

Gniewkowo, 29 listopada 2021 r.

SK. 1431.87.2021

Pan



W odpowiedzi na wniosek o udostępnienie informacji publicznej z 15 listopada 2021 r. przesyłam w załączeniu umowę zawartą z Centrum Bezpieczeństwa Informatycznego z siedzibą w Krasnymstawie, w ramach której prowadzone są m.in. okresowe audyty KRI.

Jednocześnie informuję, że zawarte we wniosku żądanie udostępnienia okresowych raportów/sprawozdań KRI, jak i wszelkiej innej dokumentacji audytów w zakresie bezpieczeństwa informacji i nie stanowi informacji publicznej.

Przekazanie do zapoznania się przez osoby trzecie dokumentu raportu będącego efektem wszelkich audytów bezpieczeństwa systemów informacyjnych – w tym audytów przeprowadzonych na podstawie § 20 ust. 2 pkt 14 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 (dalej „KRI”) – stanowiłoby ujawnienia informacji z zakresu opisu składników systemu teleinformatycznego stanowiących część składową dokumentacji związanej z zarządzaniem systemami informatycznymi, bezpieczeństwem informacji, w tym zabezpieczeniem danych osobowych.

Zgodnie z pozostającym w aktualności (pomimo zmiany przepisów dot. ochrony danych osobowych), stanowiskiem Generalnego Inspektora Ochrony Danych Osobowych (dalej „GIODO” – dostępnym pod linkiem <https://www.giodo.gov.pl/pl/222/9906>) oraz stanowiskami opartymi na orzecznictwie judykatury, dokumentacja taka jak Polityka bezpieczeństwa i Instrukcja zarządzania systemem informatycznym to dokumenty wewnętrzne, które powinny być udostępniane jedynie ograniczonemu kręgowi osób, ponieważ służą wskazaniu środków bezpieczeństwa i procedur bezpiecznego przetwarzania informacji, w tym danych osobowych. Za część pozostającą w ścisłym związku z instrukcjami zarządzania systemem informatycznym i politykami bezpieczeństwa należy także uznać wyniki audytów sfer przez te dokumenty regulowanych.

Ponadto jak wskazuje GIODO udostępnianie na zewnątrz takich informacji osłabia ich skuteczność przez co zagraża właściwej ochronie przetwarzanych danych. Zapoznanie osób trzecich ze szczegółami rozwiązań w zakresie bezpieczeństwa danych oraz architekturą systemów zastosowanych do ich przetwarzania i niekontrolowany przepływ tych informacji może ułatwić przestępcom komputerowym ingerencję w stosowane systemy (np. poprzez zatrzymanie pracy lub niekontrolowaną modyfikację systemu, przejęcie, zniekształcenie lub



usunięcie danych w nim zawartych) lub poprzez ominięcie zastosowanych zabezpieczeń bądź ich „złamanie”.

W związku z powyższym, zgodnie ze stanowiskiem GIODO należy przyjąć zasadę, że dokumenty takie jak Polityka bezpieczeństwa i Instrukcja zarządzania systemem informatycznym – a co za tym idzie w naszej opinii także wszelkich wyników wykonywanych audytów pozostających w sferze zainteresowania w/w dokumentacji – należy traktować jako dokumenty wewnętrzne udostępniane jedynie ograniczonemu kręgowi osób, tj. tylko tym osobom, którym są niezbędne w związku z powierzonymi im zadaniami służbowymi. Przyjęta wyżej zasada dotycząca udostępniania dokumentów zawierających informacje o stosowanych środkach i procedurach bezpieczeństwa jest spójna z zaleceniami normy ISO/IEC 27002 zatytułowanej „Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji”. Powyższe stanowisko potwierdza orzecznictwo m.in. w Wyroku z 8 grudnia 2005 r. (sygn. akt II SA/WA 1539/05). Wojewódzki Sąd Administracyjny w Warszawie wskazał, że biorąc pod uwagę wymaganą przepisami prawa zawartość Polityki bezpieczeństwa nie powinna być ona udostępniana publicznie. W ocenie WSA, elementy Polityki bezpieczeństwa mają charakter informacji niejawnych i w związku z tym ich udostępnienie podlega ograniczeniu, zgodnie z art. 5 ust. 1 ustawy o dostępie do informacji publicznej. Również orzeczenie Naczelnego Sądu Administracyjnego z dnia 10 stycznia 2014, sygn. akt. I OSK 2254/13, stwierdza iż informacje techniczne, dotyczące np. sposobu funkcjonowania danego narzędzia użytkowanego przez organ, nie stanowią informacji publicznej. Jest to uzasadnione przyczynami związanymi z potrzebą zapewnienia bezpieczeństwa i integralności danego narzędzia przed ingerencją tak wewnętrzną jak i zewnętrzną. Udostępnianie informacji technicznych np. wskazujących na częstotliwość logowania się do danego narzędzia czy przedstawiających okresy aktywności lub zmniejszonej aktywności w systemie teleinformatycznym organu, może prowadzić do ujawnienia danych mających istotny wpływ np. na bezpieczeństwo danego narzędzia informatycznego (okresy kiedy będzie mniej lub bardziej podatne na ataki). Z tego powodu dane takie, mające w zasadzie charakter techniczny, nie będą stanowiły informacji publicznej, w tym nie powinny zostać udostępnione innym osobom niż te, którym informacje te są niezbędne w związku z powierzonymi im zadaniami lub uprawnionym do tego publicznym organom kontroli.

Mając na uwadze powyższe, zgodnie z przedstawionymi stanowiskami GIODO oraz orzecznictwem judykatury, w tym przede wszystkim wyrokiem Naczelnego Sądu Administracyjnego z dnia 10 stycznia 2014, sygn. akt. I OSK 2254/13, należy uznać, że żądane dot. udostępnienia okresowych raportów/sprawozdań KRI, jak i wszelkiej innej dokumentacji audytów w zakresie bezpieczeństwa informacji i nie stanowi informacji publicznej.

BURMISTRZ

mgr Adam Straszynski



GNIEWKOWO

Urząd Miejski

ul. 17 Stycznia 11, 88-140 Gnieńkowo

Telefon: (52) 354 30 08

Fax: (52) 354 30 37

urząd@gniewkowo.com.pl

www.gniewkowo.com.pl

o wykonywanie zadań Inspektora Ochrony Danych oraz świadczenia usług w zakresie doradztwa informatycznego

zawarta w dniu 13 grudnia 2019 roku w Gniewkowie pomiędzy:

Gminą Gniewkowo, z siedzibą przy ul. 17 Stycznia 11, 88-140 Gniewkowo, NIP: 556-25-63-314,

reprezentowaną przez:

Adama Straszynskiego - Burmistrza

przy kontrasygnacie:

Wioletty Kucharskiej - Skarbnika

zwaną w dalszej części umowy „**Zleceniodawcą**”

a

Radosławem Szymaszkim prowadzącym działalność gospodarczą pod firmą **Radosław Szymaszek Centrum Bezpieczeństwa Informatycznego** z siedzibą w Krasnymstawie, ul. Graniczna 11, 22-300 Krasnymstaw, NIP: 564-144-74-18, zwanym w dalszej części umowy „**Zleceniobiorcą**”,

zwane łącznie – „**Stronami**”,

a każda z osobna zwana: „**Stroną**”.

§ 1

Przedmiot umowy

1. Przedmiotem umowy jest świadczenie usług u Zleceniodawcy w zakresie pełnienia funkcji Inspektora Ochrony Danych (zwanego w dalszej części niniejszej Umowy również jako: „Inspektor”), o którym mowa w art. 37-39 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.Urz.UE.L 2016 Nr 119, str. 1 ze zm.; dalej: „Rozporządzenie” lub „RODO”) oraz na zasadach określonych w ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 ze zm.) wraz z aktami wykonawczymi, osobiście lub przez wyznaczoną osobę, a także świadczenie usług doradztwa informatycznego w zakresie ochrony danych osobowych, zaś Zleceniodawca zobowiązany będzie do zapłaty z tego tytułu wynagrodzenia.
2. Zleceniobiorca na wniosek Zleceniodawcy oraz po udzieleniu mu stosownego pełnomocnictwa zawiadomi Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu Inspektora Ochrony Danych. Wszelkie koszty z tego tytułu (w szczególności koszty opłaty skarbowej od pełnomocnictwa) ponosi Zleceniodawca.
3. Zleceniobiorca zobowiązuje się do wypełniania następujących zadań Inspektora:

- a) informowania Zleceniodawcy jako Administratora, o którym mowa w art. 4 pkt 7 RODO, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz przepisów o ochronie danych osobowych i doradzanie im w tej sprawie;
 - b) monitorowania przestrzegania przepisów Rozporządzenia, innych przepisów Unii lub polskich przepisów prawa o ochronie danych osobowych oraz polityk Administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
 - c) udzielaniu na żądanie Zleceniodawcy zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie wykonania zaleceń pokontrolnych po takiej ocenie zgodnie z art. 35 Rozporządzenia;
 - d) współpracy z krajowym organem nadzorczym powołanym w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych oraz ułatwianiu swobodnego przepływu danych osobowych – Prezesem Urzędu Ochrony Danych Osobowych (zwanym dalej jako „organ nadzorczy”);
2. 4. W ramach świadczonych usług, o których mowa w § 1 ust. 3 lit. a) Zleceniobiorca zobowiązuje się wydawać opinie w sprawach dotyczących problemów prawnych Administratora danych osobowych związanych z ochroną danych osobowych w nieprzekraczalnym terminie 10 dni od daty wpłynięcia zapytania na adres poczty elektronicznej Inspektora Ochrony Danych lub adres inspektor@cbi24.pl. W przypadku wpływu do Zleceniobiorcy korespondencji e-mail po godzinie 15:30 danego dnia, termin wpływu będzie liczony od godziny 7:30 następnego dnia roboczego.
5. Zleceniobiorca wytworzy i przekaże Zleceniodawcy wzory dokumentów wg. załącznika nr 1 do Umowy, które zobowiązuje się aktualizować, w szczególności w przypadku zmiany stanu prawnego. Inspektor Ochrony Danych opracowuje projekty dokumentów wymienionych w zdaniu poprzednim w terminie nie dłuższym, niż 3 (słownie: trzy) miesiące kalendarzowe, licząc od dnia zawarcia umowy, określonego w § 7 ust. 1, za wyjątkiem dokumentu wskazanego w pkt 2 tego załącznika („Analiza ryzyka systemu informatycznego oraz danych osobowych”), który może być opracowany w terminie późniejszym, po zebraniu pełnych danych niezbędnych do jego wytworzenia, lecz nie później niż w terminie 5 (słownie: pięciu) miesięcy, licząc od ww. terminu zawarcia umowy. W trakcie trwania Umowy dokumentacja, o której mowa w zdaniu poprzednim będzie dostosowywana do stanu faktycznego jednostki we współpracy z Administratorem. Po zaakceptowaniu treści ww. dokumentów Administrator wdraża je zarządzeniem lub innym wewnątrznie wiążącym aktem prawnym.
6. Zleceniobiorca w ramach świadczenia usług dotyczących doradztwa informatycznego zobowiązany będzie do:
- a) udzielania konsultacji, wydawania zaleceń oraz wsparcia merytorycznego w sprawach związanych z przetwarzaniem danych osobowych w systemie informatycznym w terminie 10 dni od daty wpłynięcia zapytania na adres poczty elektronicznej it@cbi24.pl. W przypadku wpływu do Zleceniobiorcy korespondencji e-mail po godzinie 15:30 danego dnia, termin wpływu będzie liczony od godziny 7:30 następnego dnia roboczego, w wymiarze nie przekraczającym 3 porad w miesiącu,

b) wykonania Audytu Informatycznego (dalej: Audyt IT) w oparciu o przepisy Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. 2017 r., poz. 2247 ze zm.) lub inne przepisy wydane w miejsce tego rozporządzenia.

7. Do przeprowadzenia w imieniu Zleceniobiorcy Audytu IT, o którym mowa w § 1 ust. 6 lit. b) Umowy, upoważnieni są audytorzy Zleceniobiorcy wskazani w załączniku nr 2 do Umowy.

8. Zleceniobiorca zobowiązuje się, iż obowiązki Inspektora Ochrony Danych będzie pełnić osoba, która:

- a) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych,
- b) posiada studia podyplomowe z tego zakresu lub ukończone szkolenie dla inspektorów danych osobowych,
- c) posiada kwalifikacje i wiedzę fachową niezbędną do realizacji zadań, o których mowa w art. 39 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. Urz. UE L 119 z 04.05.2016, str. 1) i obowiązujących przepisach krajowych,
- d) nie był karany za przestępstwo lub przestępstwo skarbowe oraz wobec której nie jest prowadzone postępowanie o przestępstwo ścigane z oskarżenia publicznego lub przestępstwo skarbowe,
- e) posiada co dwuletnie doświadczenie w projektowaniu, wdrażaniu oraz utrzymaniu systemów ochrony danych osobowych,
- f) posiada doświadczenie w prowadzeniu audytów z zakresu ochrony danych osobowych

§ 2

Zasady wykonywania umowy

1. Zleceniobiorca będzie wykonywał swoje obowiązki z należyтым uwzględnieniem ryzyka związanego z operacjami przetwarzania danych osobowych występującymi u Zleceniodawcy, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. Obie strony zgodnie oświadczają, że działalność Zleceniobiorcy ma charakter pomocniczo-doradczy i nie zwalnia Zleceniodawcy z obowiązku stosowania adekwatnych środków technicznych i organizacyjnych (w tym właściwych procedur i dobrych praktyk) w celu zapewnienia odpowiedniego stopnia bezpieczeństwa przetwarzanych danych.
2. Zleceniodawca oświadcza dodatkowo, że w celu uczynienia zadość obowiązkowi, o którym mowa w ust. 1, wymagana jest ścisła współpraca z Inspektorem.

3. Zleceniobiorca wyznacza osobę do wykonywania zadań Inspektora, o czym informuje Zleceniodawcę. Zleceniobiorca oświadcza, że osoba ta posiada stosowne kwalifikacje zawodowe, wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności do wypełnienia zadań, o których mowa w art. 39 ust. 1 RODO. Inspektor, w zgodzie z art. 38 ust. 3 zd. 3 Rozporządzenia, podlega w zakresie wykonywania czynności, o których mowa w § 1 ust. 3 Umowy, bezpośrednio najwyższemu kierownictwu Zleceniodawcy – Administratora.
4. W przypadku usprawiedliwionej nieobecności Inspektora lub wykonania czynności wynikających z Umowy do których konieczna jest wyspecjalizowana i fachowa wiedza, Zleceniobiorca zobowiązuje się do zapewnienia ciągłości obsługi Zleceniodawcy w zakresie Umowy przez pozostałych pracowników Zleceniobiorcy posiadających odpowiednie kompetencje, na co Zleceniodawca wyraża zgodę.
5. Zleceniodawca wyraża zgodę na przeprowadzenie przez Zleceniobiorcę czynności w zakresie objętym wszelkimi audytami, w tym udziela Zleceniobiorcy zgody na przetwarzanie danych zgromadzonych podczas Audytów IT (w tym – danych osobowych), przy czym Zleceniobiorca zobowiązany jest do:
 - a) przetwarzania danych jedynie w zakresie i celu wykonania Umowy, co obejmuje również uprawnienie do przetwarzania danych w okresie po zakończeniu obowiązywania niniejszej Umowy w celu ewentualnego wykonywania roszczeń z tytułu niewykonania lub niewłaściwego wykonania Umowy;
 - b) dopuszczania do przetwarzania danych jedynie osoby posiadające stosowne upoważnienie Zleceniobiorcy;
 - c) na wniosek Zleceniodawcy – do informowania go o zasadach przetwarzania przez niego danych uzyskanych w związku z przeprowadzaniem monitoringiem w zakresie wykorzystania sprzętu i legalności oprogramowania systemów informatycznych, o którym mowa w § 1 ust. 6 lit. b) Umowy, jak również wykonywaniem obowiązków umownych oraz do udostępniania mu wytworzonej w związku z przetwarzaniem danych dokumentacji oraz informacji o stosowanych przez niego procedurach przetwarzania danych;
 - d) stosowania adekwatnych środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa danych.
6. Zleceniobiorca zobowiązany jest zapewnić poufność informacji oraz wszelkiego rodzaju danych (w tym danych osobowych), które uzyskał od Zleceniodawcy w związku z realizacją niniejszej Umowy. Zleceniobiorca nie będzie ujawniać tych informacji bez uprzedniej pisemnej zgody Zleceniodawcy, za wyjątkiem sytuacji, w których do ich ujawnienia zobowiązują go przepisy powszechnie obowiązującego prawa. Zobowiązanie, o którym mowa w zdaniu poprzedzającym, zachowuje moc również bezterminowo po zakończeniu obowiązywania niniejszej Umowy.
7. Zleceniodawca przyjmuje do wiadomości, że w celu prawidłowego wykonywania obowiązków wynikających z niniejszej Umowy, Zleceniobiorca powinien mieć uprawnienie do przetwarzania danych osobowych przetwarzanych w siedzibie Zleceniodawcy, uprawnienie do wstępu do wskazanych pomieszczeń, uprawnienie do dostępu do urządzeń, komputerów oraz systemów informatycznych znajdujących się

w siedzibie Zleceniodawcy oraz wykonywania wszelkich innych niezbędnych czynności faktycznych, przy czym zgodę na ww. czynności wyraża.

§ 3

Obowiązki Stron Umowy w zakresie Audytu IT

1. Zleceniodawca oświadcza, że w celu umożliwienia prawidłowego wykonania usługi przez Zleceniobiorcę, o której mowa w § 1 ust. 6 lit. b Umowy, wyraża zgodę na instalację oprogramowania monitorującego, którym dysponuje Zleceniobiorca. W przypadku niewyrażenia przez Zleceniodawcę zgody, o której mowa w zdaniu poprzedzającym, Zleceniobiorca wykona Audyt IT z wykluczeniem m.in. danych inwentaryzacyjnych oraz danych dotyczących aktywności użytkowników stacji roboczych.
2. Zleceniodawca zobowiązuje się do przedłożenia Zleceniobiorcy pisemnego oświadczenia o poinformowaniu użytkowników stacji roboczych znajdujących się w sieci komputerowej Zleceniodawcy o fakcie dokonywania monitorowania wykorzystania sprzętu i legalności oprogramowania znajdującego się na tym sprzęcie w celu przeprowadzenia Audytu IT, o którym mowa w § 1 ust. 6 lit. b) Umowy. Wzór oświadczenia, o którym mowa w zdaniu poprzednim stanowi załącznik nr 3 do Umowy.
3. W przypadku nieprzedłożenia przez Zleceniodawcę oświadczenia, o którym mowa w ustępie powyżej Zleceniobiorca wykona Audyt IT z wykluczeniem m.in. danych dotyczących aktywności użytkowników stacji roboczych.
4. W przypadku niewykonania przez Zleceniodawcę obowiązku poinformowania użytkowników stacji roboczych znajdujących się w sieci komputerowej Zleceniodawcy i wprowadzenia w tym zakresie w błąd Zleceniobiorcę przedkładając mu nieprawdziwe oświadczenie, o którym mowa w ust. 1, Zleceniodawca ponosi wyłączną odpowiedzialność w pełnej wysokości za ewentualną szkodę, jaką z tego tytułu może ponieść Zleceniobiorca, a Zleceniobiorcy przysługiwać będzie w takim wypadku uprawnienie do rozwiązania niniejszej Umowy ze skutkiem natychmiastowym (bez wypowiedzenia).
5. Oprogramowanie służące wykonaniu Audytu IT zostanie odinstalowane bez zbędnej zwłoki w sposób zdalny przez Zleceniobiorcę po wygenerowaniu raportu z Audytu IT. W przypadku problemów z odinstalowaniem oprogramowania Zleceniodawca ustali ze Zleceniobiorcą termin i sposób usunięcia oprogramowania.
6. W przypadku problemów z odinstalowaniem oprogramowania, o którym mowa w ust. 4 niniejszego paragrafu Zleceniobiorca będzie uprawniony do przetwarzania danych gromadzonych przez oprogramowanie ze stacji roboczych przez okres od dnia wygenerowania raportu z Audytu IT do dnia jego skutecznego odinstalowania.

§ 4

Zasady postępowania z danymi

1. Zleceniobiorca oświadcza, że dane Zleceniodawcy gromadzone na jego serwerach w ramach wykonywania monitorowania, o którym mowa w § 1 ust. 6 lit. b) Umowy, zabezpieczone są zgodnie z wymogami międzynarodowej normy standaryzującej systemy zarządzania bezpieczeństwem informacji PN-ISO/IEC 27001:2014-12. Zleceniobiorca

posiada ważny, wydany przez jednostkę akredytowaną przez Polskie Centrum Akredytacji, certyfikat w tym zakresie.

2. Zleceniobiorca po ustaniu Umowy z jakiegokolwiek przyczyny (tj. po jej wygaśnięciu, wypowiedzeniu, odstąpieniu, rozwiązaniu, etc.) zobowiązuje się do niezwłocznego, trwałego usunięcia danych Zleceniodawcy, uzyskanych w związku wykonywaniem Umowy. Obowiązek, o którym mowa w zdaniu poprzedzającym, nie dotyczy przypadku, o którym mowa w § 3 ust. 5 Umowy.
3. Zleceniodawca powierza Zleceniobiorcy dane osobowe uzyskane w związku z wykonywaniem monitorowania, o którym mowa w § 1 ust. 6 lit. b) Umowy, do przetwarzania w celu wykonania niniejszej Umowy; przepisy § 2 ust. 5 Umowy stosuje się odpowiednio.

§ 5

Szczególny obowiązek zawarcia umowy ubezpieczenia

1. Zleceniobiorca ponosi odpowiedzialność za szkody wyrządzone Zleceniodawcy i jego pracownikom, osobom trzecim, spowodowane niewykonaniem lub nienależnym wykonaniem usług będących przedmiotem niniejszej umowy, a także za powstałe w związku z wykonywaną usługą, z wyłączeniem zdarzeń będących wynikiem siły wyższej lub powstałych z wyłącznej winy Zleceniodawcy.
2. Zleceniobiorca w okresie obowiązywania umowy będzie posiadał ubezpieczenie od odpowiedzialności cywilnej w zakresie prowadzonej działalności gospodarczej związanej z przedmiotem niniejszej umowy na łączną wartość nie mniejszą niż 1 000 000 zł (słownie: jeden milion złotych) oraz zobowiązuje się do posiadania nieprzerwanej ochrony ubezpieczeniowej przez cały okres trwania umowy. Kopia polisy ubezpieczeniowej zostanie wydana do wglądu na każde żądanie Zleceniodawcy.
3. W przypadku polisy opłacanej w ratach, Zleceniobiorca każdorazowo przedstawi do wglądu niezwłocznie Zleceniodawcy na jego żądanie potwierdzenie jej opłacenia.

§ 6

Wynagrodzenie umowne

1. Z tytułu realizacji niniejszej Umowy Zleceniobiorcy przysługiwać będzie ryczałtowe wynagrodzenie miesięczne, płatne z góry, w wysokości 813,01 zł netto (słownie: osiemset trzynaście złotych jeden grosz netto) plus należny podatek VAT wedle stawki obowiązującej w danym miesiącu (w dalszej części niniejszej Umowy zwane również jako: „Wynagrodzenie”).
2. Okres rozliczeniowy wynosi jeden miesiąc, z wyjątkiem pierwszego, który obejmuje okres od daty rozpoczęcia obowiązywania Umowy do ostatniego kalendarzowego dnia miesiąca, w którym Zleceniobiorca otrzymał egzemplarz podpisanej Umowy.
3. W przypadku, o którym mowa w ust. 2 pierwsza wystawiona przez Zleceniobiorcę faktura obejmować będzie okres od dnia rozpoczęcia obowiązywania Umowy do ostatniego kalendarzowego dnia miesiąca, w którym Zleceniobiorca otrzymał egzemplarz podpisanej Umowy.

4. Wynagrodzenie będzie płatne w terminie 7 dni od daty dostarczenia Zleceniodawcy prawidłowo wystawionej faktury VAT, przelewem na rachunek Zleceniobiorcy podany na fakturze. W przypadku opóźnienia w zapłacie Wynagrodzenia Zleceniodawca zobowiązany będzie do zapłaty odsetek ustawowych za opóźnienie na rzecz Zleceniobiorcy. Faktura VAT wystawiona zostanie najpóźniej do 7-go dnia każdego miesiąca obowiązywania Umowy.
5. W tym miejscu Strony określają dane potrzebne do wystawienia faktury VAT:
 - a) **NABYWCA:** Gmina Gniewkowo, ul. 17 Stycznia 11, 88-140 Gniewkowo, NIP: 556-25-63-314
 - b) **ODBIORCA:** Gmina Gniewkowo, ul. 17 Stycznia 11, 88-140 Gniewkowo, NIP: 556-25-63-314
6. Zleceniodawca oświadcza, że wyraża zgodę na przysyłanie drogą elektroniczną faktur, faktur korygujących, jak również duplikatów tych faktur wystawionych przez Zleceniobiorcę zgodnie z powszechnie obowiązującymi przepisami, w formacie PDF, na adres e-mail: urząd@gniewkowo.com.pl
7. Zleceniobiorca oświadcza, że faktury, faktury korygujące, jak również duplikaty tych faktur będą przysyłane z adresu e-mail: faktury@cbi24.pl.
8. Strony oświadczają, iż zmiana adresów e-mail określonych w ust. 6 i 7 nie stanowi zmiany Umowy i nie wymaga zgody drugiej Strony. O zmianie adresów e-mail określonych w ust. 6 i 7 Strony będą sobie przekazywać informacje niezwłocznie w formie pisemnej lub elektronicznej.
9. Faktury, faktury korygujące, jak również duplikaty tych faktur Strony uznają za skutecznie doręczone z dniem ich wysłania przez Zleceniobiorcę na adres e-mail określony w ust. 6 niniejszego paragrafu.

§ 7

Okres obowiązywania Umowy oraz możliwość jej wypowiedzenia

1. Niniejsza Umowa zostaje zawarta na czas określony od dnia **13 grudnia 2019 r.** do dnia **31 grudnia 2020 r.**
2. Każdej ze Stron przysługuje uprawnienie do wypowiedzenia niniejszej Umowy z zachowaniem trzymiesięcznego okresu wypowiedzenia ze skutkiem na koniec miesiąca, następującego po miesiącu, w którym oświadczenie o wypowiedzeniu zostało złożone drugiej Stronie.
3. Jeżeli Zleceniodawca nie odwoła Inspektora Ochrony Danych wskazanego przez Zleceniobiorcę na mocy niniejszej Umowy najpóźniej ostatniego dnia obowiązywania Umowy, ulega ona przekształceniu w Umowę na czas nieokreślony. Oświadczenie o odwołaniu Inspektora ochrony danych, o którym mowa w zdaniu poprzedzającym, może zostać wyrażone w formie pisemnej, bądź w drodze wiadomości e-mail. Umowa zawarta na czas nieokreślony może zostać wypowiedziana, z zachowaniem terminu określonego w ustępie 2.

§ 8

Kary umowne

1. W przypadku niewykonania lub nienależytego wykonania umowy Zleceniobiorca zobowiązuje się zapłacić Zleceniodawcy kary umowne z następujących tytułów, w wysokości:

1) w przypadku opóźnienia w realizacji usług opisanych w § 1 ust. 4, ust. 5 i ust. 6 oraz § 9 ust. 9 niniejszej umowy, Zleceniobiorca zapłaci Zleceniodawcy karę umowną w wysokości 1% wynagrodzenia miesięcznego, o którym mowa w § 6 ust. 1 Umowy, przysługującego z tytułu realizacji umowy za każdy dzień opóźnienia;

2. Kary umowne będą potrącane z wynagrodzenia należnego Zleceniobiorcy na podstawie pisemnego powiadomienia przez Zleceniodawcę o potrąceniu.

3. Jeżeli wysokość poniesionej szkody przewyższy wysokość zastrzeżonych kar umownych, Zleceniodawca będzie dochodził odszkodowania na zasadach ogólnych, określonych przepisami Kodeksu Cywilnego.

§ 9

Powierzenie danych do przetwarzania

1. Zleceniodawca powierza Zleceniobiorcy przetwarzanie danych osobowych w związku z wykonaniem niniejszej Umowy i w celu jej wykonania.
2. Przetwarzanie dotyczyć będzie danych osobowych osób wykonujących pracę na rzecz Zleceniodawcy (niezależnie od podstawy prawnej świadczenia pracy), które są przetwarzane w związku z niniejszą Umową.
3. Zleceniobiorca przetwarza dane osobowe wyłącznie na udokumentowane polecenie Zleceniodawcy oraz:
 - a) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
 - b) podejmuje odpowiednie środki techniczne oraz organizacyjne, mające na celu zapewnienia przetwarzanych bezpieczeństwa danych osobowych;
 - c) w miarę możliwości pomaga Zleceniodawcy, poprzez odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w art. 12-23 Rozporządzenia;
 - d) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Zleceniodawcy wywiązać się z obowiązków określonych w art. 32-36 Rozporządzenia;
 - e) po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji Zleceniodawcy, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, w tym również te, zawarte na nośnikach danych, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

- f) udostępnia Zleceniodawcy wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia oraz umożliwia Zleceniodawcy (lub upoważnionemu przez niego audytorowi) przeprowadzanie audytów, w tym inspekcji.
 - g) Jeżeli powierzone dane osobowe są przetwarzane w formie elektronicznej na serwerach i nośnikach danych Zleceniobiorcy, te serwery i nośniki nie mogą znajdować się poza obszarem Unii Europejskiej i Europejskiego Obszaru Gospodarczego.
4. Zleceniobiorca zobowiązuje się do każdorazowego i niezwłocznego informowania Zleceniodawcy o przypadkach naruszenia przepisów prawa dotyczących ochrony powierzonych danych osobowych, w tym w szczególności przepisów RODO, zaistniałych w okresie obowiązywania niniejszej Umowy. Zleceniobiorca współdziała ze Zleceniodawcą przy ustalaniu szczegółów związanych ze zgłoszonym Zleceniodawcy naruszeniem, w szczególności przyczyn i skutków jego wystąpienia oraz wdraża zalecane przez Zleceniodawcę środki, mające na celu złagodzenie ewentualnych niekorzystnych skutków naruszenia danych osobowych oraz środki naprawcze.
5. W przypadku stwierdzenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 Rozporządzenia, Zleceniobiorca zgłasza je Zleceniodawcy bez zbędnej zwłoki. Zgłoszenie naruszenia ochrony danych osobowych do Zleceniodawcy powinno nastąpić w formie pisemnej lub elektronicznej i powinno obejmować co najmniej:
- a) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane osobowe dotyczą, oraz kategorie i przybliżoną liczbę wpisów, których dotyczy naruszenie;
 - b) możliwe konsekwencje naruszenia ochrony danych osobowych;
 - c) środki zastosowane lub proponowane przez Zleceniobiorcę w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
6. Na wypadek naruszenia przez Zleceniobiorcę zasad przetwarzania danych osobowych (określonych w przepisach powszechnie obowiązującego prawa, Rozporządzenia oraz niniejszej Umowy), skutkującego zobowiązaniem Zleceniodawcy (w szczególności na mocy prawomocnego orzeczenia sądu, ugody sądowej bądź porozumienia mediacyjnego, lub też decyzji/postanowienia) do wypłaty odszkodowania, zadośćuczynienia, grzywny lub kary pieniężnej lub też w przypadku poniesienia przez Zleceniodawcę innej szkody, Zleceniobiorca zobowiązuje się zrekompensować Zleceniodawcy doznaną z tego tytułu szkodę w pełnej wysokości, jeżeli powstanie tego obowiązku jest wynikiem zawinionego działania Zleceniobiorcy.
7. Zleceniobiorca zapewnia, że dane osobowe nie będą udostępniane osobom wykonującym pracę na jego rzecz, przed podpisaniem przez nich oświadczeń lub umów o zachowaniu poufności. Zachowanie poufności nie ustaje po rozwiązaniu lub wygaśnięciu stosunku pracy lub umowy cywilnoprawnej, niezależnie od przyczyny tego rozwiązania lub wygaśnięcia.
8. Zleceniobiorca zobowiązuje się do monitorowania i stosowania przepisów prawa, powszechnie dostępnych wskazówek i zaleceń organu nadzorczego oraz unijnych organów doradczych, zajmujących się ochroną danych osobowych, w zakresie przetwarzania powierzonych mu danych, po uprzednim uzgodnieniu wpływu tych regulacji na przetwarzanie danych z Zleceniodawcą.

9. Zleceniodawca przez cały okres obowiązywania Umowy jest uprawniony do kontroli poprawności zabezpieczenia i przetwarzania danych powierzonych Zleceniobiorcy. Kontrola może zostać przeprowadzona m.in. w formie bezpośredniej inspekcji polegającej na dopuszczeniu przedstawicieli Zleceniodawcy do wszystkich obszarów przetwarzania danych osobowych objętych niniejszą Umową we wszystkich lokalizacjach Zleceniobiorcy, w sposób nieutrudniający nadmiernie jego bieżącej działalności, z co najmniej 14-dniowym uprzedzeniem. Zleceniobiorca zobowiązany jest do przedstawienia odpowiednich dokumentów do kontroli oraz wyjaśnień na piśmie na każde wezwanie Zleceniodawcy w terminie do 30 dni od otrzymania wezwania.
10. W przypadku, gdy kontrola, o której mowa w ust. 9, wykaże jakiegokolwiek nieprawidłowości Zleceniodawca ma prawo żądać od Zleceniobiorcy niezwłocznego wdrożenia zgodnych z prawem zaleceń Zleceniodawcy wynikających z ustaleń pokontrolnych. Zalecenia te przedstawiane będą w formie ustnej, pisemnej lub elektronicznej.
11. Zleceniodawca wyraża zgodę na podpowierzenie przez Zleceniobiorcę powierzonych danych osobowych podmiotom współpracującym z nim (tzw. podpowierzenie). Podpowierając przetwarzanie danych osobowych innym podmiotom, Zleceniobiorca jest obowiązany zapewnić w dalszej umowie powierzenia spełnienie przez ten podmiot wszelkich wymogów w zakresie ochrony danych osobowych na poziomie, co najmniej takim samym jak przewidziany w niniejszej Umowie. Zleceniobiorca przy podpowierzeniu danych osobowych innym podmiotom zobowiąże te podmioty również do przestrzegania postanowień niniejszej umowy w zakresie obowiązków dotyczących ochrony danych osobowych.
12. Zleceniobiorca zobowiązuje się do zachowania w tajemnicy wszelkich danych osobowych, informacji i materiałów przekazanych lub udostępnionych mu lub o których wiedzę powziął w związku z realizacją Umowy, a także powstałych w wyniku jej wykonania informacji i materiałów w formie pisemnej, graficznej lub jakiegokolwiek innej formie. Informacje i materiały są objęte tajemnicą i nie mogą być bez uprzedniej pisemnej zgody Zleceniodawcy udostępniane jakiegokolwiek osobie trzeciej, ani też ujawnione w inny sposób, chyba że w dniu ich ujawnienia były powszechnie znane albo muszą być ujawnione zgodnie z powszechnie obowiązującymi przepisami prawa, orzeczeniem sądu lub organu państwowego.
13. Zleceniobiorca zapewnia, że osoby upoważnione do przetwarzania danych osobowych będą obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia. Obowiązek zachowania tajemnicy nie ustaje po zaprzestaniu przetwarzania danych z jakiegokolwiek podstawy.

§ 10

Postanowienia końcowe

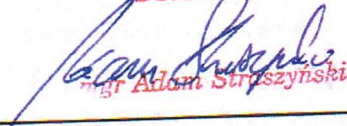
1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym egzemplarzu dla każdej ze Stron.
2. Osoby upoważnione do kontaktu ze strony **Zleceniodawcy**:
 - a) Magdalena Tyburek , tel.: 52 35-43-020; e- mail: tyburek@gniewkowo.com.pl
3. Osoby upoważnione do kontaktu ze strony **Zleceniobiorcy**:

- a) Biuro, tel.: 82 561 13 02, e-mail: biuro@cbi24.pl
b) Dział księgowości, tel.: 533-858-100, e-mail: faktury@cbi24.pl.
4. Wszelkie zmiany i uzupełnienia niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
5. W przypadku sporu pozostającego w związku z niniejszą Umową sądem właściwym dla rozpatrzenia sprawy będzie sąd miejscowo właściwy według siedziby Zleceniodawcy.
6. Strony zgodnie oświadczają, iż poza niniejszą Umową i w zakresie objętym jej treścią nie istnieją dokonane między nimi jakiegokolwiek dodatkowe ważne pisemne lub ustne ustalenia i porozumienia.

Załączniki:

1. Wykaz dokumentów,
2. Upoważnienie,
3. Wzór oświadczenia.

BURMISTRZ


mgr Andrzej Straszynski

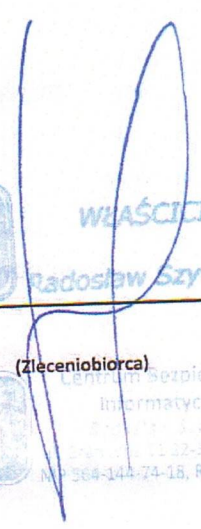
(Zleceniodawca)

Skarbnik Gminy


mgr Wioletta Kucharska

(Kontrasygnata Skarbnika)

WŁAŚCICIEL


Radosław Szymaszek

(Zleceniobiorca)

Centrum Bezpieczeństwa
Informatycznego

ul. 17 stycznia 11
88-140 Gniewkowo
tel: (52) 354-30-08, fax-37
NIP 556-25-63-314

GMINA GNIEWKOWO

ul. 17 stycznia 11
88-140 Gniewkowo
tel: (52) 354-30-08, fax-37
NIP 556-25-63-314

Załącznik nr 1

Wykaz dokumentów, które Inspektor Danych Osobowych opracuje we współpracy ze Zleceniodawcą w ramach Umowy:

1. Rejestr **czynności** przetwarzania danych;
2. Analiza **ryzyka** systemu informatycznego oraz danych osobowych;
3. **Polityka** ochrony danych z załącznikami tj.:
 - b) Procedura zgłaszania naruszeń ochrony danych osobowych;
 - c) Procedura realizacji uprawnień wynikających z RODO;
 - d) Wykaz osób zapoznanych z Polityką Ochrony Danych;
 - e) Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych;
 - f) Wzór odwołania zgody na przetwarzanie danych osobowych;
 - g) Wzór klauzuli informacyjnej;
 - h) Realizacja prawa dostępu do danych osobowych;
 - i) Wzór wniosku o nadanie upoważnienia do przetwarzania danych osobowych/
uprawnienia do pracy w systemie informatycznym;
 - j) Wzór upoważnienia do przetwarzania danych osobowych;
 - k) Wzór ewidencji osób upoważnionych do przetwarzania danych;
 - l) Opis środków technicznych i organizacyjnych;
 - m) Wzór oświadczenia o zachowaniu w poufności danych;
 - n) Wzór umowy powierzenia;
 - o) Wzór rejestru umów powierzenia przetwarzania danych osobowych;
 - p) Wzór rejestru naruszeń ochrony danych;
 - q) Wzór zgłoszenia naruszenia ochrony danych organowi nadzorcemu;
 - r) Wzór zawiadomienia o naruszeniu danych osobowych;
 - s) Wzór notatki z kontroli uprawnień;
 - t) Oświadczenie o monitorowaniu komputerów służbowych.

Upoważnienie

CBI/...../.....

wydane w dniu r

Ja niżej podpisany Radosław Szymaszek, prowadzący działalność gospodarczą pod firmą Radosław Szymaszek Centrum Bezpieczeństwa Informatycznego z siedzibą w Krasnymstawie – jako Zleceniobiorca, upoważniam:

Pana/Panią

.....

posiadającego identyfikator o numerze ID ../CBI do przeprowadzenia Audytu IT.

Numer upoważnienia oraz jego status, można zweryfikować na stronie CBI, pod adresem: www.cbi24.pl/weryfikacja/.....

(miejscowość)

(data)

**Oświadczenie Zleceniodawcy
o poinformowaniu wszystkich użytkowników stacji roboczych znajdujących się w sieci
komputerowej o zainstalowaniu oprogramowania monitorującego**

Oświadczam, iż poinformowano wszystkich użytkowników stacji roboczych znajdujących się w sieci komputerowej Zleceniodawcy o zamiarze zainstalowania oprogramowania monitorującego w zakresie ilościowego i jakościowego wykorzystania sprzętu pracowniczego i legalności oprogramowania, w celu wykonania Audytu IT.

(podpis)