Polityka Ochrony Danych Osobowych

Żłobek Gminny w Jaczowie

ul. Główna 21 L

67-210 Jaczów

SPIS TREŚCI

1 SPIS TREŚCI 1
2 WSTĘP 2
3 INWENTARYZACJA DANYCH, ZGODNOŚĆ Z PRAWEM, UPOWAŻNIENIA 2
3.1 Inwentaryzacja danych 2
3.2 Zgodność z prawem 2
3.3 Upoważnienia 2
4 ANALIZY RYZYKA / OCENA SKUTKÓW 3
5 INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI 3
6 REGULAMIN OCHRONY DANYCH OSOBOWYCH 4
7 SZKOLENIA 4
8 REJESTR CZYNNOŚCI PRZETWARZANIA 4
9 AUDYTY, PROCEDURY 4
10 WYKAZ ZABEZPIECZEŃ 5

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.

INWENTARYZACJA DANYCH, ZGODNOŚĆ Z PRAWEM, UPOWAŻNIENIA

INWENTARYZACJA DANYCH

1. Dane osobowe wymagające ochrony zostały wykazane w załączniku 1. Wykaz zbiorów danych osobowych.
2. Wykaz obejmuje zbiory ze stwierdzonym potencjalnym ryzykiem naruszenia praw lub wolności osób fizycznych.
3. Każdy ze zbiorów jest opisany w sposób umożliwiający przeprowadzenie analizy ryzyka.
4. Opis zbiorów obejmuje takie informacje, jak:
    a. nazwę zbioru,
    b. opis celów przetwarzania,
    c. charakter, zakres, kontekst, dokumentowane dane osobowe,
    d. odbiorcy,
    e. funkcjonalny opis operacji przetwarzania,
    f. aktywa służące do przetwarzania danych osobowych (Informacje, Programy, systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing),
    g. Informacja o konieczności wpisu do rejestru czynności przetwarzania,
    h. Informacja o konieczności przeprowadzenia oceny skutków dla zbioru.

ZGODNOŚĆ Z PRAWEM

1. Administrator zapewnia, że:
    a. dane są legalnie przetwarzane (na podstawie art. 6, 9),
    b. dane osobowe są adekwatne w stosunku do celów przetwarzania,
    c. dane osobowe są przetwarzane przez określony konkretny czas (retencja danych),
    d. wobec osób, które przetwarza administrator wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14) wraz ze wskazaniem im praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu),
    e. zapewniono ochronę danych w przypadku powierzenia przetwarzania danych w postaci umów powierzenia z podmiotami przetwarzającymi (art. 28).
2. Potwierdzenie zgodności z prawem przetwarzanych danych osobowych w zbiorach, znajduje się w załączniku 1. Wykaz zbiorów danych osobowych.
3. Klauzule informacyjne znajdują się w załączniku 3. Klauzule informacyjne.
4. Przykładowa umowa powierzenia znajduje się w załączniku 4. umowa powierzenia

UPOWAŻNIENIA

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie – patrz załącznik 5.1. Upoważnienie do przetwarzania danych osobowych .

4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia.
5. Inspektor Ochrony Danych 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 5.2. Ewidencja osób upoważnionych.

ANALIZY RYZYKA / OCENA SKUTKÓW

1. Opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.
2. Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru danych osobowych lub grupy zbiorów charakteryzujących się podobieństwem celów i sposobów przetwarzania.
3. W przypadku konieczności przeprowadzenia oceny skutków (Art. 35), wymagane jest wykonanie następujących czynności:
    a. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania – zawarty w załączniku 1. Wykaz zbiorów danych osobowych,
    b. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów – zawartą w załączniku 1. Wykaz zbiorów danych osobowych,
    c. ocenę ryzyka – patrz 11. Szacowanie procesów - Analiza ryzyka,

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 –patrz załącznik 6. 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 – zgłasza je organowi nadzorczemu.

REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Patrz – 8. Regulamin Ochrony Danych Osobowych.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zatrudniane otrzymują upoważnienie do przetwarzania danych osobowych wraz z oświadczeniem o zachowaniu poufności są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania, patrz 5.1. przykład upoważnienia.

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 IOD.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia za pomocą załącznika 7.1. Plan szkolenia RODO.
4. Materiały szkoleniowe dla uczestników szkolenia opracowano w formie załącznika 7.2. Szkolenie wewnętrzne RODO.
5. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania, patrz 5.1 przykład upoważnienia.

REJESTR CZYNNOŚCI PRZETWARZANIA

1. W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Administratora, wypełnia załącznik 2. RCP - Rejestr czynności prowadzony przez Administratora.

AUDYTY, PROCEDURY

1. Procedura audytu

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W tym celu Administrator stosuje procedurę audytów – patrz 10. Procedury – 1. Procedura audytu.

2. Procedura niszczenia danych
W przypadku koniczności zniszczenia danych należy odwołać się do procedury niszczenia danych - patrz 10. Procedury – 2. Procedura niszczenia danych.

3. Procedura tworzenia kopii zapasowych

Tworzenie kopii zapasowych odbywa się regularnie zgodnie z opisem w procedurze tworzenia kopii zapasowych - patrz 10. Procedury – 3. Procedura tworzenia kopii zapasowych.

4. Procedura zarządzania uprawnieniami
Zmiana modyfikacja lub inne działanie na uprawnieniach użytkownika oraz sposób korzystania z uprawnień został opisanych w procedurach zarządzania uprawnieniami - patrz 10. Procedury – 4. Procedura zarządzania uprawnieniami.

5. Procedura naprawy w serwisach zewnętrznych
Sposób postępowania ze sprzętem komputerowych w przypadku konieczności naprawy w serwisie zewnętrznym został opisany w procedurach naprawy w serwisach zewnętrznych - patrz 10. Procedury – 5. Procedura naprawy w serwisach zewnętrznych.

WYKAZ ZABEZPIECZEŃ

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych, patrz załącznik 11. Wykaz zabezpieczeń.
2. W wykazie wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne.
3. Wykaz jest aktualizowany po każdej analizie ryzyka.