POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH
CENTRANS SP. Z O.O.
z siedzibą w Poznaniu

Poznań, dnia 25 maja 2018 r.

Niniejsza Polityka Bezpieczeństwa ochrony danych osobowych określa zasady bezpieczeństwa, zarządzania bezpieczeństwem systemów oraz zasady przetwarzania danych osobowych, których Administratorem jest **CENTRANS Sp. z o.o.** z siedzibą w Poznaniu (60-115), ul. Poniecka 4, zarejestrowana w Sądzie Rejonowym Poznań- Nowe Miasto i Wilda w Poznaniu, VIII Wydział Krajowego Rejestru Sądowego pod numerem 0000686280, posiadająca NIP 783-176-19-75, REGON 367779683 o kapitale zakładowym 50 000,00 PLN (słownie: pięćdziesiąt tysięcy złotych) w zakresie prowadzonej działalności gospodarczej

I. Postanowienia ogólne

1. Administrator podejmuje wszelkie działania do zapewnienia bezpieczeństwa przetwarzanych danych osobowych.
2. Biorąc pod uwagę charakter, zakres i cele przetwarzania danych osobowych, a także ryzyko naruszenia praw lub/i wolności osób fizycznych wdraża się wraz z niniejszą Polityką Bezpieczeństwa odpowiednie środki techniczne, fizyczne i organizacyjne, których celem jest skuteczne zabezpieczenie przetwarzanych danych osobowych oraz spełnienia wymogów nałożonych przez przepisy prawa, w tym również RODO.
3. Niniejsza Polityka definiuje mechanizmy, zasady i procedury ochrony danych osobowych stosowane przez Firmę oraz dotyczy wszystkich danych osobowych przetwarzanych przez Firmę.
4. Z niniejszym dokumentem powinny być zapoznane wszystkie osoby mające dostęp bądź wykonujące działania na danych Firmy, w szczególności pracownicy i współpracownicy.
5. Innymi dokumentami regulującymi ochronę danych osobowych w Firmie są:
   - Zasady zarządzania zgodami na przetwarzanie danych osobowych,
   - Zarządzanie naruszeniami ochrony danych osobowych,
   - Zasady realizacji praw osób, których dane są przetwarzane,
   - Wzór upoważnienia do przetwarzania danych osobowych,
   - Procedura oceny skutków dla ochrony danych (DPIA).

II. Słowniczek definicji, pojęć i skrótów

FIRMA	**CENTRANS SP. Z O.O.**
RODO	Rozporządzenie 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.
SZBI	System Zarządzania Bezpieczeństwem Informacji
ABI	Administrator Bezpieczeństwa Informacji
ADO	Administrator Danych Osobowych – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych - **CENTRANS Sp. z o.o.**
IODO	Inspektor Ochrony Danych Osobowych – osoba wyznaczona przez Administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych

PUODO	Prezes Urzędu Ochrony Danych Osobowych, krajowy organ nadzoru w obszarze ochrony danych osobowych
DANE OSOBOWE	Zgodnie z artykułem 4 ust.1 RODO dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
SZCZEGÓLNE KATEGORIE DANYCH OSOBOWYCH	Dane wrażliwe, dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
ZBIÓR DANYCH	Każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
PRZETWARZANIE DANYCH OSOBOWYCH	Przez przetwarzanie danych RODO definiuje operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
PODMIOT PRZETWARZAJĄCY	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych.
NARUSZENIE OCHRONY DANYCH OSOBOWYCH	Naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
PRAWO DOSTĘPU PRZYSŁUGUJĄCE OSOBIE, KTÓREJ DANE DOTYCZĄ	Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz informacji wymienionych w tym przepisie.
PRAWO DO SPROSTOWANIA DANYCH	Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
PRAWO DO BYCIA ZAPOMNIANYM I PRAWO DO OGRANICZANIA	Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

PRZETWARZANIA	**a)** dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane, **b)** osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania, **c)** osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania, **d)** dane osobowe były przetwarzane niezgodnie z prawem, **e)** dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator, **f)** dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.
PRAWO DO PRZENOSZENIA DANYCH	Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Administratorowi, oraz ma prawo przesłać te dane osobowe innemu Administratorowi bez przeszkód ze strony Administratora, któremu dostarczono te dane osobowe, jeżeli: **a)** przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) oraz **b)** przetwarzanie odbywa się w sposób zautomatyzowany.
PRAWO DO SPRZECIWU	Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI W INDYWIDUALNYCH PRZYPADKACH, W TYM PROFILOWANIE	Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Przy czym „profilowanie" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
PSEUDONIMIZACJA	Przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie bez użycia dodatkowych informacji.
PROFILOWANIE	Dowolna forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych

	czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
ZGODA PODMIOTU DANYCH	Dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
WEWNĘTRZNA SIEĆ TELEINFORMATYCZNA	Sieć Administratora, łącząca co najmniej dwa indywidualne stanowiska komputerowe, umożliwiające użytkownikom określony dostęp do danych, w tym danych osobowych.

III. Cele i zakres stosowania

1. Celem Polityki Bezpieczeństwa danych osobowych jest:

- Wprowadzenie systemu ochrony danych osobowych poprzez ich zabezpieczenie adekwatnie do ryzyka i zidentyfikowanych zagrożeń,
- Dostosowanie do wymagań przepisów prawa i wytycznych w obszarze ochrony danych osobowych, w szczególności Rozporządzenia 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,
- Wskazanie zasad i reguł postępowania, aby Administrator danych mógł właściwie wykonywać zadania w zakresie ochrony danych osobowych.

2. Polityka Bezpieczeństwa dotyczy:

- Każdej osoby mającej dostęp do tychże danych osobowych,
- Pracowników Firmy przetwarzających dane osobowe,
- Współpracowników Firmy przetwarzających dane osobowe,
- Innych firm, z którymi Firma zawrze Umowy Powierzenia przetwarzania danych osobowych.

IV. Zasady ochrony danych osobowych

1. Osoby przetwarzające dane osobowe Firmy są zobowiązane do ochrony przetwarzanych danych osobowych oraz realizacji praw osób, których dane są przetwarzane.

2. Podmioty, których dane osobowe są przetwarzane i przekazywane do przetwarzania na mocy niniejszego dokumentu posiadają następujące prawa:

1) prawo dostępu do danych,
2) prawo do bycia informowanym,
3) prawo do poprawiania danych,
4) prawo do ograniczenia przetwarzania danych,
5) prawo do usuwania danych („prawo do bycia zapomnianym"),
6) prawo do przenoszenia danych,
7) prawo do wniesienia sprzeciwu,

Zasady realizacji powyższych praw zostały opisane w Zasadach realizacji praw osób, których dane są przetwarzane.

3. Ochrona danych osobowych realizowana jest poprzez zabezpieczenia organizacyjne, fizyczne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych.
4. Zastosowane zabezpieczenia mają służyć utrzymaniu bezpieczeństwa danych osobowych w Firmie i zapewnieniu danym osobowym następujących cech:
   1) dostępności informacji – rozumianej jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
   2) poufności danych – rozumianej jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
   3) integralności danych – rozumianej jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   4) rozliczalności danych – rozumianej jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
   5) integralności systemu – rozumianej jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej,
   6) zarządzania ryzykiem – rozumianego jako proces kontrolowania, identyfikowania, i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.
5. Dane osobowe przetwarzane przez Firmę muszą być:
   1) zbierane w określonych, wyraźnych i prawnie uzasadnionych celach (zasada minimalizowania ilości danych osobowych do treści niezbędnych),
   2) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych,
   3) chronione za pomocą odpowiednich środków technicznych, fizycznych lub organizacyjnych przed niedozwolonym, niezgodnym z prawem przetwarzaniem, przypadkową utratą, zniszczeniem, zniekształceniem lub uszkodzeniem,
   4) nieprzetwarzane w sposób niezgodny z celem, w jakim zostały zebrane,
   5) ograniczone do tego, co jest niezbędne dla realizacji celów, dla których są przetwarzane,
   6) przetwarzane zgodnie z prawem w sposób przejrzysty, jasny i zrozumiały dla osoby, której dane dotyczą,
   7) prawidłowe i w razie potrzeby uaktualniane lub ograniczane,
   8) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą,
   9) przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.
6. Przetwarzanie danych osobowych jest możliwe jedynie gdy spełniona jest przynajmniej jedna z wymienionych przesłanek:
   1) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Firmie,
   2) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym,
   3) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie danych osobowych w jednym lub większej liczbie skonkretyzowanych celów,
   4) przetwarzanie jest niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
   5) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą,
   6) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
   7) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których

nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą.

7. Firma będzie wdrażać odpowiednie środki techniczne, fizyczne i organizacyjne, aby zbierane i przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Obowiązek ten dotyczy również okresu przechowywania danych osobowych.
8. Za podmiot nieupoważniony uważa się podmiot, który nie otrzymał upoważnienia, zgody bądź powierzenia Administratora na udostępnienie mu danych osobowych.
9. Wszelkie rejestry prowadzone przez Administratora, bądź w jego imieniu przez inne osoby będą udostępniane organowi nadzorczemu na jego żądanie.

V. Podział obowiązków

1. Na dzień sporządzenia audytu uznano, że CENTRANS Sp. z o.o. nie wymaga powołania Inspektora Ochrony Danych Osobowych, a zatem do zadań Zarządu Spółki bądź osoby wyznaczonej przez Zarząd do spraw RODO należy:
   1) nadzór nad organizacją bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i przepisami krajowymi o ochronie danych osobowych,
   2) kontakt z organem nadzorczym ochrony danych osobowych,
   3) kontakt z osobami, których dane są przetwarzane,
   4) zapewnienie przetwarzania danych zgodnie z zasadami Polityki Bezpieczeństwa i innymi dokumentami wewnętrznymi Firmy,
   5) nadzorowanie procesu nadawania upoważnień do przetwarzania danych osobowych,
   6) prowadzenie rejestru czynności przetwarzania,
   7) prowadzenie rejestru obowiązujących wzorów zgód na przetwarzanie danych osobowych i obowiązków informacyjnych,
   8) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
   9) koordynacja realizacji praw osób, których dane są przetwarzane,
   10) nadzór realizacji praw pracowników w zakresie ochrony danych osobowych,
   11) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
   12) inicjowanie i podejmowanie przedsięwzięć w zakresie udoskonalania ochrony danych osobowych
   13) przeprowadzenie przeglądu dokumentów związanych z ochroną danych osobowych co najmniej raz w roku, a w przypadku konieczności wprowadzenia zmian, ich dokonywanie,
   14) kontrola poszczególnych działów Firmy pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych
   15) nadzór nad Informatykiem pod kątem przestrzegania przepisów i regulacji wewnętrznych firmy w zakresie ochrony danych osobowych,
   16) zlecenie przeprowadzenia audytu zgodności z RODO firmie zewnętrznej bądź zewnętrznemu Inspektorowi Ochrony Danych Osobowych celem uzyskania sprawozdania rocznego z funkcjonowania systemu ochrony danych osobowych w Firmie.
2. Do zadań Informatyka w zakresie ochrony danych osobowych należy:
   1) prowadzenie bieżącego monitoringu działania systemu informatycznego oraz baz danych,
   2) przeprowadzanie instalacji i konfiguracji sprzętu sieciowego i serwerowego oraz oprogramowania systemowego i sieciowego,
   3) zapewnienie ciągłości systemu informatycznego oraz baz danych,
   4) optymalizacja wydajności systemu informatycznego,
   5) zarządzanie licencjami, procedurami ich dotyczącymi,
   6) wdrażanie środków ochrony informatycznej ustanowionych w ramach systemu ochrony danych osobowych,

7) prowadzenie profilaktyki antywirusowej,
8) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego,
9) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
10) konfiguracja i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
11) nadzór nad bezpieczeństwem danych osób korzystających ze stron internetowych Firmy,
12) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
13) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
14) przyznawanie na wniosek Administratora danych osobowych wskazanych uprawnień dostępu do informacji w danym systemie,
15) kierowanie do Administratora danych osobowych wniosków w sprawie usprawnienia/zmian procedur bezpieczeństwa i standardów zabezpieczeń,
16) prowadzenie polityki haseł na urządzeniach służbowych,
17) współpraca z dostawcami usług oraz sprzętu sieciowego i serwerowego.

3. Do zadań pracowników i współpracowników, a także wszystkich osób przetwarzających dane osobowe w należy:
1) identyfikacja powierzenia przetwarzania danych osobowych w ramach umów zawieranych z podmiotami zewnętrznymi,
2) dobieranie odpowiednich środków ochronnych przetwarzanych danych,
3) dbanie o bezpieczeństwo i prawidłowość przetwarzanych danych osobowych,
4) zgłaszanie wszelkich naruszeń ochrony danych osobowych zgodnie z Procedurą zarządzania naruszeń,
5) realizowanie praw osób, których dane są przetwarzane.

VI. Upoważnienia do przetwarzania danych osobowych

1. Zgodnie z art. 29 Rozporządzenia 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 (RODO), podmiot przetwarzający oraz każda osoba działająca z upoważnienia Administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie Administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.
2. Administrator Danych lub osoba upoważniona w jego imieniu nadaje upoważnienia do przetwarzania danych osobowych wszystkim osobom, które przetwarzają dane osobowe Firmy, dotyczy to osób zatrudnionych na podstawie umowy o pracę, umowy cywilno-prawnej, praktykantów i stażystów.
3. Udzielając upoważnienia Administrator zapoznaje daną osobę z obowiązującymi w Firmie zasadami ochrony danych osobowych i przepisami dotyczącymi ochrony danych osobowych.
4. Upoważnienie powinno być sporządzone na piśmie w dwóch egzemplarzach i zostać podpisane zarówno przez osobę upoważnianą oraz przez Administratora Danych.
5. Jeden egzemplarz upoważnienia otrzymuje osoba, której dokument dotyczy, zaś drugi jest przechowywane w aktach osobowych pracownika w części B lub w ewidencji prowadzonej przez Kadry.

6. Upoważnienie ustaje w momencie rozwiązania lub wygaśnięcia umowy, będącej podstawą relacji pomiędzy **CENTRANS Sp. z o. o.** a osobą upoważnioną lub w przypadku odwołania przedmiotowego upoważnienia.
7. Upoważnienie może zostać odwołane w każdej chwili.

W Firmie obowiązuje wzór Upoważnienia.

VII. Obowiązek informacyjny

1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, Administrator podczas pozyskiwania danych osobowych podaje jej do wiadomości następujące informacje:
   1) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela,
   2) dane kontaktowe do osoby, która została wyznaczona do spraw RODO (w przypadku posiadania Inspektora Ochrony Danych Osobowych powinny być to dane do niego).
   3) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania,
   4) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią,
   5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
   6) informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.
2. Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych Administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:
   1) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
   2) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
   3) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
   4) informacje o prawie wniesienia skargi do organu nadzorczego,
   5) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
   6) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
3. Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.

4. W przypadku zbierania danych z innych źródeł niż od osób, których te dane dotyczą, należy niezwłocznie, najpóźniej w ciągu 30 dni poinformować podmiot danych w zakresie wskazanym w ust. 1 i 2 powyżej, a także o źródle pochodzenia danych osobowych.
5. Zarząd lub osoba przez niego wyznaczona prowadzi rejestr obowiązujących wzorów zgód na przetwarzanie danych osobowych i obowiązków informacyjnych.

VIII. Zasady wyrażania zgody

1. Zgoda na przetwarzanie danych osobowych osoby, której dane dotyczą powinna być zawarta w formie dokumentowalnej (dotyczy to zarówno zgody w formie papierowej, ustnej (udzielonej przykładowo podczas rozmowy telefonicznej) jak i elektronicznej).
2. Zgody powinny być przechowywane w taki sposób, aby możliwe było wykazanie ich posiadania przez Administratora Danych (zasada rozliczalności danych), a także dokonywanie operacji na nich (ograniczanie, aktualizacja, usuwanie, przekazywanie, udzielenie dostępu).
3. Zgoda powinna zostać sformułowana w sposób jasny i prosty.
4. Wyrażenie zgody wymaga aktywności ze strony osoby jej udzielającej.
5. Jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania umowy, to jej wykonanie nie może być uzależnione od wyrażenia zgody.
6. Osoba, której dane przetwarzane są na podstawie zgody powinna zostać poinformowana w momencie pobierania zgody o możliwości jej wycofania w każdym momencie.
7. Cofnięcie zgody powinno być tak samo proste, jak jej wyrażenie.
8. Zarząd lub osób przez niego wyznaczona prowadzi rejestr obowiązujących wzorów zgód na przetwarzanie danych osobowych i obowiązków informacyjnych.

IX. Podmioty przetwarzające

1. W sytuacji, gdy przetwarzanie danych osobowych ma być wykonywane w imieniu **CENTRANS Sp. z o.o.**, należy korzystać z usług podmiotów, którzy zapewnią, aby środki łączności wykorzystywane do zbierania, odbioru, przekazywania oraz przechowywania danych gwarantowały ich zabezpieczenie przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią oraz przed przypadkową utratą, zniszczeniem, zniekształceniem oraz uszkodzeniem danych osobowych.
2. Podmioty przetwarzające powinny dawać gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz niniejszej Polityki Bezpieczeństw Danych Osobowych, a także chroniło prawa osób, których dane dotyczą.
3. **CENTRANS Sp. z o.o.** z każdym podmiotem, któremu powierza przetwarzanie danych osobowych podpisze stosowną umowę (lub wprowadzi klauzulę w umowie głównej), która kompleksowo ureguluje wszystkie kwestie, procedury i zasady powierzenia danych osobowych.
4. Powierzenie jakichkolwiek danych osobowych podmiotowi zewnętrznemu będzie możliwe wyłącznie po podpisaniu umowy powierzenia lub umowy zawierającej klauzulę o powierzeniu danych przez obie strony.
5. Umowy powierzenia podlegają ewidencjonowaniu przez Zarząd lub osobę przez nią wyznaczoną do spraw RODO.
6. Firma dysponuje wzorem Umowy powierzenia danych osobowych.

X. Zmiany w przetwarzaniu danych osobowych

1. Wszystkie czynności przetwarzania danych osobowych są ewidencjonowane w postaci rejestru czynności przetwarzania danych.
2. Rejestr jest prowadzony i aktualizowany przez osobę wyznaczoną do spraw RODO, na podstawie informacji przekazywanych z poszczególnych działów Firmy.
3. Firma posiada wzór Rejestru czynności przetwarzania.
4. Osoby przetwarzające dane osobowe w Firmie zobowiązane są do niezwłocznego informowania osobę wyznaczoną do spraw RODO o jakichkolwiek zmianach w zakresie sposobu przetwarzania danych osobowych oraz ilości i rodzaju przetwarzanych danych.

XI. Ochrona danych osobowych w fazie planowania nowych rozwiązań

1. Osoby przetwarzające dane Administratora są zobowiązane, aby uwzględnić przepisy prawa dotyczące ochrony danych osobowych oraz wszystkie wewnętrzne regulacje Administratora, w tym niniejszą Politykę Bezpieczeństwa Ochrony Danych Osobowych, również w fazie projektowania nowych rozwiązań technicznych czy procesów, a także w razie wprowadzania modyfikacji w już istniejących rozwiązania i procesach.
2. W przypadku, gdy dany rodzaj przetwarzania stwarza wysokie ryzyko naruszenia praw lub wolności osób fizycznych należy w pierwszej kolejności dokonać oceny skutków zgodnie z Procedurą oceny skutków dla ochrony danych (DPIA- Firma posiada odrębny dokument w tym zakresie), przed zastosowaniem tego rodzaju przetwarzania.
3. Administrator stosuje wytyczne polskiego organu nadzoru przy dokonywaniu identyfikacji operacji mogących powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
4. Administrator na każdym etapie zobowiązany jest zbadać czy nie istnieje u niego konieczność powołania Inspektora Ochrony Danych Osobowych.

XII. Archiwizacja

Archiwizacja dokumentacji odbywa się zgodnie z przepisami prawa oraz z regulacjami wewnętrznymi obowiązującymi w zakresie ochrony danych osobowych

XIII. Szkolenia

1. Każdy pracownik lub współpracownik powinien być poddany przed podjęciem pracy przeszkoleniu w zakresie ochrony danych osobowych oraz obchodzenia się z danymi osobowymi zgodnie z technologicznymi oraz organizacyjnymi środkami bezpieczeństwa obowiązującymi w Firmie, a także wszelkimi regulacjami prawnymi oraz wytycznymi.
2. Za przeprowadzenie szkolenia odpowiada osoba wyznaczona do spraw RODO.
3. Zakres oraz częstotliwość szkoleń, o których mowa powyżej powinny być adekwatne do funkcji, jaką pełnią poszczególne osoby personelu, ponoszonej przez nich odpowiedzialności oraz częstotliwości, z jaką będą oni przetwarzali oraz obchodzili się z danymi osobowymi.

XIV. Postanowienia końcowe

1. Niniejsza Polityka Bezpieczeństwa powinna być poddawana przeglądowi przez zewnętrznego Inspektora Ochrony Danych osobowych lub firmę zewnętrzną zajmującą się sprawami RODO nie rzadziej niż raz do roku.
2. Treść Polityki Bezpieczeństwa jest aktualizowana w przypadku wprowadzenia lub zmiany środków technicznych lub organizacyjnych służących ochronie danych osobowych.

3. Po dokonaniu aktualizacji tworzy się nową wersję Polityki Bezpieczeństwa oraz przedstawia się ją pracownikom i współpracownikom do wglądu i omawia zmiany, jakie zaszły.
4. Nieprzestrzeganie Polityki Bezpieczeństwa, a także innych związanych z nią dokumentów obowiązujących u Administratora danych osobowych, może skutkować wyciągnięciem konsekwencji służbowych zgodnie z odrębnymi regulacjami.
5. Polityka Bezpieczeństwa wchodzi w życie z dniem jej podpisania.