POLITYKA BEZPIECZEŃSTWA INFORMACJI W „L'Art de la Danse" Towarzystwo Wspierania i Rozwoju Sztuki Baletowej w Krakowie

(Rynek Główny 34, 31-010 Kraków)

Kraków, dnia 25 maja 2018 r.

I. Postanowienia ogólne

1. Administratorem danych osobowych jest „L'Art de la Danse" Towarzystwo Wspierania i Rozwoju Sztuki Baletowej w Krakowie (adres do korespondencji: ul. Rynek Główny 34, 31-010 Kraków) (zwany dalej Administratorem).
2. Polityka dotyczy wszystkich Danych osobowych przetwarzanych przez Administratora niezależnie od formy ich przetwarzania oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
3. Polityka została stworzona dla:

a. Pracowników, posiadających dostęp do danych osobowych przetwarzanych przez Administratora,
b. Współpracowników, posiadających dostęp do danych osobowych przetwarzanych przez Administratora,
c. Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora,

Wszystkie w/w osoby na potrzeby niniejszej Polityki będą zwane w dalszej części Polityki Pracownikami.
4. Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych.
5. Dla skutecznej realizacji Polityki Administrator zapewnia:
a) odpowiednie do zagrożeń i kategorii danych, objętych ochroną środki techniczne i rozwiązania organizacyjne,
b) kontrolę i nadzór nad przetwarzaniem danych osobowych,
c) monitorowanie zastosowanych środków ochrony.
6. Monitorowanie przez Administratora zastosowanych środków ochrony obejmuje m.in. monitorowanie pracowników przetwarzających dane osobowe oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
7. Administrator zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą Polityką oraz odpowiednimi przepisami prawa.

II. Dane osobowe przetwarzane u Administratora

1.Administrator przetwarza dane osobowe wyłącznie wówczas, gdy spełniony jest, co najmniej jeden z poniższych warunków:

a. jest to niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy,
b. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego, ciążącego na Administratorze,
c. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej,
d. przetwarzanie jest niezbędne do celów, wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią,
e. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie danych osobowych w jednym lub większej liczbie określonych celów.

2. Administrator nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.

3. Administrator danych prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi **Załącznik nr 1** do niniejszej Polityki.

III. Obowiązki i odpowiedzialność z zakresie zarządzania bezpieczeństwem

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Polityką, a także innymi dokumentami wewnętrznymi i procedurami związanymi z przetwarzaniem danych osobowych.

2. Wszystkie dane osobowe są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:

a) W każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych.

b) Dane osobowe przetwarzane są rzetelnie i w sposób przejrzysty.

c) Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

d) Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych.

e) Dane osobowe są prawidłowe i w razie potrzeby uaktualniane.

f) Czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane.

g) Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny,

h) Dane są zabezpieczone przed naruszeniami zasad ich ochrony.

3. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych uważa się w szczególności:
a) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
d) niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
e) przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych;
g) naruszenie praw osób, których dane są przetwarzane.
5. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych podmiot przetwarzający dane osobowe w imieniu Administratora zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora.
6. Do obowiązków Administratora w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników należy dopilnowanie, by:
a) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków,
b) każdy z podmiotów przetwarzających dane osobowe w imieniu Administratora był pisemnie upoważniony do przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych" – wzór Upoważnienia stanowi **Załącznik nr 2** do niniejszej Polityki,
c) każdy pracownik zobowiązał się do zachowania danych osobowych przetwarzanych przez Administratora w tajemnicy - „Oświadczenie i zobowiązanie osoby przetwarzającej dane osobowe do zachowania tajemnicy" stanowi element „Upoważnienia do przetwarzania danych osobowych".
7. Pracownicy zobowiązani są do:
a) ścisłego przestrzegania zakresu nadanego upoważnienia;
b) przetwarzania i ochrony danych osobowych zgodnie z przepisami;
c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych.

IV. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są dane osobowe obejmuje biuro zlokalizowane w Krakowie przy ul. Rynek Główny 14, 31-010 Kraków.

2. Dodatkowo obszar, w którym przetwarzane są dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.

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

1. Administrator zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych kategorii danych.
3. Środki obejmują:
a. zabezpieczanie danych osobowych zgromadzonych w dokumentach w formie papierowej,
b. zasady bezpiecznego użytkowania sprzętów IT, dysków i programów,
c. zasady korzystania z poczty elektronicznej i Internetu,
d. zasady wynoszenia nośników danych poza siedzibę Administratora.

VI. Zabezpieczanie danych osobowych zgromadzonych w dokumentach w formie papierowej

1. Pracownicy są zobowiązani do stosowania tzw. „Polityki czystego biurka" w części biura, do którego dostęp mają Klienci bądź inne postronne osoby. Polityka czystego biurka polega na zabezpieczaniu (zamykaniu na klucz) dokumentów w szafach, szafkach i biurkach przed kradzieżą lub wglądem osób postronnych.
2. Na stanowisku pracy, w czasie, gdy w biurze są obecni klienci bądź inne osoby postronne powinien zawsze pozostawać przynajmniej jeden pracownik.
3. Po każdym wyjściu z biura albo poszczególnych jego pomieszczeń, zarówno biuro, jak i dane pomieszczenie powinno zostać zamknięte przez ostatnią wychodzącą z niego osobę.
4. Pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach.
5. Pracownicy nie mogą pozostawiać dokumentów w miejscach dostępnych dla osób postronnych, w tym klientów.
6. Zabrania się wyrzucania niezniszczonych dokumentów do śmietnika.

VII. Zasady bezpiecznego użytkowania sprzętów IT, dysków i programów

1. Pracownik odpowiada za zabezpieczenie przed zniszczeniem, uszkodzeniem oraz utratą sprzętu IT (komputerów, tabletów, smartfonów).
2. Podłączanie nowych urządzeń jest zabronione.
3. Pracownik jest zobowiązany do usuwania tymczasowych plików z miejsc, gdzie dostęp do nich miałyby osoby nieupoważnione.
4. Pracownicy są zobowiązani do przekazywania informatykowi nośników przeznaczonych do zniszczenia.
5. Każdy użytkownik komputerów, programów i systemu operacyjnego zobowiązany jest do pracy na własnym koncie. Zabronione jest udostępnianie konta innemu użytkownikowi.
6. Użytkownik komputera oraz programów rozpoczyna i kończy pracę logowaniem i wylogowaniem się.
7. Użytkownik komputera jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach.
8. Użytkownik komputera przed tymczasowym odejściem od komputera musi włączyć wygaszacz ekranu albo wylogować się z systemu bądź z programu.
9. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu, o ile nie została ona zweryfikowana przez informatyka.
10. Po zakończeniu pracy, użytkownik komputera zobowiązany jest wylogować się z systemu informatycznego oraz zabezpieczyć nośniki, na których znajdują się dane osobowe.
11. Dostęp do komputera powinien być chroniony hasłem.
12. Hasła powinny składać się z 8 znaków.
13. Hasła powinny zawierać duże litery + małe litery + cyfry.
14. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach, nie naklejać na monitorze komputera, nie trzymać w otwartym biurku albo szafce.
15. Hasła powinny być zmieniane raz na pół roku.

VIII. Zasady korzystania z poczty elektronicznej i Internetu

1. Pracownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
2. Pracownicy są zobowiązani zgłaszać informatykowi przypadki podejrzanych e-maili.
3. Podczas wysyłania wiadomości elektronicznej do wielu adresatów jednocześnie, należy korzystać z metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".
4. Pracownicy są zobowiązani do korzystania ze służbowych skrzynek pocztowych, celem wysyłania korespondencji służbowej. Zakazane jest

korzystanie z prywatnych skrzynek pocztowych na potrzeby służbowej korespondencji.
5. Zabrania się instalowania na służbowych komputerach programów ściągniętych z Internetu bez konsultacji z informatykiem
6. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie ściągnięte na służbowy komputer bez konsultacji z informatykiem.

IX. Zasady wynoszenia nośników z danymi osobowymi poza siedzibę Administratora

1. Użytkownicy nie mogą wynosić bez zgody Administratora, na zewnątrz, niezaszyfrowanych nośników z danymi osobowymi, tj. między innymi przenośnych dysków twardych, pen-drive, płyt CD, DVD, pamięci typu Flash, jak również dokumentów w wersji papierowej.
2. Dokumentacja papierowa, o ile istnieje potrzeba jej przeniesienia poza biuro Administratora, powinna być przewożona w teczce, celem jej zabezpieczenia przed zagubieniem bądź kradzieżą.

X. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zgłoszenia określa **Załącznik nr 3** do niniejszej Polityki.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.
4. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Pracodawcy / Zleceniodawcy w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
5. Do sytuacji wymagających powiadomienia, należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,

c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

6. Do incydentów wymagających powiadomienia, należą:

a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

7.Typowe przykłady incydentów wymagające reakcji:

d. ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
e. zniszczenie dokumentacji bez użycia niszczarki,
f. obecność w budynku lub pomieszczeniach biura osób zachowujących się podejrzanie,
g. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
h. ustawienie monitorów pozwalająca na wgląd osób postronnych w dane osobowe,
i. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Pracodawcy,
j. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
k. próby wyłudzenia danych osobowych – telefoniczne i mailowe,
l. kradzież, zagubienie komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi,
m. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
n. hasła do komputera są niezabezpieczone w pobliżu komputera.

XI. Powierzenie przetwarzania danych osobowych

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.

Wzór umowy powierzenia przetwarzania danych osobowych stanowi **Załącznik nr 4** do niniejszej umowy.
2. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.
1. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do:
a. przetwarzania danych osobowych wyłącznie w celu i zakresie powierzonych jej zadań
b. zachowania w tajemnicy danych osobowych do których ma
c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych jej zadań
d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
2. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego
3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych
4. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana zabezpieczenia danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem

XII. Przekazywanie danych do państwa trzeciego

Administrator Danych Osobowych nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.

XIII. Postanowienia końcowe

1.Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Integralną część niniejszej Polityki stanowią następujące Załączniki:
Załącznik nr 1 Wzór rejestru czynności przetwarzania
Załącznik nr 2 Wzór upoważnienia do przetwarzania danych osobowych
Załącznik nr 3 Wzór zgłoszenia incydentu naruszenia ochrony danych osobowych
Załącznik nr 4 Wzór umowy powierzenia przetwarzania danych osobowych

Załącznik nr 1 Wzór rejestru czynności przetwarzania

Opis kategorii osób, kategorie danych osobowych, kategorie odbiorców, terminy usunięcia, podstawa prawna przetwarzania	Nośniki, na których dane osobowe zostaną zapisane, Infrastruktura	Proces przetwarzania
1.Opis kategorii osób (nazwa zbioru) **2. Opis kategorii danych osobowych** **3. Cele przetwarzania** **4.Kategorie odbiorców danych osobowych** **5. Kategorie odbiorców w państwach trzecich lub w organizacjach międzynarodowych (i ich nazwy) –** **6. Planowane terminy usunięcia poszczególnych kategorii danych**	**1. Dokumentacja papierowa** **2. Programy i systemy operacyjne** **3. Infrastruktura IT** **4. Infrastruktura**	

Załącznik nr 4 Wzór umowy powierzenia przetwarzania danych osobowych

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w Krakowie, dnia …….. r. pomiędzy:

„L'art. de la Danse" Towarzystwo Wspierania i Rozwoju Sztuki Baletowej w Krakowie, ul. Rynek Główny 14, 31-010 Kraków, NIP: 676-21-55-000, reprezentowane przez …….

zwane w dalszej części niniejszej Umowy „Zleceniodawcą"

a

……..
…….

w dalszej części niniejszej Umowy zwanym „Zleceniobiorcą"

dalej łącznie zwanymi „Stronami"

Strony niniejszym postanawiają, co następuje:

1. Zleceniodawca oświadcza, że jest Administratorem danych osobowych.
2. Zleceniodawca powierza Zleceniobiorcy przetwarzanie danych osobowych w zakresie i celu określonym w niniejszej Umowie, a Zleceniobiorca zobowiązuje się przetwarzać te dane w sposób zapewniający spełnienie wymogów określonych w 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) jak również w innych przepisach mających zastosowanie do przetwarzania powierzonych danych i obowiązujących w trakcie realizacji umowy. Przedmiotową umową będą objęte dane osobowe zwykłe, a nie wrażliwe.
3. Powierzenie przetwarzania danych osobowych, o którym mowa w ust. 2, przez Zleceniodawcę obejmuje dane osobowe w zakresie: ……..
4. Celem przetwarzania danych przez Zleceniobiorcę jest wykonanie umowy polegającej na ……
5. Przedmiotem przetwarzania są dane osobowe wskazane w treści niniejszej Umowy.
6. Kategoria osób, których dotyczą dane powierzane do przetwarzania, obejmuje pracowników i klientów Zleceniodawcy.
7. Powierzone do przetwarzania dane osobowe będą przetwarzane przez Zleceniobiorcę w sposób ciągły i systematyczny, z wykorzystaniem systemów informatycznych oraz …….
8. Powierzone do przetwarzania dane osobowe będą przetwarzanie przez Zleceniobiorcę przez okres obowiązywania umowy o świadczenie usług księgowych.
9. Zleceniobiorca zobowiązuje się do:

a) wykorzystania powierzonych przez Zleceniodawcę danych osobowych wyłącznie w zakresie określonym w pkt 3 niniejszej Umowy i celu określonym w pkt 4 niniejszej Umowy, na udokumentowane polecenie Zleceniodawcy, chyba że obowiązek przetwarzania w inny sposób nakładają na Zleceniobiorcę przepisy prawa;

b) poinformowania Zleceniodawcy, przed rozpoczęciem przetwarzania, o obowiązku prawnym skutkującym koniecznością przetwarzania danych osobowych inaczej niż na udokumentowane polecenie Zleceniodawcy, chyba że przepisy prawa zabraniają udzielania takiej informacji z uwagi na ważny interes publiczny;

c) niewykonywania żadnych czynności związanych z dalszym przekazywaniem danych osobowych nieuregulowanych w niniejszej Umowie

d) zobowiązania osób upoważnionych do przetwarzania danych osobowych do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;

e) wdrożenia wymaganych przepisami prawa środków technicznych i organizacyjnych, zapewniających stopień bezpieczeństwa powierzonych do przetwarzania danych osobowych odpowiadający ryzyku naruszenia praw i wolności osób fizycznych w szczególności poprzez zastosowania urządzeń zapewniających pseudonimizację i szyfrowanie danych osobowych;

f) zgłaszania Zleceniodawcy naruszenia ochrony powierzonych do przetwarzania danych osobowych bez zbędnej zwłoki po stwierdzeniu tego naruszenia;

g) pomagania Zleceniodawcy w wywiązywaniu się z jego obowiązków związanych z przetwarzaniem powierzonych do przetwarzania danych osobowych;

h) niezwłocznego zwrócenia Zleceniodawcy danych osobowych po rozwiązaniu lub wygaśnięciu Umowy oraz usunięcia tych danych oraz ich kopii ze wszelkich elektronicznych nośników danych, na których zostały one utrwalone przez Zleceniobiorcę dla realizacji celu określonego w pkt 4 niniejszej umowy, chyba, że przepisy prawa nakazują przechowywanie tych danych;

i) wdrożenia wymaganych przepisami prawa środków zapewniających poufność, integralność, dostępność danych osobowych i odporność systemów wykorzystanych do ich przetwarzania;

j) regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

10. Prawidłowe usunięcie danych osobowych oraz ich kopii, o których mowa w pkt 9 lit. h, niniejszej Umowy zostanie potwierdzone pisemnym protokołem podpisanym przez Strony.
11. Zleceniobiorca jest odpowiedzialny wobec Zleceniodawcy z tytułu niewykonania lub nienależytego wykonania postanowień niniejszej Umowy. W przypadku, gdy wskutek naruszenia przez Zleceniobiorcę postanowień niniejszej Umowy Zleceniodawca zostanie obciążony karami pieniężnymi lub grzywną, wymierzoną Zleceniodawcy, osobom reprezentującym Zleceniodawcę lub pracownikom Zleceniodawcy z

powyższego tytułu, Zleceniobiorca zobowiązuje się do zapłaty kwoty równej wartości uiszczonej kary lub grzywny.

12. Zleceniodawca ma prawo do przeprowadzania kontroli zastosowanych przez Zleceniobiorcę sposobów ochrony powierzonych danych osobowych. Zleceniobiorca ma obowiązek umożliwienia Zleceniodawcy przeprowadzenia takiej kontroli niezwłocznie po wezwaniu. Jeżeli zdaniem Zleceniobiorcy polecenie wydane mu w związku z realizacją przez Zleceniodawcę prawa do kontroli stanowi naruszenie przepisów o ochronie danych, Zleceniobiorca niezwłocznie informuje o tym Zleceniodawcę.

13. Zleceniobiorca zobowiązuje się zająć niezwłocznie i właściwie każdym pytaniem Zleceniodawcy dotyczącym przetwarzania powierzonych mu na podstawie Umowy danych osobowych, w szczególności tych dotyczących organizacji ochrony danych osobowych u Zleceniobiorcy oraz związanych z żądaniem osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w przepisach o ochronie danych osobowych. W tym celu Zleceniobiorca wdroży odpowiednie środki techniczne i organizacyjne umożliwiające sprawne udzielenie Zleceniodawcy żądanych informacji.

14. Zleceniodawca upoważnia Zleceniobiorcę do przetwarzania danych osobowych w zakresie i celu określonym w niniejszej Umowie, a także do udzielenia dalszych upoważnień do przetwarzania danych osobom współpracującym z Zleceniobiorcą na podstawie umowy o pracę lub umowy cywilnoprawnej, które mają dostęp do przetwarzanych danych osobowych.

15. W przypadku gdy Zleceniodawca uzna to za konieczne, celem zapewnienia należytej najwyższej ochrony danych osobowych osób których one dotyczą, Zleceniobiorca zobowiązany jest pomóc Zleceniodawcy w realizowaniu obowiązków wynikających z powszechnie obowiązujących przepisów prawa w szczególności zawiadamianiu osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, ocenie skutków dla ochrony danych i uprzednich konsultacjach oraz zapewnieniu bezpieczeństwa danych osobowych.

16. Zleceniodawca oraz Zleceniobiorca zgodnie postanawiają, że w przypadku przesyłania danych osobowych, dane te będą należycie zabezpieczone.

17. Zleceniodawca ma prawo odstąpić od Umowy gdy Zleceniobiorca:

a. wykorzystał dane osobowe w sposób niezgodny z Umową,,

b. nie zaprzestanie niewłaściwego przetwarzania danych osobowych.

18. Strony zobowiązują się, że podczas realizacji Umowy będą ze sobą ściśle współpracować, informując się wzajemnie o wszystkich okolicznościach mających lub mogących mieć wpływ na wykonanie Umowy.

19. Zleceniodawca nie jest odpowiedzialny za zobowiązania Zleceniobiorcy wobec osób trzecich nie przewidzianych niniejszą Umową ani za zobowiązania Zleceniobiorcy wobec osób, które ten upoważnił do przetwarzania danych.

20. Ze strony Zleceniodawcy osobami do kontaktów w sprawie realizacji Umowy są:

a. ……....adres poczty elektronicznej: ……...

b. ……..adres poczty elektronicznej: ……

22. Ze strony Zleceniobiorcy osobami do kontaktów w sprawie realizacji Umowy są:

a. ……....adres poczty elektronicznej: ……...

b. ……..adres poczty elektronicznej: ……

23. Zmiana danych dotyczących osób do kontaktu, wskazanych w pkt 21 i 22 nie jest traktowana jako zmiana warunków Umowy.

24. Zleceniobiorca zobowiązany jest do niezwłocznego poinformowania Zleceniodawcy, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie powszechnie obowiązujących przepisów prawa krajowego oraz unijnego w tym w zakresie w jakim regulują one zasady ochrony danych osobowych.

25. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron Umowy.

Zleceniodawca Zleceniobiorca