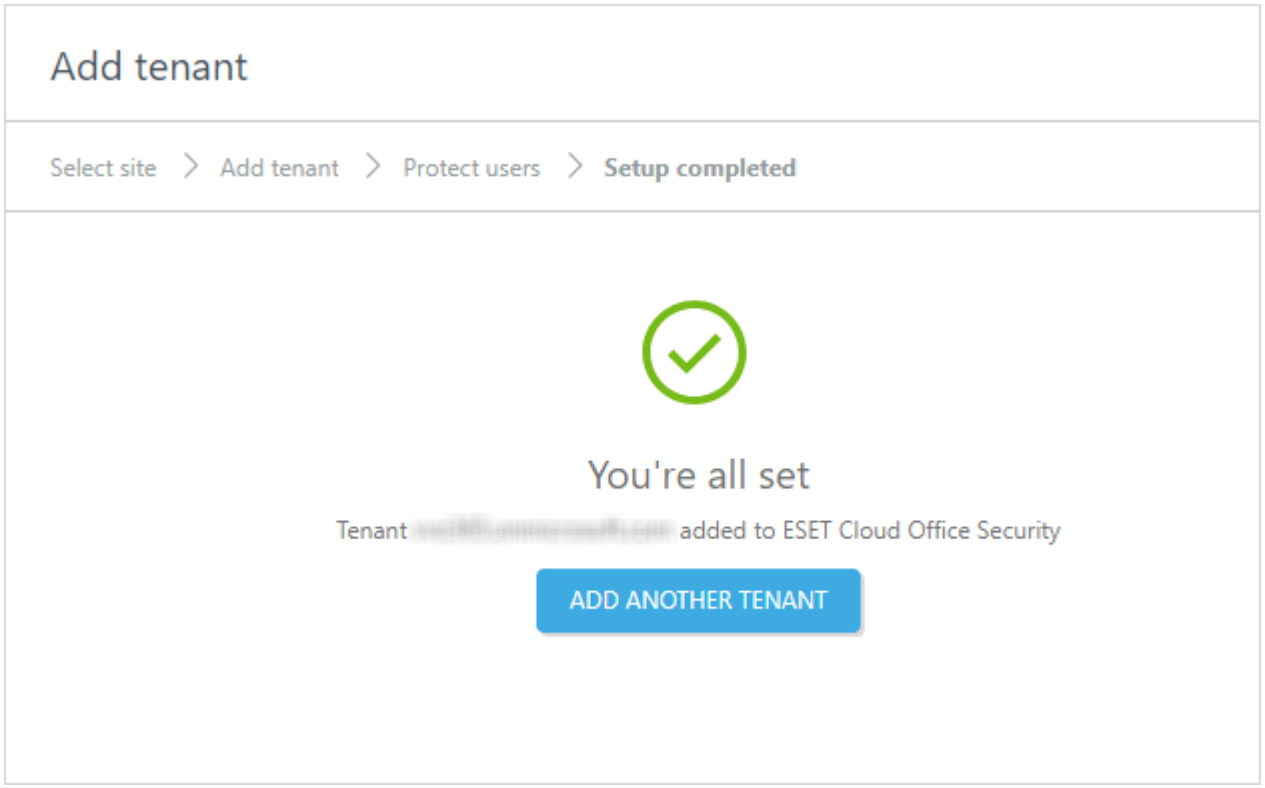


7. Po zakończeniu działania aplikacji ESET Cloud Office Security wróć do konsoli ESET Cloud Office Security. Kliknij **Podaj konto Google i dodaj dzierżawę**, aby zweryfikować własność i kontynuować.

8. Dodano dzierżawę Google Workspace wraz z użytkownikami.



9. Aby zakończyć konfigurację, kliknij przycisk **Dalej** i wybierz użytkowników do **ochrony**. W takim razie wszystko gotowe.

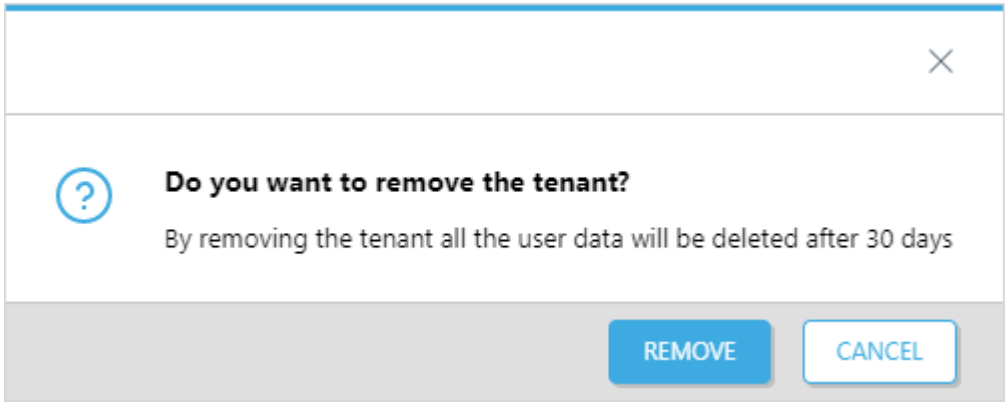


Usuń dzierżawcę z ESET Cloud Office Security

1. Wybierz **Ustawienia**.

2. Wybierz odpowiednią dzierżawę i kliknij przycisk **Usuń**.

3. Okno powiadomienia zawiera ostrzeżenie, że ten proces usunie dane zgodnie z opisem w Polityce dotyczącej ograniczeń i przechowywania danych, a użytkownicy utracą ochronę. Kliknij przycisk **Usuń**, aby potwierdzić usunięcie.



Po usunięciu dzierżawy z konsoli ESET Cloud Office Security okres przechowywania danych dzierżawy wynosi 30 dni (Kwarantanna, Dzienniki skanowania i Statystyki są usuwane po 30 dniach). Jeśli dodasz dzierżawcę ponownie w ciągu 30 dni, wszystkie dane zostaną przywrócone. Inne obiekty (dzierżawcy, użytkownicy, grupy, witryny, raporty, zasady) są trwale usuwane po 90 dniach. Aby uzyskać więcej informacji, zapoznaj się z Polityką dotyczącą ograniczeń i przechowywania danych.

Usuń ESET Cloud Office Security z portalu Azure

1. Zaloguj się do portalu Azure przy użyciu konta administratora.

Aby usunąć aplikację, musisz figurować jako jej właściciel lub mieć uprawnienia administracyjne.

2. Przejdź do usługi **Azure Active Directory** i wybierz pozycję **Aplikacje przedsiębiorstwa**.

3. Znajdź i wybierz aplikację **ESET Cloud Office Security** na stronie przeglądu, przejdź do **Właściwości** i kliknij **Usuń**.

Poruszanie się po ESET Cloud Office Security

Zobacz, jak poruszać się po interfejsie ESET Cloud Office Security. Wkrótce możesz zapoznać się z elementami nawigacyjnymi i narzędziami w ramach ESET Cloud Office Security, które mają być intuicyjne i łatwe w użyciu, a jednocześnie interaktywne.

Użyj paska nawigacyjnego po lewej stronie, aby przełączać się między różnymi częściami konsoli ESET Cloud Office Security:

- Użytkownicy
- Zespoły i witryny
- Wykrycia
- Kwarantanna
- Dzienniki skanowania
- Raporty
- Polityki
- Zarządzanie licencjami
- Dziennik audytu
- Ustawienia

Zwiń – Rozwiń i zwiń menu nawigacji. Zwinięcie panelu zapewni więcej miejsca na ekranie panelu kontrolnego. Aby rozwinąć panel kontrolny, kliknij ikonę .

Pasek narzędzi u góry jest dostępny przez cały czas:



Nawigator produktu — szybki dostęp do konsol ESET i innych przydatnych łączy. (Możesz zobaczyć odpowiednie produkty na podstawie licencji i praw dostępu).

ESET Business Account oraz **ESET MSP Administrator** (konto z licencją hybrydową) — jeśli masz ten sam adres e-mail zarejestrowany dla kont ESET MSP Administrator i ESET Business Account (logowanie jednokrotne), możesz przełączać się między widokami kont ESET Business Account i ESET MSP Administrator.

Wyświetl powiadomienia — Aby wyświetlić powiadomienia, kliknij ikonę dzwonka na górnym pasku.

Szybkie łącza — Zapewnia łatwy dostęp do opcji Dodaj dzierżawę, Nowa polityka, ESET Business Account lub ESET MSP Administrator.

Pomoc — Pierwsze łącze w tym menu zawsze prowadzi do Pomocy online dotyczącej bieżącego ekranu. Jeśli nie możesz rozwiązać problemu, przeszukaj bazę wiedzy ESET lub forum pomocy technicznej. Alternatywnie można przesłać opinię lub **przesłać próbkę do analizy**. Otwórz stronę Informacje, która zawiera szczegółowe informacje o wersji ESET Cloud Office Security i łącza do dokumentów prawnych.

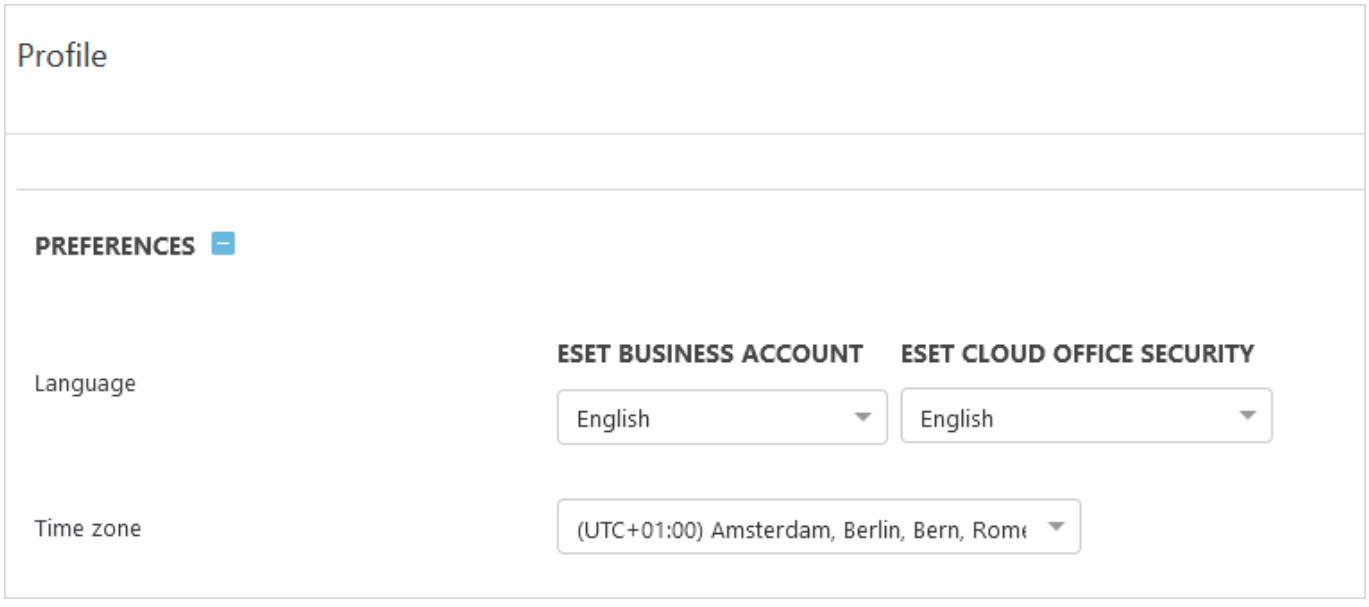
Użytkownik (aktualnie zalogowany) – Pokazuje nazwę użytkownika. Kliknij **Set theme** (Ustaw motyw) i wybierz żądany motyw z menu rozwijanego:

- **Default (light) theme** (Domyślny motyw (jasny) — ESET Cloud Office Security będzie używać jasnego schematu kolorów (standard).
- **Ciemny motyw** — ESET Cloud Office Security będzie używać ciemnego schematu kolorów (tryb ciemny).
- **Operating system theme** (Motyw systemu operacyjnego) — schemat kolorów ESET Cloud Office Security zależy od ustawień systemu operacyjnego.

Wyloguj — Kliknij tę stale widoczną ikonę, aby zamknąć konsolę ESET Cloud Office Security.

Zmień język dla portalu ESET Cloud Office Security

Zaloguj się do konta ESET Business Account lub ESET MSP Administrator, przejdź do sekcji **Zarządzanie użytkownikami** i wybierz pozycję **Edytuj** użytkownika. Poszukaj ustawienia języka dla ESET Cloud Office Security, a następnie zmień język na preferowany i kliknij **Zapisz** przed opuszczeniem ekranu **Profil**.



ESET LiveGuard Advanced

ESET LiveGuard Advanced zapewnia kolejną warstwę zabezpieczeń, wykorzystując zaawansowaną technologię opartą na chmurze ESET do wykrywania nowych, nieznanych wcześniej typów zagrożeń. ESET LiveGuard Advanced zapewnia korzyści w postaci ochrony przed możliwymi konsekwencjami spowodowanymi nowymi zagrożeniami. Gdy rozwiązanie ESET LiveGuard Advanced wykryje podejrzany kod lub podejrzaną aktywność, zapobiega dalszej aktywności zagrożenia, tymczasowo umieszczając je w kwarantannie.

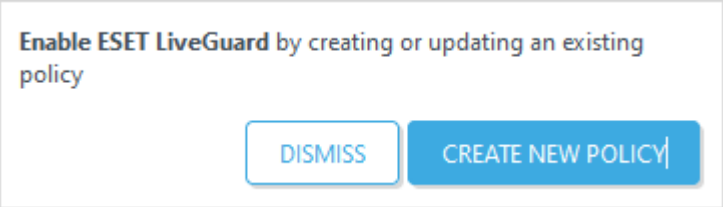
Podejrzana próbka (plik lub wiadomość e-mail) jest automatycznie przesyłana do chmury ESET, gdzie serwer ESET LiveGuard Advanced analizuje ją przy użyciu najnowocześniejszych silników detekcji szkodliwego oprogramowania. Podczas gdy pliki lub wiadomości e-mail są w kwarantannie, program ESET Cloud Office Security czeka na wyniki z serwera ESET LiveGuard Advanced.

Po ukończeniu analizy program ESET Cloud Office Security odbiera raport z podsumowaniem działania przeanalizowanej próbki. Jeśli próbka okaże się nieszkodliwa, zostanie zwolniona z kwarantanny. W przeciwnym razie zostanie zatrzymana w kwarantannie.

W przypadku wiadomości e-mail wyniki z serwera ESET LiveGuard Advanced dla próbek zwykle docierają w ciągu kilku minut. Domyślny interwał oczekiwania jest ustawiony na 5 minut. W rzadkich przypadkach, gdy wyniki z serwera ESET LiveGuard Advanced nie dotrą w czasie zdefiniowanym interwałem, wiadomość jest zwalniana z kwarantanny. Interwał można zmienić na preferowany przez użytkownika (w zakresie od 5 do 60 minut, w odstępach 1-minutowych).

Licencja programu ESET Cloud Office Security umożliwia korzystanie z funkcji ESET LiveGuard Advanced bez dodatkowych opłat. Zobaczysz etykietę ELG obok identyfikatora licencji w obszarze Zarządzanie licencjami.

Gdy pojawi się małe wyskakujące okienko, możesz aktywować usługę ESET LiveGuard Advanced, tworząc nową politykę lub aktualizując istniejącą.



Aby uzyskać bardziej szczegółowe informacje na temat usługi ESET LiveGuard Advanced, zobacz temat Jak działają warstwy wykrywania ESET LiveGuard Advanced .

Panel kontrolny

Panel kontrolny to zbiór widżetów, które zapewniają przegląd działań związanych z zabezpieczeniami usługi Microsoft 365. Panel kontrolny zawiera podstawowe informacje w każdej z kart przeglądowych (Przegląd, Exchange Online, OneDrive, grupy zespołów, witryn SharePoint, Gmail, Google Drive oraz ESET LiveGuard Advanced). **Przegląd** to główny ekran panelu kontrolnego, który jest wyświetlany przy każdym logowaniu do konsoli ESET Cloud Office Security. Wyświetla informacje ogólne i statystyczne.

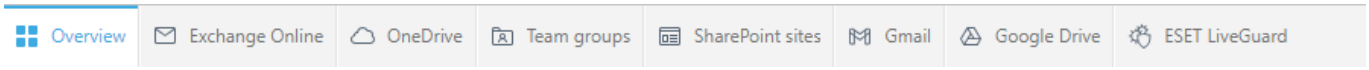
> Zawartość panelu jest odświeżana co 10 minut. Jeśli nie widzisz najnowszych informacji w panelu kontrolnym, naciśnij klawisz **F5**, aby odświeżyć je ręcznie.

Aby wyświetlić statystyki panelu kontrolnego, użyj filtrów u góry i wybierz odpowiedni **Okres** (Ostatnie 24

godziny, Ostatnie 7, 30 lub 90 dni) i **Dzierżawę**. Dodatkowe statystyki i wykresy dotyczące wykryć są widoczne na stronach usług **Exchange Online**, **OneDrive**, **grup zespołów** i **witryn SharePoint**, **Gmail**, **Google Drive** oraz na kartach przeglądu **ESET LiveGuard Advanced**. Są to statystyki przedstawiające liczbę zeskanowanych wiadomości e-mail i plików oraz ilość wykrytego spamu/prób wyłudzenia informacji/szkodliwego oprogramowania. Wykresy przedstawiają ruch dla każdego typu wykrywania — spamu, szkodliwego oprogramowania i wyłudzania informacji.

Od czasu do czasu może pojawić się pasek anonsu. Kolory wskazują typ anonsu (niebieski = informacyjny, żółty = uświadamiający, czerwony = ostrzegawczy).

Użyj zakładek panelu kontrolnego, aby przełączać między oknami widoku.



Omówienie

pokazuje
- liczbę dzierżaw i wykorzystywanych licencji
- statystyki dla każdej dzierżawy:
  - Całkowita liczba użytkowników / Użytkownicy niechronieni
  - Najwięksi odbiorcy spamu / ataków typu „phishing” / szkodliwego oprogramowania
  - Konta OneDrive z największą ilością podejrzanych akcji
  - Zespoły z największą ilością podejrzanych elementów
  - Witryny programu SharePoint z największą liczbą podejrzanych elementów

przechodzenie do szczegółów
- kliknij kafelek Całkowita liczba użytkowników, aby otworzyć sekcję Użytkownicy
- kliknij użytkownika w sekcji statystyk (spam/phishing/szkodliwe oprogramowanie/OneDrive), aby wyświetlić odpowiednie Wykrycia, lub kliknij grupę lub witrynę, aby wyświetlić wykrycia i szczegóły dotyczące podejrzanej grupy zespołu lub witryny programu SharePoint.

Exchange Online

wyświetla
- łączna liczba przeskanowanych wiadomości e-mail
- statystyki wykrytego spamu, szkodliwego oprogramowania i wiadomości e-mail z próbami wyłudzeń informacji
- wykresy przedstawiające ruch spamu, szkodliwego oprogramowania i prób wyłudzeń informacji

Kafelki są interaktywne. Kliknij interesujący Cię kafelek i przejdź do odpowiedniej sekcji w konsoli ESET Cloud Office Security. Na przykład: zostanie otwarta sekcja Dzienniki skanowania z odpowiednimi zapisami dziennika.

Onedrive

wyświetla
- liczbę chronionych użytkowników
- łączną liczbę przeskanowanych plików
- statystyki dotyczące wykrytego szkodliwego oprogramowania
- wykres reprezentujący ruch szkodliwego oprogramowania

Kafelki są interaktywne. Kliknij interesujący Cię kafelek i przejdź do odpowiedniej sekcji w konsoli ESET Cloud Office Security. Na przykład: zostanie otwarta sekcja Dzienniki skanowania z odpowiednimi zapisami dziennika.

Grupy zespołu

wyświetla
- liczbę chronionych grup
- łączną liczbę przeskanowanych plików
- statystyki dotyczące wykrytego szkodliwego oprogramowania
- wykres reprezentujący ruch szkodliwego oprogramowania

Kafelki są interaktywne. Kliknij interesujący Cię kafelek i przejdź do odpowiedniej sekcji w konsoli ESET Cloud Office Security. Na przykład: zostanie otwarta sekcja Dzienniki skanowania z odpowiednimi zapisami dziennika.

 Lokacje SharePoint

wyświetla
- liczbę chronionych stron
- łączną liczbę przeskanowanych plików
- statystyki dotyczące wykrytego szkodliwego oprogramowania
- wykres reprezentujący ruch szkodliwego oprogramowania

Kafelki są interaktywne. Kliknij interesujący Cię kafelek i przejdź do odpowiedniej sekcji w konsoli ESET Cloud Office Security. Na przykład: zostanie otwarta sekcja Dzienniki skanowania z odpowiednimi zapisami dziennika.

 Gmail

wyświetla
- łączna liczba przeskanowanych wiadomości e-mail
- statystyki wykrytego spamu, szkodliwego oprogramowania i wiadomości e-mail z próbami wyłudzeń informacji
- wykresy przedstawiające ruch spamu, szkodliwego oprogramowania i prób wyłudzeń informacji

Kafelki są interaktywne. Kliknij interesujący Cię kafelek i przejdź do odpowiedniej sekcji w konsoli ESET Cloud Office Security. Na przykład: zostanie otwarta sekcja Dzienniki skanowania z odpowiednimi zapisami dziennika.

 Dysk Google

wyświetla
- liczbę chronionych użytkowników
- łączną liczbę przeskanowanych plików
- statystyki dotyczące wykrytego szkodliwego oprogramowania
- wykres reprezentujący ruch szkodliwego oprogramowania

Kafelki są interaktywne. Kliknij interesujący Cię kafelek i przejdź do odpowiedniej sekcji w konsoli ESET Cloud Office Security. Na przykład: zostanie otwarta sekcja Dzienniki skanowania z odpowiednimi zapisami dziennika.

 ESET LiveGuard Advanced

wyświetla
- przesłane pliki (liczba obejmuje duplikaty i ta liczba może być wyższa niż liczba unikatowych plików)
- liczba wykrytych wystąpień
- średni czas analizy
- wykres przedstawiający przesłane pliki
- właściciele z największą liczbą przesłanych plików
- typy przesłanych plików

Kafelki są interaktywne. Kliknij interesujący Cię kafelek i przejdź do odpowiedniej sekcji w konsoli ESET Cloud Office Security. Na przykład: zostanie otwarta sekcja Dzienniki skanowania z odpowiednimi zapisami dziennika.

Użytkownicy

Centralnym elementem chronionym przez ESET Cloud Office Security jest konto użytkownika. Dwukrotnie kliknij użytkownika, aby znaleźć przydatne informacje, takie jak Przegląd, Ustawienia zdefiniowane przez polityki, Lista polityk przypisanych do użytkownika oraz Wykrycia w usługach Gmail, Google Drive, Exchange Online i OneDrive.

Możesz również wybrać, którzy użytkownicy będą chronieni, a którzy nie. Użytkownicy są sortowani w grupy, z których każda jest dzierżawą usługi Microsoft 365 zawierającą jej użytkowników. Aby ułatwić sobie wyszukiwanie określonego użytkownika w grupie, można użyć filtrowania z wieloma kryteriami.

> Użytkownicy bez licencji usługi Microsoft 365 nie będą domyślnie wyświetlani w konsoli ESET Cloud Office Security. Obejmuje to skrzynki współużytkowane bez licencji usługi Microsoft 365.
> Jeśli chcesz zobaczyć wszystkich użytkowników usługi Microsoft 365 i zarządzać nimi, przejdź do pozycji Ustawienia i wyłącz opcję Użytkownicy posiadający licencję Microsoft 365.

Stan ochrony:

Stan	Opis
Brak ochrony	Użytkownik nie jest obecnie chroniony
Automatyczna ochrona	Chroniony użytkownik z automatyczną ochroną.
Oczekujący	Stan przejściowy, który występuje podczas procesu ochrony użytkownika. Po jego zakończeniu stan użytkownika zmieni się na Chroniony.
Pod ochroną	Skrzynka pocztowa użytkownika i usługa OneDrive są chronione przez domyślne lub niestandardowe polityki.
OSTRZEŻENIE	Proces ochrony użytkownika nie powiódł się. Mógł wystąpić błąd zasobów, skrzynki pocztowej lub usługi OneDrive. Jest prawdopodobne, że oba zasoby nie są dostępne dla użytkownika. Sprawdź, czy użytkownik ma przypisaną prawidłową licencję usługi Microsoft 365.

Nawiguj po drzewie, aby wyświetlić użytkowników określonej dzierżawy lub grupy. Aby wyświetlić wszystkich użytkowników w każdej dzierżawie i grupie, kliknij przycisk **Wszystkie**.

Aby uzyskać szczegółowe informacje, kliknij dwukrotnie użytkownika lub kliknij ikonę i wybierz (**Pokaż szczegóły**, **Chroń** lub **Przestań chronić**). Kliknij użytkownika, aby otworzyć okno **Pokaż szczegóły**, które składa się z czterech części:

Czynność	Sposób użycia
Omówienie	Zawiera podstawowe informacje o użytkowniku załadowanym z usługi Microsoft 365 (poczta e-mail, przynależność do grupy, stanowisko itp.). Wyświetlany jest również bieżący stan ochrony skrzynki pocztowej i usługi OneDrive.
Konfiguracja	Zawiera listę ustawień tylko do odczytu i przypisane polityki dla tego użytkownika. Przełączaj się między kartami w celu wyświetlenia konfiguracji lub listy przypisanych polityk. W tym miejscu nie można jednak modyfikować ustawień ani przypisywać polityk do użytkowników. Aby to zrobić, przejdź do sekcji Polityki.
Wykrycia	Pokaż wszystkie wykrycia dla tego konta użytkownika w usłudze Gmail, Google Drive, Exchange Online lub OneDrive.
Kwarantanna	Pokaż wszystkie wiadomości e-mail i pliki z kwarantanny przechowywane dla tego użytkownika. Możesz również wykonać akcję: Zwolnij, Pobierz lub Usuń e-maile lub pliki kwarantanny.

Możliwe jest filtrowanie użytkowników według kilku kryteriów. Kliknij **Dodaj filtr** i wybierz typ filtra z menu rozwijanego lub wprowadź ciąg (powtórz czynność podczas łączenia wielu kryteriów):

Dodaj filtr	Sposób użycia
Stan ochrony	Wybierz stan użytkownika Chroniony, Niechroniony, Ostrzeżenie lub Oczekujący.
Automatyczna ochrona	Pokaż tylko automatycznie chronionych użytkowników.
Nazwa	Wpisz prawidłową nazwę użytkownika.

Dodaj filtr	Sposób użycia
E-mail	Wpisz prawidłowy adres e-mail użytkownika.
Typ	Wybierz typ użytkownika (Nieznany, Użytkownik, Połączony, Udostępniona skrzynka pocztowa, Pokój, Sprzęt, Inne).

Chroń użytkowników

1. Wybierz **użytkowników**, którzy będą chronieni, a następnie kliknij przycisk **Chroń**.
2. Wybierz **pulę licencji** załadowaną z ESET Business Account i kliknij przycisk **OK**. Wybrani użytkownicy są teraz chronieni przez politykę domyślną.
3. W razie potrzeby określ niestandardowe polityki dla użytkowników w sekcji Polityki.

Wyłącz ochronę użytkowników

Wybierz **użytkowników**, którzy nie będą chronieni, a następnie kliknij przycisk **Przestań chronić**.

Zespoły i lokacje

ESET Cloud Office Security zapewnia ochronę grup zespołu oraz witryn programu SharePoint.

Przełączaj się między kartami grup zespołu i witryn programu SharePoint. Wyświetlona zostanie lista grup zespołu lub witryn programu SharePoint dla każdej dzierżawy.

Grupy zespołu

wyświetla obiekty grupowe w usłudze Microsoft 365, w tym domyślną witrynę SharePoint zespołu i zawartość OneDrive:

- nazwa
- status
- wiadomość e-mail
- dzierżawa

Aby chronić grupy zespołu, pamiętaj że co najmniej jeden członek musi być chroniony przez ESET Cloud Office Security. Każda grupa w usłudze Microsoft 365 ma domyślną witrynę SharePoint zespołu i usługę OneDrive, które również są chronione.

Lokacje SharePoint

wyświetla wszystkie witryny główne SharePoint niezwiązane z grupą w usłudze Microsoft 365:

- nazwa
- status
- Adres URL
- dzierżawa

Witryny SharePoint są chronione automatycznie, podobnie jak witryny podrzędne (niepokazane)

Aby uzyskać bardziej szczegółowe informacje, kliknij grupę zespołu lub witrynę programu SharePoint, aby otworzyć okno **Pokaż szczegóły**, które składa się z czterech części:

Czynność	Sposób użycia
Omówienie	Pokazuje niezbędne informacje na temat grup zespołu lub witryn programu SharePoint załadowanych z usługi Microsoft 365 (poczta e-mail, właściciel, członkowie, autor, adres URL itp.). Ponadto wyświetlany jest bieżący stan ochrony dla grupy zespołu lub witryny programu SharePoint.
Konfiguracja	Zawiera listę ustawień tylko do odczytu i przypisane polityki. Przełączaj się między kartami w celu wyświetlenia konfiguracji lub listy przypisanych polityk. W tym miejscu nie można jednak modyfikować ustawień ani przypisywać polityk. Aby to zrobić, przejdź do sekcji Polityki.
Wykrycia	Pokaż wszystkie wykrycia dla grupy zespołu lub witryny programu SharePoint.
Kwarantanna	Pokaż wszystkie pliki poddane kwarantannie. Możesz również wykonać akcję: Zwolnij, Pobierz lub Usuń pliki poddane kwarantannie.

Kliknij pozycję **Dodaj filtr**, aby zastosować filtr dla grup zespołu lub witryn programu SharePoint.

Wykrycia

Wyświetla listę wszystkich wykryć według ESET Cloud Office Security. Przełączaj się między kartami usług Gmail, Google Drive, Exchange Online i OneDrive, grup zespołu oraz witryn programu SharePoint. Wyświetlaj informacje dotyczące poszczególnych wykryć. Na przykład wykryte pliki, które zostały przekazane do grupy zespołu, będą wyświetlane na karcie Grupy zespołu.

Kliknij ikonę , aby otworzyć pasek boczny z podsumowaniem określonych zapisów dziennika (wykryć). Aby uzyskać szczegółowe informacje, kliknij ikonę i wybierz pozycję **Pokaż szczegóły**.

Nawiguj po drzewie, aby wyświetlić wykrycia tylko dla określonej dzierżawy lub grupy. Aby wyświetlić wszystkie wykrycia w każdej dzierżawie i grupie, kliknij przycisk **Wszystkie**. Aby ułatwić sobie wyszukiwanie określonego wykrycia, można zastosować filtrowanie przy użyciu wielu kryteriów. Kliknij **Dodaj filtr** i wybierz typ filtra z menu rozwijanego lub wprowadź ciąg (powtórz podczas łączenia kryteriów):

Dodaj filtr	Sposób użycia
Wystąpienie od	Określ zakres „data od”.
Wystąpienie do	Określ zakres „daty do”.
Temat	Reguła jest stosowana do wiadomości, które zawierają w temacie określony tekst (lub wyrażenie regularne) albo go nie zawierają.
ID komunikatu	Filtruj wiadomości e-mail według unikalnego identyfikatora wiadomości podczas wyszukiwania określonej wiadomości, szczególnie w przypadku dużych dzienników z wieloma wiadomościami lub wieloma próbami dostarczenia.
Nadawca	Filtrowanie wiadomości według określonego nadawcy.
Adresat	Filtrowanie wiadomości według adresatów.
Skrzynka pocztowa	Reguła jest stosowana do wiadomości znajdujących się w określonej skrzynce pocztowej.
Wynik skanowania	Należy wybrać jedną z następujących opcji: Szkodliwe oprogramowanie, Szkodliwe oprogramowanie (wykryte przez ESET LiveGuard Advanced), phishing lub spam.
Czynność	Wybierz jedną z dostępnych czynności.
Zespół	Wpisz prawidłową nazwę zespołu.
Lokacja	Wpisz prawidłową nazwę lokacji.

Dodaj filtr	Sposób użycia
Obiekt	Wpisz prawidłową nazwę obiektu.
Wykrycie	Wpisz prawidłową nazwę wykrycia.
Skrót	Wpisz prawidłowy skrót wykrycia.

Po kliknięciu ikony opcja **Usuń z białej listy** będzie dostępna, jeśli wcześniej dodano do białej listy podobny obiekt, który opuścił kwarantannę tego samego użytkownika. Użyj tej opcji, aby usunąć plik z białej listy. W przyszłości wszystkie takie pliki zostaną poddane kwarantannie.

Okres przechowywania wykryć wynosi 90 dni. Wykrycia starsze niż 90 dni zostaną usunięte na stałe.

Raport fałszywie dodatni (false positive) / fałszywie ujemny (false negative)

Wykrycia FP i FN można ręcznie zgłosić jako spam, phishing lub szkodliwe oprogramowanie, wysyłając próbkę do laboratoriów firmy ESET w celu analizy. Adresy e-mail, na które można wysłać próbki:

Spam - wyślij wiadomość e-mail na adres nospam_ecos@eset.com w przypadku wiadomości e-mail nieprawidłowo oznaczonych jako spam lub na adres spam_ecos@eset.com w przypadku niewykrytego spamu, dołączając oryginalną wiadomość e-mail jako załącznik w formacie *.eml* lub *.msg*.

Phishing - aby zgłosić wykrycia false positive lub false negative phishingu, wyślij nową wiadomość e-mail na adres samples@eset.com, wpisując w temacie *'phishing email'* i dołączając wiadomość wyłudzającą informacje jako załącznik w formacie *.eml* lub *.msg*.

Szkodliwe oprogramowanie - aby zgłosić wykrycia false positive lub false negative szkodliwego oprogramowania, wyślij nową wiadomość e-mail na adres samples@eset.com, wpisując w temacie *'False positive'* lub *'Suspected infection'* i dołączając pliki skompresowane do formatu *.zip* lub *.rar*.

Raporty

Raporty ESET Cloud Office Security zapewniają Ci stały przegląd statystyk ochrony przez ESET Cloud Office Security. Możesz wybrać jeden z dwóch typów raportów: Raporty statystyczne lub Raporty kwarantanny poczty.

Raporty statystyczne zawierają informacje na temat ochrony Gmail, Google Drive, Exchange Online, OneDrive, grup zespołu i witryn programu SharePoint oraz liczbę przeskanowanych wiadomości e-mail, plików, wykrytego szkodliwego oprogramowania, ataków typu „phishing” i spamu w określonym przedziale czasu. Raporty mogą być generowane ręcznie i pobierane w formacie *PDF* lub *CSV* oraz planowane i dostarczane do wybranych odbiorców za pośrednictwem poczty elektronicznej. Format wyjściowy *PDF* przedstawia dane w postaci wykresu, pokazuje długoterminową średnią dla porównania, a także obejmuje informacje o ruchu dla każdego typu ochrony i głównych adresatów szkodliwego oprogramowania, phishingu i spamu.

Raport kwarantanny poczty zawiera listę nowo poddanych kwarantannie obiektów. Raport jest dostarczany do wybranych odbiorców za pośrednictwem poczty e-mail. Odbiorcy mogą zwalniać wiadomości spamowe z kwarantanny (jeśli zostaną uznane za bezpieczne lub uzasadnione), klikając link **Zwolnij**. Dotyczy tylko spamu; inne typy obiektów poddanych kwarantannie nie mogą zostać zwolnione.

Możesz mieć dostęp do statystyk za pośrednictwem poczty e-mail; nie musisz logować się do konsoli ESET Cloud Office Security. Możesz skonfigurować i zaplanować raporty cykliczne oraz określić adresatów wiadomości e-mail. Ponadto możesz natychmiast wygenerować statystyki raportu z poziomu konsoli ESET Cloud Office Security. Wybierz istniejący raport (może to być również raport zaplanowany) i kliknij przycisk **Wygeneruj i pobierz**. Możesz

też kliknąć prawym przyciskiem myszy i użyć menu rozwijanego. Możesz łatwo utworzyć nowy szablon raportu z ustawieniami niestandardowymi.

Nowa raport

Kliknij opcję Nowa raport, aby otworzyć kreatora szablonów raportów i określić niestandardowe ustawienia. Wpisz nazwę i opis raportu.

Język

Wybierz żądany język z menu rozwijanego. Raport zostanie wygenerowany w wybranym języku.

Typ

Wybierz dane, które chcesz uwzględnić w statystykach.

Raporty statystyczne

Utwórz raport zaplanowany lub na żądanie, zawierający informacje zgodnie z wybranymi opcjami.

Raporty kwarantanny poczty

Aby poinformować użytkowników o ich nowych wiadomościach e-mail objętych kwarantanną, wyślij wiadomości e-mail z powiadomieniami do wybranych użytkowników. Można przypisać jednego lub wielu odbiorców lub grupę. Wybierz interwał dla raportów oraz datę i godzinę rozpoczęcia. Jeśli jest to raport powtarzany, wybierz, kiedy powtarzanie ma się zakończyć (w konkretnym dniu, po kilku wystąpieniach lub nigdy). Raport kwarantanny poczty jest wyzwalany tylko wtedy, gdy pojawiają się nowe elementy. Odbiorcy raportu mogą zwalniać wiadomości spamowe z kwarantanny (jeśli zostaną uznane za bezpieczne lub uzasadnione), klikając link Zwolnij (w przeglądarce internetowej zostanie otwarte okno potwierdzenia). Wiadomość spamowa zwolniona z kwarantanny jest dostarczana w osobnej wiadomości e-mail jako załącznik.

Dzierżawa

Ta opcja jest dostępna dla środowiska z wieloma dzierżawami. Można wybrać wiele dzierżaw, dla których mają być generowane statystyki. Raport zostanie wygenerowany dla każdej dzierżawy oddzielnie i zostanie dostarczony w jednej wiadomości e-mail z produktu ESET Cloud Office Security z raportem w postaci wielu załączników.

Okres

Zdefiniuj okres wyświetlania wyników (ostatnie 24 godziny, tydzień, miesiąc). Po wybraniu opcji Niestandardowy możesz określić zakres (Data od i Data do).

Wyniki

Wybierz odpowiedni format pliku. Można wybrać *PDF* lub *CSV*. W przypadku formatu *PDF* będą dostępne wykresy. Z kolei format *CSV* zawiera surowe dane. Raporty będą zbierane zgodnie z określonymi opcjami. Jeśli wybrano dane usługi (Exchange Online, usługi OneDrive, grupy zespołu oraz witryny SharePoint, Gmail, Google Drive), plik wyjściowy będzie miał postać archiwum w formacie ZIP zawierającym pliki raportów w formacie *PDF* lub *CSV*.

Produkt sprzedawany pod marką dystrybutora

Jeśli chcesz, aby logo firmy pojawiały się w raporcie, włącz tę funkcję. Możesz wybrać nagłówek raportu pod wspólną marką przedstawiający Twoje logo wraz z logo ESET lub zawierający tylko Twoje logo. Prześlij logo w

formacie *PNG* lub *JPEG*.

Zaplanowane

Użyj harmonogramu, aby raporty były generowane w określonym dniu i godzinie, również jako zdarzenie cykliczne. Zaplanowane raporty są dostarczane do wybranych odbiorców, którzy otrzymują wiadomość e-mail z raportami z produktu ESET Cloud Office Security w postaci załączników.

Powtórz

Wybierz, czy raport ma być generowany raz czy wielokrotnie:

- **Raz** — raport zostanie wygenerowany tylko raz.
- **Codziennie** — raport będzie generowany i dostarczany wielokrotnie, każdego dnia (chyba że wybierzesz ustawienie ponawiania o nazwie koniec po wystąpieniach).
- **Co tydzień** — raport będzie generowany i dostarczany wielokrotnie, w wybranym dniu tygodnia.
- **Co miesiąc** — raport będzie generowany i dostarczany raz w miesiącu w wybranym dniu.

Począwszy od

Wybierz datę początkową raportów.

Koniec

Wybierz, kiedy kończy się interwał cyklu.

Odbiorcy

Określ adres e-mail adresata raportu i naciśnij Enter, aby potwierdzić. Powtórz tę czynność, aby dodać wielu adresatów.

Aby uzyskać szczegółowe informacje lub zobaczyć działania, kliknij ikonę i wybierz działanie:

Czynność	Sposób użycia
Pokaż szczegóły	Wyświetla szczegółowe informacje o raporcie.
Wygeneruj & Pobierz	Kliknij pozycję Wygeneruj i pobierz i wybierz format *PDF* lub *CSV*. Format *PDF* zapewnia przedstawienie danych w postaci wykresów, a *CSV* zawiera surowe dane. Raporty będą zbierane zgodnie z określonymi opcjami. Jeśli wybrano dane usługi Exchange Online, usługi OneDrive, grupy zespołu oraz witryny SharePoint, plik wyjściowy będzie miał postać archiwum w formacie *ZIP* zawierającym pliki raportów w formacie PDF lub *CSV*.
Edytuj	Edytuj konfigurację istniejącego raportu.
Usuń	Całkowicie usuń wybrany raport.

Kliknij **Dodaj filtr** i wybierz typ filtra z menu rozwijanego lub wprowadź ciąg (powtórz czynność podczas łączenia wielu kryteriów):

Dodaj filtr	Sposób użycia
Nazwa	Wpisz pełną nazwę raportu lub jej część.
Zaplanowane	Wybierz opcję Nie zaplanowano, Raz, Raz dziennie, Co tydzień lub Co miesiąc.

Dodaj filtr	Sposób użycia
Dane	Wybierz pozycję Exchange Online, OneDrive, grupy zespołu lub witryny programu SharePoint, aby filtrować według danych.

Kwarantanna

Proste zarządzanie obiektami (wiadomościami e-mail i plikami), które zostały poddane kwarantannie przez ESET Cloud Office Security. Przełączaj się między usługami Gmail, Google Drive, Exchange Online i OneDrive, grup zespołu oraz witryn programu SharePoint za pomocą kart. Możesz zobaczyć istotne informacje na temat każdego obiektu.

Kliknij ikonę , aby otworzyć pasek boczny z podsumowaniem określonego obiektu. Aby uzyskać szczegółowe informacje, kliknij ikonę i wybierz pozycję **Pokaż szczegóły**.

Nawiguj po drzewie, aby wyświetlić obiekty tylko dla określonej dzierżawy lub grupy. Aby wyświetlić wszystkie wykrycia w każdej dzierżawie i grupie, kliknij przycisk **Wszystkie**.

Sprawdź wiadomości e-mail lub pliki poddane kwarantannie i podejmij działanie (**Usuń** lub **Zwolnij**). Możesz również **pobrać** oryginalny plik lub archiwum chronione hasłem w formacie *.zip*.

> Jeśli wykrycie zostanie uznane za nieszkodliwe (false positive), można **przywrócić** plik z kwarantanny. Przywrócony plik jest automatycznie umieszczany na białej liście na podstawie skrótu. Wszystkie przyszłe wystąpienia tego samego pliku dla tego samego użytkownika nie zostaną wykryte jako podejrzane i nie zostaną poddane kwarantannie. Automatyczne umieszczanie na białej liście odbywa się odrębnie dla każdego użytkownika. W przypadku innych użytkowników ten sam plik będzie nadal wykrywany jako podejrzany i będzie poddawany kwarantannie.
> Możesz usunąć plik z białej listy Wykrycia, korzystając z opcji **Usuń z białej listy.**

Kliknij ikonę i wybierz działanie:

Czynność	Sposób użycia
Pokaż szczegóły	Wyświetla bardziej szczegółowe informacje o wiadomości e-mail poddanej kwarantannie.
Zwolnij (wiadomości e-mail lub pliki)	Wysyła wiadomość e-mail z powiadomieniem z kwarantanny do pierwotnych adresatów z oryginalną wiadomością jako załącznikiem. W przypadku usługi OneDrive plik zostanie przekazany do jego oryginalnej lokalizacji w usłudze OneDrive użytkownika. Po zwolnieniu z kwarantanny pliku pochodzącego z grupy zespołu lub witryny programu SharePoint plik pojawi się ponownie w pierwotnej lokalizacji. Przywrócony plik jest automatycznie umieszczany na białej liście na podstawie skrótu. Zapobiega to ponownemu poddaniu pliku kwarantannie.
Usuń	Usuwa element z kwarantanny.
Pobierz oryginalny plik	Niechroniony plik zostaje pobrany w oryginalnej postaci.
Pobierz archiwum chronione hasłem	Pobierz chronione archiwum, podając hasło.
Przesyłanie próbek	Okno dialogowe przesyłania próbek umożliwia wysłanie podejrzanego pliku lub spamu do firmy ESET w celu analizy. Wybierz powód przesłania próbki z menu rozwijanego.

Aby ułatwić sobie wyszukiwanie określonego obiektu poddanego kwarantannie, można filtrować elementy przy użyciu wielu kryteriów. Kliknij **Dodaj filtr** i wybierz typ filtra z menu rozwijanego lub wprowadź ciąg (powtórz podczas łączenia kryteriów):

Dodaj filtr	Sposób użycia
Wystąpienie od	Określ zakres „data od”.
Wystąpienie do	Określ zakres „daty do”.
Temat	Reguła jest stosowana do wiadomości, które zawierają w temacie określony tekst (lub wyrażenie regularne) albo go nie zawierają.
ID komunikatu	Filtruj wiadomości e-mail według unikalnego identyfikatora wiadomości podczas wyszukiwania określonej wiadomości, szczególnie w przypadku dużych dzienników z wieloma wiadomościami lub wieloma próbami dostarczenia.
Nadawca	Filtrowanie wiadomości według określonego nadawcy.
Adresat	Filtrowanie wiadomości według adresatów.
Skrzynka pocztowa	Reguła jest stosowana do wiadomości znajdujących się w określonej skrzynce pocztowej.
Wynik skanowania	Należy wybrać jedną z następujących opcji: Szkodliwe oprogramowanie, Szkodliwe oprogramowanie (wykryte przez ESET LiveGuard Advanced), phishing lub spam.
Zespół	Wpisz prawidłową nazwę zespołu.
Obiekt	Wpisz prawidłową nazwę obiektu.
Lokacja	Wpisz prawidłową nazwę lokacji.

Okres przechowywania obiektów poddanych kwarantannie wynosi 30 dni. Obiekty starsze niż 30 dni zostaną trwale usunięte z kwarantanny.

Dzienniki skanowania

Wyświetla listę wszystkich wyników skanowania według ESET Cloud Office Security. Dzienniki są podobne do Wykryć, tyle że w ich przypadku na liście mogą występować także czyste obiekty (włącz w zasadach ustawienie Zapisz wszystkie obiekty). Przełączanie między usługami Gmail, Google Drive, Exchange Online, OneDrive, grupami zespołu, witrynami programu SharePoint i przesłanymi plikami za pomocą kart. Możesz zobaczyć znaczną ilość informacji dla każdego wykrycia. Przesłane pliki to lista plików wysłanych do ESET LiveGuard Advanced celem analizy.

Kliknij ikonę , aby otworzyć pasek boczny z podsumowaniem określonego zapisu dziennika. Aby uzyskać szczegółowe informacje, kliknij ikonę i wybierz pozycję **Pokaż szczegóły**.

Nawiguj po drzewie, aby wyświetlić zapisy dziennika tylko dla określonej dzierżawy lub grupy. Aby wyświetlić wszystkie wykrycia w każdej dzierżawie i grupie, kliknij przycisk **Wszystkie**.

Jeśli wynik skanowania jest oznaczony jako **Nieskanowane**, przyczyny mogą być różne. Szczegółowe informacje można znaleźć w informacji o ograniczeniach..

Po kliknięciu ikony koła zębatego w prawym górnym rogu, aby uzyskać dostęp do opcji **Eksportuj do CSV** z menu kontekstowego, można wyeksportować siatkę tabeli do formatu *CSV* i użyć jej w innych aplikacjach do pracy z listą.

Aby ułatwić sobie wyszukiwanie określonego zapisu dziennika, można filtrować elementy przy użyciu wielu kryteriów. Kliknij **Dodaj filtr** i wybierz typ filtra z menu rozwijanego lub wprowadź ciąg (powtórz podczas łączenia kryteriów):

Dodaj filtr	Sposób użycia
Wystąpienie od	Określ zakres „data od”.

Dodaj filtr	Sposób użycia
Wystąpienie do	Określ zakres „daty do”.
Źródło danych	Należy wybrać jedną z następujących opcji: Exchange Online, OneDrive, grupa zespołu lub witryna SharePoint.
Skrzynka pocztowa	Reguła jest stosowana do wiadomości znajdujących się w określonej skrzynce pocztowej.
Nadawca	Filtrowanie wiadomości według określonego nadawcy.
Adresat	Filtrowanie wiadomości według adresatów.
Temat	Stosowane do wiadomości, które zawierają w temacie określony tekst albo go nie zawierają.
ID komunikatu	Filtruj wiadomości e-mail według unikalnego identyfikatora wiadomości podczas wyszukiwania określonej wiadomości, szczególnie w przypadku dużych dzienników z wieloma wiadomościami lub wieloma próbami dostarczenia.
Wynik skanowania	Należy wybrać jedną z następujących opcji: Szkodliwe oprogramowanie, szkodliwe oprogramowanie (wykrycia przez ESET LiveGuard Advanced), phishing, spam, wyleczone, nieskanowane, błąd lub wyłączone.
Czynność	Wybierz jedną z dostępnych czynności.
Właściciel	Wpisz prawidłową nazwę właściciela.
Obiekt	Wpisz prawidłową nazwę obiektu.
Wykrycie	Wpisz prawidłową nazwę wykrycia.
Skrót	Wpisz prawidłowy skrót wykrycia.
Zespół	Wpisz prawidłową nazwę zespołu.
Lokacja	Wpisz prawidłową nazwę lokacji.

Istnieje 90-dniowy okres przechowywania rekordów dziennika. Wykrycia starsze niż 90 dni zostaną usunięte na stałe. Przy stosowaniu polityki używającej opcji **Zapisz wszystkie obiekty**, okres przechowywania zapisów dziennika ze stanem **Wyleczone** wynosi 3 dni. Wyleczone wyniki skanowania starsze niż 3 dni zostaną usunięte na stałe.

Polityki

Większe organizacje mają zwykle wiele działów i chcą skonfigurować różne ustawienia ochrony dla każdej jednostki organizacyjnej. ESET Cloud Office Security zapewnia ustawienia ochrony oparte na politykach, które można dostosować i przypisać do wybranych użytkowników, grup użytkowników, dzierżaw, grup zespołu lub witryn programu SharePoint.

Aby dodać kryteria filtrowania, kliknij przycisk **Dodaj filtr** i wybierz odpowiednią **nazwę** elementu i wpisz prawidłową nazwę polityki. Drzewo polityk pokazuje dzierżawy i ich grupy użytkowników, grupy zespołu, witryny programu SharePoint, w tym grupę **Nieprzypisane**, która zawiera polityki niestandardowe, nieprzypisane do żadnego obiektu docelowego.

Można dodać nową politykę lub zmodyfikować istniejącą i jej ustawienia:

1. Kliknij kolejno opcje **Polityki** > **Nowa polityka**.

2. Wpisz **nazwę** i **opis** nowej polityki.

3. Wybierz obiekt docelowy i skonfiguruj politykę dla:

   • **Dzierżawy** – Konfigurowanie ochrony usługi Gmail, Google Drive, Exchange Online, OneDrive, witryn programu SharePoint i grup zespołu oraz przypisywanie jej do wybranych dzierżaw

• **Użytkowników** – konfigurowanie ochrony usługi Gmail, Google Drive, Exchange Online i OneDrive oraz przypisywanie jej do wybranych użytkowników lub grup użytkowników

• **Grupy zespołu** – Konfigurowanie ochrony grup zespołu i przypisywanie jej do wybranych grup

• **Witryny programu SharePoint** – Konfigurowanie ochrony witryn programu SharePoint i przypisywanie jej do wybranych witryn

4. Skonfiguruj ustawienia ochrony w sekcji **Settings** (Ustawienia) dla usługi Exchange Online, Gmail, OneDrive, Google Drive, grup zespołów, witryn programu SharePoint lub ESET LiveGuard Advanced, a następnie kliknij przycisk **Next** (Dalej).

5. Kliknij przycisk **Przypisz** i wybierz obiekt docelowy, do którego zostanie przypisana polityka.

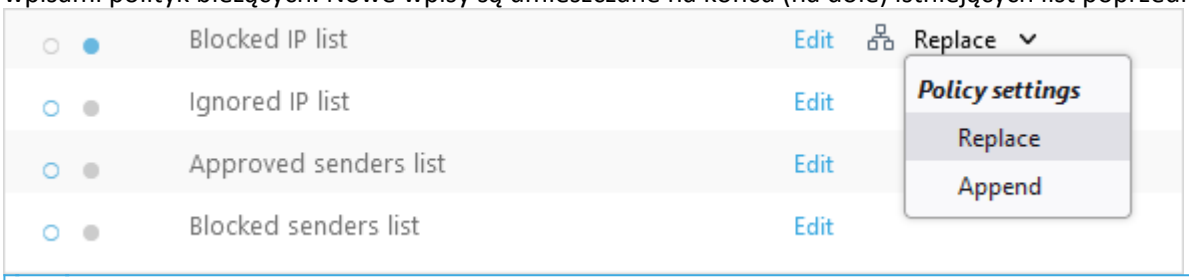
6. Kliknij **Zapisz politykę**, aby zapisać ustawienia polityki.

Zasady polityki

Polityka domyślna • Dotyczy wszystkich użytkowników (chronionych i niechronionych) • Nie może być modyfikowana oraz nie można jej usunąć
Politykę niestandardową można przypisać do: • **Użytkownicy** — dotyczy ręcznie wybranych użytkowników indywidualnych • **Grupy** — dotyczy wszystkich członków grupy użytkowników • **Dzierżawy** — dotyczy wszystkich jednostek w obrębie dzierżawy • **Grupy zespołu** — dotyczy grupy zespołu • **Witryny programu SharePoint** — dotyczy witryny programu SharePoint
Polityki niestandardowe przypisane do **dzierżawy** lub **grupy** są scalane z polityką domyślną. Niestandardowa **polityka dzierżawy**, **polityka grupy**, **polityka grup zespołu** lub **polityka witryn programu SharePoint** ma pierwszeństwo przed polityką domyślną. Polityka niestandardowa przypisana do **użytkownika** jest scalana z polityką **dzierżawy**, **grupy**, **grup zespołu**, **witryn programu SharePoint** i polityką domyślną. Niestandardowe zasady **Użytkownika** mają priorytet nad zasadami dzierżawy lub grupy i zasadami domyślnymi. Jednak gdy użytkownik prześle plik do grupy zespołu lub witryny programu SharePoint, stosowane są polityki dla grupy zespołu lub witryny programu SharePoint.
Użytkownikom i Dzierżawom można przypisać wiele **niestandardowych polityk**, ale obowiązujące polityki są obliczane na podstawie priorytetu (kolejności).

Ustawienia list modułu Anti-Spam podczas scalania polityk

Opcja scalania dotyczy list Anti-Spam i ustawień administratora powiadomień (adresy powiadomień e-mail przez Anti-Malware i Anti-Phishing).
Jeśli masz wiele polityk z listami modułu Anti-Spam (listy adresów IP domen lub adresów e-mail Zatwierdzonych, Zablokowanych i Ignorowanych) lub adresami administratorów ochrony przed szkodliwym oprogramowaniem i phishingiem dla wiadomości e-mail z powiadomieniami, wybierz strategię scalania:
Zamień — zachowaj tylko nowe pozycje listy (opcja domyślna). Nowe wpisy list polityk bieżących zastępują wszystkie listy z poprzednich polityk.
Dołącz — rozszerza listy poprzednich polityk, dodając nowe wpisy. Scal listy z poprzednich polityk z nowymi wpisami polityk bieżących. Nowe wpisy są umieszczane na końcu (na dole) istniejących list poprzednich polityk.



Zanim opcja scalania stała się dostępna, domyślnym zachowaniem było **Zamień**. Jeśli używasz już polityk z określonymi listami modułu ochrony przed spamem, możesz zachować domyślną opcję **Zamień** lub zmienić ją na **Dołącz**, jeśli jest to preferowane.

Utwórz nową politykę ze zdefiniowaną listą modułu Anti-Spam i wybierz opcję scalania (zakładając, że istnieją już polityki z listami modułu Anti-Spam).
1. Kliknij kolejno opcje **Polityki** > **Nowa polityka**.
2. Wpisz **nazwę** i **opis** nowej polityki, wybierz **Dzierżawy** jako obiekt docelowy i kliknij przycisk **Dalej**.
3. Rozwiń menu **Exchange Online — Ochrona przed spamem** i kliknij opcję **Edytuj** obok listy Zablokowane adresy IP.
4. Kliknij opcję **Dodaj**, wpisz adres IP, naciśnij klawisz **Enter**, aby zakończyć działanie (alternatywnie zaimportuj listę z pliku), a następnie kliknij przycisk **Zapisz zmiany**.
5. Wybierz opcję **Dołącz** jako opcję scalania z menu rozwijanego i kliknij przycisk **Dalej**.
6. Kliknij **Przypisz**, z menu rozwijanego wybierz polecenie **Przypisz do dzierżaw**, zaznacz pole wyboru obok dzierżawy i kliknij przycisk **OK**.
7. Kliknij **Zapisz zmiany**, aby zakończyć proces.

Aby zmienić priorytet polityki, kliknij **Zmień kolejność**. Wybierz politykę lub wiele polityk, a następnie kliknij przycisk **Zastosuj wcześniej** lub **Zastosuj później**, aby zmienić ich priorytet. Polityki są stosowane globalnie (niezależnie od przypisania — do dzierżawy, grupy lub użytkownika) w określonej kolejności od góry do dołu. Polityka domyślna jest zawsze stosowana jako pierwsza.

Aby wykonać następujące czynności, wybierz politykę i kliknij ikonę ⋮:

Czynność	Sposób użycia
Pokaż szczegóły	Wyświetlanie szczegółowych informacji o utworzonej polityce, ustawieniach i o tym, do kogo polityki są przypisane.
Edytuj	Zmień konfigurację istniejącej polityki.
Przypisywanie	Wybierz użytkowników, dzierżawy, grupy zespołu oraz witryny programu SharePoint, do których ma zostać przypisana polityka.
Zduplikuj	Utwórz nową politykę na podstawie wybranego szablonu. Dla zduplikowanej polityki konieczne będzie podanie nowej nazwy.
Usuń	Całkowicie usuń zaznaczoną politykę.

Utwórz niestandardowe polityki dzierżawy, aby widzieć wszystkie wyniki skanowania (w tym wyleczone) w Dziennikach skanowania. Polityka dzierżawy ma zastosowanie do wszystkich użytkowników (chronionych i niechronionych).

1. Kliknij kolejno opcje **Polityki** > **Nowa polityka**.
2. Wpisz **nazwę** i **opis** nowej polityki, wybierz **Dzierżawy** jako obiekt docelowy i kliknij przycisk **Dalej**.
3. Rozwiń **Exchange Online — Ogólne** i użyj przełącznika, aby włączyć opcję **Zapisz wszystkie obiekty**.
4. Rozwiń **OneDrive — Ogólne** i użyj przełącznika, aby włączyć opcję **Zapisz wszystkie obiekty**.
5. Rozwiń **Grupy zespołu — Ogólne** i użyj przełącznika, aby włączyć opcję **Zapisz wszystkie obiekty**.
6. Rozwiń **Witryny SharePoint — Ogólne** i użyj przełącznika, aby włączyć opcję **Zapisz wszystkie obiekty**, a następnie kliknij przycisk **Dalej**.
7. Kliknij **Przypisz**, zaznacz pole wyboru obok dzierżawy, a następnie kliknij przycisk **OK**.
8. Kliknij **Zapisz zmiany**, aby zakończyć proces.

Utwórz niestandardowe polityki dla określonych użytkowników z ustawieniami zaawansowanymi, które będą miały wpływ na sposób postępowania ze szkodliwym oprogramowaniem, spamem i wyłudzaniem informacji. Dzięki tym politykom załączniki wiadomości e-mail zawierające szkodliwe oprogramowanie zostaną usunięte, wiadomości spamowe zostaną przeniesione do folderu spam użytkownika, wiadomości e-mail wyłudzające informacje będą oznaczane i poddawane kwarantannie, a zawartość plików złośliwego oprogramowania znajdujących się w usłudze OneDrive zostanie zastąpiona zwykłym tekstem, aby zapobiec wyrządzeniu szkody.

1. Kliknij kolejno opcje **Polityki** > **Nowa polityka**.
2. Wpisz **nazwę** i **opis** nowej polityki, wybierz **Użytkownicy** jako obiekt docelowy i kliknij przycisk **Dalej**.
3. Rozwiń pozycję **Exchange Online — Ochrona przed szkodliwym oprogramowaniem** i użyj menu rozwijanego obok pozycji **Gdy zostaną wykryte elementy**, aby wybrać opcję **Usuń załącznik**.
4. Rozwiń pozycję **Exchange Online — Ochrona przed spamem** i użyj menu rozwijanego obok pozycji **Gdy zostaną wykryte elementy**, aby wybrać pozycję **Przenieś do spamu**.
5. Rozwiń pozycję **Exchange Online — Ochrona przed atakami typu „phishing”** i kliknij przełącznik, aby włączyć opcję **Oznacz wiadomość**. Możesz również zmienić **tekst znacznika**, aby go dostosować.
6. Otwórz rozwijane menu **OneDrive — Ochrona przed szkodliwym oprogramowaniem** obok pozycji **Gdy zostaną wykryte elementy**, aby wybrać opcję **Zamień** i kliknij przycisk **Dalej**.
7. Kliknij opcję **Przypisz**, zaznacz pola wyboru obok użytkowników, do których chcesz zastosować politykę, a następnie kliknij przycisk **OK**. Jeśli użytkownik ma zastosowaną istniejącą politykę niestandardową, zostanie ona nadpisana nową.
8. Kliknij **Zapisz zmiany**, aby zakończyć proces.

Ustawienia ochrony dla usługi Exchange Online

Ta sekcja zawiera informacje o zmianie ogólnych ustawień usługi Exchange Online, ochrony przed szkodliwym oprogramowaniem, spamem lub Anti-Phishing oraz o opcjach.

Exchange Online — Ogólne

ESET LiveGrid®Opinia dotycząca aplikacji
Próbka zostanie przesłana do ESET Research Lab w celu przeprowadzenia dalszej analizy. Przeczytaj więcej o ESET LiveGrid® w glosariuszu .
Zapisuj w dzienniku informacje o wszystkich obiektach
Jeśli ta opcja jest zaznaczona, w Dziennikach skanowania będą widoczne wszystkie wyniki skanowania (w tym wyleczone). Zasady przechowywania wyników czystego skanowania wynoszą trzy dni. Wyniki skanowania starsze niż trzy dni zostaną usunięte na stałe.

Exchange Online — Ochrona przed szkodliwym oprogramowaniem

Włącz ochronę przed szkodliwym oprogramowaniem w Exchange Online
Ta funkcja jest aktywna po włączeniu i można skonfigurować opcje dodatkowe.
Ochrona raportowania i uczenia maszynowego
Zaawansowane uczenie maszynowe jest teraz częścią silnika detekcji jako zaawansowana warstwa ochrony, która poprawia wykrywanie. Przed zmodyfikowaniem progu (lub poziomu) kategorii Raportowanie należy zapoznać się z poniższymi informacjami:
Czynność po wykryciu zagrożenia
• **Brak czynności** — nie jest wykonywana żadna akcja, a wiadomość e-mail jest dostarczana do odbiorcy
• **Przenieś do spamu** — wiadomość e-mail zostanie przeniesiona do folderu Spam.
• **Przenieś do kosza** — wiadomość e-mail zostanie przeniesiona do folderu Kosz.
• **Usuń wiadomość** — wiadomość e-mail zostanie usunięta
• **Quarantine message** (Poddaj wiadomość kwarantannie) — oryginalna wiadomość e-mail zostanie usunięta, a jej kopia będzie przechowywana w kwarantannie. Jeśli zdecydujesz się zwolnić wiadomość e-mail z kwarantanny, zostanie ona wysłana jako załącznik w nowej wiadomości e-mail i dostarczona do odbiorcy.
• **Usuń załącznik** — załącznik do wiadomości zostanie usunięty i wiadomość zostanie dostarczona do adresata bez załącznika.
• **Zastąp załącznik** — powoduje zastąpienie załącznika plikiem tekstowym zawierającym szczegółowe informacje o wykonanej czynności.
• **Poddaj załącznik kwarantannie** — Załącznik zostanie usunięty z wiadomości e-mail i umieszczony w kwarantannie.
Tekst zastępczy załącznika
Powoduje zastąpienie załącznika plikiem tekstowym zawierającym szczegółowe informacje o wykonanej czynności.
Znacznik tematu
Włączenie tej opcji umożliwia modyfikowanie szablonów dołączanych do tematu zainfekowanych wiadomości.
Tekst znacznika tematu
Możesz dodać niestandardowy znacznik do tematów wiadomości, których dotyczy problem.
Powiadamianie właściciela skrzynki pocztowej
Gdy opcja ta jest włączona, w przypadku wykrycia zagrożenia użytkownik otrzyma wiadomość e-mail z powiadomieniem.
Język
Wybierz żądany język z menu rozwijanego. Właściciel skrzynki pocztowej będzie otrzymywać wiadomości e-mail z powiadomieniami w wybranym języku, gdy obiekt zostanie zwolniony z kwarantanny w ramach usługi Exchange Online. Ta opcja zastępuje domyślny język dzierżawy w ustawieniach.
Powiadamianie administratora
Określ adres e-mail (naciśnij Enter, aby dodać wiele adresów), pod którym będą odbierane powiadomienia za każdym razem, gdy zostanie wykryte zagrożenie.

Exchange Online — Ochrona przed spamem

Włącz ochronę przed spamem w Exchange Online
Ta funkcja jest aktywna po włączeniu i można skonfigurować opcje dodatkowe.
Czynność po wykryciu zagrożenia
- **Brak czynności** — nie jest wykonywana żadna akcja, a wiadomość e-mail jest dostarczana do odbiorcy
- **Przenieś do spamu** — wiadomość e-mail zostanie przeniesiona do folderu Spam.
- **Przenieś do kosza** — wiadomość e-mail zostanie przeniesiona do folderu Kosz.
- **Usuń wiadomość** — wiadomość e-mail zostanie usunięta
- **Quarantine message** (Poddaj wiadomość kwarantannie) — oryginalna wiadomość e-mail zostanie usunięta, a jej kopia będzie przechowywana w kwarantannie. Jeśli zdecydujesz się zwolnić wiadomość e-mail z kwarantanny, zostanie ona wysłana jako załącznik w nowej wiadomości e-mail i dostarczona do odbiorcy.

Znacznik tematu
Włączenie tej opcji umożliwia modyfikowanie szablonów dołączanych do tematu zainfekowanych wiadomości.
Tekst znacznika tematu
Możesz dodać niestandardowy znacznik do tematów wiadomości, których dotyczy problem.
Listy elementów **zatwierdzonych**, **zablokowanych** i **ignorowanych** można skonfigurować, określając kryteria, takie jak adres lub zakres adresów IP czy nazwa domeny. Aby dodać, zmodyfikować lub usunąć kryterium, należy kliknąć opcję **Edytuj** obok listy, która ma być zarządzana. W celu zaimportowania listy niestandardowej z pliku (zamiast dodawania pojedynczych wpisów ręcznie) należy kliknąć opcję **Importuj**, a następnie wskazać (*.txt*) plik zawierający wpisy, które mają zostać dodane do listy. Jeśli natomiast konieczne jest wyeksportowanie istniejącej już listy do pliku (*.txt*), należy wybrać z menu kontekstowego opcję **Eksportuj**.

Lista zatwierdzonych adresów IP	Automatycznie dodaje do białej listy wiadomości e-mail pochodzące z określonych adresów IP. Zawartość wiadomości e-mail nie zostanie sprawdzona.
Lista zablokowanych adresów IP	Automatycznie blokuje wiadomości e-mail pochodzące z określonych adresów IP.
Lista ignorowanych adresów IP	Lista adresów IP, które są ignorowane podczas klasyfikacji. Zawartość wiadomości e-mail zostanie sprawdzona.
Lista zatwierdzonych nadawców	Dodaje do białej listy wiadomości e-mail pochodzące od określonego nadawcy lub domeny. Tylko jeden adres nadawcy lub cała domena jest używana do weryfikacji na podstawie następującego priorytetu: 1.Adres połączenia SMTP „MAIL FROM” 2.Pole nagłówka wiadomości e-mail „Return-Path:” 3.Pole nagłówka wiadomości e-mail „X-Env-Sender:” 4.Pole nagłówka wiadomości e-mail „From:” 5.Pole nagłówka wiadomości e-mail „Sender:” 6.Pole nagłówka wiadomości e-mail „X-Apparently-From:”
Lista zablokowanych nadawców	Blokuje wiadomości e-mail pochodzące od określonego nadawcy lub domeny. Wszystkie zidentyfikowane adresy nadawców lub całe domeny są używane do weryfikacji: Adres połączenia SMTP „MAIL FROM” Pole nagłówka wiadomości e-mail „Return-Path:” Pole nagłówka wiadomości e-mail „X-Env-Sender:” Pole nagłówka wiadomości e-mail „From:” Pole nagłówka wiadomości e-mail „Sender:” Pole nagłówka wiadomości e-mail „X-Apparently-From:”

Exchange Online — Ochrona przed atakami typu „phishing”

Włącz Anti-Phishing w Exchange Online
Ta funkcja jest aktywna po włączeniu i można skonfigurować opcje dodatkowe.
Czynność po wykryciu zagrożenia
• **Brak czynności** — nie jest wykonywana żadna czynność, a wiadomość e-mail ze szkodliwym załącznikiem jest dostarczana do odbiorcy.
• **Przenieś do spamu** — wiadomość e-mail zostanie przeniesiona do folderu Spam.
• **Przenieś do kosza** — wiadomość e-mail zostanie przeniesiona do folderu Kosz.
• **Usuń wiadomość** — wiadomość e-mail zostanie usunięta
• **Quarantine message** (Poddaj wiadomość kwarantannie) — oryginalna wiadomość e-mail zostanie usunięta, a jej kopia będzie przechowywana w kwarantannie. Jeśli zdecydujesz się zwolnić wiadomość e-mail z kwarantanny, zostanie ona wysłana jako załącznik w nowej wiadomości e-mail i dostarczona do odbiorcy.
Znacznik tematu
Włączenie tej opcji umożliwia modyfikowanie szablonów dołączanych do tematu zainfekowanych wiadomości.
Tekst znacznika tematu
Możesz dodać niestandardowy znacznik do tematów wiadomości, których dotyczy problem.
Powiadamianie właściciela skrzynki pocztowej
Gdy opcja ta jest włączona, w przypadku wykrycia zagrożenia użytkownik otrzyma wiadomość e-mail z powiadomieniem.
Powiadamianie administratora
Określ adres e-mail (naciśnij Enter, aby dodać wiele adresów), na który będą wysyłane powiadomienia za każdym razem, gdy dla dowolnego użytkownika usługi Exchange Online zostanie wykryte zagrożenie.

Ustawienia ochrony dla Gmail

Ta sekcja zawiera informacje o zmianie ogólnych ustawień usługi Gmail, ochrony przed szkodliwym oprogramowaniem, spamem lub Anti-Phishing oraz o opcjach.

Gmail — ogólne

ESET LiveGrid®Opinia dotycząca aplikacji
Próbka zostanie przesłana do ESET Research Lab w celu przeprowadzenia dalszej analizy. Przeczytaj więcej o ESET LiveGrid® w glosariuszu .
Zapisuj w dzienniku informacje o wszystkich obiektach
Jeśli ta opcja jest zaznaczona, w Dziennikach skanowania będą widoczne wszystkie wyniki skanowania (w tym wyleczone). Zasady przechowywania wyników czystego skanowania wynoszą trzy dni. Wyniki skanowania starsze niż trzy dni zostaną usunięte na stałe.

Ochrona Gmaila przed szkodliwym oprogramowaniem

Włącz Ochronę Gmaila przed szkodliwym oprogramowaniem
Ta funkcja jest aktywna po włączeniu i można skonfigurować opcje dodatkowe.
Ochrona raportowania i uczenia maszynowego
Zaawansowane uczenie maszynowe jest teraz częścią silnika detekcji jako zaawansowana warstwa ochrony, która poprawia wykrywanie. Przed zmodyfikowaniem progu (lub poziomu) kategorii Raportowanie należy zapoznać się z poniższymi informacjami:
Czynność po wykryciu zagrożenia
- **Brak czynności** — nie jest wykonywana żadna akcja, a wiadomość e-mail jest dostarczana do odbiorcy
- **Przenieś do spamu** — wiadomość e-mail zostanie przeniesiona do folderu Spam.
- **Przenieś do kosza** — wiadomość e-mail zostanie przeniesiona do folderu Kosz.
- **Usuń wiadomość** — wiadomość e-mail zostanie usunięta
- **Quarantine message** (Poddaj wiadomość kwarantannie) — oryginalna wiadomość e-mail zostanie usunięta, a jej kopia będzie przechowywana w kwarantannie. Jeśli zdecydujesz się zwolnić wiadomość e-mail z kwarantanny, zostanie ona wysłana jako załącznik w nowej wiadomości e-mail i dostarczona do odbiorcy.
- **Usuń załącznik** — załącznik do wiadomości zostanie usunięty i wiadomość zostanie dostarczona do adresata bez załącznika.
- **Zastąp załącznik** — Powoduje zastąpienie załącznika plikiem tekstowym zawierającym szczegółowe informacje o wykonanej czynności.
- **Poddaj załącznik kwarantannie** — Załącznik zostanie usunięty z wiadomości e-mail i umieszczony w kwarantannie.

Tekst zastępczy załącznika
Powoduje zastąpienie załącznika plikiem tekstowym zawierającym szczegółowe informacje o wykonanej czynności.
Znacznik tematu
Włączenie tej opcji umożliwia modyfikowanie szablonów dołączanych do tematu zainfekowanych wiadomości.
Tekst znacznika tematu
Możesz dodać niestandardowy znacznik do tematów wiadomości, których dotyczy problem.
Powiadamianie właściciela skrzynki pocztowej
Gdy opcja ta jest włączona, w przypadku wykrycia zagrożenia użytkownik otrzyma wiadomość e-mail z powiadomieniem.
Język
Wybierz żądany język z menu rozwijanego. Właściciel skrzynki pocztowej będzie otrzymywać wiadomości e-mail z powiadomieniami w wybranym języku, gdy obiekt zostanie zwolniony z kwarantanny. Ta opcja zastępuje domyślny język dzierżawy w ustawieniach.
Powiadamianie administratora
Określ adres e-mail (naciśnij Enter, aby dodać wiele adresów), pod którym będą odbierane powiadomienia za każdym razem, gdy zostanie wykryte zagrożenie.

Ochrona Gmaila przed spamem

Włącz Ochronę Gmaila przed spamem
Ta funkcja jest aktywna po włączeniu i można skonfigurować opcje dodatkowe.
Czynność po wykryciu zagrożenia
- **Brak czynności** — nie jest wykonywana żadna akcja, a wiadomość e-mail jest dostarczana do odbiorcy
- **Przenieś do spamu** — wiadomość e-mail zostanie przeniesiona do folderu Spam.
- **Przenieś do kosza** — wiadomość e-mail zostanie przeniesiona do folderu Kosz.
- **Usuń wiadomość** — wiadomość e-mail zostanie usunięta
- **Quarantine message** (Poddaj wiadomość kwarantannie) — oryginalna wiadomość e-mail zostanie usunięta, a jej kopia będzie przechowywana w kwarantannie. Jeśli zdecydujesz się zwolnić wiadomość e-mail z kwarantanny, zostanie ona wysłana jako załącznik w nowej wiadomości e-mail i dostarczona do odbiorcy.

Znacznik tematu
Włączenie tej opcji umożliwia modyfikowanie szablonów dołączanych do tematu zainfekowanych wiadomości.
Tekst znacznika tematu
Możesz dodać niestandardowy znacznik do tematów wiadomości, których dotyczy problem.
Listy elementów **zatwierdzonych**, **zablokowanych** i **ignorowanych** można skonfigurować, określając kryteria, takie jak adres lub zakres adresów IP czy nazwa domeny. Aby dodać, zmodyfikować lub usunąć kryteria, należy kliknąć opcję **Edytuj** obok listy, która ma być zarządzana. W celu zaimportowania listy niestandardowej z pliku (zamiast dodawania pojedynczych wpisów ręcznie) należy kliknąć opcję **Importuj**, a następnie wskazać (*.txt*) plik zawierający wpisy, które mają zostać dodane do listy. Jeśli natomiast konieczne jest wyeksportowanie istniejącej już listy do pliku (*.txt*), należy wybrać z menu kontekstowego opcję **Eksportuj**.

Lista zatwierdzonych adresów IP	Automatycznie dodaje do białej listy wiadomości e-mail pochodzące z określonych adresów IP. Zawartość wiadomości e-mail nie zostanie sprawdzona.
Lista zablokowanych adresów IP	Automatycznie blokuje wiadomości e-mail pochodzące z określonych adresów IP.
Lista ignorowanych adresów IP	Lista adresów IP, które są ignorowane podczas klasyfikacji. Zawartość wiadomości e-mail zostanie sprawdzona.
Lista zatwierdzonych nadawców	Dodaje do białej listy wiadomości e-mail pochodzące od określonego nadawcy lub domeny. Tylko jeden adres nadawcy lub cała domena jest używana do weryfikacji na podstawie następującego priorytetu: 1.Adres połączenia SMTP „MAIL FROM” 2.Pole nagłówka wiadomości e-mail „Return-Path:” 3.Pole nagłówka wiadomości e-mail „X-Env-Sender:” 4.Pole nagłówka wiadomości e-mail „From:” 5.Pole nagłówka wiadomości e-mail „Sender:” 6.Pole nagłówka wiadomości e-mail „X-Apparently-From:”
Lista zablokowanych nadawców	Blokuje wiadomości e-mail pochodzące od określonego nadawcy lub domeny. Wszystkie zidentyfikowane adresy nadawców lub całe domeny są używane do weryfikacji: Adres połączenia SMTP „MAIL FROM” Pole nagłówka wiadomości e-mail „Return-Path:” Pole nagłówka wiadomości e-mail „X-Env-Sender:” Pole nagłówka wiadomości e-mail „From:” Pole nagłówka wiadomości e-mail „Sender:” Pole nagłówka wiadomości e-mail „X-Apparently-From:”

Ochrona przed atakami typu „phishing” w Gmailu

Włącz ochronę Gmaila przed atakami typu „phishing”
Ta funkcja jest aktywna po włączeniu i można skonfigurować opcje dodatkowe.
Czynność po wykryciu zagrożenia
• **Brak czynności** — nie jest wykonywana żadna czynność, a wiadomość e-mail ze szkodliwym załącznikiem jest dostarczana do odbiorcy.
• **Przenieś do spamu** — wiadomość e-mail zostanie przeniesiona do folderu Spam.
• **Przenieś do kosza** — wiadomość e-mail zostanie przeniesiona do folderu Kosz.
• **Usuń wiadomość** — wiadomość e-mail zostanie usunięta
• **Quarantine message** (Poddaj wiadomość kwarantannie) — oryginalna wiadomość e-mail zostanie usunięta, a jej kopia będzie przechowywana w kwarantannie. Jeśli zdecydujesz się zwolnić wiadomość e-mail z kwarantanny, zostanie ona wysłana jako załącznik w nowej wiadomości e-mail i dostarczona do odbiorcy.
Znacznik tematu
Włączenie tej opcji umożliwia modyfikowanie szablonów dołączanych do tematu zainfekowanych wiadomości.
Tekst znacznika tematu
Możesz dodać niestandardowy znacznik do tematów wiadomości, których dotyczy problem.
Powiadamianie właściciela skrzynki pocztowej
Gdy opcja ta jest włączona, w przypadku wykrycia zagrożenia użytkownik otrzyma wiadomość e-mail z powiadomieniem.
Powiadamianie administratora
Określ adres e-mail (naciśnij Enter, aby dodać wiele adresów), pod którym będą odbierane powiadomienia za każdym razem, gdy zostanie wykryte zagrożenie.

Ustawienia ochrony dla usługi OneDrive

Ta sekcja zawiera informacje o zmianie ustawień ogólnych i opcji ochrony przed szkodliwym oprogramowaniem w usłudze OneDrive.

OneDrive — Ogólne

ESET LiveGrid®Opinia dotycząca aplikacji
Próbka zostanie przesłana do ESET Research Lab w celu przeprowadzenia dalszej analizy. Więcej informacji na temat aplikacji tego typu można znaleźć w słowniczku.
Zapisuj w dzienniku informacje o wszystkich obiektach
Jeśli ta opcja jest zaznaczona, w Dziennikach skanowania będą widoczne wszystkie wyniki skanowania (w tym wyleczone). Zasady przechowywania wyników czystego skanowania wynoszą trzy dni. Wyniki skanowania starsze niż trzy dni zostaną usunięte na stałe.

Onedrive — Ochrona przed szkodliwym oprogramowaniem

Onedrive — Ochrona przed szkodliwym oprogramowaniem
Ta funkcja jest aktywna po włączeniu i można skonfigurować opcje dodatkowe.
Ochrona raportowania i uczenia maszynowego
Zaawansowane uczenie maszynowe jest teraz częścią silnika detekcji jako zaawansowana warstwa ochrony, która poprawia wykrywanie. Przed zmodyfikowaniem progu (lub poziomu) kategorii Raportowanie należy zapoznać się z poniższymi informacjami:
Czynność po wykryciu zagrożenia
- **Brak czynności** — nie jest wykonywana żadna akcja, a plik pozostaje w usłudze OneDrive
- **Przenieś do kosza** — przenosi plik do Kosza.
- **Zastąp** — zawartość oryginalnego pliku jest zastępowana tekstem zdefiniowanym poniżej w oknie „Tekst zastępczy pliku”
- **Kwarantanna** — oryginalny plik zostanie przeniesiony do kosza i skopiowany do kwarantanny. Po zwolnieniu pliku poprzednio usunięty plik pozostaje w koszu, a nowa kopia zostanie przekazana do oryginalnego folderu usługi OneDrive.

Tekst zastępczy pliku
Powoduje zastąpienie załącznika plikiem tekstowym zawierającym szczegółowe informacje o wykonanej czynności.
Powiadamianie właściciela
Gdy opcja ta jest włączona, w przypadku wykrycia zagrożenia użytkownik otrzyma wiadomość e-mail z powiadomieniem.
Powiadamianie administratora
Określ adres e-mail (naciśnij Enter, aby dodać wiele adresów), pod którym będą odbierane powiadomienia za każdym razem, gdy zostanie wykryte zagrożenie.

Ustawienia ochrony dla usługi Google Drive

Ta sekcja zawiera informacje o zmianie ustawień ogólnych i opcji Dysku Google oraz opcji ochrony przed szkodliwym oprogramowaniem w usłudze Dysk Google.

Ogólne informacje o Dysku Google

ESET LiveGrid®Opinia dotycząca aplikacji
Próbka zostanie przesłana do ESET Research Lab w celu przeprowadzenia dalszej analizy. Więcej informacji na temat aplikacji tego typu można znaleźć w słowniczku.
Zapisuj w dzienniku informacje o wszystkich obiektach
Jeśli ta opcja jest zaznaczona, w Dziennikach skanowania będą widoczne wszystkie wyniki skanowania (w tym wyleczone). Zasady przechowywania wyników czystego skanowania wynoszą trzy dni. Wyniki skanowania starsze niż trzy dni zostaną usunięte na stałe.

Ochrona przed szkodliwym oprogramowaniem na Dysku Google

Ochrona przed szkodliwym oprogramowaniem na Dysku Google
Ta funkcja jest aktywna po włączeniu i można skonfigurować opcje dodatkowe.
Ochrona raportowania i uczenia maszynowego
Zaawansowane uczenie maszynowe jest teraz częścią silnika detekcji jako zaawansowana warstwa ochrony, która poprawia wykrywanie. Przed zmodyfikowaniem progu (lub poziomu) kategorii Raportowanie należy zapoznać się z poniższymi informacjami:
Czynność po wykryciu zagrożenia
- **Brak czynności** — nie jest wykonywana żadna akcja, a plik pozostaje w usłudze Google Drive
- **Przenieś do kosza** — przenosi plik do Kosza.
- **Zastąp** — zawartość oryginalnego pliku jest zastępowana tekstem zdefiniowanym poniżej w oknie „Tekst zastępczy pliku”.
- **Kwarantanna** — oryginalny plik zostanie przeniesiony do kosza i skopiowany do kwarantanny.
- **Usuń** — oryginalny plik zostanie trwale usunięty z Dysku Google.

Tekst zastępczy pliku
Powoduje zastąpienie załącznika plikiem tekstowym zawierającym szczegółowe informacje o wykonanej czynności.
Powiadamianie właściciela
Gdy opcja ta jest włączona, w przypadku wykrycia zagrożenia użytkownik otrzyma wiadomość e-mail z powiadomieniem.
Powiadamianie administratora
Określ adres e-mail (naciśnij Enter, aby dodać wiele adresów), pod którym będą odbierane powiadomienia za każdym razem, gdy zostanie wykryte zagrożenie.

Ustawienia ochrony dla grup zespołu

Ta sekcja zawiera informacje o zmianie ustawień ogólnych i opcji ochrony przed szkodliwym oprogramowaniem w grupach zespołu.

Grupy zespołu – Ogólne

ESET LiveGrid®Opinia dotycząca aplikacji
Próbka zostanie przesłana do ESET Research Lab w celu przeprowadzenia dalszej analizy. Więcej informacji na temat aplikacji tego typu można znaleźć w słowniczku.
Zapisuj w dzienniku informacje o wszystkich obiektach
Jeśli ta opcja jest zaznaczona, w Dziennikach skanowania będą widoczne wszystkie wyniki skanowania (w tym wyleczone). Polityka przechowywania wyników skanowania, które zostały wyleczone, wynosi 3 dni. Wyniki skanowania starsze niż trzy dni zostaną usunięte na stałe.

Grupy zespołu – Ochrona przed szkodliwym oprogramowaniem

Grupy zespołu – Ochrona przed szkodliwym oprogramowaniem
Po włączeniu funkcja jest aktywna i można skonfigurować opcje dodatkowe.
Ochrona raportowania i uczenia maszynowego
Zaawansowane uczenie maszynowe jest teraz częścią silnika detekcji jako zaawansowana warstwa ochrony, która poprawia wykrywanie. Przed zmodyfikowaniem progu (lub poziomu) kategorii Raportowanie należy zapoznać się z poniższymi informacjami:
Czynność po wykryciu zagrożenia
- **Brak czynności** — nie jest wykonywana żadna czynność, plik pozostaje nienaruszony
- **Przenieś do kosza** — przenosi plik do folderu Kosz grupy zespołu.
- **Zastąp** — zawartość oryginalnego pliku jest zastępowana tekstem zdefiniowanym poniżej w oknu „Tekst zastępczy pliku”
- **Kwarantanna** — oryginalny plik zostanie przeniesiony do folderu Kosz grupy zespołu i skopiowany do kwarantanny Po zwolnieniu pliku poprzednio usunięty plik pozostanie w folderze Kosz, a nowa kopia zostanie przeniesiona do oryginalnej lokalizacji.

Tekst zastępczy pliku
Powoduje zastąpienie załącznika plikiem tekstowym zawierającym szczegółowe informacje o wykonanej czynności.
Powiadamianie właściciela
Gdy opcja ta jest włączona, w przypadku wykrycia zagrożenia użytkownik otrzyma wiadomość e-mail z powiadomieniem.
Powiadamianie administratora
Określ adres e-mail (naciśnij Enter, aby dodać wiele adresów), pod którym będą odbierane powiadomienia za każdym razem, gdy zostanie wykryte zagrożenie.

Ustawienia ochrony dla witryn programu SharePoint

Ta sekcja zawiera informacje o zmianie ustawień ogólnych i opcji ochrony przed szkodliwym oprogramowaniem dla witryn programu SharePoint.

Lokacje SharePoint – Ogólne

ESET LiveGrid®Opinia dotycząca aplikacji
Próbka zostanie przesłana do ESET Research Lab w celu przeprowadzenia dalszej analizy. Więcej informacji na temat aplikacji tego typu można znaleźć w słowniczku.
Zapisuj w dzienniku informacje o wszystkich obiektach
Jeśli ta opcja jest zaznaczona, w Dziennikach skanowania będą widoczne wszystkie wyniki skanowania (w tym wyleczone). Polityka przechowywania wyników skanowania, które zostały wyleczone, wynosi 3 dni. Wyniki skanowania starsze niż trzy dni zostaną usunięte na stałe.

Lokacje SharePoint – Ochrona przed szkodliwym oprogramowaniem

Lokacje SharePoint – Ochrona przed szkodliwym oprogramowaniem
Po włączeniu funkcja jest aktywna i można skonfigurować opcje dodatkowe.
Ochrona raportowania i uczenia maszynowego
Zaawansowane uczenie maszynowe jest teraz częścią silnika detekcji jako zaawansowana warstwa ochrony, która poprawia wykrywanie. Przed zmodyfikowaniem progu (lub poziomu) kategorii Raportowanie należy zapoznać się z poniższymi informacjami:
Czynność po wykryciu zagrożenia
- **Brak czynności** — nie jest wykonywana żadna czynność, plik pozostaje nienaruszony
- **Przenieś do kosza** — przenosi plik do folderu Kosz w programie SharePoint.
- **Zastąp** — zawartość oryginalnego pliku jest zastępowana tekstem zdefiniowanym poniżej w oknu „Tekst zastępczy pliku”
- **Kwarantanna** — oryginalny plik zostanie przeniesiony do folderu Kosz w programie SharePoint i skopiowany do kwarantanny Po zwolnieniu pliku poprzednio usunięty plik pozostanie w folderze Kosz, a nowa kopia zostanie przeniesiona do oryginalnej lokalizacji.

Tekst zastępczy pliku
Powoduje zastąpienie załącznika plikiem tekstowym zawierającym szczegółowe informacje o wykonanej czynności.
Powiadamianie właściciela
Gdy opcja ta jest włączona, w przypadku wykrycia zagrożenia użytkownik otrzyma wiadomość e-mail z powiadomieniem.
Powiadamianie administratora
Określ adres e-mail (naciśnij Enter, aby dodać wiele adresów), na który będą wysyłane powiadomienia za każdym razem, gdy zostanie wykryte zagrożenie.

Ustawienia ochrony dla ESET LiveGuard Advanced

Aby użyć funkcji ESET LiveGuard Advanced, skonfiguruj politykę, która umożliwia analizę ESET LiveGuard Advanced. Użytkownicy lub grupy przypisane do tej polityki będą miały dodatkową ochronę. Pliki wysłane do ESET LiveGuard Advanced celem analizy są wymienione na karcie Przesłane pliki; dotyczy to nieznanych (nigdy wcześniej nie widzianych) podejrzanych próbek. Znane szkodliwe pliki (na podstawie skrótów) nie są wysyłane do analizy ESET LiveGuard Advanced.

Wyniki ESET LiveGuard Advanced widoczne będą w Dziennikach skanowania (Exchange Online, OneDrive, grupy zespołu lub witryny SharePoint) oznaczone jako .

ESET LiveGuard Advanced

Po włączeniu funkcja jest aktywna i można skonfigurować opcje dodatkowe.

> ESET LiveGuard Advanced automatycznie włączy opinię ESET LiveGrid®. Próbka zostanie przesłana do ESET Research Lab w celu przeprowadzenia dalszej analizy. Przeczytaj więcej o ESET LiveGrid® w glosariuszu .

Próg wykrycia

Wyniki ze wskazanym poziomem progowym i wyższym będą traktowane jako zagrożenia.

Automatyczne przesyłanie podejrzanych próbek (menu rozwijane)

To ustawienie jest związane z ESET LiveGrid® i umożliwia następujące działania: Wszystkie, Wszystkie oprócz dokumentów, Brak.

Automatyczne przesyłanie podejrzanych próbek (suwaki)

Wybierz typy plików, które mają być przesyłane do ESET LiveGuard Advanced, jeśli zawierają podejrzany kod przypominający zagrożenia, mają nietypowe cechy lub zachowanie:

- **Pliki wykonywalne** – .exe, .dll, .sys
- **Archiwa** – .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- **Skrypty** – .bat, .cmd, .hta, .js, .vbs, .js, .ps1
- **Inne** – .jar, .reg, .msi, .swf, .lnk

Usuń podejrzane próbki z serwerów ESET

Wybierz, kiedy usunąć próbki, które zostały wysłane do analizy. Usuń próbki z chmury ESET LiveGuard Advanced: Nigdy, po 30 dniach, natychmiast po analizie.

Dokumenty

Użyj suwaka, aby zezwolić na wysyłanie dokumentów pakietu Microsoft Office, plików PDF i innych typów dokumentów do ESET LiveGuard Advanced celem analizy.

Usuń dokumenty z serwerów firmy ESET

Usuń próbki w formacie plików dokumentu z chmury ESET LiveGuard Advanced: Nigdy, po 30 dniach, natychmiast po analizie.

Ochrona raportowania i uczenia maszynowego

Silnik detekcji chroni przed złośliwymi atakami systemowymi, skanując pliki, wiadomości e-mail i komunikację sieciową. Jeśli zostanie wykryty obiekt sklasyfikowany jako szkodliwe oprogramowanie, rozpoczną się działania naprawcze. Silnik detekcji może go wyeliminować, najpierw blokując go, a następnie podejmując działania takie jak leczenie, usunięcie lub przeniesienie do kwarantanny.

Ochrona w czasie rzeczywistym i uczenie maszynowe

Zaawansowane uczenie maszynowe jest teraz częścią silnika detekcji jako zaawansowana warstwa ochrony, która poprawia wykrywanie. Więcej informacji na temat ochrony tego typu można znaleźć w słowniczku. Możesz skonfigurować poziomy raportowania dla następujących kategorii:

Szkodliwe oprogramowanie

Wirus komputerowy to fragment złośliwego kodu, który jest wprowadzony lub dołączony do istniejących plików na komputerze. Jednak termin „wirus” jest często nadużywany. „Malware” (szkodliwe oprogramowanie) jest terminem dokładniejszym. Wykrywanie szkodliwego oprogramowania wykonywane jest przez moduł silnika detekcji w połączeniu z mechanizmem uczenia maszynowego. Więcej informacji na temat aplikacji tego typu można znaleźć w słowniczku.

Potencjalnie niepożądane aplikacje

Potencjalnie niepożądana aplikacja to oprogramowanie, którego zamiary nie są jednoznacznie złośliwe. Ale może zainstalować dodatkowe niepożądane oprogramowanie, zmienić działanie urządzenia cyfrowego, wykonać działania, które nie zostały zatwierdzone ani nie są oczekiwane przez użytkownika, lub ma inne niejasne

przeznaczenie.
Ta kategoria obejmuje oprogramowanie wyświetlające reklamy, otoki pobierania, różne paski narzędzi przeglądarek, oprogramowanie o działaniu wprowadzającym w błąd, pakiety oprogramowania, oprogramowanie do śledzenia.
Więcej informacji na temat aplikacji tego typu można znaleźć w słowniczku.

Potencjalnie podejrzane aplikacje

Jest to oprogramowanie skompresowane za pomocą programów pakujących lub zabezpieczających, które używają własnościowych metod kompresji i/lub szyfrowania. Programy te są często używane do zniechęcania przed odtwarzaniem kodu źródłowego lub zaciemniania zawartości pliku wykonywalnego (na przykład w celu ukrycia szkodliwego oprogramowania).
Ta kategoria obejmuje wszystkie nieznane aplikacje skompresowane za pomocą programów pakujących lub zabezpieczających często używanych do kompresowania szkodliwego oprogramowania.

Potencjalnie niebezpieczne aplikacje

Ta klasyfikacja obejmuje legalne oprogramowanie komercyjne, które może zostać wykorzystane do szkodliwych celów. Niebezpieczna aplikacja może oznaczać legalne oprogramowanie posiadające potencjał do wykorzystania go w nieodpowiednim celu.
Ta kategoria obejmuje narzędzia do crackowania, generatory kluczy licencji, narzędzia do hackowania, narzędzia do zdalnego dostępu lub sterowania, aplikacje do łamania haseł, programy rejestrujące znaki wprowadzane na klawiaturze itp. Domyślnie opcja ta jest wyłączona.
Więcej informacji na temat aplikacji tego typu można znaleźć w słowniczku.

Raportowanie

Raportowanie jest realizowane przez silnik detekcji i komponent uczenia maszynowego. Próg raportowania można dostosować do danego środowiska i potrzeb. Nie ma jednej poprawnej konfiguracji. W związku z tym zaleca się monitorowanie zachowania w danym środowisku i podjęcie decyzji, czy inne ustawienia raportowania są bardziej odpowiednie.

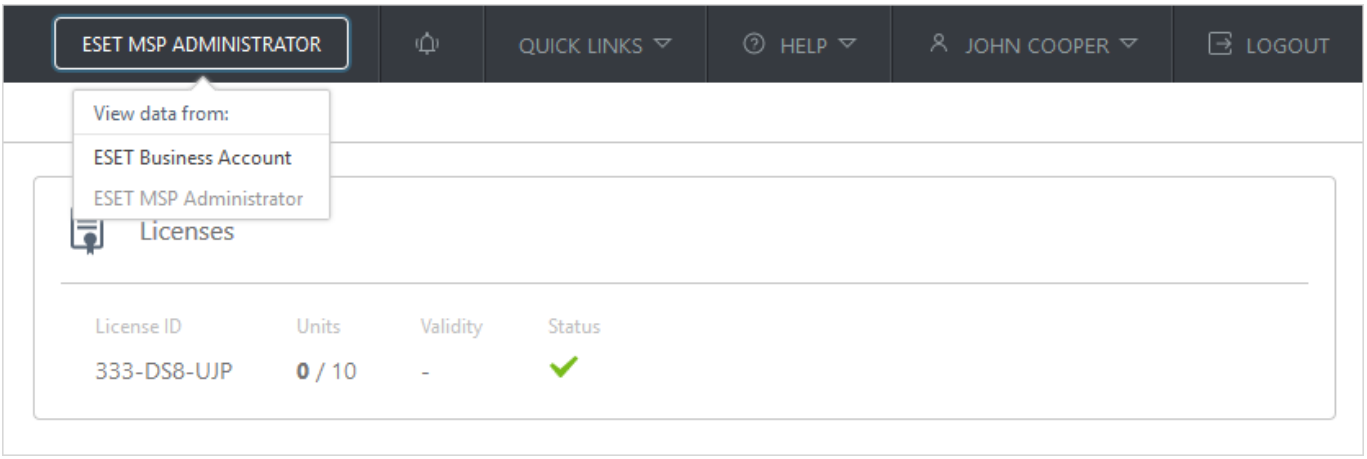
Raportowanie nie podejmuje działań z obiektami. Tylko przekazuje informacje do odpowiedniej warstwy ochrony, która następnie podejmuje właściwie działanie.

Agresywne	**Raportowanie ustawione na maksymalną czułość. Zgłaszane jest więcej wykryć. Chociaż ustawienie Agresywne może wydawać się najbezpieczniejsze, często okazuje się zbyt czułe, co może przynieść efekt przeciwny do zamierzonego.** Ustawienie agresywne może fałszywie rozpoznawać obiekty jako złośliwe, co powoduje podejmowanie określonych działań (w zależności od ustawień ochrony).
Zrównoważone	To ustawienie zapewnia zrównoważone działanie, w tym wydajność, częstotliwość wykrywania i jak najmniejszą liczbę obiektów błędnie uznawanych za zagrożenia.
Ostrożne	Raportowanie skonfigurowane tak, aby zminimalizować ilość błędów polegających na traktowaniu bezpiecznego pliku jako zagrożenia. Obiekt jest raportowany jako szkodliwy tylko wtedy, gdy działanie aplikacji odpowiada zachowaniu aplikacji szkodliwych.
Wył.	Raportowanie nie jest aktywne. Nie przeprowadza się wykrywania zagrożeń. Nie są one zgłaszane, a problematyczne pliki nie są leczone. Nie można dezaktywować raportowania szkodliwego oprogramowania, dlatego w przypadku szkodliwego oprogramowania ustawienie Wyłącz nie jest dostępne.

Zarządzanie licencjami

W oknie głównym znajduje się przegląd tych licencji, które są pobierane z konta ESET Business Account lub ESET MSP Administrator. Możesz zobaczyć wszystkie pule licencji, witryny lub firmy, które są dostępne w portalu ESET Business Account lub ESET MSP Administrator. Zarządzanie licencjami umożliwia zapewnienie lub zaprzestanie ochrony użytkowników.

Jeśli masz ten sam adres e-mail zarejestrowany dla kont ESET MSP Administrator i ESET Business Account (logowanie jednokrotne), możesz przełączać się między widokami kont ESET Business Account i ESET MSP Administrator (konto z licencją hybrydową).



Licencja ESET Cloud Office Security pozwala na korzystanie z funkcji ESET LiveGuard Advanced bez dodatkowych opłat. Obok identyfikatora licencji widoczna będzie etykieta ELG.

Zarządzanie licencjami za pomocą konta ESET Business Account

Wyświetla informacje o licencji i użyciu (nazwa puli licencji, identyfikator licencji, jednostki, ważność i stan). Licencje i pule licencji są ładowane z ESET Business Account. Pule licencji są dostępne tylko wtedy, gdy masz istniejące witryny w ramach ESET Business Account (witryny są przydatne do kategoryzacji). Jedna jednostka reprezentuje ochronę ESET Cloud Office Security pojedynczego użytkownika w usłudze Exchange Online i OneDrive.

> Na każdego chronionego użytkownika zużywana jest jednostka licencji. Jest to niezależne od tego, jakie usługi Microsoft 365 są używane. Użytkownik z usługą Exchange Online lub OneDrive (lub obiema) zawsze zużywa jedną jednostkę licencji. Jednostka licencji nie jest używana przez grupy zespołów lub lokalizacje SharePoint.

Każdy nowy użytkownik pojawi się w sekcji Użytkownicy jako Niechroniony. Jeśli korzystasz z automatycznej ochrony dla dzierżawy lub grupy, nowi użytkownicy są chronieni automatycznie i będą wyświetlani jako Chroniony.
Podczas ochrony użytkowników dostępne są dwie opcje:

- **Automatyczna ochrona przez dzierżawę lub grupę (zalecane)** — to bezobsługowa opcja, w ramach której każdy nowo dodany użytkownik, który należy do grupy Azure AD lub należy do dzierżawy, jest automatycznie chroniony. Szczegółowe informacje znajdują się w notatce poniżej.
- **Indywidualna ochrona użytkowników** — wymaga zarządzania, a każdego nowego użytkownika należy chronić ręcznie.

Ochrona użytkowników (bez puli licencji)

1. Kliknij pozycję **Chroń**.
2. Wybierz pozycję Dzierżawa lub Grupa, aby uzyskać automatyczną ochronę użytkownika, a następnie kliknij przycisk **Chroń**. Aby uzyskać ochronę poszczególnych użytkowników, wybierz tych, których chcesz chronić, i kliknij przycisk **Chroń**. Użytkownicy są teraz chronieni przez politykę domyślną.
3. W razie potrzeby określ niestandardowe polityki dla użytkowników w sekcji Polityki.

Ochrona użytkowników (przy użyciu puli licencji)

1. Wybierz pulę licencji i kliknij ikonę z trzema kropkami > **Pokaż szczegóły** obok puli licencji.
2. Kliknij pozycję **Chroń**.
3. Wybierz pozycję Dzierżawa lub Grupa, aby uzyskać automatyczną ochronę użytkownika, a następnie kliknij przycisk **Chroń**. Aby uzyskać ochronę poszczególnych użytkowników, wybierz tych, których chcesz chronić, i kliknij przycisk **Chroń**. Użytkownicy są teraz chronieni przez politykę domyślną.
4. W razie potrzeby określ niestandardowe polityki dla użytkowników w sekcji Polityki.

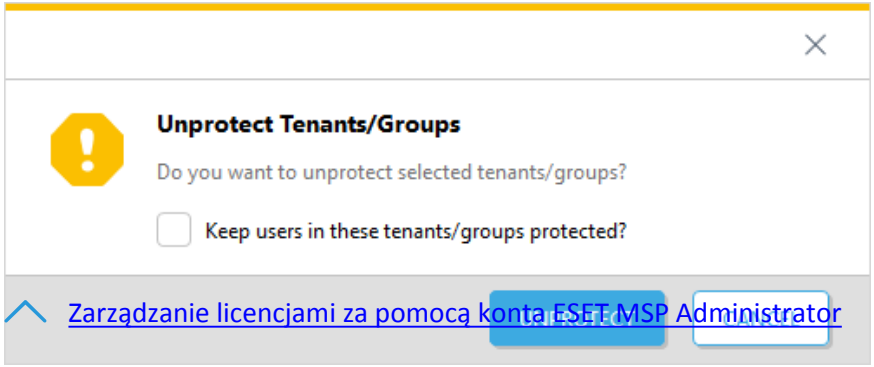
> Upewnij się, że masz wystarczającą liczbę jednostek licencji, szczególnie z włączoną automatyczną ochroną, gdy liczba użytkowników wzrośnie. Po wykorzystaniu wszystkich jednostek licencji żaden nowy użytkownik, który zostanie członkiem dzierżawy lub grupy, nie będzie chroniony. Ochrona istniejących użytkowników pozostaje niezmieniona.
> Jeśli tymczasowo brakuje Ci jednostek licencji i chcesz, aby poszczególni użytkownicy byli chronieni, użyj niechronionych grup (nie używaj automatycznej ochrony) i ręcznie chroń użytkowników. Po zwiększeniu puli licencji o więcej jednostek można powrócić do automatycznej ochrony w celu łatwiejszego zarządzania.

Przenieś

Aby przenieść użytkowników między pulami licencji lub uzyskać dostęp do bardziej zaawansowanych operacji z licencjami, otwórz ESET Business Account .

Brak ochrony

1. Wybierz poszczególnych użytkowników, dzierżawę lub grupę, a następnie kliknij przycisk **Przestań chronić**.
2. Podczas usuwania dzierżawy lub grupy automatycznej ochrony zostaniesz zapytany, czy **zachować użytkowników w dzierżawach/grupach chronionych** Jeśli zdecydujesz się nie używać tej opcji, użytkownicy stracą ochronę. Jeśli zaznaczysz to pole wyboru, automatyczna ochrona dzierżawy lub grupy zostanie dezaktywowana i zmieni się w ochronę poszczególnych użytkowników. Użytkownicy są nadal chronieni, ale musisz ręcznie chronić wszystkich nowo dodanych użytkowników.



Zarządzanie licencjami za pomocą konta ESET MSP Administrator

Wyświetla informacje o licencji i użyciu (firma klienta, identyfikator licencji, jednostki i stan).

> Na każdego chronionego użytkownika zużywana jest jednostka licencji. Jest to niezależne od tego, jakie usługi Microsoft 365 są używane. Użytkownik z usługą Exchange Online lub OneDrive (lub obiema) zawsze zużywa jedną jednostkę licencji.
> Jednostka licencji nie jest używana przez grupy zespołów lub lokalizacje SharePoint.

Każdy nowy użytkownik pojawi się w sekcji Użytkownicy jako **Niechroniony**. Jeśli korzystasz z automatycznej ochrony dla dzierżawy lub grupy, nowi użytkownicy są chronieni automatycznie i będą wyświetlani jako **Chroniony**.

Podczas ochrony użytkowników dostępne są dwie opcje:

- **Automatyczna ochrona przez dzierżawę lub grupę (zalecane)** — to bezobsługowa opcja, w ramach której każdy nowo dodany użytkownik, który jest członkiem grupy usługi Azure AD lub należy do dzierżawy, jest automatycznie chroniony. Szczegółowe informacje można znaleźć w notatce poniżej.
- **Indywidualna ochrona użytkownika** — wymaga zarządzania i ręcznego ustawienia ochrony każdego z nowych użytkowników.

Chroń użytkowników

1. Kliknij pozycję **Chroń**.
2. Wybierz pozycję Dzierżawa lub Grupa, aby uzyskać automatyczną ochronę użytkownika, a następnie kliknij przycisk **Chroń**. Aby uzyskać ochronę poszczególnych użytkowników, wybierz tych, których chcesz chronić, i kliknij przycisk **Chroń**. Użytkownicy są teraz chronieni przez politykę domyślną.
3. W razie potrzeby określ niestandardowe polityki dla użytkowników w sekcji Polityki.

> Upewnij się, że masz wystarczającą liczbę jednostek licencji, szczególnie z włączoną automatyczną ochroną, gdy liczba użytkowników wzrośnie. Po wykorzystaniu wszystkich jednostek licencji żaden nowy użytkownik, który zostanie członkiem dzierżawy lub grupy, nie będzie chroniony. Ochrona istniejących użytkowników pozostaje niezmieniona.
> Jeśli tymczasowo brakuje Ci jednostek licencji i chcesz, aby poszczególni użytkownicy byli chronieni, użyj niechronionych grup (nie używaj automatycznej ochrony) i ręcznie chroń użytkowników. Po zwiększeniu puli licencji o więcej jednostek można powrócić do automatycznej ochrony w celu łatwiejszego zarządzania.

Brak ochrony

1. Wybierz poszczególnych użytkowników, dzierżawę lub grupę, a następnie kliknij przycisk **Przestań chronić**.
2. Podczas usuwania dzierżawy lub grupy automatycznej ochrony zostaniesz zapytany, czy **zachować użytkowników w dzierżawach/grupach chronionych** Jeśli zdecydujesz się nie używać tej opcji, użytkownicy stracą ochronę. Jeśli zaznaczysz to pole wyboru, automatyczna ochrona dzierżawy lub grupy zostanie dezaktywowana i zmieni się w ochronę poszczególnych użytkowników. Użytkownicy są nadal chronieni, ale musisz ręcznie chronić wszystkich nowo dodanych użytkowników.

Dostęp użytkownika ESET Cloud Office Security do konkretnej firmy

W środowisku z wieloma dzierżawami można zapewnić użytkownikowi dostęp do ESET Cloud Office Security, zezwalając mu przy tym na wyświetlanie tylko określonej firmy (z uprawnieniami do odczytu lub zapisu). Jest to zwykle wykorzystywane przez dostawców usług zarządzanych.

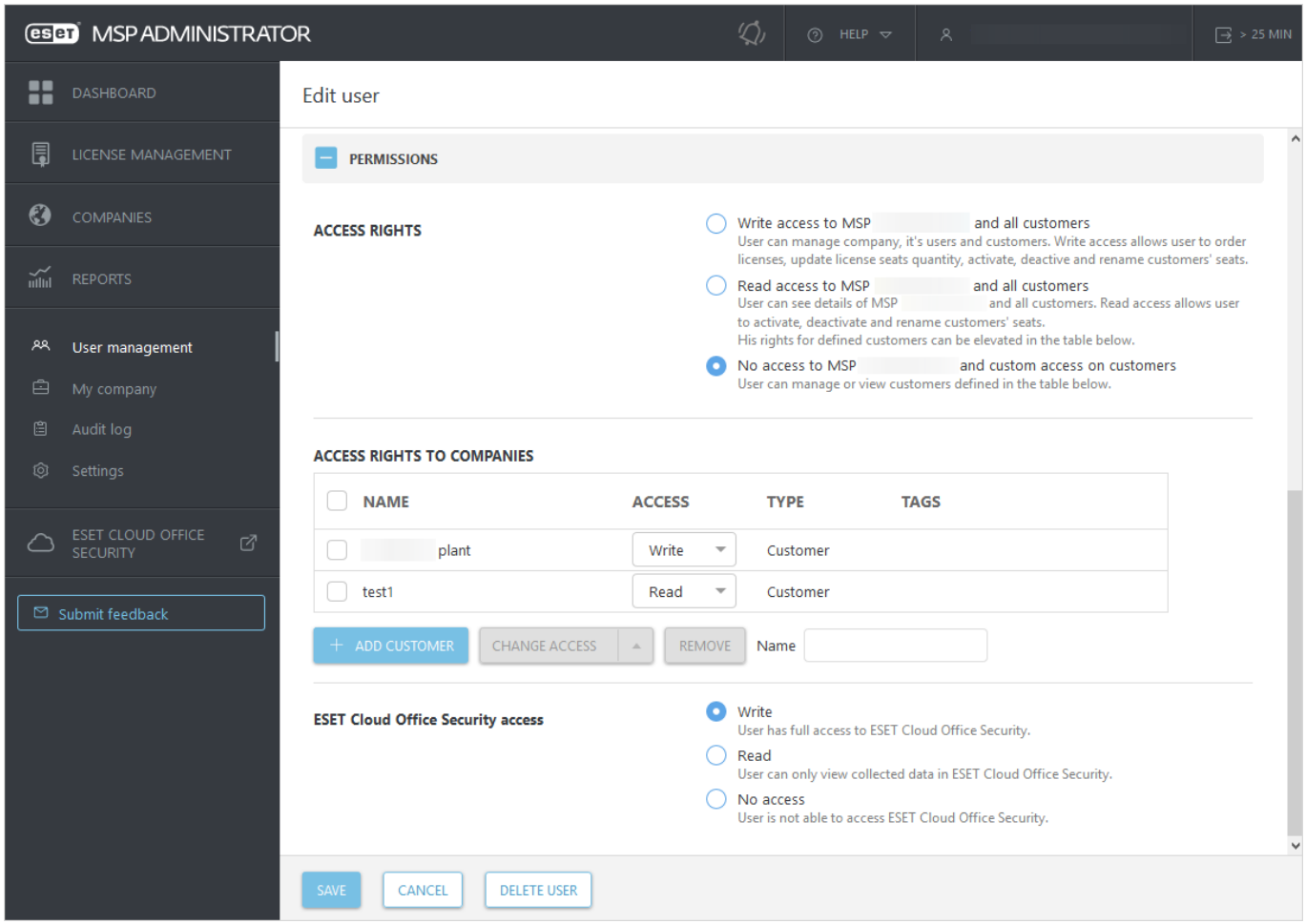
Skonfiguruj prawa dostępu ESET MSP Administrator, przypisując firmę z uprawnieniami do **Zapisu** i dostępem do **Zapisu** w ESET Cloud Office Security:

1. Zaloguj się do ESET MSP Administrator jako administrator.

2. Edytuj użytkownika i skonfiguruj **prawa dostępu do firm** w obszarze Uprawnienia, a następnie wybierz dostęp do **zapisu**. Użytkownik będzie mógł zobaczyć tylko przypisaną firmę z jej pulą licencji.

3. Ustaw dostęp do ESET Cloud Office Security z prawem do **zapisu**, aby użytkownik mógł chronić firmę,

dodając dzierżawę. Użytkownik z dostępem do odczytu nie może dodać ani usunąć dzierżawy.



Tylko jeden typ dostępu do ESET Cloud Office Security można skonfigurować jako ustawienie globalne i mające zastosowanie do wszystkich firm (jeśli użytkownikowi przypisano wiele firm).

Dziennik audytu

Śledzi zmiany w konfiguracji lub ochronie ESET Cloud Office Security. Rekordy dziennika audytu są dowodem działań i pokazują sekwencję, w jakiej wystąpiły. Dzienniki audytu przechowują informacje o określonej operacji lub zdarzeniu. Dzienniki audytu są tworzone za każdym razem, gdy obiekt ESET Cloud Office Security (pula licencji, użytkownik, polityka, raport, element kwarantanny, taki jak załącznik) jest tworzony lub modyfikowany.

Po kliknięciu ikony koła zębatego w prawym górnym rogu, aby uzyskać dostęp do opcji **Eksportuj do CSV** z menu kontekstowego, można wyeksportować siatkę tabeli do formatu *CSV* i użyć jej w innych aplikacjach do pracy z listą.

Kliknij ikonę , aby otworzyć pasek boczny z podsumowaniem określonego zapisu dziennika audytu. Aby uzyskać szczegółowe informacje, kliknij ikonę i wybierz pozycję **Pokaż szczegóły**.

Kafelek	Szczegóły
Informacje podstawowe	Pokazuje ogólne dane dziennika audytu (Wystąpienie, Akcja, Ważność, Wynik, Sekcja).
Użytkownik	Wyświetla informacje o użytkowniku, który podjął działanie lub wprowadził zmianę, obejmują adres e-mail i adres IP użytkownika.
Zmiany	Szczegółowe informacje o wprowadzonych zmianach.

Kafelek	Szczegóły
Stare ustawienia	Pokazuje poprzednie ustawienia polityki.
Nowe ustawienia	Pokazuje bieżące ustawienia polityki.
Obiekty	Wyświetla listę obiektów, na które zmiana lub akcja ma wpływ (użytkownik, polityka, załącznik itp.).

Możliwe jest filtrowanie użytkowników według kilku kryteriów. Kliknij **Dodaj filtr** i wybierz typ filtra z menu rozwijanego lub wprowadź ciąg (powtórz czynność podczas łączenia wielu kryteriów):

Dodaj filtr	Sposób użycia
Czynność	Wybierz jedną z dostępnych czynności.
Obiekt	Wpisz prawidłową nazwę obiektu.
Stan	Należy wybrać jedną z następujących opcji: Powodzenie, Niepowodzenie, Rozpoczęto lub Częściowo się powiodło
Użytkownik	Wpisz użytkownika, który wykonał zmiany.
Stopień szczegółowości	Wybierz poziom szczegółowości: Niska, Średnia lub Wysoka
Wystąpienie od / Wystąpienie do	Filtrowanie według czasu wystąpienia. Użyj opcji Wystąpienie od i kliknij datę, aby wyświetlić tylko rekordy nowsze niż określona data. Użyj Wystąpienie dla rekordów wcześniejszych niż lub użyj obu dla żądanego zakresu czasu.
Zainicjowano uruchomienie systemu	Filtruje zapisy wykonane przez system.

Prześlij opinię

Aby przesłać opinię, użyj paska narzędzi w prawym górnym rogu w konsoli ESET Cloud Office Security, umieść kursor myszy na pozycji **Pomoc**, a następnie kliknij pozycję **Prześlij opinię**, wybierz pozycję **Przekaż nam swoją opinię** (podziel się pomysłami i doświadczeniami) lub **Zgłoś problem lub błąd**.

Pomoc techniczna

Skorzystaj z poniższych łączy do informacji pomagających w rozwiązywaniu problemów, które można napotkać:

Przeszukaj bazę wiedzy ESET

Baza wiedzy ESET — zawiera odpowiedzi na często zadawane pytania oraz zalecane rozwiązania różnych problemów. Dzięki regularnej aktualizacji przez specjalistów z firmy ESET baza wiedzy jest bardzo skutecznym narzędziem do rozwiązywania różnego rodzaju problemów.

Odwiedź forum firmy ESET dotyczące zabezpieczeń

Forum pomocy technicznej — forum firmy ESET zapewnia użytkownikom produktów firmy ESET łatwy sposób uzyskiwania pomocy i pomagania innym. Można opublikować na nim dowolny problem lub pytanie związane z produktami ESET.

Kontakt z działem pomocy technicznej

Formularz pomocy technicznej ESET — wypełnij formularz, podając w nim swoje dane, w tym opis problemu.

Skontaktuj się z lokalnym partnerem firmy ESET, aby uzyskać pomoc

Skontaktuj się z lokalną pomocą techniczną firmy ESET — dane kontaktowe pomocy technicznej firmy ESET w swoim regionie można znaleźć w wiadomości e-mail dotyczącej licencji, otrzymanej od firmy ESET.

Wyślij opinię

Prześlij opinię — daj nam znać, co myślisz (podziel się pomysłami i doświadczeniami), lub zgłoś problem albo błąd.

Zaproponuj ulepszenie pomocy online

Możesz opublikować swoją ocenę i przekazać opinię na określony temat w pomocy online, klikając łącze **Czy te informacje były pomocne?** pod stroną pomocy. Daj nam znać, czy treść pomogła lub jak Twoim zdaniem twórca treści technicznych może ją poprawić.

Dostępność usług

Portal stanu ESET wyświetla bieżący stan usług chmurowych ESET, zaplanowane przestoje i historię incydentów. Jeśli występuje problem z obsługiwaną usługą ESET i nie widzisz jej na liście na Portalu stanu, skontaktuj się z działem pomocy technicznej firmy ESET.

Zespoły monitorujące weryfikują potencjalne problemy wewnętrznie, a potwierdzone incydenty są publikowane i aktualizowane ręcznie w celu zachowania wiarygodności i dokładności. W związku z tym pojawiają się one na Portalu stanu z niewielkim opóźnieniem. Nie możemy publikować krótkich incydentów, jeśli zostaną one rozwiązane przed ręcznym potwierdzeniem.

Security for ESET Cloud Office Security

Wprowadzenie

Celem tego dokumentu jest podsumowanie praktyk bezpieczeństwa i środków kontroli bezpieczeństwa stosowanych w programie ESET Cloud Office Security. Praktyki i środki kontroli bezpieczeństwa mają na celu ochronę poufności, integralności i dostępności informacji klientów. Należy pamiętać, że praktyki bezpieczeństwa i środki kontroli mogą ulec zmianie.

Zakres

Zakres niniejszego dokumentu ma na celu podsumowanie praktyk bezpieczeństwa i środków kontroli bezpieczeństwa infrastruktury ESET Cloud Office Security, ESET Business Account (zwanych dalej „EUNB”), ESET Data Framework, ESET LiveGrid, aktualizacji, ochrony przed spamem, infrastruktury ESET Dynamic Threat Defense, organizacji, personelu i procesów operacyjnych. Praktyki i kontrole bezpieczeństwa obejmują następujące elementy:

1. Polityki bezpieczeństwa informacji
2. Organizacja bezpieczeństwa informacji
3. Bezpieczeństwo zasobów ludzkich
4. Zarządzanie aktywami
5. Kontrola dostępu
6. Kryptografia

7. Bezpieczeństwo fizyczne i środowiskowe
8. Bezpieczeństwo operacyjne
9. Bezpieczeństwo komunikacji
10. Pozyskiwanie, rozwój i konserwacja systemów
11. Relacje z dostawcą
12. Zarządzanie incydentami związanymi z bezpieczeństwem informacji
13. Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
14. Zgodność z przepisami

Koncepcja bezpieczeństwa

Firma ESET s.r.o. posiada certyfikat ISO 27001:2013 z zakresem zintegrowanego systemu zarządzania wyraźnie obejmującym ESET Cloud Office Security, EBA i inne usługi.

W związku z tym, koncepcja bezpieczeństwa informacji wdraża warstwową ochronną strategię bezpieczeństwa zgodną z normą ISO 27001 podczas stosowania kontroli bezpieczeństwa na poziomie sieci, systemów operacyjnych, baz danych, aplikacji, personelu i procesów operacyjnych. Stosowane praktyki bezpieczeństwa i środki kontroli w zakresie ochrony mają się na siebie nakładać i uzupełniać.

Praktyki bezpieczeństwa i środki kontroli

1. Polityki bezpieczeństwa informacji

Firma ESET korzysta z polityk bezpieczeństwa informacji, aby objąć wszystkie aspekty normy ISO 27001, w tym zarządzanie bezpieczeństwem informacji oraz mechanizmy kontroli i praktyki w zakresie bezpieczeństwa. Zasady są poddawane corocznemu przeglądowi i aktualizowane po istotnych zmianach, aby zapewnić ich ciągłą przydatność, adekwatność i skuteczność.

Firma ESET przeprowadza coroczne przeglądy tej polityki i wewnętrzne kontrole bezpieczeństwa w celu zapewnienia zgodności z nią. Nieprzestrzeganie zasad polityki bezpieczeństwa informacji podlega działaniom dyscyplinarnym wobec pracowników firmy ESET lub karom umownym do momentu rozwiązania umowy z dostawcami.

2. Organizacja bezpieczeństwa informacji

Organizacja zabezpieczenia informacji dla ESET Cloud Office Security obejmuje wiele zespołów i osób zaangażowanych w bezpieczeństwo informacji oraz IT, w tym:

- Kierownictwo wykonawcze ESET
- Zespoły ds. bezpieczeństwa wewnętrznego ESET
- Zespoły IT ds. aplikacji biznesowych
- Inne zespoły wspierające

Obowiązki w zakresie zabezpieczenia informacji są przydzielane zgodnie z obowiązującymi politykami zabezpieczenia informacji. Procesy wewnętrzne identyfikuje się i ocenia pod kątem ryzyka nieautoryzowanej lub niezamierzonej modyfikacji lub niewłaściwego użycia zasobów firmy ESET. Ryzykowne lub wrażliwe działania procesów wewnętrznych przyjmują zasadę podziału obowiązków w celu ograniczenia ryzyka.

Zespół prawny ESET jest odpowiedzialny za kontakty z organami rządowymi, w tym z polskimi organami regulacyjnymi w zakresie cyberbezpieczeństwa i ochrony danych osobowych. Zespół ds. bezpieczeństwa wewnętrznego firmy ESET jest odpowiedzialny za kontaktowanie się ze stowarzyszeniami specjalistycznymi, takimi jak ISACA. Zespół laboratorium badawczego firmy ESET jest odpowiedzialny za komunikację z innymi

firmami zajmującymi się bezpieczeństwem i większą społecznością zajmującą się cyberbezpieczeństwem.

Bezpieczeństwo informacji jest uwzględniane w zarządzaniu projektami przy użyciu stosowanych ram zarządzania projektami obejmujących etapy od koncepcji do zakończenia projektu.

Praca zdalna i telepraca są objęte polityką wdrożoną na urządzeniach mobilnych, która obejmuje stosowanie silnej kryptograficznej ochrony danych na urządzeniach mobilnych podczas podróży przez niezaufane sieci. Mechanizmy kontroli bezpieczeństwa na urządzeniach przenośnych są zaprojektowane do działania niezależnie od wewnętrznych sieci i systemów ESET.

3. Bezpieczeństwo zasobów ludzkich

Firma ESET stosuje standardowe praktyki w zakresie zasobów ludzkich, w tym polityki mające na celu utrzymanie bezpieczeństwa informacji. Praktyki te obejmują cały cykl życia pracownika i mają zastosowanie do wszystkich zespołów, które uzyskują dostęp do środowiska ESET Cloud Office Security.

4. Zarządzanie aktywami

Infrastruktura ESET Cloud Office Security jest uwzględniana w inwentarzu zasobów ESET ze ścisłą własnością i regułami stosowanymi odpowiednio do typu i wrażliwości zasobów. ESET ma zdefiniowany wewnętrzny schemat klasyfikacji. Wszystkie dane i konfiguracje ESET Cloud Office Security są klasyfikowane jako poufne.

5. Kontrola dostępu

Polityka kontroli dostępu firmy ESET reguluje każdy dostęp w programie ESET Cloud Office Security. Kontrola dostępu jest ustawiana na poziomie infrastruktury, usług sieciowych, systemu operacyjnego, bazy danych i aplikacji. Pełne zarządzanie dostępem użytkowników na poziomie aplikacji jest autonomiczne. Logowanie jednokrotne w ESET Cloud Office Security i ESET Business Account jest zarządzane przez centralnego dostawcę tożsamości, który zapewnia, że użytkownik może uzyskać dostęp tylko do autoryzowanej dzierżawy. Aplikacja używa standardowych uprawnień ESET Cloud Office Security do wymuszania kontroli dostępu opartej na rolach dla dzierżawy.

Dostęp do zaplecza ESET jest ściśle ograniczony do upoważnionych osób i ról. Standardowe procesy ESET dotyczące (de)rejestracji użytkowników, (de)aprowizacji, zarządzania uprawnieniami i przeglądu praw dostępu użytkowników służą do zarządzania dostępem pracowników ESET do infrastruktury ESET Cloud Office Security i do sieci.

Silne uwierzytelnianie ma na celu ochronę dostępu do wszystkich danych ESET Cloud Office Security.

6. Kryptografia

Aby chronić dane ESET Cloud Office Security, stosuje się silną kryptografię do szyfrowania danych w spoczynku i podczas przesyłania. Korzystanie z usług urzędu certyfikacji cieszących się powszechnym uznaniem w zakresie wystawiania certyfikatów dla usług publicznych. Wewnętrzna infrastruktura kluczy publicznych ESET służy do zarządzania kluczami w infrastrukturze ESET Cloud Office Security. Dane przechowywane w bazie danych są chronione przez klucze szyfrujące wygenerowane w chmurze. Wszystkie dane kopii zapasowych są chronione przez klucze zarządzane przez ESET.

7. Bezpieczeństwo fizyczne i środowiskowe

Ponieważ ESET Cloud Office Security i ESET Business Account są oparte na chmurze, polegamy na Microsoft Azure w zakresie bezpieczeństwa fizycznego i środowiskowego. Microsoft Azure wykorzystuje certyfikowane centra danych z solidnymi fizycznymi środkami zabezpieczającymi. Fizyczna lokalizacja centrum danych zależy od wyboru

regionu przez klienta.

8. Bezpieczeństwo operacyjne

Usługa ESET Cloud Office Security jest obsługiwana za pomocą zautomatyzowanych środków opartych na ścisłych procedurach operacyjnych i szablonach konfiguracyjnych. Wszystkie zmiany, w tym zmiany konfiguracji i wdrażanie nowych pakietów, są zatwierdzane i testowane w dedykowanym środowisku testowym przed wdrożeniem w środowisku produkcyjnym. Środowiska programistyczne, testowe i produkcyjne są od siebie oddzielone. Dane ESET Cloud Office Security znajdują się tylko w środowisku produkcyjnym.

Środowisko ESET Cloud Office Security jest nadzorowane za pomocą monitorowania operacyjnego w celu szybkiego identyfikowania problemów i zapewnienia wystarczającej pojemności wszystkim usługom na poziomie sieci i hosta.

Wszystkie dane konfiguracyjne są przechowywane w naszych regularnie archiwizowanych repozytoriach, aby umożliwić automatyczne odzyskiwanie konfiguracji środowiska. Kopie zapasowe danych ESET Cloud Office Security są przechowywane zarówno na miejscu, jak i poza nim.

Kopie zapasowe są szyfrowane i regularnie testowane pod kątem możliwości odzyskania w ramach testów ciągłości działania.

Audyt systemów odbywa się zgodnie z wewnętrznymi standardami i wytycznymi. Dzienniki i zdarzenia dotyczące infrastruktury, systemu operacyjnego, bazy danych, serwerów aplikacji i mechanizmów kontroli bezpieczeństwa są zbierane w sposób ciągły. Dzienniki są następnie przetwarzane przez zespoły IT i zespoły ds. bezpieczeństwa wewnętrznego w celu identyfikacji anomalii operacyjnych i bezpieczeństwa oraz incydentów związanych z bezpieczeństwem informacji.

Firma ESET wykorzystuje ogólny proces zarządzania lukami technicznymi do obsługi występowania luk w zabezpieczeniach w infrastrukturze ESET, w tym ESET Cloud Office Security oraz w innych produktach ESET. Proces ten obejmuje proaktywne skanowanie luk w zabezpieczeniach i powtarzające się testy penetracyjne infrastruktury, produktów i aplikacji.

Firma ESET określa wewnętrzne wytyczne dotyczące bezpieczeństwa infrastruktury wewnętrznej, sieci, systemów operacyjnych, baz danych, serwerów aplikacji i aplikacji. Wytyczne te są sprawdzane za pomocą monitorowania zgodności technicznej i naszego wewnętrznego programu audytu zabezpieczeń informacji.

9. Bezpieczeństwo komunikacji

Środowisko ESET Cloud Office Security jest segmentowane za pomocą natywnej segmentacji chmury z dostępem do sieci ograniczonym tylko do niezbędnych usług między segmentami sieci. Dostępność usług sieciowych osiąga się za pomocą natywnych kontroli w chmurze, takich jak strefy dostępności, równoważenie obciążenia i nadmiarowość. Dedykowane składniki równoważenia obciążenia są wdrażane w celu zapewnienia określonych punktów końcowych dla routingu instancji ESET Cloud Office Security, które wymuszają autoryzację ruchu i równoważenie obciążenia. Ruch sieciowy jest stale monitorowany pod kątem anomalii dotyczących działania i bezpieczeństwa. Potencjalnym atakom można zapobiegać, korzystając z natywnych mechanizmów kontroli w chmurze lub wdrożonych rozwiązań zabezpieczających. Cała komunikacja sieciowa jest szyfrowana za pomocą ogólnie dostępnych technik, w tym IPsec i TLS.

10. Pozyskiwanie, rozwój i konserwacja systemów

Rozwój systemów ESET Cloud Office Security odbywa się zgodnie z polityką bezpiecznego rozwoju oprogramowania firmy ESET. Zespoły ds. bezpieczeństwa wewnętrznego są włączone do projektu rozwojowego ESET Cloud Office Security od początkowej fazy i pomijają wszystkie działania związane z rozwojem i utrzymaniem.

Zespół ds. bezpieczeństwa wewnętrznego definiuje i sprawdza spełnienie wymagań bezpieczeństwa na różnych etapach tworzenia oprogramowania. Bezpieczeństwo wszystkich usług, w tym nowo opracowanych, jest testowane w sposób ciągły po jego wydaniu.

11. Relacje z dostawcą

Odpowiednie relacje z dostawcą są utrzymywane zgodnie z obowiązującymi wytycznymi firmy ESET, które obejmują całość zarządzania relacjami i wymagania umowne z punktu widzenia bezpieczeństwa informacji i prywatności. Jakość i bezpieczeństwo usług świadczonych przez dostawcę usług o znaczeniu krytycznym są regularnie oceniane.

12. Zarządzanie bezpieczeństwem informacji

Zarządzanie incydentami w zakresie bezpieczeństwa informacji w ESET Cloud Office Security odbywa się podobnie jak w przypadku innych infrastruktur firmy ESET i opiera się na zdefiniowanych procedurach reagowania na incydenty. Role w zakresie reagowania na incydenty są definiowane i przydzielane wielu zespołom, w tym zespołowi IT, zespołowi ds. zabezpieczeń, działowi prawnemu, HR, public relations i członkom zarządzania wykonawczego. Skład zespołu reagowania na incydenty jest ustalany na podstawie klasyfikacji incydentów przez zespół ds. bezpieczeństwa wewnętrznego. Zespół ten zapewni dalszą koordynację innych zespołów zajmujących się incydentem. Zespół ds. bezpieczeństwa wewnętrznego jest również odpowiedzialny za gromadzenie dowodów i wyciąganie wniosków. Informacje o wystąpieniu i rozwiązaniu incydentu są przekazywane zainteresowanym stronom. Zespół prawny firmy ESET jest odpowiedzialny za powiadamianie organów regulacyjnych w razie potrzeby zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO) i ustawą o cyberbezpieczeństwie przy transpozycji dyrektywy w sprawie bezpieczeństwa sieci i informacji (NIS).

13. Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania

Ciągłość działania usługi ESET Cloud Office Security jest zakodowana w solidnej architekturze służącej do maksymalizacji dostępności świadczonych usług. Całkowite przywrócenie z kopii zapasowych i danych konfiguracyjnych poza siedzibą firmy jest możliwe w przypadku katastrofalnej awarii wszystkich nadmiarowych węzłów dla komponentów ESET Cloud Office Security lub usługi ESET Cloud Office Security. Proces przywracania jest regularnie testowany.

14. Zgodność z przepisami

Zgodność z wymogami regulacyjnymi i umownymi ESET Cloud Office Security jest poddawana regularnym ocenom oraz przeglądom podobnie jak w przypadku innych elementów infrastruktury oraz procesów ESET, a także podejmowane są niezbędne kroki w celu zapewnienia zgodności w sposób ciągły. Firma ESET jest zarejestrowana jako dostawca usług cyfrowych dla usługi cyfrowej Cloud Computing obejmującej wiele usług ESET, w tym ESET Cloud Office Security. Należy pamiętać, że działania firmy ESET w zakresie zgodności niekoniecznie oznaczają, że są spełnione ogólne wymagania klientów dotyczące zgodności.

Warunki korzystania

Obowiązuje od 23 października 2023 r. | Zobacz poprzednią wersję Warunków użytkowania | Porównaj zmiany

Niniejsza Umowa ESET Cloud Office Security (zwana dalej „Warunkami”) stanowi specjalną umowę pomiędzy firmą ESET, spol. s r. o., z siedzibą pod adresem Einsteinova 24, 85101 Bratislava, Slovak Republic, zarejestrowaną w Rejestrze Handlowym prowadzonym przez I Sąd Rejonowy w Bratysławie, sekcja Sro, wpis nr 3586/B, numer rejestracyjny działalności gospodarczej: 31333532 (zwaną dalej „ESET” lub „Dostawcą”) a Tobą, osobą fizyczną lub prawną (zwaną dalej „Tobą” lub „Użytkownikiem”), która korzysta z konta w celu administracji, obsługi ESET

Cloud Office Security oraz która korzysta z portalu online kontrolowanego przez ESET (zwanego dalej „Kontem”) w celu korzystania z ESET Cloud Office Security. Jeśli Licencjobiorca korzysta z Konta i rozwiązania ESET Cloud Office Security (zwanych dalej łącznie „Produktem”) w imieniu organizacji, akceptuje niniejsze Warunki w jej imieniu oraz gwarantuje, że ma odpowiednie uprawnienia, aby zobowiązać tę organizację do przestrzegania tych Warunków. W takim przypadku określenie „Licencjobiorca” i „Użytkownik” odnosi się do tej organizacji. Należy uważnie zapoznać się z niniejszymi Warunkami. Odnoszą się one również do usług udostępnianych przez firmę ESET za pośrednictwem Produktu lub w związku z nim. Szczegółowe warunki korzystania z poszczególnych usług nieobjęte niniejszymi Warunkami omówiono w ramach każdej z usług, przy czym ich zaakceptowanie stanowi część procesu aktywacji usługi. Załączone aneksy uzupełniają niniejsze Warunki.

Bezpieczeństwo i ochrona danych

Konto zapewnia dostęp do usług udostępnianych przez firmę ESET. Do rejestracji i używania Konta oraz do konfiguracji i konserwacji usług dostępnych za jego pośrednictwem jest wymagane imię i nazwisko Licencjobiorcy, nazwa firmy, kraj, prawidłowy adres e-mail, numer telefonu, dane licencyjne oraz dane statystyczne. Niniejszym Licencjobiorca wyraża zgodę na gromadzenie danych i przesyłanie ich na serwery Dostawcy lub serwery jego partnerów. Celem takiego postępowania jest zapewnienie funkcjonalności i autoryzacja użycia Oprogramowania, a także ochrona praw Dostawcy. Po wyrażeniu zgody na niniejsze Warunki Dostawca lub jego partnerzy będą uprawnieni do przekazywania, przetwarzania i przechowywania kluczowych danych identyfikacyjnych Licencjobiorcy w celach związanych z udzielaniem pomocy technicznej i realizacją postanowień niniejszych Warunków. Licencjobiorca jest upoważniony do korzystania z Konta wyłącznie w takich celach i w taki sposób, jak określono to w niniejszych Warunkach, warunkach poszczególnych usług oraz dokumentacji.

Licencjobiorca ponosi odpowiedzialność za zapewnienie bezpieczeństwa swojego Konta ESET i poświadczeń potrzebnych do zalogowania się na nim. Firma ESET nie ponosi odpowiedzialności za żadne straty ani szkody powstałe w wyniku niewywiązania się przez Licencjobiorcę ze wspomnianego obowiązku zapewnienia bezpieczeństwa. Użytkownik ponosi również odpowiedzialność za wszelkie działania związane z użytkowaniem Konta bez względu na to, czy uzyskano ich zatwierdzenie. W razie naruszenia zabezpieczeń Konta Użytkownik powinien natychmiast powiadomić Dostawcę.

W celu świadczenia usługi administracji Kontem jest wymagane gromadzenie danych dotyczących zarządzanych urządzeń oraz informacji administracyjnych (dalej zwanych „Danymi”). Dane są przesyłane przez Użytkownika do firmy ESET wyłącznie na potrzeby usługi administrowania Kontem. Dane są przetwarzane i przechowywane zgodnie z zasadami i praktykami firmy ESET dotyczącymi zabezpieczeń, a także zgodnie z Polityką prywatności.

Szczegółowe informacje dotyczące prywatności, ochrony danych osobowych i praw Licencjobiorcy jako osoby, której dane dotyczą, zawiera Polityka prywatności.

Polityka właściwego użytkowania

Licencjobiorca jest zobowiązany do przestrzegania ograniczeń technicznych określonych w dokumentacji. Licencjobiorca zgadza się korzystać z Konta i jego funkcji w sposób, który nie ograniczy dostępu do tych usług innym użytkownikom. Dostawca zastrzega sobie prawo do ograniczenia zakresu usług udostępnianych konkretnym użytkownikom w celu zapewnienia możliwości korzystania z nich jak największej liczbie użytkowników. Ograniczenie zakresu usług może również oznaczać całkowitą blokadę funkcji Konta oraz usunięcie danych i informacji.

Szczegółowe informacje na temat ograniczeń technicznych można znaleźć w sekcji Ograniczenia.

Lokalizacja

Dostawca może zezwolić Licencjobiorcy na wybór z dostępnych lokalizacji hostingowych dla Konta, w tym zalecanej lokalizacji wybranej przez Dostawcę. Licencjobiorca zgadza się, że wybór lokalizacji innej niż zalecana może wpłynąć na sposób korzystania z usługi. Zależnie od wybranej lokalizacji, zastosowanie mogą mieć Umowa o ochronie danych zawarta w Aneksie nr 2 do niniejszej Umowy oraz Standardowe klauzule umowne zawarte w Aneksie nr 3 do niniejszej Umowy. ESET zastrzega sobie prawo do zmiany określonej lokalizacji w dowolnym czasie bez uprzedniego powiadomienia w celu ulepszania usług świadczonych przez ESET zgodnie z preferencjami użytkownika w zakresie lokalizacji (np. Unia Europejska).

Oprogramowanie

Prawa autorskie do wszystkich dostępnych w Produkcie elementów oprogramowania (zwanych dalej „Oprogramowaniem”) należą do firmy ESET lub jej odpowiednich dostawców bądź mogą być przez nich egzekwowane. Z Oprogramowania można korzystać tylko zgodnie z Umową Licencyjną Użytkownika Końcowego załączoną w postaci aneksu nr 1 do niniejszej Umowy. Inne informacje dotyczące licencji, praw autorskich, dokumentacji oraz znaków towarowych zamieszczono w Informacje prawne.

Ograniczenia

Licencjobiorca nie może kopiować, rozpowszechniać ani wyodrębniać składników Konta, jak również nie może tworzyć dzieł pochodnych na podstawie Konta. Korzystając z Konta, Licencjobiorca musi przestrzegać następujących ograniczeń:

(a) Licencjobiorca nie może używać, modyfikować, tłumaczyć ani odtwarzać Konta bądź przekazywać praw do korzystania z Konta lub jego składników w sposób inny niż wyszczególniony w niniejszych Warunkach.

(b) Licencjobiorca nie może sprzedawać Konta, udzielać na nie podlicencji, oddawać go w użytkowanie, wypożyczać go innym osobom ani pożyczać go od innych osób, a także nie może używać Konta w celu świadczenia usług o charakterze dochodowym.

(c) Licencjobiorca nie może podejmować prób odtworzenia kodu źródłowego Konta na drodze dekompilacji lub dezasemblacji ani w żaden inny sposób, chyba że pozwalają mu na to przepisy, które w stosownym zakresie wyraźnie znoszą niniejsze postanowienie.

(d) Licencjobiorca zobowiązuje się używać Konta w sposób zgodny z wszelkimi przepisami, które mają zastosowanie do Konta ze względu na właściwość terytorialną Licencjobiorcy, w tym między innymi ze stosownymi ograniczeniami dotyczącymi prawa autorskiego i innych praw własności intelektualnej.

Zrzeczenie się odpowiedzialności

LICENCJOBIORCA PRZYJMUJE KONTO ORAZ USŁUGI W STANIE TAKIM, W JAKIM ZOSTAŁY MU DOSTARCZONE, BEZ JAKICHKOLWIEK WYRAŹNYCH LUB DOROZUMIANYCH GWARANCJI, O ILE PRAWO WŁAŚCIWE TEGO NIE ZABRANIA. ANI DOSTAWCA, ANI JEGO LICENCJODAWCY CZY PODMIOTY STOWARZYSZONE, ANI WŁAŚCICIELE STOSOWNYCH PRAW AUTORSKICH NIE UDZIELAJĄ ŻADNYCH WYRAŹNYCH ANI DOROZUMIANYCH GWARANCJI, W TYM MIĘDZY INNYMI GWARANCJI PRZYDATNOŚCI HANDLOWEJ LUB PRZYDATNOŚCI DO OKREŚLONEGO CELU, JAK RÓWNIEŻ NIE GWARANTUJĄ, ŻE KONTO LUB USŁUGI NIE BĘDĄ NARUSZAĆ PRAW PATENTOWYCH, PRAW AUTORSKICH, PRAW DO ZNAKÓW TOWAROWYCH ANI INNYCH PRAW OSÓB TRZECICH. ANI DOSTAWCA, ANI ŻADNA INNA STRONA NIE GWARANTUJĄ, ŻE KONTO LUB USŁUGI SPEŁNIAJĄ WYMAGANIA LICENCJOBIORCY LUB ŻE DZIAŁANIE KONTA LUB USŁUG BĘDZIE NIEZAKŁÓCONE I POZBAWIONE BŁĘDÓW. WSZELKA ODPOWIEDZIALNOŚĆ ZA DOBÓR KONTA I USŁUG ODPOWIEDNICH DO OSIĄGNIĘCIA ZAMIERZONYCH CELÓW LICENCJOBIORCY ORAZ ZA ICH UŻYCIE

I ZA WYNIKI TEGO UŻYCIA, A TAKŻE RYZYKO WYNIKAJĄCE Z TEGO DOBORU I UŻYCIA SPOCZYWAJĄ NA LICENCJOBIORCY.

W niniejszych Warunkach określono wszystkie zobowiązania Dostawcy i jego licencjodawców.

Ograniczenie odpowiedzialności

W MAKSYMALNYM ZAKRESIE DOPUSZCZONYM PRZEZ PRAWO WŁAŚCIWE ANI DOSTAWCA, ANI JEGO PRACOWNICY CZY KONTRAHENCI NIE PONOSZĄ ŻADNEJ ODPOWIEDZIALNOŚCI ZA JAKIEKOLWIEK UTRATY ZYSKÓW, PRZYCHODÓW, ŹRÓDEŁ PRZYCHODÓW LUB DANYCH, SZKODY MAJĄTKOWE LUB OBRAŻENIA CIAŁA, ZAKŁÓCENIA DZIAŁALNOŚCI PRZEDSIĘBIORSTWA, UTRATY DANYCH HANDLOWYCH CZY JAKIEKOLWIEK SZKODY SZCZEGÓLNE, BEZPOŚREDNIE, POŚREDNIE, UBOCZNE, GOSPODARCZE, MORALNE LUB WYNIKOWE, JAK RÓWNIEŻ NIE BĘDĄ PONOSIĆ KOSZTÓW NABYCIA ZASTĘPCZYCH TOWARÓW LUB USŁUG ANI POKRYWAĆ RÓŻNIC MIĘDZY CENAMI KONTRAKTOWYMI A CENAMI TRANSAKCJI. ZASTRZEŻENIE OKREŚLONE W POWYŻSZYM ZDANIU MA ZASTOSOWANIE BEZ WZGLĘDU NA PRZYCZYNĘ POWSTANIA SZKODY I NA TO, CZY EWENTUALNE ROSZCZENIE ZOSTAŁO ZGŁOSZONE NA PODSTAWIE UMOWY, PRZEPISÓW O CZYNACH NIEDOZWOLONYCH, PRZEPISÓW DOTYCZĄCYCH ZANIEDBAŃ CZY NA JAKIEJKOLWIEK INNEJ PODSTAWIE ORAZ CZY ZOSTAŁO ONO ZGŁOSZONE W ZWIĄZKU Z UŻYCIEM, CZY Z NIEMOŻNOŚCIĄ UŻYCIA KONTA. ZASTRZEŻENIE TO MA ZASTOSOWANIE TAKŻE WÓWCZAS, GDY DOSTAWCA LUB JEGO KONTRAHENCI BĄDŹ PODMIOTY STOWARZYSZONE ZOSTALI POWIADOMIENI O MOŻLIWOŚCI WYSTĄPIENIA DANEJ SZKODY. W PRZYPADKU JURYSDYKCJI, KTÓRE NIE ZEZWALAJĄ NA WYŁĄCZENIE ODPOWIEDZIALNOŚCI ODSZKODOWAWCZEJ, LECZ DOPUSZCZAJĄ JEJ OGRANICZENIE, ODPOWIEDZIALNOŚĆ DOSTAWCY, JEGO PRACOWNIKÓW, KONTRAHENTÓW LUB PODMIOTÓW STOWARZYSZONYCH JEST OGRANICZONA DO KWOTY ZAPŁACONEJ PRZEZ LICENCJOBIORCĘ ZA LICENCJE.

Zgodność z przepisami o kontroli handlu

(a) Licencjobiorca nie będzie, bezpośrednio ani pośrednio, eksportować, reeksportować, przekazywać lub w inny sposób udostępniać Oprogramowania jakiejkolwiek osobie, nie będzie używać go w jakikolwiek sposób, ani też nie będzie uczestniczyć w jakichkolwiek działaniach, które mogłyby spowodować, że firma ESET lub jej spółki holdingowe, spółki zależne oraz spółki zależne dowolnych z jej spółek holdingowych, jak również podmioty kontrolowane przez jej spółki holdingowe („Podmiotami stowarzyszonymi”), naruszyłyby przepisy o kontroli handlu, obejmujące:

i. wszelkie przepisy prawne, które kontrolują, ograniczają lub nakładają wymogi licencyjne na eksport, reeksport lub transfer towarów, oprogramowania, technologii lub usług, wydane lub przyjęte przez jakikolwiek rząd, stan lub organ regulacyjny Stanów Zjednoczonych, Singapuru, Wielkiej Brytanii, Unii Europejskiej lub dowolnego z jej państw członkowskich, albo jakikolwiek kraj, w którym mają być wykonywane zobowiązania wynikające z niniejszych Warunków lub w którym firma ESET lub dowolny z jej Podmiotów stowarzyszonych są zarejestrowane lub prowadzą działalność;

ii. wszelkie gospodarcze, finansowe (handlowe lub inne) sankcje, ograniczenia, embarga, zakazy importu lub eksportu, zakazy przekazywania funduszy lub aktywów bądź świadczenia usług, lub też równoważne środki nałożone przez jakikolwiek rząd, stan lub organ regulacyjny Stanów Zjednoczonych, Singapuru, Wielkiej Brytanii, Unii Europejskiej lub dowolnego z jej państw członkowskich, albo jakikolwiek kraj, w którym mają być wykonywane zobowiązania wynikające z niniejszych Warunków lub w którym firma ESET lub dowolny z jej Podmiotów stowarzyszonych są zarejestrowane lub prowadzą działalność (akty prawne, o których mowa w pkt i i ii powyżej, łącznie nazywane są „Przepisami dotyczącymi kontroli handlu).

(b) Firma ESET ma prawo zawiesić swoje zobowiązania wynikające z niniejszych Warunków lub wypowiedzieć je ze skutkiem natychmiastowym w następujących przypadkach:

i. Gdy firma ESET stwierdzi na podstawie stosownego uzasadnienia, że Użytkownik naruszył lub może naruszyć

postanowienie punktu (a) klauzuli dotyczącej zgodności z przepisami o kontroli handlu w niniejszych Warunkach; lub

ii. Gdy Użytkownik końcowy i/lub Oprogramowanie podlegają przepisom o kontroli handlu i w związku z tym firma ESET stwierdzi na podstawie stosownego uzasadnienia, że dalsze wykonywanie zobowiązań wynikających z niniejszych Warunków mogłoby spowodować, że firma ESET lub jej Podmioty stowarzyszone naruszyłyby przepisy o kontroli handlu lub byłyby narażone na negatywne konsekwencje wynikające z tych przepisów.

(c) Żadne z postanowień niniejszych Warunków nie ma na celu ani nie powinno być interpretowane lub odczytywane jako nakłanianie bądź wymaganie od którejkolwiek ze stron działania lub powstrzymania się od działania (albo wyrażenia zgody na działanie lub powstrzymanie się od działania) w sposób niezgodny z obowiązującymi przepisami o kontroli handlu, zabroniony przez te przepisy lub podlegający karze w związku z tymi przepisami.

Prawo właściwe i język

Wykładnią niniejszych Warunków jest prawo obowiązujące na terenie Słowacji. Użytkownik końcowy i Dostawca stwierdzają, że do niniejszych Warunków nie mają zastosowania reguły kolizyjne ani Konwencja Organizacji Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów. Konsumenci mający miejsce zwykłego pobytu w UE mają również zapewnioną dodatkową ochronę przez przepisy prawa bezwzględnie obowiązujące w ich kraju zamieszkania.

Licencjobiorca wyraźnie stwierdza, że wszelkie spory lub roszczenia względem Dostawcy wynikające z wyrażenia zgody na niniejsze Warunki, jak również wszelkie spory lub roszczenia związane z użyciem Oprogramowania, Konta lub Usług bądź wynikające z niniejszych Warunków bądź Warunków szczególnych (jeśli dotyczy) będą rozstrzygane przez Sąd Rejonowy dla okręgu Bratislava I. Licencjobiorca wyraźnie poddaje się jurysdykcji tego sądu. Konsumenci mający miejsce zwykłego pobytu w UE mają prawo wnieść roszczenie w celu egzekwowania swoich praw konsumenckich w miejscu wyłącznej jurysdykcji lub w kraju UE, w którym mieszkają. Ponadto mogą również skorzystać z platformy internetowego rozstrzygania sporów, do której można uzyskać dostęp tutaj: https://ec.europa.eu/consumers/odr/. Jednak przed oficjalnym wniesieniem jakiegokolwiek roszczenia warto rozważyć kontakt z nami.

W przypadku jakichkolwiek rozbieżności między wersjami językowymi niniejszych Warunków pierwszeństwo zawsze ma wersja angielska dostępna tutaj.

Postanowienia ogólne

Firma ESET zastrzega sobie prawo do modyfikowania niniejszych Warunków oraz dokumentacji lub dowolnej ich części w dowolnym czasie poprzez aktualizowanie odpowiednich dokumentów odzwierciedlające zmiany wprowadzone w obowiązującym prawie lub Koncie. Licencjobiorca będzie powiadamiany o wszelkich zmianach w niniejszych Warunkach przez Konto. Jeśli Licencjobiorca nie wyrazi zgody na te zmiany, może anulować Konto. Do czasu anulowania konta po otrzymaniu powiadomienia o takich zmianach Licencjobiorca jest zobowiązany do przestrzegania wszelkich zmian lub modyfikacji wprowadzanych w niniejszych Warunkach. Zachęcamy Licencjobiorcę do okresowego odwiedzania niniejszej strony w celu zapoznawania się z aktualną treścią niniejszych Warunków, które regulują sposób korzystania z Konta.

Zawiadomienia

Wszystkie zawiadomienia należy kierować na adres: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Aneks nr 1

Umowę Licencyjną Użytkownika Końcowego

Aneks nr 2

Umowa o przetwarzaniu danych

Aneks nr 3

Standardowe klauzule umowne

Umowa licencyjna użytkownika końcowego

WAŻNE: Przed pobraniem, zainstalowaniem, skopiowaniem lub użyciem Oprogramowania należy się dokładnie zapoznać z poniższymi warunkami korzystania z produktu. **POBRANIE, ZAINSTALOWANIE, SKOPIOWANIE LUB UŻYCIE OPROGRAMOWANIA OZNACZA WYRAŻENIE ZGODY NA NINIEJSZE WARUNKI I AKCEPTACJĘ DOKUMENTU POLITYKA PRYWATNOŚCI.**

Umowę Licencyjną Użytkownika Końcowego

Niniejsza Umowa licencyjna użytkownika końcowego (w dalszej części nazywana „Umową”), zawierana między spółką ESET, spol. s r. o., z siedzibą w Słowacji pod adresem Einsteinova 24, 851 01 Bratislava, Slovak Republic, zarejestrowaną w Rejestrze Handlowym Sądu Rejonowego dla okręgu Bratislava I, w sekcji Sro pod numerem 3586/B, numer w rejestrze przedsiębiorców: 31333532 (w dalszej części nazywaną „firmą ESET” lub „Dostawcą”), a licencjobiorcą, który jest osobą fizyczną lub prawną (w dalszej części nazywanym „Licencjobiorcą” lub „Użytkownikiem końcowym”), uprawnia Licencjobiorcę do korzystania z Oprogramowania określonego w punkcie 1 niniejszej Umowy. Oprogramowanie określone w punkcie 1 niniejszej Umowy może znajdować się na nośniku danych albo zostać przesłane pocztą elektroniczną, pobrane z Internetu, pobrane z serwerów Dostawcy lub uzyskane z innych źródeł na warunkach wyszczególnionych poniżej.

NINIEJSZA UMOWA DOTYCZY WYŁĄCZNIE OKREŚLENIA PRAW UŻYTKOWNIKA KOŃCOWEGO I NIE STANOWI UMOWY SPRZEDAŻY. Dostawca pozostaje właścicielem kopii Oprogramowania i nośnika fizycznego zawartego w opakowaniu z produktem, a także wszystkich innych kopii Oprogramowania, które Użytkownik końcowy może wykonać zgodnie z niniejszą Umową.

Kliknięcie opcji „Akceptuję” lub „Akceptuję...” w trakcie instalowania, pobierania, kopiowania lub używania Oprogramowania oznacza, że Licencjobiorca wyraża zgodę na warunki określone w niniejszej Umowie. Jeśli Licencjobiorca nie wyraża zgody na którykolwiek warunek określony w niniejszej Umowie, powinien niezwłocznie kliknąć opcję anulowania i przerwać instalację lub pobieranie albo zniszczyć Oprogramowanie, nośnik instalacyjny, dokumentację towarzyszącą Oprogramowaniu i dowód sprzedaży Oprogramowania bądź zwrócić je Dostawcy lub w miejscu zakupu Oprogramowania.

LICENCJOBIORCA PRZYJMUJE DO WIADOMOŚCI, ŻE KORZYSTANIE Z OPROGRAMOWANIA OZNACZA ZAPOZNANIE SIĘ Z NINIEJSZĄ UMOWĄ, ZROZUMIENIE WARUNKÓW W NIEJ OKREŚLONYCH ORAZ ZOBOWIĄZANIE DO ICH PRZESTRZEGANIA.

1. **Oprogramowanie.** W niniejszej Umowie termin „Oprogramowanie” oznacza: (i) program komputerowy, do którego dołączono niniejszą Umowę, i wszystkie jego składniki; (ii) całą zawartość dysków, płyt CD-ROM i płyt DVD, wiadomości e-mail wraz z ich załącznikami oraz innych nośników, do których jest dołączona niniejsza Umowa, w tym Oprogramowanie w formie kodu obiektowego dostarczone na nośniku danych albo za pośrednictwem poczty elektronicznej lub Internetu; (iii) wszelkie powiązane drukowane materiały instruktażowe oraz wszelką inną dokumentację powiązaną z Oprogramowaniem, w tym przede wszystkim wszelkie opisy Oprogramowania, jego dane techniczne, wszelkie opisy jego właściwości lub działania, wszelkie opisy środowiska

operacyjnego, w którym Oprogramowanie jest używane, instrukcje obsługi lub instalacji Oprogramowania oraz wszelkie opisy sposobu korzystania z Oprogramowania (w dalszej części nazywane „Dokumentacją"); (iv) wszelkie ewentualne kopie Oprogramowania, poprawki możliwych błędów Oprogramowania, dodatki do Oprogramowania, rozszerzenia Oprogramowania, zmodyfikowane wersje Oprogramowania oraz aktualizacje składników Oprogramowania, na które Dostawca udziela Licencjobiorcy licencji zgodnie z zapisami w punkcie 3 niniejszej Umowy. Oprogramowanie będzie dostarczane wyłącznie w postaci wykonywalnego kodu obiektowego.

2. **Instalacja, komputer i klucz licencyjny**. Oprogramowanie dostarczone na nośniku danych, otrzymane za pośrednictwem poczty elektronicznej, pobrane z Internetu, pobrane z serwerów Dostawcy lub uzyskane z innych źródeł musi zostać zainstalowane. Oprogramowanie należy zainstalować na prawidłowo skonfigurowanym komputerze, który spełnia minimalne wymagania określone w Dokumentacji. Procedurę instalacji również opisano w Dokumentacji. Na komputerze, na którym zostanie zainstalowane Oprogramowanie, nie można instalować sprzętu komputerowego ani programów komputerowych, które mogłyby niekorzystnie wpłynąć na Oprogramowanie. Komputer oznacza sprzęt, w tym między innymi komputery osobiste, laptopy, stacje robocze, palmtopy, smartfony, przenośne urządzenia elektroniczne lub inne urządzenia elektroniczne, dla których przeznaczone jest Oprogramowanie, na których zostanie zainstalowane i/lub będzie używane. Klucz licencyjny oznacza niepowtarzalny ciąg symboli, liter, cyfr i znaków specjalnych, dostarczony Użytkownikowi końcowemu w celu umożliwienia mu legalnego korzystania z Oprogramowania, jego określonych wersji lub rozszerzenia warunków Licencji zgodnie z niniejszą Umową.

3 **Licencja**. Dostawca udziela Licencjobiorcy praw określonych poniżej (w dalszej części nazywanych zbiorczo „Licencją"), jeśli Licencjobiorca zobowiązał się przestrzegać i przestrzega wszelkich warunków określonych w niniejszej Umowie:

a) **Instalacja i użycie.** Licencjobiorcy przysługują niewyłączne, nieprzenoszalne prawa do zainstalowania Oprogramowania na dysku twardym komputera lub na innym nośniku do trwałego przechowywania danych, do zainstalowania i przechowywania Oprogramowania w pamięci systemu komputerowego oraz do zaimplementowania, przechowywania i wyświetlania Oprogramowania.

b) **Postanowienia w sprawie liczby Licencji.** Prawo do korzystania z Oprogramowania w ramach jednej Licencji jest ograniczone do jednego Użytkownika końcowego. Jeden Użytkownik końcowy oznacza: (i) instalację Oprogramowania na jednym systemie komputerowym lub, jeśli liczba Licencji zależy od liczby skrzynek pocztowych, (ii) użytkownika komputera, który odbiera pocztę elektroniczną za pośrednictwem klienta poczty elektronicznej. Jeśli do klienta poczty elektronicznej dociera poczta elektroniczna, która jest następnie automatycznie dystrybuowana do innych użytkowników, liczbę Użytkowników końcowych stanowi liczba wszystkich użytkowników, do których jest dostarczana poczta. Jeśli serwer poczty pełni funkcję bramy pocztowej, liczba Użytkowników końcowych jest równa liczbie użytkowników serwera poczty, którzy są obsługiwani przez tę bramę. Jeśli jeden użytkownik odbiera pocztę przesyłaną na różne adresy e-mail (np. za pośrednictwem usługi aliasów), a liczba tych adresów jest nieokreślona i wiadomości nie są automatycznie dystrybuowane przez klienta poczty elektronicznej do większej liczby użytkowników, wymagana jest Licencja na jednego użytkownika komputera. Z jednej Licencji można korzystać każdorazowo tylko na jednym komputerze. Użytkownik końcowy może wprowadzić klucz licencyjny do Oprogramowania tylko w zakresie, w jakim przysługuje mu prawo do korzystania z Oprogramowania zgodnie z ograniczeniami wynikającymi z liczby Licencji przyznanych przez Dostawcę. Klucz licencyjny ma charakter poufny, Licencjobiorca nie może udostępniać Licencji stronom trzecim ani pozwalać im na używanie klucza licencyjnego, o ile nie dopuszcza tego niniejsza Umowa lub Dostawca. W przypadku naruszenia klucza licencyjnego należy bezzwłocznie powiadomić Dostawcę.

c) **Wersja Business Edition.** W przypadku zamiaru zainstalowania i użycia Oprogramowania na serwerze poczty, w systemie przekazywania wiadomości e-mail lub w połączeniu z bramą pocztową bądź internetową wymagane jest nabycie wersji Business Edition Oprogramowania.

d) **Okres obowiązywania Licencji**. Prawo do korzystania z Oprogramowania jest ograniczone w czasie.

e) **Oprogramowanie dostarczone przez producenta urządzenia (OEM)**. Prawo do korzystania z Oprogramowania, które zostało dostarczone przez producenta zakupionego urządzenia (OEM, Original Equipment Manufacturer), jest ograniczone do tego urządzenia. Prawa tego nie można przenosić na inne urządzenia.

f) **Oprogramowanie w wersji próbnej lub nieprzeznaczonej do obrotu handlowego**. Nie można pobierać opłat za korzystanie z Oprogramowania, które jest oznaczone napisem „Not for resale" lub „NFR" (Nie do sprzedaży) albo „TRIAL" (Wersja próbna). Oprogramowanie takie jest przeznaczone wyłącznie do prezentacji lub testowania jego funkcji.

g) **Wygaśnięcie Licencji**. Licencja wygasa automatycznie po upływie okresu jej obowiązywania. Jeśli Licencjobiorca naruszył którekolwiek z postanowień niniejszej Umowy, Dostawca jest uprawniony do rozwiązania niniejszej Umowy oraz do wykonania wszelkich innych praw i zastosowania wszelkich innych środków prawnych przysługujących mu w takiej sytuacji. W razie anulowania Licencji Licencjobiorca musi natychmiast usunąć lub zniszczyć Oprogramowanie i wszystkie jego kopie zapasowe lub zwrócić je na własny koszt do firmy ESET bądź w miejscu zakupu Oprogramowania. Po wygaśnięciu Licencji Dostawca jest też uprawniony do anulowania prawa Użytkownika końcowego do używania funkcji Oprogramowania, które wymagają połączenia z serwerami Dostawcy lub serwerami innych firm.

4.**Wymagania dotyczące funkcji gromadzących dane i połączenia z Internetem**. Aby Oprogramowanie działało poprawnie, wymagane jest stałe połączenie z Internetem oraz regularne połączenia z serwerami Dostawcy lub z serwerami innych firm, a gromadzenie potrzebnych danych powinno odbywać się zgodnie z obowiązującą Polityką prywatności. Połączenie z Internetem oraz gromadzenie potrzebnych danych są wymagane w przypadku następujących funkcji Oprogramowania:

a) **Aktualizacje Oprogramowania.** Dostawca jest uprawniony do wprowadzania w Oprogramowaniu zmian w formie aktualizacji (w dalszej części nazywanych „Aktualizacjami"), przy czym nie jest on ograniczony żadnymi terminami wprowadzenia takich zmian ani nie jest zobowiązany do ich wprowadzenia. Funkcja Aktualizacji jest domyślnie włączona w ustawieniach standardowych Oprogramowania, dlatego Aktualizacje są instalowane automatycznie, o ile Użytkownik końcowy nie zmienił ustawienia automatycznego instalowania Aktualizacji. W celu przeprowadzania aktualizacji wymagana jest weryfikacja autentyczności Licencji, w tym informacji dotyczących komputera i/lub platformy, na której zostało zainstalowane Oprogramowanie zgodnie z Polityką prywatności.

b) Przekazywanie szkodliwego oprogramowania i informacji o komputerze do Dostawcy. Oprogramowanie obejmuje funkcje, które gromadzą próbki wirusów komputerowych, innych szkodliwych programów komputerowych oraz podejrzanych, problematycznych, potencjalnie niepożądanych lub niebezpiecznych obiektów, takich jak pliki, adresy URL, pakiety IP oraz ramki Ethernet (odtąd ogólnie „Szkodliwe oprogramowanie"), po czym wysyłają je do Dostawcy. Wysyłane dane obejmują m.in. informacje o procesie instalacji, komputerze i/lub platformie, na której zainstalowano Oprogramowanie, a także informacje o działaniu i funkcjonalności Oprogramowania (odtąd ogólnie „Informacje"). Informacje oraz Szkodliwe oprogramowanie mogą obejmować dane Użytkownika końcowego (w tym jego dane osobowe pobrane losowo lub przypadkowo) lub dane innych użytkowników komputera, na którym zainstalowano Oprogramowanie, a także pliki uszkodzone przez Szkodliwe oprogramowanie wraz z powiązanymi z nimi metadanymi. Informacje oraz Szkodliwe oprogramowanie mogą być gromadzone przy użyciu następujących funkcji Oprogramowania:

i. Funkcja systemu reputacji LiveGrid służy do gromadzenia i wysyłania do Dostawcy jednokierunkowych skrótów związanych ze Szkodliwym oprogramowaniem. Funkcję tę można włączyć w ustawieniach standardowych Oprogramowania.

ii. System informacji zwrotnych LiveGrid służy do gromadzenia i wysyłania do Dostawcy Szkodliwego oprogramowania wraz z powiązanymi metadanymi, a także Informacji.

Dostawca może wykorzystać otrzymane Informacje oraz Szkodliwe oprogramowanie tylko w celu analizy

Szkodliwego oprogramowania, usprawnienia Oprogramowania i zweryfikowania autentyczności Licencji i jest zobowiązany do podjęcia stosownych środków gwarantujących zachowanie poufności Szkodliwego oprogramowania i Informacji. Włączenie tej funkcji Oprogramowania oznacza, że Dostawca może gromadzić i przetwarzać Szkodliwe oprogramowanie i Informacje zgodnie z Polityką prywatności i obowiązującymi przepisami prawa. Użytkownik może wyłączyć te funkcje w każdej chwili.

Na potrzeby niniejszej Umowy konieczne jest gromadzenie, przetwarzanie i przechowywanie danych umożliwiających Dostawcy identyfikację Licencjobiorcy zgodnie z Polityką prywatności. Licencjobiorca niniejszym zgadza się, aby Dostawca, korzystając z własnych środków, mógł sprawdzić, czy Licencjobiorca używa Oprogramowania zgodnie z postanowieniami niniejszej Umowy. Licencjobiorca zgadza się, że na potrzeby niniejszej Umowy konieczne jest przekazywanie jego danych podczas komunikacji pomiędzy Oprogramowaniem a systemami komputerowymi Dostawcy lub jego partnerów handlowych w ramach sieci dystrybucyjnej i wsparcia Dostawcy w celu zapewnienia funkcjonalności Oprogramowania i upoważnienia do używania Oprogramowania oraz ochrony praw Dostawcy.

Po zawarciu niniejszej Umowy Dostawca i każdy z jego partnerów handlowych, w ramach sieci dystrybucyjnej i wsparcia Dostawcy, będzie uprawniony do przekazywania, przetwarzania i przechowywania istotnych danych identyfikujących Licencjobiorcę w celach związanych z rozliczaniem opłat, wykonywaniem niniejszej Umowy i przekazywaniem powiadomień na komputerze Licencjobiorcy. Licencjobiorca niniejszym wyraża zgodę na otrzymywanie powiadomień i wiadomości, w tym między innymi informacji marketingowych.

Szczegółowe informacje na temat ochrony prywatności, danych osobowych i praw Licencjobiorcy jako podmiotu danych dostępne są w Polityce prywatności w witrynie Dostawcy, bezpośrednio podczas procesu instalacji. Można do niej przejść także z poziomu sekcji pomocy w Oprogramowaniu.

5. Okno **Wykonywanie praw Użytkownika końcowego**. Licencjobiorca może wykonywać swoje prawa wyłącznie osobiście lub za pośrednictwem swoich pracowników. Licencjobiorca może korzystać z Oprogramowania wyłącznie w celu zapewnienia ciągłości swojej działalności gospodarczej i w celu zabezpieczenia komputerów lub systemów komputerowych, na które uzyskał Licencję.

6. **Ograniczenie praw.** Licencjobiorca nie może kopiować, rozpowszechniać ani wyodrębniać składników Oprogramowania, jak również nie może tworzyć produktów na podstawie Oprogramowania (nie może wykonywać dzieł pochodnych). Korzystając z Oprogramowania, Licencjobiorca musi przestrzegać następujących ograniczeń:

a) Licencjobiorca może wykonać jedną kopię Oprogramowania na nośniku przeznaczonym do trwałego przechowywania danych i przechowywać tę kopię w charakterze archiwalnej kopii zapasowej, tj. nie może zainstalować ani użyć takiej kopii na żadnym komputerze. Wszelkie inne kopie Oprogramowania wykonane przez Licencjobiorcę stanowią naruszenie warunków określonych w niniejszej Umowie.

b) Licencjobiorca nie może używać, modyfikować, tłumaczyć ani odtwarzać Oprogramowania ani jego kopii w sposób inny niż wyszczególniony w niniejszej Umowie.

c) Licencjobiorca nie może sprzedawać Oprogramowania, udzielać na nie podlicencji, oddawać go w użytkowanie, wypożyczać go innym osobom ani pożyczać go od innych osób, a także nie może używać Oprogramowania w celu świadczenia usług o charakterze dochodowym.

d) Licencjobiorca nie może podejmować prób odtworzenia kodu źródłowego Oprogramowania na drodze dekompilacji lub dezasemblacji ani w żaden inny sposób, chyba że pozwalają mu na to przepisy, które w stosownym zakresie wyraźnie znoszą niniejsze postanowienie.

e) Licencjobiorca zobowiązuje się używać Oprogramowania w sposób zgodny z wszelkimi przepisami, które mają zastosowanie do Oprogramowania ze względu na właściwość terytorialną Licencjobiorcy, w tym między innymi ze

stosownymi ograniczeniami dotyczącymi prawa autorskiego i innych praw własności intelektualnej.

f) Licencjobiorca zgadza się korzystać z Oprogramowania i jego funkcji w sposób, który nie ograniczy dostępu do tych usług innym Użytkownikom końcowym. Dostawca zastrzega sobie prawo do ograniczenia zakresu usług udostępnianych konkretnym Użytkownikom końcowym w celu zapewnienia możliwości korzystania z nich jak największej liczbie Użytkowników końcowych. Ograniczenie zakresu usług może również oznaczać całkowitą blokadę funkcji Oprogramowania oraz usunięcie Danych i informacji przechowywanych na serwerach Dostawcy lub zewnętrznego podmiotu związanych z wybranymi funkcjami Oprogramowania.

g) Licencjobiorca zobowiązuje się nie podejmować działań obejmujących korzystanie z klucza licencyjnego, niezgodnych z postanowieniami niniejszej Umowy lub prowadzących do przekazania klucza licencyjnego osobie nieuprawnionej do korzystania z Oprogramowania, takich jak przekazanie wykorzystanego lub niewykorzystanego klucza licencyjnego w dowolnej formie, a także nieautoryzowana reprodukcja lub dystrybucja zduplikowanych lub wygenerowanych kluczy licencyjnych albo korzystanie z Oprogramowania w wyniku wykorzystania klucza licencyjnego uzyskanego z innego źródła niż Dostawca.

7. **Prawo autorskie**. Oprogramowanie i wszystkie prawa z nim związane, w tym między innymi prawa własności i prawa własności intelektualnej do Oprogramowania, należą do firmy ESET i/lub jej licencjodawców. Prawa te gwarantują zapisy traktatów międzynarodowych oraz wszelkie właściwe przepisy ustawowe obowiązujące w kraju, w którym jest używane Oprogramowanie. Struktura Oprogramowania, sposób jego zorganizowania i kod w nim zawarty są cennymi tajemnicami handlowymi oraz informacjami poufnymi firmy ESET i/lub jej licencjodawców. Licencjobiorca nie może kopiować Oprogramowania poza okolicznościami opisanymi w punkcie 6(a). Wszelkie kopie utworzone przez Licencjobiorcę zgodnie z niniejszą Umową muszą zawierać te same informacje o prawie autorskim i innych prawach własności, które znajdują się w Oprogramowaniu. Licencjobiorca niniejszym przyjmuje do wiadomości, że w razie naruszenia postanowień niniejszej Umowy przez podjęcie próby odtworzenia kodu źródłowego Oprogramowania na drodze dekompilacji lub dezasemblacji albo w inny sposób prawa do wszelkich informacji uzyskanych przez Licencjobiorcę w wyniku podjęcia takiej próby zostaną uznane za automatycznie i nieodwołalnie przeniesione w całości na Dostawcę już w momencie powstania takich informacji i to niezależnie od praw przysługujących Dostawcy w związku z naruszeniem przez Licencjobiorcę warunków określonych w niniejszej Umowie.

8. **Zastrzeżenie praw**. Dostawca niniejszym zastrzega sobie wszelkie prawa do Oprogramowania, z wyjątkiem praw wyraźnie udzielonych Licencjobiorcy, występującemu w charakterze Użytkownika końcowego, na podstawie niniejszej Umowy.

9. **Różne wersje językowe, Oprogramowanie obsługujące wiele urządzeń i wiele kopii Oprogramowania**. Jeśli Oprogramowanie może obsługiwać wiele platform lub języków bądź jeśli Licencjobiorca uzyskał wiele kopii Oprogramowania, Oprogramowania można używać tylko na tych systemach komputerowych i w tych wersjach, na które Licencjobiorca uzyskał Licencje. Licencjobiorca nie może sprzedawać wersji ani kopii Oprogramowania, których nie używa, jak również nie może ich oddawać w użytkowanie, udzielać na nie podlicencji, wypożyczać ich ani przenosić do nich praw na inne osoby.

10. **Rozpoczęcie i zakończenie obowiązywania Umowy**. Niniejsza Umowa wchodzi w życie z datą wyrażenia przez Licencjobiorcę zgody na warunki określone w tej Umowie. Licencjobiorca może rozwiązać niniejszą Umowę w dowolnej chwili przez trwałe odinstalowanie i zniszczenie Oprogramowania, wszystkich jego kopii zapasowych i wszelkich powiązanych materiałów dostarczonych przez Dostawcę lub jego partnerów handlowych bądź przez zwrócenie tych produktów na własny koszt. Bez względu na powód rozwiązania niniejszej Umowy po zakończeniu jej obowiązywania nadal obowiązują postanowienia zawarte w punktach 7, 8, 11, 13, 19 i 21.

11. **OŚWIADCZENIA UŻYTKOWNIKA KOŃCOWEGO**. LICENCJOBIORCA (WYSTĘPUJĄCY W CHARAKTERZE UŻYTKOWNIKA KOŃCOWEGO) PRZYJMUJE OPROGRAMOWANIE W STANIE TAKIM, W JAKIM ZOSTAŁO MU ONO DOSTARCZONE, BEZ JAKICHKOLWIEK WYRAŹNYCH LUB DOROZUMIANYCH GWARANCJI, O ILE PRAWO WŁAŚCIWE

TEGO NIE ZABRANIA. ANI WŁAŚCICIELE STOSOWNYCH PRAW AUTORSKICH NIE UDZIELAJĄ ŻADNYCH WYRAŹNYCH ANI DOROZUMIANYCH GWARANCJI, W TYM MIĘDZY INNYMI GWARANCJI PRZYDATNOŚCI HANDLOWEJ LUB PRZYDATNOŚCI DO OKREŚLONEGO CELU, JAK RÓWNIEŻ NIE GWARANTUJĄ, ŻE OPROGRAMOWANIE NIE BĘDZIE NARUSZAĆ PRAW PATENTOWYCH, PRAW AUTORSKICH, PRAW DO ZNAKÓW TOWAROWYCH ANI INNYCH PRAW OSÓB TRZECICH. ANI DOSTAWCA, ANI ŻADNA INNA OSOBA NIE GWARANTUJE, ŻE FUNKCJE OPROGRAMOWANIA SPEŁNIAJĄ WYMAGANIA LICENCJOBIORCY LUB ŻE DZIAŁANIE OPROGRAMOWANIA BĘDZIE NIEZAKŁÓCONE I POZBAWIONE BŁĘDÓW. LICENCJOBIORCA BIERZE NA SIEBIE WSZELKĄ ODPOWIEDZIALNOŚĆ I RYZYKO ZA DOBÓR OPROGRAMOWANIA ODPOWIEDNIEGO DO OSIĄGNIĘCIA CELÓW LICENCJOBIORCY ORAZ ZA PRZEPROWADZENIE INSTALACJI OPROGRAMOWANIA, ZA JEGO UŻYCIE I ZA WYNIKI TEGO UŻYCIA.

12. **Brak innych zobowiązań**. W niniejszej Umowie określono wszystkie zobowiązania Dostawcy i jego licencjodawców.

13. **OGRANICZENIE ODPOWIEDZIALNOŚCI**. O ILE PRAWO WŁAŚCIWE TEGO NIE ZABRANIA, ANI DOSTAWCA, ANI JEGO PRACOWNICY CZY LICENCJODAWCY NIE PONOSZĄ ŻADNEJ ODPOWIEDZIALNOŚCI ZA JAKIEKOLWIEK UTRATY ZYSKÓW, PRZYCHODÓW, ŹRÓDEŁ PRZYCHODÓW LUB DANYCH, SZKODY MAJĄTKOWE LUB OBRAŻENIA CIAŁA, ZAKŁÓCENIA DZIAŁALNOŚCI PRZEDSIĘBIORSTWA, UTRATY DANYCH HANDLOWYCH CZY JAKIEKOLWIEK SZKODY SZCZEGÓLNE, BEZPOŚREDNIE, POŚREDNIE, UBOCZNE, GOSPODARCZE, MORALNE LUB WYNIKOWE, JAK RÓWNIEŻ NIE BĘDĄ PONOSIĆ KOSZTÓW NABYCIA ZASTĘPCZYCH TOWARÓW LUB USŁUG ANI POKRYWAĆ RÓŻNIC MIĘDZY CENAMI KONTRAKTOWYMI A CENAMI TRANSAKCJI. ZASTRZEŻENIE OKREŚLONE W POWYŻSZYM ZDANIU MA ZASTOSOWANIE BEZ WZGLĘDU NA PRZYCZYNĘ POWSTANIA SZKODY I NA TO, CZY EWENTUALNE ROSZCZENIE ZOSTAŁO ZGŁOSZONE NA PODSTAWIE UMOWY, PRZEPISÓW O CZYNACH NIEDOZWOLONYCH, PRZEPISÓW DOTYCZĄCYCH ZANIEDBAŃ CZY NA JAKIEJKOLWIEK INNEJ PODSTAWIE ORAZ CZY ZOSTAŁO ONO ZGŁOSZONE W ZWIĄZKU Z UŻYCIEM, CZY Z NIEMOŻNOŚCIĄ UŻYCIA OPROGRAMOWANIA. ZASTRZEŻENIE TO MA ZASTOSOWANIE TAKŻE WÓWCZAS, GDY DOSTAWCA LUB JEGO LICENCJODAWCY BĄDŹ PODMIOTY STOWARZYSZONE ZOSTALI POWIADOMIENI O MOŻLIWOŚCI WYSTĄPIENIA DANEJ SZKODY. W PRZYPADKU JURYSDYKCJI, KTÓRE NIE ZEZWALAJĄ NA WYŁĄCZENIE ODPOWIEDZIALNOŚCI ODSZKODOWAWCZEJ, LECZ DOPUSZCZAJĄ JEJ OGRANICZENIE, ODPOWIEDZIALNOŚĆ DOSTAWCY, JEGO PRACOWNIKÓW, LICENCJODAWCÓW LUB PODMIOTÓW STOWARZYSZONYCH JEST OGRANICZONA DO KWOTY ZAPŁACONEJ PRZEZ LICENCJOBIORCĘ ZA LICENCJE.

14. Jeśli którekolwiek postanowienie niniejszej Umowy jest sprzeczne z ustawowymi prawami konsumenckimi jakiejkolwiek osoby, postanowienie to nie może być interpretowane w sposób naruszający te prawa.

15. **Pomoc techniczna**. Usługi pomocy technicznej świadczą wedle własnego uznania i bez udzielania jakichkolwiek gwarancji firma ESET lub inne firmy, którym firma ESET zleca świadczenie takich usług. Przed skorzystaniem z usługi pomocy technicznej Użytkownik końcowy musi utworzyć kopię zapasową wszystkich istniejących danych, programów i aplikacji. Ani firma ESET, ani inne firmy, którym firma ESET zleca świadczenie usług pomocy technicznej, nie mogą wziąć na siebie odpowiedzialności za uszkodzenie lub utratę danych, własności, oprogramowania lub urządzeń, jak również nie mogą odpowiadać za utratę zysków spowodowaną świadczeniem usług pomocy technicznej. Firma ESET i/lub inne firmy, którym firma ESET zleca świadczenie usług pomocy technicznej, zastrzegają sobie prawo do odmowy wykonania usługi, jeśli uznają, że nie mieści się ona w zakresie oferowanych usług pomocy technicznej. Firma ESET zastrzega sobie prawo do odmowy, wstrzymania lub zaprzestania świadczenia usług pomocy technicznej, jeśli uzna to za stosowne. Informacje dotyczące licencji, Informacje i inne dane zgodne z Polityką prywatności mogą być wymagane na potrzeby świadczenia pomocy technicznej.

16. **Przeniesienie Licencji**. Jeśli odpowiednie postanowienia niniejszej Umowy tego nie zabraniają, Oprogramowanie można przenosić między poszczególnymi systemami komputerowymi. O ile nie jest to sprzeczne z warunkami określonymi w niniejszej Umowie, za zgodą Dostawcy Użytkownik końcowy może trwale przenieść Licencję i wszelkie prawa przysługujące mu na podstawie niniejszej Umowy na innego Użytkownika końcowego, pod warunkiem że (i) nie zachowa dla siebie żadnych kopii Oprogramowania; (ii) przeniesienie praw będzie

bezpośrednie, tj. prawa zostaną przeniesione bezpośrednio na nowego Użytkownika końcowego; (iii) nowy Użytkownik końcowy przejmie na siebie wszystkie prawa i obowiązki wynikające z niniejszej Umowy, które miały dotąd zastosowanie do Użytkownika końcowego przenoszącego Licencję; (iv) nowy Użytkownik końcowy otrzyma od Użytkownika końcowego przenoszącego Licencję dokumentację, która umożliwi mu stwierdzenie zgodnie z zapisami w punkcie 17, czy Oprogramowanie jest oryginalne.

17. **Weryfikowanie oryginalności Oprogramowania**. Użytkownik końcowy może wykazać swoje uprawnienia do korzystania z Oprogramowania w jeden z poniższych sposobów: (i) na podstawie certyfikatu licencyjnego wystawionego przez Dostawcę lub inną firmę wskazaną przez Dostawcę; (ii) na podstawie pisemnej umowy licencyjnej, jeśli została ona zawarta; (iii) na podstawie wiadomości e-mail od Dostawcy z danymi dotyczącymi licencji (nazwą użytkownika i hasłem). Informacje dotyczące licencji oraz dane identyfikujące Użytkownika końcowego zgodne z Polityką prywatności mogą być wymagane w celu weryfikacji oryginalności Oprogramowania.

18. **Udzielanie Licencji organom władzy publicznej i rządowi USA**. Organy władzy publicznej, w tym rząd Stanów Zjednoczonych Ameryki Północnej, otrzymują Licencje na Oprogramowanie zgodnie z postanowieniami niniejszej Umowy, tj. z uwzględnieniem wszystkich praw i obowiązków określonych w niniejszej Umowie.

19. **Zgodność z przepisami o kontroli handlu**.

a) Licencjobiorca nie będzie, bezpośrednio ani pośrednio, eksportować, reeksportować, przekazywać lub w inny sposób udostępniać Oprogramowania jakiejkolwiek osobie, nie będzie używać go w jakikolwiek sposób, ani też nie będzie uczestniczyć w jakichkolwiek działaniach, które mogłyby spowodować, że firma ESET lub jej spółki holdingowe, spółki zależne oraz spółki zależne dowolnych z jej spółek holdingowych, jak również podmioty kontrolowane przez jej spółki holdingowe (zwane dalej „Podmiotami stowarzyszonymi"), naruszyłyby przepisy o kontroli handlu, obejmujące:

i. wszelkie przepisy prawne, które kontrolują, ograniczają lub nakładają wymogi licencyjne na eksport, reeksport lub transfer towarów, oprogramowania, technologii lub usług, wydane lub przyjęte przez jakikolwiek rząd, stan lub organ regulacyjny Stanów Zjednoczonych, Singapuru, Wielkiej Brytanii, Unii Europejskiej lub dowolnego z jej państw członkowskich, albo jakikolwiek kraj, w którym mają być wykonywane zobowiązania wynikające z Umowy lub w którym firma ESET lub dowolny z jej Podmiotów stowarzyszonych są zarejestrowane lub prowadzą działalność (zwane dalej „Przepisami o kontroli eksportu");

ii. wszelkie gospodarcze, finansowe (handlowe lub inne) sankcje, ograniczenia, embarga, zakazy importu lub eksportu, zakazy przekazywania funduszy lub aktywów bądź świadczenia usług, lub też równoważne środki nałożone przez jakikolwiek rząd, stan lub organ regulacyjny Stanów Zjednoczonych, Singapuru, Wielkiej Brytanii, Unii Europejskiej lub dowolnego z jej państw członkowskich, albo jakikolwiek kraj, w którym mają być wykonywane zobowiązania wynikające z Umowy lub w którym firma ESET lub dowolny z jej Podmiotów stowarzyszonych są zarejestrowane lub prowadzą działalność (zwane dalej „Przepisami o sankcjach").

b) Firma ESET ma prawo zawiesić swoje zobowiązania wynikające z niniejszych warunków lub wypowiedzieć je ze skutkiem natychmiastowym w następujących przypadkach:

i. Gdy firma ESET stwierdzi na podstawie stosownego uzasadnienia, że Użytkownik naruszył lub może naruszyć postanowienia punktu 19.a Umowy.

ii. Gdy Użytkownik końcowy i/lub Oprogramowanie podlegają przepisom o kontroli handlu i w związku z tym firma ESET stwierdzi na podstawie stosownego uzasadnienia, że dalsze wykonywanie zobowiązań wynikających z Umowy mogłoby spowodować, że firma ESET lub jej Podmioty stowarzyszone naruszyłyby przepisy o kontroli handlu lub byłyby narażone na negatywne konsekwencje wynikające z tych przepisów.

c) Żadne z postanowień Umowy nie ma na celu ani nie powinno być interpretowane lub odczytywane jako

nakłanianie bądź wymaganie od którejkolwiek ze stron działania lub powstrzymania się od działania (albo wyrażenia zgody na działanie lub powstrzymanie się od działania) w sposób niezgodny z obowiązującymi przepisami o kontroli handlu, zabroniony przez te przepisy lub podlegający karze w związku z tymi przepisami.

20. **Zawiadomienia**. Wszystkie zawiadomienia oraz zwroty Oprogramowania i Dokumentacji należy kierować na adres: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

21. **Prawo właściwe**. Niniejsza Umowa podlega przepisom prawnym obowiązującym w Słowacji i powinna być interpretowana zgodnie z tymi przepisami. Użytkownik końcowy i Dostawca niniejszym stwierdzają, że do niniejszej Umowy nie mają zastosowania przepisy dotyczące konfliktu praw ani Konwencja Organizacji Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów. Licencjobiorca wyraźnie stwierdza, że wszelkie spory lub roszczenia względem Dostawcy wynikające z zawarcia niniejszej Umowy, jak również wszelkie spory lub roszczenia związane z użyciem Oprogramowania będą rozstrzygane przez Sąd Rejonowy dla okręgu Bratislava I. Licencjobiorca wyraźnie poddaje się jurysdykcji tego sądu.

22. **Postanowienia ogólne**. Uznanie któregokolwiek z postanowień niniejszej Umowy za nieważne lub niewykonalne nie wpływa na ważność innych postanowień niniejszej Umowy, które pozostają wówczas w mocy zgodnie z warunkami określonymi w niniejszej Umowie. W przypadku rozbieżności pomiędzy wersjami językowymi niniejszej Umowy pierwszeństwo ma wersja angielska. Zmiana niniejszej Umowy musi mieć formę pisemną i musi zostać zatwierdzona podpisem złożonym przez upoważnionego przedstawiciela Dostawcy lub przez osobę wyraźnie upoważnioną do reprezentowania Dostawcy na zasadzie pełnomocnictwa.

Niniejsza Umowa stanowi całość porozumienia między Dostawcą a Licencjobiorcą w sprawie Oprogramowania i zastępuje wszelkie wcześniejsze oświadczenia, negocjacje, zobowiązania, wymiany zdań lub reklamy związane z Oprogramowaniem.

EULA ID: BUS-ECOS-20-01

Data Processing Agreement

Zgodnie z wymogami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, a także uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO”), dostawca (zwany dalej „Podmiotem przetwarzającym”) i właściciel (zwany dalej „Administratorem danych”) przystępują do stosunku umownego dotyczącego przetwarzania danych w celu określenia warunków przetwarzania danych osobowych, sposobu ich ochrony, a także innych praw i obowiązków obu stron w odniesieniu do przetwarzania danych osobowych osób, których dane dotyczą, w imieniu Administratora danych podczas wykonywania przedmiotu niniejszych Warunków jako umowy głównej.

1. **Przetwarzanie danych osobowych.** Usługi świadczone zgodnie z niniejszymi Warunkami mogą obejmować przetwarzanie danych dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, o których mowa w Polityce prywatności usługi dostępnej w witrynie help.eset.com (zwanych dalej „danymi osobowymi”).

2. **Upoważnienie.** Administrator danych upoważnia Podmiot przetwarzający do przetwarzania danych osobowych, zakładając, że:

(i) „cel przetwarzania” oznacza świadczenie usług zgodnie z niniejszymi Warunkami. Procesor może przetwarzać Dane Osobowe wyłącznie w imieniu Administratora w zakresie świadczenia usług żądanych przez Administratora. Wszelkie informacje zebrane w dodatkowych celach są przetwarzane poza stosunkiem umownym pomiędzy Administratorem a Podmiotem przetwarzającym.

(ii) okres przetwarzania oznacza okres rozpoczynający się w momencie nawiązania wzajemnej współpracy na

podstawie niniejszych Warunków aż do zakończenia świadczenia usług;

(iii) Zakres i kategorie danych osobowych. Usługi są przeznaczone wyłącznie do przetwarzania ogólnych danych osobowych. Jednakże Administrator ponosi wyłączną odpowiedzialność za określenie zakresu danych osobowych.

(iv) „osoba, której dane dotyczą" oznacza osobę fizyczną będącą autoryzowanym użytkownikiem urządzeń Administratora danych;

(v) operacje przetwarzania oznaczają wszystkie operacje niezbędne do przetwarzania;

(vi) „udokumentowane instrukcje" oznaczają instrukcje opisane w niniejszych Warunkach i aneksach do nich, Polityce prywatności oraz dokumentacji usługi. Administrator odpowiada za prawną dopuszczalność przetwarzania Danych Osobowych przez Podmiot przetwarzający w zakresie odpowiednich obowiązujących przepisów prawa o ochronie danych.

3. **Obowiązki Podmiotu przetwarzającego dane.** Podmiot przetwarzający jest zobowiązany do:

(i) dane osobowe są przetwarzane wyłącznie na podstawie udokumentowanych poleceń i w celu określonym w Warunkach, Załącznikach, Polityce Prywatności i dokumentacji serwisowej,

(ii) poinstruowania osób upoważnionych do przetwarzania danych osobowych (dalej „Osoby upoważnione") o ich prawach i obowiązkach wynikających z GDPR, o ich odpowiedzialności w przypadku naruszenia, a także do upewnienia się, że Osoby upoważnione zobowiązały się do zachowania poufności i przestrzegania udokumentowanych poleceń,

(vi) „udokumentowane instrukcje" oznaczają instrukcje opisane w niniejszych Warunkach i aneksach do nich, Polityce prywatności oraz dokumentacji usługi.

(iv) Podmiot będzie pomagać Administratorowi w odpowiadaniu na wnioski Podmiotów danych dotyczące ich praw. Podmiot przetwarzający nie będzie poprawiał, usuwał ani ograniczał przetwarzania Danych Osobowych bez polecenia Administratora. Wszelkie wnioski Podmiotu Danych dotyczące Danych Osobowych przetwarzanych w imieniu Administratora będą niezwłocznie przekazywane Administratorowi.

(iv) Podmiot będzie pomagać Administratorowi w powiadamianiu organu nadzorczego i Podmiotu Danych o naruszeniu ochrony danych osobowych, Podmiot przetwarzający dane powiadomi Administratora o wszelkich naruszeniach w zakresie przetwarzania lub bezpieczeństwa danych osobowych natychmiast po ich odkryciu. Podmiot przetwarzający dane będzie współpracował w rozsądnym zakresie w dochodzeniu i działaniach naprawczych dotyczących takiego naruszenia, a także podejmie rozsądne środki, aby ograniczyć dalsze negatywne konsekwencje.

(v) zgodnie z postanowieniem Administratora, wszystkie dane osobowe zostaną usunięte lub zwrócone Administratorowi danych po zakończeniu okresu przetwarzania. Administrator zobowiązuje się poinformować Podmiot przetwarzający dane o swojej decyzji w ciągu dziesięciu (10) dni po zakończeniu okresu przetwarzania. Niniejsze postanowienie nie wpływa na prawo Podmiotu przetwarzającego dane do zachowania danych osobowych w stopniu wymaganym do celów archiwizacji w związku z interesem publicznym, badaniami naukowymi, celami statystycznymi lub do ustalenia, wykonania lub obrony roszczeń prawnych.

(vii) przechowywania aktualnego rejestru wszystkich kategorii czynności związanych z przetwarzaniem, które są wykonywane w imieniu Administratora danych;

(vii) Podmiot będzie udostępniać Administratorowi wszystkie informacje niezbędne do wykazania zgodności w ramach niniejszych Warunków i aneksów do nich, Polityki prywatności oraz dokumentacji usługi. W przypadku audytu lub kontroli przetwarzania danych osobowych po stronie Administratora jest on zobowiązany do pisemnego powiadomienia Podmiotu przetwarzającego dane co najmniej trzydzieści (30) dni przed planowanym

audytem lub kontrolą.

4. **Angażowanie innego podmiotu przetwarzającego dane** Podmiot przetwarzający jest upoważniony do zaangażowania innego podmiotu przetwarzającego do wykonywania określonych czynności, takich jak świadczenie usług przechowywania w chmurze i zapewnianie infrastruktury dla usługi zgodnie z niniejszymi Warunkami, niniejszym aneksem, Polityką prywatności oraz dokumentacją usługi. Obecnie Microsoft zapewnia przechowywanie i infrastrukturę w chmurze w ramach Azure Cloud Service. Nawet w takich przypadkach Podmiot przetwarzający pozostaje jedynym punktem kontaktu oraz stroną odpowiedzialną za zgodność z wymaganiami. Administrator niniejszym zobowiązuje się poinformować Podmiot przetwarzający dane o dodaniu lub wymianie innego administratora w celu możliwości zgłoszenia sprzeciwu.

5. **Terytorium przetwarzania.** Podmiot przetwarzający zapewnia, że przetwarzanie będzie odbywać się na terytoriom Europejskiego Obszaru Gospodarczego lub kraju uznanego decyzją Komisji Europejskiej za bezpieczny, zależnie od decyzji Administratora danych. W przypadku przekazywania i przetwarzania danych poza terytorium Europejskiego Obszaru Gospodarczego lub kraju uznanego decyzją Komisji Europejskiej za bezpieczny obowiązują standardowe klauzule umowne.

6. **Zabezpieczenia.** Podmiot przetwarzający posiada certyfikat ISO 27001:2013 i wdraża warstwową ochronną strategię bezpieczeństwa zgodną z normą ISO 27001 podczas stosowania kontroli bezpieczeństwa na poziomie sieci, systemów operacyjnych, baz danych, aplikacji, personelu i procesów operacyjnych. Zgodność z wymogami regulacyjnymi i umownymi jest poddawana regularnym ocenom oraz przeglądom podobnie jak w przypadku innych elementów infrastruktury oraz procesów Podmiotu przetwarzającego, a także podejmowane są niezbędne kroki w celu zapewnienia zgodności w sposób ciągły. Podmiot przetwarzający zorganizował zabezpieczenia danych z wykorzystaniem systemu ISMS na podstawieISO 27001. Dokumentacja bezpieczeństwa obejmuje przede wszystkich dokumenty dotyczące zasad bezpieczeństwa informacji, bezpieczeństwa fizycznego i bezpieczeństwa sprzętu, zarządzania incydentami, postępowania w przypadku wycieku danych oraz incydentów bezpieczeństwa itp.

7. **Środki techniczne i organizacyjne**. Podmiot przetwarzający dane będzie chronić dane osobowe przed przypadkowym i bezprawnym uszkodzeniem i zniszczeniem, przypadkową utratą, zmianą, nieupoważnionym dostępem i ujawnieniem. W tym celu Podmiot przetwarzający dane zastosuje odpowiednie środki techniczne i organizacyjne odpowiadające trybowi przetwarzania i zagrożeniom związanym z przetwarzaniem dla praw osób, których dane dotyczą, zapewniając zgodność z wymaganiami GDPR. Szczegółowy opis środków technicznych i organizacyjnych można znaleźć w Polityce bezpieczeństwa.

8. **Dane kontaktowe Podmiotu przetwarzającego dane.** Wszelkie powiadomienia, wnioski, żądania i inną komunikację dotyczącą ochrony danych osobowych należy kierować na adres: ESET, spol. s.r.o., do rąk: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.

Standard Contractual Clauses

SEKCJA I

Klauzula 1 Cel i zakres

(a) Niniejsze standardowe klauzule umowne mają na celu zapewnienie zgodności z wymogami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych) (1) w zakresie przekazywania danych osobowych do państwa trzeciego.

(b) Strony:

(i) osoby fizyczne lub prawne, organy publiczne, agencje lub inne organy (zwane dalej „podmiotami”) przekazujące dane osobowe, wymienione w załączniku I część A(zwane dalej „podmiotem przekazującym dane”) oraz

(ii) podmioty w państwie trzecim otrzymujące dane osobowe od podmiotu przekazującego dane, bezpośrednio lub pośrednio za pośrednictwem innego podmiotu, będącego również Stroną niniejszych klauzul, umieszczone w wykazie w załączniku I część A(zwane dalej „podmiotem odbierającym dane”)

uzgodniły niniejsze standardowe klauzule umowne (zwane dalej „klauzulami”).

(c) Niniejsze klauzule mają zastosowanie do przekazywania danych osobowych, jak określono w załączniku I część B.

(d) Dodatek do niniejszych klauzul zawierający wymienione w nich załączniki stanowi integralną część niniejszych klauzul.

Klauzula 2 Skutek i niezmienność klauzul

(a) Niniejsze klauzule określają odpowiednie zabezpieczenia, w tym egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej, zgodnie z art. 46 ust. 1 i art. 46 ust. 2 lit. c) rozporządzenia (UE) 2016/679, oraz standardowe klauzule umowne zgodnie z art. 28 ust. 7 rozporządzenia (UE) 2016/679 w odniesieniu do przekazywania danych od administratorów do podmiotów przetwarzających lub od podmiotów przetwarzających do podmiotów przetwarzających, pod warunkiem że klauzule te nie są modyfikowane, z wyjątkiem modyfikowania w celu wyboru odpowiedniego modułu lub odpowiednich modułów lub w celu dodania informacji do dodatku lub aktualizacji takich informacji. Nie uniemożliwia to Stronom włączania standardowych klauzul umownych określonych w niniejszych klauzulach do szerszej umowy lub dodawania innych klauzul lub dodatkowych zabezpieczeń, pod warunkiem że nie są one bezpośrednio ani pośrednio sprzeczne z niniejszymi klauzulami ani nie naruszają podstawowych praw lub wolności osób, których dane dotyczą.

(b) Niniejsze klauzule nie naruszają obowiązków, którym podlega podmiot przekazujący dane na mocy rozporządzenia (UE) 2016/679.

Klauzula 3: Rzecz osoby trzeciej

(a) Osoby, których dane dotyczą, mogą powoływać się na niniejsze klauzule i egzekwować je, jako osoby trzecie, na rzecz których zawarto umowę, względem podmiotu przekazującego dane lub podmiotu odbierającego dane, z następującymi wyjątkami:

klauzula 1, klauzula 2, klauzula 3, klauzula 6, klauzula 7;

(ii) klauzula 8 – moduł pierwszy: klauzula 8.5 lit. e) i klauzula 8.9 lit. b); moduł drugi: klauzula 8.1 lit. b), klauzula 8.9 lit. a), c), d) i e); moduł trzeci: klauzula 8.1 lit. a), c) i d) oraz klauzula 8.9 lit. a), c), d), e), f) i g); moduł czwarty: klauzula 8.1 lit. b) oraz klauzula 8.3 lit. b);

(iii) klauzula 9 – moduł drugi: klauzula 9 lit. a), c), d) i e); moduł trzeci: klauzula 9 lit. a), c), d) i e);

(iv) klauzula 12 – moduł pierwszy: klauzula 12 lit. a) i d); moduły drugi i trzeci: klauzula 12 lit. a), d) i f);

(v) klauzula 13;

(vi) klauzula 15.1 lit. c), d) i e);

(vii) klauzula 16 lit. e);

(viii) klauzula 18 – moduły pierwszy, drugi i trzeci: klauzula 18 lit. a) i b); moduł czwarty: Klauzula 18

(b) Lit. a) pozostaje bez uszczerbku dla praw osób, których dane dotyczą, w trybie rozporządzenia (UE) 2016/679.

Klauzula 4 Interpretacja

(a) W przypadku gdy w niniejszych klauzulach stosuje się terminy zdefiniowane w rozporządzeniu (UE) 2016/679, terminy te mają znaczenie nadane im w tym rozporządzeniu.

(b) Niniejsze klauzule należy odczytywać i interpretować w świetle przepisów rozporządzenia (UE) 2016/679.

(c) Klauzul tych nie należy interpretować w sposób sprzeczny z prawami i obowiązkami określonymi w rozporządzeniu (UE) 2016/679.

Klauzula 5 Hierarchia

W przypadku sprzeczności między niniejszymi klauzulami a postanowieniami powiązanych umów między Stronami, obowiązujących w chwili uzgodnienia niniejszych klauzul, lub zawartych w późniejszym terminie, niniejsze klauzule mają pierwszeństwo.

Klauzula 6 Opis przekazywania danych

Szczegóły dotyczące przekazywania danych, w szczególności kategorie przekazywanych danych osobowych oraz cel lub cele ich przekazywania, określono w załączniku I część B.

Klauzula 7 – Nieobowiązkowa Klauzula przystąpienia

(a) Podmiot, który nie jest Stroną niniejszych klauzul, może za zgodą Stron przystąpić do tych klauzul w dowolnym momencie albo jako podmiot przekazujący dane, albo jako podmiot odbierający dane, wypełniając dodatek i podpisując załącznik I część A.

(b) Po wypełnieniu dodatku i podpisaniu załącznika I część A podmiot przystępujący staje się Stroną niniejszych klauzul oraz nabywa prawa i obowiązki podmiotu przekazującego dane lub podmiotu odbierającego dane, zgodnie z jego określeniem w załączniku I część A.

(c) Podmiot przystępujący nie ma żadnych praw ani obowiązków wynikających z niniejszych klauzul w odniesieniu do okresu, zanim został ich Stroną.

SEKCJA II – OBOWIĄZKI STRON

Klauzula 8 Zabezpieczenia służące ochronie danych

Podmiot przekazujący dane gwarantuje, że dołożył zasadnych starań w celu ustalenia, że podmiot odbierający dane jest w stanie – dzięki wdrożeniu odpowiednich środków technicznych i organizacyjnych – wypełnić swoje obowiązki określone w niniejszych klauzulach.

MODUŁ PIERWSZY: Przekazywanie między administratorami

8.1. Ograniczenie celu

Podmiot odbierający dane przetwarza dane osobowe wyłącznie w określonym celu lub określonych celach przekazywania, jak wskazano w załączniku I część B. Może on przetwarzać dane osobowe w innym celu wyłącznie w przypadku:

(i) uzyskania uprzedniej zgody osoby, której dane dotyczą;

(ii) gdy jest to niezbędne do ustalenia, dochodzenia lub obrony roszczeń w kontekście szczególnego postępowania administracyjnego, regulacyjnego lub sądowego; lub

(iii) gdy jest to niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

8.2. Przejrzystość

(a) W celu umożliwienia osobom, których dane dotyczą, skutecznego wykonywania ich praw zgodnie z klauzulą 10, podmiot odbierający dane przekazuje im, bezpośrednio lub za pośrednictwem podmiotu przekazującego dane, informacje dotyczące:

(i) swoich danych identyfikujących i danych kontaktowych;

(ii) kategorii przetwarzanych danych osobowych;

(iii) prawa do otrzymania kopii niniejszych klauzul;

(iv) w przypadku gdy planuje dalsze przekazywanie danych osobowych stronie trzeciej lub stronom trzecim – odbiorcy lub kategorii odbiorców (w razie potrzeby w celu przekazania istotnych informacji), celu dalszego przekazania oraz jego uzasadnienia zgodnie z klauzulą 8.7.

(b) Lit. a) nie ma zastosowania w przypadku, gdy osoba, której dane dotyczą, już posiada te informacje, w tym gdy podmiot przekazujący dane przekazał już te informacje lub przekazanie ich jest niemożliwe lub wymagałoby niewspółmiernego wysiłku ze strony podmiotu odbierającego dane. W tym drugim przypadku podmiot odbierający dane udostępnia publicznie dane w zakresie, w jakim jest to możliwe.

(c) Strony udostępniają bezpłatnie na żądanie osobie, której dane dotyczą, kopię niniejszych klauzul, w tym dodatek wypełniony przez Strony. W zakresie koniecznym w celu ochrony tajemnic handlowych lub innych informacji poufnych, w tym danych osobowych, Strony mogą częściowo zredagować tekst dodatku przed udostępnieniem jego kopii, lecz przekazują stosowne streszczenie, jeżeli bez takiego streszczenia osoba, której dane dotyczą, nie byłaby w stanie zrozumieć treści takiego tekstu lub korzystać ze swoich praw. Na żądanie Strony przekazują osobie, której dane dotyczą, powody zredagowania tekstu, w miarę możliwości bez ujawniania utajnionych informacji.

(d) Postanowienia zawarte w lit. a)–c) pozostają bez uszczerbku dla obowiązków spoczywających na podmiocie przekazującym dane na mocy art. 13 i 14 rozporządzenia (UE) 2016/679.

8.3. Prawidłowość i minimalizacja danych

(a) Każda Strona zapewnia, aby dane osobowe były prawidłowe i w razie potrzeby uaktualniane. Podmiot odbierający dane podejmuje wszelkie zasadne działania, aby dane osobowe, które są nieprawidłowe w świetle celu lub celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

(b) Jeżeli jedna ze Stron zda sobie sprawę, że przekazane lub otrzymane przez nią dane osobowe są nieprawidłowe lub nieaktualne, powiadamia o tym bez zbędnej zwłoki drugą Stronę.

(c) Podmiot odbierający dane zapewnia, aby dane osobowe były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celu lub celów przetwarzania.

8.4. Ograniczenie przechowywania

Podmiot odbierający dane zatrzymuje dane osobowe przez okres nie dłuższy, niż jest to niezbędne do celu lub celów, w których dane te są przetwarzane. Wdraża on odpowiednie środki techniczne lub organizacyjne, aby zapewnić wypełnienie tego obowiązku, w tym usunięcie lub anonimizację (2) danych oraz wszelkich kopii zapasowych po zakończeniu okresu zatrzymywania.

8.5. Bezpieczeństwo przetwarzania

(a) Podmiot odbierający dane, a podczas przesyłania również podmiot przekazujący dane, wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych osobowych, w tym ochrony przeciwko naruszeniu bezpieczeństwa prowadzącemu do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu (zwanego dalej „naruszeniem ochrony danych osobowych"). Przy ocenie odpowiedniego poziomu bezpieczeństwa podmioty te uwzględniają stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cel lub cele przetwarzania, a także ryzyko wynikające z przetwarzania dla osoby, której dane dotyczą. Strony rozważą w szczególności posłużenie się szyfrowaniem lub pseudonimizacją, w tym podczas przesyłania, w przypadkach, gdy cel przetwarzania może być spełniony w ten sposób.

(b) Strony uzgodniły środki techniczne i organizacyjne określone w załączniku II. Podmiot odbierający dane przeprowadza regularne kontrole, aby zagwarantować, że środki te wciąż zapewniają odpowiedni poziom bezpieczeństwa.

(c) Podmiot odbierający dane zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

(d) W przypadku naruszenia ochrony danych osobowych dotyczącego danych osobowych przetwarzanych przez podmiot odbierający dane na podstawie niniejszych klauzul podmiot odbierający dane stosuje odpowiednie środki w celu zaradzenia naruszeniu danych osobowych, w tym środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

(e) W przypadku naruszenia ochrony danych osobowych, które może powodować ryzyko naruszenia praw i wolności osób fizycznych, podmiot odbierający dane bez zbędnej zwłoki zgłasza takie naruszenie zarówno podmiotowi przekazującemu dane, jak i właściwemu organowi nadzorczemu zgodnie z klauzulą 13. Zgłoszenie takie zawiera: (i) opis charakteru naruszenia (w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie), (ii) jego możliwe konsekwencje, (iii) środki zastosowane lub proponowane w celu zaradzenia naruszeniu oraz (iv) szczegółowe dane dotyczące punktu kontaktowego, w którym można uzyskać więcej informacji. W zakresie, w jakim dla podmiotu odbierającego dane niemożliwe jest udzielenie wszystkich informacji w tym samym czasie, może udzielać ich sukcesywnie bez zbędnej zwłoki.

(f) W przypadku naruszenia ochrony danych osobowych, które może powodować ryzyko naruszenia praw i wolności osób fizycznych, administrator bez zbędnej zwłoki zgłasza również osobom, których dane dotyczą, naruszenie ochrony danych osobowych oraz jego charakter, w stosownych przypadkach we współpracy z podmiotem przekazującym dane, wraz z informacjami, o których mowa w lit. e) ppkt (ii)–(iv), chyba że podmiot odbierający dane wdrożył środki służące istotnemu ograniczeniu ryzyka naruszenia praw lub wolności osób fizycznych lub zgłoszenie wymagałoby niewspółmiernie dużego wysiłku. W tym drugim przypadku podmiot odbierający dane zamiast tego wydaje komunikat publiczny lub podejmuje podobne działanie w celu poinformowania ogółu społeczeństwa o naruszeniu ochrony danych osobowych.

(g) Podmiot odbierający dane dokumentuje wszelkie istotne fakty związane z naruszeniem ochrony danych osobowych, w tym jego skutki oraz wszelkie podjęte działania zaradcze.

8.6. Dane wrażliwe

Gdy przekazywanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby lub dane dotyczące wyroków skazujących lub czynów zabronionych (zwane dalej „danymi wrażliwymi"), podmiot odbierający dane stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia dostosowane do szczególnego charakteru danych i ponoszonego ryzyka. Mogą one obejmować ograniczenia w zakresie personelu, któremu zezwala się na dostęp do danych osobowych, dodatkowe środki bezpieczeństwa (takie jak pseudonimizacja) lub dodatkowe ograniczenia dotyczące dalszego ujawniania.

8.7. Dalsze przekazywanie danych

Podmiot odbierający dane nie ujawnia danych osobowych stronie trzeciej zlokalizowanej poza terytorium Unii Europejskiej (3) (w tym samym państwie co podmiot odbierający dane lub w innym państwie trzecim; dalej „dalsze przekazanie"), chyba że strona trzecia jest związana niniejszymi klauzulami bądź zgadza się im podlegać, na mocy odpowiedniego modułu. W innych przypadkach dalsze przekazanie przez podmiot odbierający dane może mieć miejsce wyłącznie wówczas, gdy:

(i) odbywa się do państwa objętego decyzją stwierdzającą odpowiedni stopień ochrony, zgodnie z art.45 rozporządzenia (UE) 2016/679, obejmującą dalsze przekazywanie;

(ii) strona trzecia zapewnia winny sposób odpowiednie zabezpieczenia w odniesieniu do przedmiotowego przetwarzania zgodnie z art. 46 lub 47 rozporządzenia (UE) 2016/679;

(iii) strona trzecia zawiera wiążący instrument z podmiotem odbierającym dane, zapewniający taki sam poziom ochrony danych jak poziom przewidziany w niniejszych klauzulach, a podmiot odbierający dane przekazuje kopię tych zabezpieczeń podmiotowi przekazującemu dane;

(iv) gdy jest to niezbędne do ustalenia, dochodzenia lub obrony roszczeń w kontekście szczególnego postępowania administracyjnego, regulacyjnego lub sądowego; lub

(v) jest ono jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej; lub

(vi) jeżeli żaden z pozostałych warunków nie ma zastosowania – podmiot odbierający dane uzyskał wyraźną zgodę osoby, której dane dotyczą, na dalsze ich przekazywanie w określonej sytuacji, po uprzednim poinformowaniu tej osoby ocelu lub celach dalszego przekazania, tożsamości odbiorcy oraz ewentualnym ryzyku, na które – ze względu na brak odpowiednich zabezpieczeń służących ochronie danych – może być narażona osoba, której dane dotyczą, w związku z tym przekazaniem. W takim przypadku podmiot odbierający dane informuje podmiot przekazujący dane i na żądanie tego ostatniego przekazuje mu kopię informacji przekazanych osobie, której dane dotyczą.

Wszelkie dalsze przekazanie odbywa się pod warunkiem przestrzegania przez podmiot odbierający dane wszystkich pozostałych zabezpieczeń na mocy niniejszych klauzul, w szczególności ograniczenia celu.

8.8. Przetwarzanie z upoważnienia podmiotu odbierającego dane

Podmiot odbierający dane zapewnia, aby każda osoba działająca z jego upoważnienia, w tym podmiot przetwarzający, przetwarzała dane wyłącznie na jego polecenie.

8.9. Dokumentacja i zgodność

(a) Każda ze Stron będzie wstanie wykazać, że przestrzega ciążących na niej obowiązków wynikających z

niniejszych klauzul. W szczególności podmiot odbierający dane przechowuje odpowiednią dokumentację wykonanych czynności przetwarzania, za które odpowiada.

(b) Podmiot odbierający dane udostępnia tę dokumentację na żądanie właściwego organu nadzorczego.

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

8.1. Polecenie

(a) Podmiot odbierający dane przetwarza dane osobowe wyłącznie na udokumentowane polecenie podmiotu przekazującego dane. Podmiot przekazujący dane może wydawać takie polecenia w całym okresie obowiązywania umowy.

(b) Podmiot odbierający dane niezwłocznie informuje podmiot przekazujący dane, jeżeli nie może wykonać tego polecenia.

8.2. Ograniczenie celu

Podmiot odbierający dane przetwarza dane osobowe wyłącznie w określonym celu/określonych celach przekazywania, jak wskazano w załączniku I część B, chyba że działa na podstawie dalszych poleceń wydanych przez podmiot przekazujący dane.

8.3. Przejrzystość

Podmiot przekazujący dane udostępnia bezpłatnie na żądanie osobie, której dane dotyczą, kopię niniejszych klauzul, w tym dodatku wypełnionego przez Strony. W zakresie koniecznym w celu ochrony tajemnic handlowych lub innych informacji poufnych, w tym środków opisanych w załączniku II i danych osobowych, podmiot przekazujący dane może częściowo zredagować tekst dodatku do tych klauzul przed udostępnieniem jego kopii, lecz przekazuje stosowne streszczenie, jeżeli bez takiego streszczenia osoba, której dane dotyczą, nie byłaby w stanie zrozumieć treści takiego tekstu lub korzystać ze swoich praw. Na żądanie Strony przekazują osobie, której dane dotyczą, powody zredagowania tekstu, w miarę możliwości bez ujawniania utajnionych informacji. Klauzula ta pozostaje bez uszczerbku dla obowiązków spoczywających na podmiocie przekazującym dane na mocy art.13 i 14 rozporządzenia (UE) 2016/679.

8.4. Prawidłowość

Jeżeli podmiot odbierający dane zda sobie sprawę, że otrzymane przez niego dane osobowe są nieprawidłowe lub nieaktualne, powiadamia o tym bez zbędnej zwłoki podmiot przekazujący dane. W takim przypadku podmiot odbierający dane współpracuje z podmiotem przekazującym dane w celu ich usunięcia lub sprostowania.

8.5. Czas trwania przetwarzania oraz usuwanie lub zwrot danych

Przetwarzanie danych przez podmiot odbierający dane odbywa się wyłącznie przez czas określony w załączniku I część B. Po zakończeniu świadczenia usług przetwarzania podmiot odbierający dane, zgodnie z wyborem podmiotu przekazującego dane, albo usuwa wszystkie dane osobowe przetworzone w imieniu podmiotu przekazującego dane i potwierdza podmiotowi przekazującemu dane ich usunięcie, albo zwraca podmiotowi przekazującemu dane wszystkie dane osobowe przetworzone w jego imieniu i usuwa istniejące kopie. Do czasu usunięcia lub zwrotu danych podmiot odbierający dane nadal zapewnia zgodność z niniejszymi klauzulami. Jeżeli lokalne prawo obowiązujące podmiot odbierający dane zabrania zwrotu lub usunięcia danych osobowych, podmiot odbierający dane gwarantuje, że będzie w dalszym ciągu zapewniał przestrzeganie niniejszych klauzul oraz że będzie przetwarzał je wyłącznie w zakresie i w czasie wymaganym przez to prawo lokalne. Zasada ta pozostaje bez uszczerbku dla klauzuli 14, w szczególności wymogu określonego w klauzuli 14 lit. e), aby podmiot odbierający dane zgłaszał w okresie obowiązywania umowy podmiotowi przekazującemu dane, jeżeli ma powody,

aby sądzić, że podlega lub zaczął podlegać przepisom lub praktykom niezgodnym z wymogami określonymi w klauzuli 14 lit. a).

8.6. Bezpieczeństwo przetwarzania

(a) Podmiot odbierający dane, a podczas przesyłania również podmiot przekazujący dane, wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych, w tym ochrony przeciwko naruszeniu bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do tych danych (zwanego dalej „naruszeniem ochrony danych osobowych"). Przy ocenie odpowiedniego poziomu bezpieczeństwa Strony uwzględniają stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cel lub cele przetwarzania, a także ryzyko wynikające z przetwarzania dla osób, których dane dotyczą. Strony rozważą w szczególności posłużenie się szyfrowaniem lub pseudonimizacją, w tym podczas przesyłania, w przypadkach, gdy cel przetwarzania może być spełniony w ten sposób. W przypadku pseudonimizacji dodatkowe informacje w celu przypisania danych osobowych konkretnej osobie, której dane dotyczą, pozostają, jeżeli jest to możliwe, pod wyłączną kontrolą podmiotu przekazującego dane. W ramach obowiązków w trybie niniejszej litery podmiot odbierający dane wdraża co najmniej środki techniczne i organizacyjne określone w załączniku II. Podmiot odbierający dane przeprowadza regularne kontrole, aby zagwarantować, że środki te wciąż zapewniają odpowiedni poziom bezpieczeństwa.

(b) Podmiot odbierający dane udziela dostępu do danych osobowych członkom swojego personelu wyłącznie w zakresie ściśle niezbędnym do wykonywania umowy, zarządzania umową oraz jej monitorowania. Zapewnia on, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

(c) W przypadku naruszenia ochrony danych osobowych dotyczącego danych osobowych przetwarzanych przez podmiot odbierający dane na podstawie niniejszych klauzul podmiot odbierający dane stosuje odpowiednie środki w celu zaradzenia temu naruszeniu, w tym środki w celu zminimalizowania jego negatywnych skutków. Po stwierdzeniu naruszenia podmiot odbierający dane zgłasza je również bez zbędnej zwłoki podmiotowi przekazującemu dane. Zgłoszenie takie zawiera szczegóły dotyczące punktu kontaktowego, w którym można uzyskać więcej informacji, opis charakteru naruszenia (w tym, gdy jest to możliwe, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie), jego możliwe konsekwencje oraz środki zastosowane lub proponowane w celu zaradzenia naruszeniu, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków. Jeżeli oraz w zakresie, w jakim niemożliwe jest udzielenie wszystkich informacji w tym samym czasie, pierwotne zgłoszenie zawiera informacje dostępne w danym momencie, a dalszych informacji udziela się sukcesywnie, bez zbędnej zwłoki w miarę, jak staną się one dostępne.

(d) Podmiot odbierający dane współpracuje z podmiotem przekazującym dane i pomaga mu, aby umożliwić podmiotowi przekazującemu dane wypełnienie obowiązków określonych w rozporządzeniu (UE) 2016/679, w szczególności obowiązku powiadomienia właściwego organu nadzorczego oraz poszkodowanych osób, których dane dotyczą, uwzględniając charakter przetwarzania oraz informacje, do których podmiot odbierający dane ma dostęp.

8.7. Dane wrażliwe

Gdy przekazywanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby lub dane dotyczące wyroków skazujących i czynów zabronionych (zwane dalej „danymi wrażliwymi"), podmiot odbierający dane stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia opisane w załączniku I część B.

8.8. Dalsze przekazywanie danych

Podmiot odbierający dane ujawnia dane osobowe stronie trzeciej wyłącznie na podstawie udokumentowanego polecenia podmiotu przekazującego dane. Ponadto dane mogą zostać ujawnione stronie trzeciej zlokalizowanej poza terytorium Unii Europejskiej (4) (w tym samym państwie co podmiot odbierający dane lub w innym państwie trzecim; dalej „dalsze przekazanie") wyłącznie wówczas, gdy strona trzecia jest związana niniejszymi klauzulami bądź zgadza się im podlegać na mocy odpowiedniego modułu lub jeżeli:

(i) dalsze przekazanie odbywa się do państwa objętego decyzją stwierdzającą odpowiedni stopień ochrony, zgodnie z art.45 rozporządzenia (UE) 2016/679, obejmującą dalsze przekazywanie;

(ii) strona trzecia zapewnia winny sposób odpowiednie zabezpieczenia w odniesieniu do przedmiotowego przetwarzania zgodnie z art.46 lub 47 rozporządzenia (UE) 2016/679;

(iii) dalsze przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń w kontekście szczególnego postępowania administracyjnego, regulacyjnego lub sądowego; lub

(iv) dalsze przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

Wszelkie dalsze przekazanie odbywa się pod warunkiem przestrzegania przez podmiot odbierający dane wszystkich pozostałych zabezpieczeń na mocy niniejszych klauzul, w szczególności ograniczenia celu.

8.9. Dokumentacja i zgodność

(a) Podmiot odbierający dane niezwłocznie i w odpowiedni sposób rozpatruje sformułowane przez podmiot przekazujący dane zapytania dotyczące przetwarzania na mocy niniejszych klauzul.

Strony będą w stanie wykazać przestrzeganie niniejszych klauzul. W szczególności podmiot odbierający dane przechowuje odpowiednią dokumentację czynności przetwarzania wykonanych w imieniu podmiotu przekazującego dane.

(c) Podmiot odbierający dane udostępnia podmiotowi przekazującemu dane wszelkie informacje niezbędne, aby wykazać przestrzeganie obowiązków określonych w niniejszych klauzulach oraz aby na żądanie podmiotu przekazującego dane umożliwić przeprowadzenie audytów czynności przetwarzania objętych niniejszymi klauzulami w rozsądnych odstępach czasu lub w przypadku wystąpienia oznak niespełnienia tych obowiązków, a także aby wnieść wkład w te audyty. Podejmując decyzję dotyczącą przeprowadzenia przeglądu lub audytu podmiot przekazujący dane może uwzględnić certyfikacje posiadane przez podmiot odbierający dane.

(d) Podmiot przekazujący dane może przeprowadzić audyt samodzielnie lub zlecić jego przeprowadzenie niezależnemu audytorowi. Audyty mogą obejmować kontrole w siedzibie lub obiektach podmiotu odbierającego dane i, w stosownych przypadkach, przeprowadzane są po powiadomieniu z rozsądnym wyprzedzeniem.

(e) Strony udostępniają właściwym organom nadzorczym na żądanie informacje, o których mowa w lit. b) i c), w tym wyniki wszelkich audytów.

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

8.1. Polecenie

(a) Podmiot przekazujący dane poinformował podmiot odbierający dane, że działa jako podmiot przetwarzający na polecenie administratora/administratorów danych, które to polecenie podmiot przekazujący dane udostępnia podmiotowi odbierającemu dane przed ich przetwarzaniem.

(b) Podmiot odbierający dane przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, zakomunikowane podmiotowi odbierającemu dane przez podmiot przekazujący dane, oraz na każde dodatkowe udokumentowane polecenia podmiotu przekazującego dane. Takie dodatkowe polecenia nie mogą być sprzeczne z poleceniami administratora. Administrator lub podmiot przekazujący dane może wydawać dalsze udokumentowane polecenia dotyczące przetwarzania danych w okresie obowiązywania umowy.

(c) Podmiot odbierający dane niezwłocznie informuje podmiot przekazujący dane, jeżeli nie może wykonać tego polecenia. Jeżeli podmiot odbierający dane nie może wykonać polecenia administratora, podmiot przekazujący dane niezwłocznie zgłasza ten fakt administratorowi.

(d) Podmiot przekazujący gwarantuje, że na podmiot odbierający dane nałożył takie same obowiązki ochrony danych – na mocy prawa Unii lub prawa państwa członkowskiego – jak w umowie lub innym akcie prawnym między administratorem a podmiotem przekazującym dane (5).

8.2. Ograniczenie celu

Podmiot odbierający dane przetwarza dane osobowe wyłącznie w określonym celu/określonych celach przekazywania, jak wskazano w załączniku I część B, chyba że działa na podstawie dalszych poleceń administratora wydanych podmiotowi odbierającemu dane przez podmiot przekazujący dane lub dalszych poleceń podmiotu przekazującego dane.

8.3. Przejrzystość

Podmiot przekazujący dane udostępnia bezpłatnie na żądanie osobie, której dane dotyczą, kopię niniejszych klauzul, w tym dodatku wypełnionego przez Strony. W zakresie koniecznym w celu ochrony tajemnic handlowych lub innych informacji poufnych, w tym danych osobowych, podmiot przekazujący dane może częściowo zredagować tekst dodatku przed udostępnieniem jego kopii, lecz przekazuje stosowne streszczenie, jeżeli bez takiego streszczenia osoba, której dane dotyczą, nie byłaby w stanie zrozumieć treści takiego tekstu lub korzystać ze swoich praw. Na żądanie Strony przekazują osobie, której dane dotyczą, powody zredagowania tekstu, w miarę możliwości bez ujawniania utajnionych informacji.

8.4. Prawidłowość

Jeżeli podmiot odbierający dane zda sobie sprawę, że otrzymane przez niego dane osobowe są nieprawidłowe lub nieaktualne, powiadamia o tym bez zbędnej zwłoki podmiot przekazujący dane. W takim przypadku podmiot odbierający dane współpracuje z podmiotem przekazującym dane w celu ich sprostowania lub usunięcia.

8.5. Czas trwania przetwarzania oraz usuwanie lub zwrot danych

Przetwarzanie danych przez podmiot odbierający dane odbywa się wyłącznie przez czas określony w załączniku I część B. Po zakończeniu świadczenia usług przetwarzania podmiot odbierający dane, zgodnie z wyborem podmiotu przekazującego dane, albo usuwa wszystkie dane osobowe przetworzone w imieniu administratora i potwierdza podmiotowi przekazującemu dane ich usunięcie, albo zwraca podmiotowi przekazującemu dane wszystkie dane osobowe przetworzone w jego imieniu i usuwa istniejące kopie. Do czasu usunięcia lub zwrotu danych podmiot odbierający dane nadal zapewnia zgodność z niniejszymi klauzulami. Jeżeli lokalne prawo obowiązujące podmiot odbierający dane zabrania zwrotu lub usunięcia danych osobowych, podmiot odbierający dane gwarantuje, że będzie w dalszym ciągu zapewniał przestrzeganie niniejszych klauzul oraz że będzie przetwarzał je wyłącznie w zakresie i w czasie wymaganym przez to prawo lokalne. Zasada ta pozostaje bez uszczerbku dla klauzuli 14, w szczególności wymogu określonego w klauzuli 14 lit. e), aby podmiot odbierający dane zgłaszał w okresie obowiązywania umowy podmiotowi przekazującemu dane, jeżeli ma powody, aby sądzić, że podlega lub zaczął podlegać przepisom lub praktykom niezgodnym z wymogami określonymi w klauzuli 14 lit. a).

8.6. Bezpieczeństwo przetwarzania

(a) Podmiot odbierający dane, a podczas przesyłania również podmiot przekazujący dane, wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych, w tym ochrony przeciwko naruszeniu bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do tych danych (zwanego dalej „naruszeniem ochrony danych osobowych"). Przy ocenie odpowiedniego poziomu bezpieczeństwa podmioty te uwzględniają stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cel lub cele przetwarzania, a także ryzyko wynikające z przetwarzania dla osoby, której dane dotyczą. Strony rozważą w szczególności posłużenie się szyfrowaniem lub pseudonimizacją, w tym podczas przesyłania, w przypadkach, gdy cel przetwarzania może być spełniony w ten sposób. W przypadku pseudonimizacji dodatkowe informacje do celu przypisania danych osobowych konkretnej osobie, której dane dotyczą, pozostają, jeżeli jest to możliwe, pod wyłączną kontrolą podmiotu przekazującego dane lub administratora. W ramach obowiązków w trybie niniejszej litery podmiot odbierający dane wdraża co najmniej środki techniczne i organizacyjne określone w załączniku II. Podmiot odbierający dane przeprowadza regularne kontrole, aby zagwarantować, że środki te wciąż zapewniają odpowiedni poziom bezpieczeństwa.

(b) Podmiot odbierający dane udziela dostępu do danych członkom swojego personelu wyłącznie w zakresie ściśle niezbędnym do wykonania umowy, zarządzania umową oraz jej monitorowania. Zapewnia on, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

(c) W przypadku naruszenia ochrony danych osobowych dotyczącego danych osobowych przetwarzanych przez podmiot odbierający dane na podstawie niniejszych klauzul podmiot odbierający dane stosuje odpowiednie środki w celu zaradzenia temu naruszeniu, w tym środki w celu zminimalizowania jego negatywnych skutków. Po stwierdzeniu naruszenia podmiot odbierający dane zgłasza je również bez zbędnej zwłoki podmiotowi przekazującemu dane oraz – w razie potrzeby i w miarę możliwości – administratorowi. Zgłoszenie takie zawiera szczegóły dotyczące punktu kontaktowego, w którym można uzyskać więcej informacji, opis charakteru naruszenia (w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie), jego możliwe konsekwencje oraz środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych, w tym środki w celu zminimalizowania jego ewentualnych negatywnych skutków. Jeżeli oraz w zakresie, w jakim niemożliwe jest udzielenie wszystkich informacji w tym samym czasie, pierwotne zgłoszenie zawiera informacje dostępne w danym momencie, a dalszych informacji udziela się sukcesywnie, bez zbędnej zwłoki w miarę, jak staną się one dostępne.

(d) Podmiot odbierający dane współpracuje z podmiotem przekazującym dane i pomaga mu, aby umożliwić podmiotowi przekazującemu dane wypełnienie obowiązków określonych w rozporządzeniu (UE) 2016/679, w szczególności obowiązku powiadomienia administratora, aby ten mógł z kolei powiadomić właściwy organ nadzorczy i poszkodowane osoby, których dane dotyczą, uwzględniając charakter przetwarzania oraz informacje, do których podmiot odbierający dane ma dostęp.

8.7. Dane wrażliwe

Gdy przekazywanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby lub dane dotyczące wyroków skazujących i czynów zabronionych (zwane dalej „danymi wrażliwymi"), podmiot odbierający dane stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia określone w załączniku I część B.

8.8. Dalsze przekazywanie danych

Podmiot odbierający dane ujawnia dane osobowe stronie trzeciej wyłącznie na podstawie udokumentowanego polecenia administratora przekazanego podmiotowi odbierającemu dane przez podmiot przekazujący dane. Ponadto dane mogą zostać ujawnione stronie trzeciej zlokalizowanej poza terytorium Unii Europejskiej (6) (w tym samym państwie co podmiot odbierający dane lub w innym państwie trzecim; dalej „dalsze przekazanie") wyłącznie wówczas, gdy strona trzecia jest związana niniejszymi klauzulami bądź zgadza się im podlegać na mocy odpowiedniego modułu lub jeżeli:

(i) dalsze przekazanie odbywa się do państwa objętego decyzją stwierdzającą odpowiedni stopień ochrony, zgodnie z art.45 rozporządzenia (UE) 2016/679, obejmującą dalsze przekazywanie;

(ii) strona trzecia winny sposób zapewnia odpowiednie zabezpieczenia zgodnie z art. 46 lub 47 rozporządzenia (UE) 2016/679;

(iii) dalsze przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń w kontekście szczególnego postępowania administracyjnego, regulacyjnego lub sądowego; lub

(iv) dalsze przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

Wszelkie dalsze przekazanie odbywa się pod warunkiem przestrzegania przez podmiot odbierający dane wszystkich pozostałych zabezpieczeń na mocy niniejszych klauzul, w szczególności ograniczenia celu.

8.9. Dokumentacja i zgodność

(a) Podmiot odbierający dane niezwłocznie i w odpowiedni sposób rozpatruje zapytania podmiotu przekazującego dane lub administratora dotyczące przetwarzania na mocy niniejszych klauzul.

Strony będą w stanie wykazać przestrzeganie niniejszych klauzul. W szczególności podmiot odbierający dane przechowuje odpowiednią dokumentację czynności przetwarzania wykonanych w imieniu administratora.

(c) Podmiot odbierający dane udostępnia podmiotowi przekazującemu dane wszelkie informacje niezbędne, aby wykazać przestrzeganie obowiązków określonych w niniejszych klauzulach, a podmiot przekazujący dane przekazuje te informacje administratorowi.

(d) Podmiot odbierający dane umożliwia przeprowadzanie przez podmiot przekazujący dane audytów czynności przetwarzania objętych niniejszymi klauzulami w rozsądnych odstępach czasu lub w przypadku wystąpienia oznak niespełnienia tych obowiązków, a także wnosi wkład w te audyty. Dotyczy to również sytuacji, w których podmiot przekazujący dane żąda audytu wykonania polecenia administratora. Podejmując decyzję dotyczącą przeprowadzenia audytu, podmiot przekazujący dane może uwzględnić odpowiednie certyfikacje posiadane przez podmiot odbierający dane.

(e) Jeżeli audyt dotyczy polecenia administratora, podmiot przekazujący dane udostępnia wyniki administratorowi.

(f) Podmiot przekazujący dane może przeprowadzić audyt samodzielnie lub zlecić jego przeprowadzenie niezależnemu audytorowi. Audyty mogą obejmować kontrole w siedzibie lub obiektach podmiotu odbierającego dane i, w stosownych przypadkach, przeprowadzane są po powiadomieniu z rozsądnym wyprzedzeniem.

(g) Strony udostępniają właściwym organom nadzorczym na żądanie informacje, o których mowa w lit. b) i c), w tym wyniki wszelkich audytów.

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi

8.1. Polecenie

(a) Podmiot przekazujący dane przetwarza dane osobowe wyłącznie na udokumentowane polecenie podmiotu odbierającego dane występującego w roli administratora.

(b) Podmiot przekazujący dane niezwłocznie powiadamia podmiot odbierający dane, jeżeli nie może wykonać tego polecenia, w tym jeżeli takie polecenie narusza przepisy rozporządzenia (UE) 2016/679 lub inne przepisy prawa Unii lub państwa członkowskiego dotyczące ochrony danych.

(c) Podmiot odbierający dane powinien zaniechać wszelkich działań, które uniemożliwiłyby podmiotowi przekazującemu dane wywiązanie się z obowiązków ciążących na nim na podstawie rozporządzenia (UE) 2016/679, w tym w kontekście podwykonawstwa przetwarzania lub w odniesieniu do współpracy z właściwymi organami nadzorczymi.

(d) Po zakończeniu świadczenia usług przetwarzania podmiot przekazujący dane, zgodnie z wyborem podmiotu odbierającego dane, albo usuwa wszystkie dane osobowe przetworzone w imieniu podmiotu odbierającego dane i potwierdza podmiotowi odbierającemu dane ich usunięcie, albo zwraca podmiotowi odbierającemu dane wszystkie dane osobowe przetworzone w jego imieniu i usuwa istniejące kopie.

8.2. Bezpieczeństwo przetwarzania

(a) Strony wdrażają odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych, w tym podczas przesyłania, oraz ochrony przeciwko naruszeniu bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu (zwanego dalej „naruszeniem ochrony danych osobowych”). Przy ocenie odpowiedniego poziomu bezpieczeństwa podmioty te uwzględniają stan wiedzy technicznej, koszty wdrażania oraz charakter danych osobowych (7), charakter, zakres, kontekst i cel lub cele przetwarzania, a także ryzyko wynikające z przetwarzania dla osoby, której dane dotyczą, a w szczególności rozważają posłużenie się szyfrowaniem lub pseudonimizacją, w tym podczas przesyłania, w przypadkach gdy cel przetwarzania może być spełniony w ten sposób.

(b) Podmiot przekazujący dane pomaga podmiotowi odbierającemu dane zapewnić odpowiednie bezpieczeństwo danych zgodnie z lit. a). W przypadku naruszenia ochrony danych osobowych dotyczącego danych osobowych przetwarzanych przez podmiot przekazujący dane na mocy niniejszych klauzul podmiot przekazujący dane niezwłocznie powiadamia podmiot odbierający dane, kiedy tylko dowie się, że doszło do takiego naruszenia, i pomaga podmiotowi przekazującemu dane w zaradzeniu temu naruszeniu.

(c) Podmiot przekazujący dane zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

8.3. Dokumentacja i zgodność

(a) Strony będą w stanie wykazać przestrzeganie niniejszych klauzul.

(b) Podmiot przekazujący dane udostępnia podmiotowi odbierającemu dane wszelkie informacje niezbędne do wykazania przestrzegania obowiązków określonych w niniejszych klauzulach oraz do umożliwienia przeprowadzania audytów, a także wniesienia wkładu w te audyty.

Klauzula 9 Korzystanie z usług podwykonawców przetwarzania

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

Podmiot odbierający dane ma ogólną zgodę podmiotu przekazującego dane na angażowanie podwykonawców przetwarzania widniejących w uzgodnionym wykazie. Podmiot odbierający dane wyraźnie informuje na piśmie

podmiot przekazujący dane o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub zastąpieniu podwykonawców przetwarzania z wyprzedzeniem wynoszącym co najmniej [określić przedział czasu], dając w ten sposób podmiotowi przekazującemu dane wystarczający czas na wyrażenie sprzeciwu wobec takich zmian przed zaangażowaniem podwykonawcy lub podwykonawców przetwarzania. Podmiot odbierający dane dostarcza podmiotowi przekazującemu dane informacje niezbędne do umożliwienia mu wykonania prawa do sprzeciwu.

Jeżeli podmiot odbierający dane angażuje podwykonawcę przetwarzania do celów wykonania określonych czynności przetwarzania (w imieniu podmiotu przekazującego dane), czyni to na podstawie pisemnej umowy, która zasadniczo przewiduje takie same obowiązki w odniesieniu do ochrony danych, jakie wiążą podmiot odbierający dane na mocy niniejszych klauzul, w tym w zakresie praw osób, których dane dotyczą, przysługujących im jako osobom trzecim, na rzecz których zawarto umowę. (8) Strony uzgadniają, że przestrzegając niniejszej klauzuli, podmiot odbierający dane wypełnia swoje obowiązki wynikające z klauzuli 8.8. Podmiot odbierający dane zapewnia, aby podwykonawca przetwarzania wywiązywał się z obowiązków, którym podmiot odbierający dane podlega na podstawie niniejszych klauzul.

(c) Na żądanie podmiotu przekazującego dane podmiot odbierający dane przekazuje podmiotowi przekazującemu dane kopię umowy dotyczącej podwykonawstwa przetwarzania oraz wszelkich późniejszych zmian. W zakresie koniecznym do zapewnienia ochrony tajemnic handlowych lub innych informacji poufnych, w tym danych osobowych, podmiot odbierający dane może zredagować tekst umowy przed udostępnieniem jej kopii.

(d) Podmiot odbierający dane pozostaje w pełni odpowiedzialny wobec podmiotu przekazującego dane za wykonywanie obowiązków podwykonawcy przetwarzania wynikających z umowy zawartej przez niego z podmiotem odbierającym dane. Podmiot odbierający dane powiadamia podmiot przekazujący dane o każdym przypadku niewypełnienia przez podwykonawcę przetwarzania obowiązków wynikających z tej umowy.

(e) Podmiot odbierający dane uzgadnia z podwykonawcą przetwarzania klauzulę na rzecz osoby trzeciej, na rzecz której zawarto umowę, na mocy której to klauzuli – w przypadku gdy podmiot odbierający dane przestał istnieć faktycznie lub formalnie lub stał się niewypłacalny – podmiot przekazujący dane ma prawo rozwiązać umowę dotyczącą podwykonawstwa przetwarzania i polecić podwykonawcy przetwarzania usunięcie lub zwrot danych osobowych.

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

(a) Podmiot odbierający dane ma ogólną zgodę administratora na angażowanie podwykonawców przetwarzania widniejących w uzgodnionym wykazie. Podmiot odbierający dane wyraźnie informuje administratora na piśmie o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub zastąpieniu podwykonawców przetwarzania z wyprzedzeniem wynoszącym co najmniej [określić przedział czasu], dając w ten sposób administratorowi wystarczający czas na wyrażenie sprzeciwu wobec takich zmian przed zaangażowaniem podwykonawcy lub podwykonawców przetwarzania. Podmiot odbierający dane dostarcza administratorowi informacje niezbędne do umożliwienia mu wykonania prawa do sprzeciwu. Podmiot odbierający dane informuje podmiot przekazujący dane o zaangażowaniu podwykonawcy lub podwykonawców przetwarzania.

(b) Jeżeli podmiot odbierający dane angażuje podwykonawcę przetwarzania do celów wykonania określonych czynności przetwarzania (w imieniu administratora), czyni to na podstawie pisemnej umowy, która zasadniczo przewiduje takie same obowiązki w odniesieniu do ochrony danych, jakie wiążą podmiot odbierający dane na mocy niniejszych klauzul, w tym w zakresie praw osób, których dane dotyczą, przysługujących im jako osobom trzecim, na rzecz których zawarto umowę. (9) Strony uzgadniają, że przestrzegając niniejszej klauzuli, podmiot odbierający dane wypełnia swoje obowiązki wynikające z klauzuli 8.8. Podmiot odbierający dane zapewnia, aby podwykonawca przetwarzania wywiązywał się z obowiązków, którym podmiot odbierający dane podlega na podstawie niniejszych klauzul.

(c) Na żądanie podmiotu przekazującego dane lub administratora podmiot odbierający dane przekazuje kopię

umowy dotyczącej podwykonawstwa przetwarzania oraz wszelkich późniejszych zmian. W zakresie koniecznym do zapewnienia ochrony tajemnic handlowych lub innych informacji poufnych, w tym danych osobowych, podmiot odbierający dane może zredagować tekst umowy przed udostępnieniem jej kopii.

(d) Podmiot odbierający dane pozostaje w pełni odpowiedzialny wobec podmiotu przekazującego dane za wykonywanie obowiązków podwykonawcy przetwarzania wynikających z umowy zawartej przez niego z podmiotem odbierającym dane. Podmiot odbierający dane powiadamia podmiot przekazujący dane o każdym przypadku niewypełnienia przez podwykonawcę przetwarzania obowiązków wynikających z tej umowy.

(e) Podmiot odbierający dane uzgadnia z podwykonawcą przetwarzania klauzulę na rzecz osoby trzeciej, na rzecz której zawarto umowę, na mocy której to klauzuli – w przypadku gdy podmiot odbierający dane przestał istnieć faktycznie lub formalnie lub stał się niewypłacalny – podmiot przekazujący dane ma prawo rozwiązać umowę dotyczącą podwykonawstwa przetwarzania i polecić podwykonawcy przetwarzania usunięcie lub zwrot danych osobowych.

Klauzula 10 Prawa osoby, której dane dotyczą

MODUŁ PIERWSZY: Przekazywanie między administratorami

Podmiot odbierający dane, w stosownych przypadkach z pomocą podmiotu przekazującego dane, rozpatrzy – bez zbędnej zwłoki, a najpóźniej w terminie jednego miesiąca od otrzymania zapytania lub żądania – wszelkie zapytania i żądania otrzymane od osoby, której dane dotyczą, związane z przetwarzaniem jej danych osobowych i wykonywaniem jej praw na mocy niniejszych klauzul. (10). Podmiot odbierający dane stosuje odpowiednie środki mające na celu ułatwienie występowania z takimi zapytaniami i żądaniami oraz wykonywania praw osób, których dane dotyczą. Wszelkie informacje przekazywane osobie, której dane dotyczą, muszą być podane w zrozumiałej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka.

(b) W szczególności, na żądanie osoby, której dane dotyczą, podmiot odbierający dane jest zobowiązany do nieodpłatnego:

(i) przekazania osobie, której dane dotyczą, potwierdzenia, czy dotyczące jej dane osobowe są przetwarzane – a jeżeli przetwarzanie takie ma miejsce – kopii odnoszących się do niej danych oraz informacji określonych w załączniku I; jeżeli dane osobowe zostały lub zostaną dalej przekazane – przekazania informacji o odbiorcach lub kategoriach odbiorców (w stosownych przypadkach w celu dostarczenia istotnych informacji), którym dane osobowe zostały lub zostaną dalej przekazane, ocelu takiego dalszego przekazywania i jego podstawie wynikającej z klauzuli 8.7 oraz przekazania informacji oprawie do wniesienia skargi do organu nadzorczego zgodnie z klauzulą 12 lit. c) ppkt (i);

(ii) sprostowania nieprawidłowych lub uzupełnienia niekompletnych danych odnoszących się do osoby, której dane dotyczą;

(iii) usunięcia danych osobowych osoby, której dane dotyczą, jeżeli dane te są lub były przetwarzane z naruszeniem którejkolwiek z niniejszych klauzul zapewniających przysługiwanie jej praw jako osobie trzeciej, na rzecz której zawarto umowę, lub jeżeli osoba, której dane dotyczą, wycofa zgodę, na podstawie której przetwarzanie się odbywa.

(c) Jeżeli podmiot odbierający dane przetwarza dane osobowe do celów marketingu bezpośredniego, musi zaprzestać takiego przetwarzania, jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec takiego przetwarzania.

(d) Podmiot odbierający dane nie może podjąć decyzji opierającej się jedynie na zautomatyzowanym przetwarzaniu przekazanych danych osobowych (zwanym dalej „zautomatyzowanym podejmowaniem decyzji”), która to decyzja wywoływałaby skutki prawne względem osoby, której dane dotyczą, lub wywierałaby na nią

podobny znaczący wpływ, o ile taki podmiot nie uzyskał wyraźnej zgody osoby, której dane dotyczą, lub nie został do tego upoważniony na mocy przepisów państwa przeznaczenia, o ile przepisy te obejmują stosowne środki w celu zabezpieczenia praw i uzasadnionych interesów osoby, której dane dotyczą. W takim przypadku podmiot odbierający dane, w razie potrzeby we współpracy z podmiotem przekazującym dane, musi:

(i) poinformować osobę, której dane dotyczą, o planowanym zautomatyzowanym podejmowaniu decyzji, przewidywanych konsekwencjach oraz o zasadach podejmowania decyzji oraz

(ii) wdrożyć odpowiednie zabezpieczenia, przynajmniej poprzez umożliwienie osobie, której dane dotyczą, zakwestionowania decyzji, wyrażenia swojego punktu widzenia i zyskania możliwości przeprowadzenia weryfikacji przez człowieka.

(e) Jeżeli żądania osoby, której dane dotyczą, są nadmierne, w szczególności ze względu na swój ustawiczny charakter, podmiot odbierający dane może pobrać rozsądną opłatę, uwzględniając administracyjne koszty spełnienia żądania, albo odmówić podjęcia działań w związku z żądaniem.

(f) Podmiot odbierający dane może odmówić spełnienia żądania osoby, której dane dotyczą, jeżeli taka odmowa jest dozwolona na mocy przepisów państwa przeznaczenia oraz w demokratycznym społeczeństwie jest środkiem niezbędnym i proporcjonalnym służącym ochronie jednego z celów wymienionych wart.23 ust.1 rozporządzenia (UE) 2016/679.

(g) W przypadku gdy podmiot odbierający dane zamierza odmówić spełnienia żądania osoby, której dane dotyczą, informuje ją o przyczynach odmowy oraz o możliwości złożenia skargi do właściwego organu nadzorczego lub dochodzenia roszczeń na drodze sądowej.

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

(a) Podmiot odbierający dane bezzwłocznie powiadamia podmiot przekazujący dane o każdym żądaniu otrzymanym od osoby, której dane dotyczą. Nie odpowiada on na to żądanie samodzielnie, chyba że został do tego upoważniony przez podmiot przekazujący dane.

(b) Podmiot odbierający dane pomaga podmiotowi przekazującemu dane w wypełnianiu jego obowiązków w zakresie odpowiadania na żądania osób, których dane dotyczą, związane z wykonywaniem praw przysługujących tym osobom na podstawie rozporządzenia (UE) 2016/679. W związku z tym Strony określają w załączniku II odpowiednie środki techniczne i organizacyjne, uwzględniając charakter przetwarzania, w drodze których zapewniana będzie pomoc, jak również zakres wymaganej pomocy.

(c) Wywiązując się z obowiązków spoczywających na nim na podstawie lit. a) i b), podmiot odbierający dane postępuje zgodnie z poleceniem podmiotu przekazującego dane.

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

(a) Podmiot odbierający dane bezzwłocznie powiadamia podmiot przekazujący dane i– w stosownych przypadkach – administratora o każdym żądaniu otrzymanym od osoby, której dane dotyczą, inie odpowiada na to żądanie, chyba że został do tego upoważniony przez administratora.

(b) Podmiot odbierający dane pomaga administratorowi, w razie potrzeby we współpracy z podmiotem przekazującym dane, w wypełnianiu jego obowiązków w zakresie odpowiadania na żądania osób, których dane dotyczą, związane z wykonywaniem praw przysługujących tym osobom na podstawie rozporządzenia (UE) 2016/679 lub w stosownych przypadkach rozporządzenia (UE) 2018/1725. W związku z tym Strony określają w załączniku II odpowiednie środki techniczne i organizacyjne, uwzględniając charakter przetwarzania, w drodze których zapewniana będzie pomoc, jak również zakres wymaganej pomocy.

(c) Wywiązując się z obowiązków spoczywających na nim na podstawie lit. a) i b), podmiot odbierający dane

postępuje zgodnie z poleceniem administratora przekazanym przez podmiot przekazujący dane.

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi

Strony udzielają sobie wzajemnej pomocy w zakresie zapytań i żądań ze strony osób, których dane dotyczą, zgodnie z lokalnym prawem, któremu podlega podmiot odbierający dane, lub – w przypadku przetwarzania danych w Unii przez podmiot przekazujący dane – zgodnie z rozporządzeniem (UE) 2016/679.

Klauzula 11 Zadośćuczynienie

(a) Podmiot odbierający dane – w sposób przejrzysty i łatwo dostępny w drodze indywidualnego zawiadomienia lub na swojej stronie internetowej – informuje osoby, których dane dotyczą, o tym, który punkt kontaktowy jest upoważniony do rozpatrywania skarg. Podmiot ten niezwłocznie rozpatruje wszelkie skargi otrzymane od osoby, której dane dotyczą.

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

(b) W przypadku gdy między osobą, której dane dotyczą, a jedną ze Stron wystąpi spór co do przestrzegania klauzul, Strona ta dokłada wszelkich starań, aby rozwiązać spór w sposób polubowny i terminowy. Strony na bieżąco przekazują sobie informacje na temat pojawienia się takich sporów i w stosownych przypadkach współpracują, by je rozwiązać.

(c) W przypadku gdy osoba, której dane dotyczą, powoła się na wynikające z klauzuli 3 prawo przysługujące jej jako osobie trzeciej, na rzecz której zawarto umowę, podmiot odbierający dane akceptuje decyzję osoby, której dane dotyczą, aby:

(i) złożyć skargę do organu nadzorczego w państwie członkowskim miejsca zwykłego pobytu lub miejsca pracy tej osoby lub do właściwego organu nadzorczego zgodnie z klauzulą 13;

(ii) skierować spór do sądów właściwych w rozumieniu klauzuli 18.

(d) Strony akceptują, że osobę, której dane dotyczą, mogą reprezentować podmiot, organizacja lub zrzeszenie, które nie mają charakteru zarobkowego, na warunkach określonych wart. 80 ust.1 rozporządzenia (UE) 2016/679.

(e) Podmiot odbierający dane stosuje się do decyzji wiążącej na podstawie obowiązującego prawa Unii lub państwa członkowskiego.

(f) Podmiot odbierający dane potwierdza, że wybór, jakiego dokona osoba, której dane dotyczą, pozostanie bez uszczerbku dla praw podmiotowych lub procesowych przysługujących jej zgodnie z mającymi zastosowanie przepisami.

Klauzula 12: Odpowiedzialność

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi

(a) Każda Strona ponosi odpowiedzialność wobec podmiotu lub podmiotów będących drugą Stroną za wszelkie wyrządzone im przez siebie szkody wynikające z naruszenia niniejszych klauzul.

(b) Każda Strona ponosi odpowiedzialność wobec osoby, której dane dotyczą, a osobie, której dane dotyczą, przysługuje prawo do odszkodowania z tytułu jakichkolwiek szkód majątkowych lub niemajątkowych wyrządzonych osobie, której dane dotyczą, przez Stronę w wyniku naruszenia praw przysługujących jej jako osobie trzeciej, na rzecz której zawarto umowę, na podstawie niniejszych klauzul. Zasada ta pozostaje bez uszczerbku dla odpowiedzialności spoczywającej na podmiocie przekazującym dane na podstawie rozporządzenia (UE) 2016/679.

(c) W przypadku gdy za jakiekolwiek szkody wobec osoby, której dane dotyczą, wynikające z naruszenia niniejszych klauzul, odpowiedzialność ponosi więcej niż jednak Strona, wszystkie odpowiedzialne Strony ponoszą odpowiedzialność solidarną, a osobie, której dane dotyczą, przysługuje prawo do wystąpienia do sądu przeciwko którejkolwiek z tych Stron.

(d) Strony uzgadniają, że w przypadku pociągnięcia na podstawie lit. c) jednej Strony do odpowiedzialności przysługuje jej prawo do żądania od podmiotu lub podmiotów będących drugą Stroną odszkodowania w wysokości odpowiadającej stopniowi odpowiedzialności za wyrządzoną szkodę.

(e) Podmiot odbierający dane nie może powołać się na postępowanie podmiotu przetwarzającego ani podwykonawcy przetwarzania, aby uniknąć własnej odpowiedzialności.

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

(a) Każda Strona ponosi odpowiedzialność wobec podmiotu lub podmiotów będących drugą Stroną za wszelkie wyrządzone im przez siebie szkody wynikające z naruszenia niniejszych klauzul.

(b) Podmiot odbierający dane ponosi odpowiedzialność wobec osoby, której dane dotyczą, a osobie, której dane dotyczą, przysługuje prawo do odszkodowania z tytułu jakichkolwiek szkód majątkowych lub niemajątkowych wyrządzonych osobie, której dane dotyczą, przez podmiot odbierający dane lub jego podwykonawcę przetwarzania w wyniku naruszenia praw przysługujących jej jako osobie trzeciej, na rzecz której zawarto umowę, na podstawie niniejszych klauzul.

(c) Niezależnie od postanowień lit. b) podmiot przekazujący dane ponosi odpowiedzialność wobec osoby, której dane dotyczą, a osobie, której dane dotyczą, przysługuje prawo do odszkodowania z tytułu jakichkolwiek szkód majątkowych lub niemajątkowych wyrządzonych osobie, której dane dotyczą, przez podmiot przekazujący dane lub podmiot odbierający dane (lub jego podwykonawcę przetwarzania) w wyniku naruszenia praw przysługujących jej jako osobie trzeciej, na rzecz której zawarto umowę, na podstawie niniejszych klauzul. Zasada ta pozostaje bez uszczerbku dla odpowiedzialności spoczywającej na podmiocie przekazującym dane, a w przypadku gdy podmiot przekazujący dane jest podmiotem przetwarzającym działającym w imieniu administratora – bez uszczerbku dla odpowiedzialności administratora na podstawie rozporządzenia (UE) 2016/679 lub w stosownych przypadkach rozporządzenia (UE) 2018/1725.

(d) Strony uzgadniają, że w przypadku pociągnięcia na podstawie postanowień lit. c) podmiotu przekazującego dane do odpowiedzialności za szkody wyrządzone przez podmiot odbierający dane (lub jego podwykonawcę przetwarzania) przysługuje mu prawo do żądania od podmiotu odbierającego dane odszkodowania w wysokości odpowiadającej stopniowi odpowiedzialności podmiotu odbierającego dane za wyrządzoną szkodę.

(e) W przypadku gdy za jakiekolwiek szkody wobec osoby, której dane dotyczą, wynikające z naruszenia niniejszych klauzul, odpowiedzialność ponosi więcej niż jednak Strona, wszystkie odpowiedzialne Strony ponoszą odpowiedzialność solidarną, a osobie, której dane dotyczą, przysługuje prawo do wystąpienia do sądu przeciwko którejkolwiek z tych Stron.

(f) Strony uzgadniają, że w przypadku pociągnięcia na podstawie postanowień lit. e) jednej Strony do

odpowiedzialności przysługuje jej prawo do żądania od podmiotu lub podmiotów będących drugą Stroną odszkodowania w wysokości odpowiadającej stopniowi odpowiedzialności za wyrządzoną szkodę.

(g) Podmiot odbierający dane nie może powołać się na postępowanie podwykonawcy przetwarzania, aby uniknąć własnej odpowiedzialności.

Klauzula 13 Nadzór

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

(a) [W przypadku gdy podmiot przekazujący dane posiada jednostkę organizacyjną w państwie członkowskim UE:] Organ nadzorczy odpowiedzialny za zapewnianie, aby podmiot przekazujący dane przestrzegał przepisów rozporządzenia (UE) 2016/679 w odniesieniu do przekazywania danych, jak wskazano w załączniku I część C, działa w charakterze właściwego organu nadzorczego.

[W przypadku gdy podmiot przekazujący dane nie ma jednostki organizacyjnej w państwie członkowskim UE, lecz jest objęty terytorialnym zakresem stosowania rozporządzenia (UE) 2016/679 zgodnie z art. 3 ust. 2 tego rozporządzenia i wyznaczył przedstawiciela na podstawie art. 27 ust. 1 rozporządzenia (UE) 2016/679:] Organ nadzorczy państwa członkowskiego, w którym przedstawiciel w rozumieniu art. 27 ust. 1 rozporządzenia (UE) 2016/679 posiada jednostkę organizacyjną, jak wskazano w załączniku I część C, działa w charakterze właściwego organu nadzorczego.

[W przypadku gdy podmiot przekazujący dane nie ma jednostki organizacyjnej w państwie członkowskim UE, lecz jest objęty terytorialnym zakresem stosowania rozporządzenia (UE) 2016/679 zgodnie z art. 3 ust. 2 tego rozporządzenia, jednak nie wyznaczył przedstawiciela na podstawie art. 27 ust. 2 rozporządzenia (UE) 2016/679:] Organ nadzorczy z jednego z państw członkowskich, w którym przebywają osoby, których dane dotyczą, których dane osobowe są przekazywane na podstawie niniejszych klauzul w związku z oferowaniem im towarów lub usług lub których zachowanie jest monitorowane, jak wskazano w załączniku I część C, działa w charakterze właściwego organu nadzorczego.

(b) Podmiot odbierający dane zgadza się poddać jurysdykcji właściwego organu nadzorczego i współpracować z tym organem w zakresie wszystkich procedur ukierunkowanych na zapewnienie przestrzegania niniejszych klauzul. W szczególności podmiot odbierający dane zgadza się odpowiadać na zapytania, poddawać się audytom i przestrzegać środków przyjętych przez organ nadzorczy, w tym środków zaradczych i kompensacyjnych. Przedstawia on organowi nadzorczemu pisemne potwierdzenie podjęcia się realizacji niezbędnych działań.

SEKCJA III – LOKALNE PRAWA I OBOWIĄZKI W PRZYPADKU DOSTĘPU PRZEZ ORGANY PUBLICZNE

Klauzula 14 Prawa i praktyki lokalne wpływające na przestrzeganie klauzul

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi (w przypadku gdy podmiot

przetwarzający z UE łączy dane osobowe otrzymane od administratora z państwa trzeciego z danymi osobowymi zgromadzonym przez administratora w UE)

(a) Strony gwarantują, że nie mają podstaw, by uważać, iż prawa i praktyki w państwie trzecim przeznaczenia, mające zastosowanie do przetwarzania danych osobowych przez podmiot odbierający dane, w tym wszelkie wymogi dotyczące ujawniania danych osobowych lub środki upoważniające organy publiczne do uzyskania dostępu, uniemożliwiają podmiotowi odbierającemu dane wypełnienie jego obowiązków wynikających z niniejszych klauzul. Opiera się to na założeniu, że przepisy i praktyki, które nie naruszają istoty podstawowych praw i wolności oraz nie wykraczają poza to, co jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym służącym zabezpieczeniu jednego z celów wymienionych w art. 23 ust. 1 rozporządzenia (UE) 2016/679, nie są sprzeczne z niniejszymi klauzulami.

(b) Strony oświadczają, że składając gwarancję, o której mowa w lit. a), należycie uwzględniły w szczególności następujące elementy:

(i) szczególne okoliczności przekazywania, w tym długość łańcucha przetwarzania, liczbę zaangażowanych podmiotów i wykorzystywane kanały przekazywania; planowane dalsze przekazywanie; rodzaj odbiorcy; cel przetwarzania danych; kategorie i format przekazywanych danych osobowych; sektor gospodarki, w którym dochodzi do przekazywania danych; miejsce przechowywania przekazywanych danych;

(ii) przepisy i praktyki państwa trzeciego przeznaczenia, w tym przepisy i praktyki wymagające ujawnienia danych organom publicznym lub upoważniające takie organy do uzyskania dostępu, istotne w świetle szczególnych okoliczności przekazywania danych oraz mających zastosowanie ograniczeń i zabezpieczeń (12);

(iii) wszelkie stosowne zabezpieczenia umowne, techniczne lub organizacyjne wprowadzone w celu uzupełnienia zabezpieczeń wynikających z niniejszych klauzul, w tym środki stosowane w czasie przekazywania i przetwarzania danych osobowych w państwie przeznaczenia.

(c) Podmiot odbierający dane gwarantuje, że przeprowadzając ocenę na podstawie postanowień lit. b), dołożył wszelkich starań, aby udostępnić podmiotowi przekazującemu dane odpowiednie informacje, oraz wyraża zgodę na dalszą współpracę z podmiotem przekazującym dane w zakresie zapewnienia zgodności z niniejszymi klauzulami.

(d) Strony zgadzają się udokumentować ocenę, o której mowa w lit. b), i udostępnić ją na żądanie właściwego organu nadzorczego.

(e) Podmiot odbierający dane zobowiązuje się do niezwłocznego powiadomienia podmiotu przekazującego dane, jeśli po uzgodnieniu niniejszych klauzul i okresie obowiązywania umowy ma powody, aby sądzić, że podlega lub zaczął podlegać przepisom lub praktykom niezgodnym z wymogami określonymi w lit. a), w tym w wyniku zmiany przepisów państwa trzeciego lub środka (takiego jak żądanie ujawnienia danych) wskazującego na stosowanie takich przepisów w praktyce, które nie jest zgodne z wymogami określonymi w lit. a). [W przypadku modułu trzeciego: Podmiot przekazujący dane przekazuje to powiadomienie administratorowi.]

(f) Po otrzymaniu powiadomienia zgodnie z lit. e) lub jeżeli podmiot przekazujący dane ma inny powód, by sądzić, że podmiot odbierający dane nie może dłużej wypełniać swoich obowiązków wynikających z niniejszych klauzul, podmiot przekazujący dane bezzwłocznie określa odpowiednie środki (na przykład środki techniczne lub organizacyjne służące zapewnieniu bezpieczeństwa i poufności), które podmiot przekazujący dane lub podmiot odbierający dane powinni przyjąć w celu zaradzenia zaistniałej sytuacji [w przypadku modułu trzeciego: w stosownych przypadkach w porozumieniu z administratorem]. Podmiot przekazujący dane wstrzymuje przekazywanie danych, jeżeli uzna, że zapewnienie odpowiednich zabezpieczeń w odniesieniu do takiego przekazywania jest niemożliwe, lub na polecenie [w przypadku modułu trzeciego: administratora lub] właściwego organu nadzorczego. W takim przypadku podmiot przekazujący dane jest uprawniony do rozwiązania umowy – o ile problem dotyczy przetwarzania danych osobowych na podstawie niniejszych klauzul. W przypadku gdy umowa

dotyczy więcej niż dwóch Stron, podmiot przekazujący dane może skorzystać z tego prawa do rozwiązania umowy tylko w odniesieniu do odpowiedniej Strony, chyba że Strony uzgodniły inaczej. W przypadku rozwiązania umowy na podstawie niniejszej klauzuli zastosowanie ma klauzula 16 lit. d) i e).

Klauzula 15 Obowiązki podmiotu odbierającego dane w przypadku dostępu przez organy publiczne

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi (w przypadku gdy podmiot przetwarzający z UE łączy dane osobowe otrzymane od administratora z państwa trzeciego z danymi osobowymi zgromadzonym przez administratora w UE)

15.1. Powiadomienie

(a) Podmiot odbierający dane zobowiązuje się do niezwłocznego powiadomienia podmiotu przekazującego dane oraz, o ile to możliwe, osoby, której dane dotyczą (w stosownych przypadkach z pomocą podmiotu przekazującego dane), jeśli:

(i) otrzyma od organu publicznego, w tym sądowego, prawnie wiążące żądanie – zgodnie z przepisami państwa przeznaczenia – ujawnienia danych osobowych przekazywanych na podstawie niniejszych klauzul; takie powiadomienie zawiera informacje na temat danych osobowych, których dotyczy żądanie, organu występującego z żądaniem, podstawy prawnej żądania oraz udzielonej odpowiedzi; lub

(ii) dowie się o jakimkolwiek przypadku bezpośredniego dostępu przez organy publiczne do danych osobowych przekazywanych na podstawie niniejszych klauzul zgodnie z przepisami państwa przeznaczenia; takie powiadomienie zawiera wszelkie informacje, do których podmiot odbierający dane ma dostęp.

[W przypadku modułu trzeciego: Podmiot przekazujący dane przekazuje to powiadomienie administratorowi.]

(b) Jeżeli podmiotowi odbierającemu dane zakazano powiadamiania podmiotu przekazującego dane lub osoby, której dane dotyczą, na mocy przepisów państwa przeznaczenia, zgadza się on dołożyć wszelkich starań, aby uzyskać zwolnienie z tego zakazu w celu przekazania jak największej ilości informacji w jak najkrótszym czasie. Podmiot odbierający dane zgadza się udokumentować swoje starania, aby móc je wykazać na żądanie podmiotu przekazującego dane.

(c) Jeżeli jest to dopuszczalne zgodnie z przepisami państwa przeznaczenia, podmiot odbierający dane zgadza się dostarczać podmiotowi przekazującemu dane, w regularnych odstępach czasu w okresie obowiązywania umowy, jak najwięcej istotnych informacji o otrzymanych żądaniach (w szczególności na temat liczby żądań, rodzaju wymaganych danych, organu lub organów występujących z żądaniem, a także informacji o tym, czy żądania były przedmiotem środków zaradczych służących ich zakwestionowaniu i jaki był wynik takich działań itp.). [W przypadku modułu trzeciego: Podmiot przekazujący dane przekazuje te informacje administratorowi.]

(d) Podmiot odbierający dane zgadza się przechowywać informacje, o których mowa w lit. a)–c), przez okres obowiązywania umowy i udostępniać je na żądanie właściwego organu nadzorczego.

(e) Lit. a)–c) pozostają bez uszczerbku dla obowiązku podmiotu odbierającego dane wynikającego z klauzuli 14 lit. e) i klauzuli 16, dotyczącego niezwłocznego poinformowania podmiotu przekazującego dane, w przypadku gdy nie

może on zapewnić zgodności z postanowieniami niniejszych klauzul.

15.2. Kontrola legalności i minimalizacja danych

(a) Podmiot odbierający dane zgadza się skontrolować legalność żądania ujawnienia danych, a szczególności kwestii, czy mieści się ono w zakresie uprawnień przyznanych organowi publicznemu występującemu z żądaniem, oraz zakwestionować ważność żądania, jeżeli po dokonaniu starannej oceny stwierdzi, że istnieją uzasadnione podstawy do uznania, iż żądanie jest niezgodne z prawem w świetle przepisów państwa przeznaczenia, mających zastosowanie zobowiązań wynikających z prawa międzynarodowego i zasad kurtuazji międzynarodowej. Podmiot odbierający dane korzysta z możliwości odwołania się na tych samych warunkach. Kwestionując żądanie, podmiot odbierający dane dąży do zastosowania środków tymczasowych w celu zawieszenia skutków żądania do czasu rozstrzygnięcia istoty sprawy przez właściwy organ sądowy. Nie może ujawniać danych osobowych, których dotyczy żądanie, dopóki nie będzie do tego zobowiązany na mocy mających zastosowanie przepisów procesowych. Wymogi te pozostają bez uszczerbku dla obowiązków podmiotu odbierającego dane wynikających z klauzuli 14 lit. e).

(b) Podmiot odbierający dane zgadza się udokumentować swoją ocenę prawną, a także wszelkie przypadki zakwestionowania żądania ujawnienia danych oraz, w zakresie dopuszczalnym przez przepisy państwa przeznaczenia, udostępnić dokumentację podmiotowi przekazującemu dane. Udostępnia ją również na żądanie właściwego organu nadzorczego. [W przypadku modułu trzeciego: Podmiot przekazujący dane udostępnia wyniki oceny administratorowi.]

(c) Podmiot odbierający dane zgadza się dostarczyć minimalną dopuszczalną ilość informacji, udzielając odpowiedzi na żądanie ujawnienia danych na podstawie jego rozsądnej interpretacji.

SEKCJA IV – POSTANOWIENIA KOŃCOWE

Klauzula 16 Brak zgodności z klauzulami i rozwiązanie umowy

(a) Podmiot odbierający dane niezwłocznie informuje podmiot przekazujący dane, jeżeli z jakiegokolwiek powodu nie może zapewnić przestrzegania postanowień niniejszych klauzul.

(b) W przypadku gdy podmiot odbierający dane narusza postanowienia niniejszych klauzul lub nie może zapewnić przestrzegania ich postanowień, podmiot przekazujący dane czasowo, do chwili ponownego zapewnienia przestrzegania klauzul lub rozwiązania umowy, wstrzymuje przekazywanie danych osobowych do podmiotu odbierającego. Powyższe pozostaje bez uszczerbku dla postanowień klauzuli 14 lit. f).

(c) Podmiot przekazujący dane jest uprawniony do rozwiązania umowy – o ile problem dotyczy przetwarzania danych osobowych na podstawie niniejszych klauzul – w przypadku gdy:

(i) podmiot przekazujący dane wstrzymał przekazywanie danych osobowych do podmiotu odbierającego dane na podstawie lit. b), a zgodność z postanowieniami niniejszych klauzul nie została przywrócona w rozsądnym terminie, a w każdym razie w ciągu jednego miesiąca od wstrzymania;

(ii) podmiot odbierający dane poważnym stopniu lub uporczywie narusza postanowienia niniejszych klauzul; lub

(iii) podmiot odbierający dane nie zastosował się do wiążącej decyzji właściwego sądu lub organu nadzorczego dotyczącej jego obowiązków wynikających z niniejszych klauzul.

W takich przypadkach informuje on właściwy organ nadzorczy [w przypadku modułu trzeciego: oraz administratora] o takim przypadku niezastosowania się do decyzji. W przypadku gdy umowa dotyczy więcej niż dwóch Stron, podmiot przekazujący dane może skorzystać z tego prawa do rozwiązania umowy tylko w

odniesieniu do odpowiedniej Strony, chyba że Strony uzgodniły inaczej.

d) [Dla modułów pierwszego, drugiego i trzeciego: Dane osobowe przekazane przed rozwiązaniem umowy na podstawie lit. c) muszą zostać – w zależności od wyboru dokonanego przez podmiot przekazujący dane – niezwłocznie zwrócone temu podmiotowi lub w całości usunięte. To samo dotyczy wszelkich kopii tych danych.] [W przypadku modułu czwartego: Dane osobowe zgromadzone przez podmiot przekazujący dane w UE, które zostały przekazane przed rozwiązaniem umowy na podstawie lit. c), a także wszelkie ich kopie, muszą niezwłocznie zostać w całości usunięte.] Podmiot odbierający dane poświadcza usunięcie danych podmiotowi przekazującemu. Do czasu usunięcia lub zwrotu danych podmiot odbierający dane nadal zapewnia zgodność z niniejszymi klauzulami. Jeżeli lokalne prawo obowiązujące podmiot odbierający dane zabrania zwrotu lub usunięcia przekazanych danych osobowych, podmiot odbierający dane gwarantuje, że będzie w dalszym ciągu zapewniał przestrzeganie niniejszych klauzul oraz że będzie przetwarzał dane wyłącznie w zakresie i w czasie wymaganym przez to prawo lokalne.

(e) Każda ze Stron może wycofać swoją zgodę na związanie się niniejszymi klauzulami, w przypadku gdy: (i) Komisja Europejska przyjmie decyzję na podstawie art. 45 ust. 3 rozporządzenia (UE) 2016/679 obejmującą przekazywanie danych osobowych, do których mają zastosowanie niniejsze klauzule; lub (ii) rozporządzenie (UE) 2016/679 stanie się częścią ram prawnych państwa, do którego przekazywane są dane osobowe. Powyższe pozostaje bez uszczerbku dla pozostałych obowiązków mających zastosowanie do przedmiotowego przetwarzania na podstawie rozporządzenia (UE) 2016/679.

Klauzula 17: Prawo właściwe

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

Niniejsze klauzule podlegają przepisom prawa jednego z państw członkowskich UE, pod warunkiem że prawo to dopuszcza prawa osób trzecich, na rzecz których zawarto umowę. Strony uzgadniają, że jest to prawo określone w Warunkach.

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi

Niniejsze klauzule podlegają przepisom prawa państwa, które dopuszcza prawa osób trzecich, na rzecz których zawarto umowę. Strony uzgadniają, że jest to prawo określone w Warunkach.

Klauzula 18 Wybór forum i jurysdykcji

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

(a) Wszelkie spory wynikające z niniejszych klauzul są rozstrzygane przez sądy państwa członkowskiego UE.

(b) Strony uzgadniają, że będą to sądy określone w Warunkach użytkowania.

(c) Osoba, której dane dotyczą, może również wszcząć postępowanie sądowe przeciwko podmiotowi przekazującemu dane lub podmiotowi odbierającemu dane przed sądami państwa członkowskiego, w którym znajduje się jej miejsce zwykłego pobytu.

(d) Strony uzgadniają, że będą podlegały jurysdykcji tych sądów.

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi

Wszelkie spory wynikające z niniejszych Klauzul będą rozstrzygane przez sądy określone w Warunkach użytkowania.

DODATEK

UWAGA WYJAŚNIAJĄCA: Musi istnieć możliwość wyraźnego rozróżnienia informacji mających zastosowanie do każdego przekazania lub kategorii przekazywania oraz, w związku z tym, określenia odnośnych ról stron jako podmiotów przekazujących dane lub podmiotów odbierających dane. Nie jest konieczne wypełnienie i podpisanie oddzielnych dodatków dla każdego przekazania/kategorii przekazywania lub stosunku umownego, w przypadku gdy przejrzystość można uzyskać za pomocą jednego dodatku. W przypadkach, w których konieczne jest zapewnienia jasności, należy jednak stosować oddzielne dodatki.

ZAŁĄCZNIK I

A. WYKAZ STRON

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi

Podmiot(y) przekazujący(-e) dane: [Dane identyfikujące i dane kontaktowe podmiotu(-ów) przekazującego(-ych) dane oraz w stosownych przypadkach jego/ich inspektora ochrony danych lub przedstawiciela w Unii Europejskiej]

1. Administrator zdefiniowany w Umowie powierzenia przetwarzania danych

2. Podmiot przetwarzający dane zdefiniowany w Umowie powierzenia przetwarzania danych

(na podstawie przepływu danych)

Podmiot(y) odbierający(-e) dane: [Dane identyfikujące i dane kontaktowe podmiotu(-ów) odbierającego(-ych) dane, w tym każdej osoby wyznaczonej do kontaktów odpowiedzialnej za ochronę danych]

1. Administrator zdefiniowany w Umowie powierzenia przetwarzania danych

2. Podmiot przetwarzający dane zdefiniowany w Umowie powierzenia przetwarzania danych

(na podstawie przepływu danych)

B. OPIS PRZEKAZYWANIA DANYCH

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

MODUŁ CZWARTY: Przekazywanie przez podmiot przetwarzający administratorowi

Kategorie osób, których dane dotyczą i których dane są przekazywane Zdefiniowano w Umowie powierzenia przetwarzania danych.

Kategorie przekazywanych danych osobowych Zdefiniowano w Umowie powierzenia przetwarzania danych i w Polityce prywatności.

Przekazywane dane wrażliwe (w stosownych przypadkach) oraz stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nim ryzyko, takie jak na przykład ścisłe ograniczenie celu, ograniczenia dostępu (w tym dostęp wyłącznie dla pracowników, który odbyli specjalistyczne szkolenie), przechowywanie zapisów przypadków udostępnienia danych, ograniczenia dalszego przekazywania lub dodatkowe środki bezpieczeństwa Zdefiniowano w Umowie powierzenia przetwarzania danych i w Polityce prywatności.

Częstotliwość przekazywania danych (np. czy dane są przekazywane jednorazowo, czy w sposób ciągły): W sposób ciągły.

Charakter przetwarzania: Automatyczne.

Cel(e) przekazywania danych i dalszego przetwarzania: Świadczenie usługi będzie odbywać się w sposób zdefiniowany w Warunkach usługi, Załącznikach, Polityce prywatności i w dokumentacji usługi.

Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu Zdefiniowano w Umowie powierzenia przetwarzania danych.

W przypadku przekazywania podwykonawcom przetwarzania należy również określić przedmiot, charakter i czas trwania przetwarzania Zdefiniowano w Umowie powierzenia przetwarzania danych.

C. WŁAŚCIWY ORGAN NADZORCZY

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

Należy określić właściwy organ nadzorczy/organy nadzorcze zgodnie z klauzulą 13 Zdefiniowano w Polityce prywatności

ZAŁĄCZNIK II ŚRODKI TECHNICZNE I ORGANIZACYJNE, W TYM ŚRODKI TECHNICZNE I ORGANIZACYJNE MAJĄCE NA CELU ZAPEWNIENIE BEZPIECZEŃSTWA DANYCH

MODUŁ PIERWSZY: Przekazywanie między administratorami

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

UWAGA WYJAŚNIAJĄCA: Środki techniczne i organizacyjne muszą być opisane w sposób szczegółowy (a nie ogólny). Zob. również ogólna uwaga na pierwszej stronie dodatku, w szczególności w odniesieniu do potrzeby

wyraźnego wskazania, które środki mają zastosowanie do każdego jednorazowego lub wielokrotnego przekazania.

Opis środków technicznych i organizacyjnych wdrożonych przez podmiot(y) odbierający(-e) dane (w tym odpowiednich certyfikacji) w celu zapewnienia odpowiedniego poziomu ochrony, biorąc pod uwagę charakter, zakres, kontekst i cel przetwarzania oraz ryzyko dla praw i wolności osób fizycznych. Zdefiniowano w Polityce prywatności

W przypadku przekazywania danych podmiotom przetwarzającym (lub podwykonawcom przetwarzania) należy również opisać konkretne środki techniczne i organizacyjne, które ma zastosować ten podmiot lub podwykonawca, aby móc udzielać pomocy administratorowi, a w przypadku przekazywania danych od podmiotu przetwarzającego do podwykonawczy – podmiotowi przekazującemu dane.

ZAŁĄCZNIK III WYKAZ PODWYKONAWCÓW PRZETWARZANIA

MODUŁ DRUGI: Przekazywanie przez administratora podmiotowi przetwarzającemu

MODUŁ TRZECI: Przekazywanie między podmiotami przetwarzającymi

UWAGA WYJAŚNIAJĄCA: Niniejszy załącznik wymaga uzupełniania o moduły drugi i trzeci w przypadku szczególnego upoważnienia podwykonawców przetwarzania (klauzula 9 lit. a), wariant 1).

Administrator zezwolił na korzystanie z usług następujących podwykonawców przetwarzania: Zdefiniowano w Umowie powierzenia przetwarzania danych

Odwołania:

(1) Gdy podmiot przekazujący dane jest podmiotem przetwarzającym podlegającym rozporządzeniu (UE) 2016/679, działającym w imieniu instytucji lub organu Unii, poleganie na niniejszych klauzulach przy angażowaniu innego podmiotu przetwarzającego (podwykonawstwo przetwarzania) niepodlegającego rozporządzeniu (UE) 2016/679 zapewnia również zgodność z art.29 ust.4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39) w zakresie, w jakim niniejsze klauzule oraz obowiązki dotyczące ochrony danych, określone w umowie lub innym akcie prawnym zawartym między administratorem a podmiotem przetwarzającym zgodnie z art. 29 ust. 3 rozporządzenia (UE) 2018/1725, są ze sobą zgodne. Będzie to dotyczyło w szczególności sytuacji, gdy administrator i podmiot przetwarzający opierają się na standardowych klauzulach umownych zawartych w decyzji 2021/915

(2) Oznacza to dokonanie anonimizacji danych w taki sposób, aby osób, których dane dotyczą, nie można było zidentyfikować, zgodnie z motywem 26 rozporządzenia (UE) 2016/679, oraz aby proces ten był nieodwracalny.

(3) W Porozumieniu o Europejskim Obszarze Gospodarczym (Porozumienie EOG) przewidziano rozszerzenie rynku wewnętrznego Unii Europejskiej na trzy państwa EOG – Islandię, Liechtenstein i Norwegię. Unijne prawodawstwo dotyczące ochrony danych, w tym rozporządzenie (UE) 2016/679, jest objęte Porozumieniem EOG i zostało włączone do jego załącznika XI. W związku z tym wszelkie ujawnianie danych stronie trzeciej zlokalizowanej w EOG przez podmiot odbierający dane nie kwalifikuje się jako dalsze przekazanie do celów niniejszych klauzul.

(4) W Porozumieniu o Europejskim Obszarze Gospodarczym (Porozumienie EOG) przewidziano rozszerzenie rynku wewnętrznego Unii Europejskiej na trzy państwa EOG – Islandię, Liechtenstein i Norwegię. Unijne prawodawstwo dotyczące ochrony danych, w tym rozporządzenie (UE) 2016/679, jest objęte Porozumieniem EOG i zostało włączone do jego załącznika XI. W związku z tym wszelkie ujawnianie danych stronie trzeciej zlokalizowanej w

EOG przez podmiot odbierający dane nie kwalifikuje się jako dalsze przekazanie do celów niniejszych klauzul.

(5) Zob. art. 28 ust. 4 rozporządzenia (UE) 2016/679, a w przypadku gdy administrator jest instytucją lub organem Unii – art. 29 ust. 4 rozporządzenia (UE) 2018/1725.

(6) W Porozumieniu o Europejskim Obszarze Gospodarczym (Porozumienie EOG) przewidziano rozszerzenie rynku wewnętrznego Unii Europejskiej na trzy państwa EOG – Islandię, Liechtenstein i Norwegię. Unijne prawodawstwo dotyczące ochrony danych, w tym rozporządzenie (UE) 2016/679, jest objęte Porozumieniem EOG i zostało włączone do jego załącznika XI. W związku z tym wszelkie ujawnianie danych stronie trzeciej zlokalizowanej w EOG przez podmiot odbierający dane nie kwalifikuje się jako dalsze przekazanie do celów niniejszych klauzul.

(7) Obejmuje to kwestię, czy przekazywanie i dalsze przetwarzanie dotyczy danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby lub dane dotyczące wyroków skazujących lub czynów zabronionych.

(8) Podwykonawca przetwarzania może spełnić ten wymóg, przystępując do niniejszych klauzul na podstawie odpowiedniego modułu zgodnie z klauzulą 7.

(9) Podwykonawca przetwarzania może spełnić ten wymóg, przystępując do niniejszych klauzul na podstawie odpowiedniego modułu zgodnie z klauzulą 7.

(10) Termin ten można przedłużyć w niezbędnym zakresie maksymalnie o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. Podmiot odbierający dane należycie i niezwłocznie informuje osobę, której dane dotyczą, o każdym takim przedłużeniu.

(11) Podmiot odbierający dane może zaoferować możliwość niezależnego rozwiązywania sporów za pośrednictwem sądu arbitrażowego wyłącznie wówczas, gdy posiada jednostkę organizacyjną w państwie, które ratyfikowało Konwencję nowojorską o uznawaniu i wykonywaniu zagranicznych orzeczeń arbitrażowych.

(12) Jeżeli chodzi o wpływ takich przepisów i praktyk na zgodność z niniejszymi klauzulami, w ogólnej ocenie można wziąć pod uwagę różne elementy. Do elementów takich można zaliczyć odpowiednie i udokumentowane praktyczne doświadczenie w związku z wcześniejszymi przypadkami żądania przez organy publiczne ujawnienia danych lub brakiem takich żądań, obejmujące wystarczająco reprezentatywne ramy czasowe. Dotyczy to w szczególności wewnętrznych rejestrów lub innych dokumentów, sporządzanych na bieżąco zgodnie z zasadą należytej staranności i certyfikowanych przez kadrę kierowniczą wyższego szczebla, pod warunkiem że informacje te mogą być zgodnie z prawem udostępniane stronom trzecim. Jeżeli takie praktyczne doświadczenie stanowi podstawę do stwierdzenia, że podmiot odbierający dane nie będzie miał utrudnionej możliwości przestrzegania niniejszych klauzul, musi być ono poparte innymi istotnymi, obiektywnymi elementami i to do Stron należy staranne rozważenie, czy elementy te łącznie są wystarczająco istotne pod względem ich wiarygodności i reprezentatywności, aby potwierdzić takie stwierdzenie. W szczególności Strony muszą wziąć pod uwagę, czy ich praktyczne doświadczenie jest potwierdzone i czy nie zaprzeczają mu publicznie udostępnione lub w inny sposób dostępne wiarygodne informacje na temat występowania lub braku żądań w tym samym sektorze lub stosowania prawa w praktyce, takie jak orzecznictwo i sprawozdania sporządzone przez niezależne organy nadzoru.

Zasady ochrony prywatności

Obowiązuje od 21 marca 2023 r. | Zobacz poprzednią wersję Polityki prywatności | Porównaj zmiany

Jako administrator danych, firma ESET, spol. s r. o., z siedzibą pod adresem Einsteinova 24, 851 01 Bratislava, Slovak Republic, zarejestrowana w Rejestrze Handlowym prowadzonym przez Sąd Rejonowy dla okręgu Bratislava

I, w sekcji Sro pod numerem 3586/B, numer w rejestrze przedsiębiorców: 31333532 („ESET” lub „My”), przykłada szczególną wagę do kwestii ochrony danych osobowych. Chcemy spełnić wymóg przejrzystości znormalizowany prawnie zgodnie z Ogólnym rozporządzeniem o ochronie danych UE („RODO”). W związku z tym publikujemy niniejszą Politykę prywatności wyłącznie w celu przekazania klientowi jako osobie, której dane dotyczą (dalej „Użytkownik końcowy” lub „Ty”), informacji na następujące tematy z obszaru ochrony danych osobowych:

- Podstawa prawna przetwarzania danych osobowych,
- Udostępnianie danych i poufność,
- Bezpieczeństwo danych,
- Prawa osoby, której dane dotyczą,
- Przetwarzanie danych osobowych
- Informacje kontaktowe.

Podstawa prawna przetwarzania danych osobowych

Firma ESET przetwarza dane wyłącznie w oparciu o kilka podstaw prawnych przewidzianych przepisami prawa dotyczącymi ochrony prywatności danych osobowych. Przetwarzanie danych osobowych przez firmę ESET jest niezbędne głównie do realizacji Warunki korzystania („Warunki”) z Użytkownikiem końcowym (art. 6 ust. 1 lit. b ustawy RODO), która obejmuje dostarczanie produktów lub usług firmy ESET, chyba że wyraźnie zaznaczono inaczej, np.:

- Podstawa prawna dotycząca uzasadnionego interesu (art. 6 ust. 1 lit. f ustawy RODO), która umożliwia firmie ESET przetwarzanie danych oraz monitorowanie sposobu korzystania i zadowolenia z Usług przez użytkowników w celu zapewnienia najlepszej możliwej ochrony, wsparcia i doświadczenia. W świetle obowiązujących przepisów prawa działania marketingowe są uznawane za uzasadniony interes, dlatego firma ESET polega na nich w komunikacji marketingowej z klientami.
- Firma ESET może wymagać od Użytkownika zgody w określonych sytuacjach (art. 6 ust. 1 lit. a ustawy RODO), gdy taka podstawa prawna zostanie uznana za najodpowiedniejszą lub jeśli wymaga tego prawo.
- Przestrzeganie obowiązków prawnych (art. 6 ust. 1 lit. c ustawy RODO), np. określenie wymagań dotyczących komunikacji elektronicznej, fakturowania lub dokumentów rozliczeniowych.

Udostępnianie danych i poufność

Nie udostępniamy Twoich danych stronom trzecim. Jednakże ESET jest firmą działającą na całym świecie za pośrednictwem swoich spółek stowarzyszonych oraz partnerów będących częścią sieci sprzedaży, usług i pomocy technicznej. Przetwarzane przez firmę ESET informacje dotyczące licencji, rozliczeń i pomocy technicznej mogą być przesyłane między nami a naszymi partnerami oraz spółkami stowarzyszonymi z tytułu realizacji Umowy Licencyjnej Użytkownika Końcowego, na przykład świadczenia usług lub udzielania pomocy technicznej.

Firma ESET woli przetwarzać swoje dane w Unii Europejskiej (UE). Jednak w zależności od Twojej lokalizacji (w razie korzystania z naszych produktów i/lub usług poza UE) i/lub wybranej usługi może być konieczne przekazanie Twoich danych do kraju spoza UE. Na przykład korzystamy z usług stron trzecich w związku z przetwarzaniem w chmurze. W takich przypadkach starannie dobieramy naszych usługodawców i zapewniamy odpowiedni poziom ochrony danych za pomocą wymogów umownych oraz środków technicznych i organizacyjnych. Z reguły zawieramy standardowe klauzule umowne UE, w razie potrzeby uzupełniając je dodatkowymi przepisami umownymi.

W przypadku niektórych krajów spoza UE, takich jak Wielka Brytania i Szwajcaria, UE określiła już porównywalny poziom ochrony danych. Ze względu na ten porównywalny poziom ochrony danych przekazywanie danych do tych krajów nie wymaga żadnego specjalnego upoważnienia ani zgody.

Polegamy na usługach stron trzecich związanych z przetwarzaniem w chmurze, świadczonych przez dostawców

usług w chmurze Microsoft.

Bezpieczeństwo danych

Firma ESET stosuje odpowiednie środki techniczne i organizacyjne w celu zapewnienia poziomu zabezpieczeń odpowiedniego do zagrożeń. Dokładamy wszelkich starań, aby zapewnić nieprzerwaną poufność, integralność, dostępność i odporność systemów oraz usług związanych z przetwarzaniem danych. W przypadku naruszenia ochrony danych zagrażającego prawom i wolnościom Użytkownika końcowego jesteśmy jednak gotowi do powiadomienia o tym fakcie odpowiednich organów nadzorczych oraz osoby, których dane dotyczą.

Prawa osób, których dane dotyczą

Prawa każdego Użytkownika końcowego są ważne i chcemy poinformować, że wszyscy Użytkownicy końcowi (z dowolnego kraju UE oraz spoza UE) mają następujące prawa zagwarantowane przez firmę ESET. Aby skorzystać z praw osoby, której dane dotyczą, możesz skontaktować się z nami za pośrednictwem formularza pomocy technicznej lub poczty elektronicznej, wysyłając wiadomość na adres dpo@eset.sk. W celach identyfikacyjnych prosimy o podanie następujących informacji: Imię i nazwisko, adres e-mail oraz – jeśli jest dostępny – klucz licencyjny lub numer klienta oraz przynależność do firmy. Prosimy o powstrzymanie się od przesyłania nam jakichkolwiek innych danych osobowych, takich jak data urodzenia. Zwracamy uwagę, że aby móc przetworzyć Twoje zapytanie, a także w celach identyfikacyjnych, będziemy przetwarzać Twoje dane osobowe.

Prawo do wycofania zgody. Prawo do wycofania zgody obowiązuje wyłącznie w przypadku przetwarzania na podstawie udzielonej zgody. Jeśli przetwarzamy Twoje dane osobowe na podstawie Twojej zgody, masz prawo wycofać tę zgodę w dowolnym momencie bez podania przyczyn. Wycofanie zgody jest skuteczne tylko na przyszłość i nie wpływa na zgodność z prawem danych przetwarzanych przed jej wycofaniem.

Prawo do wyrażenia sprzeciwu. Prawo do wyrażenia sprzeciwu wobec przetwarzania danych obowiązuje wyłącznie w przypadku przetwarzania na podstawie uzasadnionego interesu firmy ESET lub strony trzeciej. Jeśli przetwarzamy Twoje dane osobowe w celu ochrony uzasadnionego interesu, będąc osobą, której dane dotyczą, masz prawo w dowolnym momencie sprzeciwić się uzasadnionemu interesowi wskazanemu przez nas i przetwarzaniu Twoich danych osobowych. Sprzeciw jest skuteczny tylko na przyszłość i nie wpływa na zgodność z prawem danych przetwarzanych przed jego wyrażeniem. Jeśli przetwarzamy Twoje dane osobowe w celach marketingu bezpośredniego, nie jest konieczne podawanie powodów Twojego sprzeciwu. Dotyczy to również profilowania, o ile jest ono związane z marketingiem bezpośrednim. We wszystkich innych przypadkach prosimy o krótkie poinformowanie nas o powodzie sprzeciwu wobec przetwarzania Twoich danych osobowych zgodnie z uzasadnionym interesem firmy ESET.

Należy pamiętać, że w niektórych przypadkach, pomimo wycofania zgody, jesteśmy uprawnieni do dalszego przetwarzania Danych osobowych na podstawie innej podstawy prawnej, na przykład w celu realizacji umowy.

Prawo do uzyskania dostępu. Jako osoba, której dane dotyczą, masz prawo do bezpłatnego uzyskania w dowolnym momencie informacji o Twoich danych przechowywanych przez firmę ESET.

Prawo do sprostowania. Jeśli nieumyślnie przetwarzamy Twoje nieprawidłowe dane osobowe, masz prawo do ich poprawienia.

Prawo do usunięcia danych i prawo do ograniczenia przetwarzania. Jako osoba, której dane dotyczą, masz prawo do zażądania usunięcia lub ograniczenia przetwarzania swoich danych osobowych. Jeśli przetwarzamy Twoje dane osobowe, na przykład na mocy wyrażonej przez Ciebie zgody, którą następnie wycofujesz, a nie istnieje żadna inna podstawa prawna, taka jak umowa, natychmiast usuwamy Twoje dane osobowe. Twoje dane osobowe zostaną również usunięte z końcem naszego okresu przechowywania, gdy tylko nie będą już potrzebne do określonych dla nich celów.

Jeśli wykorzystujemy Twoje dane osobowe wyłącznie do celów marketingu bezpośredniego i zdecydujesz się odwołać swoją zgodę lub sprzeciwisz się leżącemu u podstaw przetwarzania uzasadnionemu interesowi firmy ESET, ograniczymy przetwarzanie Twoich danych osobowych, umieszczając Twoje dane kontaktowe na naszej wewnętrznej czarnej liście, aby uniknąć niechcianego kontaktu. W innych przypadkach Twoje dane osobowe zostaną usunięte.

Należy pamiętać, że możemy być zobowiązani do przechowywania Twoich danych do czasu wygaśnięcia obowiązków przechowywania i okresów wymaganych przez ustawodawcę lub organy nadzorcze. Obowiązki i okresy przechowywania mogą również wynikać z ustawodawstwa słowackiego. Po ich upłynięciu właściwe dane zostaną rutynowo usunięte.

Prawo do przeniesienia danych. Z przyjemnością przekazujemy Użytkownikowi będącemu osobą, której dane dotyczą, jego dane osobowe przetwarzane przez firmę ESET w formacie xls.

Prawo do wniesienia skargi. Jako osoba, której dane dotyczą, masz prawo do wniesienia w dowolnym momencie skargi do organu nadzorczego. Firma ESET podlega prawu słowackiemu i obowiązują ją przepisy Unii Europejskiej o ochronie danych. Właściwym organem nadzorczym ds. danych jest Urząd Ochrony Danych Osobowych Republiki Słowackiej z siedzibą pod adresem Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Przetwarzanie danych osobowych

Usługi firmy ESET zaimplementowane w produkcie działającym w sieci WWW są przez nas świadczone zgodnie z Warunkami korzystania („Warunki korzystania”), ale niektóre z nich mogą wymagać szczególnej uwagi. Chcemy przekazać szczegółowe informacje na temat przetwarzania danych związanych z dostarczanymi przez nas produktami i usługami. Świadczymy różne usługi opisane w Warunkom szczególnym oraz powiązanej z danym produktem dokumentacja. Abyśmy mogli dostarczać nasze usługi, musimy gromadzić następujące informacje:

Dane licencyjne i rozliczeniowe. Imię i nazwisko, adres e-mail, klucz licencyjny i (w stosownych przypadkach) adres, przynależność do firmy i dane dotyczące płatności są gromadzone i przetwarzane przez firmę ESET w celu ułatwienia aktywacji licencji, dostarczenia klucza licencyjnego, przypomnień o wygaśnięciu, realizacji wniosków o pomoc techniczną, weryfikacji autentyczności licencji, świadczenia naszych usług oraz dostarczania innych powiadomień, w tym wiadomości marketingowych, zgodnie z obowiązującymi przepisami lub zgodą użytkownika. Firma ESET jest prawnie zobowiązana do przechowywania informacji rozliczeniowych przez okres 10 lat, jednak informacje licencyjne zostaną zanonimizowane nie później niż 12 miesięcy po wygaśnięciu licencji.

Aktualizacja i inne statystyki. Przetwarzane informacje obejmują informacje na temat procesu instalacji oraz komputera użytkownika końcowego (np. platformy, na której jest zainstalowany nasz produkt), a także informacje o działaniu i funkcjach naszych produktów, takie jak informacje o systemie operacyjnym, dane dotyczące sprzętu, identyfikatory instalacji, identyfikatory licencji, adres IP, adres MAC oraz ustawienia konfiguracji produktu. Są one przetwarzane do celów dostarczania aktualizacji usług oraz konserwacji, zapewniania bezpieczeństwa i ulepszania naszej infrastruktury.

Informacje te są przechowywane oddzielnie od informacji identyfikacyjnych wymaganych do celów licencjonowania i fakturowania, ponieważ nie wymagają identyfikacji Użytkownika końcowego. Okres przechowywania wynosi do 4 lat.

System reputacji ESET LiveGrid®. Skróty jednokierunkowe związane z infekcjami są przetwarzane na potrzeby systemu reputacji ESET LiveGrid®, który poprawia wydajność naszych rozwiązań do ochrony przed szkodliwym oprogramowaniem, porównując skanowane pliki z białą i czarną listą obiektów w chmurze. Użytkownik końcowy nie jest identyfikowany podczas tego procesu.

System informacji zwrotnych ESET LiveGrid®. Próbki podejrzanego kodu i metadanych używane przez system

reputacji ESET LiveGrid®, które pozwalają produktom ESET reagować natychmiast na potrzeby użytkowników końcowych i zapewnić ochronę przed najnowszymi zagrożeniami. Korzystamy następujących danych otrzymanych od użytkowników końcowych

- Dane dotyczące infekcji, takie jak próbki potencjalnych wirusów i innych szkodliwych programów, a także podejrzane, potencjalnie niepożądane i potencjalnie niebezpieczne obiekty (np. pliki wykonywalne i wiadomości e-mail zgłoszone jako spam lub oznaczone przez nasz produkt);
- Informacje dotyczące korzystania z Internetu, takie jak adres IP, informacje geograficzne, pakiety IP, adresy URL i ramki sieci Ethernet;
- Pliki zrzutu awaryjnego i informacje w nich zawarte.

Nie mamy zamiaru gromadzić danych spoza tego zakresu, jednak czasami nie da się tego uniknąć. Przypadkowo zebrane dane mogą być zawarte w samym szkodliwym oprogramowaniu (i zebrane bez wiedzy i zgody użytkownika końcowego) lub mogą stanowić część nazwy pliku lub adresu URL. Nie zamierzamy wykorzystywać tych danych w naszych systemach ani przetwarzać ich w celu określonym w tej Polityce prywatności.

Wszystkie informacje uzyskane i przetwarzane za pośrednictwem systemu informacji zwrotnych ESET LiveGrid® są przeznaczone do użycia bez identyfikowania Użytkownika końcowego.

Pomoc techniczna. Aby zapewnić możliwość świadczenia pomocy technicznej lub pomocy innego rodzaju, mogą być wymagane dane kontaktowe i informacje dotyczące licencji przesyłane w zgłoszeniach do działu pomocy. W zależności od wybranego przez Użytkownika końcowego sposobu komunikacji możemy gromadzić następujące dane: adres e-mail, numer telefonu, informacje o licencji, szczegółowe informacje o produkcie oraz opis zgłoszenia do pomocy technicznej. W celu podniesienia jakości udzielanej pomocy technicznej możemy poprosić Użytkownika końcowego o dodatkowe informacje. Dane przetwarzane w celu świadczenia pomocy technicznej są przechowywane przez 4 lata.

Należy pamiętać, że jeśli osoba korzystająca z naszych produktów i usług nie jest Użytkownikiem końcowym, który zakupił produkt lub usługę i zaakceptował Warunki (np. pracownik Użytkownika końcowego, członek rodziny lub osoba w inny sposób upoważniona przez Użytkownika końcowego do korzystania z produktu lub usługi zgodnie z Warunkami), przetwarzanie danych odbywa się w uzasadnionym interesie firmy ESET w rozumieniu art. 6 ust. 1 lit. f ustawy RODO, aby umożliwić użytkownikowi upoważnionemu przez Użytkownika końcowego korzystanie z produktów i usług świadczonych przez nas zgodnie z Warunkami.

Informacje kontaktowe

Jeżeli użytkownik chce skorzystać z prawa przysługującego mu jako osobie, której dane dotyczą, a także w przypadku pytań lub wątpliwości, użytkownik może przesłać do nas wiadomość na adres:

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