Wewnętrzna Polityka Bezpieczeństwa

stosowana w

Firmie MEBLEMAR MEBLE NA ZAMÓWIENIE Początek Marek, 35-330 Rzeszów, Św. Rocha 136, nip: 813-222-09-26

Spis treści

I. Deklaracja

1. Firma MEBLEMAR MEBLE NA ZAMÓWIENIE Początek Marek, 35-330 Rzeszów, Św. Rocha 136, nip: 813-222-09-26, zwana dalej w niniejszym dokumencie „**Przedsiębiorcą**" lub „**Administratorem danych**" ma świadomość znaczenia bezpieczeństwa procesów przetwarzania danych w prowadzonej przez siebie działalności. Przedsiębiorca ma świadomość ryzyka reputacyjnego oraz prawnego związanego z przetwarzaniem danych osobowych Klientów.

2. Przedsiębiorca uwzględnia aspekt bezpieczeństwa informacji przy zarządzaniu usługami świadczonymi na rzecz swoich Klientów na poziomie celów, strategii oraz działań

oraz deklaruje, że promuje i wspiera działania związane z zapewnieniem bezpieczeństwa informacji, stosownie do wymagań określonych w niniejszej Polityce.

3. Dążąc do zapewnienia bezpieczeństwa usług świadczonych drogą elektroniczną na rzecz Klientów Przedsiębiorca stale doskonali procesy zarządzania przetwarzaniem danych osobowych przy uwzględnieniu zmian w środowisku prawnym oraz przy uwzględnieniu rozwoju rozwiązań technologicznych.

4. Cele stosowania zabezpieczeń i zabezpieczenia stosowane u Przedsiębiorcy w związku z wykonywaniem procesów w zakresie przetwarzania danych osobowych zostały dobrane w oparciu o rezultaty i wnioski wynikające z procesów szacowania i postępowania z ryzykiem, wymagania prawne, charakterystykę prowadzonej działalności, w tym jej lokalizację, aktywa i technologie.

5. Stosowane u Przedsiębiorcy zasady ochrony informacji mogą być poddawane niezależnej i wiarygodnej ocenie ze strony wyspecjalizowanego podmiotu zewnętrznego.

6. Przedsiębiorca określił, że stosowany u Przedsiębiorcy system zarządzania bezpieczeństwem informacji obejmuje swoim zakresem:
   a) całą działalność Przedsiębiorcy, w tym w szczególności nadzorowanie rozwiązań informatycznych oraz świadczenie wszelkich usług na rzecz Klientów,
   b) wszystkie lokalizacje geograficzne, w których Przedsiębiorca prowadzi swoją działalność.

7. W ramach systemu zarządzania bezpieczeństwem informacji Przedsiębiorca ustanawia Wewnętrzną Politykę Bezpieczeństwa, której cele i zasady zamieszczono poniżej.

II. Zakres dokumentu

1. Niniejsza Wewnętrzna Polityka Bezpieczeństwa formułuje zasady bezpieczeństwa informacji obowiązujące u Przedsiębiorcy, w tym w szczególności systemów teleinformatycznych wykorzystywanych w ramach świadczenia usług przez Przedsiębiorcę.

2. Za związane z niniejszą Wewnętrzną Polityką Bezpieczeństwa będą uznawane wszystkie zatwierdzone dokumenty niższych poziomów, w szczególności procedury i instrukcje wewnętrzne.

3. Niniejsza Wewnętrzna Polityka Bezpieczeństwa nie wyczerpuje wszystkich zagadnień dotyczących ochrony danych osobowych u Przedsiębiorcy. Określona prawnie materia dotycząca zabezpieczenia i przetwarzania danych osobowych regulowana jest równolegle w odrębnych dokumentach.

III. Definicje

Niniejszy dokument zawiera podstawowe definicje pojęć dotyczących systemu zarządzania bezpieczeństwem informacji u Przedsiębiorcy. Definicje pojęć dodatkowych mogą znajdować się w dokumentach związanych.

1. **Aktywa (informacyjne)** - wszelkie zasoby: oprogramowanie, dane, sprzęt, zasoby administracyjne, fizyczne lub komunikacyjne lub ludzkie, które stanowią dla Przedsiębiorcy wartość chronioną

2. **Autentyczność** - właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana. Autentyczność dotyczy takich podmiotów jak użytkownicy, procesy, systemy i informacje

3. **Bezpieczeństwo informacji** - zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność

4. **Dostępność** - właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot

5. **Incydent związany z bezpieczeństwem informacji** - pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji

6. **Integralność danych** - właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany

7. **Integralność systemu** - właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej

8. **Niezaprzeczalność** - możliwość przeprowadzenia dowodu, że działanie lub zdarzenie miało miejsce, tak że nie można temu działaniu lub zdarzeniu później zaprzeczyć

9. **Niezawodność** - właściwość oznaczająca spójne, zamierzone zachowanie i skutki

10. **Podatność** - słabość aktywu lub grupy aktywów, które mogą być wykorzystane przez jedno lub więcej zagrożeń

11. **Poufność** - właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom

12. **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane

w sposób jednoznaczny tylko temu podmiotowi

13. **Ryzyko związane z bezpieczeństwem informacji** - potencjalna sytuacja, w której dane zagrożenie wykorzysta podatności aktywów lub grupy aktywów, co spowoduje szkodę dla Przedsiębiorcy; ryzyko jest funkcją prawdopodobieństwa zdarzenia i jego konsekwencji

14. **Zagrożenie** - potencjalna przyczyna incydentu, który może spowodować stratę w systemie lub szkodę dla Przedsiębiorcy

15. **Zarządzanie ryzykiem** - skoordynowane działania kierowania i kontrolowania z uwzględnieniem ryzyka

IV. Podstawowe zasady bezpieczeństwa informacji

1. Organizacja wewnętrzna Przedsiębiorcy, procedury wewnętrzne oraz systemy teleinformatyczne zakładają bezpieczną realizację usług świadczonych na rzecz Klientów poprzez zapewnienie :
   a) poufności, integralności, dostępności i autentyczności danych przetwarzanych w ramach realizacji usług,
   b) autentyczności czynności dokonywanych przez Przedsiębiorcę oraz inne osoby pracujące na rzecz Przedsiębiorcy jako użytkownicy systemów w systemach teleinformatycznych Przedsiębiorcy,
   c) rozliczalności i niezaprzeczalności działań i zdarzeń zachodzących w systemach teleinformatycznych Przedsiębiorcy,
   d) niezawodności i dostępności systemów realizujących usługi na rzecz Klientów i Partnerów Przedsiębiorcy.

2. W celu zapewnienia bezpieczeństwa informacji stosuje się następujące ogólne zasady:
   a) „minimalnych przywilejów" - oznaczającą przydzielanie praw dostępu tylko w zakresie niezbędnym do wykonania określonego zadania,
   b) „wiedzy koniecznej" - oznaczającą, iż każdy użytkownik ma potrzebę wiedzy o aktywach, do których ma prawo dostępu,
   c) ,,domniemanej odmowy" - oznaczającą, iż w założeniu wszystko jest zabronione, dopóki nie jest wyraźnie dozwolone.

3. Systemy informatyczne są zabezpieczone przed nieupoważnionym dostępem, modyfikacją lub zniszczeniem.

4. Informacje są chronione w sposób proporcjonalny do ich wrażliwości, zagrożeń lub wymagań stawianych przez odpowiednie przepisy prawne.

5. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe:
   - pomieszczenia znajdujące się w budynku przy ul. płk. Kazimierza Iranka -

Osmeckiego 9 lok. 1 (35-506 Rzeszów), zajmowane przez Przedsiębiorcę („**Siedziba**"),

- dane osobowe w postaci dokumentacji papierowej przechowywane są w zamkniętych szafach w pomieszczeniach o ograniczonych prawach dostępu znajdujących się w Siedzibie Przedsiębiorcy,
- nośniki informacji przechowywane są w Siedzibie Przedsiębiorcy,
- uszkodzone komputerowe nośniki zawierające dane osobowe są przechowywane w Siedzibie Przedsiębiorcy.

6. Obszar, w którym przetwarzane są dane osobowe zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe jest dopuszczalne za zgodą Administratora danych lub w jego obecności.

7. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.

8. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie zapasowe:
   a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
   b) usuwa się niezwłocznie po ustaniu ich użyteczności.

9. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   a) likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
   c) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

10. Dane osobowe co do zasady nie są przetwarzane poza Siedzibą.

11. W związku z przetwarzaniem przez Przedsiębiorcę danych osobowych występują następujące zagrożenia i ryzyka dla poufności, integralności rozliczalności przetwarzanych danych: nieuprawnione ujawnienie, modyfikacja lub zniszczenie, kradzież, oszustwa, wandalizm. Wszystkie zasoby należy uznać za podatne na zagrożenia, których sprawcą jest człowiek. Ze szczególną uwagą należy traktować inżynierię społeczną i typowe pomyłki ludzkie, zwłaszcza wynikające z niedbalstwa i braku wiedzy.

Dla zapewnienia poufności danych osobowych Przedsiębiorca stosuje następujące środki:

a) **organizacyjne:**
   - wyznaczono obszar przetwarzania danych osobowych;
   - opracowano i wdrożono instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
   - wyznaczono ograniczoną liczbę użytkowników dopuszczonych do przetwarzania danych osobowych.

b) **techniczne:**
   - ograniczony dostęp do pomieszczeń na obszarze przetwarzania danych osobowych;
   - system logowania do systemu informatycznego;
   - system antywirusowy;
   - system Backup'owy.

Dla zapewnienia integralności danych osobowych Przedsiębiorca stosuje następujące środki:

a) **organizacyjne:**
   - każdy użytkownik ma określone własne prawa dostępu;

b) **techniczne:**
   - kopie bezpieczeństwa;

V. Zasada privacy by design (zasada prywatności w fazie projektowania)

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, Administrator danych – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by chronić prawa osób, których dane dotyczą.

2. Powyższe w szczególności może dotyczyć zasad tworzenia, utrzymania i wycofywania z użycia aplikacji, przeprowadzania testów bezpieczeństwa, monitorowania bezpieczeństwa infrastruktury, a także zarządzania zmianą.

3. Aby osiągnąć odpowiedni poziom ochrony danych osobowych, Administrator danych musi ocenić, jakie zabezpieczenia będą proporcjonalne do ryzyka naruszenia danych osobowych przetwarzanych w ramach działalności posługując się m.in.:

a) wytycznymi i najlepszymi praktykami dotyczącymi zarządzania bezpieczeństwem informacji, np. normy ISO, metodyka MARION,
b) rekomendacjami uznanych organizacji (The OWASP, ENISA),
c) wytycznymi i zaleceniami Grupy Roboczej Art. 29, Europejskiej Rady Ochrony Danych Osobowych,
d) zatwierdzonymi kodeksami postępowania,
e) zatwierdzonymi mechanizmami certyfikacji.

4. Zastosowane środki ochrony danych osobowych powinny zapewnić:
   a) możliwość szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
   b) poufność, integralność, dostępność i odporność systemów i usług przetwarzania,
   c) możliwość regularnego testowania, mierzenia i oceniania ich skuteczności.

VI. Zasada privacy by default (zasada prywatności w ustawieniach domyślnych)

1. Administrator danych jest zobowiązany wdrażać takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne w stosunku do każdego konkretnego celu przetwarzania. Dotyczy to ilości zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Omawiane środki powinny zapewniać w szczególności, aby domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

2. W tym kontekście istotne jest zapewnienie inwentaryzacji danych i wdrożenie środków bezpieczeństwa zgodnie z wykonaną oceną profilu ryzyka i krytyczności danych.

VII. Privacy impact assessment – mechanizm oceny wpływu przetwarzania danych osobowych na prywatność osób, których dane są przetwarzane

1. Przed rozpoczęciem czynności przetwarzania Administrator danych jest zobowiązany do dokonania oceny skutków operacji przetwarzania dla ochrony danych. Ocena powinna w szczególności uwzględniać takie czynniki jak: charakter, zakres, kontekst i cele operacji przetwarzania czy zastosowanie nowych technologii.

2. Minimalne elementy dokonywanej oceny: opis planowanych operacji przetwarzania, ocenę ich niezbędności i proporcjonalności w stosunku do celów, ocenę ryzyka oraz opis środków podejmowanych w celu zaradzenia ryzykom.

3. W razie stwierdzenia ryzyka naruszenia praw lub wolności osób fizycznych, którego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii

i kosztów wdrożenia, Administrator danych zobowiązany jest skonsultować się w tym zakresie z organem nadzorczym przed rozpoczęciem czynności przetwarzania.

VIII. Transfer danych osobowych do państw trzecich

1. Transfer danych osobowych do państw trzecich jest możliwy wtedy, gdy państwa te zapewniają adekwatny poziom ochrony. Inne transfery są możliwe po zapewnieniu odpowiednich gwarancji tj. na podstawie klauzul modelowych, wiążących reguł korporacyjnych, zatwierdzonych kodeksów postępowania oraz jeśli zarówno przekazujący, jak i odbierający dane uzyskali „certyfikat europejskiej ochrony danych osobowych".

2. Adekwatność poziomu ochrony danych osobowych może być stwierdzona decyzją Komisji Europejskiej.

IX. Naruszenie ochrony danych i powiadamianie organu nadzoru o naruszeniu ochrony danych

1. Przez naruszenie danych osobowych rozumie się przypadkowe lub bezprawne zniszczenie, utratę, zmianę, nieuprawnione ujawnienie lub dostęp do danych osobowych przetwarzanych przez Przedsiębiorcę.

2. Administrator jest zobligowany do zgłoszenia właściwemu organowi nadzorczemu incydentu polegającego na:
   a) przypadkowym lub niezgodnym z prawem zniszczeniu, utracie, modyfikacji,
   b) nieuprawnionym ujawnieniu lub
   c) nieuprawnionym dostępie do przetwarzanych danych osobowych.

3. Incydentami podlegającymi zgłoszeniu są np. takie zdarzenia jak wejście nieupoważnionej osoby do systemu informatycznego, w którym są przetwarzane dane osobowe, jak również zgubienie komputera przenośnego.

4. Zgłoszenia dokonuje się niezwłocznie, jednak nie później niż w ciągu 72 godzin od stwierdzenia naruszenia.

5. Zawiadomienie o naruszeniu ochrony danych osobowych nie jest wymagane w przypadku, gdy jest mało prawdopodobne, że naruszenie mogło spowodować zagrożenie dla praw i wolności osób, których dane dotyczą.

6. Administrator danych prowadzi stosowny rejestr naruszeń danych osobowych.

7. W wyniku wykrycia naruszenia ochrony danych przeprowadza się postępowanie wyjaśniające oraz wdraża stosowne środki w celu zaradzenia naruszeniu ochrony danych osobowych.

8. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu, wzór stanowi załącznik nr 1 do niniejszej Wewnętrznej Polityki Bezpieczeństwa, powinno wskazywać:
   a) datę i godzinę naruszenia,
   b) osobę powiadamiającą o naruszeniu oraz inne osoby zaangażowane lub przesłuchane w związku z naruszeniem,
   c) lokalizację zdarzenia,
   d) rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu,
   e) podjęte działania,
   f) wstępną ocenę przyczyn wystąpienia naruszenia,
   g) w jaki sposób zostało przeprowadzone postępowanie wyjaśniające i naprawcze, jakie środki zostały zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach jakie zastosowano środki w celu zminimalizowania ewentualnych negatywnych skutków.

X. Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Użytkownik, który stwierdza lub podejrzewa naruszenie ochrony danych w systemie informatycznym, zobowiązany jest niezwłocznie poinformować o tym zdarzeniu administratora sieci i ustalić dalszy tok postępowania.

2. Administrator danych dokumentuje zaistniały przypadek naruszenia jako incydent bezpieczeństwa oraz sporządza raport, który zawiera w szczególności:
   a) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób, które złożyły wyjaśnienia w związku z naruszeniem;
   b) określenie czasu i miejsca naruszenia oraz powiadomienia o naruszeniu;
   c) określenie rodzaju naruszenia i okoliczności mu towarzyszących;
   d) wyszczególnienie uwzględnionych przesłanek wyboru metody postępowania i opis podjętego działania;
   e) wstępną ocenę przyczyn wystąpienia naruszenia;
   f) ocenę przeprowadzonego postępowania wyjaśniającego i działań podjętych w celu usunięcia naruszenia i jego skutków.

3. Po przywróceniu prawidłowego funkcjonowania systemu informatycznego, Administrator danych przeprowadza szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz podejmuje kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

XI. Procedura postępowania w przypadku zgłoszenia żądania dostępu do danych osobowych

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora danych

potwierdzenia, czy Przedsiębiorca przetwarza dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

a) cele przetwarzania;
b) kategorie odnośnych danych osobowych;
c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
e) 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;
f) informacje o prawie wniesienia skargi do organu nadzorczego;
g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu –w tym przypadku – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Administrator danych niezwłocznie potwierdza otrzymanie zgłoszenia żądania dostępu do danych osobowych.

3. Żądanie zostaje odnotowane w systemie informatycznym Administratora danych oraz zostaje mu nadany dalszy bieg.

4. Administrator po otrzymaniu żądania powinien zbadać treść żądania pod kątem spełniania przez niego wymogów, tj. tego, czy wynika z jego treści, kto go wnosi oraz czego żąda, w przypadku gdy żądanie nie może zostać zrealizowane – wezwać osobę zgłaszającą żądanie do uzupełnienia jego braków w terminie nie krótszym niż 14 dni z pouczeniem że nieuzupełnienie żądania w określonym terminie spowoduje pozostawienie żądania bez rozpoznania.

5. Żądanie nieuzupełnione pozostawia się bez rozpoznania.

6. Realizacja żądania polega na poinformowaniu osoby, czy Przedsiębiorca przetwarza jej dane oraz poinformowaniu osoby o szczegółach przetwarzania, a także udzieleniu osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych.

7. Na żądanie Przedsiębiorca wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

8. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu bez pobierania kosztów. Za wszelkie kolejne kopie, o które zwróci się osoba,

której dane dotyczą, Administrator danych może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.

9. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się drogą elektroniczną.

10. Prawo do uzyskania kopii danych nie może niekorzystnie wpływać na prawa i wolności innych osób.

XII. Procedura postępowania w przypadku zgłoszenia sprzeciwu, cofnięcia zgody, żądania sprostowania i uzupełnienia danych

1. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego osoba, której dane dotyczą może wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie w jakim przetwarzanie jest związane z takim marketingiem. Sprzeciw wobec przetwarzania danych osobowych może być wyrażony w dowolnej formie – ustnie, pisemnie za pośrednictwem poczty, pocztą elektroniczną czy z wykorzystaniem profilu w mediach społecznościowych.

2. Administrator danych niezwłocznie potwierdza adresatowi otrzymanie sprzeciwu.

3. Sprzeciw zostaje odnotowany w systemie informatycznym Administratora danych oraz zostaje mu nadany dalszy bieg.

4. Administrator danych powinien zbadać treść sprzeciwu pod kątem spełniania przez niego wymogów, tj. tego, czy wynika z jego treści, kto go wnosi oraz czego żąda, w przypadku gdy sprzeciw nie może zostać zrealizowany – wezwać osobę zgłaszającą sprzeciw do uzupełnienia jego braków terminie nie krótszym niż 14 dni z pouczeniem że nieuzupełnienie sprzeciwu w określonym terminie spowoduje pozostawienie sprzeciwu bez rozpoznania.

5. W przypadku wątpliwości odnośnie do zakresu sprzeciwu należy:
   a) stwierdzić, w jakiej części żądanie sprzeciwu jest jasne – i niezwłocznie tę część sprzeciwu zrealizować, tj. zaprzestać przetwarzania danych osobowych w zakresie niebudzącym wątpliwości;
   b) stwierdzić, w jakiej części żądanie sprzeciwu nie jest jasne lub nie daje się wykonać z przyczyn obiektywnych i niezwłocznie odpowiedzieć na sprzeciw.

6. Odpowiedź powinna zawierać informację o tym, w jakim zakresie sprzeciw został już wykonany, a w jakim zakresie administrator danych prosi o doprecyzowanie sprzeciwu.

7. Sprzeciw nieuzupełniony pozostawia się bez rozpoznania.

8. Realizacja sprzeciwu polega na zidentyfikowaniu, jakie procesy u Administratora danych opierają się na przetwarzaniu danych osobowych w zakresie objętym sprzeciwem oraz na wylistowaniu wszystkich takich procesów oraz na skierowaniu do ich dysponentów informacji o konieczności zaprzestania przetwarzania danych osobowych.

9. Sprzeciw może być wniesiony w każdym czasie i nie ma znaczenia to, że podmiot danych wcześniej zgodził się na przetwarzanie jego danych.

10. Po wniesieniu sprzeciwu kontynuowanie przetwarzania danych osobowych jest niedopuszczalne. Administrator danych powinien natychmiast zaprzestać przetwarzania. Może sobie jednak pozostawić dane identyfikujące jednoznacznie osobę, która zgłosiła sprzeciw (imię, nazwisko, PESEL, adres), ale jedynie na potrzeby uniknięcia ponownego przetwarzania danych tej osoby.

11. Procedurę postepowania w zakresie sprzeciwu stosuje się odpowiednio w przypadku cofnięcia zgody, żądania sprostowania i uzupełnienia danych.

12. Przedsiębiorca uzupełnia i aktualizuje dane na żądanie osoby. Przedsiębiorca ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Przedsiębiorca nie musi przetwarzać danych, które są Przedsiębiorcy zbędne). Przedsiębiorca może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Przedsiębiorcę procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

13. Przedsiębiorca dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Przedsiębiorca ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Przedsiębiorca informuje osobę o odbiorcach danych, na żądanie tej osoby.

14. Komunikacja z osobą zgłaszającą żądanie jest wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Administrator danych może:
    a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
    b) odmówić podjęcia działań w związku z żądaniem.

XIII. Procedura postępowania w przypadku zgłoszenia żądania przeniesienia danych

1. Przeniesienie danych osobowych może nastąpić wyłącznie w przypadku, gdy przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą oraz w sposób zautomatyzowany.

2. W przypadku zgłoszenia żądania przeniesienia danych należy powiadomić osobę o przyjęciu takiego zgłoszenia.

3. Przedsiębiorca dokonuje analizy zgłoszenia, a w przypadku braków wzywa do uzupełnienia zgłoszenia.

4. Jeżeli wykonanie żądania przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), Przedsiębiorca może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

5. Przedsiębiorca informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

6. Komunikacja z osobą zgłaszającą żądanie jest wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Administrator danych może:
   a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
   b) odmówić podjęcia działań w związku z żądaniem.

XIV. Procedura postępowania w przypadku zgłoszenia żądania usunięcia danych

1. W przypadku zgłoszenia żądania usunięcia danych należy powiadomić osobę o przyjęciu takiego zgłoszenia.

2. Przedsiębiorca dokonuje analizy zgłoszenia, a w przypadku braków wzywa do uzupełnienia zgłoszenia.

3. Na żądanie osoby, Przedsiębiorca usuwa dane, gdy:
   a) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
   b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
   c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
   d) dane były przetwarzane niezgodnie z prawem,
   e) konieczność usunięcia wynika z obowiązku prawnego,
   f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

4. W przypadku usunięcia danych Przedsiębiorca informuje osobę o odbiorcach danych, na żądanie tej osoby.

5. Przedsiębiorca informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

7. Komunikacja z osobą zgłaszającą żądanie jest wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Administrator danych może:
   a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
   b) odmówić podjęcia działań w związku z żądaniem.

XV. Ograniczenie przetwarzania

1. Przedsiębiorca dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
c) Przedsiębiorca nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Przedsiębiorcy zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

2. W trakcie ograniczenia przetwarzania Przedsiębiorca przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

3. Przedsiębiorca informuje osobę przed uchyleniem ograniczenia przetwarzania.

4. W przypadku ograniczenia przetwarzania danych Przedsiębiorca informuje osobę o odbiorcach danych, na żądanie tej osoby.

XVI. Zasady rozpowszechniania Wewnętrznej Polityki Bezpieczeństwa

1. Z treścią niniejszego dokumentu zapoznawane są wszystkie osoby wykonujące usługi na rzecz Przedsiębiorcy.

2. Z treścią dokumentów uzupełniających niższego poziomu tj. regulaminów, zasad, procedur i instrukcji zapoznane są osoby wykonujące usługi na rzecz Przedsiębiorcy w zakresie niezbędnym do realizacji powierzonych zadań.

XVII. Zasady dokonywania zmian w niniejszym dokumencie

1. Niniejsza Wewnętrzna Polityka Bezpieczeństwa i dokumenty związane są tworzone i rozwijane w zgodzie z systemem zarządzania bezpieczeństwem informacji. Oznacza to, że fakty wystąpienia poważnych incydentów w dziedzinie bezpieczeństwa będą

skutkowały zmianami w dokumencie niniejszej Polityki i dokumentach związanych albo innymi niezbędnymi działaniami.

2. Ponadto, niniejsza Wewnętrzna Polityka Bezpieczeństwa i inne dokumenty związane mogą podlegać zmianie w przypadku:
   a) ogłoszenia nowych lub modyfikacji istniejących przepisów prawa,
   b) przekazania istotnych uwag przez odbiorców Polityki,
   c) powstania zaleceń poaudytowych,
   d) zmian organizacyjnych,
   e) zmian zakresu świadczenia usług.