Środki techniczne i organizacyjne

W NTT pragniemy, **dzięki technologii i innowacjom,** budować **bezpieczną przyszłość opartą na powszechnej łączności.** Opracowaliśmy środki techniczne i organizacyjne („ŚTO"), dzięki którym zapewniamy ochronę danych osobowych w sposób przejrzysty, uczciwy, etyczny i zgodny z przepisami prawa.

Nasze ŚTO są oparte na najlepszych praktykach branżowych i wymogach prawnych obowiązujących w jurysdykcjach, w których prowadzimy działalność, oraz uwzględniają charakter danych, które przetwarzamy, i koszt wdrożenia ich ochrony.

Spis treści

(A) Poufność danych i środki ochrony

1 Nadzór i model operacyjny

1.1 Firma NTT jest zobowiązana do wykazywania się odpowiedzialnością podczas przetwarzania danych osobowych oraz do wdrożenia struktury organizacyjnej, a także ról i obowiązków dotyczących zarządzania przetwarzaniem danych i zapewniania nadzoru nad tym procesem.

1.2 Wdrożono liczne struktury nadzorcze, w ramach których stosowne komórki kierownicze NTT analizują kwestie poufności i ochrony danych. Ostateczną odpowiedzialność za poufność i ochronę danych ponosi Zarząd NTT Ltd, przy wsparciu wyznaczonych osób w różnych działach, m.in. Inspektorów Ochrony Danych lub osób piastujących podobne stanowiska, w sytuacjach, gdy wymagają tego przepisy o ochronie danych.

2 Polityki, procesy i wytyczne

2.1 NTT wdrożyła i udostępniła swoje polityki, procesy, normy i wytyczne, które szczegółowo opisują sposób, w jaki pracownicy NTT powinni przetwarzać dane osobowe.
Powyższe obejmuje:

2.1.1 Politykę w zakresie poufności i ochrony danych;

2.1.2 Politykę w zakresie praw osób, których dane dotyczą; oraz Politykę zgłaszania naruszeń ochrony danych osobowych.

2.2 NTT zdefiniowała i udostępniła komunikaty o ochronie danych, które informują pracowników, klientów i innych interesariuszy o tym, w jakim sposób przetwarza się ich dane osobowe.

2.3 NTT opracowała proces oceny skutków dla ochrony danych („DPIA") i przeprowadza takie oceny, gdy jest to konieczne i wymagane na podstawie przepisów o ochronie danych.

3 Uwzględnianie ochrony danych w fazie projektowania

3.1 NTT zobowiązała się do wdrożenia zasadnych środków, które wspierają jej klientów w przestrzeganiu przepisów o ochronie danych. W miarę możliwości w trakcie tworzenia i realizacji produktów, usług i rozwiązań oferowanych przez NTT stosuje się zasadę uwzględniania ochrony danych w fazie projektowania oraz zasadę domyślnej ochrony danych.

4 Struktura danych

4.1 NTT wdrożyła procesy, które umożliwiają identyfikację, rejestrację, ocenę i utrzymanie odpowiedniego zrozumienia danych osobowych, które NTT przetwarza.

4.2 NTT prowadzi ewidencję przetwarzanych danych osobowych zgodną z przepisami o ochronie danych.

5 Zarządzanie cyklem życia informacji

5.1 NTT wdrożyła polityki i procesy, które zapewniają prawidłowe przetwarzanie danych osobowych w całym ich cyklu życia (od gromadzenia, przez wykorzystywanie, przechowywanie, ujawnianie aż do zniszczenia).

5.2 Obowiązujące w niektórych krajach przepisy prawa o ochronie danych gwarantują osobom, których dane dotyczą, szczególne prawa odnośnie do ich danych osobowych. NTT jest zobowiązana do przestrzegania tych praw i zapewnia, że reaguje na wnioski osób, których dane dotyczą, w sposób przejrzysty, uczciwy, etyczny i zgodny z przepisami prawa.

5.3 NTT wdrożyła Politykę w zakresie praw osób, których dane dotyczą, oraz Politykę w zakresie wniosków osób, których dane dotyczą, aby przestrzegać praw osób, których dane dotyczą, zgodnie z obowiązującymi przepisami o ochronie danych.

5.4 NTT prowadzi ewidencję wszystkich wniosków osób, których dane dotyczą, i działań podejmowanych w odpowiedzi na te wnioski. NTT zapewni klientom, na ich życzenie, wszelkie niezbędne wsparcie podczas odpowiadania na wnioski osób, których dane dotyczą, zgodnie z postanowieniami zawartych umów.

5.5 NTT utrzymuje Politykę w zakresie przechowywania danych oraz Załącznik, które są dostosowane do obowiązujących przepisów. NTT przechowuje dane osobowe wyłącznie w przypadku, gdy wynika to z jej prawnie uzasadnionych celów biznesowych oraz gdy wymagają tego przepisy prawa.
NTT niszczy, usuwa lub anonimizuje dane osobowe po upływie okresu ich przechowywania, gdy nie ma już uzasadnionego celu biznesowego ich dalszego przechowywania.

5.6 NTT przechowuje dane osobowe przetwarzane w imieniu jej klientów zgodnie z wymogami klienta i niszczy je,

usuwa, anonimizuje lub zwraca na życzenie klienta, gdy przestają obowiązywać wymogi prawne nakazujące ich przechowywanie.

5.7 NTT dokłada wszelkich zasadnych starań, aby zapewnić poprawność, kompletność i aktualność danych osobowych.

5.8 NTT polega na standardowych klauzulach umownych, które umożliwiają zgodny z prawem transfer danych osobowych poza kraj, w którym zostały pierwotnie zgromadzone, oraz zawarła stosowne umowy ze swoimi podmiotami zależnymi, podmiotami powiązanymi, podmiotami przetwarzającymi, podwykonawcami podmiotu przetwarzającego i klientami dotyczące transgranicznego transferu danych.

6 Szkolenia i wiedza z zakresu poufności i ochrony danych

6.1 NTT wymaga od swoich pracowników corocznego odbywania szkolenia z zakresu poufności i ochrony danych. Wszelkie polityki, procesy, normy i wytyczne dotyczące poufności i ochrony danych są dostępne pracownikom, którzy są o nich regularnie informowani. W stosownych przypadkach pracownikom zapewnia się także szkolenia lokalne, regionalne lub funkcyjne, dotyczące przestrzegania wymogów w zakresie ochrony danych, które obowiązują w poszczególnych krajach lub regionach albo dotyczą poszczególnych funkcji biznesowych.

7 Bezpieczeństwo i ochrona prywatności

7.1 Zespoły odpowiedzialne za poufność i ochronę danych oraz za bezpieczeństwo informacji w NTT współpracują w celu wdrożenia stosownego nadzoru i kontroli nad ochroną danych, aby zapewniać poufność, spójność i dostępność danych osobowych.

Nasze metodyki zapewniania bezpieczeństwa są zgodne z normą ISO27001 i ramami cyberbezpieczeństwa NIST („CSF").

8 Reakcja na naruszenia i powiadomienia

8.1 NTT opracowała polityki, procesy i procedury rozpoznawania i wykrywania naruszeń ochrony danych, reagowania na takie naruszenia, usuwania ich skutków oraz powiadamiania o nich odpowiednich interesariuszy. Obejmuje to mechanizmy umożliwiające analizę przyczyn źródłowych oraz podejmowanie działań naprawczych.

8.2 NTT jest zobowiązana do powiadamiania właściwych organów odpowiedzialnych za ochronę danych, poszkodowanych klientów i poszkodowane osoby, których dane dotyczą, o przypadkach naruszenia ochrony danych, zgodnie z obowiązującymi przepisami o ochronie danych i wszelkimi zobowiązaniami umownymi.

8.3 NTT prowadzi ewidencję wszystkich przypadków naruszenia ochrony danych i działań podejmowanych w odpowiedzi na nie.

8.4 Stosowane przez NTT środki zarządzania incydentami, które umożliwiają rozpoznawanie i wykrywanie naruszeń bezpieczeństwa informacji, reagowanie na takie naruszenia i usuwanie ich skutków, zostały opisane w rozdziale B (Bezpieczeństwo informacji) niniejszych ŚTO.

9 Zarządzanie podmiotami trzecimi

9.1 NTT odpowiada za działania swoich podmiotów przetwarzających (tj. podwykonawców podmiotu przetwarzającego), które przetwarzają dane osobowe w imieniu NTT, i ocenia ich zdolność do ochrony danych osobowych zarówno w momencie wyboru takich podmiotów, jak i później, w formie regularnych ocen przeprowadzanych z politykami NTT.

9.2 Podmioty przetwarzające NTT są zobowiązane podpisać stosowne umowy, które regulują przetwarzanie i ochronę danych osobowych oraz wymagają nakładania na wszelkich podwykonawców podmiotu przetwarzającego angażowanych przez NTT takich samych zobowiązań, jak te, które wynikają z umowy powierzenia przetwarzania. NTT dokłada wszelkich zasadnych starań, aby zawierać umowy powierzenia przetwarzania ze wszystkimi podmiotami przetwarzającymi.

10 Monitorowanie i ocena

10.1 NTT regularnie informuje o skuteczności projektowej i operacyjnej swoich działań dotyczących poufności i ochrony danych Komitet ds. Audytu i Ryzyka NTT Ltd oraz kierownictwo wyższego szczebla.

Obejmuje to sprawozdawczość wizualną, samooceny kierownictwa, certyfikacje, analizy audytów wewnętrznych, niezależne audyty i oceny.

(B) Środki z zakresu bezpieczeństwa informacji

NTT jest zobowiązana do wdrożenia mechanizmów kontroli bezpieczeństwa informacji oraz odpowiedniego zarządzania nimi w celu zapewnienia ochrony poufności, spójności i dostępności danych osobowych przetwarzanych w imieniu i na zlecenie klientów.

NTT opracowała obowiązujący w całej grupie system zarządzania bezpieczeństwem informacji („ISMS"), który jest zgodny z wiodącymi praktykami i normami z zakresu bezpieczeństwa informacji z całego świata, w tym z normami serii ISO 27000 i ramami cyberbezpieczeństwa NIST („CSF").

11 Bezpieczeństwo informacji

11.1 Role i obowiązki z zakresu bezpieczeństwa informacji zostały formalnie przypisane wraz z systemem podległości służbowych, który zapewnia niezależność poszczególnych komórek, m.in. dyrektora ds. bezpieczeństwa („CSO"), dyrektora ds. bezpieczeństwa informacji („CISO") i specjalistów ds. bezpieczeństwa informacji („ISO").

11.2 Pracownicy NTT odpowiadają za działanie zgodne z politykami, procesami, normami i wytycznymi z zakresu bezpieczeństwa informacji w swojej codziennej pracy.

11.3 NTT udokumentowała i udostępniła zestaw polityk z zakresu bezpieczeństwa informacji, które ułatwiają realizację wymogów systemu ISMS.
Polityki i dokumentacja dodatkowa podlegają okresowym przeglądom.

11.4 NTT wdrożyła środki, które zapewniają ochronę urządzeń mobilnych (w tym laptopów, telefonów komórkowych, tabletów, urządzeń umożliwiających zdalny dostęp oraz programów pozwalających na korzystanie z urządzeń prywatnych w pracy) i ich zawartości.
NTT podjęła uzasadnione działania, aby zapewnić instalację oprogramowania do zarządzania urządzeniami mobilnymi („MDM") na wszystkich urządzeniach mobilnych, które mają dostęp do sieci firmowej NTT.

11.5 W miarę możliwości, osoby pracujące zdalnie mają dostęp do infrastruktury NTT wyłącznie za pośrednictwem wirtualnej sieci prywatnej („VPN").

12 Kadry

12.1 NTT weryfikuje przeszłość i historię zatrudnienia swoich pracowników, w zakresie dopuszczalnym przez obowiązujące prawo, aby mieć pewność, że można im powierzyć przetwarzanie danych firmy i jej klientów (w tym również danych osobowych). Zakres weryfikacji jest proporcjonalny do wymogów biznesowych i klasyfikacji informacji, do których pracownik będzie miał dostęp.

12.2 NTT wymaga od swoich pracowników (również od podwykonawców i pracowników tymczasowych) zgody na zachowanie poufności danych wewnętrznych NTT i danych klientów (w tym również danych osobowych).

12.3 Pracownicy NTT są zobowiązani co roku odbywać szkolenie z zakresu świadomości bezpieczeństwa informacji. Polityki dotyczące bezpieczeństwa informacji oraz powiązane procedury, procesy i wytyczne są dostępne dla pracowników, którzy otrzymują stosowne informacje dotyczące trendów, zagrożeń i najlepszych praktyk za pośrednictwem platform komunikacyjnych NTT.

13 Mechanizmy kontroli dostępu

13.1 NTT opracowała Politykę dopuszczalnego użytkowania, która wspiera poprawne i skuteczne użytkowanie i ochronę aktywów korporacyjnych NTT, m.in. zasobów, produktów, usług, rozwiązań i infrastruktury komputerowej i telekomunikacyjnej.

13.2 NTT stosuje Politykę klasyfikacji informacji, która opisuje stosowne techniczne i organizacyjne środki kontroli dostępu do informacji w oparciu o ich klasyfikację. Informacje i aktywa są chronione zgodnie z przypisaną klasyfikacją.

14 Zarządzanie aktywami

14.1 NTT stosuje Politykę kontroli dostępu, procedury dodatkowe oraz środki dostępu logicznego i fizycznego, dzięki którym do informacji mają dostęp wyłącznie upoważnione osoby zgodnie z zasadą minimalnych uprawnień.

14.2 Regularnie przeprowadza się przeglądy dostępów do zasobów informatycznych, aplikacji, systemów i baz danych, aby dostęp do nich miały wyłącznie upoważnione osoby.

14.3 Podmioty przetwarzające NTT (tj. podwykonawcy podmiotu przetwarzającego) muszą logować się do systemów NTT za pomocą kont imiennych. Zabronione jest korzystanie z kont generycznych i/lub dzielenie się danymi uwierzytelniającymi, o ile kierownictwo lub klienci nie wydadzą wyraźnej zgody na odstępstwo od tej zasady.

14.4 NTT dokłada stosownych starań, aby ściśle ograniczać liczbę użytkowników

uprzywilejowanych („adminów") w swoich aplikacjach, systemach i bazach danych.

15 Bezpieczeństwo fizyczne i bezpieczeństwo otoczenia

15.1 Zgodnie z Polityką bezpieczeństwa fizycznego NTT wdrożyła stosowne i odpowiednie środki, aby zapobiegać nieuprawnionemu dostępowi fizycznemu do informacji, aplikacji, systemów, baz danych i infrastruktury NTT, a także ich uszkodzeniu lub innej ingerencji; środki te są wdrożone w następujących obszarach:

15.1.1 mechanizmy kontroli dostępu fizycznego;

15.1.2 monitorowanie i kontrolowanie dostępu fizycznego;

15.1.3 ochrona przed zagrożeniami środowiskowymi;

15.1.4 zabezpieczanie aktywów fizycznych;

15.1.5 bezpieczeństwo okablowania;

15.1.6 obsługa aktywów fizycznych i informatycznych;

15.1.7 utrzymywanie i utylizacja aktywów fizycznych;

15.1.8 zasada czystego biurka i pulpitu;

15.1.9 dostęp gości i jego kontrola;

15.1.10 procedury BHP.

16 Bezpieczeństwo operacyjne

16.1 Dział informatyki i technologii („I&T") w NTT odpowiada za zarządzanie aplikacjami, systemami, bazami danych i infrastrukturą NTT.
I&T dokumentuje, prowadzi i wdraża wszystkie polityki i procedury operacyjne z zakresu informatyki, które są zgodne z normami COBIT i ITIL.

16.2 NTT stosuje politykę i procedury dodatkowe z zakresu zarządzania zmianami w naszych procesach biznesowych, aplikacjach, systemach, bazach danych i infrastrukturze.
NTT ustanowiła struktury nadzorcze, w ramach których są analizowane i zatwierdzane wszelkie zmiany z uwzględnieniem rozmiaru i zakresu danej zmiany oraz celów strategicznych.
Wszelkie zgłaszane wnioski i wyniki ich analizy są rejestrowane i dokumentowane.

16.3 NTT opracowała program zarządzania zagrożeniami i podatnością na ataki, który dzięki wykorzystaniu standardowych narzędzi branżowych umożliwia rozpoznawanie i ograniczanie czynników ryzyka dotyczących informacji, w tym danych osobowych pracowników i klientów, oraz zarządzanie takimi czynnikami ryzyka.

Obejmuje to system nowej generacji do wykrywania podejrzanych aktywności na urządzeniach końcowych i reagowania na nie („EDR") na potrzeby narzędzi antywirusowych i chroniących przed złośliwym oprogramowaniem, regularne skanowanie środowisk, protokoły poprawek oraz zarządzanie działaniami naprawczymi i ulepszającymi.

16.4 Wymogi dotyczące mocy obliczeniowej są nieustannie monitorowane i podlegają regularnym przeglądom, a wyniki tych przeglądów stanowią podstawę zarządzania systemami i sieciami oraz ich skalowania.

16.5 Dostępność systemu obejmuje architekturę, projektowanie z myślą o wysokiej dostępności i/lub kopie zapasowe, zgodnie z wymogami dotyczącymi ryzyka i dostępności określonymi dla każdego systemu. Sposób utrzymywania dostępności systemu lub jego odzyskiwania, w tym zakres i częstotliwość tworzenia kopii zapasowych, określa się na podstawie wymogów biznesowych NTT, w tym wymagań klientów, oraz wagi informacji.

Monitorowanie procesu tworzenia kopii zapasowych ma zapewniać pomyślne tworzenie takich kopii oraz zarządzanie wszelkimi powiązanymi problemami, wyjątkami lub błędami.

16.6 NTT dokłada stosownych starań, aby prowadzić dzienniki kontroli aplikacji i systemów. Dzienniki te podlegają okresowym przeglądom i są dostępne na potrzeby dochodzeń.
Dostęp do tych dzienników mają wyłącznie upoważnione osoby.

17 Nabywanie, rozwój i utrzymywanie systemów

17.1 NTT stosuje Politykę architektury i projektowania na rzecz bezpieczeństwa oraz dodatkowe normy i procedury, które zapewniają uwzględnianie bezpieczeństwa w fazie projektowania w cyklu życia rozwoju oprogramowania.

17.2 NTT nie zezwala na wykorzystywanie żadnych danych produkcyjnych, danych klientów, danych osobowych ani informacji poufnych na potrzeby testów.
W szczególnych przypadkach dane produkcyjne lub dane klienta mogą być wykorzystane za zgodą danego klienta lub przedsiębiorcy.

18 Zarządzanie podmiotami trzecimi

18.1 NTT stosuje Politykę bezpieczeństwa podmiotów trzecich oraz procedury dodatkowe, aby zapewniać ochronę zasobów informacyjnych podczas współpracy z zewnętrznymi usługodawcami i/lub podmiotami przetwarzającymi. Obejmuje to wymogi dotyczące analizy due diligence i ocen ryzyka bezpieczeństwa informacji, które przeprowadza się w celu:

18.1.1 wyraźnego sformułowania i udokumentowania wymogów z zakresu bezpieczeństwa informacji w umowach z podmiotami przetwarzającymi NTT;

18.1.2 wdrożenia przez podmioty przetwarzające NTT takiego samego poziomu ochrony i kontroli, jaki stosuje NTT;

18.1.3 zobowiązania podmiotów przetwarzających do terminowego zgłaszania NTT wszelkich podejrzanych lub faktycznych incydentów bezpieczeństwa.

18.2 NTT dokłada wszelkich zasadnych starań, aby zawierać odpowiednie umowy z podmiotami przetwarzającymi, które mają dostęp do informacji, aplikacji, systemów, baz danych i infrastruktury NTT.
Umowy te obejmują normy bezpieczeństwa informacji obowiązujące w NTT, które zapewniają poufność, spójność i dostępność informacji NTT.

19 Zarządzanie incydentami związanymi z bezpieczeństwem informacji

19.1 NTT opracowała polityki, procesy i procedury rozpoznawania i wykrywania incydentów związanych z bezpieczeństwem informacji, w tym naruszeń ochrony danych, reagowania na takie naruszenia, usuwania ich skutków i powiadamiania o nich odpowiednich interesariuszy.
Obejmuje to mechanizmy umożliwiające analizę przyczyn źródłowych oraz podejmowanie działań naprawczych.

19.2 NTT opracowała obowiązujący w całej grupie system bezpieczeństwa, aby proaktywnie monitorować wszystkie sieci i zasoby komputerowe oraz zarządzać nimi. System ten jest wspierany przez narzędzia techniczne umożliwiające reagowanie na incydenty związane z bezpieczeństwem informacji i usuwanie ich skutków.

20 Ciągłość działania

20.1 NTT opracowała plany zapewniania ciągłości działania i usuwania skutków awarii. NTT przyjęła podejście warstwowe, które zapewnia dostępność naszych systemów i danych.

21 Przestrzeganie przepisów

21.1 NTT określiła role i obowiązki w zakresie rozpoznawania przepisów i regulacji, które mają wpływ na działalność firmy. Odpowiedzialność za przestrzeganie przepisów i regulacji jest odpowiednio przypisana na poziomie grupowym i regionalnym, aby zapewnić, że NTT spełnia zarówno wymogi globalne, jak i lokalne.

21.2 NTT dba o spójne podejście do bezpieczeństwa informacji w całej swojej działalności. Produkty, usługi i rozwiązania NTT są zgodne z normą ISO 27001 i – w zakresie, w jakim zostały certyfikowane zgodnie z umową z klientem – podlegają dorocznym audytom zgodnym z powyższą normą.

W razie jakichkolwiek pytań, proszę kontaktować się z biurem ds. ochrony danych pod adresem:
privacyoffice@global.ntt

Together we do great things