Plan ochrony danych

Niniejszy Plan ochrony danych („**Plan**") ma zastosowanie, jeśli Usługi świadczone Klientowi przez Dell sp. z o.o. lub EMC Computer Systems Poland 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. W przypadku sprzeczności między niniejszym Planem a Umową pierwszeństwo mają postanowienia Planu.

1. **Definicje:** Poniższe terminy mają następujące znaczenie:

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

   (b) „**Klauzule wzorcowe**" oznaczają Standardowe klauzule umowne (transfer od Administratora do Podmiotu przetwarzającego) zatwierdzone przez Komisję Europejską dotyczące przenoszenia danych osobowych do krajów poza Europejskim Obszarem Gospodarczym („**EOG**"), które nie zostały uznane przez Komisję Europejską jako kraje zapewniające należyty poziom ochrony danych.

   (c) „**Dane osobowe**" oznaczają wszelkie informacje dotyczące zidentyfikowanej bądź możliwej do zidentyfikowania osoby fizycznej, które są przetwarzane przez Dell EMC występujący w roli Podmiotu przetwarzającego w imieniu Klienta w związku z dostarczaniem Usług i podlegają Przepisom o ochronie prywatności.

   (d) „**Przepisy o ochronie prywatności**" oznaczają wszelkie przepisy, statuty, dyrektywy lub rozporządzenia (oraz wszelkie poprawki lub nowe wersje wspomnianych dokumentów) dotyczące ochrony danych lub prywatności, którym podlega strona niniejszej Umowy i które mają zastosowanie w przypadku dostarczanych Usług.

   (e) „**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.

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

   (g) „**Incydent dotyczący bezpieczeństwa**" oznacza istotne naruszenie zobowiązań w zakresie bezpieczeństwa na mocy niniejszego Planu przez Dell EMC prowadzące w przypadkowy lub bezprawny sposób do zniszczenia, utraty, zmiany, bezprawnego ujawnienia lub uzyskania dostępu do Danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

   (h) „**Podwykonawca przetwarzania**" oznacza osobę trzecią zatrudnioną przez Dell EMC (w tym między innymi podmiot powiązany lub podwykonawcę Dell EMC) w związku z przetwarzaniem Danych osobowych w zakresie dostarczania Usług.

2. **Instrukcje i szczegółowe informacje dotyczące przetwarzania:** Klient upoważnia Dell EMC do przetwarzania Danych osobowych w celu dostarczania Usług zgodnie z prawami i obowiązkami Dell EMC na mocy Umowy oraz wszelkich kolejnych zestawień zakresu prac lub zamówień na usługi oraz do wykorzystania danych o wynikach dotyczących dostarczania Usług i przetwarzania Danych osobowych w celu poprawy jakości lub ulepszenia produktów i usług Dell EMC. 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. Klient akceptuje, że nie będzie wymagać, by Dell EMC podejmował lub angażował się w działania, które wymagałyby lub powodowałyby, że Dell EMC będzie występował w charakterze Administratora. 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. Szczegółowe informacje dotyczące przedmiotu przetwarzania, jego czasu trwania, charakteru i celu oraz rodzaju

Danych osobowych i osób, których one dotyczą, określono w opisie Usług, Umowie lub Załączniku 1 do Klauzul wzorcowych (jeśli został podpisany). Z wyjątkiem przypadków, w których wyraźnie określono inaczej, Klient jest Administratorem, a Dell EMC jest Podmiotem przetwarzającym Dane osobowe przetwarzane na mocy Umowy.

3. **Ujawnianie:** Dell EMC może ujawniać Dane osobowe osobom trzecim (m.in. Podwykonawcom przetwarzania, podmiotom powiązanym oraz podwykonawcom) wyłącznie w celu: (a) stosowania się do uzasadnionych i zgodnych z prawem instrukcji Klienta; (b) zgodnie z wymaganiami związanymi z Usługami oraz na ile jest to dopuszczalne w ramach niniejszego Planu lub (c) na ile jest to konieczne, aby przestrzegać Przepisów o ochronie prywatności bądź nakazu dowolnego sądu, trybunału, organu regulacyjnego lub agencji rządowej z właściwą jurysdykcją, której podlega Dell EMC POD WARUNKIEM, że Dell EMC (w zakresie dozwolonym przepisami prawa) poinformuje Klienta z wyprzedzeniem o każdym przypadku ujawnienia Danych osobowych i będzie współpracować w sposób zasadny z Klientem w celu ograniczenia zakresu takiego ujawnienia wyłącznie w stopniu wymaganym przez prawo.

4. **Zgodność z przepisami:** Klient i Dell EMC zgadzają się przestrzegać odpowiednich zobowiązań wynikających z Przepisów o ochronie prywatności dotyczących Usług. Klient gwarantuje i oświadcza (w imieniu swoim oraz wszystkich swoich podmiotów powiązanych), że uzyskał wszelkie niezbędne upoważnienia i zgody wymagane do przestrzegania Przepisów o ochronie prywatności przed ujawnieniem, przeniesieniem lub udostępnieniem w inny sposób jakichkolwiek Danych osobowych na rzecz Dell EMC. Jeśli jest to wymagane w związku z Usługami i w zakresie, w którym jest to praktyczne ze względów handlowych, Dell EMC będzie pomagać Klientowi w odpowiadaniu na żądania wykonywania praw poszczególnych osób na mocy obowiązujących Przepisów o ochronie prywatności. Dell EMC zastrzega sobie prawo do obciążenia Klienta kosztami takiej pomocy, jeśli przekraczają one kwotę nominalną. Dell EMC powiadomi Klienta tak szybko jak będzie to uzasadnione ze względów praktycznych o wszystkich żądaniach, które Dell EMC otrzyma od osób fizycznych dotyczących wykonywania ich praw na mocy obowiązujących Przepisów o ochronie prywatności w okresie obowiązywania Umowy (w zakresie, w którym takie żądanie dotyczy Danych osobowych).

5. **Poufność:** W zakresie, w którym Dane osobowe są poufne (zgodnie z obowiązującym prawem), Dell EMC zachowa poufność Danych osobowych zgodnie z Przepisami o ochronie prywatności dotyczącymi Podmiotów przetwarzających i zadba o to, by pracownicy lub przedstawiciele Dell upoważnieni do przetwarzania Danych osobowych (w tym Podwykonawcy przetwarzania) zobowiązali się do przestrzegania poufności.

6. **Bezpieczeństwo:** 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 Aneksie 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. Dell EMC wprowadzi i udokumentuje odpowiednie plany ciągłości działalności oraz odtwarzania po awarii, co pozwoli na dalsze dostarczanie lub wznowienie Usług (w tym przywrócenie dostępu do Danych osobowych w zasadnych przypadkach) we właściwym czasie po zdarzeniu powodującym zakłócenia. Dell EMC będzie co jakiś czas testować i monitorować skuteczność swoich planów ciągłości działalności oraz odtwarzania po awarii. Dell EMC na pisemną prośbę Klienta przekaże mu podsumowanie planów ciągłości działalności oraz odtwarzania po awarii w formie pisemnej.

7. **Przekazywanie między państwami:** Dell EMC może 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 EOG do krajów poza EOG (które nie są objęte decyzją w sprawie odpowiedniej ochrony danych osobowych wydaną na mocy Przepisów o ochronie prywatności), takie przekazanie będzie podlegać następującym wymaganiom: (a) ma zawarte umowy wewnątrz grupy kapitałowej z podmiotami powiązanymi, które mogą mieć dostęp do Danych osobowych, a do umów zostały włączone Klauzule wzorcowe; i (b) Dell EMC ma zawarte umowy z Podwykonawcami przetwarzania, do których to umów w stosownych przypadkach zostały włączone Klauzule wzorcowe.

8. **Podwykonawcy przetwarzania:** Klient zgadza się, że Dell EMC może wyznaczać oraz korzystać z usług Podwykonawców przetwarzania, aby przetwarzać Dane osobowe w związku z Usługami POD

WARUNKIEM, że: (a) Dell EMC sporządzi umowę na piśmie z każdym Podwykonawcą przetwarzania, która będzie nakładać zobowiązania (i) stosowne dla usług, które mają dostarczyć Podwykonawcy przetwarzania, oraz (ii) istotny sposób odzwierciedlające prawa lub zobowiązania przyznane lub nałożone na Dell EMC na mocy niniejszego Planu, a także (b) jeśli Podwykonawca przetwarzania nie wypełni zobowiązań ochrony danych, jak określono powyżej, Dell EMC będzie odpowiadać wobec Klienta za wypełnienie zobowiązań Podwykonawcy przetwarzania.

9. **Klauzula dotycząca Oceny wpływu na prywatność (PIA):** 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 wszelkimi 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.
10. **Incydenty dotyczące bezpieczeństwa:** Jeżeli Incydent dotyczący bezpieczeństwa jest spowodowany tym, że Dell EMC nie przestrzega zobowiązań wynikających z niniejszego Planu, Dell EMC powiadomi Klienta bezzwłocznie po ustaleniu wystąpienia Incydentu dotyczącego bezpieczeństwa, jeżeli jest to wymagane na mocy obowiązujących Przepisów o ochronie prywatności, i:
    (a) w zakresie, w którym takie informacje są znane i dostępne Dell EMC w danym czasie, przekaże Klientowi szczegółowe informacje na temat Incydentu dotyczącego bezpieczeństwa, punktu kontaktowego oraz środków podejmowanych lub które zostaną podjęte w przypadku wystąpienia Incydentu dotyczącego bezpieczeństwa;
    (b) będzie odpowiednio współpracować z Klientem oraz udzieli mu pomocy w zakresie dochodzenia związanego z Incydentem dotyczącym bezpieczeństwa lub podejmowanych w związku z nim środków zaradczych (w tym między innymi, jeśli wymagają tego Przepisy o ochronie prywatności, dostarczania powiadomień organom regulacyjnym oraz osobom fizycznym, których taki incydent dotyczy);
    (c) nie poinformuje żadnych niepowiązanych osób trzecich (z wyjątkiem przypadków, gdy są to inni klienci, których ten Incydent dotyczący bezpieczeństwa obejmuje, Podwykonawcy przetwarzania, którzy mogą posiadać istotne informacje, lub eksperci czy doradcy zatrudniani przez Dell) o żadnym Incydencie dotyczącym bezpieczeństwa w związku z Danymi osobowymi bez wcześniejszego uzyskania pisemnej zgody Klienta, chyba że stosowne przepisy wymagają inaczej. Niniejsze postanowienie nie zabrania Dell EMC powiadomienia innych klientów, których danych osobowych może dotyczyć Incydent dotyczący bezpieczeństwa;
    (d) w przypadku gdy Klient zamierza przekazać powiadomienie na temat Incydentu dotyczącego bezpieczeństwa podmiotowi nadzorującemu ochronę danych, innemu organowi regulacyjnemu bądź organowi ścigania, Klient zezwoli Dell EMC (chyba że zabrania tego prawo) na weryfikację powiadomienia i Klient odpowiednio uwzględni wszelkie stosowne komentarze lub poprawki zaproponowane przez Dell EMC.
11. **Usunięcie Danych osobowych:** Po zakończeniu świadczenia Usług (niezależnie od przyczyny) i na pisemny wniosek Klienta tak szybko, jak jest to uzasadnione ze względów praktycznych i zgodnie z obowiązującym prawem, Dell EMC usunie Dane osobowe z systemów Dell EMC POD WARUNKIEM, że Dell EMC: (a) zachowa jedną kopię Danych osobowych, o ile będzie to konieczne do zachowania zgodności z wymaganiami prawnymi, regulacyjnymi, sądowymi, w zakresie kontroli lub zgodności wewnętrznej; i (b) odroczy usunięcie Danych osobowych w zakresie i w czasie, w którym Danych osobowych lub ich kopii nie można wykasować z systemów Dell EMC w sposób zasadny i ze względów praktycznych. W przypadku takich okresów zachowania lub odroczenia, jak określono w punktach (a) i (b) niniejszej klauzuli, postanowienia niniejszego Planu będą nadal obowiązywać w odniesieniu do rzeczonych 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.
12. **Wykazanie zgodności:** Na uzasadniony wcześniejszy wniosek Klienta w formie pisemnej (taki wniosek nie powinien być składany częściej niż raz na dwanaście miesięcy) Dell EMC przekaże Klientowi informacje, jakie mogą być zasadnie wymagane na mocy obowiązującego prawa oraz zgodnie z praktykami Dell EMC w zakresie bezpieczeństwa, aby wykazać zgodność Dell EMC z zobowiązaniami wynikającymi z niniejszego Planu.
13. **Odpowiedzialność i koszty:** Ani Dell EMC, ani Podwykonawca przetwarzania nie będą odpowiadać za żadne roszczenia wysuwane przez Klienta lub osoby trzecie wynikające z jakiegokolwiek działania lub zaniechania przez Dell EMC lub Podwykonawców przetwarzania w zakresie, w którym takie działanie lub zaniechanie będzie wynikało z przestrzegania instrukcji Klienta, jego praktyk w zakresie bezpieczeństwa, polityk lub procesów.

Aneks 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.