Polityka Ochrony Danych Osobowych

w biurze nieruchomości Hampton Home Beata Wróblewska NIP: 8261338860

Niniejsza polityka jest polityką ochrony danych osobowych w rozumieniu rozporządzenia 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) (dalej: RODO). Polityka Ochrony Danych Osobowych opisuje zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań RODO i ma na celu jak najpełniejsze wdrożenie oraz realizację praw i obowiązków wynikających z RODO.

Na politykę składają się:
A. ogólne zasady ochrony danych przez Administratora
B. szczegółowe procedury i instrukcje w formie załączników

Administrator:

Nazwa: Hampton Home Beata Wróblewska

Adres: ul. Przejazd 4lok.U4, 02-654 Warszawa

Dane kontaktowe:

Beata Wróblewska, telefon: 505-612-305
Email: b.wroblewska@hamptonhome.pl

A. Część ogólna.

Wyjaśnienie pojęć i skrótów

Polityka Ochrony Danych Osobowych (Polityka ODO) - oznacza niniejszą Politykę ochrony danych osobowych, wdrożoną przez Administratora

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 - 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;

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

Podmiot przetwarzający (Procesor) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
Przetwarzanie danych osobowych 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;

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania
Anonimizacja – działanie przeprowadzone na danych osobowych, w wyniku którego dane nieodwracalnie tracą właściwości identyfikujące i przestraja być danymi osobowymi;
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 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.

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;

Szczególne kategorie danych osobowych (dane wrażliwe) – dane osobowe, które 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 – 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;

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;

1. Ogólne zasady ochrony danych stosowane przez Administratora

ADO przetwarza dane osobowe zgodnie z zasadami określonymi w art. 5 RODO, tj. stosuje na każdym etapie przetwarzania zasady:

a) Zgodności z prawem
b) Rzetelności
c) Przejrzystości
d) Ograniczenia celu
e) Minimalizacji danych
f) Prawidłowości

g) Ograniczenia przetwarzania
h) Rozliczalności

Wszystkie działania ADO w zakresie danych osobowych nakierowane są na ochronę praw osób, których dane ADO przetwarza, w tym także na etapie projektowania i planowania działań gospodarczych.

2. System ODO wdrożony przez Administratora

System ODO oparty jest na następujących filarach:

I. Inwentaryzacja danych – Administrator na bieżąco zbiera informacje o tym, ile danych przetwarza, o procesach przetwarzania, o źródłach danych osobowych, o ich przepływach w strukturze Administratora. W szczególności ADO identyfikuje: dane wrażliwe, dane dzieci, przypadki profilowania, kwestie współadministrowania, przypadki powierzenia przetwarzania. Dane i czynności przetwarzania ADO ewidencjonuje za pomocą Rejestru czynności przetwarzania, który jest narzędziem rozliczalności. Rejestr czynności przetwarzania (RCP) stanowi załącznik nr 1 do polityki ODO. Jest formą dokumentowania czynności przetwarzania, służy mapowaniu procesów przetwarzania, pomaga w opisaniu przepływów danych. W RCP ADO inwentaryzuje i monitoruje procesy przetwarzania. RCP jest na bieżąco uaktualniany w przypadku zidentyfikowania nowych czynności i procesów przetwarzania. RCP zawiera pozycje obowiązkowe określone w art. 30 RODO oraz pozycje dodatkowe, które ułatwiają lepszą identyfikację czynności przetwarzania i ich pełniejszy opis.

II. Wszelkie przetwarzanie danych ADO opiera na podstawach prawnych określonych w RODO, szczególności w art. 6 RODO, realizując zasadę legalności. Przetwarzanie jest możliwe tylko po wykazaniu, że opiera się na jednej z podstaw:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych.
W tym zakresie ADO opiera działania na zasadzie przejrzystości, informuje o podstawach przetwarzania, ewidencjonuje zgody na przetwarzanie, opiera się na sprawdzonych klauzulach zgód (zgoda dobrowolna, konkretna, świadoma i jednoznaczna). Wzory standardowych klauzul zgód stosowanych przez ADO stanowią **załącznik nr 2.**

III. ADO zapewnia realizację praw osób, których dane przetwarza, w szczególności poprzez realizację obowiązku informacyjnego z art. 13 i 14 RODO. ADO przekazuje wszelkie informacje w sposób przejrzysty, prostym i zrozumiałym językiem. ADO realizuje obowiązek informacyjny w przypadku zbierania danych od osoby, której dane dotyczą, jak i od podmiotów trzecich. W tym celu ADO posiada opracowane wzory standardowych klauzul informacyjnych, które stanowią **załącznik nr 3.**

IV. ADO zapewnia sprawną obsługę żądań kierowanych do niego przez osoby, których dane przetwarza (zwłaszcza przewidzianych w art. 15-21 RODO). ADO opisał i wdrożył procedury odpowiedzi na żądania, tryb ich uwzględnienia lub odmowy realizacji żądania. W szczególności dotyczy to realizacji prawa:

a) dostępu do danych
b) otrzymania kopii danych
c) sprostowania danych
d) uzupełnienia danych
e) usunięcia danych
f) ograniczenia przetwarzania
g) przenoszenia danych
h) oraz realizacji sprzeciwu.

Przykładowe procedury stanowią **załącznik nr 4.**

V. ADO wdraża zasadę minimalizacji danych poprzez reglamentację i zarządzanie dostępem do danych oraz poprzez retencję danych (ograniczenie czasowe przetwarzania). W szczególności dane przetwarzane są przez podmioty inne niż ADO tylko na podstawie upoważnienia lub powierzenia i na wyraźne polecenie ADO. Upoważnienia udzielane są na piśmie przez ADO lub przez osobę umocowaną przez ADO (wzór pełnomocnictwa stanowi **załącznik nr 5**). Upoważnienia dostosowane są do indywidualnej sytuacji, określają zakres przedmiotowy i czasowy przetwarzania przez upoważnionego. Wzory upoważnień stanowią **załącznik nr 6**. ADO ewidencjonuje upoważnienia, ich zakres, okres ważności, powiązane z upoważnieniem identyfikatory w formie rejestru upoważnień (**załącznik nr 7**). ADO zapewnia także zachowanie poufności przez osoby upoważnione, co do danych osobowych, jak i sposobów i zabezpieczenia poprzez odebranie od każdego upoważnionego oświadczenia o poufności danych (**załącznik nr 8**). ADO posiada procedury wyboru, weryfikacji i oceny podmiotów przetwarzających, którym powierza przetwarzanie danych. Powierzenie przetwarzania danych osobowych następuje w formie umowy pisemnej lub elektronicznej. ADO dokonuje wyboru tylko takiego podmiotu przetwarzającego, który gwarantuje bezpieczeństwo danych, wdrożył stosowne środki organizacyjne i techniczne ochrony danych. ADO ewidencjonuje wszystkie przypadki powierzenia w rejestrze umów powierzenia, który stanowi załącznik nr 9 do niniejszej polityki. Rejestr stanowi instrument rozliczalności, pozwala ustalić, przetwarzanie jakich danych, w jakim celu , na jaki czas zostało powierzone przez ADO.

VI. ADO zapewnia optymalny poziom ochrony i bezpieczeństwa danych. System bezpieczeństwa danych oparty jest na stale aktualizowanej analizie ryzyka, dostosowaniu środków ochrony do wyników analizy ryzyka, na wdrożeniu i utrzymaniu odpowiednich środków organizacyjnych i technicznych. ADO oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Opis zastosowanych przez ADO środków organizacyjnych i technicznych znajduje się w Instrukcji Bezpieczeństwa (**załącznik nr 10**). Instrukcja opisuje zabezpieczenia fizyczne obszaru przetwarzania danych (pomieszczenia biurowe), jak i zabezpieczenia systemu informatycznego (m.in. procedura nadawania uprawnień, zarządzania hasłami). ADO w szczególności dąży do zapewnienia:

a) zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
b) zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

Środkami umożliwiającymi osiągnięcie powyższych celów są m.in.:
regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

VII. ADO posiada oraz wdrożył procedury identyfikacji i zgłaszania naruszeń ochrony danych, w szczególności tryb postępowania opisany w art. 33 i 34 RODO **(załącznik nr 11**). W szczególności ADO prowadzi stały monitoring czynności przetwarzania, określa czy zastosowane środki bezpieczeństwa są adekwatne do ryzyk, a w razie wystąpienia naruszenia dokonuje zgłoszeń w czasie nie dłuższym niż 72 godziny oraz podejmuje niezbędne środki zaradcze w celu minimalizacji ryzyka naruszeń praw osób, których dane zostały naruszone. Kwestie naruszeń, wzajemnego zawiadamia i reagowania są także uwzględnione w umowach powierzenia zawieranych przez ADO. ADO dokumentuje w rejestrze naruszeń (**załącznik nr 12)** wszelkie naruszenia ochrony danych, w tym okoliczności naruszenia, jego skutki i podjęte działania zaradcze.

VIII. W celu zapewnienia spójnego i skutecznego systemu ochrony danych osobowych ADO na bieżąco monitoruje procesy przetwarzania i aktualizuje zabezpieczenia. ADO przeprowadza regularne (nie rzadziej niż raz na pół roku) audyty wewnętrzne systemu ochrony danych osobowych. ADO dba także o aktualizację wiedzy z zakresu ochrony danych poprzez szkolenia wewnętrzne lub zewnętrzne dla ADO i jego personelu. Plan audytów i plan szkoleń stanowią **załącznik nr 13**.

IX. ADO eliminuje przypadki eksportu danych do państw trzecich a także przetwarzania transgranicznego.

X. ADO po przeprowadzonej analizie nie powołał Inspektora Ochrony Danych Osobowych (**załącznik nr 14**)

Załączniki do niniejszej Polityki ochrony danych osobowych dostępne w biurze Hampton Home.