Warszawa, dnia 26.05.2023 r.

OŚWIADCZENIE FAPOMED POLSKA SPÓŁKA Z O.O.
W SPRAWIE ZASTRZEŻENIA MATERIAŁÓW STANOWIĄCYCH TAJEMNICĘ PRZEDSIĘBIORSTWA WRAZ Z UZASADNIENIEM

Działając w imieniu spółki FAPOMED POLSKA Spółka z o.o. z siedzibą w Warszawie (dalej „Spółka"), Spółka oświadcza, że zastrzega tajemnicę przedsiębiorstwa co do następujących kart katalogowych produktów: SET.020205, BAS.400.10, BAS.400.50, SET.070505, SET.070616, SET.CIS.02, GOW.70xx, GOW.71xx

UWAGA: Wykonawca wnosi o poinformowanie przez Zamawiającego z wyprzedzeniem o ewentualnym zamiarze odtajnienia zastrzeżonych dokumentów – w celu umożliwienia Wykonawcy obrony zasadności dokonanego zastrzeżenia tajemnicy przedsiębiorstwa przed Krajową Izbą Odwoławczą.

Uzasadnienie

1. **Stanowisko formalnoprawne - ogólnie**

Zastrzeżenie jawności informacji ze względu na tajemnicę przedsiębiorstwa stanowi wyjątek od zasady jawności postępowania, w związku z tym, przesłanki umożliwiające jego zastosowanie powinny być interpretowane ściśle. Zgodnie z brzmieniem art. 18 ust. 3 Pzp, wykonawca chcący zastrzec jawność zawartych w ofercie informacji stanowiących dla niego tajemnicę przedsiębiorstwa, zobowiązany jest zastrzec, wraz z przekazaniem takich informacji, że nie mogą być one udostępniane oraz wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.

W celu skutecznego zastrzeżenia tajemnicy przedsiębiorstwa, konieczne jest zatem nie tylko wykazanie, iż dane informacje spełniają obiektywne przesłanki uznania za tajemnicę przedsiębiorstwa w rozumieniu w art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji z dnia 16 kwietnia 1993 r. (tj. z dnia 8 października 2020 r., Dz.U. z 2020 r. poz. 1913 z późn. zm.), zwaną dalej „uznk", ale również – prawidłowe wykazanie tego faktu nie później niż w momencie ich przekazania.

Brak złożenia w ofercie uzasadnienia lub też złożenie niedostatecznie przekonującego uzasadnienia skutkować musi odtajnieniem przedmiotowych informacji. Obowiązek zbadania prawidłowości dokonanego przez wykonawcę zastrzeżenia spoczywa na Zamawiającym, który

zgodnie z art. 18 Pzp, jak również art. 16 Pzp, zobowiązany jest do rzetelnego przeprowadzenia tej czynności i ujawnienia informacji nieprawidłowo objętych przez wykonawcę klauzulą tajemnicy przedsiębiorstwa. Zgodnie z poglądami doktryny: *„W orzecznictwie KIO ugruntowało się stanowisko, że wymóg wykazania, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa oznacza, że nie składając wyjaśnień, a także w niezbędnym zakresie stosownych dowodów wykonawca rezygnuje w postępowaniu o udzielenie zamówienia z ochrony informacji, które uprzednio poza tym postępowaniem mogły spełniać przesłanki z art. 11 ust. 4 ZNKU"* (tak wyr. KIO z 28.4.2016 r.: KIO 545/16, Legalis; KIO 563/16, Legalis oraz z 3.4.2015 r., KIO 561/15, Legalis; z 28.8.2015 r., KIO 1730/15, Legalis). Pogląd ten znajduje także odzwierciedlenie w orzecznictwie sądów powszechnych – zob. wyr. SO w Przemyślu z 11.5.2015 r., I Ca 131/15, niepubl." (M. Jaworska (red.), Prawo zamówień publicznych. Komentarz, wyd. 6, 2018 r.).

Uzasadniając zastrzeżenie informacji jako tajemnicy przedsiębiorstwa, wykonawca powinien w stosunku do każdej z tych informacji wskazać i udowodnić, iż spełniają one przesłanki z art. 11 ust. 2 uznk. Nie jest wystarczające przy tym jedynie twierdzenie wykonawcy, iż informacja takie przesłanki spełnia, ale konieczne jest tego konkretne wykazanie, w odniesieniu nie tylko do rodzaju zastrzeżonych informacji, ale do konkretnych danych podlegających zastrzeżeniu przez wykonawcę. Powoływane przez wykonawcę w uzasadnieniu zastrzeżenia określone okoliczności muszą mieć charakter obiektywny i weryfikowalny, a także powinny być – stosownie do możliwości i potrzeby – poparte dowodami (np. w zakresie wykazania jakie czynności lub środki bezpieczeństwa zostały przez wykonawcę podjęte w celu zachowania określonej informacji w poufności). Przy czym w orzecznictwie Izby, wielokrotnie podkreślano, że nie jest wystarczającym powołanie się na stosowanie takich środków, konieczne jest przedstawienie dowodów potwierdzających ich stosowanie, a nie sprostanie ciężarowi dowodu w tym zakresie powinno skutkować ujawnieniem zastrzeżonych informacji.

Zasadność odtajnienia w odniesieniu do całości zastrzeżonych informacji uzasadnia nie tylko złożenie wyjaśnień ogólnych, ale również brak przedłożenia dowodów uzasadniających podjęcie działań mających na celu zachowanie informacji w poufności. W wyroku KIO z dnia 9 czerwca 2020 KIO 477/20, Izba wprost stwierdziła, że mimo iż zastrzeżone dokumenty (wyjaśnienia ceny) co do zasady posiadały walor tajemnicy jednak w związku z brakiem dowodów odtajnieniu podlegała cała ich treść. Ciężar udowodnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa spoczywa na wykonawcy, który przedmiotowego zastrzeżenia dokonuje. Powyższe stanowisko znajduje potwierdzenie w orzecznictwie Izby, zgodnie z którym *„ciężar udowodnienia skuteczności poczynionego zastrzeżenia tajemnicy przedsiębiorstwa spoczywa na podmiocie, który z tego działania wyciąga korzystne dla siebie skutki prawne"* (wyrok KIO z dnia 7 listopada 2011 r., KIO 2255/11, KIO 2283/11).

Za tajemnicę przedsiębiorstwa nie można uznać takich informacji, które są powszechnie dostępne, były lub zostaną ujawnione publicznie, lub wobec których wykonawca nie podjął

właściwych kroków zmierzających do zachowania ich poufności. W szczególności, zastrzeżenie jawności nie może być skuteczne w zakresie, w jakim obejmuje:

a) treść uzasadnienia zastrzeżenia określonych informacji jako tajemnica przedsiębiorstwa – treść takiego uzasadnienia z pewnością nie może zostać uznana za wypełniającą przesłanki tajemnicy przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji. Wyjaśnienia uzasadniające na czym polega poufny charakter informacji zawartych w składanych wyjaśnieniach nie zawierają informacji wrażliwych, o wartości gospodarczej, które zasługiwałyby na objęcie ich klauzulą poufności. Utajnienie takiego uzasadnienia rozpatrywać należy raczej w kategorii utrudniania konkurencyjnym wykonawcom skorzystania ze środków ochrony prawnej i podważania zasadności zastrzeżenia tajemnicy przedsiębiorstwa dokonanego przez wykonawcę;

b) informacje wskazywane w wykazie usług oraz dokumentach potwierdzających ich należyte wykonanie, a dotyczące zamówień realizowanych na rzecz podmiotów publicznych lub innych, zobowiązanych do stosowania ustawy o dostępie do informacji publicznej. Takie informacje jako podlegające udostępnieniu na wniosek jakiegokolwiek podmiotu, nie posiadają przymiotu poufności i nie mogą stanowić tajemnicy przedsiębiorstwa. Zasada ta dotyczy jakichkolwiek umów zawieranych z podmiotami zobowiązanymi do stosowania wyżej wskazanej ustawy, a więc nie tylko tych, podlegających regulacjom Prawa zamówień publicznych. Wykonawca dokonujący zastrzeżenia jawności informacji związanych z tego rodzaju zamówieniami, nie ma zatem możliwości obiektywnego wykazania zaistnienia w stosunku do nich wszystkich przesłanek określonych w art. 11 ust. 2 uznk. Poza tym, przesłanek uznania za tajemnicę przedsiębiorstwa nie spełniają również automatycznie zamówienia wykonywane dla podmiotów prywatnych, gdyż w stosunku do takich usług, również konieczne jest wykazanie zasadności uznania ich za tajemnicę przedsiębiorstwa, co zostało potwierdzone m.in. w wyroku KIO z dnia 10 kwietnia 2014 r., sygn. KIO 594/14;

c) informacje dotyczące zakresu udostępnionych zasobów oraz podmiotów udostępniających wykonawcy swoje zasoby, w szczególności w przypadku, gdy podmiot taki będzie brał udział w realizacji zamówienia jako podwykonawca, co oznacza, iż fakt współpracy z wykonawcą zostanie ujawniony na etapie realizacji zamówienia. Zastrzeżenie tego rodzaju informacji nie może być skuteczne jedynie w oparciu o deklarację wykonawcy, ale wymaga uzasadnienia i udowodnienia, iż zostały spełnione wszystkie przesłanki uznania ich za tajemnicę przedsiębiorstwa - tak stanowisko Krajowej Izby Odwoławczej wyrażone w wyroku z dnia 11 sierpnia 2014 r., sygn. KIO 1535/14;

d) informacje faktyczne i prawne dotyczące rozwiązania przed czasem wcześniejszych umów w sprawie zamówienia publicznego – tego typu informacje nie mogą zostać uznana za wypełniające przesłanki tajemnicy przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji, gdyż z racji tego, że dotyczą one informacji o realizacji umowy w sprawie zamówienia publicznego, to podlegają one udostepnieniu na podstawie ustawy o dostępie do informacji publicznej;

e) informacje nie zastrzeżone skutecznie jako tajemnica przedsiębiorstwa w toku ubiegania się o udzielenie zamówienia publicznego w innych postępowaniach, w tym w tych poprzednio prowadzonych przez Zamawiającego. Nawet jednorazowe udostępnienie danej informacji w innym postępowaniu powoduje, że staje się ona dostępna dla innych podmiotów, a zatem nie spełnia jednej z przesłanek określonych w art. 11 ust. 2 uznk.

2. Stanowisko formalnoprawne – omówienie przesłanek z art. 11 ust. 2 uznk

Zgodnie z legalną definicją tajemnicy przedsiębiorstwa, zamieszczoną w art. 11 ust. 2 uznk: *„przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności”*.

Z przytoczonej definicji wynika, iż za tajemnicę przedsiębiorstwa może być uznana określona informacja (wiadomość), jeżeli spełnia łącznie trzy warunki: ma charakter techniczny, technologiczny, organizacyjny lub inny posiadający wartość gospodarczą, która nie jest powszechnie znana albo łatwo dostępna dla osób zwykle zajmujących się tym rodzajem informacji, a także podjęto w stosunku do tej informacji (przy zachowaniu należytej staranności) działania w celu utrzymania jej w poufności. W dalszej części niniejszego oświadczenia, Wykonawca wskazuje na spełnienie poszczególnych przesłanek zakwalifikowania zastrzeżonych informacji jako tajemnicy przedsiębiorstwa, powołując się na dorobek orzecznictwa w tym zakresie. Cytowane orzeczenia odnoszą się do pojęcia tajemnicy przedsiębiorstwa, zawartego w art. 11 ust. 4 uznk (przed zmianą wprowadzoną na podstawie art. 1 pkt 1) ustawy z dnia 5 lipca 2018 r. o zmianie ustawy o zwalczaniu nieuczciwej konkurencji, która weszła w życie w dniu 4 września 2018 r.), lecz w odniesieniu do nowej definicji tajemnicy przedsiębiorstwa, zawartej w art. 11 ust. 2 uznk pozostają w dalszym ciągu aktualne.

Przyjmuje się, że informacja ma charakter techniczny, gdy dotyczy szeroko pojętych rozwiązań technicznych. Informacja cechuje się natomiast charakterem technologicznym, kiedy dotyczy najogólniej rozumianych sposobów wytwarzania, formuł, wzorów i metod działania.

Informacjami organizacyjnymi są natomiast dane używane w bieżącej działalności przedsiębiorstwa, takie np. jak struktura organizacyjna, procedury organizacyjne, procedury zdalnego dostępu, numery telefonów wewnętrznych, kody księgowe, systemy przetwarzania informacji, instrukcje i procedury bezpieczeństwa. Ze względu na indywidualny charakter informacji, mogących stanowić tajemnicę przedsiębiorstwa, nie jest możliwe ich wyczerpujące wyliczenie.

W orzecznictwie Sądu Najwyższego wskazano, że informacja staje się "tajemnicą", kiedy przedsiębiorca przejawia wolę zachowania jej jako niepoznawalnej dla osób trzecich. Nie traci natomiast swojego charakteru przez to, że wie o niej pewne ograniczone grono osób zobowiązanych do dyskrecji (np. pracownicy przedsiębiorstwa). Pozostanie określonych informacji tajemnicą przedsiębiorstwa wymaga, aby przedsiębiorca podjął działania zmierzające do wyeliminowania możliwości ich dotarcia do osób trzecich w normalnym toku zdarzeń, bez konieczności podejmowania szczególnych starań (por. np. orzecz. SN - Izba Cywilna z 6.06.2003, IV CKN 211/01; orzecz. SN z dnia 3.10.2000 r., I CKN 304/00, OSNC 2001, nr 4, poz. 59 oraz orzecz. SN z dnia 5.09.2001 r., I CKN 1159/00, OSNC 2002, nr 5, poz. 67). *„Art. 11 ust. 1 Ustawy o zwalczaniu nieuczciwej konkurencji - istnienie zasięgu stanu tajemnicy - uzależnia od podjęcia przez przedsiębiorcę określonych działań zmierzających do zachowania poufności objętych nią danych. Działania te - jak trafnie podnosi się w literaturze przedmiotu - powinny zmierzać do osiągnięcia takiego stanu, w którym osoby trzecie chcąc zapoznać się z treścią informacji, muszą doprowadzić do wyeliminowania przyjętych przez przedsiębiorcę mechanizmów zabezpieczających przed niekontrolowanym wypływem danych. Wybór informacji mających zostać objętymi poufnością należy oczywiście do przedsiębiorcy. Jednakże wybór ten, co do zakresu stanu tajemnicy, nie może być oderwany od możliwości podjęcia niezbędnych działań w celu zachowania w poufności wybranych informacji (art. 11 ust. 4 ustawy)”.* (zob. Wyrok Sądu Najwyższego - Izba Cywilna z 2001-09-05, I CKN 1159/00, opubl: OSNC 2002, Nr 5, poz. 67).

Odnośnie warunku trzeciego, należy zaznaczyć, iż podjęcie działań w celu zachowania poufności informacji ma prowadzić do sytuacji, w której chroniona informacja nie może dotrzeć do wiadomości osób trzecich zwykle zajmującym się tym rodzajem informacji w normalnym toku zdarzeń, bez żadnych specjalnych starań z ich strony, przy czym działania te powinny zostać powzięte przy zachowaniu należytej staranności uprawnionego, tj. być rozsądne w świetle danych okoliczności

2.1.Element formalny i materialny tajemnicy przedsiębiorstwa

W orzecznictwie przyjmuje się, że na tajemnicę przedsiębiorcy składają się łącznie dwa elementy: formalny i materialny (tak np. NSA w wyrokach z dnia 5 kwietnia 2013 r. sygn. akt I OSK 193/12 i z dnia 5 lipca 2013 r. sygn. akt I OSK 511/13).

Element formalny odnosi się do woli przedsiębiorcy utajnienia informacji i jego działań w celu zachowania określonych informacji w poufności, natomiast element materialny związany jest z zwartością gospodarczą informacji i z negatywnymi konsekwencjami jej ujawnienia w konkurencyjnym obrocie gospodarczym. W wyroku Naczelnego Sądu Administracyjnego w Warszawie z dnia 27 kwietnia 2017 roku (I OSK 2218/16) wskazano: *„Dla odmówienia udostępnienia informacji publicznej ze względu na tajemnicę przedsiębiorcy spełnione muszą być przesłanki formalne i materialne. Przesłanka formalna wyraża się w zamanifestowaniu woli konkretnego przedsiębiorcy utajnienia danych informacji. Z kolei przesłanka materialna polega na tym, że informacje objęte tajemnicą przedsiębiorcy powinny stanowić informacje, których ujawnienie mogłoby mieć wpływ na jego sytuację ekonomiczną, jakkolwiek nie muszą mieć same w sobie wartości gospodarczej."*

Przesłanka materialna – w postaci wymogu, aby zastrzeżone informacje stanowiły informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób – jest spełniona w stosunku do każdej z informacji wymienionych na wstępie.

Oczywistym jest różny charakter zastrzeżonych informacji, niektóre mają charakter techniczny lub technologiczny, inne zaś obejmują pewne informacje istotne z punktu widzenia organizacji przedsiębiorstwa jako takiego (sposobu kalkulacji cen, zabezpieczenia danych itp.), jednak z punktu widzenia skutecznego zastrzeżenia nie ma to znaczenia. Co istotne wyliczenie ustawowe nie jest przy tym wyczerpujące. Należy mieć też na uwadze stanowisko doktryny opowiadające się za liberalną wykładnią pojęcia wartości gospodarczej, które to zakłada, iż chodzi o minimalną aktualną lub potencjalną wartość gospodarczą informacji.

Uzasadnieniem uznania danej informacji za tajemnicę przedsiębiorstwa jest fakt, że istnieje realna możliwość, że udostępnienie innym podmiotom przedmiotowych informacji wpłynie negatywnie na pozycję Wykonawcy na rynku świadczonych przez niego usług/dostaw.

UWAGA: Wykonawca podnosi, iż uzyskanie przedmiotowych informacji przez jego konkurentów może doprowadzić do działań i sytuacji gospodarczo niekorzystnych, również w przyszłych potencjalnych zamówieniach, których realizacji mógłby podjąć się Wykonawca. Istotą przesłanki formalnej jest fakt, że informacja objęta tajemnicą nie może być łatwo dostępna dla osób postronnych. W doktrynie uznaje się, że „tajemnicą są wiadomości nieznane ogółowi lub osobom, które ze względu na swój zawód są zainteresowane posiadaniem takiej wiadomości. Wiadomość dotychczas nieznana traci ochronę, gdy każdy przedsiębiorca-współpracownik może się dowiedzieć o niej drogą zwykłą i dozwoloną". Zastrzeżone w niniejszym postępowaniu informacje nie są dostępne ogółowi lub osobom, które ze względu na swój zawód są zainteresowane posiadaniem takiej wiadomości, a Wykonawca podejmuje

stosowne środki ochrony mające na celu zachowania ich poufności, co szczegółowo zostało wykazane w stosunku do każdej z informacji wymienionych na wstępie.

3. **Odniesienie dotychczasowych wywodów do zastrzeganej zawartości kart katalogowych**

Zastrzegane dokumenty posiadają charakter handlowy, a więc mają wartość gospodarczą.

Karty katalogowe Spółki dla dedykowanych produktów oczekiwanych przez Zamawiającego nie są znane innym przedsiębiorcom poruszającym się na rynku dostaw, w którym funkcjonuje Spółka. W związku z tym ujawnienie kart katalogowych spowodowałoby konkretne, negatywne konsekwencje w obrocie gospodarczym Spółki.

Karty katalogowe produktów zawierają zatem informacje techniczne i technologiczne, a także obrazują posiadane przez Wykonawcę doświadczenie i wiedzę, decydujące o jego przewadze konkurencyjnej na rynku. Rozwiązanie to – jako know-how Wykonawcy – posiada zatem dla wykonawcy wartość gospodarczą, a tym samym podlega ochronie przed powszechnym ujawnianiem jako tajemnica przedsiębiorstwa.

W wyroku KIO z dnia 11 czerwca 2013 r., KIO 980/13, KIO 1067/13, KIO 1072/13, KIO 1073/13, KIO 1078/13, KIO 1080/13 wskazano, że: *„Uznano w powyższej mierze, że dobór konkretnych elementów sprzętu i oprogramowania, w ramach odpowiednich komponentów systemu, w tym opatrzenie ich dodatkowymi, wedle uznania wykonawcy elementami (przewidziana w części instrukcyjnej, poprzedzającej Tabelę 4 możliwość dopisania komponentów, jeżeli jest to konieczne w celu zapewnienia kompletności rozwiązania oferowanego przez wykonawcę) pozwala na uznanie, że w Tabeli 4, mimo że stanowi ona odwzorowanie wymagań zawartych w Opisie przedmiotu zamówienia, zawierane są informacje, które razem skomponowane w ten czy lub inny sposób przez danego wykonawcę wyrażają autorski zamysł co do kształtu poszczególnych narzędzi i komponentów, jakie zaplanowane zostały przez wykonawcę. W ramach danego komponentu Zamawiający przewidywał bowiem jedynie w sposób ogólny rodzaj sprzętu lub kategorie oprogramowania, zaś rzeczą wykonawców było wypełnienie tego wymagania konkretnymi produktami: odpowiednim sprzętem oraz oprogramowaniem, w tym dodanie - według własnej koncepcji danego wykonawcy - innych elementów sprzętu lub oprogramowania, wreszcie, dopełnienie ich oprogramowaniem autorskim, stworzonym na potrzeby przedmiotowego postępowania. W tej mierze uzewnętrzniało się zatem w Tabeli 4 autorskie rozwiązanie wykonawcy, wyrażające technologiczny i organizacyjny charakter informacji, które posiadają wartość gospodarczą."*

Analogicznie na gruncie niniejszej sprawy mamy do czynienia z ogólnymi wymaganiami technicznymi Zamawiającego określanymi w SWZ. Z kolei produkt zapewniany przez Wykonawcę w swojej specyfikacji technicznej stanowi dopełnienie wymagań

Zamawiającego według autorskich rozwiązań Wykonawcy zawartych w kartach katalogowych produktów. Karty zaś wyrażają technologiczny i organizacyjny charakter informacji, które posiadają wartość gospodarczą.

Zastrzegane informacje, nie są powszechnie znane i niewątpliwie mają istotną wartość gospodarczą - w szczególności mogą być wykorzystywane przez konkurencyjne podmioty np. do produkcji konkurencyjnych wyrobów lub w działalności marketingowej promującej konkurencyjne wyroby.

Ujawnienie zastrzeżonych informacji w niniejszym postępowaniu może wyrządzić Spółce szkodę. Szkoda ta będzie polegała na tym, że konkurencja Spółki poweźmie wiedzę na specyfikacji technicznej produktów Spółki, co będzie prowadziło do naśladownictwa produktów Spółki. W tym właśnie Spółka upatruje szkody.

Z tego powodu karty katalogowe produktów, jak i specyfikacje techniczne to nie dokumenty powszechnie dostępne i nie przeznaczone do nieograniczonego kręgu odbiorców. Dla Spółki treść kart katalogowych to zbiór pojedynczych parametrów, który jest uznany za informację podlegającą ochronie (zgodnie z wyrokiem KIO 2421/17 z 13 grudnia 2017 r.).
Ponadto powszechnie stosowaną praktyką przez podmioty z branży medycznej jest zastrzeganie tajemnicy w zakresie kart katalogowych i specyfikacji, co świadczy o realnym ryzyku wykorzystywaniu tych informacji przez konkurencję.

4. Sposób ochrony materiałów stanowiących tajemnicę przedsiębiorstwa

W stosunku do zastrzeganej dokumentacji podjęto działania w celu zachowania poufności - dokumenty te są traktowane jako poufne, ich ujawnienie osobom trzecim następuje tylko w szczególnie uzasadnionych wypadkach, a w razie złożenia tych dokumentów w postępowaniach o udzielenie zamówienia publicznego zastrzega się ich tajność zgodnie z art. 8 ust. 3 ustawy Pzp.

Wyrazem podejmowanych przez Spółkę działań ochronnych jest m.in. wprowadzenie w życie i egzekwowanie polecenia służbowego dotyczącego dokumentów zawierających tajemnicę przedsiębiorstwa, dokumenty są przechowywane w miejscach zabezpieczonych przed dostępem osób nieuprawnionych i, poza szczególnymi wyjątkami opisanymi poleceniu służbowym, nie są ujawniane osobom trzecim.

Wykonawca przedkłada m.in. wyciągi następujących regulacji obowiązujących w Spółce, których celem jest ochrona danych stanowiących tajemnicę przedsiębiorstwa oraz danych osobowych:

a) Załącznik nr 1 - Szczegółowe środki ochrony tajności informacji FAPOMED POLSKA Spółka z o.o.

b) Załącznik nr 2 – Wyciąg: obowiązek zachowania poufności z Regulaminu Ochrony Danych Osobowych w FAPOMED POLSKA Spółka z o.o.

c) Załącznik nr 3 – Wyciąg z Polityki Bezpieczeństwa informacji w FAPOMED POLSKA Spółka z o.o.

5. Podsumowanie

Mając na względzie wnioski wypływające z powołanej legalnej definicji tajemnicy przedsiębiorstwa Spółka oświadcza, że:

1. poprawnie zakwalifikowała informacje zawarte we wskazanych dokumentach – kartach katalogowych jako zawierające tajemnicę przedsiębiorstwa w rozumieniu 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji oraz wypracowanej przez doktrynę i judykaturę wykładni tego przepisu;
2. żadna z informacji wyżej wymienionych nie była uprzednio znana albo łatwo dostępna osobom zwykle zajmującym się tym rodzajem informacji, a także nie ma możliwości podjęcia o niej wiedzy tzw. „zwykłą" drogą;
3. Wykonawca podjął, przy zachowaniu należytej staranności, działania w celu utrzymania w/w informacji w poufności.

Pragniemy także wskazać, iż Europejski Trybunał Sprawiedliwości uznał ochronę tajemnicy handlowej za ogólną zasadę (wyrok z dnia 24 czerwca 1986 r. w sprawie 53/85 AKZO Chemie i AKZO Chemie UK przeciwko Komisji Rec., str. 1965, pkt 28 oraz wyrok z dnia 19 maja 1994 r. w sprawie C-36/92 P SEP przeciwko Komisji, Rec. Str. I-1911, pkt 37). Nieujawnienie zatem informacji, stanowiącej tajemnicę przedsiębiorstwa, która została przez Wykonawcę zastrzeżona w ofercie, nie narusza zasady uczciwej konkurencji i równego traktowania, a wręcz przeciwnie – stanowi wyraz ochrony uprawnionych interesów podmiotów gospodarczych uczestniczących w postępowaniu przetargowym.

Wykaz załączników:

d) Załącznik nr 1 - Szczegółowe środki ochrony tajności informacji FAPOMED POLSKA Spółka z o.o.
e) Załącznik nr 2 – Wyciąg: obowiązek zachowania poufności z Regulaminu Ochrony Danych Osobowych w FAPOMED POLSKA Spółka z o.o.
f) Załącznik nr 3 – Wyciąg z Polityki Bezpieczeństwa informacji w FAPOMED POLSKA Spółka z o.o.

_____

Za Spółkę – na podstawie udzielonego pełnomocnictwa

Załącznik nr 1 - Szczegółowe środki ochrony tajności informacji w FAPOMED POLSKA Spółka z o.o.

1. środki ochrony fizycznej:

1.1. zbiory danych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi; drzwi oddzielające halę od pomieszczeń biurowych mają właściwości przeciwpożarowe;
1.2. dostęp do pomieszczeń, w których przetwarzane są zbiory danych przez całą dobę jest nadzorowany przez służbę ochrony;
1.3. zbiory danych w formie papierowej przechowywane są w pomieszczeniach zamykanych na klucz, w szafach, częściowo zamykanych na klucz;
1.4. dane przetwarzane na serwerach zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych; kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej i usuwane są niezwłocznie po ustaniu ich użyteczności;
1.5. dokumenty zawierające dane poufne po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów;

2. środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej:

2.1. zbiory danych przetwarzane są przy użyciu komputerów stacjonarnych oraz komputerów przenośnych; osoby użytkujące komputer przenośny zawierający dane zachowują szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przedsiębiorstwa, w tym stosują środki ochrony kryptograficznej wobec przetwarzanych danych osobowych;
2.2. zastosowano urządzenia chroniące system informatyczny służący do przetwarzania danych przed skutkami awarii zasilania;
2.3. dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane poufne zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika (każdy użytkownik posiada odrębny identyfikator) oraz hasła; dostęp do systemu informatycznego, w którym przetwarzane są dane poufne zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika (każdy użytkownik posiada odrębny identyfikator) oraz hasła; identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie;
2.4. zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł dostępu do systemu operacyjnego komputera, w którym przetwarzane są dane;
2.5. zastosowano środki kryptograficznej ochrony danych dla danych przekazywanych drogą teletransmisji;

2.6. w sieci LAN zastosowano macierz dyskową w celu ochrony danych przed skutkami awarii pamięci dyskowej;
2.7. zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity;
2.8. użyto system Firewall do ochrony dostępu do sieci komputerowej;

3. środki ochrony w ramach systemowych narzędzi programowych i baz danych:

3.1. dostęp do zbiorów danych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
3.2. zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbiorów danych osobowych;
3.3. zastosowano wygaszacze ekranów i mechanizm automatycznej blokady dostępu do systemu operacyjnego komputera, a którym przetwarzane są dane, w przypadku nieaktywności pracy użytkownika

_____

Za Spółkę – na podstawie udzielonego pełnomocnictwa

Załącznik nr 2 – Wyciąg: obowiązek zachowania poufności z Regulaminu Ochrony Danych Osobowych w FAPOMED POLSKA Spółka z o.o.

Obowiązek zachowania poufności

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:

   a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w upoważnieniu do przetwarzania danych osobowych,
   b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem powierzonych zadań,
   c. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   d. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym przetwarzaniem danych osobowych.

2. Osoba upoważniona do przetwarzania danych osobowych zostaje przeszkolona z zasad ochrony danych osobowych.

3. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania organizacji, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta organizacja, oraz informacji kontaktowych innych, niż ogólnodostępne.

Postanowienia końcowe

1. Wszyscy pracownicy upoważnieni do przetwarzania danych osobowych zobowiązani są do stosowania się do zapisów Regulaminu.

2. Nieprzestrzeganie postanowień Regulaminu traktowane będzie jako niewykonywanie obowiązków i naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.

3. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę za naruszenie przepisów zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

_____

Za Spółkę – na podstawie udzielonego pełnomocnictwa

Załącznik nr 3 – Wyciąg z Polityki Bezpieczeństwa informacji w FAPOMED POLSKA Spółka z o.o.

Do biura FAPOMED POLSKA Spółka z o.o. prowadzą drzwi, które zabezpieczone są zamkiem. Kluczami do drzwi dysponują tylko osoby upoważnione. Budynek jest zabezpieczony alarmem. Budynek objęty jest całodobową ochroną zapewnioną przez administratorów. W budynku znajduję się wydzielone pomieszczenia, do każdego z pomieszczeń prowadzą drzwi z możliwością zamknięcia na zamek. Do budynku jak i pomieszczeń mają dostęp tylko osoby uprawnione (pracownicy) w godzinach pracy firmy tj.: 7:00-17:00.

Podstawowe zasady bezpieczeństwa informacji

Dążąc do możliwe jak najlepszego zabezpieczenia informacji i aktywów wspierających ich przetwarzanie wprowadza się do stosowania podstawowe zasady bezpieczeństwa informacji:

• zasada „adekwatności zabezpieczeń" – stosowane zabezpieczenia muszą być adekwatne do zidentyfikowanych zagrożeń;
• zasada „bezpiecznego przetwarzania" - przetwarzanie informacji szczególnie chronionych powinno odbywać się wyłącznie w bezpiecznych środowiskach, tj. w wydzielonych systemach informatycznych, zabezpieczonych pomieszczeniach etc.;
• zasada „bezpiecznej współpracy z podmiotami zewnętrznymi" - dokumenty regulujące współpracę z podmiotami zewnętrznymi (m.in. treść umów i porozumień) zawierają zapisy dot. bezpieczeństwa informacji, w tym klauzule bezpieczeństwa o zachowaniu poufności;
• zasada „czystego biurka – w celu wyeliminowania ryzyka przypadkowego lub celowego odczytania informacji, ich skopiowania, zniszczenia lub zmodyfikowania przez osoby nieuprawnione, opuszczając stanowisko pracy należy usunąć z blatu biurka dokumenty zawierające informacje inne niż informacje o charakterze jawnym, umieszczając je w przeznaczonych do tego celu zabezpieczonych meblach biurowych: szafach, szufladach lub sejfach;
• zasada „czystego ekranu" - na czas nieobecności dostęp do komputera należy skutecznie blokować a po zakończeniu pracy komputer wyłączyć, chyba że musi on pracować w trybie ciągłym;
• zasada „doskonalenia" – polityka w Organizacji jest dostosowywany do zmieniających się warunków w oparciu o wyniki okresowo prowadzonego monitorowania i nadzoru, • zasada „najsłabszego ogniwa" – poziom bezpieczeństwa informacji wyznacza najsłabsze ogniwo (najsłabiej zabezpieczony element);
• zasada „uprawnionego dostępu" – korzystanie z aktywów informacyjnych odbywać się może tylko w oparciu o formalne uprawnienia do korzystania z wybranych aktywów;
• zasada „wiedzy uzasadnionej" – personel dysponuje wiedzą o aktywach informacyjnych w ograniczonym zakresie, niezbędnym do realizacji powierzonych im zadań.

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

Środki organizacyjne

Do zastosowanych przez Administratora Danych Osobowych i osoby przez niego upoważnione w FAPOMED POLSKA Spółka z o.o. środków organizacyjnych służących zapewnieniu poufności, integralności i rozliczności przy przetwarzaniu danych należy:

• Opracowanie i wdrożenie „Polityki bezpieczeństwa w zakresie ochrony danych osobowych w FAPOMED POLSKA Spółka z o.o.”
• Opracowanie i wdrożenie „Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w FAPOMED POLSKA Spółka z o.o.
• Wyznaczenie przez Inspektora Ochrony Danych Osobowych (IODO) i nadanie mu upoważnienia do przetwarzania danych osobowych.
• Nadanie przez IODO pracownikom, współpracownikom, wolontariuszom, praktykantom i stażystom organizacji upoważnień do przetwarzania danych osobowych.
• Nadawanie przez IODO pracownikom i współpracownikom organizacji upoważnień do przetwarzania danych osobowych w związku z realizacją projektów/zadań, w których organizacja będzie partnerem Nadawanie przez IODO pracownikom i współpracownikom organizacji upoważnień do przetwarzania danych osobowych w pozostałych przypadkach przetwarzania danych osobowych występujących w organizacji.
• Wyznaczenie Administratora Systemu Informatycznego.
• Sprawowanie przez IODO oraz ASI kontroli i nadzoru nad procesem wprowadzania danych osobowych do zbioru oraz ich udostępniania.
• Sprawowanie przez IODO i ASI kontroli nad wydanymi uprawnieniami do systemów teleinformatycznych, Inspektor Ochrony Danych prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych. Inspektor Ochrony Danych Osobowych wraz z Administratorem Systemu Informatycznego prowadzi ewidencje nadanych uprawnień do systemów teleinformatycznych.

Środki techniczne

Dla potrzeb ochrony danych osobowych przetwarzanych w organizacji w formie papierowej stosuje się zabezpieczenia polegające na przechowywaniu:

• dokumentacji bieżącej – w szafach zamykanych na zamki w obszarach przetwarzania danych osobowych,

• dokumentacja archiwalna i dokumentacja pracownicza jest przechowywana w specjalnie do tego celu przeznaczonej szafie Do zastosowanych w organizacji środków technicznych służących zapewnieniu poufności, integralności i rozliczalności przy przetwarzaniu danych należy:

Przelewy bankowe i międzybankowe – czy strony internetowe banków, w których organizacja posiada rachunki wymagają podania loginu i hasła, a każda osoba upoważniona do dokonywania przelewów posiada indywidualny klucz dostępu, czy gwarancję zachowania poufności danych stanowi także ograniczony krąg osób upoważnionych do jego obsługi.

Dostęp do danych osobowych przetwarzanych w systemach informatycznych chroniony jest poprzez zastosowanie loginów i haseł uniemożliwiających nieuprawnione korzystanie osobom nieupoważnionym ustawienie monitorów komputerów w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

W zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych w określonym systemie, przy czym dokumenty te nie mogą być sprzeczne z regulacjami określonymi w „Polityce bezpieczeństwa". AD za pośrednictwem IODO i ASI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz RODO i zasad ustanowionych w niniejszym dokumencie.

Klasyfikacja przetwarzanych informacji Informacje przetwarzane w FAPOMED POLSKA Spółka z o.o. klasyfikowane są w następujących grupach:

• dane osobowe (w rozumieniu przepisów dot. ochrony danych osobowych i RODO),

• tajemnice przedsiębiorstwa (informacje, których ujawnienie mogłoby narazić FAPOMED POLSKA Spółka z o.o. na szkodę oraz informacje wewnętrzne udostępniane na zasadzie „wiedzy uzasadnionej"),

• informacje jawne.

Ogólne zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych

Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.

Pracownicy mający dostęp do danych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.

Pracownicy mają obowiązek podczas pracy z danymi jak i po zakończeniu pracy odpowiednio zabezpieczyć dane, z którymi pracowali.

Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.

Niedopuszczalne jest wynoszenie materiałów zawierających dane poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.

Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.

Signature Not Verified
Dokument podpisany przez Joanna Bielska
Data: 2023.05.26 13:51:43 CEST

Za Spółkę – na podstawie udzielonego pełnomocnictwa