ZARZĄDZENIE NR 421/2022
STAROSTY KARTUSKIEGO
z dnia 11 maja 2022 r.

w sprawie zmiany Zarządzenia Nr 290/2018 Starosty Kartuskiego z dnia 28 maja 2018 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji

Na podstawie § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247)

zarządza się, co następuje:

§ 1. Wzór umowy powierzenia przetwarzania danych osobowych, stanowiący załącznik nr 5 do Polityki Bezpieczeństwa Danych Osobowych Starostwa Powiatowego w Kartuzach, stanowiącej załącznik do Zarządzenia Nr 290/2018 Starosty Kartuskiego z dnia 28 maja 2018 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji, otrzymuje brzmienie, jak w załączniku do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA

/-/ Bogdan Łapa

Załącznik
do Zarządzenia Nr 421/2022
Starosty Kartuskiego
z dnia 11 maj 2022 r.

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w Kartuzach, w dniu …… roku, pomiędzy:

Starostą Kartuskim - Bogdanem Łapą, adres: Starostwo Powiatowe w Kartuzach, ul. Dworcowa 1, 83-300 Kartuzy,

(zwanym w dalszej części umowy „Administratorem danych" lub „Administratorem"),

a ……

(zwanym dalej Przetwarzającym)

dalej łącznie zwanymi „Stronami".

§ 1.

Powierzenie przetwarzania danych osobowych

1. Administrator oświadcza, że jest administratorem danych osobowych w rozumieniu art. 4 pkt 7 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 i z 2018 r. Nr 127, str. 2), zwanego w dalszej części „Rozporządzeniem", a powierzonych do przetwarzania na podstawie niniejszej umowy.
2. Na podstawie art. 28 ust. 3 Rozporządzenia Administrator powierza Podmiotowi przetwarzającemu dane osobowe do przetwarzania na zasadach i w celu określonym w niniejszej umowie. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia Podmiot przetwarzający wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
3. Podmiot 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.
4. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§ 2.

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie Umowy dane dotyczące ……*[należy podać kategorię osób, których dane dotyczą, np. pracowników*

administratora, klientów administratora itd.] w zakresie …… *[należy podać kategorie danych osobowych, np. imiona i nazwiska, adresy zamieszkania, numery PESEL itd.]*.

2. Dane osobowe powierzone przez Administratora danych będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu …… *[należy podać cel przetwarzania danych przez Podmiot przetwarzający, np. realizacji umowy z dnia …… nr …… w zakresie prowadzenia spraw kadrowych]*.

3. Podmiot przetwarzający jest upoważniony do wykonywania następujących czynności przetwarzania powierzonych danych: utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie *[należy wybrać właściwe]* – które są w minimalnym zakresie niezbędne do realizacji celu, o którym mowa w ust. 2 powyżej.

4. Powierzone do przetwarzania dane osobowe będą przetwarzane przez Podmiot przetwarzający w sposób zgodny z obowiązującymi przepisami dotyczącymi przetwarzania danych osobowych .

§ 3.

Zasady przetwarzania danych osobowych

1. Podmiot przetwarzający zobowiązuje się do:

   1) wykorzystania powierzonych przez Administratora danych osobowych w zakresie określonym w umowie, o której mowa w § 2 ust. 2;

   2) zapewnienia zachowania 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 niniejszej umowy zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu;

   3) zapewnienia ochrony danych i wdrożenia wymaganych przepisami prawa środków technicznych i organizacyjnych, zapewniających stopień bezpieczeństwa powierzonych do przetwarzania danych osobowych o których mowa w art.32 RODO;

   4) zgłaszania Administratorowi naruszenia ochrony powierzonych do przetwarzania danych osobowych bez zbędnej zwłoki po stwierdzeniu tego naruszenia, tj. w czasie nie dłuższym niż 24 godzin od momentu powzięcia informacji o zdarzeniu;

   5) prowadzenia rejestru kategorii czynności przetwarzania, dokonywanych w imieniu Administratora, stosownie do postanowień przepisu art. 30 ust. 2 Rozporządzenia;

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

   7) po zakończeniu świadczenia usług związanych z przetwarzaniem niezwłocznego *usunięcia/zwrócenia Administratorowi* wszelkich danych osobowych *[należy wybrać, czy Podmiot przetwarzający ma usunąć, czy zwrócić dane]* oraz usunięcia wszelkich ich istniejących kopii, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych

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

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

10) realizacji wytycznych Administratora w zakresie bezpieczeństwa przetwarzanych powierzonych mu danych,

11) poinformowania Administratora, przed rozpoczęciem przetwarzania, o obowiązku prawnym skutkującym koniecznością przetwarzania danych osobowych inaczej niż na udokumentowane polecenie Administratora.

2. Administrator upoważnia Podmiot przetwarzający do przetwarzania danych osobowych w zakresie i celu określonym w Umowie, a także do udzielenia dalszych upoważnień do przetwarzania danych osobom współpracującym z Podmiotem przetwarzającym na podstawie umowy o pracę lub umowy cywilnoprawnej, które mają dostęp do przetwarzanych danych osobowych.

3. Strony zobowiązują się do szczególnej staranności w wykonaniu umowy, w tym Podmiot przetwarzający zobowiązuje się do skrupulatnego i dokładnego zapoznania osób biorących udział przy przetwarzaniu danych osobowych powierzonych na podstawie umowy z przepisami prawa powszechnie obowiązującego w zakresie ochrony danych osobowych oraz zobowiązania tych osób do złożenia oświadczenia o zapoznaniu się z ww. przepisami oraz instrukcją przetwarzania danych udostępnioną przez Administratora. Każda osoba przed dopuszczeniem jej do przetwarzania danych osobowych musi otrzymać stosowne upoważnienie.

4. Strony zgodnie postanawiają, że w przypadku przesyłania danych osobowych, dane te będą zabezpieczone podczas transmisji przez sieć publiczną za pomocą kryptograficznych środków ochrony danych osobowych.

5. W przypadku gdy Administrator uzna to za konieczne celem zapewnienia należytej najwyższej ochrony danych osobowych osób, których one dotyczą, Podmiot przetwarzający zobowiązany jest pomóc Administratorowi 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.

6. 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.

7. Podmiot przetwarzający zobowiązuje się zająć niezwłocznie każdym pytaniem Administratora dotyczącym przetwarzania powierzonych mu na podstawie Umowy danych osobowych, w szczególności tych dotyczących organizacji ochrony danych osobowych u Podmiotu przetwarzającego oraz związanych z żądaniem osób, których dane dotyczą, w zakresie wykonywania jej praw określonych w przepisach o ochronie danych osobowych. W tym celu Podmiot przetwarzający wdroży odpowiednie środki techniczne i organizacyjne umożliwiające sprawne udzielenie Administratorowi żądanych informacji.

8. Administrator nie jest odpowiedzialny za zobowiązania Podmiotu przetwarzającego wobec osób trzecich nie przewidzianych Umową ani za zobowiązania Podmiotu przetwarzającego wobec osób, które ten upoważnił do przetwarzania danych.

§ 4

Prawo do kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 lit. h Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia niniejszej umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum jednodniowym jego uprzedzeniem o zamiarze przeprowadzenia kontroli.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
5. Przetwarzający zobowiązany jest do wypełnienia „ Ankiety dla podmiotu przetwarzającego" i udzielenia odpowiedzi na wszystkie w niej zawarte pytania dotyczące zastosowania odpowiednich środków technicznych i organizacyjnych, zapewniających przetwarzanie powierzonych danych osobowych zgodnie z Rozporządzeniem 2016/679 i niniejszą Umową. Ankieta służy do wykazania weryfikacji pod kątem zapewnienia zgodności powierzonych do przetwarzania danych osobowych z Rozporządzeniem 2016/679, o których mowa w art. 28 ust. 1 oraz ust. 3 lit. h) Rozporządzenia 2016/679, a której wzór stanowi załącznik do niniejszej Umowy.

§5

Podpowierzenie

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 danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora Danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający. W taki przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora Danych o tym obowiązku prawnym, o ile prawo nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w ust.1 winien spełniać te same gwarancje i 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 poinformowania Administratora danych 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 powierzonych przez Administratora danych.

§ 7

Czas obowiązywania umowy

Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas nieokreślony/określony od…….do……..

§8

Rozwiązanie umowy

Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

1) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
2) przetwarza dane osobowe w sposób niezgodny z umową;
3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych 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 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.

3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały zabezpieczenie danych poufnych w tym w szczególności danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

§10

Postanowienia końcowe

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
3. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
4. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Administratora danych.
5. Osobami uprawnionymi do kontaktów w zakresie realizacji umowy są:
   1) ze strony Administratora: Inspektor Ochrony Danych ……., tel. ……, adres e-mail:……
   2) ze strony Przetwarzającego: ....., tel. ....., adres e-mail:…….

Administrator Podmiot przetwarzający

Załącznik do Umowy powierzenia przetwarzania danych osobowych

Ankieta dla podmiotu przetwarzającego

Podmiot przetwarzający	
Nazwa podmiotu	
Dane adresowe	

Lp.	**Pytanie**	**Odpowiedź**	**Uwagi (dodatkowe informacje)**
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 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 komputerowych?		
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.	Czy organizacja posiada procedury odtwarzania systemu po awarii oraz ich testowania?		
29.	Czy organizacja przeprowadziła analizę ryzyka w zakresie świadczenia usług, związanych z przyjęciem do przetwarzania danych osobowych?		
30.	Czy organizacja prowadzi ocenę skutków dla ochrony danych?		
31.	Czy organizacja gwarantuje realizację praw osób, których dane dotyczą tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym?		
32.	Czy organizacja powołała Inspektora Ochrony Danych Osobowych ?		
33.	Czy w stosunku do pomiotu przetwarzającego były zgłaszane naruszenia danych osobowych? Lub też, czy w ciągu ostatnich trzech lat, podmiot przetwarzający sam zgłaszał naruszenia do odpowiedniego urzędu (organu administracji publicznej)?		

……
(data, podpis osoby wypełniającej ankietę)