

Środki techniczne i organizacyjne

Ochrona Danych Osobowych

Spis treści

1.	**Wprowadzenie**	**3**
2.	**Środki ochrony o prywatności danych**	**4**
2.1.	Zarządzanie i model operacyjny	4
2.2.	Polityki, procesy i wytyczne	4
2.3.	Ochrona danych w fazie projektowania	4
2.4.	Krajobraz danych	4
2.5.	Zarządzanie cyklem życia informacji	4
2.6.	Prawa osób, których dane dotyczą	5
2.7.	Transgraniczne transfery danych	5
2.8.	Kwestie regulacyjne	5
2.9.	Szkolenia i świadomość	5
2.10.	Bezpieczeństwo dla prywatności	6
2.11.	Reagowanie na naruszenia i zgłoszenia naruszeń	6
2.12.	Zarządzanie dotyczące osób trzecich	6
3.	**Środki bezpieczeństwa informacji**	**7**
3.1.	Role i obowiązki w zakresie bezpieczeństwa informacji	7
3.2.	Polityka bezpieczeństwa informacji	7
3.3.	Zarządzanie urządzeniami mobilnymi	7
3.4.	Zasoby ludzkie	7
3.5.	Dopuszczelne użytkowanie	7
3.6.	Mechanizmy kontroli dostępu	8
3.7.	Zarzadzanie aktywami i ich klasyfikacja	8
3.8.	Bezpieczeństwo fizyczne i środowiskowe	8
3.9.	Bezpieczeństwo operacyjne	9
3.10.	Pozyskiwanie, rozwój i utrzymanie systemu	9
3.11.	Zarządzanie informacjami osób trzecich	9
3.12.	Zarządzanei incydentami związanymi z bezpieczeństwem informacji	9
3.13.	Ciągłość działania	9
3.14.	Zgodność	9

Wprowadzenie

Wizją NTT DATA jest stworzenie bezpiecznej i połączonej przyszłości dzięki technologii i innowacjom. Ustanowiliśmy nasze Środki Techniczne i Organizacyjne NTT DATA („ŚTiO"), które opisują, jak zapewniamy ochronę danych osobowych w sposób przejrzysty, uczciwy, etyczny i zgodny z prawem.

Nasze ŚTiO są oparte na najlepszych praktykach branżowych i obowiązujących wymogach prawnych w jurysdykcjach, w których działamy, z uwzględnieniem charakteru przetwarzanych przez nas danych i kosztów wdrożenia.

W razie jakichkolwiek pytań dotyczących naszych ŚTiO lub tego, jaki jest ich związek z naszymi produktami, usługami i rozwiązaniami należy skontaktować się z nami pod adresem eu.pl.kontakt@nttdata.com



Nasze ŚTiO są oparte na najlepszych praktykach branżowych i obowiązujących wymogach prawnych w jurysdykcjach, w których działamy, z uwzględnieniem charakteru przetwarzanych przez nas danych i kosztów wdrożenia.

Środki ochrony o prywatności danych

2.1. Zarządzanie i model operacyjny

NTT DATA jest zobowiązana do wykazania się odpowiedzialnością przy przetwarzaniu danych osobowych. Posiadamy odpowiednią struktury organizacyjne, role i obowiązki w zakresie zarządzania i zapewnienia nadzoru nad przetwarzaniem danych osobowych.

W każdej jurysdykcji, w której działamy, jednostki organizacyjne są zobowiązane do przeznaczania odpowiednich zasobów w celu przestrzegania obowiązujących przepisów o ochronie danych. Obejmuje to wyznaczanie wykwalifikowanych zasobów ds. prywatności danych w celu nadzorowania zgodności, a także ustanawianie odpowiednich struktur raportowania.

NTT DATA okresowo przedstawia kierownictwu wyższego szczebla raporty dotyczące projektu i skuteczności operacyjnej działań w zakresie ochrony i prywatności danych.

2.2. Polityki, procesy i wytyczne

NTT DATA wdrożyła i przekazała swoje polityki, procesy, standardy i wytyczne, które szczegółowo określają, w jaki sposób pracownicy NTT DATA mają przetwarzać dane osobowe. Należą do nich:

NTT DATA sformułowana i przekazała klauzule o ochronie danych, które informują pracowników, klientów i innych interesariuszy o sposobie przetwarzania danych osobowych.

NTT DATA wdrożyło procesy służące do przeprowadzania oceny ryzyka, w tym oceny skutków dla ochrony danych (DPIA), oceny uzasadnionych interesów (LIA) i oceny ryzyka transferu danych, zgodnie z obowiązującymi przepisami o ochronie danych.

2.3. Ochrona danych w fazie projektowania

NTT DATA zobowiązuje się do wdrażania uzasadnionych środków ułatwiających jej klientom przestrzeganie przepisów o ochronie danych. W miarę możliwości zasady ochrony danych w fazie projektowania i na zasadzie domyślnej są stosowane przy opracowywaniu produktów, usług i rozwiązań NTT DATA.

2.4. Krajobraz danych

NTT DATA wdrożyła procesy mające na celu identyfikację, utrwalanie, ocenę zrozumienie danych osobowych, które przetwarza.

NTT DATA prowadzi rejestr przetwarzanych danych osobowych zgodnie z obowiązującymi przepisami o ochronie danych.

2.5. Zarządzanie cyklem życia informacji

NTT DATA wdrożyła zasady i procesy zapewniające odpowiednie przetwarzanie danych osobowych w całym cyklu ich życia (od gromadzenia, poprzez wykorzystanie, przechowywanie, ujawnianie i niszczenie).

NTT DATA posiada politykę i harmonogram przechowywania danych, które są dostosowane do obowiązujących przepisów. NTT DATA przechowuje dane osobowe tylko w uzasadnionym celu biznesowym i w ramach swoich obowiązków wynikających z przepisów prawa. NTT DATA niszczy, usuwa lub anonimizuje dane osobowe, gdy upływa okres ich przechowywania i nie ma uzasadnionego powodu biznesowego, aby były przechowywane przez dłuższy czas.

NTT DATA przechowuje dane osobowe przetwarzane w imieniu swoich klientów zgodnie z wymaganiami klienta i niszczy, usuwa, anonimizuje lub zwraca dane osobowe, gdy jest to wymagane i gdy obowiązek ich dalszego przechowywania nie wynika z obowiązującego prawa.

NTT DATA podjęła wszelkie uzasadnione działania w celu zapewnienia, że dane osobowe są prawidłowe, kompletne i aktualne.

2.6. Prawa osób, których dane dotyczą

Przepisy o ochronie danych osobowych w niektórych krajach zapewniają osobom, których dane dotyczą, określone prawa w odniesieniu do ich danych osobowych. NTT DATA zobowiązuje się do przestrzegania tych praw i zapewnienia, że NTT DATA będzie udzielać odpowiedzi na żądania osób, których dane dotyczą, w sposób przejrzysty, rzetelny, etyczny i zgodny z prawem.

NTT DATA wdrożyła odpowiednie zasady i procedury majace na celu ochronę praw osóbosób, których dane dotyczą, zgodnie z obowiązującymi przepisami o ochronie danych:

- NTT DATA realizuje następujące prawa osób, których dane dotyczą
- prawo do informacji
- prawo dostępu
- prawo do sprostowania
- prawo do bycia zapomnianym
- prawo do przenoszenia danych
- prawo do ograniczenia wykorzystania
- prawo do sprzeciwu w tym prawo do rezygnacji z marketingu bezpośredniego i sprzedaży danych osobowych)
- prawo do zakwestionowania zautomatyzowanych decyzji
- prawo do wniesienia skargi

NTT DATA zapewnia, że podmioty danych mają dostęp do odpowiednich narzędzi, dzięki którym mogą korzystać ze swoich praw w odniesieniu do danych osobowych, które NTT DATA może przetwarzać na ich imieniu.

NTT DATA prowadzi rejestr wszystkich żądań otrzymanych od osób, których dane dotyczą, oraz działań podjętych w odpowiedzi na te żądania.

NTT DATA zapewni klientom uzasadnione wsparcie w zakresie udzielania odpowiedzi na żądania osób, których dane dotyczą, w razie potrzeby i zgodnie z obowiązującymi umowami.

NTT DATA ustanowiło zasady i procedury reagowania na żądania organów publicznych dotyczące dostępu do danych osobowych zgodnie z obowiązującymi przepisami i wymogami umownymi. NTT DATA przechowuje rejestr tych żądań i ich wyników.Transgraniczne transfery danych.

2.7. Transgraniczne transfery danych

NTT DATA ustanawia odpowiednie zabezpieczenia (takie jak decyzje o adekwatności, standardowe klauzule umowne i inne narzędzia określone w obowiązujących przepisach) podczas angażowania się w transgraniczne transfery danych.

W przypadku transferu danych osobowych poza EOG, NTT DATA przeprowadza oceny skutków transferu (TIA), aby upewnić się, że kraj docelowy oferuje równoważny poziom ochrony praw i wolności osób, których dane dotyczą, co kraj, w którym dane zostały pierwotnie zebrane. W przypadku braku takiej równoważności ocenimy i przyjmiemy środki uzupełniające w celu wsparcia praw osób, których dane dotyczą, zgodnie z naszymi zasadami i wymogami prawnymi. W przypadku braku możliwości wdrożenia takich środków uzupełniających NTT DATA zaprzestanie transferu danych osobowych.

NTT DATA opiera się na standardowych klauzulach umownych w celu wsparcia zgodnego z prawem transferu danych osobowych poza kraj, w którym zostały pierwotnie zebrane. W celu wsparcia takich transferów zawarto odpowiednie umowy z podmiotami zależnymi NTT DATA, spółkami grupy, podmiotami stowarzyszonymi, podmiotami przetwarzającymi, podmiotami podprzetwarzającymi i klientami.Kwestie regulacyjne.

2.8. Kwestie regulacyjne

NTT DATA zobowiązuje się do śledzenia zmian w przepisach dotyczących ochrony danych w krajachw których działa, i wdrożyła procesy i narzędzia przydatne w przestrzeganiu tych przepisów.

2.9. Szkolenia i świadomość

NTT DATA zobowiązuje się do ciągłego podnoszenia świadomości i zgodności poprzez ciągłe szkolenia i inne inicjatywy. Wymagamy od wszystkich pracowników, aby okresowo ukończyli obowiązkowe szkolenie w zakresie prywatności i ochrony danych. Materiały szkoleniowe i powiązane zasady, procesy, standardy i wytyczne są dostępne dla pracowników i regularnie przekazywane. W razie potrzeby zapewniane są szkolenia lokalne, regionalne lub funkcjonalne, aby pomóc pracownikom działać zgodnie z wymogami w określonych krajach, regionach lub funkcjach biznesowych.

2.10. Bezpieczeństwo dla prywatności

NTT DATA wdrożyła odpowiednie środki techniczne i organizacyjne w celu zapewnienia poufności, integralności i dostępności danych osobowych, biorąc pod uwagę stan wiedzy technicznej, koszty wdrożenia oraz charakter, zakres, kontekst i cel przetwarzania danych osobowych, a także ryzyko naruszenia praw i wolności osób, których dane dotyczą.

Metodologie bezpieczeństwa NTT DATA są dostosowane do normy ISO 27001 i NIST Cyber Security Framework („CSF").

2.11. Reagowanie na naruszenia i zgłoszenia naruszeń

NTT DATA posiada polityki, procesy i procedury dotyczące identyfikacji, wykrywania, reagowania, odzyskiwania i powiadamiania odpowiednich interesariuszy w przypadku naruszenia danych osobowych. Obejmują one również mechanizmy przeprowadzania analizy przyczyn źródłowych i podejmowania działań naprawczych.

NTT DATA zobowiązuje się do zapewnienia, że właściwe organy ochrony danych, zainteresowani klienci i osoby, których dane dotyczą, zostaną powiadomione w przypadku naruszenia danych osobowych zgodnie z obowiązującymi przepisami o ochronie danych i umowami.

NTT DATA prowadzi rejestr wszystkich naruszeń danych osobowych oraz działań podjętych w odpowiedzi na te zdarzenia.

SEKCJA 3: Środki bezpieczeństwa informajci w NTT DATA, służące do identyfikacji, wykrywania, reagowania i usuwania skutków incydentów związanych z bezpieczeństwem informacji, zostały przedstawione w sekcji 3.

2.12. Zarządzanie dotyczące osób trzecich

NTT DATA ponosi odpowiedzialność za działania swoich podmiotów przetwarzających i podwykonawców przetwarzania, którzy przetwarzają dane osobowe w imieniu NTT DATA. NTT DATA ocenia zdolność swoich podmiotów przetwarzających i podwykonawców przetwarzania do ochrony danych osobowych zgodnie ze standardami NTT DATA w momencie ich wyboru, a następnie okresowo.

Podmioty przetwarzające i podwykonawcy przetwarzania NTT DATA są zobowiązani do podpisania odpowiednich umów, które regulują przetwarzanie i ochronę danych osobowych. Umowy te określają wymogi mające na celu zapewnienie, że te same obowiązki zostaną przeniesione na dalsze podmioty przetwarzające, którzy mogą przetwarzać dane osobowe.



Środki bezpieczeństwa informacji

NTT DATA zobowiązuje się do zapewnienia wdrożenia i właściwego zarządzania bezpieczeństwem informacji w celu ochrony poufności, integralności i dostępności danych osobowych.

NTT DATA ustanowiło odpowiednie zasady, procesy, procedury, standardy i wytyczne, aby zapewnić bezpieczeństwo przetwarzanych danych. Metodologie bezpieczeństwa NTT DATA są zgodne z normą ISO 27001, a także innymi najlepszymi praktykami branżowymi.

3.1. Role i obowiązki w zakresie bezpieczeństwa informacji

Role i obowiązki w zakresie bezpieczeństwa informacji, włącznie z Chief Security Officer and Business Information Security Officers, zostały formalnie przypisane, a linie raportowania zapewniają niezależność tej funkcji.

Pracownicy NTT DATA są odpowiedzialni za to, aby w bieżącej działalności postępować zgodnie z polityką, procesami, normami i wytycznymi dotyczącymi bezpieczeństwa informacji.

3.2. Polityka bezpieczeństwa informacji

NTT DATA udokumentowała i opublikowała zestaw polityk bezpieczeństwa informacji,. Polityki te i dokumentacja uzupełniająca podlegają okresowym przeglądom.

3.3. Zarządzanie urządzeniami mobilnymi

NTT DATA ustanowiło zasady ograniczonego zaufania w celu wdrożenia i utrzymania kontroli bezpieczeństwa dostępu i interakcji z systemami NTT DATA i zasobami informacyjnymi. Ramy te obejmują:

- Zasady zarządzania urządzeniami użytkownika końcowego (EDM) i procedury pomocnicze.
- Kontrole i narzędzia do utrzymania bezpieczeństwa.
- Poufność, dostępność i integralność danych przedsiębiorstwa. Dane te mogą być przechowywane lub dostępne za pośrednictwem urządzeń końcowych użytkowników (w tym telefonów komórkowych, tabletów i urządzeń umożliwiających zdalny dostęp).

3.4. Zasoby ludzkie

NTT DATA przeprowadza weryfikację swoich pracowników w zakresie dozwolonym obowiązującymi przepisami prawa, aby upewnić się, że są oni odpowiedni do wykonywania pracy na danym stanowisku oraz do przetwarzania informacji o spółce i klientach (w tym danych osobowych). Zakres weryfikacji jest dostosowany do wymagań biznesowych i klasyfikacji informacji, do których pracownik będzie miał dostęp.

NTT DATA wymaga od swoich pracowników (w tym wykonawców i pracowników tymczasowych) zobowiązania się do zachowania poufności danych NTT DATA i klientów (w tym danych osobowych).

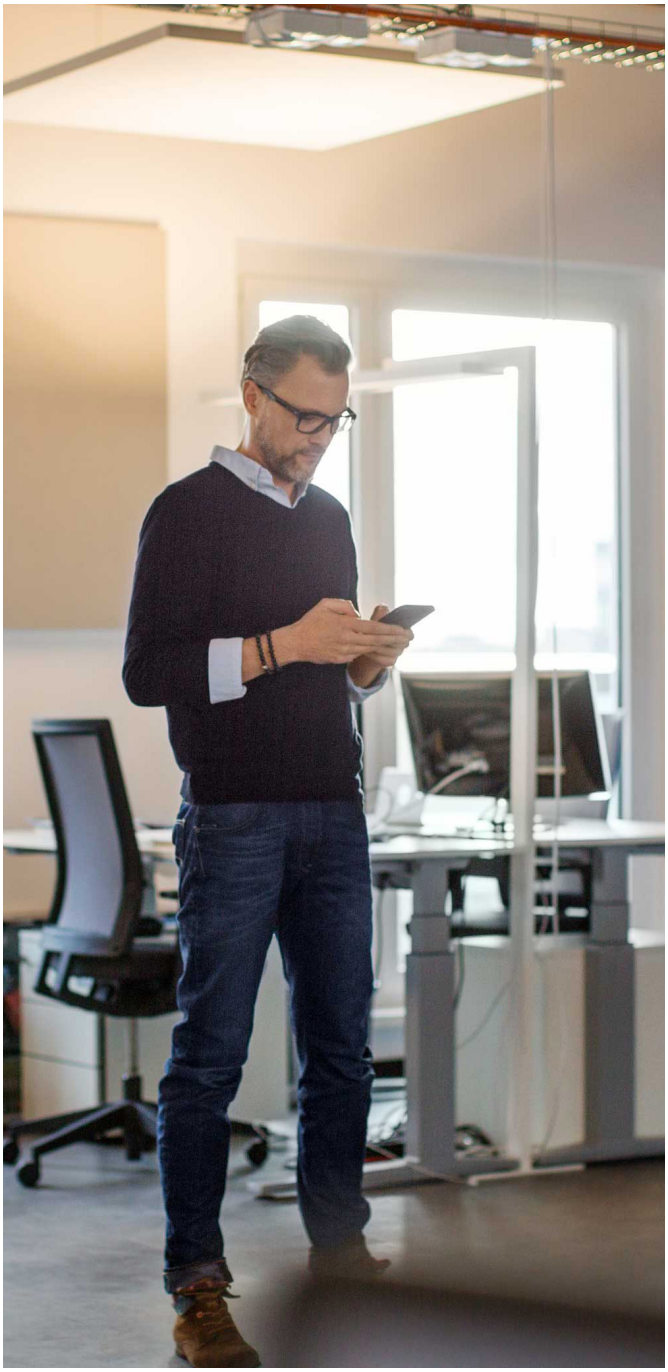
Pracownicy NTT DATA są zobowiązani do corocznego ukończenia szkolenia w zakresie świadomości bezpieczeństwa informacji oraz okresowego szkolenia uzupełniającego. Zasady bezpieczeństwa informacji wraz z uzupełniającymi ją procedurami, procesami i wytycznymi jest dostępna dla pracowników i regularnie przekazywana.

Pracownicy NTT DATA otrzymują istotne informacje o trendach, zagrożeniach i najlepszych praktykach.

3.5. Dopuszczelne użytkowanie

NTT DATA ustanowiło zasady, które wspierają właściwe i efektywne wykorzystanie zasobów informacyjnych NTT DATA, które obejmują zasoby komputerowe i telekomunikacyjne, produkty, usługi, rozwiązania i infrastrukturę informatyczną.

NTT DATA ustanowiło zasady klasyfikacji informacji, aby wspierać odpowiednie kontrole dotyczące przetwarzania informacji w oparciu o ich klasyfikację. Informacje i zasoby są chronione zgodnie z etykietą klasyfikacji.



> “Metodologie bezpieczeństwa NTT DATA są zgodne z normą ISO 27001, a także innymi najlepszymi praktykami branżowymi.”

3.6. Mechanizmy kontroli dostępu

NTT DATA posiada politykę kontroli dostępu, procedury uzupełniające oraz logiczne i fizyczne środki dostępu, aby zapewnić, że tylko upoważnione osoby mają dostęp do informacji w oparciu o zasadę najmniejszych przywilejów.

W stosownych przypadkach, NTT DATA stosuje szyfrowanie danych nieaktywnych i danych w trakcie przesyłu zgodne ze standardami branżowymi, aby zapewnić ich ochronę przed nieuprawnionym dostępem lub ujawnieniem.

Przeglądy dostępu są okresowo przeprowadzane w celu zapewnienia, że dostęp przysługuje tylko osobom upoważnionym.

NTT DATA podjęła uzasadnione działania mające na celu ścisłe ograniczenie liczby użytkowników mających uprzywilejowy dostęp systemów i i zasobów informacyjnych NTT DATA.

NTT DATA nie zezwala na udostępnianie kont ani danych uwierzytelniających, chyba że zostało to zatwierdzone w ramach odpowiedniej procedury zarządzania wyjątkami.

3.7. Zarzadzanie aktywami i ich klasyfikacja

NTT DATA ustanowiło zasady regulujące klasyfikację i obsługę aktywów fizycznych i informacyjnych, w tym bezpieczne usuwanie aktywów, aby zapewnić ochronę informacji na odpowiednim poziomie.

Aktywa są oparte na krytyczności biznesowej w celu określenia wymogów poufności. Wytyczne branżowe dotyczące obsługi danych osobowych zapewniają ramy dla zabezpieczeń technicznych, organizacyjnych i fizycznych. Zabezpieczenia te mogą obejmować takie kontrole, jak zarządzanie dostępem, szyfrowanie, rejestrowanie i monitorowanie oraz niszczenie danych.

3.8. Bezpieczeństwo fizyczne i środowiskowe

NTT DATA wdrożyła rozsądne i odpowiednie środki zgodne z polityką bezpieczeństwa fizycznego, aby zapobiec nieuprawnionemu fizycznemu dostępowi, uszkodzeniu lub zakłóceniu naszych informacji, aplikacji, systemów, baz danych i infrastruktury. Obejmują one:

- Kontrole dostępu fizycznego
- Monitorowanie i weryfikowanie dostępu fizycznego
- Ochrona przed zagrożeniami środowiskowymi
- Zabezpieczenie majątku rzeczowego
- Postępowanie z majątkiem rzeczowym
- Utrzymanie i zbycie majątku rzeczowego
- Praktyki związane z czystym biurkiem i ekranem
- Dostęp i nadzór nad odwiedzającymi

3.9. Bezpieczeństwo operacyjne

NTT DATA powołało odpowiednie zespoły specjalistów, które odpowiadają za zarządzanie i ochronę systemów informatycznych oraz infrastruktury NTT DATA.

NTT DATA posiada politykę i procedury pomocnicze które regulują zmiany w naszych procesach biznesowych, aplikacjach, systemach, bazach danych i infrastrukturze. NTT DATA stosuje kilka struktur zarządzania w celu przeglądu i zatwierdzania zmian w zależności od wielkości i zakresu zmiany oraz celów strategicznych. Wszystkie wnioski i ich wyniki są rejestrowane w dziennikach i dokumentowane.

NTT DATA posiada politykę zarządzania podatnościami i ustanowiła program zarządzania zagrożeniami i podatnościami wspierany przez narzędzia zgodne ze standardami branżowymi w celu identyfikacji, zarządzania i ograniczania ryzyka dla informacji firmowych, w tym danych osobowych pracowników i klientów. Obejmuje ona rozwiązanie Endpoint Detection and Response („EDR") dla narzędzi antywirusowych i antymalware, regularne skanowanie środowisk, protokoły łatania oraz zarządzanie działaniami naprawczymi i usprawniającymi.

Wymagania dotyczące przepustowości są stale monitorowane i regularnie weryfikowane. Systemy i sieci będą zarządzane i skalowane zgodnie z tymi przeglądami.

Dostępność systemu obejmuje architekturę, projekt wysokiej dostępności i/lub kopie zapasowe oraz odzyskiwanie po awarii,w oparciu o ryzyko i wymagania dostępności dla każdego systemu. Metoda utrzymywania dostępności lub odtwarzania systemu, w tym zakres i częstotliwość wykonywania kopii zapasowych, określa się na podstawie wymagań biznesowych NTT DATA, w tym wymagań klienta, oraz istotności informacji. Odzyskiwanei po awarii jest testowane okresowo. Jest prowadzone w celu zapewnienia pomyślnego zakończenia tworzenia kopii zapasowych, a także zarządzania wszelkimi problemami związanymi z kopiami zapasowymi, wyjątkami lub awariami.

NTT DATA podejmuje uzasadnione działania w celu prowadzenia dzienników audytu w aplikacjach i systemach. Dzienniki są okresowo przeglądane i udostępniane na potrzeby postępowania wyjaśniającego. Dostęp do dzienników jest ściśle ograniczony tylko do uprawnionego personelu.

3.10. Pozyskiwanie, rozwój i utrzymanie systemu

NTT DATA ustanowiło zasady ograniczonego zaufania, aby regulować projektowanie, nabywanie, rozwój i utrzymanie systemów informatycznych i architektury.

Polityka architektury bezpieczeństwa i projektowania oraz wspierające ją standardy i procedury zapewniające stosowanie zasad bezpieczeństwa przez projektowanie w ramach cyklu życia oprogramowania.

3.11. Zarządzanie informacjami osób trzecich

NTT DATA opracowała zasady i praktyki dotyczace zarządzania bezpieczeństwa informacji osób trzecich aby zapewnić ochronę aktywów informacyjnych, gdy NTT DATA angażuje zewnętrznych dostawców usług i/lub podmioty przetwarzające. Obejmuje ona wymagania dotyczące należytej staranności w zakresie bezpieczeństwa informacji oraz oceny ryzyka w zakresie bezpieczeństwa informacji, które należy przeprowadzić, aby zapewnić, że:

- wymagania dotyczące bezpieczeństwa informacji są jasno sformułowane i udokumentowane w umowach zgodnie ze standardami bezpieczeństwa informacji NTT DATA.
- usługodawcy i podmioty przetwarzające zaangażowane przez NTT DATA realizują ten sam poziom ochrony i kontroli co NTT DATA.
- usługodawcy i podmioty przetwarzające są zobowiązani do terminowego zgłaszania NTT DATA wszelkich podejrzewanych lub faktycznych incydentów związanych z bezpieczeństwem informacji.

3.12. Zarządzanei incydentami związanymi z bezpieczeństwem informacji

NTT DATA posiada polityki, procesy i procedury dotyczące identyfikacji, wykrywania, reagowania, odzyskiwania w przypadku incydentu związanego z bezpieczeństwem informacji, w tym naruszenia danych osobowych. jak również powiadamiania odpwoeidnich interesariuszy w przypadku takiegi naruszenia. Obejmują one również mechanizmy przeprowadzania analizy przyczyn źródłowych i podejmowania działań naprawczych aby zapobiec ponownemu wystąpieniu problemu.

NTT DATA ustanowiła ogólne zasady bezpieczeństwa w celu proaktywnego monitorowania i zarządzania wszystkimi zasobami sieciowymi i komputerowymi. Działania te są wspierane przez narzędzia techniczne służące do reagowania na incydenty związane z bezpieczeństwem informacji oraz do odzyskiwania danych.

3.13. Ciągłość działania

NTT DATA ustanowiła plany ciągłości działania i odzyskiwania danych po awarii. NTT DATA przyjęła podejście warstwowe, aby zapewnić dostępność naszych systemów i danych.

3.14. Zgodność

NTT DATA określiła role i obowiązki w zakresie ustalania przepisów prawa, które mają wpływ na działalność gospodarczą NTT DATA. Odpowiedzialność za przestrzeganie przepisów prawa ustala się na poziomie grupy i regionów, aby zapewnić spełnienie przez NTT DATA wymogów globalnych i lokalnych.


NTT DATA