Polityka prywatności

I. Informacje ogólne.

1. Administratorem danych osobowych jest **Miko-Tech Spółka z ograniczoną odpowiedzialnością** w Łaziskach Górnych, zarejestrowana w Sądzie Rejonowym Katowice-Wschód w Katowicach VIII Wydział Gospodarczy KRS pod numerem KRS: 0000362835, 43-170 Łaziska Górne, ul. Świętego Jana Pawła II 11B, NIP: 6351814493, REGON: 241686516, kapitał zakładowy: 50 000,00 PLN (dalej również „Spółka"). Można się z nami skontaktować w następujący sposób:

- listownie na adres: 43-170 Łaziska Górne, ul. Świętego Jana Pawła II 11B
- przez e-mail: info@miko-tech.pl

2. Nie powołaliśmy Inspektora Ochrony Danych. Jeśli taka osoba zostanie powołana, powiadomimy Państwa o tym. Wyznaczyliśmy osobę zajmującą się przetwarzaniem danych osobowych oraz korzystania z praw z tym przetwarzaniem związanych tj.: Maria Raczyńska

Z w/w osobą można kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw z tym przetwarzaniem związanych, w następujący sposób:

- listownie na adres: 43-170 Łaziska Górne, ul. Świętego Jana Pawła II 11B
- przez e-mail: mraczynska@miko-tech.pl

3. Spółka nie przekazuje danych osobowych poza EOG (tj. obszar obejmujący UE, Islandię, Liechtenstein oraz Norwegię). W przypadku, gdy Spółka podejmie decyzję o przekazaniu danych poza EOG zostanie to dokonane wyłącznie na warunkach i w zakresie, na jaki zezwoli prawo.
4. Posiadają Państwo prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. W przypadku, gdy przetwarzamy Twoje dane na podstawie naszego prawnie uzasadnionego interesu masz prawo zgłoszenia sprzeciwu względem przetwarzania danych. Możesz to zrobić kontaktując się z nami za pośrednictwem adresu e-mail: info@miko-tech.pl
W zakresie, w jakim Twoje dane przetwarzane są na podstawie zgody, możesz tę zgodę wycofać w dowolnym momencie, kontaktując się z nami poprzez adres e-mail: info@miko-tech.pl. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem.
5. Państwa dane osobowe będą przechowywane przez okres istnienia prawnie uzasadnionego interesu administratora, chyba że Pani / Pan wyrazi sprzeciw wobec przetwarzania danych.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

I. WSTĘP

Polityka bezpieczeństwa danych osobowych jest zestawem praw, zasad i rozwiązań regulujących przetwarzanie danych osobowych w Spółce i została przygotowana w oparciu o RODO.

Zasadniczym celem zastosowania niniejszego dokumentu jest wyznaczenie standardów bezpieczeństwa odpowiednich do funkcjonowania organizacji w erze cyfrowej, w tym stworzenie gwarancji zapewnienia ochrony danych osobowych, przetwarzanych w celu usprawiedliwionym prowadzoną działalnością.

Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Zarząd Spółki oraz osoba wyznaczona przez Zarząd do zapewnienia zgodności z ochroną danych osobowych, tj. Koordynator ds. danych osobowych – w przypadku wyznaczenia takiej osoby.

W Spółce nie powołano Inspektora Ochrony Danych Osobowych.

Spółka powinna też zapewnić zgodność postępowania kontrahentów Spółki z niniejszą polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez Spółkę.

II. DEFINICJE

Dane – dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.
Eksport danych – przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.
Osoba – osoba, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
Podmiot przetwarzający – organizacja lub osoba, której Spółka powierzyła przetwarzanie danych osobowych.
Polityka – niniejsza Polityka ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
RCPD – Rejestr Czynności Przetwarzania Danych Osobowych.
RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (Dz. Urz. UE L 119, s. 1).
Spółka – administrator Danych Osobowych, tj. Miko-Tech Spółka z ograniczoną odpowiedzialnością w Łaziskach Górnych, zarejestrowana w Sądzie Rejonowym Katowice-Wschód w Katowicach VIII Wydział Gospodarczy KRS pod numerem KRS: 0000362835, 43-170 Łaziska Górne, ul. Świętego Jana Pawła II 11B, NIP: 6351814493, REGON: 241686516, kapitał zakładowy: 50 000,00 PLN.
UODO – Urząd Ochrony Danych Osobowych.

III. ZASADY OCHRONY DANYCH OSOBOWYCH

Zasady ochrony danych osobowych stanowią:

1. Legalizm – przetwarzanie danych osobowych w oparciu o podstawę prawną i zgodnie z prawem,
2. Rzetelność – przetwarzanie danych osobowych rzetelnie i uczciwie,
3. Transparentność – przetwarzanie danych osobowych w sposób przejrzysty dla osoby, której dotyczą,
4. Minimalizacja – przetwarzanie danych osobowych w konkretnych celach,
5. Adekwatność – przetwarzanie danych osobowych w stopniu wystarczającym do realizacji celu,
6. Prawidłowość – przetwarzanie danych osobowych z dbałością o prawidłowość danych,
7. Czasowość – przetwarzanie danych osobowych nie dłużej niż zachodzi taka potrzeba,
8. Bezpieczeństwo – przetwarzanie danych osobowych zapewniając bezpieczeństwo danych,

9. Rozliczalność – przetwarzanie danych osobowych w sposób zapewniający przypisanie działań określonej osobie,
10. Poufność – przetwarzanie danych osobowych w sposób zapewniający, że dane nie zostaną udostępniane osobom nieupoważnionym,
11. Integralność – przetwarzanie danych osobowych w sposób zapewniający, że dane nie zostaną zmienione lub zniszczone w sposób nieautoryzowany,
12. Dostępność informacji – przetwarzanie danych osobowych w sposób zapewniający dostęp do informacji i związanych z nią zasobów wtedy, gdy jest do potrzebne.

IV. ZAKRES ZASTOSOWANIA

1. Polityka zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych.
2. Dane są przetwarzane w postaci dokumentacji tradycyjnej lub w formie elektronicznej.
3. Politykę stosuje się w szczególności do:

a) danych przetwarzanych w systemach komputerowych istniejących lub wdrażanych w przyszłości,
b) danych dotyczących pracowników, kandydatów do pracy, zleceniobiorców, klientów zebrane w zbiorach danych,
c) rejestru osób mających upoważnienie do przetwarzania danych,
d) odbiorców danych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia,
e) informacji dotyczących zabezpieczenia danych, w tym w szczególności kont i haseł w systemach przetwarzania danych,
f) innych dokumentów zawierających dane.

4. Dane gromadzone są w zbiorach określonych w RCPD.

V. ŚRODKI TECHNICZNE I ORGANIZACYJNE ZABEZPIECZENIA DANYCH

I. Spółka ustala zasady zabezpieczania i bezpiecznego przetwarzania danych w systemach informatycznych.

1) Zasady zabezpieczania i bezpiecznego przetwarzania danych obowiązują wszystkie osoby realizujące jakiekolwiek czynności w Spółce, niezależnie od podstawy wykonywania tych czynności, zwanych dalej „Pracownikami" i obejmują działania związane z zabezpieczeniami systemów informatycznych oraz postępowaniem mającym na celu zapewnienie poufności gromadzonych danych osobowych.
2) Spółka odpowiada za zapewnienie stosowania odpowiednich zabezpieczeń danych osobowych zbieranych w formie elektronicznej.
3) Spółka dąży do tego, żeby systemy informatyczne zachowały możliwość:
   a) pseudominizacji i szyfrowania danych osobowych,
   b) zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów informatycznych i usług przetwarzania,
   c) zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
4) Naprawa i konserwacja sprzętu komputerowego może odbywać się wyłącznie w warunkach zapobiegających dostęp do danych osobowych osób nieuprawnionych.
5) Po każdej naprawie i konserwacji komputera sprzęt jest sprawdzany pod kątem występowania wirusów i konieczności ponownego zainstalowania programu antywirusowego. Elektroniczne nośniki informacji pochodzenia zewnętrznego podlegają automatycznemu sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich.

6) Pracownicy nie są uprawnieni do instalacji jakiegokolwiek oprogramowania bez wcześniejszej wyraźnej zgody Spółki. W przypadku zainstalowania takiego oprogramowania bez odpowiedniej zgody Pracownik ponosi odpowiedzialność porządkową i materialną.
7) Oprogramowanie na komputerach może być zainstalowane wyłącznie przez osobę uprawnioną.
8) Pracownicy mogą używać połączenia z Internetem jedynie w celach służbowych i wyłącznie z przeznaczonych do tego celu komputerów.
9) Pracownicy nie mają prawa przekazywać za pośrednictwem sieci komputerowej do osób nieuprawnionych jakichkolwiek danych osobowych.
10) Pracownik ustawia monitor komputerowy w taki sposób, aby informacje na ekranie nie były widoczne dla osób postronnych i zawsze stosuje hasła dostępu, w szczególności monitor komputerowy nie może być odwrócony w stronę drzwi i okien.
11) Pracownik przy opuszczaniu stanowiska pracy wylogowuje się z systemów informatycznych.
12) Pracownik niezwłocznie informuje Spółkę w przypadku naruszenia lub zagrożenia bezpieczeństwa danych osobowych w systemach informatycznych.
13) Zarządzanie systemem informatycznym służącym do przetwarzania danych w zakresie nieuregulowanym przez Politykę, w tym dotyczącym zarządzaniem prawami dostępu do systemu informatycznego, zarządzaniem hasłami dostępu, prowadzenie listy użytkowników systemu informatycznego, zabezpieczenia serwerowni, tworzenia kopii zapasowych, ograniczenia dostępu do stron internetowych zawierających treści szkodliwe, instalacji programów antywirusowych i ich aktualizacji, odbywa się na zasadach określonych w regulacjach Spółki dotyczących zarządzania systemem informatycznym, w tym w Polityce bezpieczeństwa systemu informatycznego.

II. Spółka ustala organizacyjne zasady zabezpieczania i bezpiecznego przetwarzania danych.

1) Nadano pracownikom, współpracownikom, praktykantom i stażystom upoważnienia do przetwarzania danych.
2) Podpisano umowy powierzenia danych z podmiotami współpracującymi.
3) Przygotowano procedurę postępowania na wypadek naruszenia ochrony danych.
4) Przygotowano i wdrożono RCPD.
5) Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Spółkę.
6) Osoby zatrudnione przy przetwarzaniu danych obowiązane zostały do zachowania ich w tajemnicy.
7) Przetwarzanie danych odbywa się w sposób zabezpieczający dane przed dostępem do nich osób nieupoważnionych.
8) Przebywanie osób nieuprawnionych w pomieszczeniach, w których przetwarzane są dane osobowe, dopuszczalne jest tylko w obecności osoby upoważnionej oraz w warunkach zapewniających bezpieczeństwo danych.
9) Dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych. ewentualnie przeprowadza się taką ich modyfikację, która w sposób trwały nie pozwoli na odtworzenie ich treści.
10) Spółka zapewnia szkolenia pracowników w zakresie ochrony i przetwarzania danych.
11) Obszar Spółki częściowo objęty jest monitoringiem wizyjnym.
12) Urządzenia służące do przetwarzania danych umieszczone są w zamykanych pomieszczeniach.
13) Dokumenty i nośniki informacji zawierające dane przechowywane są w zamykanych na klucz szafkach.

VI. ZADANIA ADMINISTRATORA DANYCH

Administratorem danych jest Spółka, do której zadań należy:

1. Organizacja bezpieczeństwa i ochrony danych zgodnie z wymaganiami RODO i innymi powszechnie obowiązującymi przepisami prawa.

2. Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki i innymi dokumentami dotyczącymi przetwarzania danych.
3. Przeprowadzenie oceny skutków planowanej operacji dla ochrony danych – w przypadku, gdy organizacja wprowadza nowy rodzaj przetwarzania danych wymagający takiej oceny.
4. Wydawanie i cofanie upoważnień do przetwarzania danych.
5. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych.
6. Nadzór nad bezpieczeństwem przetwarzania danych.

VII. REJESTR CZYNOŚCI PRZETWARZANIA DANYCH

1. RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych, czyli zasady rozliczalności.
2. Spółka prowadzi RCPD, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane.
3. RCPD jest jednym z podstawowych narzędzi umożliwiających Spółce rozliczanie większości obowiązków ochrony danych.
4. W RCPD dla każdej czynności przetwarzania danych, którą Spółka uznała za odrębną dla potrzeb RCPD, Spółka odnotowuje: nazwę czynności przetwarzania danych osobowych, cel przetwarzania danych osobowych, kategorie osób, których dane są przetwarzane, kategorie przetwarzanych danych osobowych, odbiorcy danych osobowych, planowany termin usunięcia danych osobowych, środki ochrony danych osobowych, transfer do państwa trzeciego, kategorie transferowanych danych, odbiorcy danych, państwo trzecie, podstawa prawna transferu, dokumentacja odpowiednich zabezpieczeń.

VIII. OBSŁUGA PRAW JEDNOSTKI

1. Spółka dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
2. Spółka ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej Spółki informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Spółce, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu ze Spółką w tym celu.
3. Spółka dba o dotrzymanie terminów realizacji obowiązków względem osób uprawnionych.
4. Spółka określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
5. Spółka informuje osobę o przedłużeniu o ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
6. Spółka informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
7. Spółka określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie jest to możliwe (np. informacja o objęciu obszaru monitoringiem wizyjnym).
8. Spółka informuję osobę o planowanej zmianie celu przetwarzania danych.
9. Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania danych.
10. Spóła informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba, że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
11. Spółka informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z osobą.
12. Spółka bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.
13. Spółka informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

14. Spółka informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
15. Na żądanie osoby dotyczące dostępu do jej danych Spółka informuję osobę, czy przetwarza jej dane, oraz informuję osobę o szczegółach przetwarzania, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być realizowany przez wydanie kopii danych. Na żądanie Spółka wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Spółka może pobierać opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest na podstawie oszacowanego jednostkowego kosztu wydania kopii danych.
16. Spółka dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Spółka ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Spółka może polegać na oświadczeniu osoby co do uzupełniających danych, chyba że będzie to niewystarczające, aby uznać takie oświadczenie za wiarygodne.
17. Na żądanie osoby Spółka usuwa dane, gdy:
    a. Dane nie są niezbędne dla celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach.
    b. Zgoda na ich przewarzanie 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 danych wynika z obowiązku prawnego.
18. Spółka 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, żądając w zamian ograniczenia ich wykorzystywania.
    c. Spółka nie potrzebuje już żadnych danych, ale są one potrzebne osobie, której 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 Spółki zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
19. W trakcie ograniczenia przetwarzania Spółka przechowuje dane, natomiast nie przetwarza ich 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. Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania danych. W przypadku ograniczenia przetwarzania danych Spółka informuje osobę o odbiorcach danych, na jej żądanie.
20. Na żądanie osoby Spółka wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Spółce, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych.
21. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Spółkę w oparciu o uzasadniony interes Spółki lub o powierzone Spółce zadanie w interesie publicznym, Spółka uwzględni sprzeciw, o ile nie zachodzą po stronie Spółki ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
22. Jeżeli Spółka prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może wnieść umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. Spółka uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.
23. Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Spółkę na potrzeby marketingu bezpośredniego, Spółka uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

24. Jeżeli Spółka przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Spółka zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie Spółki, chyba że taka automatyczna decyzja: jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Spółką, lub jest wprost dozwolona przepisami prawa, lub opiera się na wyraźniej zgodzie odwołującej osoby.

IX. EKSPORT DANYCH

1. Spółka rejestruje w RCPD przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy.
2. Aktualnie Spółka nie eksportuje danych poza Europejski Obszar Gospodarczy.

X. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH

1. W przypadku naruszenia ochrony danych, Spółka bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je UODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego UODO po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Zgłoszenie, o którym mowa w Punkt X ppkt 1, powinno zwierać co najmniej: opis charakteru naruszenia ochrony danych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; imię i nazwisko oraz dane kontaktowe IODO lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; możliwe konsekwencje naruszenia ochrony danych; środków zastosowanych lub proponowanych przez spółkę w celu zaradzenia naruszeniu ochrony danych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków. Jeżeli wszystkich informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
3. Spółka dokumentuje wszelkie naruszenia ochrony danych, w tym okoliczności naruszenia ochrony danych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego Punktu.
4. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Spółka bez zbędnej zwłoki zawiadamia osobę jasnym i prostym językiem o takim naruszeniu. Zawiadomienie powinno opisywać charakter naruszenia ochrony danych oraz zawierać przynajmniej następujące informacje: imię i nazwisko oraz dane kontaktowe IODO lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; możliwe konsekwencje naruszenia ochrony danych; środków zastosowanych lub proponowanych przez Spółkę w celu zaradzenia naruszeniu ochrony danych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
5. Zawiadomienie, o którym mowa w Punkt 10 ppkt 4, nie jest wymagane w następujących przypadkach:
   a) Spółka wdrożyła odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   b) Spółka zastosowała następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   c) 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.

XI. POSTANOWIENIA KOŃCOWE

Załączniki do Polityki stanowią:

1. Rejestr Czynności Przetwarzania Danych Osobowych (RCPD)
2. Rejestr Kategorii Czynności Przetwarzania Danych Osobowych (RKCPD)
3. Wzory umów powierzenia przetwarzania danych osobowych.
4. Wzór upoważnienia do przetwarzania danych osobowych.
5. Wzory klauzul informacyjnych.
6. Rejestr osób upoważnionych do przetwarzania danych osobowych.
7. Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych.
8. Raport z naruszenia ochrony danych osobowych.
9. Rejestr naruszeń ochrony danych osobowych.
10. Instrukcja zarządzania systemem informatycznym.
11. Procedura realizacji żądań podmiotu danych.
12. Oświadczenie o niepowołaniu Inspektora Ochrony Danych.
13. Plan audytów i szkoleń.