POLITYKA BEZPIECZEŃSTWA

w spółce ENEXON Sp. z o.o. z siedzibą w Poznaniu

POZNAŃ, STYCZEŃ 2023 r.

Spis treści:

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 spółce Enexon Polska 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 (dalej: RODO) oraz ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000), (dalej: Ustawa).

I.
Definicje

1. **Administrator Danych – ENEXON Sp. z o.o.** z siedzibą w Poznaniu (61 – 248 Poznań), ul. Jana Czochralskiego 11, wpisaną do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy Poznań – Nowe Miasto i Wilda w Poznaniu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000418669, o kapitale zakładowym 41.270.000 zł w całości opłaconym, NIP 782-00-32-899, REGON 630164320,
2. **Inspektor Ochrony Danych (IOD) -** osoba formalnie powołana przez Administratora, zobowiązana do**:** informowania Administratora, Procesora oraz Pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy odpowiednich przepisów o ochronie danych i doradzanie im w tej sprawie; monitorowania przestrzegania przepisów o ochronie danych oraz polityki Administratora lub Procesora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane

   z tym audyty; udzielania informacji co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania.
3. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
4. **Anonimizacja danych osobowych** - pozbawienie danych osobowych cech pozwalających na identyfikacje osób fizycznych, których te dane dotyczą.
5. **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**.**
6. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji, narzędzi programowych zastosowanych w celu przetwarzania danych**.**

7. **Użytkownik** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych.
8. **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów
9. **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
10. **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
11. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika).

II.
Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w Enexon sp. z o.o. 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.
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.

7. Inspektor Ochrony Danych realizując niniejszą Politykę Bezpieczeństwa, dokłada najwyższej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
   - przetwarzane zgodnie z prawem,
   - zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   - merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   - przechowywane nie dłużej niż jest to niezbędne do realizacji celów, w których zostały zebrane.

III.
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. Inspektor Ochrony Danych prowadzi rejestr czynności przetwarzania oraz rejestr kategorii czynności przetwarzania danych osobowych. Wzory rejestrów stanowią **Załączniki nr 1 i 2 do niniejszej Polityki Bezpieczeństwa.**

IV.
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 Systemie Informatycznym, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych w Enexon Polska Sp. z o.o.

2. Wszystkie dane osobowe w Enexon Polska Sp. z o.o. 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.
   - **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. 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.
4. 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,
5. 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" – wzór Upoważnienia stanowi **Załącznik nr 3 do niniejszej Polityki Bezpieczeństwa,**

c) każdy pracownik zobowiązał się do zachowania danych osobowych przetwarzanych w spółce w tajemnicy. „Oświadczenie i zobowiązanie osoby przetwarzającej dane osobowe do zachowania tajemnicy" stanowi element „Upoważnienia do przetwarzania danych osobowych".

6. 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.

V.
Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są Dane osobowe na terenie Enexon Polska Sp. z o.o. są w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych znajdujących się w pomieszczeniach biurowych zlokalizowanych w Poznaniu, ul. Jana Czochralskiego 11, 61-248 Poznań oraz w oddziałach terenowych oraz biurach spółki zlokalizowanych na terenie Rzeczypospolitej Polski. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe stanowi **załącznik nr 6 do niniejszej Polityki Bezpieczeństwa.**

2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.

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

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności 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 dyskach przenośnych zabezpieczonych przy pomocy haseł dostępu.
   - **g)** Ochronę sprzętu komputerowego wykorzystywanego u administratora przed złośliwym oprogramowaniem.
   - **h)** Zabezpieczenie dostępu do urządzeń znajdujących się w siedzibie spółki przy pomocy haseł dostępu.
   - **i)** Wykorzystanie szyfrowania danych przy ich transmisji.

VII.
Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator 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. Wzór zgłoszenia określa **załącznik nr 5 do niniejszej Polityki Bezpieczeństwa.**

3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

VIII.
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 i nast. RODO i art. 31 ust. Ustawy.
2. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.

IX.
Przekazywanie danych do państwa trzeciego

1. Administrator Danych Osobowych nie będzie przekazywał danych osobowych do państwa trzeciego (do państwa spoza Europejskiego Obszaru Gospodarczego), poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.
2. Z uwagi na fakt, że Administrator wchodzi w skład Grupy Würth, ze względów bezpieczeństwa, z uwagi na konieczność zamieszczenia danych osobowych pracowników Administratora, danych agentów Administratora oraz danych pracowników agentów Administratora w bazie pracowników Grupy Würth oraz z uwagi na konieczność prowadzenia kontroli dostępu do systemów IT Grupy, odbiorcą danych osobowych pracowników Administratora, jego agentów oraz pracowników agentów Administratora jest Würth IT GmbH z siedzibą w Bad Mergentheim (Niemcy).

X.
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.
2. Niniejsza polityka wchodzi w życie z dniem podpisania Uchwały Zarządu.
3. Integralną część niniejszej Polityki bezpieczeństwa stanowią następujące Załączniki:

XI.
Załączniki

Załącznik nr 1. *Rejestr czynności przetwarzania danych osobowych;*
Załącznik nr 2. *Rejestr kategorii czynności przetwarzania danych osobowych;*
Załącznik nr 3. - *Upoważnienie do przetwarzania danych osobowych;*
Załącznik nr 4. - *Oświadczenie i zobowiązania osoby przetwarzającej dane osobowe;*
Załącznik nr 5. - *Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego;*
Załącznik nr 6. - *Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;*
Załącznik nr 7. *Ewidencja osób upoważnionych do przetwarzania danych osobowych*