Plan ochrony danych

Niniejszy Plan ochrony danych („**Plan**") ma zastosowanie, jeśli usługi świadczone („**Usługi**") Klientowi („**Klient**") przez Dell sp. z o.o. albo podmioty z grupy kapitałowej Dell Technologies (łącznie „**Dell EMC**") obejmują przetwarzanie Danych osobowych (jak określono poniżej), które podlega Przepisom o ochronie prywatności a Dell EMC działa jako Podmiot przetwarzający w imieniu Klienta jako Administratora. Niniejszy Plan nie ma zastosowania w przypadku, gdy Dell jest Administratorem. W przypadku sprzeczności między niniejszym Planem a Umową pierwszeństwo mają postanowienia Planu.

1. **Definicje.** Termin niezdefiniowane poniżej mają znaczenie nadane im w Umowie. Poniższe terminy mają następujące znaczenie:

1.1 „**Umowa**" oznacza umowę pomiędzy Klientem a Dell EMC w celu świadczenia Usług Klientowi.

1.2 „**Administrator danych**" oznacza podmiot, który samodzielnie bądź razem z innymi określa cele i sposoby przetwarzania Danych Osobowych.

1.3 „**RODO**" oznacza Ogólne Rozporządzenie Ochrony danych (EU) 2016/679.

1.4 „**Klauzule wzorcowe**" oznaczają Standardowe Klauzule Umowne do celów przekazywania danych osobowych (decyzja 2021/914/UE), które mogą być co pewien czas zmieniane lub zastępowane, dotyczące przekazywania z Europejskiego Obszaru Gospodarczego („**EOG**") do krajów spoza EOG (w tym do Wielkiej Brytanii („**UK**")) oraz oznaczają Standardowe Klauzule Umowne do celów przekazywania danych osobowych do Podmiotów przetwarzających (decyzja 2010/87/UE) dotyczące przekazywania z Wielkiej Brytanii do krajów, które nie są objęte decyzją stwierdzającą odpowiedni poziom ochrony na mocy UK RODO.

1.5 „**Dane osobowe**" oznaczają wszelkie informacje dotyczące zidentyfikowanej bądź możliwej do zidentyfikowania osoby fizycznej, które są przetwarzane przez Dell EMC w związku z wykonaniem Umowy.

1.6 „**Naruszenie ochrony danych osobowych**" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych na podstawie niniejszego Planu.

1.7 „**Przepisy o ochronie prywatności**" oznaczają wszelkie przepisy dotyczące ochrony danych lub prywatności, którym podlega strona Umowy i które mają zastosowanie w przypadku dostarczanych Usług, w tym RODO (i/lub UK RODO).

1.8 „**Przetwarzanie**" oznacza dowolną operację lub zestaw operacji, wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

1.9 „**Podmiot przetwarzający**" oznacza podmiot, który przetwarza Dane osobowe w imieniu Administratora.

1.10 „**Podwykonawca przetwarzania**" oznacza Podmiot przetwarzający zatrudniony przez Dell EMC w celu świadczenia Usług.

1.11 „**UK RODO**" oznacza rozporządzenie RODO w wersji utrzymanej w prawie krajowym Wielkiej Brytanii po wyjściu Wielkiej Brytanii z Unii Europejskiej, które należy interpretować wraz z brytyjską Ustawą o Ochronie Danych (ang. *UK Data Protection Act 2018*), z uwzględnieniem zmian, które mogą być wprowadzane co pewien czas.

2. **Przetwarzanie Danych osobowych**

2.1 Rola Stron. Dell może przetwarzać Dane osobowe na podstawie Umowy jako Podmiot przetwarzający w imieniu Klienta jako Administratora.

2.2 Instrukcje. Dell EMC będzie przetwarzać Dane osobowe zgodnie z udokumentowanymi instrukcjami Klienta. Niniejszy Plan, Umowa oraz wszelkie kolejne zestawienia zakresu prac lub

zamówienia na usługi oraz wszelkie konfiguracje wprowadzone przez Klienta lub jego upoważnionych użytkowników składają się na kompletne instrukcje Klienta dla Dell EMC dotyczące przetwarzania Danych osobowych. Strony muszą uzgodnić wszelkie dodatkowe lub alternatywne instrukcje na piśmie, m.in. dotyczące kosztów (jeśli występują) związanych z wypełnieniem takich instrukcji. Dell EMC nie odpowiada za ustalenie, czy instrukcje Klienta są zgodne z obowiązującym prawem. Jednak, jeśli Dell EMC jest zdania, że instrukcje Klienta naruszają obowiązujące Przepisy o ochronie prywatności, Dell EMC powiadomi o tym fakcie Klienta tak szybko, jak będzie to uzasadnione ze względów praktycznych i nie będzie związany taką naruszającą przepisy instrukcją.

2.3 Szczegółowe informacje. Szczegółowe informacje dotyczące przedmiotu przetwarzania, jego czasu trwania, charakteru i celu oraz rodzaju Danych osobowych i osób, których one dotyczą, określono w Załączniku 2 Planu

2.4 Zgodność. Klient i Dell EMC zgadzają się przestrzegać obowiązków wynikających z Przepisów o ochronie prywatności mających zastosowanie do Danych osobowych Przetwarzanych w związku z Usługami. Klient jest wyłącznie odpowiedzialny za zgodność z Przepisami o ochronie prywatności określającymi zgodność z prawem Przetwarzania Danych osobowych przed ujawnieniem, przekazaniem lub udostępnieniem w inny sposób jakichkolwiek Danych osobowych firmie Dell EMC.

3. Podwykonawcy przetwarzania

3.1 Wykorzystanie Podwykonawców przetwarzania. Dell EMC może wyznaczać oraz korzystać z usług Podwykonawców przetwarzania, aby przetwarzać Dane osobowe w związku z Usługami na podstawie ogólnej lub szczegółowej zgody Klienta. Klient zgadza się, że Dell EMC może wyznaczać oraz korzystać z usług Podwykonawców przetwarzania, aby przetwarzać Dane osobowe w związku z Usługami o ile Dell EMC sporządzi umowę w formie pisemnej z każdym Podwykonawcą przetwarzania, która będzie nakładać zobowiązania: (i) stosowne dla usług, które mają dostarczyć Podwykonawcy przetwarzania, oraz (ii) w istotny sposób odzwierciedlające prawa lub zobowiązania przyznane lub nałożone na Dell EMC na mocy niniejszego Planu. Podwykonawcy przetwarzania mogą obejmować osoby trzecie lub innych członków grupy kapitałowej Dell Technologies. Jeśli Podwykonawca przetwarzania nie wypełni zobowiązań ochrony danych, jak określono powyżej, Dell EMC będzie odpowiadać wobec Klienta za wypełnienie zobowiązań Podwykonawcy przetwarzania.

3.2 Lista Podwykonawców przetwarzania. Dell EMC przekażę listę Podwykonawców przetwarzania, których wykorzystuje do świadczenia Usług na pisemny wniosek Klienta lub udostępni ją na stronie internetowej Dell. Dell EMC poinformuje Klienta o zmianach na liście Podwykonawców przetwarzania. Jeśli Klient w uzasadniony sposób sprzeciwi się dodaniu lub usunięciu podmiotu z listy Podwykonawców przetwarzania i Dell EMC nie będzie w stanie rozsądnie dostosować się do sprzeciwu Klienta, strony w dobrej wierze podejmą rozmowy w celu omówienia obaw Klienta z ustaleniem możliwych sposobów rozwiązania tych kwestii.

4. Bezpieczeństwo

4.1 Techniczne i organizacyjne środki bezpieczeństwa. Uwzględniając standardy obowiązujące w branży, koszty wdrażania, charakter, zakres, kontekst i cele Przetwarzania oraz wszelkie inne istotne okoliczności związane z przetwarzaniem Danych osobowych w systemach Dell EMC, Dell EMC zastosuje odpowiednie środki techniczne i organizacyjne, aby zadbać o to, by bezpieczeństwo, poufność, integralność, dostępność oraz odporność systemów i usług przetwarzania używanych do przetwarzania Danych osobowych były współmierne do ryzyka względem takich Danych osobowych. Strony zgadzają się, że środki bezpieczeństwa opisane w Załączniku 1 („**Środki bezpieczeństwa informacji**”) zapewniają odpowiedni poziom bezpieczeństwa ochrony Danych osobowych, aby spełnić wymagania niniejszej klauzuli. Dell EMC będzie okresowo (i) testować i monitorować skuteczność swoich zabezpieczeń, mechanizmów kontroli, systemów i procedur oraz (ii) rozpoznawać zasadnie przewidywalne zagrożenia z wewnątrz i z zewnątrz w zakresie bezpieczeństwa, poufności i integralności Danych osobowych, aby zapewnić przed nimi ochronę.

4.2 Postęp technologiczny. Środki bezpieczeństwa informacji podlegają procesowi postępu i rozwoju i Dell EMC może zmodyfikować te środki, o ile wprowadzone modyfikacje nie pogorszą ogólnego bezpieczeństwa Usług świadczonych na podstawie Umowy.

4.3 Dostęp. Dell EMC zapewni, że osoby mające dostęp do Danych osobowych: (i) zobowiązały się do zachowania poufności albo podlegają odpowiedniemu ustawowemu obowiązkowi zachowania poufności i (ii) będą miały dostęp do Danych osobowych tylko na podstawie udokumentowanych

instrukcji Dell EMC, chyba że dostęp wymagany jest przepisami prawa.

5. **Naruszenie ochrony danych osobowych.** Dell EMC poinformuje Klienta niezwłocznie o powzięciu wiadomości o Naruszeniu ochrony danych osobowych w związku z Usługami świadczonymi przez DELL EMC na podstawie Umowy i dołoży należytej staranności w celu asystowania Klientowi wzłagodzeniu, tam gdzie to możliwe, niekorzystnych skutków Naruszenia ochrony danych osobowych.

6. **Przekazywanie między państwami.** Dell EMC jest uprawniony, w związku z dostarczaniem Usług lub w ramach zwykłej działalności przekazywać Dane osobowe podmiotom powiązanym lub Podwykonawcom przetwarzania znajdującym się na całym świecie. Podczas takiego przekazywania Dell EMC zadba o zastosowanie odpowiedniej ochrony, aby zabezpieczyć Dane osobowe przekazywane na mocy lub w związku z niniejszą Umową. Jeżeli dostarczanie Usług obejmuje przekazywanie Danych osobowych z Europejskiego Obszaru Gospodarczego („**EOG**") lub Wielkiej Brytanii do krajów poza EOG lub Wielką Brytanią (które nie są objęte decyzją w sprawie odpowiedniej ochrony danych osobowych wydaną namocy Przepisów o ochronie prywatności lub odpowiednio UK RODO), takie przekazanie będzie podlegać następującym wymaganiom: (a) Dell EMC ma zawarte umowy wewnątrz grupy kapitałowej z podmiotami powiązanymi, któremogą mieć dostęp do Danych osobowych, a do umów zostały włączone odpowiednie Klauzule wzorcowe; i (b) Dell EMC ma zawarte umowy z Podwykonawcami przetwarzania, do których to umów w stosownych przypadkach zostały włączone odpowiednie Klauzule wzorcowe.

7. **Usunięcie Danych osobowych.** Po zakończeniu świadczenia Usług (niezależnie od przyczyny) i na pisemny wniosek Klienta tak szybko, jak jest to uzasadnione ze względów praktycznych, Dell EMC usunie lub zwróci Dane osobowe z systemów Dell EMC, chyba że właściwe przepisy wymagają przechowywania Danych osobowych. Dell może odłożyć w czasie usunięcie Danych osobowych w zakresie, w jakim Dane osobowe i ich kopie nie mogą zostać rozsądnie i praktycznie usunięte z systemów Dell EMC. W takim wypadku postanowienia niniejszego Planu będą miały w dalszym ciągu zastosowanie do takich Danych osobowych. Dell EMC zastrzega sobie prawo do obciążenia Klienta wszelkimi uzasadnionymi kosztami i wydatkami poniesionymi przez Dell EMC na skutek usunięcia Danych osobowych zgodnie z niniejszą klauzulą.

8. Współpraca

8.1 Żądania Podmiotów danych. Dell EMC niezwłocznie poinformuje Klienta o wszelkich żądaniach otrzymanych od osób fizycznych wykonujących swoje prawa podmiotów danych zgodnie z Przepisami o ochronie prywatności. Klient odpowiada za odpowiedzi na takie żądania. Dell EMC w rozsądny sposób może wspomóc Klienta w odpowiedzi na takie żądania, w zakresie w jakim Klient nie jest w stanie samodzielnie dotrzeć do właściwych Danych osobowych wykorzystywanych w ramach świadczonych Usług. Dell EMC zastrzega sobie prawo do obciążenia Klienta wszelkimi uzasadnionymi kosztami i wydatkami poniesionymi przez Dell EMC na skutek pomocy ponad kwotę nominalną.

8.2 Żądania podmiotów trzecich. Jeśli Dell EMC otrzyma jakiekolwiek żądanie od osoby trzeciej lub wniosek z sądu, trybunału, organu administracji lub agencji rządowej właściwej jurysdykcji w zakresie, w jakim Dell EMC jest podmiotem związanym z Przetwarzaniem Danych osobowych zgodnie z Umową, Dell EMC niezwłocznie przekieruje takie żądanie do Klienta. Dell EMC nie odpowie na takie żądanie bez wcześniejszej zgody Klienta, chyba że obowiązek odpowiedzi wynika z przepisów prawa. Dell EMC, o ile przepisy prawa tego nie zabraniają, poinformuje Klienta uprzednio o ujawnieniu Danych osobowych i będzie współpracować z Klientem w celu ograniczenia zakresu tak przekazywanych danych to niezbędnego prawnie minimum.

8.3 Oceny wpływu na prywatność i uprzednie konsultacje. W zakresie w jakim jest to wymagane Przepisami o ochronie prywatności, Dell EMC zapewni Klientowi możliwość odpowiedniej współpracy i pomocy w zakresie stosownym do przetwarzania Danych osobowych przez Dell EMC i w zakresie uzgodnionych Usług w związku z ocenami wpływu na ochronę danych, których może dokonać Klient w związku z przetwarzaniem Danych osobowych przez Dell EMC, m.in. wszelkie wymagane wcześniejsze konsultacje z podmiotami nadzorującymi. Dell EMC zastrzega sobie prawo do obciążenia Klienta stosowną opłatą za zapewnienie takiej współpracy i pomocy.

9. **Wykazanie zgodności:** Na uzasadniony wcześniejszy wniosek Klienta w formie pisemnej (złożony zgodnie z odpowiednimi warunkami Umowy) Dell EMC przekaże Klientowi informacje, jakie mogą być zasadnie wymagane aby wykazać zgodność Dell EMC z zobowiązaniami wynikającymi z niniejszego Planu w celu umożliwienia audytów, inspekcji wykonanych przez Klienta

Załącznik 1

Środki bezpieczeństwa informacji

Dell traktuje kwestie bezpieczeństwa informacji bardzo poważnie. Niniejsze omówienie kwestii bezpieczeństwa informacji dotyczy środków nadzoru korporacyjnego stosowanych przez Dell w celu zabezpieczania danych osobowych, które są przetwarzane i przekazywane między spółkami grupy Dell. Program bezpieczeństwa informacji Dell pozwala personelowi zapoznać się ze swoimi obowiązkami. Niektóre rozwiązania klienckie mogą posiadać alternatywne zabezpieczenia opisane w zestawieniu zakresu prac w zależności od ustaleń z poszczególnymi klientami.

Praktyki w zakresie bezpieczeństwa

Dell wprowadził praktyki i standardy w zakresie bezpieczeństwa informacji przedsiębiorstwa, które mają na celu chronić środowisko przedsiębiorstwa Dell oraz regulować kwestie: (1) bezpieczeństwa informacji; (2) zarządzania systemami i zasobami; (3) rozwoju oraz (4) zarządzania. Te praktyki i standardy są zatwierdzane przez dyrektora ds. informatycznych Dell i raz w roku podlegają oficjalnej ocenie.

Bezpieczeństwo organizacji

Przestrzeganie tych praktyk i standardów jest obowiązkiem wszystkich osób w organizacji. Aby ułatwić przestrzeganie tych praktyk i standardów w wymiarze przedsiębiorstwa, pion bezpieczeństwa informacji zapewnia:

1. strategię i zgodność z zasadami/standardami oraz regulacjami, wiedzę i edukację, ocenę ryzyka i zarządzanie ryzykiem, zarządzanie wymaganiami bezpieczeństwa umów, doradztwo w zakresie aplikacji i infrastruktury, testowanie kontroli i kieruje bezpieczeństwem firmy,
2. testowanie bezpieczeństwa, opracowywanie i wdrażanie rozwiązań z zakresu bezpieczeństwa, aby umożliwić przyjmowanie środków nadzoru bezpieczeństwa w całym środowisku przedsiębiorstwa,
3. podejmowanie czynności bezpieczeństwa w zakresie wdrożonych rozwiązań bezpieczeństwa, środowiska i zasobów oraz zarządzania odpowiedzią na zdarzenia,
4. prowadzenie dochodzeń w postępowaniach sądowych z zasobami działów bezpieczeństwa operacji, prawnym, ochrony danych i zasobów ludzkich będące przedmiotem dochodzenia, w tym eDiscovery i eForensics.

Klasyfikacja i kontrola zasobów

Praktyką Dell jest śledzenie zasobów fizycznych i logicznych oraz zarządzanie nimi. przykładowe zasoby, które może śledzić dział informatyczny Dell:

- zasoby informacyjne, np. zidentyfikowane bazy danych, plany odtwarzania po awarii, plany ciągłości działalności, klasyfikacje danych, informacje archiwizowane,
- zasoby oprogramowania, np. zidentyfikowane aplikacji i oprogramowanie systemowe,
- zasoby fizyczne, np. zidentyfikowane serwery, komputery stacjonarne/laptopy, taśmy zawierające kopie zapasowe/archiwa, drukarki i sprzęt komunikacyjny.

Zasoby są klasyfikowane w oparciu o znaczenie dla prowadzonej działalności po to, by ustalić wymagania związane z poufnością. Zalecenia dla branży dotyczące obsługi danych osobowych zawierają wytyczne w zakresie zabezpieczeń technicznych, organizacyjnych i fizycznych. Mogą one obejmować środki nadzoru, takie jak zarządzanie dostępem, szyfrowanie, logowanie i monitoring oraz niszczenie danych.

Bezpieczeństwo personelu

W ramach procesu rekrutacji pracownicy przechodzą kontrolę bezpieczeństwa w zgodzie z lokalnymi przepisami. Doroczne szkolenie Dell z zakresu zgodności obejmuje wymóg, by pracownicy ukończyli kurs internetowy oraz zdali sprawdzian dotyczący bezpieczeństwa informacji i prywatności danych. Program wiedzy o bezpieczeństwie może również zapewnić materiały specyficzne dla niektórych stanowisk.

Bezpieczeństwo fizyczne i środowiskowe

W zakresie ograniczania ryzyka Dell w ramach swojego programu bezpieczeństwa fizycznego wykorzystuje rozwiązania technologiczne i operacyjne. Zespół ds. bezpieczeństwa ściśle współpracuje z poszczególnymi zakładami, aby ustalić, czy istnieją odpowiednie środki zaradcze i stale monitorować wszelkie zmiany dotyczące infrastruktury fizycznej, przedsiębiorstwa i znanych zagrożeń. Monitoruje również środki w zakresie najlepszych praktyk wykorzystywane przez inne podmioty w branży i starannie dobiera rozwiązania, które są nie tylko wyjątkowe w zakresie praktyk biznesowych, ale również spełniają wymagania Dell. Dell równoważy swoją koncepcję bezpieczeństwa, uwzględniając elementy nadzoru, które obejmują architekturę, operacje i systemy.

Zarządzanie komunikacją i operacjami

Dział IT zarządza zmianami w infrastrukturze, systemach i aplikacjach przedsiębiorstwa poprzez scentralizowany program zarządzania zmianami, który może obejmować testowanie, analizę wpływu na działalność oraz zatwierdzanie zarządzania w stosownych przypadkach.

Istnieją procedury odpowiedzi na zdarzenia na wypadek incydentów dotyczących bezpieczeństwa i ochrony danych. Mogą obejmować analizę incydentów, zabezpieczanie przed nimi, reagowanie na nie, podejmowanie środków zaradczych w przypadku ich wystąpienia, zgłaszanie ich oraz powrót do zwykłej działalności.

W celu ochrony przed złośliwym użyciem zasobów i złośliwym oprogramowaniem mogą zostać wprowadzone dodatkowe środki nadzoru w zależności od ryzyka. Takie środki nadzoru mogą obejmować m.in. praktyki i standardy w zakresie bezpieczeństwa informacji, ograniczony dostęp, wyznaczony rozwój i środowiska testowe, wykrywanie wirusów na serwerach, komputerach stacjonarnych i laptopach, skanowanie załączników w wiadomościach e-mail pod kątem wirusów, skanowanie pod kątem zgodności z systemem, monitorowanie pod kątem ochrony przed włamaniami oraz reagowanie na nie, logowanie i wysyłanie alertów w przypadku istotnych zdarzeń, procedury obsługi informacji w oparciu o typ danych, bezpieczeństwo sieci

oraz aplikacji do handlu elektronicznego, skanowanie pod kątem luk w zabezpieczeniach systemów i aplikacji.

Środki kontroli dostępu

Dostęp do systemów przedsiębiorstwa jest ograniczony, oparty na procedurach mających zapewnić odpowiednie zgody. Aby ograniczyć ryzyko nieodpowiedniego użycia niezależnie od tego, czy jest ono celowe, dostęp jest udzielany w oparciu o podział obowiązków oraz przyznawanie możliwie najmniejszych uprawnień.

Dostęp zdalny oraz funkcje łączności bezprzewodowych są ograniczone i w celu dostępu wymagają istnienia zabezpieczeń użytkownika i systemu.

Określone dzienniki zdarzeń z kluczowych urządzeń i systemów są gromadzone centralnie i zgłaszane w oparciu o wyjątki, aby umożliwić reagowanie na zdarzenia i przeprowadzanie dochodzeń.

Tworzenie i konserwacja systemu

Luki w zabezpieczeniach innych producentów podane do publicznej wiadomości są weryfikowane pod kątem znaczenia dla środowiska Dell. W zależności od ryzyka dla działalności i klientów Dell istnieją z góry ustalone ramy czasowe do podjęcia środków zaradczych. Ponadto dla nowych i istotnych aplikacji oraz infrastruktury wykonuje się skanowanie i ocenę pod kątem luk w zabezpieczeniach w oparciu o ryzyko. Weryfikacje kodu i skanery wykorzystywane są w środowisku programistycznym przed przekazaniem do produkcji, w celu aktywnego wykrywania luk w zabezpieczeniach kodu w oparciu o ryzyko. Te procesy umożliwiają aktywną identyfikację luk w zabezpieczeniach oraz zgodność.

Zgodność z przepisami

Działy ds. bezpieczeństwa informacji, prawny, prywatności i zgodności z przepisami pracują w celu identyfikacji praw i regulacji regionalnych dotyczących przedsiębiorstwa Dell. Wymagania te dotyczą takich kwestii, jak własność intelektualna przedsiębiorstwa i naszych klientów, licencje na oprogramowanie, ochrona danych osobowych pracowników i klientów, procedury ochrony danych i obsługi danych, transgraniczna transmisja danych, procedury finansowe i operacyjne, ustawowe przepisy eksportowe w zakresie technologii oraz wymagania z dziedziny kryminalistyki.

Takie rozwiązania, jak program bezpieczeństwa informacji, rada prywatności kadry kierowniczej, audyty/oceny zewnętrzne/wewnętrzne, konsultacje z wewnętrznym i zewnętrznym doradcą prawnym, ocena wewnętrznych środków nadzoru, oceny wewnętrznych testów penetracyjnych i luk w zabezpieczeniach, zarządzanie umowami, wiedza o bezpieczeństwie, konsultacje w zakresie bezpieczeństwa, weryfikacje wyjątków w polityce oraz zarządzanie ryzykiem, łącznie pozwalają zachować zgodność z tymi wymaganiami.

Załącznik 2

Opis przetwarzania danych

1. Przedmiot i czas trwania Przetwarzania

Przedmiot i czas trwania Przetwarzania będą zgodne z Umową.

2. Cel przetwarzania

Dane osobowe będą przetwarzane w celu świadczenia usług związanych z gwarancją i wsparciem lub wdrożeniem, zgodnie i odpowiednio z wybranymi poziomami usług i opcjami wsparcia. Umowa i odpowiednie opisy usług oraz wyszczególnienia zakresu prac mają zastosowanie do szczegółów i możliwych dodatkowych usług.

3. Charakter przetwarzania.

3.1. Wsparcie IT: Podmiot przetwarzający przetwarza głównie adresy IP, adresy MAC lub inne identyfikatory techniczne systemów informatycznych, które mogą być przypisane do osoby. Zwykle dzieje się to, jeśli to konieczne, poprzez analizę dzienników błędów.

3.2. Usługi pomocy technicznej: personel Podmiotu przetwarzającego może wejść w kontakt z Danymi osobowymi, w zależności od regulacji wewnętrznych Administratora, przy okazji świadczenia usług wsparcia i pomocy technicznej. Może się to zdarzyć, w czasie zapewniania zdalnego wsparcia lub wchodząc do pomieszczeń Administratora w celu naprawy sprzętu. W takich przypadkach technik może zobaczyć dokumenty, plakietki, treści na ekranach. To samo może mieć miejsce w przypadku zdalnego wsparcia poprzez udostępnianie ekranu (np. przez webex), jeśli Administrator nie zamknął odpowiednich programów przed połączeniem.

3.3. Pliki trace dump: W przypadku niektórych produktów i niektórych sytuacji wsparcia plik trace dump może być analizowany w celu oceny problemu. Plik trace dump zawiera aktywność odczytu/zapisu lub transferu powiązanego z błędem. Treść jest napisana w ogólnym formacie błędu danego Systemu Operacyjnego i jest niezależna od typów plików. Rekonstrukcja plików i ich potencjalnej zawartości nie jest częścią analizy. Jest bardzo mało prawdopodobne, że jakiekolwiek dane osobowe będą możliwe do odczytania podczas analizy.

3.4. Urządzenia do przechowywania danych: Zwrot lub odnowienie sprzętowych urządzeń pamięci masowej (np. dysków twardych, dysków SSD itp.), Wszystkie dane na nich zawarte zostaną usunięte lub zniszczone w zautomatyzowanych procesach.

4. Kategorie podmiotów danych

Osoby, których dane dotyczą, mogą być użytkownikami końcowymi Klienta, pracownikami, kontrahentami, dostawcami i innymi stronami trzecimi związanymi z Usługami.

5. Kategorie danych osobowych

Kategorie danych osobowych, które mogą być przesyłane przez klienta, to:

- **Dane kontaktowe:** mogą zawierać imię i nazwisko, adres, adres e-mail, telefon, faks, inne dane kontaktowe, dane kontaktowe awaryjne, powiązane informacje o lokalnej strefie czasowej.
- **Dane klienta:** mogą zawierać dane kontaktowe, dane do fakturowania i dane dotyczące finansów.
- **Systemy informatyczne i informacje operacyjne:** mogą obejmować identyfikatory osobiste, głos, nagrania wideo i danych, dane użytkownika i hasło, nazwa komputera, adres e-mail, nazwa domeny, nazwy użytkowników, hasła, adresy IP, dane o zezwoleniach (według stanowisk), informacje o kontach i delegowaniu do usług komunikacyjnych, indywidualne skrzynki pocztowe i katalogi, dane komunikacyjne czatu, spis oprogramowania i sprzętu, śledzenie informacje dotyczące wzorców korzystania z oprogramowania i Internetu (np. plików cookie) oraz informacje o nich zapisane do celów operacyjnych i/lub szkoleniowych).
- **Treść wiadomości e-mail osób, których dane dotyczą oraz dane o ruchu / transmisji;** interaktywna i głosowa komunikacja online (taka jako blogi, czat, kamera internetowa i sesje sieciowe); usługi wsparcia (dostęp przypadkowy może obejmować dostęp do treść wiadomości e-mail i dane dotyczące wysyłania, kierowania i dostarczania wiadomości e-mail)
- **Inne:** wszelkie inne dane osobowe przekazane przez Klienta Dostawcy jako Podmiotowi przetwarzającemu w imieniu Klienta.

6. Podwykonawcy przetwarzania

6.1. Podmiot przetwarzający może angażować spółki powiązane, z zastrzeżeniem wymogów określonych w Planie ochrony danych, co obejmuje m.in. zawarcie Standardowych Klauzul Umownych UE w przypadku przekazywania poza Europejski Obszar Gospodarczy.

6.2. Dodatkowo mogą zostać zaangażowane strony trzecie, z zastrzeżeniem wymogów określonych w Planie ochrony danych, co obejmuje zawarcie Standardowych Klauzul Umownych UE w przypadku przekazywania poza Europejski Obszar Gospodarczy.

Szczegółowe informacje dotyczące Podwykonawców przetwarzania Dell EMC wymienionych w sekcjach 6.1 i 6.2

znajdują się na stronie www.dell.com/subprocessors

7. Dane kontaktowe Podmiotu przetwarzającego

W przypadku zapytań o ochronę danych możesz wysłać zapytanie:

1. Osobie kontaktowej wskazanej w Umowie; lub
2. Przez wiadomość e-mail na adres: privacy@dell.com