

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH – PO ZMIANIE

z dnia

pomiędzy:

Narodowym Instytutem Fryderyka Chopina z siedzibą w Warszawie przy ul. Tamka 43, wpisanym do rejestru instytucji kultury pod numerem RIK 51/2001, NIP: 525-22-14-269, numer REGON: 017307171, reprezentowanym przez:

Pana dr Artura Szklenera - Dyrektora

Panią Dorot Bałacka- Głównego Księgowego,

zwanym dalej **Administratorem**

a

.....
.....
.....

zwanym dalej **Przetwarzającym**.

zwanymi dalej łącznie **Stronami** lub pojedynczo **Stroną**.

PREAMBUŁA

W związku z zawarciem pomiędzy Stronami umowy nr z dnia, której przedmiotem jest (zwaną dalej „**Umową Główną**”), Strony postanowiły zawrzeć umowę o następującej treści (zwaną dalej „**Umową**”):

§ 1. Definicje pojęć używanych w niniejszej umowie:

1. **Rozporządzenie (RODO)** - Rozporządzenie Parlamentu Europejskiego i Rady UE 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.
2. **Podwykonawca** – inny niż Przetwarzający podmiot przetwarzający dane osobowe,
3. **Dni Robocze** - dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.

§ 2. Powierzenie przetwarzania danych osobowych

1. Strony postanawiają, że w celu spełnienia obowiązków wynikających z przepisów prawa, a w szczególności przepisów Rozporządzenia, Administrator powierza Przetwarzającemu, dane osobowe do przetwarzania na zasadach i w celu określonym w Umowie, jak również w celu właściwej realizacji postanowień Umowy Głównej.
2. Przetwarzający 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. Zakres i cel przetwarzania danych

1. Powierzone przez Administratora dane osobowe będą przetwarzane przez Przetwarzającego wyłącznie w celu realizacji Umowy Głównej.
2. Administrator oświadcza, że powierzone Przetwarzającemu dane osobowe zgromadził zgodnie z obowiązującymi przepisami prawa.
3. Na mocy niniejszej Umowy Przetwarzający będzie przetwarzał dane osobowe osób korzystających z usług objętych Umową Główną, w zakresie niezbędnym do jej realizacji, obejmującym:
 - 1) imię i nazwisko,
 - 2) płeć,
 - 3) datę urodzenia,
 - 4) obywatelstwo,
 - 5) dane dokumentu podróży, w tym numer i rodzaj dokumentu, datę jego ważności oraz kraj wydania,
 - 6) adres zamieszkania lub pobytu - jeżeli jest wymagany do realizacji danej usługi,
 - 7) numer telefonu,
 - 8) adres poczty elektronicznej,
 - 9) kod rezerwacji,
 - 10) numer biletu,
 - 11) datę i trasę podróży,
 - 12) dane dotyczące rezerwacji i realizacji podróży,
 - 13) dane niezbędne do wystawienia faktury lub innego dokumentu księgowego,
 - 14) informacje dotyczące programów lojalnościowych linii lotniczych - jeżeli zostały przekazane przez osobę korzystającą z usługi,
 - 15) informacje dotyczące bagażu - w zakresie niezbędnym do realizacji usługi.

Powierzenie nie obejmuje danych kart płatniczych, w szczególności numerów kart płatniczych, dat ich ważności oraz kodów zabezpieczających.
4. Przetwarzanie danych osobowych powierzonych Przetwarzającemu będzie miało charakter ciągły i odbywać się będzie w formie elektronicznej lub papierowej poprzez wykonywanie wszystkich czynności (operacji na danych osobowych) uzasadnionych wykonywaniem lub realizacją Umowy Głównej. Zakres czynności wykonywanych na danych osobowych obejmuje: przechowywanie danych, przeglądanie danych, wprowadzanie danych, modyfikowanie danych, opracowywanie danych, generowanie wydruków z danymi, usuwanie danych na zlecenie Administratora.
5. Charakter przetwarzania wynika z Umowy Głównej i określony jest rolą Przetwarzającego, jako podmiotu świadczącego usługę.
6. Umowa Główna i wykonywane zgodnie z jej zapisami zlecenia będą traktowane przez Przetwarzającego, jako udokumentowane polecenia Administratora.

§ 4. Sposób wykonania Umowy

1. Przetwarzający oświadcza, że posiada zasoby infrastrukturalne, doświadczenie, wiedzę oraz wykwalifikowany personel, w zakresie umożliwiającym należyte wykonanie Umowy, w zgodzie z obowiązującymi przepisami prawa, w szczególności, że znane mu są zasady przetwarzania i zabezpieczenia danych osobowych wynikające z Rozporządzenia.
2. Przetwarzający w terminie 7 dni roboczych od dnia podpisania niniejszej Umowy dostarczy Administratorowi wypełnioną ankietę dotyczącą stosowanych środków technicznych i organizacyjnych zapewniających ochronę powierzonych danych osobowych, która stanowi **załącznik nr 1** do niniejszej Umowy.
3. Przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
4. Przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
5. Przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji Umowy.
6. Przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust. 3 lit. b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji Umowy, zarówno w trakcie zatrudnienia, jak i po jego ustaniu.
7. Po zakończeniu obowiązywania Umowy Głównej lub w przypadku jej wcześniejszego rozwiązania Przetwarzający zgodnie z dyspozycją Administratora zwróci lub zniszczy, w sposób i w terminie odrębnie ustalonym z Administratorem, wszelkie powierzone na podstawie Umowy dane osobowe i ich kopie, chyba że właściwe przepisy prawa krajowego lub unijnego nakazują przechowywanie tych danych osobowych. Strony postanawiają, iż w przypadku podjęcia przez Administratora decyzji o zwrocie ww. danych osobowych lub ich kopii nastąpi ono w formie wcześniej uzgodnionej z Administratorem w terminie 14 dni roboczych, licząc od dnia zakończenia lub wygaśnięcia/rozwiązania Umowy (bez uwzględnienia §9 ust. 2 Umowy).
8. Po stwierdzeniu naruszenia ochrony powierzonych Przetwarzającemu przez Administratora danych osobowych, Przetwarzający, bez zbędnej zwłoki, jednak w miarę możliwości nie później niż w ciągu 24 godzin od wykrycia naruszenia, zgłasza je Administratorowi. Przetwarzający zobowiązany jest przekazać, co najmniej następujące informacje:
 - 1) datę i godzinę zdarzenia (jeśli jest znana; w razie potrzeby możliwe jest określenie w przybliżeniu),
 - 2) datę i godzinę kiedy Przetwarzający powziął informację o zdarzeniu;
 - 3) opis charakteru i okoliczności naruszenia (w tym wskazanie, na czym polegało naruszenie, określenie miejsca, w którym fizycznie doszło do naruszenia, wskazanie nośników, na których znajdowały się dane będące przedmiotem naruszenia),
 - 4) kategorie i przybliżoną liczbę wpisów (rekordów), których dotyczyło naruszenie,
 - 5) kategorie i przybliżoną liczbę osób, których dotyczyło naruszenie,
 - 6) opis potencjalnych konsekwencji i niekorzystnych skutków naruszenia dla osób, których dane dotyczą,

- 7) opis środków technicznych i organizacyjnych, które zostały lub mają być zastosowane w celu złagodzenia potencjalnych niekorzystnych skutków naruszenia,
- 8) imię, nazwisko i dane kontaktowe do osoby, od której można uzyskać więcej informacji na temat zgłoszonego naruszenia.

§ 5. Audyt

1. Zgodnie z art. 28 ust. 3 lit. h Rozporządzenia Administrator danych ma prawo przeprowadzenia audytu, mającego na celu weryfikację, czy Przetwarzający spełnia obowiązki wynikające z Rozporządzenia.
2. O chęci skorzystania z uprawnień, o których mowa w ust. 1 Administrator zobowiązany jest powiadomić Przetwarzającego, na co najmniej 7 Dni Roboczych.
3. Strony postanawiają, iż realizacja uprawnień, o których mowa w ust. 1 nie będzie mogła utrudniać bieżącej działalności Przetwarzającego, w tym w szczególności nie będzie stanowiła przeszkody do wykonywania pracy przez Przetwarzającego oraz jego pracowników lub współpracowników.
4. Audyt, o którym mowa w ust. 1 powyżej może być przeprowadzany w dniach roboczych w godzinach pracy Przetwarzającego i nie może trwać dłużej niż 3 dni.
5. Podczas realizacji uprawnień, o których mowa w ust. 1 Administrator zobowiązany będzie do poszanowania i stosowania się do polityki i regulaminów obowiązujących u Przetwarzającego w zakresie przetwarzania danych osobowych i przepisów BHP oraz do bezterminowego zachowania w tajemnicy wszelkich informacji stanowiących tajemnicę przedsiębiorstwa Przetwarzającego oraz innych informacji poufnych dotyczących Przetwarzającego, w których posiadanie wejdzie Administrator w związku z przeprowadzonym audytem, o którym mowa w ust. 1 powyżej.
6. Przetwarzający zobowiązany jest również do umożliwienia przeprowadzenia przez właściwy organ administracji kontroli zgodności przetwarzania danych osobowych (powierzonych Przetwarzającemu zgodnie z Umową) z powszechnie obowiązującymi przepisami.

§ 6. Dalsze powierzenie przetwarzania danych osobowych

1. Przetwarzający nie będzie korzystał z usług innego podmiotu przetwarzającego (zwanego dalej Podwykonawcą) bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Administratora. W przypadku ogólnej pisemnej zgody Przetwarzający informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia Podwykonawców, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
2. Przetwarzający zapewnia, że na Podwykonawcę nałożone zostaną – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii Europejskiej lub prawu krajowemu – te same obowiązki ochrony danych, jakie na Przetwarzającego nakłada niniejsza Umowa, a w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom rozporządzenia.
3. Przetwarzający odpowiada za działania i zaniechania Podwykonawcy, jak za działania i zaniechania własne. W szczególności, jeżeli Podwykonawca nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków Podwykonawcy spoczywa na Przetwarzającym.
4. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na udokumentowane polecenie Administratora, chyba że obowiązek taki nakłada na Przetwarzającego prawo Unii lub prawo państwa członkowskiego, któremu podlega

Przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

§ 7. Współdziałanie Stron

1. W trakcie obowiązywania niniejszej Umowy, Strony zobowiązują się ściśle współpracować - w tym za pośrednictwem Inspektorów Ochrony Danych, jeżeli zostali wyznaczeni przez którąkolwiek ze Stron - informując się wzajemnie o wszystkich okolicznościach mających lub mogących mieć wpływ na realizację niniejszej Umowy.
2. Przetwarzający ma obowiązek pomagać Administratorowi jako Administratorowi Danych Osobowych w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie powierzonych do przetwarzania danych osobowych oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.

§ 8. Odpowiedzialność Przetwarzającego

1. Przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie osobom nieupoważnionym powierzonych do przetwarzania danych osobowych.
2. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Przetwarzającego danych osobowych określonych w Umowie, o jakiegokolwiek decyzji administracyjnej lub jakimkolwiek orzeczeniu dotyczących przetwarzania tych danych, skierowanych do Przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania u Przetwarzającego tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

§ 9. Okres obowiązywania Umowy

1. Umowa zostaje zawarta na czas określony: od dnia podpisania Umowy Głównej tj. od do (tj. okres równy okresowi obowiązywania Umowy Głównej), z zastrzeżeniem ust. 2 i §10 ust. 2.
2. W przypadku podjęcia przez Administratora decyzji o zwrocie danych osobowych lub ich kopii, o których mowa w §4 ust. 7 Umowy termin obowiązywania niniejszej Umowy zostaje wydłużony do dnia upływu terminu wskazanego w §4 ust. 7.
3. Przetwarzanie danych osobowych powierzonych Przetwarzającemu zgodnie z Umową odbywać się będzie w okresie obowiązywania Umowy.

§ 10. Rozwiązanie Umowy

1. Administrator uprawniony jest do rozwiązania niniejszej Umowy bez zachowania okresu wypowiedzenia ze skutkiem natychmiastowym:
 - a) w przypadku rażącego naruszenia przez Przetwarzającego celu i zakresu przetwarzania powierzonych danych osobowych określonych w niniejszej Umowie,
 - b) w przypadku nieusunięcia uchybień stwierdzonych podczas audytu, o którym mowa w §5 Umowy w wyznaczonym terminie;
 - c) w przypadku powierzenia przetwarzania danych osobowych innemu podmiotowi bez zgody Administratora.

2. Umowa ulega również rozwiązaniu bez konieczności składania przez Strony dodatkowych oświadczeń w przypadku rozwiązania lub wypowiedzenia Umowy Głównej.

§11 Zasady zachowania poufności

1. Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób, a także danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy, w formie ustnej, pisemnej lub elektronicznej (dalej jako „Dane poufne”).
2. Przetwarzający oświadcza, że w związku z zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§12 Postanowienia końcowe

1. W przypadku wyznaczenia u Administratora lub odpowiednio u Przetwarzającego osoby pełniącej funkcję inspektora ochrony danych, każda ze Stron powiadomi drugą Stronę w formie pisemnej lub elektronicznej o osobie pełniącej u danej Strony funkcję inspektora ochrony danych oraz przekaze dane kontaktowe do tej osoby. W analogiczny sposób Strony będą powiadamiać się wzajemnie o zmianie osoby pełniącej u danej Strony funkcję inspektora ochrony danych.
2. Mając na uwadze, iż niniejsza Umowa zawarta została w związku i w celu realizacji Umowy Głównej Przetwarzający potwierdza, iż kalkulacja wynagrodzenia należnego Przetwarzającemu na podstawie Umowy Głównej została dokonana przy uwzględnieniu zobowiązań Przetwarzającego wynikających z Umowy i zobowiązania określone w niniejszej Umowie zostaną wykonane przez Przetwarzającego w ramach wynagrodzenia określonego w Umowie Głównej.
3. Strony będą dążyć do polubownego rozstrzygnięcia wszelkich sporów, jakie mogą wyniknąć w związku z interpretacją lub wykonywaniem Umowy.
4. Jeżeli działanie podjęte w myśl ust. 3 niniejszego paragrafu nie przyniosą rezultatu zadowalającego obie Strony, sądem właściwym do rozstrzygania wszelkich sporów wynikających z niniejszej Umowy jest sąd powszechny dla siedziby Administratora.
5. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
6. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
7. Niniejsza Umowa wchodzi w życie z dniem jej podpisania przez obie Strony.
8. W sprawach nieuregulowanych niniejszą Umową zastosowanie mają obowiązujące przepisy prawa, w szczególności Rozporządzenia.

Załączniki:

Załącznik nr 1 – Wykaz środków technicznych i organizacyjnych stosowanych przez Przetwarzającego;

.....

Przetwarzający

.....

Administrator

ANKIETA DLA PRZETWARZAJĄCEGO DANE OSOBOWE		
Lp.	Pytanie	Odpowiedź
1.	Czy zgodnie z art. 29 RODO osoby wykonujące operacje na danych osobowych otrzymały od podmiotu przetwarzającego upoważnienia do przetwarzania danych, w których został określony w szczególności zakres przetwarzanych przez te osoby danych?	
2.	Czy podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania zawierający wszystkie informacje wskazane w art. 30 ust. 2 RODO?	
3.	Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych?	
4.	Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych zasad dotyczących przetwarzania osobowych m. in. poprzez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych?	
5.	Czy podmiot przetwarzający zapewnia, aby nowozatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych został odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa?	
6.	Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników poprzez cykliczne szkolenia oraz inne działania mające na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych?	
7.	Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy?	
8.	Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 RODO?	

9.	Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych?	
10.	Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych/ podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych?	
11.	Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu?	
12.	Czy zapewniono fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez organizację od tych, które należą do innych organizacji?	
13.	Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona), bądź dostęp ten jest szczegółowo nadzorowany?	
14.	Czy każdy pracownik otrzymuje imienny identyfikator do systemów informatycznych?	
15.	Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowe zmiany haseł oraz zmian w razie zaistniałej potrzeby?	
16.	Czy pracownicy zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów poprzez blokadę ekranu lub w inny równoważny sposób?	
17.	Czy pracownicy zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników?	
18.	Czy w organizacji jest stosowana polityka tzw. „czystego biurka”?	
19.	Czy dane osobowe gromadzone w formie papierowej, po godzinach pracy organizacji, przechowywane są w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych?	

20.	Czy zapewniono oprogramowanie antywirusowe na wszystkich stacjach?	
21.	Czy oprogramowanie posiada licencję i jest na bieżąco aktualizowane?	
22.	Czy stosuje się szyfrowanie dysków komputerów przenośnych?	
23.	Czy urządzenia mobilne posiadają skonfigurowaną kontrolę dostępu?	
24.	Czy wobec urządzeń mobilnych stosuje się techniki kryptograficzne?	
25.	Czy na urządzeniach mobilnych zainstalowano oprogramowania antywirusowe?	
26.	Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?	
27.	Jaki przyjęto zakres oraz częstotliwość tworzenia kopii zapasowych?	
28.	Gdzie są przechowywane kopie zapasowe?	
29.	Czy organizacja posiada procedury odtwarzania systemu po awarii oraz ich testowania?	
30.	Czy organizacja wdraża nowe rozwiązania zgodnie z zasadą "privacy by design"?	
31.	Czy organizacja działa zgodnie z zasadą "privacy by default"?	
32.	Czy organizacja prowadzi ocenę skutków dla ochrony danych?	
33.	Czy organizacja gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym?	

.....

Przetwarzający