

POLITYKA BEZPIECZEŃSTWA INFORMACJI



Gdańsk, dnia 23 maja 2018 roku

Niniejsza Polityka Bezpieczeństwa Informacji, zwana dalej Polityką, została sporządzona w celu zapewnienia i wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych, w tym z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej jako „RODO”).

Definicje:

1. **Administrator Danych:** SCG Sp. z o.o. S.K. KRS 0000796658, REGON: 363281041.
2. **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
3. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych.
4. **Użytkownik** - osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych.
5. **Zbiór danych** - każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów.
6. **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.

7. **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.
8. **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.
9. **Uwierzytelnianie** - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika).

I. Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w **SCG Sp. z o.o. S.K** (dalej jako Administrator Danych lub Spółka) niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, Systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w Zbiorach danych.
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora Danych.
3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do Przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
4. W zakresie Przetwarzania danych pozyskanych w związku z wykonywaniem czynności objętych tajemnicą przedsiębiorstwa Administrator Danych stosuje się także do regulacji dotyczących zachowania tej tajemnicy.
5. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
 - a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
 - b) kontrolę i nadzór nad Przetwarzaniem danych osobowych,
 - c) monitorowanie zastosowanych środków ochrony.

6. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
7. Administrator Danych zapewnia, że czynności wykonywane w związku z Przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą Polityką oraz odpowiednimi przepisami prawa.

II. 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 nast. 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.

III. 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 Danych Polityką Bezpieczeństwa, Instrukcją Zarządzania Systemem Informatycznym, a także innymi dokumentami wewnętrznymi i procedurami związanymi z przetwarzaniem danych osobowych w Spółce.
2. Wszystkie Dane osobowe są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
 - a) w każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla Przetwarzania danych,
 - b) Dane osobowe przetwarzane są rzetelnie i w sposób przejrzysty,
 - c) Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny 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 osobowych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane,
 - g) wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO; wzory informacji dla kandydatów do pracy i klientów stanowią odpowiednio **załączniki numer 1 i 2** do niniejszej Polityki,
 - h) Dane osobowe są zabezpieczone przed naruszeniami zasad ich ochrony.
3. Administrator Danych nie przekazuje osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej (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 umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym,
 - c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia Danym osobowym ochrony,
 - d) niedopełnienie obowiązku zachowania w 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 zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych.
6. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy dopilnowanie, by:
- a) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków,

- b) każdy z przetwarzających Dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych” - wzór Upoważnienia stanowi **Załącznik nr 3** do niniejszej Polityki Bezpieczeństwa,
- c) każdy pracownik zobowiązał się do zachowania Danych osobowych przetwarzanych w kancelarii w tajemnicy. „Oświadczenie i zobowiązanie osoby przetwarzającej dane osobowe do zachowania tajemnicy” stanowi **Załącznik nr 4** do niniejszej Polityki i stosowane jest łącznie z „Upoważnieniem do przetwarzania danych osobowych”.

7. Pracownicy zobowiązani są do:

- a) ścisłego przestrzegania zakresu nadanego upoważnienia,
- b) przetwarzania i ochrony Danych osobowych zgodnie z przepisami,
- c) zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia,
- d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.

IV. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są Dane osobowe na terenie Spółki obejmuje pomieszczenie biurowe zlokalizowane w biurze Spółki w Gdańsku przy ul. Doki 1.
2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.

V. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych, Środki obejmują:
 - 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 upoważnionej,

- b) zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w pkt. IV powyżej na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich,
 - c) wykorzystanie zamkniętych szafek i sejfów do zabezpieczenia dokumentów,
 - d) wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe, lub innych bezpiecznych i skutecznych środków,
 - e) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall,
 - f) ochronę sprzętu komputerowego wykorzystywanego u administratora przed złośliwym oprogramowaniem,
 - g) zabezpieczenie dostępu do urządzeń Spółki przy pomocy Hasła dostępu,
 - h) ochronę telefonów i smartfonów wykorzystywanych przez wspólników, pracowników i współpracowników Spółki poprzez wyłączenie dostępu do tych urządzeń i niepozostawianie urządzeń bez nadzoru użytkownika (zabezpieczenie przed dostępem osób trzecich),
 - i) wykorzystanie szyfrowania danych przy ich transmisji.
3. Sposób zarządzania Systemem informatycznym przetwarzającym Dane osobowe w Spółce, w tym zabezpieczenie dostępu do urządzeń Spółki przy pomocy Hasła dostępu, wykorzystanie szyfrowania danych przy ich transmisji i inne elementy zabezpieczeń, reguluje **Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe w SCG Sp. z o.o. S.K w Gdańsku.**

VI. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony Danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorcemu bez zbędnej zwłoki - jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zgłoszenia określa **Załącznik nr 5** do niniejszej polityki.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

VII. Powierzenie przetwarzania danych osobowych

1. Administrator Danych osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28.
2. Przed powierzeniem Przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia Danych osobowych.

VIII. 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 obowiązek taki zaistniałby na mocy obowiązującego prawa.

IX. Postanowienia końcowe.

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, Przepisów o ochronie danych osobowych.
2. Integralną część niniejszej Polityki bezpieczeństwa stanowią następujące Załączniki:

Załącznik nr 1

Wzór informacji dla kandydata do pracy.

Załącznik nr 2

Wzór informacji dla klienta.

Załącznik nr 3

Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik nr 4

Wzór Oświadczenia i zobowiązania osoby przetwarzającej dane osobowe.

Załącznik nr 5

Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego.