Polityka ochrony danych osobowych
w firmie EstateValue Mateusz Piętak

Celem Polityki ochrony danych osobowych, zwanej dalej **Polityką**, jest wprowadzenie i utrzymanie wymaganej przez przepisy rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 r. oraz ustawy o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000) właściwej ochrony danych osobowych w związku z przetwarzaniem danych osobowych w firmie EstateValue Mateusz Piętak z siedzibą we Wrocławiu przy ulicy Zakładowej 7G lokal nr 24.

Niniejsza Polityka dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny jak i w systemach informatycznych. Dotyczy istniejących oraz przetwarzanych w przyszłości zbiorów danych osobowych. W skład obszaru przetwarzania danych osobowych w EstateValue Mateusz Piętak wchodzi lokal nr 24 przy ulicy Zakładowej 7G we Wrocławiu, zwany dalej **siedzibą**.

Administratorem danych osobowych jest EstateValue Mateusz Piętak zwany dalej **Administratorem**.

Określenia użyte w Polityce ochrony danych osobowych oznaczają:

dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, 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 – operacja 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,

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),

państwo trzecie – państwo nienależące do Europejskiego Obszaru Gospodarczego,

polityka – niniejsza Polityka ochrony danych osobowych,

1. Zasady przetwarzania danych osobowych

Dane osobowe przetwarzane są w zbiorach z wykorzystaniem systemów informatycznych lub w formie papierowej. Zbiory danych osobowych są zlokalizowane w siedzibie firmy.

Pozyskiwanie informacji o użytkownikach odbywa się przez stronę internetową https://mateuszpietak.pl poprzez:
a) dobrowolnie wprowadzone w formularzach informacje,
b) zapisywanie w urządzeniach końcowych pliki cookie (tzw. "ciasteczka").

Administrator danych przetwarza dane osobowe w postaci imienia i nazwiska oraz adresu e-mail, które są zbierane za pomocą formularza kontaktowego, a przetwarzane są w celu udzielenia odpowiedzi na zadane poprzez formularz pytanie oraz kontaktu z osobą składająca zapytanie. Wszelkie inne dane osobowe jakie osoba zawrze w zapytaniu będą przetwarzane tylko na potrzeby zapytania.

Dodatkowo dane pozyskiwane są każdorazowo podczas zawierania umowy w formie pisemnej o wykonanie usługi.

Potwierdzenie spełniania obowiązków informacyjnych przez administratora danych stanowią klauzule informacyjne przekazywane osobom, których dane są przetwarzane. W przypadku klientów przekazywane im są w momencie zawierania umowy w formie pisemnej.

Dane będą przetwarzane nie dłużej, niż jest to przewidziane w przepisach prawa.

2. Ogóle zasady bezpieczeństwa danych osobowych

a) Dostęp do danych osobowych ma wyłącznie administrator.

b) Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności administratora, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.

c) Administrator przechowujący dane osobowe zobowiązany jest do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.

d) Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych.

e) Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.

f) W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej administrator zobowiązany jest do stosowania zasady tzw. czystego biurka, która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym.

g) Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.

h) Klucze do szafek, w których znajdują się dane osobowe nie mogą być pozostawione w zamku w drzwiach. Administrator zobowiązany jest do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.

i) Komputer przenośny zawierający dane osobowe powinien być zabezpieczony hasłem, które uniemożliwi dostęp osobom trzecim do tych danych.

.

3. Analiza ryzyka

Administrator danych prowadzi analizę ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń. Analiza prowadzona jest w przypadku zaistnienia zagrożenia oraz cyklicznie raz do roku.

4. Rejestr czynności przetwarzania

Administrator danych prowadzi rejestr czynności przetwarzania. W rejestrze tym zamieszcza się:

a) imię i nazwisko oraz dane kontaktowe administratora,
b) cele przetwarzania,
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
e) gdy ma to zastosowanie, informacje na temat przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentację odpowiednich zabezpieczeń,

f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

5. Procedura postępowania z incydentami

Administrator danych wprowadza do stosowania procedurę postępowania z incydentami naruszenia ochrony danych osobowych. Celem tej procedury jest wypełnienie obowiązku wynikającego z art. 33 RODO. Procedura określa sposób definiowania incydentów zagrażających bezpieczeństwu danych osobowych oraz sposób reagowania na nie, a także procedurę wprowadzenia działań naprawczych.

Powiadomienia wymagają:

- niewłaściwe zabezpieczenie sprzętu elektronicznego, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych, udostępnienie haseł osobom postronnym,
- niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
- nieprzestrzeganie zasad ochrony danych osobowych (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek, przyklejanie kartek z hasłami w szufladach),
- ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
- dokumentacja zawierająca dane osobowe niszczona bez użycia niszczarki,
- otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
- złe ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
- wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz jednostki bez upoważnienia administratora danych,
- awarie serwera, komputerów, twardych dysków, oprogramowania,
- udostępnienie danych osobowych osobom nieupoważnionym,
- telefoniczne próby wyłudzenia danych osobowych,
- kradzież, zagubienie komputerów lub CD, twardych dysków, pen-drive z danymi osobowymi,
- e-maile nakłaniające do ujawnienia identyfikatora lub hasła,
- zainfekowanie komputerów wirusem lub inne błędne zachowanie komputerów,
- zdarzenia losowe (pożar obiektu, zalanie wodą, utrata zasilania, utrata łączności),
- włamanie do systemu informatycznego lub pomieszczeń,
- kradzież danych/sprzętu,
- świadome zniszczenie dokumentów.

Należy dokumentować wystąpienie incydentu, jego skutki oraz podjęte działania naprawcze i zaradcze. W przypadku gdy incydent skutkuje naruszeniem praw lub wolności osób fizycznych, administrator danych zgłasza je w ciągu 72 godzin Prezesowi Urzędu Ochrony Danych Osobowych oraz gdy istnieje

taki wymóg, powiadamia o tym fakcie osoby, których incydent dotyczył.

6. Uzyskanie informacji o przetwarzaniu danych osobowych

Kontakt z administratorem w sprawach związanych z ochroną danych osobowych możliwy jest za pośrednictwem poczty e-mail pod adresem: kontak@estatevalue.pl.