Załącznik nr 11 do SWZ

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu …… w Piotrkowie Trybunalskim pomiędzy:

Miejską Biblioteką Publiczną im. Adama Próchnika, ul. M. Curie-Skłodowskiej 3, 97-300 Piotrków Trybunalski, NIP: 771-23-49-820, reprezentowaną przez ……, zwaną dalej „Administratorem”,

a

…… (KRS/CEIDG, NIP, REGON), reprezentowaną/ym przez ……, zwaną/ym dalej „Podmiotem przetwarzającym”.

§ 1. Przedmiot i podstawa powierzenia

1. Administrator powierza Podmiotowi przetwarzającemu, na podstawie art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (dalej: RODO), przetwarzanie danych osobowych w zakresie i celu określonych w niniejszej umowie, w związku z realizacją umowy nr …… na usługi ochrony osób i mienia (dalej: Umowa główna).
2. Przez incydent rozumie się naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO oraz każde inne zdarzenie lub podejrzenie zdarzenia, które może zagrozić poufności, integralności lub dostępności danych osobowych lub informacji Administratora, w tym zdarzenia wskazane w załączniku nr 5 do Umowy głównej.
3. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora. Poleceniem są postanowienia Umowy głównej, jej załączników oraz dalsze pisemne (w tym e-mailowe) wskazówki Administratora.

§ 2. Zakres, charakter i cel przetwarzania

1. Cel przetwarzania: realizacja Umowy głównej, tj. ochrona osób i mienia w budynku Administratora.
2. Charakter przetwarzania (operacje na danych): wydawanie i odbiór kluczy oraz kart dostępu, prowadzenie ewidencji wejść i wyjść, bieżąca obserwacja obrazu z monitoringu wizyjnego, zabezpieczanie nagrań w razie zdarzenia i przekazywanie ich Administratorowi, przekazywanie niezbędnych informacji służbom (policji, straży pożarnej, straży miejskiej) w razie zagrożenia, odnotowywanie zdarzeń w książce pełnienia służby.
3. Kategorie osób, których dane dotyczą: pracownicy i współpracownicy Administratora, czytelnicy i uczestnicy wydarzeń, goście, dostawcy i wykonawcy oraz inne osoby przebywające w obiekcie.
4. Rodzaje przetwarzanych danych:
   1) imię i nazwisko;
   2) wizerunek utrwalony w systemie monitoringu wizyjnego oraz data i godzina zdarzenia;
   3) data i godzina wejścia i wyjścia, nazwa podmiotu i cel wizyty (jeżeli są odnotowywane w ewidencji);
   4) dane o wydanych kluczach, kartach i kodach dostępu (osoba, data i godzina wydania i zwrotu);

5) numer dokumentu tożsamości – wyłącznie jeżeli Administrator wskaże na piśmie, że jest to niezbędne dla danego rodzaju wejść [zapis do decyzji Administratora; domyślnie dokumentów tożsamości się nie ewidencjonuje];

6) dane zawarte w opisie zdarzeń w książce pełnienia służby, w zakresie niezbędnym do opisu zdarzenia.

5. Strony nie przewidują powierzenia szczególnych kategorii danych (art. 9 RODO) ani danych o wyrokach skazujących (art. 10 RODO). Jeżeli takie dane pojawią się incydentalnie (np. na nagraniu), Podmiot przetwarzający chroni je z zachowaniem co najmniej wymogów niniejszej umowy i załącznika nr 5 oraz niezwłocznie informuje o tym Administratora.

6. Czas przetwarzania: okres obowiązywania Umowy głównej oraz okres do zwrotu lub usunięcia danych zgodnie z § 6.

7. Dane są przetwarzane wyłącznie na terytorium Europejskiego Obszaru Gospodarczego. Przekazywanie danych do państw trzecich lub organizacji międzynarodowych wymaga uprzedniej pisemnej zgody Administratora.

§ 3. Obowiązki Podmiotu przetwarzającego

Podmiot przetwarzający zobowiązuje się w szczególności do:

1. przetwarzania danych wyłącznie zgodnie z poleceniami Administratora; jeżeli obowiązek przetwarzania wynika z prawa Unii lub prawa państwa członkowskiego, poinformowania o nim Administratora przed rozpoczęciem przetwarzania, o ile prawo nie zabrania takiej informacji;

2. niezwłocznego poinformowania Administratora, jeżeli jego zdaniem polecenie narusza RODO lub inne przepisy o ochronie danych;

3. nadania imiennych upoważnień osobom, które będą przetwarzać dane, prowadzenia ich ewidencji, zapewnienia, że osoby te zobowiązały się do zachowania poufności także po ustaniu zatrudnienia, oraz przeszkolenia ich z ochrony danych zgodnie z § 8 ust. 8 i 9 Umowy głównej;

4. stosowania środków technicznych i organizacyjnych odpowiednich do ryzyka, zgodnie z art. 32 RODO, w tym środków określonych w załączniku nr 5 do Umowy głównej;

5. niewykorzystywania danych do własnych celów, nietworzenia kopii danych (w tym nagrań, zdjęć ekranu, odpisów ewidencji) poza wymaganymi do realizacji Umowy głównej oraz niewynoszenia danych poza obiekt Administratora;

6. pomocy Administratorowi w realizacji praw osób, których dane dotyczą (art. 15–22 RODO); żądanie otrzymane od osoby Podmiot przetwarzający przekazuje Administratorowi w terminie 2 dni roboczych i nie udziela odpowiedzi bez uzgodnienia z Administratorem;

7. pomocy Administratorowi w wypełnianiu obowiązków z art. 32–36 RODO (bezpieczeństwo przetwarzania, zgłaszanie naruszeń, ocena skutków, konsultacje z organem nadzorczym), z uwzględnieniem charakteru przetwarzania i dostępnych informacji;

8. zgłaszania Administratorowi każdego incydentu niezwłocznie, nie później niż w ciągu 24 godzin od jego stwierdzenia, telefonicznie i e-mailem na dane z § 8. Zgłoszenie zawiera, o ile są znane: opis zdarzenia, czas i miejsce, kategorie i przybliżoną liczbę osób oraz danych, możliwe skutki oraz podjęte i planowane środki zaradcze. Brak pełnych informacji nie zwalnia z obowiązku terminowego zgłoszenia; informacje uzupełnia się na bieżąco. Podmiot przetwarzający zabezpiecza dowody (np.

nagrania, ewidencje), dokumentuje incydent i udziela pomocy w powiadomieniu organu nadzorczego i osób, których dane dotyczą;

9. prowadzenia rejestru kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO, i udostępniania go na żądanie Administratora lub organu nadzorczego;
10. współpracy z organem nadzorczym oraz niezwłocznego informowania Administratora o kontroli lub postępowaniu organu dotyczącym powierzonych danych;
11. nieudostępniania danych osobom trzecim, w tym służbom i organom, bez uprzedniego uzgodnienia z Administratorem; nagrania z monitoringu mogą być udostępniane wyłącznie przez Administratora lub za jego pisemną zgodą. Obowiązek ten nie dotyczy zawiadamiania służb o zagrożeniu zgodnie z § 4 ust. 1 Umowy głównej ani sytuacji, gdy udostępnienie jest wprost wymagane przepisami prawa; wówczas Podmiot przetwarzający niezwłocznie informuje Administratora, o ile prawo tego nie zabrania.

§ 4. Dalsze powierzenie (podwykonawcy)

1. Podmiot przetwarzający może skorzystać z usług innego podmiotu przetwarzającego (podwykonawcy) wyłącznie po uzyskaniu uprzedniej, pisemnej zgody Administratora wskazującej podwykonawcę i zakres powierzenia.
2. O zamiarze zmiany lub dodania podwykonawcy Podmiot przetwarzający informuje Administratora z co najmniej 14-dniowym wyprzedzeniem. Administrator może wyrazić sprzeciw.
3. Podwykonawca jest związany pisemną umową nakładającą te same obowiązki ochrony danych, które wynikają z niniejszej umowy i załącznika nr 5 do Umowy głównej. Na żądanie Administratora Podmiot przetwarzający przedstawia tę umowę (z pominięciem informacji handlowych).
4. Podmiot przetwarzający ponosi wobec Administratora pełną odpowiedzialność za wypełnienie obowiązków przez podwykonawcę.

§ 5. Kontrola i audyt

1. Administrator ma prawo kontrolować przestrzeganie niniejszej umowy, w tym przeprowadzać audyty i inspekcje w miejscu świadczenia usług oraz żądać informacji i dokumentów niezbędnych do wykazania wypełnienia obowiązków z art. 28 RODO.
2. Kontrola odbywa się po powiadomieniu Podmiotu przetwarzającego z co najmniej 3-dniowym wyprzedzeniem. Po wystąpieniu incydentu lub uzasadnionym podejrzeniu naruszenia kontrola może odbyć się bez zapowiedzi.
3. Podmiot przetwarzający usuwa stwierdzone uchybienia w terminie wskazanym w zaleceniach pokontrolnych, nie dłuższym niż 14 dni, chyba że Strony uzgodnią inaczej.
4. Kontrola nie może zakłócać ciągłości świadczenia usług ochrony.

§ 6. Zakończenie przetwarzania

1. W terminie 14 dni od zakończenia świadczenia usług Podmiot przetwarzający, według wyboru Administratora, zwróci lub trwale usunie wszystkie powierzone dane osobowe i ich kopie, w tym ewidencje wejść, ewidencje kluczy i kart, odpisy zdarzeń oraz nośniki z nagraniami, i potwierdzi to na piśmie (protokołem).

2. Jeżeli przepisy prawa wymagają dalszego przechowywania danych, Podmiot przetwarzający niezwłocznie poinformuje o tym Administratora, wskaże podstawę prawną i zapewni ich ochronę do czasu usunięcia.
3. Obowiązek zachowania poufności trwa także po zakończeniu przetwarzania, bez ograniczenia w czasie.

§ 7. Odpowiedzialność

1. Podmiot przetwarzający odpowiada za szkody powstałe w związku z przetwarzaniem danych niezgodnym z niniejszą umową lub RODO, na zasadach określonych w art. 82 RODO oraz w Umowie głównej.
2. W razie naruszenia obowiązków z niniejszej umowy stosuje się kary umowne przewidziane w § 15 ust. 8 Umowy głównej.
3. Poważne naruszenie niniejszej umowy uprawnia Administratora do rozwiązania Umowy głównej na zasadach określonych w jej § 17 ust. 4.

§ 8. Osoby kontaktowe

1. Administrator: Inspektor Ochrony Danych – Efigo Sp. z o.o., e-mail: iod@efigo.pl. Osoba do kontaktów w sprawie incydentów: ……, tel. ……, e-mail: …….
2. Podmiot przetwarzający: osoba do kontaktów w sprawie ochrony danych i incydentów: ……, tel. ……, e-mail: …….
3. Zmiana osób kontaktowych nie wymaga aneksu, a jedynie pisemnego lub e-mailowego zawiadomienia drugiej Strony.

§ 9. Postanowienia końcowe

1. Umowa wchodzi w życie z dniem rozpoczęcia obowiązywania Umowy głównej i obowiązuje przez okres jej trwania, z zastrzeżeniem § 6 ust. 3.
2. W zakresie ochrony danych osobowych w razie rozbieżności postanowienia niniejszej umowy mają pierwszeństwo przed Umową główną.
3. W sprawach nieuregulowanych stosuje się RODO oraz Kodeks cywilny.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

……	……
ADMINISTRATOR	**PODMIOT PRZETWARZAJĄCY**