POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA,

ul. Dolnych Młynów 5, 31-124 Kraków,

KRS 0000600455, REGON 363659491, **NIP** 6762500968

Wydanie	**1**
Obowiązuje od	**05.03.2019r.**
Zatwierdził do stosowania	**Magdalena Plewniak - Właściciel**

Spis treści:

Wstęp

Niniejszy dokument Polityki Bezpieczeństwa Danych Osobowych, zwany dalej **Polityką**, powstał w związku z wymaganiami Rozporządzenia o Ochronie Danych Osobowych Parlamentu Europejskiego i Rady (UE) 2016/679[1], które wprowadzone zostało w sposób bezpośredni do stosowania w Polskim systemie prawnym;
Rozporządzenie w motywie 78 obliguje Administratora, by ten przyjął wewnętrzne polityki i wdrożył środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych.
Niniejsza Polityka uwzględniając powyższe wymaganie określa zasady ochrony danych, wskazując obszar zabezpieczenia, podział zadań oraz wymagania na zabezpieczenia w STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA

Definicje

RODO:
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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).

USTAWA:
Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).

UODO:
Urząd Ochrony Danych Osobowych

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.

Dane szczególnej kategorii:
dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

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,

[1] Pełna nazwa: Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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).

przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

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.

Zbiór danych:
oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

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; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
W odniesieniu do niniejszej Polityki Administratorem jest: STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA, ul. Dolnych Młynów 5, 31-124 Kraków

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

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 jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

Strona trzecia:
oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

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.

Rejestr:
oznacza „Rejestr czynności przetwarzania danych osobowych” (vide art. 30 pkt 1 RODO: Rejestr prowadzony przez Administratora).

Rejestr kategorii:

oznacza „Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora" (vide art. 30 pkt 2 RODO: Rejestr prowadzony przez podmiot przetwarzający).

Osoba:
osoba, której dane dotyczą.

Obowiązek informacyjny:
Informowanie osób, których dane dotyczą o przetwarzaniu ich danych osobowych (vide art. 13 i 14 RODO).

Firma: STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA, ul. Dolnych Młynów 5, 31-124 Kraków

OBSZAR ZABEZPIECZENIA

Zarządzanie ochroną danych osobowych w STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA polega na stosowaniu reguł i podejmowaniu działań w następujących zakresach:

§ 1. Legalność przetwarzania danych, tj.:

1.1. Przetwarzanie danych musi zachodzić zgodnie z zasadami:

1.1.1. **zgodności** przetwarzania z przepisami prawa, w sposób rzetelny i przejrzysty;

1.1.1.1. „zasada legalizmu" daje zamknięty katalog sytuacji, w których można przetwarzać dane osobowe (vide art. 6 RODO) – należy ustalić przesłankę prawną na podstawie której przetwarzanie będzie realizowane;

1.1.1.2. STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA spełnia względem osób, których dane będą przetwarzane wymóg realizacji obowiązku informacyjnego (vide art. 13 i 14 RODO) w sposób zwięzły przejrzysty, zrozumiały i w łatwo dostępnej formie (vide art. 12 RODO);

1.1.2. **ograniczenia celu** *(tj. przetwarzane tylko dla celu, dla którego dane były zbierane)*;

1.1.3. **minimalizacji zakresu** danych do niezbędnego względem celu przetwarzania oraz ograniczeniu dostępu do danych do niezbędnego personelu;

1.1.4. gwarancji **prawidłowość** danych *(przy wdrożeniu mechanizmów aktualizacji i usuwania błędnych danych)*;

1.1.5. ograniczenia przechowywania danych *(pozwalających na identyfikację Osoby)* do niezbędnego minimum;

1.1.6. zapewnienia **poufności i integralności**[2] przetwarzanych danych;

1.1.7. zapewnienia **rozliczalności** przetwarzania, tj. zapewnienia dowodu, że przetwarzanie na każdym etapie jest zgodne z prawem.

1.2. W przypadku, kiedy przetwarzanie wiąże się z udostępnieniem danych podmiotowi przetwarzającemu, STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA będzie zawierać **umowę powierzenia** przetwarzania z podmiotem przetwarzającym (podwykonawcą, który w związku z świadczoną usługą będzie miał dostęp do danych osobowych, których Administratorem jest STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA

1.3. W przypadku, kiedy przetwarzanie wiąże się z przekazywaniem danych osobowych do **państw trzecich**, STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA będzie

[2] tj. w sposób gwarantujący, iż dane nie będą w sposób nieuprawniony zmodyfikowane lub zniszczone.

stosować odpowiednie mechanizmy prawne *(np. w oparciu o: decyzję KE stwierdzająca odpowiedni stopień ochrony; wiążące reguły korporacyjne; standardowe klauzule ochrony danych osobowych; zatwierdzone kodeksy postępowania; zgodę właściciela danych(zgoda na ryzyko); niezbędność ze względu na: {1}wykonanie umowy zawartej z Osobą, {2}ochronę żywotnych interesów Osoby, {3}posiadane roszczenia)*.

§ 2. Świadomość zadań związanych z wymaganiami przetwarzania danych osobowych, tj.:

2.1. Każda z osób mających dostęp do danych osobowych, których Administratorem jest STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA musi posiadać **wiedzę** z zakresu ochrony danych osobowych;

2.2. Administrator **buduje świadomość** zagrożeń i odpowiedzialności za przetwarzanie danych osobowych poprzez śledzenie aktualnych wytycznych i standardów dotyczących stosowania RODO i Ustawy, oraz uwzględnianie tej wiedzy w codziennych zadaniach związanych z przetwarzaniem danych osobowych;

2.3. STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA wprowadza do powszechnego stosowania zasady {1}**uwzględniania ochrony danych w fazie projektowania** oraz {2}**domyślnej ochrony danych**;

2.3.1. Każde podejmowane w STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA działanie (np. wdrożenie nowego systemu informatycznego; wdrożenie nowego procesu, czy zawarcie umowy) będzie poprzedzone analizą możliwości realizacji przedsięwzięcia oraz ustalenia warunków, przy których możliwe jest zapewnienie należytego zabezpieczenia przetwarzania..

§ 3. Stosowanie adekwatnych do potrzeb przetwarzania zabezpieczeń, tj.:

3.1. Właściciel STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA nie wyznaczył Inspektora Ochrony Danych (bowiem nie przetwarza szczególnych kategorii danych) i wszelkie działania związane z ochroną danych osobowych wykonuje osobiście, w szczególności zadania kontrolne, zapewnienie szkoleń, jak też związanych z pełnieniem funkcji tzw. punktu kontaktowego.

3.2. Administrator **zinwentaryzował procesy w których przetwarza dane osobowe oraz zidentyfikował kontekst przetwarzania** (miejsce, sposób tradycyjny/elektroniczny, przetwarzanie we własnym zakresie/ powierzenie przetwarzania – w przypadku powierzenia: określił warunki umowy powierzenia). Wynik tych działań zawiera załącznik nr 1 do niniejszej Polityki.

3.2.1. Administrator określił i wdrożył do stosowania **zabezpieczenia organizacyjne, techniczne oraz informatyczne** określone w załączniku nr 1 do niniejszej Polityki, w którym określono: kto i w jakim zakresie ma dostęp do danych osobowych, gdzie są przetwarzane dane osobowe.

§ 4. Wypełnianie obowiązków względem UODO, tj.:

4.1. W STUDIO MŁYN MATULSKA I WSPÓLNICY SPÓŁKA JAWNA wdrożono do stosowania **zasady postępowania ze zdarzeniami** związanymi z naruszeniem bezpieczeństwa danych osobowych, oraz zgłaszania tych zdarzeń do UODO, które polega na tym, iż:

4.1.1. Każdy z pracowników/współpracowników bezzwłocznie (nie później jednak niż w ciągu 24 godzin od uzyskania informacji) informuje Właściciela Firmy, o zdarzeniach związanych z naruszeniem bezpieczeństwa danych osobowych, podając co najmniej: {a}datę i godzinę zdarzenia; {b}okoliczności naruszenia danych osobowych; {c} kategorię danych i przybliżoną liczbę osób fizycznych, których dotyczy

naruszenie; {d}kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

4.1.2. Właściciel Firmy podejmuje decyzję w zakresie kwalifikacji zdarzenia, podjęcia działań naprawczych a w przypadku tego wymagającym, zgłoszenia sprawy do UODO w terminie do 72 godzin od stwierdzenia naruszenia.

4.1.3. Właściciel Firmy gromadzi dokumentację ww. działań zawierającą zgłoszenie, decyzję w sprawie obsługi zgłoszenia, opis postępowania, korespondencję z UODO.

4.2. Przypisano zadania związane z konsultacjami i wdrożeniem ustaleń, które prowadzi się z UODO w ramach konsultacji związanych z ustaleniem sposobu postępowania z wysokim ryzykiem przetwarzania.

§ 5. Wypełnianie obowiązków względem osób, których dane są przetwarzane, tj:

5.1. Właściciel Firmy opracował treści obowiązków informacyjnych oraz ustalenia dotyczące sposobu ich stosowania (wzory, w celu udokumentowania i sprawnego stosowania włącza się do dokumentacji Bezpieczeństwa).

5.2. Właściciel Firmy ustalił i wdrożył do stosowania zasady obsługi praw osób, których dane dotyczą w zakresie w procedurze „Wykonanie obowiązków względem osoby której dane dotyczą":

5.2.1. prawa do cofnięcia zgody na przetwarzanie danych osobowych;
5.2.2. prawa dostępu do danych (w tym możliwości uzyskania kopii);
5.2.3. prawa do sprostowania;
5.2.4. prawa do uzupełnienia danych;
5.2.5. prawa do usunięcia danych;
5.2.6. prawa do ograniczenia przetwarzania;
5.2.7. prawa do przenoszenia danych;
5.2.8. prawa do sprzeciwu w szczególnej sytuacji;
5.2.9. prawa do sprzeciwu względem działań marketingowych;
5.2.10. prawa do ludzkiej interwencji przy automatycznym przetwarzaniu.

§ 6. Przegląd i aktualizacja Polityki Bezpieczeństwa Danych Osobowych

6.1. Wdrożona Dokumentacja Bezpieczeństwa (DB) oraz procedury wykonawcze podlegają okresowym (co rocznym) przeglądom pod kątem zgodności z wymaganiami prawnymi w kontekście zmian prawnych i innych zmian wynikających z otoczenia.

……
Podpis Właściciela Firmy, data