Wymagania w zakresie bezpieczeństwa informacji dla kontrahentów oraz podmiotów współpracujących z PKM Sp. z o.o. w Sosnowcu

§ 1.

Wymagania w zakresie bezpieczeństwa informacji dla kontrahentów oraz podmiotów współpracujących z PKM Sp. z o.o. w Sosnowcu stanowią dokument, którego celem jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych standardu przetwarzania informacji powierzanych kontrahentom oraz podmiotom współpracującym w związku z realizacją umów. Niniejszy dokument jest udostępniany każdemu kontrahentowi oraz podmiotowi współpracującemu przed zawarciem umowy.

§ 2.

Wymagania w zakresie bezpieczeństwa informacji dla kontrahentów oraz podmiotów współpracujących z PKM Sp. z o.o. w Sosnowcu zostały opracowane w oparciu o:

1. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024);
2. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U., poz. 745);
3. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U., poz. 719);
4. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2016 r., poz. 113);
5. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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)(Dz.Urz.UE L119 z 4 maja 2016 r.);
6. Wewnętrzne procedury w zakresie bezpieczeństwa informacji zawierających dane osobowe obowiązujące w PKM Sp. z o.o. w Sosnowcu.

§ 3.

Ilekroć w niniejszym dokumencie jest mowa o:

1. **Administratorze Danych Osobowych (ADO)** – należy przez to rozumieć organ, jednostkę organizacyjną, podmiot lub osobę decydujące o celach i środkach przetwarzania danych osobowych (kontrahenta);
2. **Administratorze Bezpieczeństwa Informacji (ABI)** – należy przez to rozumieć osobę fizyczną powołaną przez Administratora Danych Osobowych, odpowiedzialną za zapewnienie przestrzegania przepisów o ochronie danych osobowych oraz prowadzenie przez administratora danych wymaganej dokumentacji w tym zakresie. Po zmianie przepisów krajowych w związku z wejściem w życie Rozporządzenia

ogólnego (RODO), funkcję Administratora Bezpieczeństwa Informacji pełni **Inspektor Ochrony Danych Osobowych (IOD);**

3. **Informatyku (Administratorze Systemów Informatycznych – ASI)** – należy przez to rozumieć wyznaczoną przez ADO osobę fizyczną odpowiedzialną za bezpieczeństwo organizacyjne, fizyczne oraz techniczne danych osobowych przetwarzanych
w systemie informatycznym;
4. **Kontrahencie/podmiocie współpracującym** – należy przez to rozumieć stronę umowy;
5. **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
6. **PUODO** – należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych
7. **IZSI/Instrukcji** – należy przez to rozumieć obowiązujący u kontrahenta dokument o nazwie Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
8. **Nośnikach danych** – należy przez to rozumieć przedmioty fizyczne (elektroniczne, papierowe), na których możliwe jest zapisanie informacji w celu ich przechowywania, przetwarzania i transmisji;
9. **Odbiorcy danych** – należy przez to rozumieć każdego, komu udostępniane są dane osobowe, z wyłączeniem organów i osób wymienionych w art. 3 ust. 1 i 2 oraz art. 7 pkt 6 ustawy o ochronie danych osobowych;
10. **PBI / Polityce** – należy przez to rozumieć obowiązujący u kontrahenta dokument regulujący zasady bezpiecznego przetwarzania danych osobowych, zgodny z wymogami przepisów prawa, o których mowa w § 2 ust. 1-6;
11. **Pracowniku** – należy przez to rozumieć osobę fizyczną świadczącą pracę lub wykonującą czynności w oparciu o zawarte umowy cywilnoprawne w/na rzecz kontrahenta;
12. **Przetwarzaniu danych** – należy przez to rozumieć wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemie informatycznym;
13. **Systemie informatycznym (Systemie IT)** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych u kontrahenta w celu przetwarzania danych osobowych;
14. **Użytkowniku** – należy przez to rozumieć osobę, która uzyskała upoważnienie od kontrahenta do przetwarzania danych osobowych w systemie informatycznym oraz podpisała oświadczenie o zachowaniu poufności zobowiązującym ją do zachowania w tajemnicy przetwarzanych danych;

§ 4.

Wymagania w zakresie bezpieczeństwa informacji dla kontrahentów oraz podmiotów współpracujących z PKM Sp. z o.o. w Sosnowcu określają kryteria zapewnienia przez kontrahentów oraz podmioty współpracujące bezpieczeństwa informacjom zawierającym

dane osobowe, niezbędne środki organizacyjne i techniczne zapewniające ochronę tych danych, reguły postępowania w sytuacji naruszenia ich bezpieczeństwa oraz konsekwencje naruszenia przepisów o ochronie danych osobowych przez kontrahentów, ich pracowników oraz pozostałe osoby upoważnione przez kontrahentów do przetwarzania tych danych.

§ 5.

Utrzymanie bezpieczeństwa informacji, w tym w szczególności bezpieczeństwa danych osobowych przetwarzanych przez kontrahenta rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na poziomie wymaganym przepisami prawa.

§ 6.

Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych. Zarządzanie ryzykiem rozumiane jest jako proces identyfikowania, monitorowania i minimalizowania lub eliminowania ryzyka, które może dotyczyć systemów informatycznych i tradycyjnych służących do przetwarzania danych osobowych.

§ 7.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, pełni funkcję kontrolną w zakresie poprawnego przetwarzania danych osobowych oraz jest odpowiedzialny za zapewnienie środków organizacyjnych i technicznych służących utrzymaniu poziomu bezpieczeństwa tych danych, zgodnie w wymaganiami określonymi w przepisach prawa.

§ 8.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do prowadzenia aktualnej i zgodnej z przepisami prawa dokumentacji w postaci Polityki Bezpieczeństwa Informacji oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 9.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do ujawnienia Spółce obowiązujących u niego zasad w zakresie:

1) wypełniania obowiązku informacyjnego, wynikającego z przepisów prawa,
2) zastosowanych środków technicznych i organizacyjnych służących zachowaniu szczególnej staranności przy przetwarzaniu danych osobowych,
3) możliwości aktualizowania przetwarzanych danych osobowych, czasowego lub stałego wstrzymania przetwarzania danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane,
4) nadawania i anulowania upoważnień do przetwarzania danych osobowych oraz zgodności stosowanych upoważnień z wymaganiami określonymi w przepisach prawa,
5) ewidencjonowania osób upoważnionych do przetwarzania danych osobowych (wykaz osób upoważnionych do przetwarzania danych osobowych),
6) zobowiązywania osób upoważnionych do przetwarzania danych osobowych do zachowania ich w tajemnicy z określeniem okresu obowiązywania tego zobowiązania

(oświadczenie o zachowaniu poufności),

7) sprawowania kontroli nad udostępnianiem i powierzaniem danych osobowych oraz prowadzenia wymaganej przepisami dokumentacji w tym zakresie.

§ 10.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do przekazania informacji o wyznaczeniu oraz zgłoszeniu do PUODO Inspektora Ochrony Danych (IOD). W przypadku niepowołania IOD, funkcje mu przypisane kontrahent wypełnia osobiście w granicach przewidzianych przepisami prawa. Po zmianie przepisów krajowych w związku z wejściem w życie Rozporządzenia ogólnego (RODO), kontrahent / podmiot współpracujący będzie zobligowany do poinformowania Spółki o wypełnieniu formalności związanych z wyznaczeniem Inspektora Ochrony Danych Osobowych.

§ 11.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do określenia w dokumentacji bezpieczeństwa informacji kompetencji Inspektora Ochrony Danych Osobowych.

§ 12.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do opracowania zasad prowadzenia przez Inspektora Ochrony Danych Osobowych jawnego rejestru danych osobowych.

§ 13.

Inspektor Ochrony Danych Osobowych pełniący obowiązki u/na rzecz kontrahenta / podmiotu współpracującego zobowiązany jest do cyklicznego (nie rzadziej niż jeden raz w roku) przeprowadzania analizy ryzyk związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych oraz prowadzenia dokumentacji w tym zakresie.

§ 14.

Inspektor Ochrony Danych Osobowych pełniący obowiązki u/na rzecz kontrahenta / podmiotu współpracującego jest ponadto odpowiedzialny za prowadzenie i aktualizację dokumentacji w postaci:

1) wykazu pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania,
2) wykazu udostępnień danych osobowych innym podmiotom,
3) wykazu podmiotów, którym powierzono dane osobowe do przetwarzania,
4) wykazu udostępnień danych osobowych osobom, których dane dotyczą.

§ 15.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do wyznaczenia osoby (informatyka, administratora systemu), zobowiązanej do

sprawowania nadzoru nad bezpieczeństwem informacji przetwarzanych w systemie informatycznym stosowanym u kontrahenta / w podmiocie współpracującym.

§ 16.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do opracowania dokumentacji w postaci Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, określającej procedury nadawania uprawnień do przetwarzania danych osobowych przez użytkowników tego systemu, metody i środki uwierzytelniania, zasady konfiguracji oraz użytkowania sprzętu stacjonarnego oraz urządzeń mobilnych i elektronicznych nośników danych przez użytkowników systemu oraz zasady zabezpieczania danych w systemie informatycznym.

§ 17.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do opracowania procedur tworzenia i przechowywania kopii zapasowych, wykonywania przeglądów, konserwacji i napraw sprzętu wchodzącego w skład systemu informatycznego oraz zasad postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa tego systemu.

§ 18.

W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy prawa wymienione w § 2 ust. 1 – 6.