POLITYKA BEZPIECZEŃSTWA RODO

DILBUD.PL spółka z ograniczoną odpowiedzialnością z siedzibą w Witaszycach

Niniejsza polityka bezpieczeństwa, zwana dalej: „polityką", została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w DILBUD.PL sp. z o.o. , w tym z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.),dalej: RODO.

Definicje:

1. Administrator danych: DILBUD.PL spółka z ograniczoną odpowiedzialnością z siedzibą w Witaszycach, ul. Kolejowa 10A, 63-230 Witaszyce, zarejestrowana przez Sąd Rejonowy Poznań – Nowe Miasto i Wilda w Poznaniu, IX Wydział Gospodarczy Krajowego Rejestru Sądowego, KRS 0001071567, NIP 6172228117, REGON 527043062, adres poczty e-mail: (sklep@dilbud.pl(zwana dalej: „Administratorem Danych" lub „Spółką").
2. Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
3. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych.
4. Użytkownik – osoba upoważniona przez administratora danych do przetwarzania danych osobowych.
5. Zbiór danych – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów.
6. Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych.
7. Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (użytkownika) w razie przetwarzania danych osobowych w takim systemie.
8. Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (użytkownikowi) w razie przetwarzania danych osobowych w takim systemie.
9. Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (użytkownika).

I. Postanowienia ogólne

1. Polityka dotyczy wszystkich danych osobowych przetwarzanych
w Spółce, niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej
w siedzibie Administratora Danych.
3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się
z jej treścią.
4. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne
i rozwiązania organizacyjne,
b) kontrolę i nadzór nad Przetwarzaniem danych osobowych,
c) monitorowanie zastosowanych środków ochrony.
5. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m. in. działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
6. Administrator Danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.
II. Dane osobowe przetwarzane u Administratora Danych
1. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych.
2. Administrator Danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.
3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
4. Administrator Danych prowadzi rejestr czynności przetwarzania.
III. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem
1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie
z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką Bezpieczeństwa, Instrukcją Zarządzania Systemem Informatycznym, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych w Spółce.
2. Wszystkie dane osobowe w przedsiębiorstwie są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
a) W każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych.
b) Dane są przetwarzane są rzetelnie i w sposób przejrzysty.
c) Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane

dalej w sposób niezgodny z tymi celami.
d) Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych.
e) Dane osobowe są prawidłowe i w razie potrzeby uaktualniane.
f) Czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane zgodnie z obowiązującymi przepisami.
g) Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO.
h) Dane są zabezpieczone przed naruszeniami zasad ich ochrony.
3. Administrator Danych nie przekazuje osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej (art. 14 ust. 5 pkt d RODO).
4. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:
a) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach;
b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
d) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;
e) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych;
g) naruszenie praw osób, których dane są przetwarzane.
5. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych Użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych,
6. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy dopilnowanie, by:
a) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków,
b) każdy z przetwarzających Dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych”
c) każdy pracownik zobowiązał się do zachowania danych osobowych przetwarzanych w przedsiębiorstwie w tajemnicy. „Oświadczenie i zobowiązanie osoby przetwarzającej dane osobowe do zachowania tajemnicy” stanowi element „Upoważnienia do przetwarzania danych osobowych”.
7. Pracownicy zobowiązani są do:
a) ścisłego przestrzegania zakresu nadanego upoważnienia;

b) przetwarzania i ochrony danych osobowych zgodnie z przepisami;
c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.
IV. Obszar przetwarzania danych osobowych
1. Obszar, w którym przetwarzane są Dane osobowe na terenie Spółki obejmuje pomieszczenia biurowe i handlowe przedsiębiorstwa zlokalizowane w Witaszycach przy ul. Kolejowej 10 A, a także w oddziałach Spółki w przypadku ich występowania.
2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.
V. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozłączalności przetwarzanych danych
1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozłączalności i ciągłości Przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów
i kategorii danych, Środki obejmują:
a) Ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej.
b) Zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w pkt IV powyżej na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich.
c) Wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów.
d) Wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe.
e) Ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall.
f) Wykonywanie kopii awaryjnych danych na macierzach dyskowych i niekasowalnych nośnikach danych tj płyta DVD Blu-Ray
g) Ochronę sprzętu komputerowego wykorzystywanego u administratora przed złośliwym oprogramowaniem.
h) Zabezpieczenie dostępu do urządzeń przedsiębiorstwa przy pomocy haseł dostępu.
i) Wykorzystanie szyfrowania danych przy ich transmisji.
VI. Naruszenia zasad ochrony danych osobowych
1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator Danych dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia

o incydencie także osobę, której dane dotyczą.

VII. Powierzenie przetwarzania danych osobowych

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.

2. Przed powierzeniem przetwarzania danych osobowych Administrator Danych w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.

3. Dane osobowe Klienta przekazywane są dostawcom usług, z których korzysta Administrator Danych przy prowadzeniu Sklepu Internetowego. Dostawcy usług, którym przekazywane są dane osobowe, w zależności od uzgodnień umownych i okoliczności, albo podlegają poleceniom Administratora Danych co do celów i sposobów przetwarzania tych danych (podmioty przetwarzające) albo samodzielnie określają cele i sposoby ich przetwarzania (administratorzy).

4. Podmioty przetwarzające. Administrator Danych korzysta z dostawców, którzy przetwarzają dane osobowe wyłącznie na jego polecenie. Należą do nich m.in. dostawcy świadczący usługę hostingu, usługi księgowe, dostarczający systemy do marketingu, systemy do analizy ruchu w Sklepie Internetowym, systemy do analizy skuteczności kampanii marketingowych.

5. Inni administratorzy. Administrator Danych korzysta z dostawców, którzy nie działają wyłącznie na polecenie i sami ustalają cele i sposoby wykorzystania danych osobowych Klientów. Świadczą oni usługi płatności elektronicznych oraz bankowe.

6. Lokalizacja. Dostawcy usług mają siedziby w Polsce i w innych krajach Europejskiego Obszaru Gospodarczego (EOG).

VIII. Przekazywanie danych do państwa trzeciego

1. Administrator Danych Osobowych nie będzie przekazywał danych osobowych do państwa trzeciego poza obręb Europejskiego Obszaru Gospodarczego poza sytuacjami, w których następuje to na wniosek osoby, której dane dotyczą.

IX. Postanowienia końcowe

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, Przepisów o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych objętych tajemnicą zawodową.

Podmioty upoważnione przez Spółkę do przetwarzania podanych przez Klientów danych osobowych:

– InPost spółką z ograniczoną odpowiedzialnością z siedzibą w Krakowie, przy ul. Pana Tadeusza 4, 30-727 KRAKÓW, KRS: 0000543759, NIP: 6793108059, REGON: 360781085

– Autopay S.A. z siedzibą w Sopocie, ul. Powstańców Warszawy 6, 81-718 Sopot, zarejestrowana w Sądzie Rejonowym Gdańsk-Północ VIII Wydział Gospodarczy KRS pod nr 0000320590, NIP 585-13-51-185, REGON 191781561