# POLITYKA BEZPIECZEŃSTWA

**SUPERSTACJA SP. Z O.O.**

**AL. STANÓW ZJEDNOCZONYCH**

| | |
|---|---|
| **Data i miejsce sporządzenia dokumentu:** | 25/05/2018 Warszawa |
| **Ilość stron:** | 13 |

# SPIS TREŚCI

# 1. WSTĘP

## 1.1. INFORMACJE OGÓLNE

1. Administratorem Danych, wdrażającym Politykę Bezpieczeństwa jest Spółka Superstacja Sp. z o.o. z siedzibą w Warszawie przy Al. Stanów zjednoczonych 53, KRS:227371 NIP:525-23-25-721, REGON: 140051055

2. Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania Superstacji Sp. z o.o. z przepisami prawa regulującymi kwestię administrowania i przetwarzania danych osobowych. Niniejsza Polityka Bezpieczeństwa opisuje w szczególności zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.

3. Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

   - Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000)
   - Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm.)
   - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 ze zm.),
   - 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 (rozporządzenie ogólne o ochronie danych).

## 1.2. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Obszarem przetwarzania danych osobowych przez Superstację Sp. z o.o. jest każdorazowy adres siedziby Spółki Superstacja Sp. z o.o.
2. Ochrona danych osobowych realizowana jest poprzez stosowanie zabezpieczeń w postaci środków organizacyjnych, środków ochrony fizycznej oraz środków technicznych systemu informatycznego w ramach procedur zawartych w instrukcji zarządzania systemem informatycznym.

3. Utrzymanie bezpieczeństwa przetwarzania danych osobowych w Superstacji Sp. z o.o. rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
4. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów:
   a) Poufność danych – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
   b) Integralność danych – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   c) Dostępność danych – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny temu podmiotowi,
   d) Autentyczność danych – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
   e) Integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.
   f) Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.
5. Superstacja Sp. z o.o. gromadzi oraz przetwarza dane osobowa w następujących celach:
   a) Wykonywania obowiązków pracodawcy w zakresie zatrudnienia pracowników (dokumentacja i przebieg zatrudnienia oraz płace pracowników),
   b) Wykonywania obowiązków zleceniodawcy w zakresie zawieranych umów cywilnoprawnych (dokumentacja przebiegu zlecenia oraz wypłaty należnego wynagrodzenia),
   c) Realizacja audycji telewizyjnych w części polegającej na przyjmowaniu gości występujących w audycjach telewizyjnych (dokumentacja przebiegu zlecenia polegająca na przywiezieniu gości z pod wskazanych przez nich adresów, często adresów zameldowania oraz wypłaty należnego wynagrodzenia).

## 1.3 WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

1. Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

**Polityka Bezpieczeństwa** – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych w Superstacji Sp. z o.o.,

**Administrator danych** – Administratorem Danych Osobowych w rozumieniu niniejszej Polityki Bezpieczeństwa jest Superstacja Sp. z o.o., która zgodnie z Umową Spółki reprezentowana jest przez Prezesa Zarządu działającego samodzielnie,

**ASI** – Administrator Systemów Informatycznych, osoba, odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych. ASI powołuje Administrator Danych Osobowych

**ustawa** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000) lub Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm.)

**rozporządzenie** – Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 ze. zm.),

**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 (rozporządzenie ogólne o ochronie danych).

**dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,

**zbiór danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

**baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe,

**usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą.

**przetwarzanie danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

**poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

**System informatyczny** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,

**Bezpieczeństwo systemu informatycznego** – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed nieuprawnionym przetwarzaniem danych,

**Użytkownik –** rozumie się przez to osobę wyznaczoną i upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych, przeszkoloną w zakresie ochrony tych danych.

**Stacja robocza –** stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

# 2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

## 2.1. INFORMACJE OGÓLNE

1. Osoby odpowiedzialne za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, Rozporządzenia, RODO, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemami informatycznymi w Superstacji Sp. z o.o. to:
   a) Administrator Danych – Superstacja Sp. z o.o.
   b) Administrator Systemów Informatycznych,
   c) Osoby wykonujące pracę bądź świadczące usługi cywilnoprawne na rzecz Administratora Danych Osobowych, które uzyskały upoważnienie do przetwarzania danych osobowych.

## 2.2. ADMINISTRATOR DANYCH

1. Administratorem Danych Osobowych w rozumieniu niniejszej Polityki Bezpieczeństwa jest Superstacja Sp. z o.o., z siedzibą w Warszawie, przy ul. Al. Stanów Zjednoczonych 53, NIP: 525-23-25-721 Regon: 140051055 która zgodnie z Umową Spółki reprezentowana jest przez Prezesa Zarządu działającego samodzielnie.
2. W ramach wykonywanych obowiązków w zakresie ochrony danych osobowych Administrator Danych m.in. wyznacza Administratora Systemów Informatycznych.

3. Do najważniejszych obowiązków Administratora Danych należy zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

    a) Organizację bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych oraz innych przepisów regulujących zasady bezpieczeństwa i ochrony danych osobowych;

    b) Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa;

    c) Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych;

    d) Przeprowadzanie szkoleń użytkowników przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe;

    e) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

    f) Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;

    g) Nadzór nad bezpieczeństwem danych osobowych;

    h) Kontrola działań osób uprawnionych do przetwarzania danych osobowych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;

    i) Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;

    j) Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych;

1. Administrator Danych swoje ustawowe zadania może realizować, w szczególności poprzez:

    a) stały nadzór nad treścią Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym,

    b) aktualizację i modyfikację ww. dokumentów,

    c) udział w kontrolach prowadzonych przez uprawnione do tego organy,

    d) udzielanie odpowiedzi na zapytania kierowane do Administratora Danych przez podmioty zewnętrzne, dotyczące administrowanych zbiorów danych osobowych,

    e) przeprowadzanie szkoleń z zakresu ochrony danych osobowych ,

    f) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,

    g) prowadzenie aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych we wszystkich zbiorach oraz nadzór nad prowadzeniem rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych,

    h) nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe,

i) monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych.

## 2.3 ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Do uprawnień i obowiązków Administratora Systemów Informatycznych należą m. in.:
   a) nadawanie / nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
   b) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
   c) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
   d) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych,
   e) sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi opisanymi w Instrukcji zarządzania systemem informatycznym,
   f) Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
   g) Optymalizacja wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
   h) Zmiana lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
   i) Zarządzanie licencjami oraz procedurami ich dotyczącymi,
   j) Prowadzenie profilaktyki antywirusowej.

## 2.4 OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia, RODO, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

3. Ewidencja osób upoważnionych do przetwarzania danych osobowych w Superstacji Sp. z o.o. jest prowadzona przez Administratora Danych zgodnie ze wzorem formularza stanowiącym załącznik nr 6 do Polityki Bezpieczeństwa przetwarzania danych osobowych w Superstacji Sp. z o.o.

## 3. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych na mocy art. 24 RODO.
2. Upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych przez Administratora Danych Osobowych.
3. W celu otrzymania przez Użytkownika upoważnienia do przetwarzania danych osobowych, należy dostarczyć do Administratora Danych podpisane oświadczenie użytkownika.
4. Na podstawie otrzymanego oświadczenia Administrator Danych Osobowych upoważnia Użytkownika do przetwarzania danych osobowych i wydaje upoważnienie do przetwarzania danych osobowych sporządzane wg. wzoru stanowiącego załącznik nr 2 i 3 do Polityki Bezpieczeństwa. Upoważnienia, o których mowa powyżej przechowywane są u Administratora Danych.
5. Upoważnienie może być w każdym czasie odwołane przez Administratora Danych Osobowych. Oświadczenie o odwołaniu upoważnienia do przetwarzania danych osobowych powinno być sporządzone na piśmie.
6. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą ustania przesłanki będącej podstawą wydania upoważnienia, w tym w szczególności wygaśnięcia stosunku pracy lub umowy cywilnoprawnej łączącej Użytkownika z Administratorem Danych Osobowych.

# 4. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi każdy pracownik lub współpracownik Spółki Superstacja Sp. z o.o. mający dostęp do danych.
2. Pracownicy oraz współpracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
3. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy oraz współpracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka". Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników i współpracowników.
4. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
5. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych lub wykonywania zlecenia. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony lub Administrator Danych.
6. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
7. Pracownicy oraz współpracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy lub wykonywania zlecenia, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

# 5. INSTRUKCJA POSTĘPOWNIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi Danych i/lub Administratorowi Systemów Informatycznych (w odniesieniu do danych przetwarzanych w systemach informatycznych).
2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Danych i/lub Administratora Systemów Informatycznych lub upoważnionej przez nich osoby, osoba powiadamiająca powinna:
    a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
    b) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
    c) udokumentować wstępnie zaistniałe naruszenie,
    d) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.
3. Po przybyciu na miejsce naruszenia ochrony danych osobowych, Administrator Danych lub Administrator Systemów Informatycznych lub osoba ich zastępująca:
    a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania
    b) wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
4. Administrator Danych i/lub Administrator Systemów Informatycznych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport.
5. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator Danych i/lub Administrator Systemów Informatycznych, zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych

# 6. KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Okresowy przegląd Polityki Bezpieczeństwa powinien mieć na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Superstacji Sp. z o.o. oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.

## 7. SPOSÓB PRZEPŁYWU DANYCH OSOBOWYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI

1. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.

2. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora Danych Osobowych.

3. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.

4. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

## 8. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

1. Dane osobowe mogą być przetwarzane wyłącznie w obszarze przetwarzania danych osobowych, na które składają się pomieszczenia biurowe w siedzibie Superstacja Sp. z o.o., z wyjątkiem sytuacji udostępnienia danych osobowych lub powierzenia przetwarzania danych osobowych.
2. Dane osobowe w Superstacji Sp. z o.o. przetwarzane są przy zastosowaniu zabezpieczeń zapewniających ich ochronę w postaci środków organizacyjnych, technicznych i środków ochrony fizycznej.