PROCEDURA RODO

DOTYCZĄCA

OHRONY DANYCH OSOBOWYCH PRZETWARZANYCH

W

Firmie Handlowo-Usługowej "MAJK" S.C. ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ

PRZEZ OSOBY UPOWAŻNIONE

I

Upoważnienia do przetwarzania danych osobowych

1. Przetwarzaniem Danych Osobowych jest każda czynność dokonywana na danych osobowych, w tym ich posiadanie, przechowywanie, pozyskiwanie, usuwanie.
2. Do przetwarzania Danych Osobowych w Firmie Handlowo-Usługowej "MAJK" S.C. ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ, mogą zostać dopuszczone wyłącznie osoby posiadające stosowne upoważnienie.
3. Upoważnienia do przetwarzania danych osobowych udzielają wspólnicy spółki cywilnej.
4. Upoważnienia do przetwarzania Danych Osobowych udziela się w odrębnym dokumencie wydanym papierowo.
5. Upoważnienie do przetwarzania Danych Osobowych szczególnych kategorii wydają wspólnicy spółki w formie pisemnej oddzielnie od ogólnego upoważnienia do przetwarzania Danych Osobowych.
6. Jeżeli w toku wykonywania pracy Osoba Upoważniona będzie przetwarzać Dane Osobowe w zakresie niewynikającym z poprzednio udzielonego upoważnienia, Administrator nadaje tej osobie upoważnienie szczególne, dedykowane tym dodatkowym obowiązkom. Upoważnienie szczególne może być stałe lub czasowe, w zależności od skonkretyzowanych potrzeb Osoby Upoważnionej.
7. Administrator odpowiada za nadzór nad dostępem do Danych Osobowych, pilnując, aby wszystkie osoby przetwarzające dane osobowe posiadały stosowne upoważnienie.
8. W Firmie Handlowo-Usługowej "MAJK" S.C. ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ prowadzony jest rejestr osób upoważnionych do przetwarzania Danych Osobowych. Do rejestru wpisuje się każdą osobę upoważnioną, niezależnie od formy i czasu posiadanego upoważnienia.
9. Administrator jest obowiązany do niezwłocznego odbioru upoważnienia pracownikowi, który zakończył pracę lub zaprzestał przetwarzania Danych Osobowych objętych dotychczasowym upoważnieniem.

II

Udostępnianie Danych Osobowych

1. Udostępnienie Danych Osobowych innym podmiotom lub osobom jest dozwolone wyłącznie po zapewnieniu odpowiedniej podstawy prawnej do dokonania udostępnienia, zgodnie z art. 6, 9 i 10 RODO.
2. Udostępnienie Danych Osobowych może być dokonywane:
   1) na podstawie przepisów prawa jako działanie stałe i powtarzające się, np. do Zakładu Ubezpieczeń Społecznych, Urzędów Skarbowych, jednostek Krajowej Administracji Skarbowej, Państwowego Funduszu Osób Niepełnosprawnych,

2) na podstawie przepisów prawa na wniosek podmiotów uprawnionych np. Państwowej Inspekcji Pracy, Policji, sądom, innym organom ścigania, Zakładowi Ubezpieczeń Społecznych, Urzędowi Skarbowemu w ramach kontroli,
3) na wniosek innych podmiotów.

3. Każdy nowy przypadek udostępnienia Danych Osobowych, powinien zostać zweryfikowany, w szczególności udostępnienie Danych Osobowych na wniosek innych podmiotów.
4. Administrator weryfikuje wszystkie okoliczności udostępniania Danych Osobowych, w szczególności:
   1) podstawy prawne planowanego udostępnienia,
   2) zakres udostępnianych Danych Osobowych,
   3) sposób udostępnienia Danych Osobowych, w szczególności zapewnienie bezpieczeństwa tych Danych Osobowych podczas ich przekazywania.
5. Za legalność udostępnienia oraz bezpieczeństwo Danych Osobowych do momentu otrzymania ich przez podmiot, do którego następuje udostępnienie, odpowiada Osoba Upoważniona, która dokonuje wysyłki lub przekazania.
6. Nie udostępnia się żadnych Danych Osobowych drogą telefoniczną, chyba że:
   1) są tzw. dane służbowe, tj. imię, nazwisko oraz dane służbowe pracownika: służbowy numer telefonu, służbowy adres e-mail, inne podstawowe informacje, np. godziny pracy, stanowisko, jeżeli są potrzebne do skutecznego podjęcia kontaktu służbowego z tą osobą,
   2) została wdrożona procedura weryfikacji tożsamości

III

Zasady bezpieczeństwa przetwarzania Danych Osobowych przez Osoby Upoważnione przetwarzające Dane Osobowe w formie papierowej

1. Każda Osoba Upoważniona do przetwarzania Danych Osobowych zobowiązana jest do ochrony Danych Osobowych przed dostępem do nich osób nieuprawnionych, niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.
2. Osoby Upoważnione zobowiązane są do zabezpieczenia materiałów zawierających Dane Osobowe w sposób uniemożliwiający: nieuprawniony dostęp do Danych Osobowych osobom nieupoważnionym do ich przetwarzania, nieuprawnione ujawnienie Danych Osobowych, nieautoryzowany dostęp, niedozwolone: powielanie, modyfikację, zniszczenie, utratę, nieprawidłowe wykorzystanie lub kradzież.
3. W miejscu przetwarzania Danych Osobowych utrwalonych w formie papierowej Osoby Upoważnione zobowiązane są do niepozostawiania materiałów zawierających Dane Osobowe w miejscach umożliwiających fizyczny dostęp do nich osobom nieuprawnionym. Po zakończeniu pracy lub podczas czasowej przerwy w pracy, jeżeli dostęp do pomieszczenia mają osoby nieposiadające upoważnienia, materiały zawierające Dane Osobowe powinny być przechowywane w szafach zamykanych na klucz (tzw. **zasada czystego biurka**). Niedopuszczalne jest pozostawienie materiałów zawierających Dane Osobowe na biurku, regale, w niezamkniętej szafie i innych miejscach, do których mają dostęp inne osoby.

4. Kopiowanie Danych Osobowych może odbywać się wyłącznie przez Osobę Upoważnioną w ramach posiadanego przez nią upoważnienia do przetwarzania Danych Osobowych, w związku z realizacją czynności zawodowych w Firmie Handlowo-Usługowej "MAJK" S.C. ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ. Kopie Danych Osobowych podlegają zniszczeniu niezwłocznie po realizacji celu, dla którego zostały wykonane.
5. Dokonywanie wydruków, skanowanie lub kopiowanie materiałów zawierających Dane Osobowe odbywa się wyłącznie przy obecności Osoby Upoważnionej przy urządzeniu. Niedozwolone jest pozostawienie urządzenia w trakcie drukowania/skanowania/kopiowania bez nadzoru, jeżeli materiały znajdujące się w urządzeniu zawierają Dane Osobowe.
6. Każdy dokument papierowy zawierający Dane Osobowe sporządzony jako dokument roboczy należy najpóźniej na koniec dnia pracy zniszczyć lub zamknąć w miejscu uniemożliwiającym dostęp osób nieuprawnionych.
7. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających Dane Osobowe dokonuje się wyłącznie w dedykowanych niszczarkach lub umieszcza w dedykowanych kontenerach na dokumenty przeznaczone do zniszczenia przez podmiot profesjonalny.
8. Osoby Upoważnione do przetwarzania Danych Osobowych nie mogą ich ujawniać zarówno w Firmie Handlowo-Usługowej "MAJK" S.C. ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ jak i poza nim, w zakresie wykraczającym poza wykonywanie swoich obowiązków.
9. Niedopuszczalne jest wynoszenie materiałów zawierających Dane Osobowe poza teren Firmy Handlowo-Usługowej "MAJK" S.C. ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ bez związku z wykonywaniem czynności zawodowych.

IV

Dostęp do pomieszczeń

1. Dostęp do pomieszczeń, w których przetwarzane są Dane Osobowe, mają wyłącznie Osoby Upoważnione do przetwarzania Danych Osobowych.
2. W pomieszczeniach, w których przetwarzane są Dane Osobowe, osoby nieupoważnione mogą przebywać wyłącznie w obecności Osób Upoważnionych.
3. Osoby Upoważnione do przetwarzania Danych Osobowych są obowiązane przestrzegać tzw. zasady czystego biurka, tj. nie pozostawiać dokumentów w sposób umożliwiający zapoznanie się z Danymi Osobowymi innych osób przez osoby nieupoważnione przebywające w pomieszczeniu.
4. Zakazane jest umożliwianie wstępu do pomieszczeń, w których przetwarzane są Dane Osobowe, osobom trzecim pozostawionym bez nadzoru.

V

Mobilne nośniki informacji

1. Kopiowanie Danych Osobowych na przenośne nośniki informacji danych jest zabronione, chyba, że spełnione są łącznie następujące warunki:

1) ich sporządzenie jest niezbędne do realizacji obowiązków służbowych;
2) nośnik jest nośnikiem służbowym Firmy Handlowo-Usługowej "MAJK" S.C. ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ
3) Administrator wyraził zgodę na przetwarzanie tych Danych Osobowych na przenośnym nośniku informacji.

2. Służbowe mobilne nośniki Danych Osobowych są zabezpieczone za pomocą narzędzi szyfrujących

VI

Zarządzanie uprawnieniami do systemów informatycznych

1. Uprawnienia do systemów informatycznych służących do przetwarzania Danych Osobowych nadawane są wyłącznie Osobom Upoważnionym do przetwarzania określonych Danych Osobowych.
2. Uprawnienia do systemów informatycznych są nadawane na wniosek Administratora.
3. Uprawnienia do systemów informatycznych nadawane są w zakresie najwęższym, lecz umożliwiającym swobodną realizację zadań przez użytkownika.
4. Każda osoba przetwarzająca Dane Osobowe w systemie informatycznym otrzymuje nazwę użytkownika (login).

VII

Hasła do systemów informatycznych

1. Użytkownicy systemu informatycznego przetwarzającego Dane Osobowe wykorzystują w procesie uwierzytelnienia identyfikatory (loginy) i hasła.
2. Hasło jest nadawane samodzielnie przez użytkownika systemu.
3. Hasło do systemu służącego do przetwarzania Danych Osobowych:
   1) musi składać się z co najmniej 4 znaków, w tym zawierać co najmniej małą i wielką literę, cyfrę lub znak specjalny
   2) nie może składać się ze słów, cyfr, liczb lub ich kombinacji łatwych do odgadnięcia, w szczególności: nazwy miesiąca, oznaczenia roku, daty urodzenia, imienin swoich lub osób bliskich, imion, nazwisk lub pseudonimów swoich lub osób bliskich itp.
4. Hasło należy zmieniać co najmniej raz na 60 dni.
5. W przypadku, gdy doszło do kompromitacji (odgadnięcia, ujawnienia, podglądnięcia itd.) hasła użytkownika lub użytkownik podejrzewa, że mogło do niego dojść, tj. że jego hasło jest znane innej osobie, jest obowiązany niezwłocznie zmienić hasło oraz poinformować o tym fakcie Administratora danych.
6. Użytkownik zobowiązany jest do:
   1) niezapisywania haseł, w szczególności ich nieumieszczania w miejscach dla osób trzecich,
   2) nieujawniania hasła innym osobom,
   3) zachowania hasła w tajemnicy, również po jego wygaśnięciu,
   4) przestrzegania zasad dotyczących jakości i częstotliwości zmiany hasła,

5) wprowadzania hasła do sytemu w sposób minimalizujący podejrzenie go przez osoby trzecie

VII

Bezpieczne logowanie

1. Proces uwierzytelniania składa się z wprowadzenia nazwy użytkownika oraz poufnego hasła.
2. Każdy użytkownik jest obowiązany wykonywać pracę z użyciem własnych danych uwierzytelniających: nazwy użytkownika oraz hasła. Jeżeli tę samą pracę powinna wykonać lub kontynuować inna osoba, należy wystąpić do IT o nadanie kolejnej osobie uprawnień podobnych lub tożsamych.
3. Zakazane jest udostępnianie danych uwierzytelniających innej osobie, w tym osobom przeprowadzającym kontrole, audyty, inspekcje.
4. Przy wprowadzaniu danych uwierzytelniających użytkownik obowiązany jest upewnić się, że wprowadzone hasło nie będzie widoczne dla żadnej innej osoby.

IX

Poczta elektroniczna

1. Podmiot nie umożliwia dostępu do służbowej poczty elektronicznej z innego sprzętu niż sprzęt służbowy, w szczególności dostępu z poziomu przeglądarki internetowej. Zabronione jest zapamiętywanie haseł do logowania.
2. Zabronione jest przesyłanie Danych Osobowych z innych adresów e-mail niż służbowe adresy Firmy Handlowo-Usługowej "MAJK" S.C. ADAM ŚLEDŹ. KRZYSZTOF ŚLEDŹ.
3. Zabronione jest korzystanie z prywatnych skrzynek pocztowych do celów służbowych lub związanych z tymi celami.
4. Zabronione jest przekierowywanie służbowej poczty elektronicznej na inne niż służbowe adresy e-mail.
5. Zabronione jest przesyłanie Danych Osobowych innych niż dane kontaktowe publiczną siecią Internet w sposób niezabezpieczony, chyba że odbiorca wyraźnie zażyczy sobie dokonania takiej wysyłki, po uprzednim poinformowaniu jej o ryzykach związanych z przesyłaniem niezabezpieczonej poczty elektronicznej publiczną siecią Internet oraz o możliwości wysyłania Danych Osobowych w formie zaszyfrowanej.

X

Postanowienia końcowe

1. Niniejsza Procedura RODO obowiązuje od 02.07.2018r.

Podstawa prawna:

- art. 32 RODO