POLITYKA OCHRONY DANYCH OSOBOWYCH

w
Studio GRE Agnieszka Czerwińska
Ul. Dekabrystów 25B lok. 57
42-218 Częstochowa

Spis treści

I.WSTĘP

Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**” (dalej jako **Polityka**) powstał w celu określenia standardów bezpiecznego przetwarzania danych osobowych w przedsiębiorstwie Administratora.

W związku z przetwarzaniem danych przez Administratora powołano niniejszą Politykę, której zadaniem jest zapewnienie przestrzegania podczas przetwarzania danych praw i wolności osób fizycznych, a w szczególności ich prawa do ochrony danych osobowych przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Niniejsza Polityka jest jednym z głównych środków organizacyjnych, stanowi zestaw wymogów, zasad i regulacji ochrony danych osobowych powołanych w celu zapewnienia oraz wykazania przetwarzania tych danych zgodnie z ogólnym rozporządzeniem o ochronie danych – RODO.

II.DEFINICJE

Przez użyte w Polityce określenia należy rozumieć:

Polityka - oznacza niniejszą Politykę ochrony danych osobowych.

RODO - oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).

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

W przypadku niniejszej Polityki Administratorem jest:

Studio GRE Agnieszka Czerwińska
Ul. Dekabrystów 25B lok. 57
42-218 Częstochowa

NIP: 5732580554 REGON: 360887323

Dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Przetwarzanie - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Dane wrażliwe - oznaczają dane o szczególnych kategoriach oraz dane karne.

Szczególne kategorie danych - oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Osoba - oznacza osobę fizyczną, której dane dotyczą.

Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora; Podmiot

przetwarzający jest odrębnym bytem prawnym. Może wykonywać operacje przetwarzania jedynie na udokumentowane polecenie Administratora. W obszarze ISO podmiot ten najczęściej nazywany jest – procesorem.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców.

Czynność przetwarzania - oznacza mniejszy lub większy (krótszy lub dłuższy) wycinek procesu „biznesowego"/ procesu przetwarzania danych realizowanego w konkretnym celu przetwarzania danych. Czynności przetwarzania danych składają się z operacji przetwarzania danych.

Profilowanie - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które 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.

IOD lub Inspektor - oznacza Inspektora Ochrony Danych Osobowych

Zagrożenie – jest to potencjalna przyczyna niepożądanego incydentu, który może powodować szkody dla systemu lub organizacji. Incydenty powstają wskutek zagrożeń. Na zagrożenie i jego prawdopodobieństwo mają wpływ: okoliczności, stan prawny, stan faktyczny, działania, zaniechanie działań i wydarzenia zewnętrzne oraz wewnętrzne, które mogą ale nie muszą wywołać ryzyko wystąpienia incydentu.

Incydent bezpieczeństwa informacji - jest zdarzeniem, którego bezpośrednim lub pośrednim skutkiem jest lub może być naruszenie ochrony danych osobowych.

Naruszenie ochrony danych osobowych - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. W ISO konsekwencja, rezultat zdarzenia;

Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

Zgoda - osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

Ograniczenie przetwarzania - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

Dane dotyczące zdrowia - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia; Zgodnie z Preambułą w motywie (35) - do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego

zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE; numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

Rejestr Czynności Przetwarzania Danych - (**RCPD**) stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności. Pełni również funkcję informacyjną, w tym stanowi źródło informacji o procesach przetwarzania danych w danej organizacji dla organu nadzorczego.

Ocena Skutków Dla Ochrony Danych - jeżeli planowany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Jest to sformalizowana analiza ryzyka przetwarzania danych dla sytuacji, w których to ryzyko zostało ustalone przez organizację jako wysokie.

III.OGÓLNE ZASADY OCHRONA DANYCH OSOBOWYCH

1. Zawartość polityki

Polityka zawiera:

a) opis wymogów, zasad i regulacji ochrony danych osobowych powołanych w celu zapewnienia oraz wykazania przetwarzania danych przez Administratora zgodnie z RODO;

b) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów, procesów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

2. Odpowiedzialność

Polityka Administratora oparta jest na zasadzie odpowiedzialności:

a) odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki jest Administrator reprezentowany przez Panią Agnieszkę Czerwińską – właściciela podmiotu;

b) za stosowanie niniejszej Polityki odpowiedzialni są:

- Administrator;
- wszyscy pracownicy podmiotu Administratora;

c) Administrator zapewnia by w przypadkach, w których zachodzi powierzenie danych, Administrator korzystać będzie z usług tylko takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane im powierzono.

3. Cztery fundamenty Polityki Administratora

Polityka ochrony danych Administratora oparta została na czterech fundamentalnych zasadach

1) **Zasada legalności** − Administrator dba by przetwarzanie danych odbywało się zgodnie z prawem dbając o ochronę prywatności.
2) **Zasada respektowania praw jednostki** − Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
3) **Zasada bezpiecznego przetwarzania** − Administrator zapewnia odpowiedni poziom bezpieczeństwa przetwarzania danych wdrażając odpowiednie środki bezpieczeństwa.
4) **Zasada rozliczalności** − Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

3.1. Realizacja zasady legalności

Administrator przetwarza dane osobowe w poszanowaniu i realizacji następujących zasad:

a) **Legalność –** Administrator przetwarza dane tylko w oparciu o podstawę prawną lub

zgodę, zapewniając rzetelność i przejrzystość dla i wobec osoby, której dane dotyczą.

b) **Celowość** – Administrator zbierane dane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza ich dalej w sposób niezgodny z tymi celami.

c) **Adekwatność –** Administrator zbiera dane adekwatnie, stosownie oraz ograniczając się do danych niezbędnych do realizacji celów, w których są przetwarzane.

d) **Merytoryczna poprawności** – Administrator gromadzi i przetwarza dane z dbałością o ich merytoryczną poprawność i prawidłowość.

e) **Ograniczenie czasowe** – Administrator zapewnia by przechowywanie danych w formie umożliwiającej identyfikację osoby, nie trwało przez okres dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane lub zgodnie z przepisami prawa.

f) **Właściwe zabezpieczenie** – Administrator dokłada wszelkiej staranności by sposób przetwarzania przez nią danych zapewniał dla nich odpowiedni poziom bezpieczeństwa, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem ("integralność i poufność").

3.2. Realizacja zasady respektowania praw jednostki

3.2.1. Administrator realizuje obowiązek spełnienia praw osób, których dane dotyczą poprzez:

a) dbanie o czytelność, przejrzystość, rzetelność oraz zwięzłość przekazywanych informacji w komunikacji z osobami, których dane przetwarza;

b) ułatwianie osobom w korzystaniu z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Administratora oraz w widocznym miejscu w siedzibie Administratora informacji o prawach osób, sposobie skorzystania z nich, kanałach kontaktu z Administratorem oraz ewentualnym cenniku żądań „dodatkowych" itp.;

c) dbanie o dotrzymywanie prawnych terminów realizacji obowiązków względem osób;

d) zapewnienie właściwej realizacji obowiązku informacyjnego przy zbieraniu danych i w innych sytuacjach – **Załącznik nr 1 do Polityki**;

e) stosowanie procedury pozwalającej na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych – **Załącznik nr 3 do Polityki.**

3.2.2. W celu realizacji praw jednostki Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Administratora, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.

3.2.3. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób – **Załącznik nr 4 do Polityki.**

Prawa osób, których dane dotyczą:

a) Prawo dostępu do informacji

b) Prawo do sprostowania danych

c) Prawo do usunięcia danych („prawo do bycia zapomnianym")

d) Prawo do ograniczenia przetwarzania

e) Prawo o powiadomieniu przez Administratora o sprostowaniu, usunięciu, ograniczeniu

f) Prawo do przenoszenia danych

g) Prawo do sprzeciwu

h) Prawo do nie podlegania zautomatyzowanej decyzji

3.3. Realizacja zasady bezpiecznego przetwarzania

Zapewnienie odpowiedniego bezpieczeństwa przetwarzania danych osobowych Administrator realizuje w oparciu o system ochrony danych osobowych składający się z następujących elementów:

1) **Inwentaryzacja danych.** Administrator dokonuje inwentaryzacji zasobów danych osobowych w kontekście czynności przetwarzania ze szczególnym uwzględnieniem: klas danych, okresem przechowywania danych, identyfikacją oraz skutecznością aktualnych środków bezpieczeństwa, prawnych przesłanek przetwarzania danych, obszarów przetwarzania.

2) Administrator nie ma obowiązku prowadzenia Rejestru Czynności Przetwarzania Danych

3) **Minimalizacja.** Administrator posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

   a. zasady zarządzania adekwatnością danych – **minimalizacja zakresu**:

      - Administrator każdorazowo weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania;

      - Administrator dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

   b. zasady reglamentacji i zarządzania **dostępem** do danych - **minimalizacja dostępu** (dostępu do danych):

      - Administrator stosuje ograniczenia dostępu do danych osobowych:

        - prawne *(zobowiązania do poufności, zakresy upoważnień),*
        - fizyczne *(strefy dostępu, zamykanie pomieszczeń),*
        - logiczne *(ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).*

- Administrator nadaje dostęp do przetwarzanych danych osobowych wyłącznie tym osobom, które:
  - zostały skutecznie zapoznane z wyciągiem z podstawowych zasad bezpieczeństwa danych osobowych – **Załącznik nr 12 do Polityki**,
  - zobowiązały się do jego przestrzegania w drodze oświadczenia, oraz do zachowania poufności – **Załącznik nr 13 do Polityki**,
  - oraz otrzymały upoważnienie – **Załącznik nr 14 do Polityki**, precyzujące dostęp do określonego zbioru danych osobowych .
- Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, wedle wzoru stanowiącego **załącznik nr 8.**
- Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.
- Administrator dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.
- Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Administratora.

c. zasady reglamentacji i zarządzania **dostępem** do danych - **minimalizacja czasu** (okres przechowywania danych):
   - Administrator wdraża mechanizmy kontroli cyklu życia danych osobowych w podmiocie Administratora, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.
   - Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów Administratora, jak też z akt podręcznych i głównych oraz we właściwy sposób niszczone.

4) **Bezpieczeństwo.** Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, poprzez:
   - Administrator zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
   - Administrator analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
   - Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Administrator ustala przydatność i stosuje takie środki i podejście jak:

- inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

- środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

- zastosowanie odpowiednich środków ochrony;
- monitorowanie właściwego działania zabezpieczeń oraz cykliczne audyty bezpieczeństwa;
- stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami.

5) **Powierzenie przetwarzania.** Administrator posiada zasady doboru przetwarzających dane na rzecz Administratora, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

Administrator zapewnia by w przypadkach, w których zachodzi powierzenie danych, korzystać będzie z usług tylko takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane im powierzono.

Administrator przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące **Załącznik nr 11 do Polityki – „Wzór umowy powierzenia przetwarzania danych”**.

Administrator rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

Administrator prowadzi rejestr umów powierzenia – **Załącznik nr 9 do polityki.**

3.4. Realizacja zasady rozliczalności

Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

Wszystkie działania dotyczące realizacji zasad bezpieczeństwa w podmiocie Administratora są dokumentowane. Szczególnymi dokumentami służącymi do potwierdzenia rozliczalności Administratora są:

1) **Inwentaryzacja zbirów danych**

2) **Rejestr naruszeń (załącznik nr 6 do polityki)**

3) **Rejestr incydentów (załącznik nr 7 do polityki)**

4) **Rejestr wydanych upoważnień**

5) **Rejestr umów powierzenia przetwarzania**

6) **Rejestr obsługi zgłoszeń osób fizycznych**