[WZÓR]

Umowa powierzenia przetwarzania danych osobowych nr……

zawarta w Gliwicach dnia…… pomiędzy:

……

zwanym w Umowie ***„Administratorem”***

reprezentowanym przez:

……

a ……

zwanym w Umowie ***„Podmiotem Przetwarzającym”***

reprezentowanym przez:……

(łącznie zwanymi w Umowie jako: *Strony*)

§ 1

Przedmiot umowy

1. W celu właściwej realizacji usług wykonywanych na podstawie Umowy Głównej nr…… zawartej dnia……, których przedmiotem jest ……, Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z 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), zwanego dalej „RODO”, dane osobowe do przetwarzania, na zasadach określonych w niniejszej Umowie.
2. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO.
3. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie Umowy:
   1) dane zwykłe pracowników Administratora, kategoria osób, których dane dotyczą: pracownicy, doktoranci i studenci oraz osoby wskazane przez Politechnikę Śląską, kategoria danych: imiona i nazwiska, adresy zamieszkania, adresy e-mail, nr telefonu, data urodzenia, numer paszportu, data wydania i data ważności paszportu,
   2) dane szczególne (dane wrażliwe): rodzaj danych osobowych powierzonych do przetwarzania nie obejmuje danych osobowych szczególnej kategorii.
4. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu, o którym mowa w ust. 1 niniejszego paragrafu.

§ 2

Obowiązki podmiotu przetwarzającego

1. Podmiot Przetwarzający zobowiązuje się przetwarzać powierzone dane osobowe, wyłącznie na udokumentowane polecenie Administratora, jakim jest usługa zlecona do wykonania Umową Główną, zgodnie z przedmiotową Umową, RODO oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, zwanej dalej: „UODO”.
2. Podmiot Przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzykom związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO; aktualna analiza ryzyka, stanowiąca podstawę stosowania adekwatnych środków bezpieczeństwa, jest przekazywana przez Podmiot Przetwarzający w terminie nie dłuższym niż 24 godziny od otrzymania żądania od Administratora.

3. Podmiot Przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
4. Podmiot Przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych, o których mowa w art. 29 RODO wszystkim osobom, którymi będzie posługiwać się, w celu realizacji niniejszej Umowy oraz zobowiązuje się do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, w związku z wykonywaniem Umowy; aktualny wykaz osób upoważnionych jest przekazywany przez Podmiot Przetwarzający w terminie nie dłuższym niż 3 dni robocze od otrzymania żądania od administratora, chyba że okoliczności wymagają szybszego działania – wtedy przekazanie wykazu powinno nastąpić w terminie nie dłuższym niż 24 godziny.
5. Podmiot Przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych, w celu realizacji niniejszej Umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
6. W miarę możliwości, Podmiot Przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie jej praw określonych w art. 15-22 RODO oraz wywiązać się z obowiązków określonych w art. 32-36 RODO. W przypadku, w którym podmiot danych osobowych zwróci się bezpośrednio do Podmiotu przetwarzającego, przekaże on niezwłocznie wniosek Administratorowi, nie później niż w terminie 3 dni roboczych wraz z żądanymi we wniosku informacjami, jeżeli są one w posiadaniu Podmiotu Przetwarzającego.
7. Podmiot Przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki, maksymalnie w ciągu 24 godzin od stwierdzenia naruszenia, zgłasza je Administratorowi.
8. Podmiot Przetwarzający niezwłocznie, nie później niż w terminie 3 dni roboczych informuje Administratora, jeżeli jego zdaniem wydane mu przez Administratora polecenie stanowi naruszenie przepisów RODO, UODO.
9. Podmiot Przetwarzający niezwłocznie, nie później niż w terminie 7 dni roboczych, po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
10. Podmiot Przetwarzający zobowiązuje się do prowadzenia rejestru wszystkich kategorii czynności przetwarzania danych osobowych, dokonywanych w imieniu Administratora, jeżeli taki obowiązek spoczywa na Podmiocie Przetwarzającym, zgodnie z art. 30 ust. 5 RODO.

§ 3

Obowiązki Administratora

1. Administrator zobowiązany jest współdziałać z Podmiotem Przetwarzającym w wykonaniu Umowy, udzielać Podmiotowi Przetwarzającemu wyjaśnień w razie wątpliwości co do zgodności poleceń Administratora z przepisami RODO i UODO.
2. W przypadku wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń, Podmiot Przetwarzający niezwłocznie, nie później niż w terminie 3 dni roboczych, informuje Administratora o stwierdzonej wątpliwości (uzasadniając na piśmie swoje stanowisko), pod rygorem utraty możliwości dochodzenia roszczeń z tego tytułu względem Administratora.

§ 4

Prawo kontroli

1. Administrator, zgodnie z art. 28 ust. 3 lit. h) RODO ma prawo kontroli, czy środki zastosowane przez Podmiot Przetwarzający, przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych, spełniają postanowienia Umowy i są zgodne z przekazana analizą ryzyka.
2. Administrator realizować będzie prawo kontroli w godzinach pracy Podmiotu Przetwarzającego z minimum 3-dniowym jego uprzedzeniem.
3. Podmiot Przetwarzający zobowiązuje się do usunięcia stwierdzonych podczas kontroli uchybień w terminie wskazanym przez Administratora, nie dłuższym niż 10 dni roboczych, od doręczenia Podmiotowi Przetwarzającemu protokołu z kontroli.

4. Podmiot przetwarzający udostępnia Administratorowi niezwłocznie, nie później niż w terminie 3 dni roboczych, od zgłoszenia żądania, wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

§ 5

Dalsze powierzenie danych do przetwarzania

1. Podmiot Przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom, jedynie w celu wykonania Umowy, po uzyskaniu uprzedniej pisemnej zgody Administratora, wyrażonej na podstawie pisemnego wniosku zawierającego uzasadnienie.
2. Przekazanie Powierzonych danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania, Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca obowiązany jest spełniać takie same wymagania i realizować obowiązki, jakie zostały nałożone na Podmiot Przetwarzający w niniejszej Umowie.
4. Podmiot Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu Przetwarzającego

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

§ 7

Czas obowiązywania umowy

Niniejsza umowa obowiązuje od dnia jej zawarcia przez okres trwania Umowy Głównej.

§ 8

Zasady zachowania poufności

1. Podmiot Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot Przetwarzający oświadcza, że w związku ze 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.

§ 10

Postanowienia końcowe

1. Integralną częścią niniejszej umowy, warunkującą jej podpisanie, jest pozytywy wyniki samooceny Podmiotu Przetwarzającego, dokonanej według wzoru udostępnionego przez Administratora.
2. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
3. W sprawach nieuregulowanych w niniejszej umowie będą miały zastosowanie przepisy ustawy z dnia 23 kwietnia 1964 r – Kodeks cywilny, RODO oraz UODO.
4. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy miejscowo dla Administratora.
5. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze Stron.

.....	.....
Administrator	*Podmiot przetwarzający*
[data i podpis]	[data i podpis]

Załącznik do Umowy powierzenia przetwarzania danych osobowych checklista
Dotyczy umów polegających na wielostanowiskowym przetwarzaniu danych osobowych

Lp.	PYTANIE	TAK/NIE/NIE DOTYCZY	UWAGI
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 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, jeżeli istnieje, 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 i serwerach?		
21	Czy oprogramowanie używane do przetwarzania 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, jeżeli są używane do przetwarzania danych osobowych, stosuje się techniki kryptograficzne?		
25	Czy na urządzeniach mobilnych, jeżeli są używane do przetwarzania danych osobowych, zainstalowano oprogramowania antywirusowe?		
26	Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? (ocenę należy przeprowadzić na podstawie udanych operacji odtwarzania systemu)		
27	Czy przyjęto zasady określające zakres oraz częstotliwość tworzenia kopii zapasowych?		
28	Czy kopie zapasowe przechowywane są na innych zasobach lub, odpowiednio, w innych pomieszczeniach?		
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?		
	PODSUMOWANIE		