POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

spółki Firma Meblowa Krawczyk spółka jawna z siedzibą w Ostrowie Wielkopolskim (63-400) przy ul. Sądowej 7, KRS: 0000099293 (akta rejestrowe przechowywane przez Sąd Rejonowy Poznań - Nowe Miasto i Wilda w Poznaniu, Wydział IX Gospodarczy Krajowego Rejestru Sądowego), NIP: 6220106117, REGON: 250018029

(dalej jako „Podmiot" lub „Administrator")

z dnia 11 maja 2019 r.

Rozdział 1
POSTANOWIENIA OGÓLNE

[Podstawa prawna]

§ 1

1. Podstawę prawną niniejszej Polityki stanowią obowiązujące przepisy prawa powszechnie obowiązującego, a w szczególności:
   a. 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 (dalej: RODO),
   b. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. (Dz. U. z 2018 r., poz. 1000) (dalej: Ustawa),
   c. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U 2004 r. nr 100 poz.1024), zwane dalej Rozporządzeniem,

[Zakres przedmiotowy Polityki]

§ 2

Polityka określa:

a) zasady postępowania przy przetwarzaniu danych osobowych w Podmiocie,
b) zasady umożliwiające przetwarzanie danych osobowych (podstawy przetwarzania),
c) zasady ochrony przetwarzanych danych osobowych.

[Przetwarzanie danych]

§ 3

1. **Przetwarzanie danych** - 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, a zwłaszcza te, które wykonuje się w systemach informatycznych.

2. Przez **dane osobowe** - rozumie się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
3. **Administrator Ochrony Danych Osobowych** oznacza spółkę Firma Meblowa Krawczyk spółka jawna z siedzibą w Ostrowie Wielkopolskim (63-400) przy ul. Sądowej 7, KRS: 0000099293 (akta rejestrowe przechowywane przez Sąd Rejonowy Poznań - Nowe Miasto i Wilda w Poznaniu, Wydział IX Gospodarczy Krajowego Rejestru Sądowego), NIP: 6220106117, REGON: 250018029, która przetwarza dane osobowe, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z ochroną danych osobowych. (dalej jako „**ADO**").
4. **Inspektor Ochrony Danych Osobowych** może być wyznaczony przez ADO i zapewnia przestrzeganie przepisów o ochronie danych osobowych u ADO (dalej jako „**IODO**").
5. **Podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.
6. **Odbiorca** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią (podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający).
7. **Osoba upoważniona do przetwarzania danych osobowych** - dysponuje upoważnieniem do przetwarzania danych osobowych, obowiązana jest zachować w tajemnicy dane osobowe, które przetwarza oraz sposoby ich zabezpieczenia.

[Podstawy przetwarzania danych osobowych]

§ 4

1. Administrator przetwarza dane osobowe jeżeli:
   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 wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.

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

[Prawa osób których dane są przetwarzane]

§ 5

1. Osoba, której dane przetwarza ADO, ma prawo:
   a) do uzyskania od ADO potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz informacji min. o celach przetwarzania, odbiorcach, którym dane osobowe zostały lub zostaną ujawnione (Prawo dostępu),
   b) żądania od ADO niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe (Prawo do sprostowania danych),
   c) żądania od ADO niezwłocznego usunięcia dotyczących jej danych osobowych (prawo do bycia zapomnianym),
   d) żądania od ADO ograniczenia przetwarzania (Prawo do ograniczenia przetwarzania),
   e) w zależności od podstawy przetwarzania - otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła ADO oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez ADO bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. (Prawo do przenoszenia danych),
   f) w zależności od podstawy przetwarzania - w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych (Prawo do sprzeciwu).

Obowiązek ADO względem osób których dane są przetwarzane

§ 6

ADO ma obowiązek względem osób których dane osobowe przetwarza do:

a) podania tożsamości ADO, danych kontaktowych oraz tożsamości i danych kontaktowych przedstawiciela ADO,
b) podania danych kontaktowych IODO – jeżeli został on wyznaczony,
c) wskazania celów przetwarzania danych osobowych oraz podstawy prawnej przetwarzania,
d) wskazania prawnie uzależnionych interesów realizowanych przez administratora lub przez stronę trzecią,
e) poinformowania o odbiorcach danych osobowych lub o kategoriach odbiorców, jeśli istnieją,
f) przekazania informacji związanych z zamiarem przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

]Przechowywanie danych]

§ 7

Dane osobowe mogą być przechowywane pod warunkiem przestrzegania obowiązujących regulacji prawnych, w szczególności tych wymienionych § 1 niniejszej Polityki:

a) w systemach informatycznych (mogą nim być również pojedyncze komputery),
b) w wersji papierowej tj. w teczkach, skorowidzach, aktach segregatorach.

Rozdział 2
ORGANIZACJA ZABEZPIECZANIA DANYCH OSOBOWYCH

§ 8

1. ADO wyznaczy IODO, jeżeli wystąpi jedna z przesłanek o, której mowa w art. 37 ust. 1. RODO lub uzna, że zachodzi taka potrzeba organizacyjna.
2. Wyznaczony IODO ma następujące zadania:
    a. informowanie ADO, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO polskiej Ustawy oraz innych przepisów o ochronie danych osobowych i doradzanie im w tej sprawie,
    b. monitorowanie przestrzegania przepisów RODO, innych przepisów o ochronie danych oraz polityk ADO lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość,

szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,

c. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO,
d. współpraca z organem nadzorczym,
e. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
f. IODO wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

[Osoby upoważnione do przetwarzania danych]

§ 9

1. Dane osobowe w Podmiocie mogą przetwarzać jedynie osoby posiadające pisemne upoważnienie nadane przez ADO. W upoważnieniu należy określić do jakich zbiorów danych ma dostęp dana osoba (wzór upoważnienia stanowi Załącznik do niniejszej Polityki).
2. IODO lub Osoba wyznaczona do prowadzenia rejestru upoważnień dokona weryfikacji upoważnienia w przypadku zmian osobowych skutkujących koniecznością nadania lub odebrania upoważnienia, o którym mowa w ustępie 1 powyżej. Weryfikacja wydanych upoważnień następuje na koniec każdego roku obrachunkowego.
3. W rejestrze upoważnień (stanowiący Załącznik do niniejszej Polityki) umieszcza się następujące informacje:
    1. Imię i nazwisko osoby upoważnionej do przetwarzania danych,
    2. Zakres upoważnienia do przetwarzania danych,
    3. Identyfikator, jeśli osoba została zarejestrowana w systemie teleinformatycznym,
    4. Datę nadania uprawnień,
    5. Informację o odbytym szkoleniu z zakresu danych osobowych.
4. Każda osoba przetwarzająca dane osobowe w ramach swoich obowiązków służbowych zobowiązana jest do bezwzględnego:
    a) zachowania w tajemnicy danych osobowych, z którymi zapoznał się w związku z pełnieniem obowiązków, zarówno w trakcie zatrudnienia jak i po jego ustaniu;
    b) przestrzegania obowiązujących przepisów prawa i aktów wewnętrznych dotyczących przechowywania, przetwarzania i postępowania z danymi osobowymi, a w szczególności zabezpieczenie wszelkich dokumentów służbowych i innych nośników informacji przed dostępem osób nieupoważnionych.

5. Nieprzestrzeganie regulacji dotyczących ochrony danych osobowych stanowi rażące naruszenie ustalonego porządku i dyscypliny pracy.

[Obowiązek zaznajomienia pracownika z przepisami]

§ 10

1. Tylko i wyłącznie osoby fizyczne (pracownicy, zleceniobiorcy, praktykanci) mogą zostać upoważnione do przetwarzania danych osobowych. Przedsiębiorcy i inne jednostki organizacyjne mogą przetwarzać dane tylko i wyłącznie w oparciu o umowę o powierzeniu przetwarzania, zabezpieczającą interes Podmiotu i gwarantującą realizację przepisów Ustawy.
2. Każda osoba przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych musi zostać zaznajomiona przez wskazane przez Administratora osoby z przepisami dot. ochrony danych osobowych, z uwzględnieniem z przepisów karnych wynikających z Ustawy, oraz z niniejszą Polityką.

[Obowiązki kadry kierowniczej]

§ 11

Do obowiązków kadry kierowniczej należy zrozumienie i zapewnienie świadomości bezpieczeństwa przetwarzania danych osobowych wraz z jego problematyką i wymaganiami. Kadra kierownicza zobowiązana jest do:

a) Podejmowania niezbędnych działań w celu zapewnienia bezpieczeństwa,
b) Podział zadań i obowiązków związanych z organizacją danych osobowych,
c) Wprowadzenia procedur zapewniających odpowiednie przestrzeganie przepisów dotyczących danych osobowych,
d) Poddawania przeglądom Polityki i procedur,
e) Zapewnienia aktualności, adekwatności oraz poprawności przetwarzanych danych,

[Powierzenie przetwarzania]

§12

Administrator może powierzyć przetwarzanie danych innemu podmiotowi wyłącznie na podstawie pisemnej umowy o powierzeniu przetwarzania danych. W umowie tej należy przede wszystkim określić wymagania bezpieczeństwa przetwarzania danych osobowych. Podmiot przetwarzający powinien zostać zobowiązany do podjęcia odpowiednich środków zabezpieczających przekazane mu przez Podmiot dane osobowe.

ROZDZIAŁ 3
PODSTAWOWE ZASADY PRZETWARZANIA DANYCH

[A. Organizacyjne]

§13

1. Dane osobowe mogą przetwarzać jedynie osoby posiadające aktualne upoważnienia, o których mowa w §9 powyżej.
2. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, muszą być każdorazowo zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp osób trzecich.
3. Sprzątanie ww. pomieszczeń odbywa się tylko i wyłącznie w obecności pracownika upoważnionego do przetwarzania danych osobowych.
4. W obszarach przetwarzania danych mogą przebywać jedynie osoby posiadające upoważnienie.
5. Osoby nieupoważnione mogą przebywać w pomieszczeniach przetwarzania danych jedynie w obecności osoby upoważnionej.
6. W pomieszczeniach, w których przetwarzane są dane osobowe, monitory stanowisk dostępu do danych muszą być ustawione w taki sposób, aby uniemożliwić osobom trzecim wgląd w dane.
7. Kartoteki, skorowidze, wydruki, księgi, wykazy oraz inne dokumenty osobowe powinny być tak zabezpieczone (ułożone), aby uniemożliwić w nie wglądu osobom trzecim.
8. Pracownicy są zobowiązani po zakończeniu pracy zabezpieczyć szafy, biurka, komputery itp. oraz wszelkie dokumenty i pieczątki przed dostępem osób nieuprawnionych.
9. Wydawanie zaświadczeń dot. danych osobowych, udzielanie informacji telefonicznych jest dozwolone tylko zgodnie z właściwymi przepisami prawa.
10. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

[B. Analiza ryzyka]

§ 14

Procesy przetwarzania danych osobowych, w tym wykorzystywane systemy i aplikacje powinny być poddawane ocenie ryzyka pod kątem identyfikacji i zagrożeń dla bezpieczeństwa przetwarzania danych osobowych co najmniej raz na rok. Ocena ryzyka powinna zostać również każdorazowo przeprowadzona, w przypadku dużych zmian procesów biznesowych, systemów informatycznych i aplikacji.

[C. Rejestr czynności przetwarzania danych osobowych]

§15

1. ADO i podmiot przetwarzający prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada.
2. W rejestrze tym zamieszcza się wszystkie następujące informacje:
   a) imię i nazwisko lub nazwę oraz dane kontaktowe ADO oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela ADO oraz IODO;
   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, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej;
   f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
   g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

[D. Informatyczno – techniczne]

§16

1. Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, są zabezpieczone przed utratą tych danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej przez wyznaczoną osobę z pionu technicznego.
2. Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, na podstawie zezwolenia Administratora obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem przetwarzania danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, a szczególnie jest zobowiązana:
   a) zabezpieczyć dostęp do komputera hasłem,
   b) zabronić używania komputera osobom nie upoważnionym i uniemożliwić im dostęp do danych osobowych.
3. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do:

   a) **likwidacji** – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie,

b) **przekazania** innemu podmiotowi, nie uprawnionemu do otrzymania danych osobowych – pozbawia się wcześniej zapisu tych danych,

c) **naprawy** – pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej

4. **Kopie awaryjne** należy:

   a) przechowywać w innym pomieszczeniu niż przechowywane są zbiory danych osobowych eksploatowane na bieżąco,
   b) okresowo sprawdzać pod względem ich dalszej przydatności do odtworzenia danych w razie awarii systemu,
   c) bezzwłocznie usuwać po ustaniu ich użyteczności.

5. **Ekrany monitorów** stanowisk dostępu do danych osobowych muszą być automatycznie wyłączane po upływie ustalonego czasu nieaktywności użytkownika oraz zabezpieczane specjalnym hasłem zmienianym jeden raz na miesiąc.
6. System informatyczny musi być wyposażony w **mechanizmy uwierzytelnienia** użytkownika, a także **kontroli dostępu** do tych danych, przy czym:
   a) każdy użytkownik systemu informatycznego, w którym przetwarza się dane osobowe, posiada ustalony, odrębny identyfikator i hasło,
   b) identyfikator wpisuje się wraz z imieniem i nazwiskiem do ewidencji użytkowników oraz rejestruje w systemie informatycznym,
   c) bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła,
   d) hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu,
   e) hasła użytkownika, umożliwiające dostęp do systemu informatycznego, utrzymuje się w tajemnicy, również po upływie ich ważności,
   f) identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z danego systemu informatycznego, unieważnić jej hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.
7. Administrator może powołać Administratora Systemów Informatycznych (dalej jako „**ASI**”) do zarządzania konfiguracją systemów i urządzeń, nadzoru nad prawidłowością procesu nadawania uprawnień w systemie teleinformatycznym, prowadzenia dokumentacji systemowej, bieżącego wykonywania kopii zapasowej, reagowania na awarię sprzętów informatycznych oraz nadzoru nad mechanizmem kontroli dostępu do systemów i aplikacji.

[E. Instrukcja zgłaszania incydentów]

§ 17

1. Administrator zobowiązany jest do wdrożenia Instrukcji zgłaszania incydentów oraz zaznajomienia pracowników i współpracowników z postanowieniami tej Instrukcji.
2. Każda osoba, która posiada informację mogące mieć wpływ na bezpieczeństwo danych osobowych, jest obowiązana niezwłocznie zgłosić ten fakt IODO lub ASI – a w przypadku ich niewyznaczenia, bezpośredniemu przełożonemu oraz głównemu kierownictwu Podmiotu.
3. IODO/ASI lub główne kierownictwo zobowiązane jest do:
   a) Niezwłocznego podjęcia czynności w celu powstrzymania niepożądanych skutków, w tym naruszenia praw i wolności, których dane dotyczą,
   b) Zaniechać dalszych, planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   c) Udokumentować zaistniałe naruszenie,
   d) Wybranie odpowiednich metod postępowania w celu wyeliminowania skutków naruszenia,
   e) W przypadku gdy jest to obowiązkowe – zawiadomienia organu nadzoru o zaistniałym naruszeniu, podjęcie odpowiednich środków w celu eliminacji wystąpienia naruszenia w przyszłości.

ROZDZIAŁ 4
POSTANOWIENIA KOŃCOWE

§ 18

Administrator lub osoba przez niego wyznaczony w tym IODO ma prawo wstępu do pomieszczenia, w którym zlokalizowany jest zarejestrowany zbiór danych w obecności osoby odpowiedzialnej za przetwarzanie danych w danym obszarze i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą oraz niniejszą Polityką , żądać złożenia pisemnych lub ustnych wyjaśnień i wzywać oraz przesłuchiwać osoby w celu ustalenia stanu faktycznego, żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli, żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

§ 19

1. Wszystkie załączniki do niniejszej Polityki stanowią jej integralną część .
2. Administrator zobowiązany jest do aktualizowania postanowień Polityki.

Niniejsza Polityka Bezpieczeństwa Danych Osobowych wchodzi w życie z dniem 11 maja 2019 r.