DUO.271.2.2021 załącznik nr 4 do ogłoszenia

**Umowa powierzenia**
przetwarzania danych osobowych

zawarta w dniu …………………………roku w Tychach pomiędzy:

(zwana dalej „Umową”)

**Gminą Miasta Tychy, Aleja Niepodległości 49,43-100 Tychy, NIP: 646-00-13-450**

reprezentowaną przez**:**

**Andrzeja Dziubę – Prezydenta Miasta Tychy**

**Dorotę RUSIN – Naczelnika Wydziału Organizacyjnego, Kadr i Szkolenia**zwanych w treści umowy **Administratorem danych**

a

firmą **………………….** z siedzibą przy ul. ………………………….., wpisaną do Rejestru Instytucji Szkoleniowych, NIP: …………….., REGON: …………., reprezentowaną przez:

**……………………… – właściciela firmy**,

zwaną w treści umowy **Podmiotem przetwarzającym**

**§ 1**

## **Powierzenie przetwarzania danych osobowych**

1. Administrator danych powierza Podmiotowi przetwarzającemu dane osobowe do przetwarzania w trybie art. 28 ogólnego 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 (Dz.Urz.UE.L Nr 119, str. 1) (zwanego w dalszej części Umowy „Rozporządzeniem”), na zasadach, w zakresie i w celu określonych w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się do przetwarzania powierzonych mu danych osobowych zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, chroniącymi prawa osób, których dane dotyczą.

**§ 2**

## **Zakres i cel przetwarzania danych**

1. Administrator powierza podmiotowi przetwarzającemu przetwarzanie w następującym zakresie danych osobowych zwykłych zgromadzonych w ramach zbiorów danych:
2. imię i nazwisko,
3. stanowisko.
4. Dane osobowe wskazane w ustępie 1 niniejszego paragrafu dotyczą następujących kategorii osób: pracowników Urzędu Miasta Tychy.
5. Dane osobowe powierzone przez Administratora danych będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji szkoleń w ramach projektu pn.: „Z profilaktyką na Ty – eliminowanie zdrowotnych czynników ryzyka w Urzędzie Miasta Tychy” współfinansowany ze środków Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014-2020, osi priorytetowej VIII. Regionalne kadry gospodarki opartej na wiedzy, działanie 8.3. Poprawa dostępu do profilaktyki, diagnostyki i rehabilitacji leczniczej ułatwiającej pozostanie w zatrudnieniu i powrót do pracy, poddziałanie 8.3.2. Realizowanie aktywizacji zawodowej poprzez zapewnienie właściwej opieki zdrowotnej – konkurs.
6. Podmiot przetwarzający jest upoważniony do wykonywania następujących czynności przetwarzania powierzonych danych: utrwalanie, organizowanie, porządkowanie, przechowywanie, pobieranie, przeglądanie, wykorzystywanie – które są w minimalnym zakresie niezbędne do realizacji celu, o którym mowa w ust. 2 powyżej.

**§ 3**

## **Obowiązki Podmiotu przetwarzającego**

1. Podmiot przetwarzający przy przetwarzaniu powierzonych danych osobowych zobowiązuje się do ich zabezpieczenia przez stosowanie odpowiednich środków technicznych i organizacyjnych, odpowiadających stanowi wiedzy technicznej, zapewniających zgodność z Rozporządzeniem, w tym adekwatny stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą. Lista środków technicznych i organizacyjnych stosowanych przez Podmiot przetwarzający stanowi załącznik do Umowy.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane osobowe, przy czym będą to jedynie osoby, które mają odpowiednie przeszkolenie z zakresu ochrony danych osobowych i są niezbędne do realizacji celu niniejszej Umowy.
4. Podmiot przetwarzający zapewnia, że osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zobowiążą się do zachowania tajemnicy lub będą podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, o której mowa w art. 28 ust. 3 lit. b Rozporządzenia, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu. Podmiot przetwarzający zapewnia ponadto, że osoby, o których mowa w niniejszym ustępie, będą przetwarzały dane osobowe zgodnie z zasadą wiedzy koniecznej.
5. Dla prawidłowej realizacji ust. 4 Podmiot Przetwarzający dokonuje okresowej weryfikacji listy osób, którym udzielono dostępu do danych przetwarzanych w imieniu Administratora.
6. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem niezwłocznie usuwa wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
7. Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, oraz
z obowiązków określonych w art. 32–36 Rozporządzenia. Podmiot przetwarzający –
w razie wpływu do niego żądania w zakresie realizacji praw osób, których dotyczą powierzone dane – informuje o tym Administratora w terminie 5 dni roboczych od otrzymania wiadomości. Udzielając informacji, Podmiot przetwarzający przekazuje dane nadawcy i treść żądania oraz określa, w jakim zakresie jest w stanie przyczynić się do realizacji żądania.
8. Wszelkie przypadki naruszenia ochrony danych osobowych Podmiot przetwarzający zgłasza niezwłocznie Administratorowi.

**§ 4**

## **Prawo kontroli**

1. Zgodnie z art. 28 ust. 3 lit. h Rozporządzenia Administrator danych ma prawo kontroli, mającej na celu weryfikację, czy Podmiot przetwarzający spełnia obowiązki wynikające z niniejszej Umowy.
2. Administrator danych będzie realizować prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 2 dniowym uprzedzeniem.
3. Prawo do przeprowadzenia kontroli obejmuje: wstęp do pomieszczeń, w których znajdują się zasoby uczestniczące w operacjach przetwarzania powierzonych danych osobowych; żądanie złożenia pisemnych lub ustnych wyjaśnień od osób upoważnionych do przetwarzania powierzonych danych osobowych; wgląd do wszelkich dokumentów
i wszelkich danych mających bezpośredni związek z celem kontroli; przeprowadzanie oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.
4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych, nie dłuższym niż 7 dni.

**§ 5**

## **Raportowanie**

1. Na wniosek Administratora Podmiot przetwarzający udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z Rozporządzenia.
2. Informacji, o których mowa w ust. 1, udziela się w terminie 15 dni roboczych od dnia doręczenia wniosku, z zastrzeżeniem ust. 3.
3. Jeżeli wniosek, o którym mowa w ust. 1, dotyczy realizacji obowiązku zgłoszenia naruszenia ochrony danych osobowych lub usunięcia jego skutków, Podmiot przetwarzający udziela informacji w najbliższym możliwym terminie, nie później niż w ciągu 24 godzin od doręczenia wniosku.

**§ 6**

## **Odpowiedzialność Podmiotu przetwarzającego**

1. Podmiot 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. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora
o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie,
o jakiejkolwiek decyzji administracyjnej lub jakimkolwiek orzeczeniu dotyczących 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 tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

**§ 8**

## **Czas obowiązywania Umowy**

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas określony od …………... do *………………….*
2. Każda ze stron może wypowiedzieć niniejszą Umowę z zachowaniem dwu tygodniowego okresu wypowiedzenia.

**§ 9**

## **Rozwiązanie Umowy**

1. Administrator może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
2. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie,
3. przetwarza dane osobowe w sposób niezgodny z Umową,
4. powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

**§ 10**

## **Zasada zachowania poufności**

Podmiot przetwarzający oświadcza, że w związku z zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

**§ 11**

## **Postanowienia końcowe**

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy Administratora.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Administrator danych Podmiot przetwarzający

Załącznik:

Wykaz środków technicznych i organizacyjnych stosowanych przez Podmiot przetwarzający

Załącznik do umowy powierzenia

**Wykaz środków organizacyjnych i technicznych stosowanych przez Podmiot przetwarzający**

|  |  |
| --- | --- |
| **PYTANIE** | **ODPOWIEDŹ** |
| Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych? |   |
| Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie danych osobowych, m.in. przez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych? |   |
| Czy podmiot przetwarzający zapewnia, że nowo zatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych zostanie odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa? |   |
| Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników dzięki cyklicznym szkoleniom oraz innym działaniom mającym na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych? |   |
| Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych, zostali zobowiązani do zachowania ich w tajemnicy? |   |
| Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 Rozporządzenia, lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 Rozporządzenia? |   |
| Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych? |   |

|  |  |
| --- | --- |
| 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? |   |
| Czy podmiot przetwarzający zastosował środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? |   |
| Czy podmiot przetwarzający zapewnił fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez jego organizację od tych, które należą do innych organizacji? |   |
| 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? |   |
| Czy każdy pracownik podmiotu przetwarzającego otrzymuje imienny identyfikator do systemów informatycznych? |   |
| Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowych zmian haseł oraz zmian w razie zaistniałej potrzeby? |   |
| Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów przez blokadę ekranu lub w inny równoważny sposób? |   |
| Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników? |   |
| Czy w organizacji podmiotu przetwarzającego jest stosowana polityka czystego biurka? |   |

|  |  |
| --- | --- |
| Czy dane osobowe gromadzone w formie papierowej są przechowywane, po godzinach pracy organizacji podmiotu przetwarzającego, w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych? |   |
| Czy podmiot przetwarzający zapewnił oprogramowanie antywirusowe na wszystkich stacjach? |   |
| Czy oprogramowanie ma licencję i jest na bieżąco aktualizowane? |   |
| Czy podmiot przetwarzający stosuje szyfrowanie dysków komputerów przenośnych? |   |
| Czy urządzenia mobilne mają skonfigurowaną kontrolę dostępu? |   |
| Czy podmiot przetwarzający stosuje techniki kryptograficzne wobec urządzeń mobilnych? |   |
| Czy na urządzeniach mobilnych zainstalowano oprogramowanie antywirusowe? |   |
| Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |   |
| Jaki przyjęto zakres oraz jaką częstotliwość tworzenia kopii zapasowych? |   |
| Gdzie są przechowywane kopie zapasowe? |   |
| Czy podmiot przetwarzający posiada procedury odtwarzania systemu po awarii oraz ich testowania? |   |
| Czy podmiot przetwarzający wdraża nowe rozwiązania zgodnie z zasadą privacy by design? |   |
| Czy podmiot przetwarzający działa zgodnie z zasadą privacy by default? |   |
| Czy podmiot przetwarzający prowadzi ocenę skutków dla ochrony danych? |   |
| Czy podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym? |   |