POLITYKA PRYWATNOŚCI

w spółce Metis Intech sp. z o.o.

Kwiecień 2024

Niniejsza *Polityka prywatności*, 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 Spółce, 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 (dalej RODO).

I. Administrator danych osobowych

1. Administratorem danych osobowych jest spółka Metis Intech Sp. z o.o. z siedzibą w Warszawie, ul. Twarda 18, 00-105 Warszawa, wpisana przez Sąd Rejonowy dla m.st. Warszawy XII Wydział Gospodarczy Krajowego Rejestru Sądowego do Rejestru Przedsiębiorców pod numerem KRS: 0000346294, posiadająca numer NIP 5242697220, REGON 142213792, zwana dalej „**Administratorem**".
2. Dla celów związanych z ochroną danych osobowych kontakt z Administratorem możliwy jest pisemnie pod adresem: ul. Twarda 18, 00-105 Warszawa, a także w formie korespondencji elektronicznej pod adresem e-mail: rodo@metisintech.pl, jak również telefonicznie pod numerem: +48 504 200 045.

II. Postanowienia ogólne

1. Niniejsza Polityka obejmuje wszelkie dane osobowe przetwarzane przez Administratora.
2. Polityka przechowywana jest w formie elektronicznej oraz papierowej i jest udostępniana do wglądu na wniosek osobom posiadającym upoważnienie do przetwarzania danych osobowych, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
3. Celem skutecznej realizacji niniejszej Polityki Administrator zapewnia odpowiednie środki techniczne ochrony danych osobowych oraz rozwiązania organizacyjne, uniemożliwiające naruszenie tejże ochrony, ich monitorowanie, a także kontrolę i nadzór nad przetwarzaniem danych osobowych.

4. Administrator zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą Polityką oraz odpowiednimi przepisami prawa.

III. Dane osobowe przetwarzane przez Administratora

1. Dane osobowe przetwarzane przez Administratora gromadzone są w zbiorach danych.
2. Administrator 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. Administrator prowadzi rejestr czynności przetwarzania.
4. Dane osobowe mogą być przetwarzane w formie papierowej i elektronicznej.

IV. Obszar przetwarzania danych osobowych

Dane osobowe przetwarzane są przez Administratora na terenie Rzeczypospolitej Polskiej.
Okresowo dane osobowe mogą być przetwarzane przez Administratora poza terytorium RP np. podczas podróży służbowych.

V. Obowiązki w zakresie zarządzania bezpieczeństwem danych osobowych

1. Wszystkie osoby upoważnione do przetwarzania danych osobowych, o których mowa w niniejszej Polityce, są zobowiązane do ich przetwarzania zgodnie z obowiązującymi przepisami oraz ustaloną przez Administratora Polityką prywatności.
2. Wszystkie dane osobowe 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 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 usuwane.
g) Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO.

3. Administrator jest zobowiązany dopilnować:
a) odpowiedniego przygotowania pracowników do pełnienia swoich obowiązków;
b) pisemnego upoważnienia każdego z pracowników, który przetwarza dane osobowe.

4. Każdy pracownik Administratora przetwarzający dane osobowe jest zobowiązany do:
a) przestrzegania nadanego upoważnienia do przetwarzania danych osobowych;
b) przetwarzania danych osobowych zgodnie z przepisami prawa, w tym zgodnie z RODO;
c) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych;
d) zachowania w tajemnicy danych osobowych, jak również sposobów ich zabezpieczenia.

VI. Naruszenie bezpieczeństwa danych osobowych

1. Za naruszenie bezpieczeństwa danych osobowych uznaje się w szczególności:
a) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
b) przetwarzanie danych osobowych niezgodnie z założonym celem ich zbierania;
c) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych;
d) utratę nośnika danych osobowych.

2. W przypadku stwierdzenia okoliczności naruszenia bezpieczeństwa danych osobowych pracownik Administratora podejmuje wszystkie niezbędne kroki w celu ograniczenia skutków naruszenia oraz niezwłocznie powiadamia Administratora o stwierdzeniu tych okoliczności, a także o podjętych krokach w celu ograniczenia skutków naruszenia.

3. Administrator każdorazowo ocenia, czy naruszenie ochrony danych osobowych mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. W przypadku wystąpienia prawdopodobieństwa naruszenia praw lub wolności osób fizycznych Administrator bez zbędnej zwłoki - nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.
4. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia także osobę, której dane dotyczą.

VII. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności oraz rozliczalności przetwarzania danych obejmują:

a) zamykanie pomieszczeń, w których przetwarzane są dane osobowe na czas nieobecności upoważnionego pracownika, w sposób uniemożliwiający dostęp do pomieszczenia osobie trzeciej;
b) ochronę sprzętu komputerowego wykorzystywanego u Administratora przed złośliwym oprogramowaniem;
c) usunięcie danych osobowych z nośnika danych w sposób uniemożliwiający ich ponowne przywrócenie, a w razie powierzenia tej czynności podmiotom trzecim – zawarcie stosownej umowy powierzenia przetwarzania danych osobowych;
d) wykorzystywanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe;
e) zabezpieczenie dostępu do urządzeń przy pomocy haseł dostępu,
f) stosowanie zasady „czystego biurka".

VIII. Powierzenie przetwarzania danych osobowych

1. Administrator ma prawo powierzyć przetwarzanie danych osobowych podmiotowi przetwarzającemu, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych odbywało się zgodnie z prawem i chroniło prawa osób, których dane dotyczą.

2. Powierzenie przetwarzania danych osobowych może odbyć się wyłącznie na podstawie pisemnej umowy, spełniającej warunki z art. 28 RODO.

IX. Przekazywanie danych osobowych do państwa trzeciego

Administrator nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.

X. Postanowienia końcowe

Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy oraz przepisów o ochronie danych osobowych.