POLITYKA BEZPIECZEŃSTWA INFORMACJI W

Heksagon sp. z o.o. z siedzibą w Katowicach

(nazwa Administratora Danych)

21 maja 2018 roku

(data sporządzenia)

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 przez Heksagon Sp. z o.o. ul. Mickiewicza 29, 40 -085 Katowice nip 9542668696 w tym zgodnie i na podstawie Rozporządzenia 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).

Definicje:

1. Administrator Danych – podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych- Heksagon sp. z o.o., ul. Mickiewicza 29, 40-085 Katowice, KRS 0000326312,

2. **Dane osobowe** – wszelkie informacje, w tym o stanie zdrowia, dotyczące zidentyfikowania lub możliwej do zidentyfikowania osoby fizyczne.

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 osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

6. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w Systemach informatycznych

7. **Podmiot przetwarzający**- podmiot przetwarzający w rozumieniu art. 4 pkt 8 RODO.

I. Postanowienia ogólne

1. Polityka dotyczy wszystkich danych osobowych przetwarzanych przez administratora, niezależnie od formy ich przetwarzania (przetwarzania

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 obowiązuje i jest udostępniana do wglądu wyłącznie 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) zabezpieczenie odpowiednie do zagrożeń i kategorii danych objętych ochroną, a także 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 min. działania użytkowników, naruszenie 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, modyfikacji czynności wykonywanych lub ich skali administrator danych dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.

4. Administrator danych prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi Załącznik nr 1 do niniejszej polityki.

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, a także innymi dokumentami wewnętrznymi i procedurami związanymi z przetwarzaniem danych osobowych obowiązującymi u administratora danych.

2. Wszystkie dane osobowe przetwarzane są z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa tj. dane są przetwarzane w sposób rzetelny, dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami, dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych.

3. Czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane.

4. Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO.

5. Dane osobowe są zabezpieczone przed naruszeniem zasad ich ochrony.

6. 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 umożliwianie 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 sposób ich zabezpieczania,

e) przetwarzania 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.

7. 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.

8. Do obowiązków administratora danych w zakresie zatrudnienia, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz administratora danych na podstawie innych umów cywilnoprawnych) należy, by:

a) pracownicy lub współpracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków w zakresie ochrony danych osobowych,

b) każdy z przetwarzających dane osobowe był pisemnie upoważniony do ich przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych" – wzór upoważnienia stanowi załącznik nr 2 do niniejszej polityki,

c) każdy z przetwarzających dane osobowe zobowiązał się do zachowania przetwarzanych danych osobowych w tajemnicy. „Oświadczenie o poufności" stanowi element „Upoważnienia do przetwarzania danych osobowych".

9. Użytkownicy zobowiązani są do:

a) ścisłego przestrzegania zakresu nadanego upoważnienia,

b) przetwarzania i ochrony danych osobowych zgodnie z niniejszą polityką oraz obowiązującymi przepisami prawa,

c) zachowania w tajemnicy danych osobowych oraz sposób ich zabezpieczenia,

d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu,

e) zgłaszania administratorowi danych zamiaru zwiększenia zakresu pobierania danych od osoby, przekazania danych nowemu odbiorcy, usunięcia danych, opublikowania danych, skorzystania z nowego oprogramowania lub usługi do przetwarzania danych i uzyskania pisemnej zgody na podjęcie tych czynności,

10. Naruszenie przez użytkownika obowiązków wynikających z niniejszej polityki i obowiązujących przepisów prawa skutkuje odpowiedzialnością

wynikającą z obowiązujących przepisów prawa zarówno wobec administratora danych jak i osób trzecich.

11. Niezależnie od odpowiedzialności wskazanej w pkt. 10 naruszenie przez użytkownika obowiązków wynikających z niniejszej polityki i obowiązujących przepisów prawa może stanowić naruszenie podstawowych obowiązków pracowniczych.

IV. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są dane osobowe, obejmuje pomieszczenia biurowe Heksagon sp. z o.o. zlokalizowane w Mickiewicza 29, 40-085 Katowice

2. Dodatkowo obszar, w którym przetwarzane są dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujących się poza obszarem wskazanym powyżej, a z których korzysta administrator danych lub użytkownicy.

V. Określenie środków fizycznych, technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych.

1. Administrator Danych zapewnia zastosowanie środków technicznym i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzania danych.

2. Zastosowanie środków ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych

3. Środki fizyczne 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.

   a) Zamykania pomieszczeń tworzących obszar przetwarzania danych osobowych określony na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich.

   b) Wykorzystywanie zamykanych szafek do zabezpieczenia dokumentów.

c) Wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe.

d) fizyczną ochronę osób i mienia

4. Środki techniczne obejmują procedury i zasady postępowania określone w instrukcji zarządzania systemem informatycznym obowiązującej u administratora danych, stanowiącej załącznik nr 3 do niniejszej polityki

5. Środki organizacyjne obejmują:

a) nadawanie przez administratora danych pisemnych „Upoważnień do przetwarzania danych osobowych" wraz z „Oświadczeniem o poufności" i prowadzenie ich ewidencji;

e) powierzenie przetwarzania danych osobowych podmiotowi przetwarzającemu wyłącznie na podstawie pisemnej umowy po uzyskaniu informacji o dotychczasowych praktykach podmiotu powierzającego dotyczących zabezpieczenia danych osobowych;

f) zgłaszanie i prowadzenie ewidencji incydentów naruszenia danych osobowych;

g) każdorazowe badanie skutków dla ochrony danych osobowych w przypadku zamiaru wprowadzenia u administratora danych nowych czynności przetwarzania, modyfikacji tych czynności lub ich skali;

h) konieczność uzyskania pisemnej zgody administratora danych w przypadku zamiaru zwiększenia zakresu pobierania danych od osoby, przekazania danych nowemu odbiorcy, usunięcia danych, opublikowania danych, skorzystania z nowego oprogramowania lub usługi do przetwarzania danych;

i) procedurę realizacji praw osób, których dane dotyczą;

j) bieżące monitorowanie i ocena przez administratora danych zastosowanych środków ochrony;

VI. Naruszenie 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, nie później niż w 72 godziny po stwierdzeniu naruszenia. Wzór zgłoszenia określa załącznik nr 4 do niniejszej polityki.

3. Jeżeli ryzyko naruszenia prawa 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 podmiotowi przetwarzającemu wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO – wzór umowy stanowi załącznik nr 5 do niniejszej polityki,

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

VIII. Realizacja praw osób, których dane dotyczą

1. Administrator danych osobowych zapewnia realizację uprawnień osób, których dane są przetwarzane, polegających na prawie dostępu do danych osobowych, do kopii danych, ich sprostowania, usunięcia, lub ograniczenia przetwarzania, do sprzeciwu wobec przetwarzania oraz prawie cofnięcia zgody

2. Po dokonaniu zgłoszenia przez osobę uprawnioną, której dane dotyczą administrator danych weryfikuje zasadność zgłoszenia, uwzględniając obowiązujące przepisy prawa i udziela osobie odpowiedzi w zakresie realizacji prawa lub odmowy.

3. Odpowiedź wraz z uzasadnieniem powinna być przekazana osobie, której prawa dotyczą w terminie 21 dni od zgłoszenia.

4. Administrator danych informuje odbiorców danych o zgłoszeniu osoby, której dane dotyczą.

IX. Postanowienia końcowe

1. Wszelkie zmiany niniejszej polityki wymagają formy pisemnej pod rygorem nieważności