POLITYKA OCHRONY DANYCH

CZĘŚĆ ORGANIZCYJNA

NSFLOW SP. Z O.O. | 50-343 WROCŁAW, UL. MIKOŁAJA REJA 77/4A

NSflow Sp. z o.o.
50-343 Wrocław
ul. Mikołaja Reja 77/4A
NIP: 8982241435

SPIS TREŚCI

NSflow Sp. z o.o.
50-343 Wrocław
ul. Mikołaja Reja 77/4A
NIP: 8982241435

1. WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

2. DEFINICJE

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

RODO – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016).

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej.

Przetwarzanie danych osobowych to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Anonimizacja- zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych.

Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający (**Procesor)** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu /pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. Listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Szczególne kategorie danych osobowych - ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Profilowanie – jest dowolną forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji

ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

3. REJESTR CZYNNOŚCI PRZETWARZANIA

Rejestr jest sporządzany w **NSflow Sp. z o.o.** Dokumentacja z rejestru pozwoli rozliczyć się przed organem nadzoru w przypadku kontroli. Istotne jest to, aby rejestr czynności był na bieżąco aktualizowany, a jego zawartość odpowiednio chroniona przed nieuprawnionymi osobami. Każdy administrator danych zobowiązany jest prowadzić rejestr czynności przetwarzania danych osobowych za który odpowiada. Rejestr operacji przetwarzania danych osobowych prowadzony przez podmiot przetwarzający powinien zawierać opis odnoszący się do danych osobowych powierzonych mu do przetwarzania przez innych administratorów danych. Obowiązki te realizowane są w załączniku **04 Rejestr Czynności Przetwarzania**

4. UMOWY POWIERZENIA

Podmiotem, któremu ADO (**NSflow Sp. z o.o.**) może powierzyć przetwarzanie danych może być osoba fizyczna lub prawna, organ publiczny, jednostka organizacyjna lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Jeżeli administrator chce powierzyć przetwarzanie danych w jego imieniu, to może w tym celu korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. ADO ma obowiązek dołożyć szczególnej staranności przy wyborze procesora. Administrator może ocenić czy podmiot, mający w jego imieniu przetwarzać dane, spełnia wymienione wymogi, na przykład poprzez skontrolowanie stosowanych przez niego sposobów zabezpieczenia danych. Przeprowadzanie audytów i kontroli u kontrahentów, którym powierza się dane do przetwarzania. RODO umożliwienia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania audytów. Przeprowadzania takich kontroli, leży w interesie administratora. To na nim ciąży prawna i biznesowa odpowiedzialność za przetwarzane dane. Wzór umowy powierzenia przedstawia załącznik: **11 Umowa powierzenia.**

5. OCENA SKUTKÓW (ANALIZA RYZYKA)

Ocena skutków jest formalną, określoną w art. 35 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. Jeżeli **NSflow Sp. z o.o.** nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem.

A. WSTĘP

1. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane te w postaci zbiorów (kategorii osób) zostały wykazane w załączniku **02 Wykaz zbiorów danych osobowych.**
2. Wykaz zbiorów danych obejmuje:
    a) Nazwa zbioru danych
    b) Cele przetwarzania
    c) Aktywa
    d) Planowane terminy usunięcia poszczególnych kategorii danych.
    e) Lokalizacja

B. OCENA NIEZBĘDNOŚCI ORAZ PROPORCJONALNOŚCI (ZGODNOŚĆ Z PRZEPISAMI RODO)

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator zobowiązany jest do spełnienia obowiązków prawnych wobec danych w zbiorach. W szczególności należy zapewnić, że:

a) dane te są legalnie przetwarzane (na podstawie art. 6, 9),
b) dane te są adekwatne w stosunku do celów przetwarzania,
c) dane te są przetwarzane przez określony czas (retencja danych),
d) wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14) wraz ze wskazaniem ich praw,
e) opracowano klauzule informacyjne dla powyższych osób,
f) istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28), prowadzony jest wykaz podmiotów przetwarzających prowadzony jest w załączniku **03 Rejestr umów powierzenia).**

C. ANALIZA RYZYKA

Na podstawie delegacji przewidzianej przez ustawodawcę unijnego każdy administrator danych osobowych zobowiązany został do stosowania podejścia opartego na analizie ryzyka. Kluczowym aspektem pozwalającym zrozumieć koncepcję takiego stanowiska jest prześledzenie procedowania w ramach oceny skutków dla ochrony danych, które nie jest obowiązkowe w przypadku każdej operacji przetwarzania. Przeprowadzenia oceny skutków dla ochrony danych wymaga się wyłącznie w przypadku, gdy dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Wobec powyższego podejmując decyzję o wykonaniu bądź zaniechaniu wykonania obowiązków wskazanych w art. 35 ust. 1 RODO administrator winien posiadać wiedzę o skali ryzyka występującego przy danym rodzaju przetwarzania. Wobec powyższego sam fakt niespełnienia warunków nakładających obowiązek przeprowadzenia oceny skutków dla ochrony danych nie zmniejsza jednak ogólnego obowiązku wdrożenia przez administratorów środków umożliwiających odpowiednie zarządzanie ryzykiem naruszenia prawa i wolności osób, których dane dotyczą. W praktyce oznacza to, że administratorzy muszą stale oceniać ryzyko powodowane przez czynności przetwarzania w celu określenia, kiedy dany rodzaj przetwarzania „może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych".

D. SZCZEGÓŁOWA METODYKA WYKONANIA ANALIZY RYZYKA ZAWARTA ZOSTAŁA W ZAŁĄCZNIKACH:

a) 05 Procedura Zarządzania Ryzykiem.
b) 06 Wstępna analiza ryzyka – objaśnienia.
c) 07 Wstępna analiza ryzyka – matryca.
d) 08 Szczegółowa analiza zdiagnozowanego ryzyka.
e) 09 DPIA objaśnienia.
f) 10 DPIA - matryca ryzyka.
g) 10a DPIA

E. PONOWNA ANALIZA RYZYKA

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).

6. ŚRODKI ORGANIZACYJNE I TECHNICZNE ZABEZPIECZAJĄCE DANE OSOBOWE

a) Administrator jest zobowiązany do stosowania środków technicznych i organizacyjnych (zabezpieczeń) adekwatnych do zagrożeń naruszenia praw i wolności osób, rozumianych jako zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności
b) Zastosowano środku ochrony fizycznej pomieszczeń wraz z opisem budynków (patrz załącznik **A Polityka Kluczy**).
c) Administrator zastosował środki organizacyjne:

a. wdrożona Polityka Ochrony Danych Osobowych
b. wdrożona Polityka Bezpieczeństwa Teleinformatycznego
c. wdrożona procedura w zakresie zarządzania uprawnieniami do systemów informatycznych przetwarzających dane osobowe
d. wdrożona procedura w zakresie bezpiecznego logowania i zarządzania hasłami
e. wdrożona procedura w zakresie zarządzania systemami informatycznymi
f. wdrożona procedura w zakresie opiniowania oraz akceptacji zmian w projektach oraz infrastrukturze
g. wdrożona procedura w zakresie dostępu do kodów źródłowych, ich bezpiecznego przechowywania
h. wdrożona procedura w zakresie ciągłości działania
i. wdrożona procedura w zakresie zarządzania środowiskami rozwojowymi, testowymi i deweloperskimi, ich separacji
j. wdrożona procedura w zakresie zarządzania podatnościami, aktualizacjami oraz weryfikacją pod kątem bezpieczeństwa stosowanych rozwiązań
k. stosowanie dobrych praktyk oraz wytycznych w zakresie bezpiecznego tworzenia oprogramowania
l. wyznaczona została osoba pełniąca funkcję ABI/IOD nadzorująca przestrzeganie zasad ochrony danych osobowych zgodnie z Ustawą oraz RODO
m. prowadzona jest ewidencja osób upoważnionych do przetwarzania danych gwarantująca rozliczalność procesów przetwarzania danych osobowych, zapewnienie poufności, integralności, dostępności przetwarzanych danych osobowych oraz usług przetwarzania

d) Administrator opracował załącznik **Polityka Ochrony Danych Osobowych – część techniczna** w którym zabezpieczenia fizyczne i techniczne są opisane.

7. REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin (rozumiany jako zabezpieczenie) ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Patrz załącznik - **01 Regulamin Ochrony Danych Osobowych**.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania. Osoby upoważnione przez Administratora Danych Osobowych do przetwarzania Danych Osobowych podpisują: **12 Oświadczenie poufności.**

Administrator prowadzi ewidencję osób upoważnionych – **13 Ewidencja osób upoważnionych**.

8. SZKOLENIA

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO

2. Za przeprowadzenie szkolenia odpowiada Administrator.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia za pomocą załącznika **15 Plan szkolenia.**
4. Materiały szkoleniowe dla uczestników szkolenia opracowano w formie załącznika **16 Szkolenie wewnętrzne.**
5. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania, patrz **12 Oświadczenie poufności.**

9. UPOWAŻNIENIA

A. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych.
B. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
C. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie – patrz załącznik **13 Upoważnienie do przetwarzania danych osobowych.**
D. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia.
E. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja ma charakter pomocniczy i nie jest wymagana przepisami RODO. Patrz załącznik 14 **Ewidencja osób upoważnionych**.

10. UDOSTĘPNIENIE DANYCH

Udostępnienie stanowi przekazanie danych odbiorcy, który sam decyduje o celach i środkach przetwarzania danych. Stając się administratorem danych, może on dokonywać przetwarzania wyłącznie na podstawie tzw. przesłanek legalności. Przepisy pozwalają na udostępnienie danych, jeśli jest to konieczne do realizacji prawnie uzasadnionych celów ich administratora. Przetwarzanie danych nie może naruszać praw i wolności osób, których dane dotyczą. Za legalność udostępniania danych odpowiada administrator. To od niego zależy forma wnioskowania oraz ocena, czy wniosek jest zgodny z przepisami prawa lub czy wymaga określenia przesłanki uzasadniającej. Administrator prowadzi ewidencję udostępnień – załącznik **20 Ewidencja Udostępnień.**

11. PROCEDURA REALIZACJI ŻĄDAŃ OSÓB, KTÓRYCH DANE DOTYCZĄ

Administrator ma obowiązek realizacji praw osób, których dane dotyczą, ma również obowiązek wykazać, że je wypełnia. Została przygotowana procedura, która jest wskazówką postępowania w przypadku otrzymania takiego żądania, patrz załącznik **17 Procedura realizacji żądań osób.**

12. INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego (lub jeśli jest powołany – Inspektora Ochrony Danych)
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator (lub w przypadku powołania – IOD) prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki
    b. inicjuje ewentualne działania dyscyplinarne
    c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu
    d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze posługując się Załącznikiem **18b Formularz rejestracji incydentu.**

6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – Administrator zgłasza je organowi nadzorczemu – **Załącznik 18a - Procedura zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu**.
8. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

13. PROCEDURA PRZYWRÓCENIA DOSTĘPNOŚCI DANYCH OSOBOWYCH I DOSTĘPU DO NICH W RAZIE INCYDENTU FIZYCZNEGO LUB TECHNICZNEGO (BCP)

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Administrator opracował procedury przywracania, opisane w załączniku **19 Plan ciągłości działania**.