Korporacyjna Ochrona Danych

Polityka

Wersja 2

Dokument wiodący: Policy “**Corporate Data Protection**”, Wersja 2 w języku angielskim	
	Tłumaczenie na język polski
Imię i nazwisko	Dominika Kufel
Data	02.09.2022
Podpis	DocuSigned by: Dominika Kufel 68035437753542D...

Information Type:	group restricted
Company:	NTT DATA Business Solutions AG
Information Owner:	Corporate Data Protection Officer

Spis treści

1. Historia zmian

	Wersja	Data	Autor	Zmiany
	1	25.06.2018	Klaus Brandhorst	Utworzony dokument
	2	11.01.2022	Christian Hering	Przegląd dokumentu w oparciu o EU-GDPR i dodatkowe globalne przepisy dotyczące ochrony danych

Tabela 1 - Historia zmian

2. Ogólne[1]

2.1 Cel

Zarząd NTT DATA Business Solutions („NDBS") jest odpowiedzialny za przestrzeganie obowiązujących przepisów i regulacji w zakresie ochrony danych osobowych w Grupie NDBS. Przyjmuje on tę odpowiedzialność organizacyjną i wdraża poniższe wymagania.

Ochrona Danych Osobowych jest istotną częścią systemu zgodności Grupy NDBS. Dlatego też niniejsza polityka reguluje systematyczne i zorientowane na ryzyko wdrażanie i rozwijanie odpowiednich przepisów dotyczących ochrony danych, umożliwiając Grupie NDBS działanie na tym samym, wysokim poziomie ochrony danych na całym świecie.

Niniejsza polityka reguluje przetwarzanie Danych Osobowych przez Grupę NDBS zgodnie z ogólnymi europejskimi przepisami o ochronie danych („GDPR") lub innymi obowiązującymi przepisami/regulacjami w zakresie ochrony danych, przy czym przepisy GDPR stosuje się jako standard minimalny, a obowiązujące lokalne prawa i regulacje mogą wykraczać poza te wymogi. W ten sposób niniejsze zasady chronią prawa osobiste pracowników, klientów i innych osób kontaktujących się z firmą.

Polityka ta ma na celu dalszy rozwój już istniejących środków i procesów ochrony danych, jak również stworzenie nowych, zorientowanych na ryzyko środków ochrony danych dla całej Grupy NDBS w postaci kompleksowego, skutecznego i efektywnego systemu zarządzania ochroną danych (zwanego dalej „Systemem Zarządzania Ochroną Danych, ang. Data Protection Management System (DPMS)"). DPMS łączy w sobie dotychczasowe działania Grupy NDBS w zakresie ochrony danych (np. Rejestr Czynności Przetwarzania, ang. Records of Processig Activities (RoPA)) w celu zwiększenia pewności prawnej i skuteczności w ramach systematycznej i globalnej koncepcji, która stale się rozwija. Dlatego też niniejsza polityka określa również organizację i zakres odpowiedzialności poszczególnych funkcji w ramach DPMS.

DPMS służy wspieraniu pracowników Grupy NDBS w zapobieganiu naruszeniom przepisów dotyczących ochrony danych. Środki ochrony danych nie tylko przyczyniają się do zapewnienia zgodności Grupy NDBS z GDPR i innymi obowiązującymi przepisami i regulacjami w zakresie ochrony danych, ale także chronią każdego pracownika.

[1] W tekście zastosowano pisownię męską. Ma to na celu jedynie ułatwienie czytania. W trosce o równe traktowanie, pisownię tę stosuje się do obu płci. Forma żeńska powinna być czytana tak samo.

2.2 Obowiązki

2.2.1 Zarząd i Kierownictwo Lokalne

Ogólna odpowiedzialność za przestrzeganie zasad ochrony danych spoczywa na Zarządzie NDBS. Zarząd jest odpowiedzialny za zapewnienie zgodności z wymogami ochrony danych osobowych zgodnie z niniejszą polityką. Ponadto każdy odpowiedzialny dyrektor zarządzający / kierownictwo lokalne w Grupie NDBS ponosi odpowiedzialność za swoją jednostkę zależną w przypadku nieprzestrzegania zasad.
Zarząd regularnie informuje o kulturze ochrony danych osobowych w całej Grupie NDBS.

Ponadto Zarząd regularnie informuje o aktualnym stanie ochrony danych osobowych komitet akcjonariuszy oraz radę nadzorczą, która monitoruje działania Zarządu NDBS.

2.2.2 Korporacyjny Inspektor Ochrony Danych

Zarząd NDBS powołał i oficjalnie poinformował o powołaniu Korporacyjnego Inspektora Ochrony Danych (ang. Corporate Data Protection Officer) dla Grupy NDBS w celu wdrożenia systemu DPMS i kierowania jego Strukturą. Korporacyjny Inspektor Ochrony Danych posiada wymaganą wiedzę i wiarygodność. Nie występuje konflikt interesów w związku z pełnieniem funkcji Korporacyjnego Inspektora Ochrony Danych.

Korporacyjny Inspektor Ochrony Danych jest prawnie wymaganym i powołanym inspektorem ochrony danych Grupy NDBS.

Korporacyjny Inspektor Ochrony Danych informuje i doradza Zarządowi NDBS oraz pracownikom w zakresie ich obowiązków i praw związanych z ochroną danych. Korporacyjny Inspektor Ochrony Danych jest odpowiedzialny za monitorowanie zgodności w zakresie:

- przepisów o ochronie danych osobowych
- strategii podmiotów odpowiedzialnych za ochronę danych osobowych
- przydzielania obowiązków w zakresie ochrony danych
- podnoszenia świadomości i szkoleń pracowników
- prawidłowego wykonywanie analiz stanu ochrony danych

Szczegółowe informacje znajdują się w opisie stanowiska pracy Korporacyjnego Inspektora Ochrony Danych oraz w aktualnie obowiązującym dokumencie „Roles & Responsibilities Handbook”.

Wdrażanie zasad „Privacy by Design” i „Default” jest inicjowane przez Korporacyjnego Inspektora Ochrony Danych. Dlatego działy przetwarzające dane osobowe lub planujące takie przetwarzanie (np. People, IT,

Purchising) muszą uprzednio powiadomić o tym fakcie Korporacyjnego Inspektora Ochrony Danych, aby zapewnić prawidłowe wdrożenie wszystkich niezbędnych środków ochrony danych.

Korporacyjny Inspektor Ochrony Danych podlega Korporacyjnemu Dyrektorowi ds. Zgodności (Chief Compliance Officer). Korporacyjny Inspektor Ochrony Danych podlega i raportuje również bezpośrednio Zarządowi NDBS. Przynajmniej raz w roku Korporacyjny Inspektor Ochrony Danych składa raport na temat stanu ochrony danych w Grupie NDBS.

Pracownicy Grupy NDBS, Osoby, których dane dotyczą, oraz organy ochrony danych mogą kierować swoje prośby o informacje, porady, pytania i wątpliwości dotyczące ochrony danych bezpośrednio do Korporacyjnego Inspektora Ochrony Danych. Zapytania te są zawsze traktowane jako poufne i nie są przekazywane osobom nieupoważnionym.

2.2.3 Lokalni Koordynatorzy ds. Ochrony Danych

Jeśli wymagane, w spółce zależnej w Grupie NDBS należy powołać Lokalnego Koordynatora Ochrony Danych. Niemniej jednak w spółce zależnej powinna zostać wyznaczona Lokalna Osoba Odpowiedzialna za Ochronę Danych.

Lokalny Koordynator Ochrony Danych musi posiadać kwalifikacje w zakresie wiedzy fachowej i rzetelności, aby wdrażać odpowiednie wymogi ochrony danych w swojej lokalnej spółce Grupy NDBS. Możliwe jest zatrudnienie Lokalnego Koordynatora Ochrony Danych wewnątrz lub na zewnątrz, w niepełnym lub pełnym wymiarze czasu pracy. W przypadku braku Lokalnego Koordynatora Ochrony Danych Osobowych, osobą kontaktową dla Korporacyjnego Inspektora Ochrony Danych Osobowych jest Dyrektor Zarządzający spółki zależnej. Dyrektor Zarządzający może wyznaczyć odpowiedniego zastępcę, który będzie wypełniał ten obowiązek i pełnił funkcję osoby kontaktowej dla Korporacyjnego Inspektora Ochrony Danych.

Lokalny Koordynator Ochrony Danych wspiera wdrażanie DPMS w lokalnej spółce Grupy NDBS (spółce zależnej) zgodnie z wytycznymi i/lub wymaganiami Korporacyjnego Inspektora Ochrony Danych, aby zapewnić dostosowanie lokalnych działań w zakresie ochrony danych do korporacyjnej strategii ochrony danych.

Lokalny Koordynator ds. Ochrony Danych jest pierwszym punktem kontaktowym dla pracowników danego oddziału, osób, których dane dotyczą, oraz organów ochrony danych.
Lokalny Koordynator ds. Ochrony Danych wspiera odpowiedzialne kierownictwo lokalne we wdrażaniu DPMS i niezbędnych środków ochrony danych w spółce zależnej zgodnie z korporacyjną strategią ochrony danych. Ponadto Lokalny Koordynator ds. Ochrony Danych tworzy i rozwija kulturę ochrony danych w spółce zależnej. Szczegóły dotyczące kwalifikacji, funkcji i zadań Lokalnego Koordynatora ds. Ochrony Danych

można znaleźć w odpowiednim opisie stanowiska (np. wsparcie spółki zależnej w tworzeniu i prowadzeniu lokalnego Rejestru Czynności Przetwarzania Danych, informowanie o lokalnym statusie ochrony danych i prawidłowe informowanie Podmiotów Danych).

Jeżeli Lokalny Koordynator ds. Ochrony Danych znajdzie się w sytuacji konfliktu interesów, należy powiadomić Korporacyjnego Inspektora Ochrony Danych, aby rozwiązać tę sytuację i zapewnić, że obowiązujące przepisy o ochronie danych zostaną odpowiednio uwzględnione.

2.2.4 Sieć Ochrony Danych - Struktura DPMS

Korporacyjny Inspektor Ochrony Danych oraz lokalni Koordynatorzy Ochrony Danych tworzą wspólnie Sieć Ochrony Danych (Data Protection Network).

Sieć Ochrony Danych kontynuuje rozwój i tworzenie systemu DPMS, tworząc niezbędne procesy, a także przygotowując i koordynując działania w zakresie ochrony danych. Sieć Ochrony Danych wspiera Zarząd, funkcje centralne i spółki zależne NDBS w kwestiach ochrony danych. Dlatego też pełni rolę pierwszego punktu kontaktowego w przypadku wszelkich pytań i wniosków dotyczących ochrony danych.

Sieć Ochrony Danych sprawuje ogólnogrupowe zarządzanie w odniesieniu do zadań związanych z systemem DPMS. Wszystkie działy biznesowe i funkcje korporacyjne, jak również wszystkie spółki zależne NDBS podlegają dyrektywom zarządzającemu Siecią Ochrony Danych (Head of Data Protection Network). Sieć Ochrony Danych wspiera Korporacyjnego Inspektora Ochrony Danych we wdrażaniu zasad Privacy by Design i Default w Grupie NDBS.

Sieć Ochrony Danych ściśle współpracuje z globalnymi działami: Corporate Compliance Function, Information Security Management i Audit Department w celu ujednolicenia procesów, wykorzystania synergii i zapewnienia zgodności produktów z przepisami o ochronie danych.

2.3 Zakres stosowania

Zakres stosowania jest określony w Tabela 2.

	Grupa	
		NDBS AG
	Wszyscy pracownicy	X

Tabela 2 - Zakres stosowania

Niniejsza Polityka ma zastosowanie do wszystkich spółek Grupy NTT DATA Business Solutions, czyli do wszystkich spółek krajowych i zagranicznych, w których NTT DATA Business Solutions AG posiada bezpośrednio lub pośrednio ponad 50% udziałów lub sprawuje kontrolę zarządczą.

Zakres niniejszej polityki skierowany jest do odpowiedzialnych działów przetwarzających Dane Osobowe (np. People, Sales, Marketing), działów wspierających odpowiedzialne działy w tych działaniach (np. IT) oraz użytkowników systemów przetwarzających Dane Osobowe w celu realizacji ich zadań operacyjnych w ramach Grupy NDBS. Odpowiedni dyrektorzy tych działów są odpowiedzialni za wdrożenie niniejszej polityki do działalności swoich działów. Właściwe wdrożenie musi być regularnie kontrolowane przez odpowiedzialny dział. Korporacyjny Inspektor Ochrony Danych wspiera odpowiedzialny dział w tym zadaniu.

2.4 Definicje i skróty

2.4.1 Definicje

	Termin	Opis
	Grupa NDBS, ang. NDBS Group	Wszelkie odniesienia do Grupy NDBS w niniejszej Polityce odnoszą się do NTT Data Business Solutions AG i jej spółek w 100% zależnych, jak również do każdej innej spółki, w której NTT Data Business Solutions AG lub jedna ze spółek zależnych sprawuje bezpośrednią lub pośrednią kontrolę.
	Firma Grupy NDBS, ang. NDBS Group company	Wszelkie odniesienia do spółki Grupy NDBS dotyczą odpowiedniej spółki wchodzącej w skład Grupy NDBS.
	Dane osobowe, ang. Personal Data	Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (np. imię i nazwisko, adres, data urodzenia, stan cywilny, numer personalny, fotografie, stanowisko zawodowe, identyfikator użytkownika).
	Ochrona danych, ang. Data Protection	Ochrona osób fizycznych przed naruszeniem ich praw osobistych do samodzielnego decydowania o ujawnianiu i wykorzystywaniu ich Danych Osobowych oraz o przetwarzaniu tychże Danych Osobowych. Ochrona Danych obejmuje wszelkie środki, procedury, procesy, narzędzia i instrukcje dotyczące działań, które zapewniają, że wszystkie operacje biznesowe w Grupie NDBS i ze stronami trzecimi są prowadzone zgodnie z obowiązującymi wymogami w zakresie ochrony danych, w szczególności z GDPR.
	System informatyczny, ang. IT System	Sprzęt i oprogramowanie stosowane w firmie Grupy NDBS w celu przechowywania, przetwarzania i przekazywania Danych Osobowych.
	Podmiot danych, ang. Data Subject	Podmiotem danych może być każda zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna.

Tabela 3 – Definicje

2.4.2 Skróty

	Skrót	Opis
	DPMS	System Zarządzania Ochroną Danych, ang. Data Protection Management System
	GDPR	Ogólne rozporządzenie o ochronie danych (UE) 2016/679
	NDBS	NTT DATA Business Solutions
	RoPA	Rejestr czynności przetwarzania danych, ang. Record of Processing Activities

Tabela 4 – Skróty

2.5 Inne obowiązujące dokumenty

- Patrz system zarządzania dokumentami

3. Wymagania dotyczące ochrony danych

3.1 Zasady ochrony danych

Poniższe wymagania stanowią podstawę do przetwarzania danych osobowych w ramach Grupy NDBS i poszczególnych spółek Grupy NDBS. Odpowiedzialny dział musi zawsze przestrzegać tych podstawowych zasad. W razie wątpliwości należy skontaktować się z Korporacyjnym Inspektorem Ochrony Danych lub Siecią Ochrony Danych w celu uzyskania dalszych porad.

3.1.1 Zgodność przetwarzania z prawem (Lawfullness of Processing)

Przetwarzanie Danych Osobowych w spółce Grupy NDBS jest surowo zabronione, chyba że:

- podmiot danych wyraził zgodę na przetwarzanie danych i zgoda ta została odpowiednio udokumentowana lub
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (np. umowy o pracę) lub
- przetwarzanie jest konieczne do wypełnienia obowiązku prawnego lub
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, lub
- przetwarzanie danych jest konieczne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub osobę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec takich interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

W przypadku przetwarzania szczególnych rodzajów Danych Osobowych zgodnie z 3.2.3 (Klasyfikacja Danych Osobowych) niniejszej Polityki, zastosowanie ma wyłącznie opcja (1) niniejszej sekcji 3.1.1.

Powód gromadzenia, przetwarzania i/lub wykorzystywania danych osobowych musi być udokumentowany przez odpowiedzialny dział przed rozpoczęciem przetwarzania w ramach RoPA.

3.1.2 Prywatność w fazie projektowania (Privacy by Design)

Należy gromadzić tylko te dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania.

3.1.3 Przejrzystość (Transparency)

Zabronione jest tajne przetwarzanie danych. Osoby, których dane dotyczą, muszą zostać wcześniej poinformowane o przetwarzaniu ich danych osobowych. Indywidualne wyjątki od tego wymogu muszą być wcześniej omówione z Korporacyjnym Inspektorem Ochrony Danych i przez niego zatwierdzone.

3.1.4 Ograniczenie Celu (Purpose Limitation)

Dane osobowe mogą być przetwarzane wyłącznie w określonym celu, w jakim zostały zebrane. Cel ten musi być uprzednio udokumentowany w przejrzysty sposób przez odpowiedzialny dział. Wykorzystanie Danych Osobowych do innych celów jest dozwolone wyłącznie za zgodą Podmiotu Danych lub na podstawie przepisów prawa. Przetwarzanie danych może odbywać się wyłącznie w celach służbowych Grupy NDBS, ponieważ jakiekolwiek wykorzystanie Danych Osobowych do celów prywatnych jest zabronione. Zmiana celu jest możliwa tylko pod pewnymi warunkami i musi zawsze odbywać się pod nadzorem Lokalnego Koordynatora Ochrony Danych lub, jeśli to konieczne, Korporacyjnego Inspektora Ochrony Danych.

3.1.5 Prawo do bycia zapomnianym (Rigth to be Forgotten)

Dane osobowe muszą zostać usunięte, gdy nie są już potrzebne do realizacji indywidualnego celu, dla którego zostały pierwotnie zgromadzone, chyba że istnieje prawny okres ich przechowywania, który został udokumentowany przez odpowiedzialny dział w ramach koncepcji usuwania danych.

3.2 Postanowienia dotyczące ochrony danych

Poniższe postanowienia są wiążące dla wszystkich działań związanych z przetwarzaniem Danych Osobowych w ramach Grupy NDBS i muszą być zawsze przestrzegane przez odpowiedzialny dział, jeśli ma to zastosowanie do danego działania związanego z przetwarzaniem. W razie wątpliwości należy skontaktować się z Korporacyjnym Inspektorem Ochrony Danych lub Siecią Ochrony Danych w celu uzyskania dalszych porad.

3.2.1 Bezpieczeństwo danych (Data Security)

Firma Grupy NDBS przestrzega wymogu ochrony danych osobowych w zakresie środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych. Więcej szczegółów w dokumencie „Information Security Policy”.

3.2.2 Usuwanie danych osobowych

Usuwanie danych osobowych jest niezbędne do przestrzegania przepisów o ochronie danych osobowych. Środki służące do usuwania danych osobowych zależą od stopnia wrażliwości tych danych.

Okres usuwania danych, jak również procedura usuwania danych i strona odpowiedzialna muszą być udokumentowane w koncepcji usuwania danych przez odpowiedzialny departament w ramach zgłoszenia czynności przetwarzania danych do Rejestru Czynności Przetwarzania Danych (RoPA).

Dane osobowe, które nie są już potrzebne do celów, dla których zostały zgromadzone, muszą zostać usunięte. Jeśli Dane osobowe muszą być przechowywane ze względu na wymóg prawny, prawny okres przechowywania rozszerza tę podstawową zasadę usuwania Danych osobowych. W takim przypadku okres przechowywania musi być udokumentowany w koncepcji usuwania danych z wyraźnym odniesieniem do wymogu prawnego przez odpowiedzialny dział.

Formą usunięcia danych może być ich anonimizacja. Anonimizacja danych osobowych musi zawsze odbywać się pod nadzorem Lokalnego Koordynatora ds. Ochrony Danych lub, w razie potrzeby, Korporacyjnego Inspektora Ochrony Danych.

3.2.3 Klasyfikacja danych osobowych

Dane osobowe muszą być klasyfikowane jako poufne (confidential) i odpowiednio traktowane.

Szczególne rodzaje danych osobowych, takie jak:

- Dane dotyczące zdrowia
- Dane religijne
- Dane etniczne
- Dane dotyczące orientacji seksualnej
- Dane dotyczące identyfikacji
- Dane dotyczące poglądów politycznych
- Członkostwo w związkach zawodowych
- Dane genetyczne
- Dane biometryczne itp.

muszą być klasyfikowane jako ściśle poufne (strictly confidential) i odpowiednio traktowane z zachowaniem jeszcze wyższego poziomu ochrony i bezpieczeństwa za pomocą odpowiednich środków technicznych i organizacyjnych.

Wszelkie odstępstwa od tego wymogu ochrony danych muszą być wcześniej omówione z Korporacyjnym Inspektorem Ochrony Danych.

3.2.4 Zobowiązanie do zachowania poufności danych

Zobowiązanie do zachowania tajemnicy danych jest ważnym środkiem ochrony Danych Osobowych poprzez budowanie świadomości wszystkich pracowników przetwarzających Dane Osobowe w Grupie NDBS. Pracownikom nie wolno wykorzystywać Danych Osobowych do celów prywatnych ani w inny sposób uzyskiwać nieuprawnionego dostępu do Danych Osobowych, które nie są im potrzebne do wykonywania ich zadań zgodnie z indywidualnym zakresem obowiązków (zasada ograniczonego dostępu).

Zobowiązanie to musi zostać uzyskane od pracownika przez dział HR (People Department) przed podjęciem przez niego zadań na rzecz Grupy NDBS.

Podpisany dokument musi zostać zarchiwizowany przez właściwy dział HR jako część akt pracownika.

3.2.5 Szkolenia z zakresu ochrony danych osobowych

Oprócz pisemnych instrukcji i polityk wdrożenie systemu DPMS ma być wspierane przez regularne sesje szkoleniowe dla pracowników w celu zapewnienia określonym grupom docelowym pracowników informacji na temat ogólnych i szczegółowych wymogów w zakresie ochrony danych.

Szkolenia mogą odbywać się w formie szkoleń internetowych (E-Learning) lub stacjonarnych (face-to-face). Przeprowadzenie szkoleń jest organizowane wspólnie z odpowiedzialnymi kierownikami działów i dokumentowane pisemnie przez Sieć Ochrony Danych.

3.2.6 Dostęp do systemu informatycznego

Należy dopilnować, aby dostęp do systemu informatycznego miały tylko uprawnione osoby, zwłaszcza jeśli osoba łączy się z systemem informatycznym spoza Grupy NDBS. Uprawnienia do dostępu muszą być udokumentowane na poziomie stanowiska w koncepcji uprawnień jako część RoPA i zapewnione przez odpowiedzialny dział przez cały czas.

Szczegółowe informacje na temat środków bezpieczeństwa IT dostępne w dokumencie „Information Security Policy” (programy antywirusowe, złośliwe oprogramowanie, wytyczne dotyczące haseł, środki bezpieczeństwa sieci, szyfrowanie, kopie zapasowe / ciągłość działania itp.)

3.2.7 Rejestr Czynności Przetwarzania (RoPA)

Każda firma (spółka zależna) Grupy NDBS jest zobowiązana do stworzenia i utrzymywania szczegółowej listy wszystkich metod gromadzenia, przetwarzania i/lub wykorzystywania Danych Osobowych w Rejestrze Czynności Przetwarzania (RoPA). Za utworzenie i prowadzenie Rejestru Czynności Przetwarzania odpowiedzialne jest lokalne kierownictwo. Rejestr Czynności Przetwarzania musi być prowadzony w korporacyjnym oprogramowaniu do ochrony danych „OneTrust".
Kierownik odpowiedniego działu zgłasza wszystkie nowe i zaktualizowane procedury i oprogramowanie, które odnoszą się bezpośrednio lub pośrednio do gromadzenia, przetwarzania i/lub wykorzystywania danych osobowych, za pomocą formularza zgłoszeniowego OneTrust (patrz Data Protection Intranet).

Powiadomienie zawiera niezbędne informacje na temat celu, upoważnionych stron, dat usunięcia, kategorii danych, Osób, których dane dotyczą, potencjalnych odbiorców Danych osobowych (np. partnerów biznesowych, dostawców usług SaaS) oraz podstawowe informacje na temat dodatkowego wymogu przeprowadzenia Oceny wpływu na prywatność (Privacy Impact Assesment). W oparciu o te informacje Korporacyjny Inspektor Ochrony Danych przeprowadza i dokumentuje ocenę ryzyka związanego z czynnościami przetwarzania.

We współpracy z Siecią Ochrony Danych lub, w razie potrzeby, z Korporacyjnym Inspektorem Ochrony Danych, właściciel czynności przetwarzania (kierownik działu, który wymaga gromadzenia, przetwarzania i/lub wykorzystywania Danych Osobowych) musi uprzednio wyjaśnić, czy przetwarzanie Danych Osobowych jest dozwolone, a poziom bezpieczeństwa danych jest wystarczający w stosunku do rodzajów przetwarzanych Danych Osobowych. W razie potrzeby należy wprowadzić poprawki zalecane przez Sieć Ochrony Danych / Korporacyjnego Inspektora Ochrony Danych.

Sieć Ochrony Danych będzie wspierać lokalne kierownictwo w tworzeniu i prowadzeniu Rejestru Czynności Przetwarzania w oparciu o informacje uzyskane od odpowiedzialnych działów. Właściciel działalności związanej z przetwarzaniem danych jest zobowiązany do niezwłocznego skontaktowania się z Siecią Ochrony Danych w przypadku zmiany procedury / dużej aktualizacji oprogramowania.
Dokumentacja proceduralna „Record of Processing Activities (RoPA)" zawiera dodatkowe informacje i musi być zawsze przestrzegana przez osoby odpowiedzialne.

3.2.8 Przekazywanie Danych Osobowych w ramach Grupy NDBS (Przekazanie Grupowe)

Grupa NDBS posiada na całym świecie różne spółki stowarzyszone (zwane dalej „spółkami NDBS"). Jednakże, ponieważ nie istnieje prawdziwe „wyłączenie grupowe", przekazywanie Danych Osobowych w ramach Grupy NDBS podlega tym samym warunkom, które mają zastosowanie do przekazywania Danych

Osobowych zewnętrznej stronie trzeciej. Należy rozróżnić przekazywanie Danych Osobowych do spółek NDBS znajdujących się na terenie Unii Europejskiej i poza nią.

Dział odpowiedzialny za dane osobowe musi prowadzić przegląd wszystkich firm NDBS świadczących usługi na rzecz tego działu, dla których dane osobowe są gromadzone, przetwarzane i/lub wykorzystywane. W takim przypadku firmy NDBS muszą podpisać umowę o przekazaniu grupowym. Możliwe jest zawarcie Ramowej Umowy Grupowego Przekazania Danych (Group Transfer Agreement), jednak opcja ta musi zostać wcześniej omówiona z korporacyjnym inspektorem ochrony danych. Odpowiedzialny departament musi informować Sieć Ochrony Danych o wszelkich zmianach/uzupełnieniach w przeglądzie. Ponadto firma NDBS wykonująca usługę musi utworzyć i utrzymywać własny wykaz wszystkich usług świadczonych przez nią na rzecz innych firm NDBS, w których przetwarzane są dane osobowe.

Transfer Danych Osobowych pomiędzy dwoma spółkami Grupy NDBS w Unii Europejskiej lub Europejskim Obszarze Gospodarczym może być uznany za bezpieczny. Jednakże, jeśli Dane Osobowe są przekazywane do spółki NDBS spoza tego obszaru (np. USA), należy ocenić, czy odbiorca zapewnia odpowiedni poziom ochrony Danych Osobowych. W przypadku takiego transferu bardzo ważne jest, aby przed rozpoczęciem przesyłania Danych Osobowych zawarte zostały odpowiednie umowy, np. Standardowe Klauzule Umowne UE.

W przypadku przekazywania danych osobowych poza UE, Grupa NDBS stosuje Standardowe Klauzule Umowne UE - EU Standard Contracting Clauses (tzw. „SCC”) w ich najnowszej formie. W takim przypadku Lokalny Koordynator Ochrony Danych musi zostać wcześniej zaangażowany przez odpowiedzialny dział.

Dane osobowe wykorzystywane do komunikacji wewnętrznej w ramach Grupy NDBS (adres operacyjny, dane funkcyjne, numer telefonu służbowego itp.) są wyłączone z niniejszego punktu 3.2.8.

3.2.9 Przetwarzanie danych osobowych przez strony trzecie

Przetwarzanie Danych Osobowych przez stronę trzecią polega na przekazywaniu Danych Osobowych przez jeden podmiot prawny z Grupy NDBS innemu podmiotowi prawnemu spoza grupy (np. outsourcing, usługi wspólne, usługi IT).

Jeżeli w ramach umowy firma z Grupy NDBS powierza osobie trzeciej przetwarzanie Danych Osobowych, zobowiązuje się ona do wyboru wykonawcy, który zapewni niezbędne techniczne i organizacyjne środki bezpieczeństwa dla przetwarzania Danych Osobowych zgodnie z wymogami Grupy NDBS w zakresie ochrony i bezpieczeństwa danych.

Przetwarzanie danych osobowych przez osoby trzecie musi być uregulowane w pisemnej umowie, zwanej Umową o Przetwarzaniu Danych – ang. Data Processing Agreement (DPA). Umowa o Przetwarzaniu Danych reguluje prawa i obowiązki zleceniobiorcy oraz firmy NDBS. Do tego celu należy wykorzystać standardową Umowę o Przetwarzaniu Danych NDBS. Odpowiedzialny dział musi prowadzić wykaz wszystkich usługodawców, z którymi zawarto umowę o przetwarzaniu danych, i informować Sieć Ochrony Danych o wszelkich zmianach/uzupełnieniach w tym wykazie.

Spółki zależne Grupy NDBS pozostają odpowiedzialne za prawidłowe przetwarzanie Danych Osobowych, a także pozostają osobami kontaktowymi dla Podmiotów Danych, których dotyczy przetwarzanie ich Danych Osobowych. Z tego względu konieczne jest, aby Sieć Ochrony Danych była zaangażowana w cały proces przetwarzania Danych Osobowych przez osoby trzecie, aby zapewnić, że wymagania Grupy NDBS w zakresie ochrony danych są zawsze spełnione.

Więcej szczegółowych informacji na temat umów o przetwarzaniu danych można znaleźć w polityce NDBS „Data Processing Agreements”.

3.2.10 Zakup i wdrożenie oprogramowania/sprzętu komputerowego

Sieć Ochrony Danych musi być zaangażowana w każde zamówienie produktów i usług, jak również we wdrażanie oprogramowania i sprzętu do systemu informatycznego, który jest przeznaczony lub może być wykorzystywany do gromadzenia, przetwarzania i/lub wykorzystywania Danych Osobowych. Przed wdrożeniem oprogramowania/sprzętu należy skontaktować się z Korporacyjnym Inspektorem Ochrony Danych w sprawie wszelkich wątpliwości/niezbędnych zmian w oprogramowaniu/sprzęcie.
Dlatego na początku projektu lub sprawy biznesowej należy skontaktować się z Lokalnym Koordynatorem ds. Ochrony Danych.

3.2.11 Procesy obejmujące przetwarzanie danych osobowych

Dział odpowiedzialny za przetwarzanie danych osobowych, wdrażając lub zmieniając procesy, które wiążą się z gromadzeniem, przetwarzaniem lub wykorzystywaniem danych osobowych, musi zwrócić się do Korporacyjnego Inspektora Ochrony Danych w sprawie wszelkich wątpliwości prawnych lub wymaganych zmian w procesie. Możliwe jest wprowadzenie do procesów obejmujących przetwarzanie danych osobowych bramek kontrolnych w celu zapewnienia zgodności z wymogami ochrony danych.

Dlatego na etapie tworzenia/aktualizacji procesów obejmujących przetwarzanie danych osobowych należy skontaktować się z Korporacyjnym Inspektorem Ochrony Danych.

3.2.12 Powiadamianie o naruszeniu ochrony danych

W przypadku utraty danych osobowych i/lub uzyskania wiedzy o nich przez osobę nieupoważnioną, właściwy dział musi niezwłocznie powiadomić o tym fakcie Korporacyjnego Inspektora Ochrony Danych i Lokalnego Koordynatora ds. Ochrony Danych.

Korporacyjny Inspektor Ochrony Danych poinformuje odpowiednie kierownictwo i jest uprawniony do podjęcia niezbędnych kroków zgodnie z wymogami Grupy NDBS w zakresie ochrony danych i obowiązującymi przepisami prawa (w szczególności skontaktuje się z właściwym organem ochrony danych i, w razie potrzeby, z osobami, których dane dotyczą).

3.2.13 Ocena wpływu na prywatność

W trakcie zgłoszenia czynności przetwarzania danych do RoPA ustala się, czy konieczne jest przeprowadzenie oceny wpływu na prywatność. Ocena wpływu na prywatność (Privacy Impact Assessment) to analiza ryzyka w przypadku wysokiego ryzyka dla danych osobowych osób, których dane dotyczą (np. przetwarzanie z wykorzystaniem nowych technologii, nadzór wideo, dane biometryczne), mająca na celu minimalizacji wysokiego ryzyka. Na czas przeprowadzania oceny wpływu na prywatność należy wstrzymać czynności przetwarzania. Jeżeli nie można zidentyfikować i wdrożyć rozwiązań w celu zmniejszenia wysokiego ryzyka, należy skontaktować się z właściwym organem ochrony danych w sprawie przetwarzania. Ocena wpływu na prywatność jest przeprowadzana przez odpowiedni dział NDBS, który jest wspierany przez Korporacyjnego Onspektora Ochrony Danych.

3.2.14 Prawa i informacje dla Podmiotów Danych

Zapewnienie przejrzystości w zakresie przetwarzania danych osobowych Podmiotów danych (Data Subjects), czyli osób, których przetwarzane dane dotyczą jest kluczowym elementem systemu DPMS. Wszystkie niezbędne informacje będą przekazywane Podmiotom Danych w odpowiednim czasie. Odpowiedzialny dział będzie wspierany w tym obowiązku przez Sieć Ochrony Danych. Dodatkowe prawa przysługujące Podmiotom Danych, to:

- dostęp do danych osobowych
- poprawianie danych osobowych
- usuwanie danych osobowych
- ograniczenie przetwarzania danych osobowych
- sprzeciw wobec przetwarzania danych osobowych

3.3 Rozliczalność (Accountability)

Spełnienie wymagań wynikających z niniejszej polityki musi być w każdej chwili możliwe do sprawdzenia („rozliczalność") przez odpowiedzialne strony. Dowody należy przedstawić w postaci rozstrzygającej i wyczerpującej dokumentacji pisemnej dotyczącej podjętych działań i decyzji prowadzących do ich podjęcia. Zgodność z niniejszą sekcją 3.3 „Rozliczalność" jest kontrolowana przez dział audytu wewnętrznego. Jeśli odpowiedzialny dział nie przestrzega wymogów ochrony danych w ramach niniejszej polityki, niezgodne z nimi czynności przetwarzania mogą zostać zakazane przez Korporacyjnego Inspektora Ochrony Danych.

DocuSign

Certificate Of Completion

Envelope Id: B19704B8A9034914964B0EFDE87D04E9
Status: Completed
Subject: Here is your signed document: Korporacyjna_Ochrona_Danych_PY_PL.docx
Source Envelope:
Document Pages: 18
Signatures: 1
Certificate Pages: 1
Initials: 0
AutoNav: Disabled
EnvelopeId Stamping: Disabled
Time Zone: (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Envelope Originator:
Dominika Kufel
Königsbreede 1
Bielefeld, NRW 33605
Dominika.Kufel@bs.nttdata.com
IP Address: 85.221.149.146

Record Tracking

Status: Original
9/2/2022 4:46:07 PM
Holder: Dominika Kufel
Dominika.Kufel@bs.nttdata.com
Location: DocuSign

Signer Events	Signature	Timestamp
Dominika Kufel Dominika.Kufel@bs.nttdata.com Security Level: Email, Account Authentication (None)	DocuSigned by: Dominika Kufel 68035437753542D... Signature Adoption: Pre-selected Style Using IP Address: 85.221.149.146	Sent: 9/2/2022 4:46:43 PM Viewed: 9/2/2022 4:47:06 PM Signed: 9/2/2022 4:49:23 PM Freeform Signing

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp
Doreen.Seliger@nttdata.com Security Level: Email, Account Authentication (None)	COPIED	Sent: 9/2/2022 4:49:24 PM Viewed: 9/2/2022 4:50:17 PM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	9/2/2022 4:46:44 PM
Certified Delivered	Security Checked	9/2/2022 4:47:06 PM
Signing Complete	Security Checked	9/2/2022 4:49:23 PM
Completed	Security Checked	9/2/2022 4:49:24 PM

Payment Events	Status	Timestamps