Załącznik Nr 1 do
Polityki Ochrony Danych Osobowych
w Spółce Zakład Robót Komunikacyjnych
-DOM w Poznaniu Sp. z o.o.

Wykaz definicji i pojęć

użytych w Polityce Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

Spis treści

§ 1.

Postanowienia ogólne

Wykaz definicji i pojęć użytych w Polityce Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, jest dokumentem integralnym z Polityką Ochrony Danych Osobowych i zawiera użyte definicje i pojęcia stosowane w dokumentacji.

§ 2.

Wykaz definicji i pojęć

1. **Administrator danych –(ADO)** Zakładu Robót Komunikacyjnych -DOM w Poznaniu Spółka z o.o., jako podmiot ustalający cel i sposób przetwarzania danych osobowych.
2. **Administrator systemu lub sieci teleinformatycznych (ASI)** – zwany dalej administratorem systemu – należy przez to rozumieć osobę odpowiedzialną za prawidłowe funkcjonowanie systemu lub sieci teleinformatycznych, w tym w szczególności za przestrzeganie zasad i wymagań bezpieczeństwa dla systemów i sieci teleinformatycznych, w których przetwarzane są dane osobowe.
3. **Audyt** – systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu *[PN-ISO/IEC 27000]*.
4. **Bezpieczeństwo fizyczne** – zapewnienie skutecznej ochrony informacji w Spółce poprzez kombinację środków organizacyjnych i technicznych oraz osobowych poprzez zapewnienie ochrony pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników zewnętrznych i wewnętrznych.
5. **Bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności [PN-ISO/IEC 27000].
6. **Bezpieczeństwo osobowe** – zespół odpowiednio dobranych środków organizacyjnych i procedur w przydzielaniu pracownikom obowiązków i uprawnień mających na celu bezpieczeństwo informacji.
7. **Bezpieczeństwo teleinformatyczne** – zbiór zagadnień z dziedziny telekomunikacji i informatyki związany z szacowaniem i kontrolą ryzyka wynikającego z korzystania z komputerów, sieci komputerowych i przesyłania danych do zdalnych lokalizacji, rozpatrywany z perspektywy poufności, integralności i dostępności.
8. **BIOS** – podstawowy system wejścia-wyjścia – zapisany w pamięci stałej zestaw podstawowych procedur pośredniczących pomiędzy systemem operacyjnym, a sprzętem. Jest to program zapisany w pamięci ROM płyty głównej komputera oraz innych urządzeń.
9. **Czynność** – przetwarzanie w konkretnym i prawnie uzasadnionym celu danych osobowych pochodzących ze zbioru prowadzonego przez Spółkę, wymieniona w rejestrze czynności, o którym mowa w art. 30 RODO.
10. **Dane** - zbiory liczb i tekstów o różnych formach.
11. **Dane biometryczne** – oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne *[def. RODO: art. 4 pkt. 14]*.
12. **Dane genetyczne** – oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej *[def. RODO: art. 4 pkt. 13]*.

13. **Dane dotyczące zdrowia** – dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia *[def. RODO: art. 4 pkt. 15]*.
14. **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, w rozumieniu art. 4 pkt 1 RODO.
15. **Dane osobowe „Dane osobowe szczególnych kategorii" („wrażliwe")**– dane osobowe, o których mowa w art. 9 ust. 1 RODO.
16. **Dostępność** – właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu *[PN-ISO/IEC 27000]*.
17. **Identyfikacja zagrożeń** – proces polegający na określeniu, co może się zdarzyć, powodując utratę bezpieczeństwa informacji, a także na sporządzeniu i aktualizacji katalogu zagrożeń.
18. **Identyfikowanie ryzyka** – proces wyszukiwania, rozpoznawania i opisywania ryzyka *[PN-ISO/IEC 27000]*.
19. **Incydent bezpieczeństwa informacji** – incydent związany z bezpieczeństwem informacji, o którym mowa w normie PN-ISO/IEC 27000, tzn. pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji *[PN-ISO/IEC 27000]*.
20. **Integralność** – właściwość polegająca na zapewnieniu dokładności i kompletności *[PN- ISO/IEC 27000]*.
21. **Komórka organizacyjna** - komórka organizacyjna wchodząca w skład struktury organizacyjnej jednostki organizacyjnej Spółki.
22. **Kontrola dostępu** – środki mające na celu zapewnienie, że dostęp do aktywów jest autoryzowany i ograniczony w oparciu o wymagania biznesowe i wymagania bezpieczeństwa *[PN-ISO/IEC 27000]*.
23. **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 *[def. RODO: art. 4]*.
24. **Niszczenie danych:**
    1) z nośników elektronicznych za pomocą urządzeń do niszczenia nośników danych spełniające normy bezpieczeństwa;
    2) z nośników tradycyjnych – za pomocą niszczarki odpowiadającej co najmniej klasie 2 według normy DIN66399.
25. **Nośnik informatyczny** – urządzenie służące do zapisu i przechowywania informacji w postaci cyfrowej (np. dysk twardy, dyskietka, dysk optyczny, taśma magnetyczna, pen- drive, karta pamięci, itp.).
26. **Odbiorca** –osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie

danych mającymi zastosowanie stosownie do celów przetwarzania *[def. RODO: art. 4]*.

27. **Ograniczenie przetwarzania** - oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania *[def. RODO: art. 4]*.
28. **Osoba upoważniona** – osoba posiadająca imienne upoważnienie do przetwarzania danych osobowych wydane, zgodnie z zapisami zawartymi w Polityce Ochrony Danych Osobowych.
29. **Oprogramowanie szkodliwe** - wszelkie aplikacje lub skrypty mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera.
30. **Organ nadzorczy** – niezależny organ publiczny [Prezes Urzędu Ochrony Danych Osobowych] ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO *[def. RODO: art. 4]*.
    1) **Organ nadzorczy, którego sprawa dotyczy** – organ nadzorczy, którego dotyczy przetwarzanie danych osobowych, ponieważ: administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego;
    2) przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego;
    3) wniesiono do niego skargę

    [def. RODO: art. 4].
31. **Organizacja międzynarodowa** – organizacja i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy *[def. RODO: art. 4]*.
32. **Państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.
33. **Podatność** – słabość aktywu lub zabezpieczenia, która może być wykorzystana przez co najmniej jedno zagrożenie *[PN-ISO/IEC 27000]*.
34. **Podmiot przetwarzający** – *(o.d.o.)* - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora danych *[def. RODO: art. 4]*.
35. **Podpis elektroniczny** – dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, które użyte są przez podpisującego jako podpis. Szczegółowe definicje związane z podpisem elektronicznym i usługami zaufania zawiera eIDAS.
36. **Poufność** – właściwość polegająca na tym, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom *[PN-ISO/IEC 27000]*.
37. **Postępowanie z ryzykiem** – proces modyfikowania ryzyka *[PN-ISO/IEC 27000]*.
38. **Pozbawienie zapisu** – bezpowrotne zniszczenie zapisu lub jego usunięcie z nośnika informatycznego poprzez użycie odpowiedniego profesjonalnego programu komputerowego lub urządzenia. Program powinien umożliwiać użycie odpowiedniej metody/algorytmu: DoD 5220.22-M, NAVSO P-5239-26 (RLL), NAVSO P-5239-26 (MFM), VSITR, GOST P50739-95, Petera Gutmanna.
39. **Poziom ryzyka** – wielkość ryzyka wyrażona w kategoriach kombinacji następstw oraz ich prawdopodobieństwa *[PN-ISO/IEC 27000]*.
40. **Prawdopodobieństwo** –możliwość wystąpienia zdarzenia [*PN-ISO/IEC 27000]*.

41. **Prawo do bycia zapomnianym** –jedno z praw osób, których dane dotyczą: prawo żądania od administratora danych usunięcia danych, przysługujące przy spełnieniu warunków, o których mowa w art. 17 RODO.
42. **Prawo do przenoszenia danych** - –dwa powiązane ze sobą prawa osób, których dane dotyczą: prawo otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych jej dotyczących, które dostarczyła administratorowi i związane z nim prawo do przesłania tych danych osobowych innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, przysługujące przy spełnieniu warunków, o których mowa w art. 20 RODO.
43. **Profilowanie** - dowolna forma 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 *[def. RODO: art. 4]*.
44. **Przegląd** – działanie podejmowane w celu określenia przydatności, adekwatności oraz skuteczności w dziedzinie osiągania ustalonych celów *[PN-ISO/IEC 27000]*.
45. **Przetwarzanie** – *(o.d.o.)* - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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 *[def. RODO: art. 4]*.
46. **Przetwarzanie informacji** — wszelkie operacje wykonywane na danych, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie lub udostępnianie.
47. **Pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej *[def. RODO: art. 4]*.
48. **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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 2016 r., str. 1-88).
49. **Rozliczalność** – atrybut bezpieczeństwa teleinformatycznego: właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
50. **Ryzyko** – wpływ niepewności na cele *[PN-ISO/IEC 27000]*.
51. **„Silne" hasło** – hasło dostępu:
    1) mające długość równą, co najmniej:
        a) 8 znakom w przypadku hasła użytkownika,
        b) 14 znakom w przypadku hasła administratora,
        c) 14 znakom w przypadku hasła administratora BIOS (w przypadku braku możliwości spełnienia tego wymagania, maksymalną długość na jaką pozwala wersja BIOS komputera);
    2) składające się ze znaków alfanumerycznych (duże i małe litery z

cyframi i innymi znakami z klawiatury), z wyłączeniem polskich liter, zastosowanych łącznie;

3) nie będące słowem znaczącym, występującym w słownikach, jak również imieniem, nazwiskiem czy inną nazwą własną, itp.;

52. **Skuteczność** – stopień, w jakim zaplanowane działania zostały zrealizowane i planowane wyniki osiągnięte *[PN-ISO/IEC 27000]*.
53. **Spółka** – Zakład Robót Komunikacyjnych - DOM w Poznaniu Spółka z o.o.
54. **Strona trzecia** - osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż wymienione poniżej:

    1) osoba, której dane dotyczą,
    2) administrator danych,
    3) podmiot przetwarzający,
    4) osoby, które – z upoważnienia administratora danych lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe

    [def. RODO: art. 4].

55. **System informacyjny** – system, w którym w trakcie zachodzących w nim procesów gromadzi się, przetwarza, przechowuje i udostępnia informacje, niezależnie od formy realizacji tych procesów.
56. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych (zamiennie zwany również systemem teleinformatycznym).
57. **Umowa powierzenia przetwarzania danych osobowych** – umowa zawarta na piśmie, o której mowa w art. 31 ustawy o ochronie danych osobowych.
58. **Usuwanie danych osobowych** – trwałe usunięcie danych osobowych lub ich anonimizacja.
59. **Uwierzytelnianie** – pewność, że deklarowana charakterystyka podmiotu jest poprawna *[PN-ISO/IEC 27000]*.
60. **Zagrożenie** – potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji *[PN-ISO/IEC 27000]*.
61. **Zarządzanie ryzykiem** – skoordynowane działania dotyczące kierowania i nadzorowania organizacji w odniesieniu do ryzyka *[PN-ISO/IEC 27000]*.
62. **Zbiór danych** uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie *[def. RODO: art. 4]*.

Załącznik Nr 3 do
Polityki Ochrony Danych Osobowych
w Spółce Zakład Robót Komunikacyjnych
-DOM w Poznaniu Sp. z o.o.

WZÓR

Zaświadczenia ze szkolenia z zakresu ochrony danych osobowych

.....
(miejscowość, data)

....
(pieczęć podłużna jednostki / komórki organizacyjnej)

Zaświadczenie nr / rok

Pan(i): .....
(imię i nazwisko osoby szkolonej)

zatrudnioną(ego)

w .....
(nazwa jednostki i komórki organizacyjnej)

uczestniczył(a) w szkoleniu z zakresu ochrony danych osobowych w dniu .....

w: .....
(miejsce szkolenia)

.....
(, data i podpis osoby przeprowadzającej szkolenie)

Podstawa: Polityka Ochrony Danych Osobowych

Załącznik Nr 4 do
Polityki Ochrony Danych Osobowych
w Spółce Zakład Robót Komunikacyjnych
-DOM w Poznaniu Sp. z o.o.

WZÓR

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

.....
(miejscowość, data)

.....
(pieczęć podłużna jednostki / komórki organizacyjnej)

Upoważnienie imienne
do przetwarzania danych osobowych

Na podstawie: *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 216/679 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,* upoważniam Panią (Pana):

.....
(imię i nazwisko osoby upoważnionej)

zatrudnioną(ego)

w .....
(nazwa jednostki i komórki organizacyjnej)

na stanowisku: .....
do przetwarzania danych osobowych manualnie / w systemie informatycznym:

.....
(nazwa systemu informatycznego)

w zakresie:

.....
(kody zakresu upoważnienia)

Kod zakresu upoważnienia	Zakres upoważnienia do przetwarzania danych osobowych
1	zbieranie danych
2	wprowadzanie danych do zbioru
3	przeglądanie danych
4	modyfikowanie danych - poprawianie
5	usuwanie danych
6	generowanie wydruków - raportowanie
7	tworzenie kopii zbioru lub jego fragmentów
8	tworzenie kopii awaryjnych zbioru
9	odtwarzanie zbioru z kopii awaryjnych
10	przesyłanie danych w sieci
11	administrowanie systemem (dot. administratora systemu)
12	udostępnianie danych

i nadaję identyfikator: .....[x)]

.....
(administrator systemu teleinformatycznego)

.....
(pieczęć, data i podpis kierownika jednostki organiz.(administratora danych)

Otrzymują:
Egz. nr 1 – osoba upoważniona
Egz. nr 2 – teczka personalna

[x)] identyfikator podlega wpisowi do ewidencji osób upoważnionych do przetwarzania danych osobowych w jednostce organizacyjnej Spółki oraz jest rejestrowany w systemie informatycznym

Załącznik Nr 5 do
Polityki Ochrony Danych Osobowych
w Spółce Zakład Robót Komunikacyjnych
-DOM w Poznaniu Sp. z o.o.

.....

(miejscowość, data)

Zakład Robót Komunikacyjnych-DOM w Poznaniu Spółka z o.o.
ul. Kolejowa 4, 60-715 Poznań
tel./fax: +48 (061) 63 33 659
sekretariat(at)zrk-dom.com.pl
NIP: 779-21-57-760
REGON: 634195317
KRS: 0000027669

Prezes Urzędu Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

ZGŁOSZENIE
W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Niniejszym w trybie art. 33 ogólnego rozporządzenia o ochronie danych, zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu ..... w .....

1.	**Charakter naruszenia ochrony danych:**	
2.	**Kategoria i przybliżona liczba osób, których dane dotyczą:**	
3.	**Liczba rekordów, których dotyczy naruszenie:**	
4.	**Możliwe konsekwencje naruszenia ochrony danych:**	
5.	**Środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:**	
6.	**Dane przedstawiciela/inspektora ochrony danych* lub Administratora Danych Osobowych**	Np. Imię Nazwisko nr. telefonu: XXX XXX XXX, adres e-mail: .....@kolejarz.org
7.	**Wyjaśnienie przyczyn opóźnienia**	

.....**

.....

(czytelny podpis ADO, zgodnie z reprezentacją podmiotu)

* W przypadku niepowołania należy wskazać inny punkt kontaktowy.
** W przypadku zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin, administrator danych zobowiązany jest do złożenia wyjaśnień w przedmiocie przyczyn opóźnienia.

Załącznik Nr 6 do
Polityki Ochrony Danych Osobowych
w Spółce Zakład Robót Komunikacyjnych
-DOM w Poznaniu Sp. z o.o.

REJESTR
przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych

Data zgłoszenia Naruszenia (dzień i godzina)	Zgłaszający	Rodzaj naruszenia	Miejsce naruszenia	Opis naruszenia	Skutki naruszenia	Czy naruszenie podlega zgłoszeniu do organu nadzorczego	Czy naruszenie podlega zgłoszeniu osobie, której dane dotyczą	Podjęte działania – sposób usunięcia naruszenie	Data zakończenia czynności	Status

Załącznik Nr 7 do
Polityki Ochrony Danych Osobowych
w Spółce Zakład Robót Komunikacyjnych
-DOM w Poznaniu Sp. z o.o.

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:

(zwana dalej „Umową")

Zakład Robót Komunikacyjnych - DOM w Poznaniu Spółka z o.o. **z siedzibą w 60-715 Poznań wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy Poznań - Nowe Miasto Wilda, VIII Wydział Gospodarczy Krajowego rejestru Sądowego pod numerem KRS 0000027669,**

posiadającą numer NIP PL 779-21-57-760, posiadającą numer REGON 634195317, zwaną dalej **Zamawiającym**[2)], reprezentowaną przez:

_____ *(*dane podmiotu który umowę zawiera)*

zwany w dalszej części umowy **„Zamawiającym"**

reprezentowana przez:

_____

a

siedzibą w ..... (kod poczt.: ...-.....) przy ul. .....,

wpisaną ..... prowadzonego przez ..... pod numerem ....,

posiadającą numer NIP: ....., posiadającą numer REGON

.....,

zwaną dalej „**Wykonawcą**", reprezentowaną przez

_____

§ 1

Powierzenie przetwarzania danych osobowych

1. Zamawiający powierza Wykonawcy, w trybie art. 28 ogólnego 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 (zwanego w dalszej części „Rozporządzeniem"), dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Wykonawca oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2

Zakres i cel przetwarzania danych

1. Wykonawca będzie przetwarzał, powierzone na podstawie umowy dane (**należy podać rodzaj danych*) ..... *np. dane zwykłe oraz dane szczególnych kategorii* ..... *(*należy podać kategorię osób, których dane dotyczą) np. pracowników administratora, klientów administratora itd. w postaci* ..... *np. imion i nazwisk, adresu zamieszkania, nr PESEL itd.*
2. Powierzone przez Zamawiającego dane osobowe będą przetwarzane przez Wykonawcę wyłącznie w celu ..... (**należy podać cel przetwarzania danych przez podmiot przetwarzający*) *np. realizacji umowy z dnia ..... nr ..... w zakresie prowadzenia kadr.*

§3

Obowiązki Wykonawcy

1. Wykonawca zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Wykonawca zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Wykonawca zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Wykonawca zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu

realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich u Wykonawcy, jak i po jego ustaniu.

5. Wykonawca po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe (*należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Wykonawca pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Wykonawca po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu ..... (**można wskazać np. w ciągu 24 h*).

§4

Prawo kontroli

1. Zamawiający zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Wykonawcę przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Zamawiający realizować będzie prawo kontroli w godzinach pracy Wykonawcy i z minimum ..... (**należy wpisać z ilu dniowym wyprzedzeniem Administrator informuje o kontroli*) jego uprzedzeniem.
3. Wykonawca zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni (**administrator termin może określić dowolnie*).
4. Wykonawca udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5

Dalsze powierzenie danych do przetwarzania

1. Wykonawca może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Zamawiającego.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Zamawiającego chyba, że obowiązek taki nakłada na Wykonawcę prawo Unii lub prawo państwa członkowskiego, któremu podlega Wykonawca. W takim przypadku przed rozpoczęciem przetwarzania Wykonawca informuje Zamawiającego o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §3 ust. 2 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Wykonawcę w niniejszej Umowie.

4. Wykonawca ponosi pełną odpowiedzialność wobec Zamawiającego za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Wykonawcy

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Wykonawca zobowiązuje się do niezwłocznego poinformowania Zamawiającego o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Wykonawcę danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Wykonawcy, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania u Wykonawcy tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Zamawiającego.

§7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony* od ..... do ..... .*
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem ..... * okresu wypowiedzenia.

§8

Rozwiązanie umowy

1. Zamawiający może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową;
   c) przetwarza dane osobowe niezgodnie z obowiązującymi przepisami prawa,
   d) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Zamawiającego;

§9

Zasady zachowania poufności

1. Wykonawca zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Zamawiającego i od współpracujących z nim osób oraz danych uzyskanych w

jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").

2. Wykonawca oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Zamawiającego w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych (**lub Podmiotu przetwarzającego w zależności od postanowień stron*).

_____	_____
_____	_____
Zamawiający	Wykonawca

Załącznik Nr 8 do
Polityki Ochrony Danych Osobowych
w Spółce Zakład Robót Komunikacyjnych
-DOM w Poznaniu Sp. z o.o.

WZÓR

……, dnia …… r.

……
(pieczęć i nr pisma)

Pan/i

……

……

……

Zgodnie z art. 13 ust. 1 i 2 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 (ogólne rozporządzenie o ochronie danych, Dz. Urz. UE L 119/1 z 2016 r.), zwanego dalej RODO, informuje się, że:

1. Administratorem Pani/Pana danych osobowych jest Spółka Zakład Robót Komunikacyjnych – DOM w Poznaniu Sp. z o.o. z siedzibą w Poznaniu, ul. Kolejowa 4, 60-715 Poznań.;

2. Pani/Pana dane osobowe przetwarzane będą w celu realizacji praw i obowiązków wynikających ze stosunku pracy, na podstawie art. 6 ust. 1 lit. c RODO;

3. Pani/Pana dane osobowe będą przechowywane przez okres trwania stosunku pracy oraz w obowiązkowym okresie przechowywania dokumentacji związanej ze stosunkiem pracy i akt osobowych, ustalanym zgodnie z odrębnymi przepisami;

4. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo 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;

5. Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

6. Podanie przez Panią/Pana danych osobowych jest wymogiem ustawowym, ich nieprzekazanie spowoduje niemożność realizacji zawartej umowy o pracę i związanych z nią obowiązków podatkowo – składkowych.

.....
(podpis pracownika)

Załącznik Nr 9 do
Polityki Ochrony Danych Osobowych
w Spółce Zakład Robót Komunikacyjnych
-DOM w Poznaniu Sp. z o.o.

WZÓR

Klauzula informacyjna dla klientów i kontrahentów

W związku z realizacją wymogów 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 2016 r., str. 1-88), zwanym dalej RODO, informuję, że:

1. Administratorem Pani/Pana Danych Osobowych jest Zakładu Robót Komunikacyjnych - DOM w Poznaniu Spółka z o.o., z siedzibą pod adresem: ul Kolejowa 4, 60-715 Poznań.
2. Administrator danych osobowych — przetwarza Pani/Pana dane osobowe na podstawie obowiązujących przepisów prawa, zawartych umów, w celu realizacji prawnie uzasadnionych interesów Administratora oraz na podstawie udzielonej zgody.
3. Pani/Pana dane osobowe przetwarzane są w celu/celach:
   1) zawarcia i wykonania umów z kontrahentami Administratora (podstawa prawna: art. 6 ust. 1b RODO) - przez okres trwania umowy i rozliczeń po jej zakończeniu;
   2) spełnienia ciążących na Administratorze obowiązków prawnych np. wystawienia lub przechowywania faktur i innych dokumentów księgowych, udzielanie odpowiedzi na reklamacje (podstawa prawna: art. 6 ust. 1c RODO) – przez okres jaki przepisy prawa nakazują przechowywać dane,
   3) ustalenia, obrony i dochodzenia roszczeń (podstawa prawna: art. 6 ust. 1f RODO) – przez okres, po którym przedawnią się roszczenia ,
   4) weryfikacji wiarygodności płatniczej (podstawa prawna: art. 6 ust. 1f RODO) – przez okres niezbędny do dokonania takiej oceny przy zawarciu, przedłużeniu lub rozszerzeniu zakresu umowy,
   5) marketingu bezpośredniego (podstawa prawna: art. 6 ust. 1f RODO) – przez okres trwania umowy lub do złożenia sprzeciwu,
   6) wykrywania nadużyć i zapobiegania im (podstawa prawna: art. 6 ust. 1c i 1f RODO) – przez okres trwania umowy, a następnie przez okres po którym przedawnią się roszczenia lub przez czas trwania postępowań prowadzonych przez właściwe organy publiczne,
   7) w pozostałych przypadkach Pani/Pana dane osobowe przetwarzane są wyłącznie na podstawie wcześniej udzielonej zgody w zakresie i celu określonym w treści zgody (art. 6 ust. 1a RODO) – przez okres od udzielenia zgody do jej cofnięcia.

4. W związku z przetwarzaniem danych w celach o których mowa w pkt 4 odbiorcami Pani/Pana danych osobowych mogą być podmioty z następujących kategorii:
   1) przetwarzające dane osobowe w imieniu Administratora na podstawie stosownych umów np. obsługujące systemy informatyczne Administratora, podwykonawcy, agencje reklamowe, pośrednicy, podmioty świadczące na rzecz Administratora usługi doradcze, prawne, windykacyjne, rachunkowe, audytorskie oraz usługi doręczania korespondencji i przesyłek
   2) z grupy kapitałowej, do której należy Administrator,
   3) upoważnione do ich otrzymania na podstawie obowiązujących przepisów prawa np. sądy i organy państwowe.
5. Obecnie nie planujemy przekazywać Pani/Pana danych osobowych poza EOG (obejmujący Unię Europejską, Norwegię, Lichtenstein i Islandię).
6. W związku z przetwarzaniem Pani/Pana danych osobowych przysługują Pani/Panu następujące uprawnienia:
   1) prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
   2) prawo do żądania sprostowania (poprawiania) danych osobowych – w przypadku gdy dane są nieprawidłowe lub niekompletne;
   3) prawo do żądania usunięcia danych osobowych (tzw. prawo do bycia zapomnianym), w przypadku gdy:
      - dane nie są już niezbędne do celów, dla których były zebrane lub w inny sposób przetwarzane,
      - osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych osobowych,
      - osoba, której dane dotyczą wycofała zgodę na przetwarzanie danych osobowych, która jest podstawą przetwarzania danych i nie ma innej podstawy prawnej przetwarzania danych,
      - dane osobowe przetwarzane są niezgodnie z prawem,
      - dane osobowe muszą być usunięte w celu wywiązania się z obowiązku wynikającego z przepisów prawa;
   4) prawo do przenoszenia danych – w przypadku gdy łącznie spełnione są następujące przesłanki:
      - przetwarzanie danych odbywa się na podstawie umowy zawartej z osobą, której dane dotyczą lub na podstawie zgody wyrażonej przez tą osobę,
      - przetwarzanie odbywa się w sposób zautomatyzowany;
   5) prawo sprzeciwu wobec przetwarzania danych w przypadku gdy zaistnieją przyczyny związane z Pani/Pana szczególną sytuacją, a podstawą przetwarzania jest ich niezbędność do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią (art. 6 ust. 1 f RODO), z wyjątkiem sytuacji, w których Administrator:

- wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec tych interesów, praw i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą jest dzieckiem, lub
- wykaże podstawy do ustalenia, dochodzenia lub obrony roszczeń.

7. W przypadku gdy przetwarzanie danych osobowych odbywa się na podstawie zgody osoby na przetwarzanie danych osobowych (art. 6 ust. 1 lit a RODO), przysługuje Pani/Panu prawo do cofnięcia tej zgody w dowolnym momencie. Cofnięcie to nie ma wpływu na zgodność przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, z obowiązującym prawem.
8. W przypadku powzięcia informacji o niezgodnym z prawem przetwarzaniu przez Administratora Pani/Pana danych osobowych, przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
9. W sytuacji, gdy przetwarzanie danych osobowych odbywa się na podstawie zgody osoby, której dane dotyczą, podanie przez Panią/Pana danych osobowych Administratorowi ma charakter dobrowolny. W przypadku zawierania umowy podanie danych osobowych jest dobrowolne, ale niezbędne do zawarcia i wykonania umowy.
10. Pani/Pana dane mogą być przetwarzane w sposób zautomatyzowany. Pani/Pana dane nie będą profilowane za wyjątkiem przypadku gdy dane zostały pozyskane za pośrednictwem stron internetowych Administratora oraz po uzyskaniu Pani/Pana zgody na otrzymywanie informacji handlowych, newslettera lub akceptacji stosowania plików cookies. Profilowanie wykonywane jest w oparciu o posiadane dane tj w szczególności takie jak: dane dotyczące świadczonych usług, dane transmisyjne, dane o lokalizacji, informacje pozyskane za pomocą tzw. plików cookies. Profilowanie ma wpływ na informacje marketingowe oraz oferty jakie Pani/Pan będzie otrzymywać. Szczegółowe informacje dotyczące zautomatyzowanego podejmowania decyzji, w tym profilowania zawarte są w Polityce Prywatności.

Załącznik Nr 10 do
Polityki Ochrony Danych Osobowych
w Spółce Zakład Robót Komunikacyjnych
-DOM w Poznaniu Sp. z o.o.

Obowiązek informacyjny dla osób ubiegających się o świadczenia z Funduszu Świadczeń Socjalnych

Zgodnie z art. 13 ust. 1 i 2 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 2016 r., str. 1-88), zwanym dalej RODO, informuję, że:

1) Administratorem Pani/Pana Danych Osobowych jest Zakładu Robót Komunikacyjnych -DOM w Poznaniu Spółka z o.o., z siedzibą pod adresem: ul Kolejowa 4, 60-715 Poznań.
2) Administrator prowadzi operacje przetwarzania Pani/Pana danych osobowych.
3) Pani/Pana dane osobowe przetwarzane będą w celu przyznania świadczenia socjalnego przez Pracodawcę na podstawie Zakładowego Fundusz Świadczeń Socjalnych, a w związku z tym, także:
   a) Realizacji celów rachunkowych,
   b) Realizacji celów podatkowych,
   c) Dochodzenia roszczeń. .
4) Podanie danych jest niezbędne do skorzystania ze świadczeń socjalnych objętym wnioskiem, w przypadku niepodania danych uniemożliwia realizację przyznania świadczeń socjalnych.
5) Podstawą przetwarzania danych osobowych jest art.6 ust 1 lit. c RODO, zgodnie z którym przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze .
6) Pani/Pana dane osobowe nie będą udostępniane innym odbiorcom, chyba, że przepisy szczególne stanowią inaczej.
7) Pani/Pana dane osobowe nie będą przekazane do państwa nienależącego do Europejskiego Obszaru Gospodarczego (państwa trzeciego) lub organizacji międzynarodowej w rozumieniu RODO.
8) Pani/Pana dane osobowe będą przechowywane przez okres wymagany przepisami prawa niezbędny do przyznania i realizacji świadczenia socjalnego, realizacji obowiązku podatkowego, podatkowego oraz ubezpieczeń społecznych.
9) Ma Pani/Pan prawo do żądania dostępu do treści swoich danych oraz prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania lub do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
10) Ma Pani/Pan prawo do wniesienia skargi do organu nadzorczego ochrony danych osobowych.
11) Pani/Pana dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Potwierdzam przyjęcie do wiadomości powyższych informacji:

.....
data, czytelny podpis wnioskodawcy

Załącznik Nr 11 do
Polityki Ochrony Danych Osobowych
w Spółce Zakład Robót Komunikacyjnych
-DOM w Poznaniu Sp. z o.o.

Procedura Zarządzania Ryzykiem

2018 Rok

§1. Cel

Celem procedury jest określenie ryzyka w zakresie ochrony danych osobowych i zapewnienie że poziom ryzyka naruszenia praw i wolności osób fizycznych w odniesieniu do aktywów Spółki, które wiążą się z przetwarzaniem danych osobowych jest znany i monitorowany a wdrożone odpowiednie środki techniczne i organizacyjne zapewniają odpowiedni poziom ochrony. Wskazanie odpowiednich środków bezpieczeństwa są poddawane przeglądom i uaktualnieniom

§2. Zakres

1. Procedura opisuje proces Zarządzania Ryzykiem przyjmując ryzyko jako kombinację prawdopodobieństwo zdarzenia i jego negatywny wpływ na aktywa dla utraty poufności, integralności i dostępności danych osobowych.
2. Procedura obejmuje zasady przeprowadzania analizy, minimalizacji, monitorowania ryzyka oraz skuteczności zastosowanych rozwiązań.
3. Procedura ma zastosowanie dla wszystkich aktywów zidentyfikowanych w procedurze.
4. Procedura obowiązuje wszystkich pracowników Spółki odpowiedzialnych za aktywa.
5. Niniejsza procedura jednolite podejście w Spółce do Zarządzania Ryzykiem

§3. Role i odpowiedzialność

1. Nadzór nad realizacją procedury sprawuje pracownik do ochrony informacji wyznaczony w Spółce.
2. Zarząd Spółki:
    1) Zatwierdza raport z analizy ryzyka i wyznacza akceptowalny poziom ryzyka, w tym listę ryzyka nieakceptowalnych;
    2) Zatwierdza plan minimalizacji ryzyka, w tym zapewnia niezbędne środki na wdrożenie i utrzymanie zabezpieczeń;
    3) Powołuje zespół odpowiedzialny za przeprowadzenie procesu Zarządzania ryzykiem;
    4) Wyznaczana opiekunów poszczególnych grup aktywów;
    5)
3. Opiekunowie grup aktywów wyznaczeni w niniejszej procedurze:
    1) Przeprowadzają analizę ryzyka, w tym identyfikują zagrożenia i uwzględniają znane im zabezpieczenia;
    2) Uczestniczą w opracowaniu planu minimalizacji ryzyka proponując rozwiązania redukujące ryzyko;
4.

§4. Przygotowanie procesu szacowania ryzyka

1. Za przygotowanie i koordynację procesu szacowania ryzyka odpowiada przewodniczący zespołu.
2. Przeprowadzenie analizy ryzyka wymaga:
    1) Określenie kryteriów szacowania ryzyka i jego oceny;
    2) weryfikację lity aktywów w wyniku procesu inwentaryzacji aktywów, w przypadku potrzeby aktualizacji listy aktywów;
    3) utworzeniu grup aktywów i powołania opiekunów tych grup, w przypadku potrzeby aktualizacji tych grup;

4) sporządzenie planu analizy w przypadku planowanej analizy;
5) przeprowadzenia szkolenia lub spotkań zespołu

§4. Kryteria i szacowanie ryzyka

W celu uzyskania jednolitego podejścia do szacowania ryzyka ustala się następujące kryteria:

1. Prawdopodobieństwo:
   1) Oceniając prawdopodobieństwo należy wziąć pod uwagę:
      a) Informacje o zdarzeniach w przeszłości,
      b) Zakres i ilość przetwarzanych danych osobowych,
      c) Atrakcyjność danych
      d) Najbliższe otoczenie i środowisko w jakim są przetwarzane dane
   2) Szacowanie prawdopodobieństwa należy określić przyjmując następujące wartości:

Szacowana wartość	Znaczenie	Opis
1	Zagrożenie mało prawdopodobne	zdarzenie nie miało miejsca w ciągu ostatnich 5 lat
2	Zagrożenie prawdopodobne,	zdarzenie nie miało miejsca w ciągu ostatniego roku lat
3	Zagrożenie prawie pewne	Zdarzenie miało miejsca co najmniej dwa razy w ciągu ostatniego roku

2. Kryteria oceny skutków na aktywa dla utraty poufności, dostępności, integralności:
   1) Oceniając skutki utraty poufności, dostępności, integralności, należy wziąć pod uwagę:
      a) Straty finansowe, konsekwencje prawne, utraty wizerunku, utraty praw i wolności osób, czas i koszt odtworzenia aktywów
      b) Wymagania przepisów prawa
      c) Poufność danych
      d) Dostępność do danych
      e) Integralność danych
   2) Szacowanie skutków dla utraty poufności, dostępności, integralności należy zastosować następujące wartości:

Szacowana wartość	Skutek utraty	Opis
1	Skutek mały	Brak lub niewielska strata finansowa, Brak następstw prawnych
2	Skutek o średnim znaczeniu	Strata finansowa, następstwa prawne związane z karami, utrata wizerunku
3	Skutek o istotnym znaczeniu	Następstwa prawne, utrata wizerunku, poniesienie odpowiedzialności karnej

3) Wpływ skutków jest wyliczany automatycznie jako maksymalna wartość z szacowanych skutków utraty poufności, dostępności, integralności według poniższego wzoru:
***Wsk**=maksymalna wartość(podatność, integralności, dostępności)*

3. Ryzyko przyjmuje wartości podane w poniższej tabeli:

			Skutek		
			Niski 1	Średni 2	Wysoki 3
Prawdopodobieństwo	Prawie pewne	3	3	6	9
	Prawdopodobne	2	2	4	6
	mało prawdopodobne	1	1	2	3

Wartość wynikowa ryzyka dla analizy jakościowej prawdopodobieństwa i skutków utraty poufności, dostępności integralności może wynieść os 1 do 3 Zgodnie z metodyką szacowania ryzyka wartość ryzyka bez uwzględnionych zabezpieczeń wyliczana jest według wzoru:
R = P x S
Gdzie:
P – kryteria z punktu 1
S – kryteria z punktu 2

4. Zabezpieczenie: należy wpisać zastosowane zabezpieczenie organizacyjne lub techniczne, procedurę, politykę, jeżeli nie można wskazać to przyjęte w Spółce działanie nie opisane nigdzie ale wdrożone oraz według własnego doświadczenia i wiedzy określić siłę zabezpieczenia w przyjmując wartości:

Szacowana wartość	Zabezpieczenie	Opis
1	Zabezpieczenie słabe	Brak lub niewielka ochrona
2	Zabezpieczenie o średnim znaczeniu	Działa prawidłowo, jednak może zostać naruszone
3	Zabezpieczeni mocne, bezpieczne	Mocne działanie, niewielka możliwość naruszenia ochrony

1) Ryzyko po wprowadzeniu zabezpieczenia zastosowanego w spółce
Zgodnie z metodyką szacowania ryzyka wartość ryzyka z uwzględnionymi zabezpieczeniami wyliczana jest według wzoru:
Rz = R - Z

Gdzie:
R – wyliczenie ryzyka podane w punkcie 3
Z – kryteria oceny zabezpieczeń z punktu 4

5. Kryteria oceny ryzyka przedstawia poniższa tabela:

Poziom Ryzyka	Opis działania
Niski (N)	Poziom ryzyka akceptowany – działania podejmowane w zależności od wymaganych nakładów
Średni (Ś)	Poziom ryzyka akceptowalny – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
Wysoki (W)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania
Krytyczny (K)	Poziom ryzyka nieakceptowany – działanie nie może zostać przesunięte w czasie i wymaga działania

   1) Poziom ryzyka wysokiego i krytycznego i podjętych działań dla wszystkich zagrożeń ustala zespół kierując się swoimi kwalifikacjami, wiedzą i doświadczeniem.
   2) Ustalone kryteria o których mowa w pkt. 1 są podstawą do dokonania oceny ryzyka pod kątem akceptowalności tego ryzyka i jakie ryzyko wymaga podjęcia wdrożenia działań w kierunku minimalizacji jego.
   3) Ustalone kryteria w pkt. 2 z poziomu nieakceptowalnego mogą zostać przyjęte jako ryzyko tolerowane, wobec którego Zarząd Spółki może podjąć decyzję o akceptacji ryzyka.
6. Zespół z analizy ryzyka sporządza Raport, których akceptuje Zarząd Spółki.

§4. Raport analizy ryzyka

Raport z analizy ryzyka musi zawierać:

1. Datę w jakich przeprowadzono analizę ryzyka w oparciu o przyjętą metodykę.
2. Skład zespołu oraz pismo jakim zespół został wyznaczony.
3. Zidentyfikowane zagrożenia według katalogu zagrożeń dla określonych grup aktywów zgodnie z tabelą nr 1:

Numer zagrożenia	**Zagrożenie**

4. Grupa Aktywów objęta analizą z wskazaniem aktywów oraz opiekunów poszczególnych grup aktywów.

Grupa aktywów	**Aktywa**	**Opiekun Grupy aktywów**

5. Podsumowanie szacowania ryzyka poprzez wskazanie poszczególnych poziomów ryzyka z sumowaniem ilości występowania oraz w przypadku nieakceptowalnych poziomów ryzyka z wskazaniem proponowanych do podjęcia działań minimalizujących ryzyko. W szczególnych przypadkach z wskazaniem torelowania ryzyka gdy nie ma możliwości wprowadzenia działań organizacyjnych technicznych przy wystąpieniu ryzyka nieakceptowalnego.

Firma:	
Komórka organizacyjna:	
Imię i nazwisko wypełniającego ankietę:	
Stanowisko wypełniającego ankietę:	

Lp	Tyv Aktywów	Zagrożenia	Prawdopodobieństwo wystąpienia w skali 1 – 3	Wpływ skutków na aktywa dla utraty: (w skali 1-3)			Wpływ skutków (max. Wartość z kolumny 5,6,7)	**Ryzyko**		**Siła zabezpieczenia (w skali 1-3)**	**Ryzyko po wprowadzeniu zab .**	Opisać działania redukujące ryzyko
				Poufności	Integralności	Dostępności		**Pr*Wsk**	**Zabezpieczenie opis**			*Opis podjętych działań minimalizujących*
1	2	3	4	5	6	7	8	9		10	11	12

6. Wnioski i rekomendacje.

Załącznik Nr 12 do
Polityki Ochrony Danych Osobowych
w Spółce Zakład Robót Komunikacyjnych
-DOM w Poznaniu Sp. z o.o.

Klauzula informacyjna dla aplikujących na wolne stanowisko

Zgodnie z art. 13 ust. 1 i 2 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 (ogólne rozporządzenie o ochronie danych, Dz. Urz. UE L 119/1 z 2016 r.), zwanego dalej RODO, informuje się, że:

1. Administratorem Pani/Pana danych osobowych jest Spółka Zakład Robót Komunikacyjnych – DOM w Poznaniu Sp. z o.o. z siedzibą w Poznaniu, ul. Kolejowa 4, 60-715 Poznań.;

2. Pani/Pana dane osobowe przetwarzane będą w celu przeprowadzenia procesu rekrutacji na aplikowane przez Panią/Pana stanowisko, na podstawie art. 6 ust. 1 lit. a RODO;

3. Odbiorcą Pani/Pana danych osobowych będzie Zakład Robót Komunikacyjnych – DOM w Poznaniu Spółka z o.o.;

4. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania;

5. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo 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. Oświadczenie o cofnięciu zgody na przetwarzanie danych osobowych wymaga jego złożenia w formie pisemnej lub elektronicznej na adres mailowy praca@zrk-dom.com.pl;

6. Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

Oświadczenie osoby aplikującej

Oświadczam, że wyrażam zgodę na przetwarzanie przez Zaklad Robót Komunikacyjnych – DOM w Poznaniu Spółka z o.o. z siedzibą w Poznaniu, ul. Kolejowa 4 moich danych osobowych zawartych w CV oraz pozostałych dokumentach aplikacyjnych w celu i zakresie niezbędnym do przeprowadzenia procesu rekrutacji na aplikowane przeze mnie stanowisko.

Jednocześnie oświadczam, że przekazuję moje dane całkowicie dobrowolnie i zapoznałam/łem się z klauzulą informacyjną administratora, a w szczególności przysługującym mi prawie dostępu do treści tych danych oraz możliwości ich poprawiania, a także o prawie wycofania zgody na przetwarzanie tych danych w każdym czasie".

.....
(podpis składającego oświadczenie)