POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

RETRANS T. Baran, M. Kapcia Sp.j.

adres: Regulice, ul. Transportowa 29

32-566 Alwernia, woj. małopolskie

Regulice, dnia 25.05.2018 r.

SPIS TREŚCI:

• POSTANOWIENIA OGÓLNE

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 zabezpieczania danych w *RETRANS T. Baran, M. Kapcia Sp.j. z siedzib Regulice, ul. Transportowa 29*, *w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (EU) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związki z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).*

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w RETRANS T. Baran, M. Kapcia sp.j. z siedzibą Regulice, ul. Transportowa 29, niezależnie od formy ich przetwarzania (min. przetwarzane tradycyjne zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Polityka, odpowiednio zabezpieczona, jest przechowywana w wersji elektronicznej w odrębnym folderze pod nazwą RODO RETRANS T. Baran, M. Kapcia sp.j. z siedzibą Regulice, ul. Transportowa 29, w systemie informatycznym oraz w wersji papierowej w siedzibie Administratora.
3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek wyrażony w sposób dowolny, ale jednoznaczny, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z ich treścią.
4. Dane osobowe przetwarzane w RETRANS T. Baran, M. Kapcia sp.j. z siedzibą Regulice, ul. Transportowa 29, stanowią niematerialne składniki przedsiębiorstwa, w rozumieniu art. 55^1 kodeksu cywilnego oraz art. 11 ust. 4 ustawy o zwalczaniu nieuczciwej konkurencji, w związku z czym objęte są tajemnicą przedsiębiorstwa. Dane osobowe, stanowiące określoną wartość gospodarczą, są poufne i odpowiednio zabezpieczone przed ich upublicznieniem.
5. Zakres przedmiotowy stosowania Polityki bezpieczeństwa obejmuje wszystkie zbiory danych osobowych przetwarzanych w Przedsiębiorstwie.
6. Zakres podmiotowy Polityki Bezpieczeństwa obowiązuje wszystkich Użytkowników, w tym pracowników lub współpracowników, oraz inne osoby mające dostęp do Danych osobowych, w tym stażystów, pracowników gospodarczych, osoby zatrudnione na umowę o dzieło lub umowę zlecenie oraz inne osoby realizujące zadania w Przedsiębiorstwie wynikające z profilu działalności.
7. Dla skuteczności realizacji Polityki Administrator Danych Osobowych zapewnia:
   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
   b) stałą kontrolę i nadzór nad Przetwarzaniem danych osobowych w przedsiębiorstwie,
   c) monitorowanie zastosowanych środków, w tym ocenę skuteczności zastosowanych środków, modernizowanie zastosowanych środków w związku ze zmianami organizacyjnymi w przedsiębiorstwie lub zmianami w obowiązujących przepisach prawa, czynnościami Użytkowników, analizę naruszania zasad dostępu do danych, zapewnienie integralności gromadzonych plików oraz ochronę przed atakami zewnętrznymi i wewnętrznymi.
8. Administrator danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczaniem danych osobowych są zgodne z niniejszą Polityką Bezpieczeństwa oraz odpowiednimi przepisami prawa.
9. Administrator Danych Osobowych deklaruje zaangażowanie w prawidłowym zarządzaniu bezpieczeństwem informacji w Przedsiębiorstwie oraz oświadcza, że dołoży wszelkich możliwych starań celem zapewnienia bezpieczeństwa informacji.
10. Celem Polityki Bezpieczeństwa jest zapewnienie standardów bezpieczeństwa informacji

zawierających dane osobowe, ze szczególnym uwzględnieniem zgodności z przepisami prawa.

- **DEFINICJE**

1. Administrator Danych Osobowych – RETRANS T. Baran, M. Kapcia sp.j. z siedzibą Regulice, ul. Transportowa 29 reprezentowany przez Wspólników Spółki i osób upoważnionych
2. Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej w rozumieniu Rozporządzenia.
3. Hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie.
4. Identyfikator użytkownika - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie.
5. Przetwarzanie danych - jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych.
6. RODO - *Rozporządzenie Parlamentu Europejskiego i Rady (EU) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związki z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).*
7. System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji, narzędzi programowych zastosowanych w celu przetwarzania danych.
8. Uwierzytelnianie - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika).
9. Użytkownik - osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych.
10. Zbiór danych - każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów.

- **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 art. 36 RODO.
3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
4. Administrator danych prowadzi zbiór czynności przetwarzania. Zbiór czynności przetwarzania stanowi załącznik do niniejszej polityki.
5. Rekrutacja pracowników odbywa się za pośrednictwem systemu informatycznego (wiadomości e-mail) oraz w wersji papierowej. Dane osobowe kandydatów gromadzone są w zbiorze, zabezpieczonym w wersji papierowej w zamykanej szafie, do której dostęp ma upoważniony Użytkownik. Dane osobowe kandydatów będą archiwizowane przez okres trzech miesięcy. Po upływie powyższego okresu dane osobowe kandydatów będą usuwane z systemu informatycznego, a w formie papierowej niszczone w firmowej niszczarce.

• 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 Polityką Bezpieczeństwa, Instrukcją Zarządzania Systemem Informatycznym, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych w RETRANS T. Baran, M. Kapcia sp.j. z siedzibą Regulice, ul. Transportowa 29. Wszystkie Dane osobowe w Przedsiębiorstwie są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
   a).W każdym wypadku, gdy występuje chociaż jedna z przewidzianych przepisami prawa podstaw do przetwarzania danych.
   b).Dane są przetwarzane rzetelnie i w sposób przejrzysty.
   c).Dane osobowe zbierane są w konkretnych, wyraźnie i prawnie uzasadnionych celach i przetwarzane dalej w sposób zgodny z tymi celami.
   d).Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych.
   e).Dane osobowe są prawidłowe i w razie potrzeby uaktualniane.
   f).Czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one animizowane bądź usuwane.
   g).Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 RODO i art. 14 RODO.
   h).Dane są zabezpieczone przed naruszeniami zasad ich ochrony.
3. Administrator Danych Osobowych nie przekazuje osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy przedsiębiorstwa (art. 14 ust. 5 pkt d. RODO).
4. 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 wprost nieupoważnionym.
   c). Zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia Danym osobowym ochrony.
   d).Niedopełnienie obowiązku zachowania tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia.
   e).Przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania.
   f).Spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych.
   g).Naruszenie praw osób, których dane są przetwarzane.
5. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony Danych osobowych Użytkownik jest obowiązany do podjecie wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych.
6. Do obowiązków Administratora Danych w zakresie zatrudniania, zmiany lub zakończenia stosunku pracy i innych form współpracy, jak również wobec innych osób podejmujących czynności na rzecz Administratora Danych niezależnie od łączącego strony stosunku umownego, w szczególności umów cywilnoprawnych, należy dopilnować, aby:
   a).Każdy z przetwarzających Dane osobowe był przygotowany do wykonywania swoich obowiązków.
   b).Każdy z przetwarzających Dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych" – załącznik do Polityki

Bezpieczeństwa.
c).Każdy z przetwarzających Dane osobowe zobowiązał się do zachowania tajemnicy Danych osobowych przetwarzanych w pisemnym oświadczeniu stanowiącym element składowy „Upoważnienia do przetwarzania danych osobowych" - Załącznik do Polityki Bezpieczeństwa.

7. Każdy z przetwarzających Dane osobowe jest obowiązany do:
a).Ścisłego przestrzegania zakresu nadanego upoważnienia.
b).Przetwarzania i ochrony Danych osobowych zgodnie z obowiązującymi przepisami prawa.
c).Zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia, również po zakończeniu współpracy niezależnie od rodzaju łączącego strony stosunku zobowiązaniowego,
d).Zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych, niezwłocznie nie później niż w czasie 24 godzin od momentu wykrycia naruszenia, zgłaszania incydentów niewłaściwego funkcjonowania systemu.
e).Przestrzegania tzw. zasady „czystego biurka" albowiem zabronione jest pozostawienie na stanowisku pracy jakichkolwiek dokumentów lub innych nośników danych zawierających Dane osobowe, po zakończeniu dnia pracy lub w trakcie czasowej nieobecności, która potencjalnie mogłaby umożliwić zapoznanie się z Danymi osobowymi przez osoby nieuprawnione.
8. Pracownik zewnętrznego serwisu informatycznego, któremu Administrator danych osobowych nadał upoważnienie do przetwarzania danych osobowych, w związku z koniecznością obsługi aplikacji kadrowo - płacowej jest zobowiązany do zachowania w tajemnicy nie tylko poznanych w ten sposób informacji osobowych, ale również wszelkich zasad bezpieczeństwa tej aplikacji i całego systemu informatycznego Przedsiębiorstwa. Obowiązek poufności nieustanie w momencie zakończenia współpracy lub upadłości Przedsiębiorstwa.

• OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

1. Obszar, w którym przetwarzane są Dane osobowe na terenie RETRANS T. Baran, M. Kapcia sp.j. z siedzibą Regulice, ul. Transportowa 29, obejmuje teren firmy zlokalizowany przy RETRANS T. Baran, M. Kapcia sp.j. z siedzibą Regulice, ul. Transportowa 29.
2. Obszar, w którym przetwarzane są Dane osobowe, stanowią również wszystkie urządzenia przenośne oraz inne nośniki danych, w tym komputery, telefony komórkowe, pendrive przekazane Użytkownikom na czas trwania współpracy lub jednorazowo, niezależnie od miejsca i sposobu korzystania z urządzeń.
3. W przypadku korzystania z komputerów przenośnych zawierających dane osobowe należy zachować szczególną ostrożność podczas używania komputera poza obszarem przetwarzania danych opisanych w Polityce Bezpieczeństwa. W szczególności należy stosować mechanizmy szyfrowania uruchomienia urządzenia, wygaszania ekranu komputera, dostępu do plików lub baz danych. Po ustaniu konieczności przetwarzania danych na komputerze przenośnym, należy je niezwłocznie trwale usunąć z nośnika danych. Zapisu danych obejmujących przetwarzanie Danych osobowych, należy dokonywać w systemie sieciowym, uwzględniającym wykonywanie kopii zapasowych.
4. Dane osobowe dotyczące przedsiębiorców – osób fizycznych, zgromadzone na zewnętrznych nośnikach danych, będą przetwarzane przez osoby upoważnione w okresie wykonywania ich obowiązków wynikających z umowy.
5. Pomieszczenia muszą być zabezpieczone przed dostępem osób nieupoważnionych lub osób trzecich.
7. Nośniki informacji zawierające dane osobowe muszą być przechowywane w odpowiednio zabezpieczonym miejscu przed dostępem osób nieupoważnionych lub osób trzecich.

• OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH. SYSTEM ZABEZPIECZENIA DANYCH.

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych, albowiem celem zabezpieczenia zbiorów Danych osobowych jest uniemożliwienie dostępu do Danych osobowych osobom nieupoważnionym.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych. Środki obejmują w szczególności:
   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 wyraźnie upoważnionej.
   b).Zamykanie pomieszczeń tworzących obszar Przetwarzania Danych osobowych określony w pkt V. Polityki na czas nieobecności Użytkowników w sposób uniemożliwiający w jakikolwiek dostęp do nich osób trzecich.
   c).Wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających Dane osobowe albowiem Dane osobowe w wersji papierowej, a także wydruki i kopie, należy niszczyć w stopniu uniemożliwiającym ich późniejsze odtworzenie, najlepiej w niszczarkach lub przekazywać do zniszczenia wynajętej do tego celu firmie. Zabronione jest usuwanie danych przez wyrzucenie ich do kosza na odpadki.
   d).Ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz odbywa się przy użyciu sieci firewall, ochrony antywirusowej oraz jej aktualizacji,
   e).Wykonywanie kopii awaryjnych danych w Systemie informatycznym.
   f).Ochronę sprzętu komputerowego wykorzystywanego u Administratora przed tzw. złośliwym oprogramowaniem.
   g).Zabezpieczenie dostępu do wszystkich urządzeń przy pomocy haseł dostępu.
   h).Autoryzacja Użytkowników hasłami o wysokim stopniu skomplikowania, okresowa zmiana hasła dokonywana przez każdego Użytkownika.
   i).Zabezpieczenie systemu informatycznego zgodnie z Instrukcją Zarządzania Systemem Informatycznym i kolejnymi zmianami.
   j).Aktualizacje Instrukcji Zarządzania Systemem Informatycznym, stosownie do zmiany okoliczności istotnych dla zwiększenia bezpieczeństwa przetwarzanych Danych osobowych.
   k).W przypadku nośnika zawierającego dane osobowe (papier, dysk twardy, płyta kompaktowa, dyskietka, taśma magnetyczna) przekazywanego podmiotowi nieupoważnionemu do przetwarzania danych w celu np. naprawy, likwidacji lub innym, należy zapewnić trwałe usunięcie Danych osobowych informacji stanowiących dane osobowe, lub zawarcie umowy o powierzenie przetwarzania danych osobowych.
   l).Zabezpieczenia techniczne związane ze stanowiskiem lub stanowiskami i wykonywanymi obowiązkami (min. monitoring wizyjny, zamki, szafki zamykane na klucz, sejfy na klucze, pokoje zamykane na kartę).
   ł).Zabezpieczenie połączeń w sieci wewnętrznej, oraz w sieci zewnętrznej (sieć Internet).
   m).ochrona przeciwpożarowa, zabezpiecznia BHP, Poż.
   n).całodobowy dozór terenu przedsiębiorstwa (firma zewnętrzna)
3. Mechanizm zabezpieczenia i uwierzytelnienia Użytkowników oraz procedury postępowania, w tym procedurę zarządzania uprawnieniami do systemów informatycznych szczegółowo określa Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia wymogów bezpieczeństwa

informacji.

• NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH.

1. W przypadku stwierdzenia naruszenia ochrony Danych osobowych Administrator dokonuje niezwłocznie oceny, czy zaistniałe naruszenie spowodowało lub mogło spowodować ryzyko naruszenia praw lub wolności osób fizycznych, następnie podejmuje czynności przewidziane przepisami RODO oraz aktami wewnętrznymi, w celu zminimalizowania ryzyka naruszenia Danych osobowych.
2. W każdej sytuacji, w której zaistniałe naruszenie spowodowało lub mogło spowodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych osobowych organowi nadzorczemu bez zbędnej zwłoki - jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, w szczególności, gdy spowodowałoby naruszenie dóbr osobistych, której dane dotyczą Administrator zawiadamia o incydencie także uprawnionego.
4. Każda osoba upoważniona do przetwarzania Danych osobowych, niezależnie od rodzaju przetwarzanych Danych osobowych, w zakresie swoich obowiązków czy obowiązków innych Użytkowników lub osób trzecich, jest zobowiązana do informowania Administratora Danych Osobowych o wszelkich zauważonych lub nawet podejrzanych słabościach procesu przetwarzania danych osobowych, w szczególności o:

a). Naruszeniu hasła i identyfikatora, uprawniających do pracy w systemie informatycznym.
b). Częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień.
c). Braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera.
d). Naruszaniu zasad ochrony przetwarzanych Danych osobowych przez innych Użytkowników lub osoby trzecie.

• POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych Osobowych może powierzyć przetwarzanie Danych osobowych innemu podmiotowi wyłącznie w drodze umowy o powierzenie przetwarzania danych zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO oraz w zakresie, w jakim nie jest to wyłączone z mocy przepisów prawa.
2. Przed zawarciem umowy powierzenia danych osobowych do przetwarzania podmiotowi zewnętrznemu należy bezwzględnie potwierdzić, czy spełnia on wymogi w zakresie zabezpieczeń organizacyjno – technicznych oraz dokumentacji procesu przetwarzania danych, gwarantując właściwy poziom ochrony interesów osób, których dane dotyczą.

• ODPOWIEDZIALNOŚĆ

1. Administrator Danych Osobowych zabezpiecza dane osobowe przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa obowiązujących w tym zakresie, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator Danych – odpowiedzialny jest za:

• nadzorowanie fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe oraz kontroli przebywających w nich osób,

• nadzorowanie przestrzegania zasad określonych w Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatyczny, dotyczących ochrony bezpieczeństwa danych osobowych,

- nadzorowanie wykonywania kopii zapasowych, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
- nadzorowanie przeglądów, konserwacji oraz uaktualnień systemów służących do przetwarzania danych osobowych oraz wszystkich innych czynności wykonywanych na bazach danych osobowych,
- nadzorowanie systemu komunikacji w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji (e-mail i in.),
- nadzorowanie funkcjonowania mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontroli dostępu do danych osobowych,
- podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń tego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,
- zlecenie modyfikacji uprawnień w systemach informatycznych w przypadku odebrania lub zmiany upoważnienia do przetwarzania danych osobowych,
- szkolenie osób dopuszczonych do przetwarzania danych osobowych z zakresu obowiązujących przepisów prawa oraz uregulowań wewnętrznych dotyczących bezpieczeństwa tych danych, lub zlecenie czynności podmiotowi zewnętrznemu,
- nadzorowanie zawierania umów o przetwarzanie danych osobowych z podmiotami zewnętrznymi, w tym przetwarzanie Danych osobowych przez pracowników firm w fazie realizacji i po zakończeniu współpracy, którym powierzono przetwarzanie danych osobowych lub podejmowanie jakichkolwiek czynności obejmujących przetwarzanie Danych osobowych, w tym min. konserwację urządzeń służących do przetwarzania Danych osobowych.
- odpowiedzialność za zawarcie w umowach z podmiotami zewnętrznymi odpowiednich zapisów dotyczących ochrony Danych osobowych, w zakresie w którym ochrona danych osobowych nie wynika z przepisów ustawowych.

• ZMIANY I UDOSTĘPNIENIE TEKSTU POLITYKI BEZPIECZEŃSTWA

1. Polityka Bezpieczeństwa podlega przeglądowi pod kątem aktualności i stosowalności nie rzadziej niż raz do roku. Audytu dokonuje Administrator Danych Osobowych osobiście, lub profesjonalny podmiot zewnętrzny na zlecenie Administratora Danych Osobowych.
2. Polityka Bezpieczeństwa podlega aktualizacji każdorazowo w przypadku:
- utworzenia, zmiany lub likwidacji zawartości informacyjnej zbioru,
- zmiany lokalizacji zbioru,
- zmiany przepisów prawa dotyczących ochrony danych osobowych,
- innych istotnych zmian dotyczących przetwarzania danych osobowych
3. Wprowadzenie zmian organizacyjnych w Przedsiębiorstwie wymaga aktualizacji zapisów w Polityce Bezpieczeństwa, w załącznikach do Polityki Bezpieczeństwa, lub w dokumencie Instrukcji Zarządzania Systemem Informatycznym.

• PRZEKAZYWANIE DANYCH DO PAŃSTWA TRZECIEGO

Administrator Danych Osobowych nie będzie przekazywał Danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą lub wynika to z przepisów prawa.

- **POSTANOWIENIA KOŃCOWE**

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu Użytkownik ponosi odpowiedzialność odpowiednio na podstawie Kodeksu pracy, przepisów o ochronie danych osobowych, Kodeksu karnego, ustawy o zwalczaniu nieuczciwej konkurencji lub innych przepisów prawa.
2. W celu wdrożenia w życie postanowień Polityki Bezpieczeństwa służącym do przetwarzania danych osobowych dokument ten będzie udostępniony wszystkim Użytkownikom w formie papierowej w siedzibie firmy.
3. Po zakończeniu etapu szkolenia o ochronie danych osobowych Użytkownik podpisuje stosowne oświadczenie, iż zapoznał się z treścią dokumentu oraz zobowiązuje się przestrzegać zasady Polityki bezpieczeństwa dotyczącej ochrony przetwarzania danych osobowych w Przedsiębiorstwie. Powyższa zasada obejmuje wszystkich nowych Użytkowników upoważnionych do przetwarzania danych osobowych.

Data Administrator Danych Osobowych

Numer wersji	Data zmiany	Zmiany wprowadził	Opis zmian
1	25.05.2018 r.		Opracowanie wersji ostatecznej
2	28.05.2018 r.		Aktualizacja