Polityka Ochrony Danych Osobowych

Administrator

Agata Ciołek

prowadząca działalność gospodarczą pod firmą

EcoChic Organic Beauty Studio

1 SPIS TREŚCI:

2 WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

Administrator oświadcza, że będzie podejmować wszelkie działania w celu zapewnienia bezpieczeństwa informacji i ochrony danych osobowych, w tym także w zakresie przyjęcia, wdrożenia i nadzoru nad stosowaniem zasad niniejszej Polityki przez pracowników i inne osoby zatrudnione, a także podmioty trzecie świadczące usługi na rzecz Administratora.

Podstawowe zasady dotyczące przetwarzania danych osobowych

1. Dane osobowe muszą być przetwarzane zgodnie z prawem, tak aby były rzetelne i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
2. Przetwarzanie danych powinno być tak zorganizowane, że zapewnia się:
   1) zbieranie danych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; („ograniczenie celu”);
   2) adekwatność, stosowny zakres danych oraz ograniczenie do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
   3) prawidłowość i w razie potrzeby uaktualnianie; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”)
   4) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
3. Przetwarzanie danych powinno się odbywać w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).
4. Administrator stosuje mechanizmy umożliwiające wykazanie przestrzegania zasad („rozliczalność”).

3 OGÓLNE ZASADY PRZETWARZANIA DANYCH

3.1 ZGODNOŚĆ Z PRAWEM

Świadcząc usługi lub dokonując organizacji procesów związanych z realizacją usług Administrator uwzględnia zasadę zgodności z prawem przetwarzania danych osobowych.

Przetwarzanie danych osobowych przez Administratora jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2) 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;
3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze;
4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych.

W przypadku przetwarzania w celu innym niż cel, w którym dane osobowe zostały zebrane, i nie na podstawie zgody osoby, której dane dotyczą, ani prawa – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – należy brać pod uwagę między innymi:

1) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;
2) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a Administratorem;
3) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 RODO;
4) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;
5) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

3.2 ZGODY NA PRZETWARZANIE

W przypadkach, gdy przetwarzanie odbywa się na podstawie zgody, fakt wyrażenia zgody musi być dokumentowany tak, że Administrator jest w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

Pisemne oświadczenia składane Administratorowi dotyczące wyrażenia zgody na przetwarzanie danych osobowych powinny być zrozumiałe i przedstawione w łatwo dostępnej formie, jasnym i prostym językiem, a treść oświadczenia zostać przedstawiona w sposób pozwalający wyraźnie odróżnić ją od pozostałych kwestii zwartych w formularzach stosowanych przez Administratora.

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

Uzależnianie wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy jest zabronione.

3.3 PRZETWARZANIE DANYCH WRAŻLIWYCH

Administrator nie przetwarza danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących, seksualności lub orientacji seksualnej tej osoby.

W związku z zakresem świadczonych usług, Administrator przetwarza dane związane ze stanem zdrowia osób korzystających z oferty Administratora.

Dane wrażliwe, dotyczące stanu zdrowia przetwarzane są na podstawie wyraźnej zgody na przetwarzanie tych danych osobowych w konkretnym celu związanym z usługami świadczonymi przez Administratora

3.4 OBOWIĄZKI INFORMACYJNE ADMINISTRATORA

Świadcząc usługi lub dokonując organizacji procesów związanych z realizacją usług Administrator zapewnia przejrzyste informowanie i przejrzystą komunikację z osobą, której dane dotyczą.

Informacja o przetwarzanych została sporządzona w pisemnej. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile potwierdzi się tożsamość osoby, której dane dotyczą.

W związku z faktem, iż w ramach świadczenia usług przez Administratora następuje zbieranie danych osobowych, Administrator zapewnia podczas pozyskiwania danych podanie osobie, której dane dotyczą informacji:

1) nazwie Administratora i danych kontaktowych (adres, telefon),
2) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
3) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią;
4) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

5) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
6) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
7) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO (zgoda na przetwarzanie) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
8) informacje o prawie wniesienia skargi do organu nadzorczego;
9) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

3.5 PRAWO DOSTĘPU

Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

1) cele przetwarzania;
2) kategorie danych osobowych;
3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
5) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6) informacje o prawie wniesienia skargi do organu nadzorczego;
7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;

Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Pierwsza kopia udostępniana jest bez opłat, za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

3.6 SPRZECIW, SPROSTOWANIE I USUWANIE DANYCH

Sprzeciw wobec przetwarzania danych

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO.

Po wniesieniu sprzeciwu Administrator nie może już przetwarzać tych danych osobowych, chyba że zaistnieje ważna, prawnie uzasadniona podstaw do przetwarzania, nadrzędna wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstawa do ustalenia, dochodzenia lub obrony roszczeń.

Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, Administrator nie przetwarza dalej danych osobowych tej osoby do takich celów.

Sprostowanie danych

Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczeń.

Usunięcie danych („prawo do bycia zapomnianym”), ograniczenie przetwarzania

Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane lub
2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO i nie ma innej podstawy prawnej przetwarzania,
3) inne wymienione w art. 17 RODO okoliczności

Osoba, której dane dotyczą, ma prawo żądania od Administratora ograniczenia przetwarzania w przypadkach:

1) kwestionowania prawidłowości danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych;
2) przetwarzania niezgodnego z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
3) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

4) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Powiadomienia o sprostowaniu, usunięciu danych lub ograniczeniu przetwarzania

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

4 ANALIZA RYZYKA

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

4.1 DEFINICJE

1. **Administrator (danych)** - oznacza osobę fizyczną lub prawną, która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, w przypadku niniejszego dokumentu za Administratora uważa się Agatę Ciołek prowadzącą działalność gospodarczą pod firmą EcoChic Organic Beauty Studio;
2. **Aktywa** – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych
3. **RODO** – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)
4. **Dane osobowe** - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej.
5. **Ocena skutków w ochronie danych -** to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.
6. **Przetwarzanie danych osobowych** to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.
7. **Naruszenie (Incydent) ochrony danych osobowych** - to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych
8. **Zagrożenie** - potencjalne naruszenie (potencjalny incydent)
9. **Skutki** - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia)

10. **Ryzyko** - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie aktywów

4.2 OCENA SKUTKÓW (ANALIZA RYZYKA)

Ocena skutków jest formalną, określoną w art. 35 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. Na ocenę skutków (analizę ryzyka) składają się następujące czynności:

1) Opis operacji przetwarzania (inwentaryzacja aktywów):

1. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane te w postaci zbiorów (kategorii osób) zostały wykazane w **załączniku nr 1 Rejestr czynności przetwarzania (wykaz zbiorów danych osobowych).**
2. Opis zbiorów (kategorii osób) powinien obejmować takie informacje, jak:
    a. nazwę zbioru (opis kategorii osób)
    b. opis celów przetwarzania
    c. charakter, zakres, kontekst danych osobowych
    d. odbiorcy danych
    e. funkcjonalny opis operacji przetwarzania
    f. aktywa służące do przetwarzania danych osobowych (Informacje, Programy, Systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing).
    g. informacja o konieczności wpisu do rejestru czynności przetwarzania
    h. informacja o konieczności przeprowadzenia oceny skutków dla zbioru

2) Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO)

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator zobowiązany jest do spełnienia szeregu obowiązków prawnych wobec danych zgromadzonych w zbiorach.

W szczególności Administrator odpowiedzialny jest za zapewnienie, że :

1. dane te są legalnie przetwarzane (na podstawie art. 6, 9 RODO)
2. dane te są adekwatne w stosunku do celów przetwarzania
3. dane te są przetwarzane przez określony czas (retencja danych)
4. wobec osób, których dane dotyczą wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14 RODO) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody);
5. opracowano klauzule informacyjne, które umieszczone są w formularzach stosowanych przez Administratora;
6. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO)

3) Analiza ryzyka

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania.

Wyznaczenie zagrożeń:

1. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów.

Wyliczenie ryzyka dla zagrożeń:

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A
3. Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne
4. Proponowaną Skalę skutków prezentuje Tabela B
5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S**

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
małe (do 10.000 PLN, incydent prasowy lokalny)	1
średnie (10.000-100.000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100.000 PLN, naruszenie prawa)	3

Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem.

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.

2. Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	**WARTOŚĆ** [**R = P*S**]
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

Reakcja na wartość ryzyka:

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń
2. Działania obniżające ryzyko, które może zastosować Administrator:
    a. Przeniesienie – przerzucenie ryzyka
    b. Unikanie – eliminacja działań powodujących ryzyko
    c. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka

3. Analizę ryzyka przeprowadza się przy wykorzystaniu **Arkusza analizy ryzyka RODO, stanowiącego załącznik nr 2** do niniejszej Polityki.

Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie nie rzadziej niż raz w roku lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów/kategorii osób, realizacja nowych procesów przetwarzania, zmiany prawne).

4) Plan postępowania z ryzykiem

1. W przypadku, gdy w wyniku przeprowadzonej analizy ryzyka Administrator podejmie decyzję o konieczności obniżenia ryzyka, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne - **Plan postępowania z ryzykiem stanowi załącznik nr 3** do niniejszej Polityki.
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń

5 REJESTR CZYNNOŚCI PRZETWARZANIA (INWENTARYZACJA DANYCH OSOBOWYCH)

Administrator jest zobowiązany zgodnie z art. 30 RODO do prowadzenia rejestru czynności przetwarzania. Rejestr stanowi podstawę do przeprowadzenia analizy ryzyka. Administrator prowadzi rejestr zgodnie z **załącznikiem nr 1 do niniejszej Polityki - Rejestr czynności przetwarzania (wykaz zbiorów danych osobowych).**

W rejestrze tym zamieszcza się wszystkie następujące informacje:

1) nazwę oraz dane kontaktowe Administratora;
2) cele przetwarzania;
3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
5) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
6) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
7) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
8) Rejestr, czynności przetwarzania ma formę pisemną, w tym formę elektroniczną.

Administrator udostępnia rejestr na żądanie organu nadzorczego.

6 ŚRODKI TECHNICZNE I ORGANIZACYJNE ZABEZPIECZAJĄCE DANE OSOBOWE

1. Administrator danych osobowych stosuje środki techniczne i organizacyjne (zabezpieczenia) adekwatne do zagrożeń naruszenia praw i wolności osób, których dane osobowe są przetwarzane.
2. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych.
3. Wykaz zabezpieczeń został wskazany w **Instrukcji zarządzania RODO stanowiącej załącznik nr 4 do niniejszej Polityki.**
4. W instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne.
5. Instrukcja jest aktualizowana, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka.

7 SZKOLENIA LUB ZAPOZNAWANIE OSÓB Z ZASADAMI ODO

1. Każda osoba przed dopuszczeniem z danymi osobowymi winna być poddana przeszkoleniu lub zapoznana z:
   a) przepisami RODO,
   b) zasadami ochrony danych osobowych zawartych w niniejszej Polityce i Instrukcji zarządzania RODO.
2. Za przeprowadzenie szkolenia lub zapoznanie z zasadami ochrony danych osobowych odpowiada Administrator.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia.
4. Administrator w celu zapewnienia wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania opracował i przyjął Regulamin Ochrony Danych Osobowych (rozumiany jako zabezpieczenie).
5. Każda osoba po szkoleniu lub po zapoznaniu z zasadami ochrony danych osobowych zobowiązana jest do podpisania Oświadczenia o poufności.
6. Podpisane Oświadczenia poufności archiwizowane są Administratora w odpowiednio opisanych segregatorach. Oświadczenie poufności stanowi podstawę do nadania upoważnienia do przetwarzania danych osobowych.

8 UPOWAŻNIENIA

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach (dla kategorii osób) powadzonych w postaci papierowej.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie Administratora lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są do zbiorów (dla kategorii osób) na wniosek Administratora. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie.
4. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych**. Ewidencja osób upoważnionych stanowi załącznik nr 5 do niniejszej Polityki.**
5. W przypadku powierzenia przetwarzania danych do Podmiotu przetwarzającego, Administrator jest zobowiązany do sporządzenia z nim umowy powierzenia, stanowiącą podstawę upoważnienia dla osób z Podmiotu.

9 REGULAMIN OCHRONY DANYCH OSOBOWYCH

1. Administrator w celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania opracował **Regulamin Ochrony Danych Osobowych stanowiący załącznik nr 6 do niniejszej Polityki.**
2. Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania poprzez podpisanie stosownego oświadczenia.
3. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu lub zapoznana z przepisami RODO.
4. Za przeprowadzenie szkolenia odpowiada Administrator.

10 INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu Administratora.
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
    b. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
    b. zdarzenia losowe wewnętrzne (awarie, pomyłki pracowników, utrata / zagubienie danych);
    c. umyślne incydenty (włamanie do pomieszczeń, kradzież danych, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych).
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator (prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki
    b. inicjuje ewentualne działania dyscyplinarne
    c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu
    d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze poprzez sporządzenie **Formularza rejestracji incydentu stanowiącego załącznik nr 7 do niniejszej Polityki.**
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.
8. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
9. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki
10. Zgłoszenie, o którym mowa w pkt. 7, musi co najmniej:
    1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

2) zawierać imię i nazwisko oraz dane kontaktowe Administratora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
4) opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

10.1 ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ O NARUSZENIE OCHRONY DANYCH OSOBOWYCH

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w pkt. 1, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej:
   1) imię i nazwisko oraz dane kontaktowe Administratora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   2) opisuje możliwe konsekwencje naruszenia ochrony danych osobowych;
   3) opisuje środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Zawiadomienie, o którym mowa w pkt. 1, nie jest wymagane, w następujących przypadkach:
   1) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak anonimizacja, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   2) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.