

Umowa powierzenia przetwarzania danych osobowych

zawarta w Poznaniu w dniu r. pomiędzy:

Miastem Poznań Poznańskimi Ośrodkami Sportu i Rekreacji w Poznaniu,
ul. Jana Spychalskiego 34, 61-553 Poznań, NIP: 209-00-01-440, Regon: 630603890,
reprezentowanymi przez Łukasza Miadziołko – Dyrektora POSiR
w dalszej części niniejszej umowy zwanym „**Administratorem**”
a

.....

.....

.....

w dalszej części niniejszej umowy zwanym „**Podmiotem przetwarzającym**”

łącznie zwanymi dalej „Stronami”

§1

Przedmiot Umowy

1. Administrator i Podmiot przetwarzający oświadczają, że w dniu zawarli umowę nr w przedmiocie obsługi informatycznej Administratora, zwaną dalej Umową Główną, z tytułu której będą przetwarzane dane osobowe.
2. Niniejsza – akcesoryjna względem Umowy Głównej – Umowa powierzenia przetwarzania danych osobowych, zwana dalej Umową, reguluje wzajemny stosunek Stron i obowiązki w zakresie przetwarzania danych osobowych wynikających z zawartej Umowy Głównej.

§2

Definicje

Dla potrzeb niniejszej Umowy, o ile z treści i celu Umowy nie wynika inaczej, przyjmuje się następujące znaczenie dla poniżej wymienionych sformułowań:

- 1) **RODO** – Rozporządzenie 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;
- 2) **Ustawa** – obowiązująca ustawa o ochronie danych osobowych;
- 3) **Administrator** – 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;
- 4) **Podmiot przetwarzający** - w rozumieniu art. 4 pkt. 8 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 uchylecia dyrektywy 95/46/WE;

- 5) **Inny podmiot przetwarzający** - podmiot, któremu Podmiot przetwarzający w imieniu Administratora powierzył dane osobowe do dalszego przetwarzania w całości lub częściowo.
- 6) **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- 7) **Dane zwykłe** – oznaczają dane osobowe podstawowe, inne niż dane wrażliwe;
- 8) **Dane wrażliwe** – oznaczają dane osobowe podlegające szczególnej ochronie, o których mowa w art. 9 ust. 1 oraz art. 10 RODO;
- 9) **Dane poufne** - wszelkie informacje, dane, materiały, dokumenty i dane osobowe otrzymane od Administratora i od współpracujących z nim osób oraz dane uzyskane w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej dotyczące Administratora i przedmiotu Umowy;
- 10) **Organ nadzorczy** - Prezes Urzędu Ochrony Danych Osobowych;
- 11) **Umowa** – niniejsza umowa;
- 12) **Przetwarzanie danych osobowych** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, 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.

§3

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 RODO dane osobowe do przetwarzania, na zasadach i w celu określonym w Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe na polecenie Administratora zgodnie z Umową, RODO, Ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO i daje gwarancję wdrożenia i stosowania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane są przetwarzane na podstawie Umowy.
4. Podmiot przetwarzający oświadcza, że przetwarzanie powierzonych danych osobowych będzie się odbywało na terenie Europejskiego Obszaru Gospodarczego, z zastrzeżeniem § 8 ust. 2.

5. Upoważnienia do przetwarzania danych osobowych pracownikom Podmiotu przetwarzającego którymi Podmiot przetwarzający posługuje się przy wykonywaniu niniejszej umowy nadaje Podmiot przetwarzający .

§4

Zakres i cel przetwarzania danych

1. Cel i zakres powierzenia przetwarzania danych osobowych wynika bezpośrednio i ogranicza się wyłącznie do zadań wynikających z zawartej Umowy Głównej, tj. obsługi informatycznej Administratora.

Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie Umowy:

- a) dane zwykłe, dotyczące klientów Administratora, pracowników Administratora, kontrahentów Administratora, zleceniobiorców Administratora, składających skargi, wnioski oraz innego rodzaju pisma do Administratora, których dane są wprowadzone do systemów informatycznych Administratora oraz osób objętych monitoringiem wizyjnym Administratora.
 - b) dane szczególnej kategorii, dotyczące klientów Administratora, pracowników Administratora, kontrahentów Administratora, zleceniobiorców Administratora, składających skargi, wnioski oraz innego rodzaju pisma do Administratora, których dane są wprowadzone do systemów informatycznych Administratora.
2. Dane osobowe będą przetwarzane w formie elektronicznej w systemie informatycznym poprzez wykonywanie takich operacji jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, modyfikowanie, przeglądanie, pobieranie, wykorzystywanie, rozpowszechnianie, łączenie, usuwanie, niszczenie.

§5

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia przed naruszeniem bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych (naruszenie ochrony danych osobowych) poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa zgodnie art. 32 RODO. Wykaz minimalnych środków, które zobowiązany jest wdrożyć Podmiot przetwarzający został określony w załącznik nr 1 do Umowy.
2. Przetwarzanie danych osobowych przez Podmiot przetwarzający będzie odbywać się wyłącznie na udokumentowane polecenie Administratora.
3. Za udokumentowane polecenie uznaje się zadania zlecone do wykonywania Podmiotowi przetwarzającemu na podstawie Umowy oraz Umowy Głównej.
4. Podmiot przetwarzający zobowiązuje się do:
 - a) nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które

będą przetwarzały powierzone dane w celu realizacji Umowy oraz prowadzenia ich ewidencji,

- b) zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- c) zobowiązania osób upoważnionych do przetwarzania danych osobowych do zachowania tych danych oraz sposobu ich zabezpieczenia w tajemnicy, także po zakończeniu zatrudnienia,
- d) prowadzenia rejestru wszystkich kategorii czynności przetwarzania, wykonywanych w imieniu Administratora zgodnie z art. 30 ust. 2 RODO,
- e) powiadamiania Administratora o każdym naruszeniu ochrony danych osobowych, nawet jeśli w jego ocenie nie jest ono na tyle poważne, by podlegać notyfikacji do Organu nadzorczego zgodnie z RODO, bez zbędnej zwłoki, jednak nie później niż w ciągu 24 godzin od jego wystąpienia. Powiadomienie nastąpi poprzez przesłanie wypełnionego formularza „Zgłoszenie naruszenia danych osobowych” stanowiącego załącznik nr 2 do Umowy oraz dołączenie do zgłoszenia wszelkiej niezbędnej dokumentacji dotyczącej naruszenia, tak by umożliwić Administratorowi spełnienie obowiązku powiadomienia Organu nadzorczego.

Jeżeli przekazanie wszystkich powyższych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji Podmiot przetwarzający przekazuje je Administratorowi bez zbędnej zwłoki.

- f) wdrożenia dokumentacji dotyczącej ochrony informacji, w tym danych osobowych zgodnej z RODO i Ustawą.

5. Po zakończeniu świadczenia usługi realizowanej na podstawie Umowy Głównej Podmiot przetwarzający, w zależności od decyzji Administratora, zobowiązany jest w terminie 7 dni do zwrotu danych w formacie określonym przez Administratora lub usunięcia powierzonych danych osobowych ze wszystkich nośników, zarówno w wersji elektronicznej jak i papierowej oraz do podjęcia stosownych działań w celu wyeliminowania możliwości dalszego przetwarzania danych powierzonych na podstawie Umowy, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

W przypadku usunięcia powierzonych danych osobowych, Podmiot przetwarzający zobowiązuje się w ciągu 7 dni od daty ich usunięcia przekazać Administratorowi protokół zniszczenia powierzonych danych osobowych.

Obowiązek o którym mowa w ust. 5 powyżej nie ma zastosowania w przypadku, gdy Podmiot przetwarzający w ramach świadczenia usługi realizowanej na podstawie Umowy Głównej oraz Umowy nie będzie utrzymywał i przechowywał powierzonych danych osobowych.

6. Biorąc pod uwagę charakter przetwarzania, Podmiot przetwarzający pomaga nieodpłatnie Administratorowi poprzez odpowiednie środki techniczne organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO.

7. Podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga nieodpłatnie Administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO.
8. Podmiot przetwarzający zobowiązuje się przekazać Administratorowi informację o wniesieniu żądań wprost do Podmiotu przetwarzającego przez osoby, których dane są przetwarzane w związku z realizacją niniejszej Umowy w terminie do 48 godzin od otrzymania żądania.

§6

Obowiązki informacyjne Podmiotu przetwarzającego wobec Administratora

1. Podmiot przetwarzający zobowiązuje się niezwłocznie przekazywać wszelkie informacje dotyczące zobowiązań publicznych w stosunku do policji i organów ścigania oraz służb specjalnych w zakresie przekazywania im dostępu do danych osobowych powierzonych przez Administratora, a także do niezwłocznego informowania Administratora o wszelkich pismach oraz działaniach podejmowanych przez policję, organy ścigania oraz służby specjalne pozostających w związku z realizacją Umowy.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o:
 - a) prowadzonym postępowaniu, w szczególności administracyjnym lub sądowym, prowadzonym wobec Podmiotu przetwarzającego oraz współpracujących z nim Innych podmiotów przetwarzających w związku z przetwarzaniem danych osobowych określonych w Umowie,
 - b) wydaniu decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania powierzonych danych osobowych, skierowanych do Podmiotu przetwarzającego lub współpracujących z nim Innych podmiotów przetwarzających,
 - c) wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania powierzonych danych osobowych, realizowanych wobec Podmiotu przetwarzającego lub współpracujących z nim Innych podmiotów przetwarzających, w szczególności tych prowadzonych przez Organ nadzorczy, a także o każdym piśmie tego podmiotu, dotyczącym składania wyjaśnień w zakresie powierzonych danych osobowych.
3. Podmiot przetwarzający oświadcza, że w przypadku kontroli Organu nadzorczego, prowadzonej u Administratora dotyczącej przetwarzania powierzonych danych osobowych, będzie przekazywał Administratorowi niezbędne informacje i wyjaśnienia.

§7

Prawo sprawdzenia

1. Administrator ma prawo do przeprowadzania audytów, w tym inspekcji, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy.

2. Podmiot przetwarzający przyjmuje do wiadomości, iż w związku z realizacją Umowy może być poddany sprawdzeniu zgodności przetwarzania danych z obowiązującymi przepisami prawa przez uprawnione podmioty tj. personel Administratora lub niezależnego audytora działającego na zlecenie Administratora. Audyty mogą również obejmować inspekcje w pomieszczeniach lub obiektach fizycznych Podmiotu przetwarzającego.
3. Na wniosek Administratora Podmiot przetwarzający jest zobowiązany do udzielenia informacji na temat przetwarzania powierzonych danych osobowych, w tym na temat zastosowanych przy przetwarzaniu środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w terminie 7 dni od otrzymania wniosku.
4. Administrator realizować będzie prawo sprawdzenia, w siedzibie Podmiotu przetwarzającego i/lub miejscach przetwarzania, w godzinach pracy Podmiotu przetwarzającego i z minimum 3 dniowym jego uprzedzeniem.
5. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas realizacji prawa sprawdzenia w terminie wskazanym przez Administratora nie dłuższym niż 7 dni.
6. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.

§8

Dalsze powierzenie danych do przetwarzania

1. Administrator wyraża zgodę na powierzenie danych osobowych objętych niniejszą Umową do dalszego przetwarzania Innym podmiotom przetwarzającym w celu wykonania niniejszej Umowy. W takim przypadku Podmiot przetwarzający stosuje się do poniższych postanowień określonych przez Administratora:
 - a) Podmiot przetwarzający może powierzyć dane osobowe objęte Umową do dalszego przetwarzania wyłącznie takim Innym podmiotom przetwarzającym, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie przez te podmioty przetwarzające danych osobowych, spełniało wymogi RODO i chroniło prawa osób, których dane są przetwarzane na podstawie Umowy,
 - b) Dalsze powierzenie przetwarzania danych osobowych przez Podmiot przetwarzający Innemu podmiotowi przetwarzającemu wymaga, pod rygorem nieważności, zawarcia umowy w formie pisemnej,
 - c) Umowa, o której mowa w lit. b) musi zawierać wszystkie zobowiązania określone w niniejszej Umowie oraz precyzować czas, charakter i cel przetwarzania danych z uwzględnieniem zakresu (lub kategorii) przetwarzanych danych,
 - d) Podmiot przetwarzający informuje Administratora o planowanym dalszym powierzeniu danych Innemu podmiotowi przetwarzającemu lub o jego zmianie, dając Administratorowi możliwość wyrażenia sprzeciwu w terminie 7 dni roboczych od przekazania informacji o planowanym dalszym powierzeniu danych lub zmianie Innego

podmiotu przetwarzającego.

2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na zasadach określonych w rozdziale V RODO. W takim przypadku Podmiot przetwarzający informuje Administratora o takim przekazaniu.

§9

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający ponosi odpowiedzialność 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 odpowiada za szkody poniesione przez osobę, której dotyczą przetwarzane dane osobowe, Administratora oraz osoby trzecie, spowodowane przetwarzaniem, jeśli nie dopełnił obowiązków, które nakłada Umowa, gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom jak i za te szkody, które powstały na skutek działań niezgodnych z przepisami RODO.
3. Podmiot przetwarzający ponosi odpowiedzialność za działania i zaniechania swoich pracowników oraz Innych podmiotów przetwarzających, którymi posługuje się przy wykonywaniu Umowy, jak za własne działania i zaniechania.
4. W przypadku naruszenia przepisów Ustawy lub RODO w ramach realizacji Umowy z przyczyn leżących po stronie Podmiotu przetwarzającego, w następstwie którego Administrator zostanie zobowiązany do wypłaty odszkodowania lub ukarany grzywną, prawomocnym wyrokiem lub decyzją właściwego organu, Podmiot przetwarzający zobowiązuje się do zwrócenia równowartości odszkodowania, kary pieniężnej lub grzywny zapłaconych przez Administratora.

§10

Czas obowiązywania umowy

Umowa obowiązuje od dnia jej zawarcia przez czas trwania Umowy Głównej.

§11

Rozwiązanie umowy

1. Administrator jest uprawniony do rozwiązania Umowy ze skutkiem natychmiastowym, w przypadku gdy:
 - a) Podmiot przetwarzający, pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas realizacji prawa sprawdzenia nie usunie ich w wyznaczonym terminie;
 - b) Podmiot przetwarzający naruszył zasady przetwarzania danych osobowych określonych w Umowie i/lub w RODO;
 - c) zostanie stwierdzone prawomocną decyzją administracyjną lub prawomocnym

wyrokiem sądu, że Podmiot przetwarzający naruszył zasady ochrony danych osobowych, o których mowa w Umowie oraz w RODO.

2. Rozwiązanie niniejszej Umowy stanowi podstawę do rozwiązania Umowy Głównej.

§12

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy danych poufnych.
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 w innym celu niż wykonanie Umowy lub Umowy Głównej, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy lub Umowy Głównej.
3. Podmiot przetwarzający zobowiązuje się do rozstrzygania wątpliwości w przedmiocie kwalifikacji określonych informacji uzyskanych na potrzeby wykonywania Umowy oraz Umowy Głównej, poprzez ich określenie jako informacje chronione na mocy Umowy.

§13

Administrator w roli podmiotu przetwarzającego dla innych podmiotów

W przypadku, gdy Administrator będzie występował jako podmiot przetwarzający dla innego podmiotu, niniejsza Umowa stanowi jednocześnie umowę powpowierzenia z Podmiotem przetwarzającym, a Podmiot przetwarzający zobowiązuje się do wykonywania tych samych obowiązków i wymogów, które na mocy umowy z tym innym podmiotem zostaną nałożone na Administratora.

§14

Kary umowne

1. W przypadku odstąpienia od Umowy przez którąkolwiek ze Stron z przyczyn leżących po stronie Podmiotu przetwarzającego, Administratorowi przysługuje kara umowna w wysokości 30% wynagrodzenia brutto Podmiotu przetwarzającego określonego w Umowie Głównej.
2. W przypadku niezrealizowania lub nienależytego wykonania przez Podmiot przetwarzający obowiązków objętych Umową, Podmiot przetwarzający zapłaci Administratorowi karę umowną w wysokości 30% wynagrodzenia brutto określonego w Umowie Głównej, z zastrzeżeniem ust. 3.
3. W przypadku obowiązków Podmiotu przetwarzającego, co do których w Umowie wskazano konkretny termin ich realizacji, niewykonanie tych obowiązków w tym terminie pociąga za sobą zobowiązanie Podmiotu przetwarzającego do zapłacenia kary umownej w wysokości 1000 zł za każdy dzień opóźnienia.

4. Administrator zastrzega sobie możliwość dochodzenia odszkodowania przewyższającego wysokość określonych w umowie kar umownych, na zasadach ogólnych kodeksu cywilnego.
5. Administrator ma również możliwość potrącenia naliczonych kar umownych z należności przysługujących Podmiotowi przetwarzającemu z tytułu realizacji Umowy Głównej.

§15

Postanowienia końcowe

1. W przypadku, gdy Umowa odwołuje się do przepisów prawa, oznacza to również inne przepisy dotyczące ochrony danych osobowych, a także wszelkie nowelizacje, jakie wejdą w życie po dniu zawarcia Umowy, jak również akty prawne, które zastąpią wskazane ustawy i rozporządzenia.
2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
3. W sprawach nieuregulowanych Umową mają zastosowanie przepisy prawa obowiązujące na terenie Rzeczypospolitej Polskiej, w tym Kodeksu cywilnego oraz RODO.
4. Umowa ma charakter nieodpłatny.
5. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
6. Sędem właściwym dla rozpatrzenia sporów wynikających z Umowy będzie sąd właściwy dla Administratora.
7. Kontakt do Inspektora ochrony danych, wyznaczonego przez Administratora w celu realizacji Umowy: iod@posir.poznan.pl, tel. 502 519 399.
8. Osobą wyznaczoną przez Podmiot przetwarzający w celu realizacji Umowy jest

Administrator danych:

Podmiot przetwarzający:

.....

.....

**Wykaz minimalnych środków technicznych i organizacyjnych, które zobowiązany jest wdrożyć
Podmiot przetwarzający**

I. Zabezpieczenia organizacyjne

1. Wdrożona dokumentacja w obszarze bezpieczeństwa informacji (w tym systemów informatycznych) i ochrony danych osobowych (polityki, procedury, instrukcje itp.).
2. Osoby przetwarzające dane u podmiotu przetwarzającego zostały przeszkolone w zakresie bezpieczeństwa informacji w tym związanych z systemami informatycznymi.
3. Systematycznie prowadzona analiza ryzyka w obszarze bezpieczeństwa informacji (w tym systemów informatycznych) i ochrony danych osobowych uwzględniająca ryzyka wynikające z przypadkowego lub niezgodnego z prawem:
 - zniszczenia,
 - utraty,
 - modyfikacji,
 - nieuprawnionego ujawnienia lub dostępu do danych.
4. Prowadzone są regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych.
5. Prowadzona jest ewidencja zasobów informatycznych wykorzystywanych do przetwarzania danych osobowych (sprzęt, oprogramowanie, sieć).
6. Prowadzi się regularne przeglądy i aktualizacje zasobów IT.

II. Zabezpieczenia techniczne

1. Określenie obszarów bezpiecznych (biura, pomieszczenia, serwerownie itd.) oraz odpowiednie ich zabezpieczenie przed dostępem osób nieuprawnionych (np. kraty w oknach, rolety antywłamaniowe, wzmocnione drzwi, kontrola dostępu, ochrona fizyczna, CCTV, system alarmowy).
2. Pomieszczenia, w których przetwarzane są dane zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
3. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła (min. 8 znaków, wielkie i małe litery, cyfry i znaki specjalne).
4. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity oraz ich systematyczna aktualizacja.
5. Użyto systemu Firewall do ochrony dostępu do sieci komputerowej.
6. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych w systemie informatycznym (logi).
7. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w systemie informatycznym zbioru danych osobowych.
8. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu służącego do przetwarzania danych.

9. Systemy wymuszają jakość haseł użytkowników (różne grupy znaków, długość haseł).
10. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.
11. Korzystanie z systemów operacyjnych, które mają aktualne wsparcie producenta.
12. Monitorowanie w aktywny sposób bezpieczeństwa systemów informatycznych w tym m. in. działanie serwerów, ruch na serwerach, nieautoryzowane próby wejścia na serwer, próby złamania zabezpieczeń.
13. Wykonywanie kopii zapasowych danych i konfiguracji systemów teleinformatycznych oraz regularne sprawdzanie możliwości ich odtworzenia.
14. W przypadku pracy zdalnej zabronione jest wykorzystywanie prywatnego sprzętu przez pracowników oraz wykorzystuje się bezpieczne kanały komunikacji – VPN.
15. Zabronione jest wykorzystywanie nieautoryzowanych nośników USB.
16. Użytkownicy stacji roboczych nie posiadają uprawnień do instalowania nieautoryzowanego oprogramowania.
17. Komunikacja i dostęp przez internet szyfrowana jest za pomocą protokołów kryptograficznych (TLS/SSL).
18. Dane osobowe przesyłane za pomocą poczty elektronicznej przesyłane są jako zaszyfrowany załącznik (przy użyciu algorytmu szyfrującego AES-256 oraz zabezpieczony co najmniej 9-znakowym hasłem jednorazowym, zawierającym małe i duże litery, cyfry i znaki specjalne) – hasło przekazywane jest innym bezpiecznym kanałem informacyjnym.
19. Systematycznie prowadzone są przeglądy, konserwacja i naprawy systemów informatycznych.
20. Monitoruje się pojemność i wydajność systemów informatycznych.

Załącznik nr 2 do Umowy powierzenia danych

Zgłoszenie naruszenia ochrony danych osobowych

1. Podmiot przetwarzający			
A. Dane podmiotu przetwarzającego			
Pełna nazwa podmiotu przetwarzającego			
REGON – jeśli został podany (opcjonalnie)			
NIP			
B. Adres siedziby podmiotu przetwarzającego			
Państwo		Miejscowość	
Województwo		Ulica	
Powiat		Kod pocztowy	
Gmina		Numer domu/nr	

		lokalu	
C. Inspektor ochrony danych			
Imię i nazwisko			
Numer telefonu			
Adres e-mail			
<input type="checkbox"/> Inspektor nie został wyznaczony			
Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.			
D. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)			
Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie			
2. Czas naruszenia			
1) Wykrycie naruszenia			
Data stwierdzenia naruszenia Wskaż kiedy dowiedziałeś/aś się o naruszeniu. Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.			
Sposób stwierdzenia naruszenia Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa			
Powody opóźnienia powiadomienia administratora o naruszeniu Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż czas określony w umowie powierzenia			
2) Czas naruszenia			
Data i czas zaistnienia/rozpoczęcia naruszenia Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.			
<input type="checkbox"/> Trwające naruszenie Zaznacz to pole, jeśli naruszenie trwa nadal w momencie zgłaszania.			
Data i czas zakończenia naruszenia			

(opcjonalnie) Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.	
3) Komentarz do czasu naruszenia (opcjonalnie)	
Możesz podać więcej szczegółów dotyczących czasu naruszenia i uzasadnić dlaczego nie są znane dokładne terminy zaistnienia naruszenia.	
3. Charakter naruszenia	
6. Charakter	
<div data-bbox="153 613 1528 983"> <input type="checkbox"/> Naruszenie poufności danych Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych </div> <div data-bbox="153 741 1528 819"> <input type="checkbox"/> Naruszenie integralności danych Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania </div> <div data-bbox="153 860 1528 938"> <input type="checkbox"/> Naruszenie dostępności danych Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną </div>	
7. Na czym polegało naruszenie?	
<div data-bbox="153 1050 1528 1901"> <input type="checkbox"/> Zgubienie lub kradzież nośnika/urządzenia <input type="checkbox"/> Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji <input type="checkbox"/> Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy <input type="checkbox"/> Nieuprawnione uzyskanie dostępu do informacji <input type="checkbox"/> Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń <input type="checkbox"/> Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych <input type="checkbox"/> Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing) <input type="checkbox"/> Nieprawidłowa anonimizacja danych osobowych w dokumencie <input type="checkbox"/> Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora <input type="checkbox"/> Niezamierzona publikacja <input type="checkbox"/> Dane osobowe wysłane do niewłaściwego odbiorcy <input type="checkbox"/> Ujawnienie danych niewłaściwej osobie <input type="checkbox"/> Ustne ujawnienie danych osobowych <input type="checkbox"/> Inne (wpisać jakie) </div>	
Opisz na czym polegało naruszenie.	

8. Dzieci

☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

(opcjonalnie)

9. Przyczyna naruszenia

☐ Wewnętrzne działanie niezamierzone

☐ Wewnętrzne działanie zamierzone

☐ Zewnętrzne działanie niezamierzone

☐ Zewnętrzne działanie zamierzone

Inne przyczyny (w tym nieznane)

4. Liczba osób i wpisów

Przybliżona liczba osób, których mogło dotyczyć naruszenie

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

5. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

1. Kategorie danych

Szczegółowy opis kategorii danych, których dotyczy naruszenie

Wymień jakie dane uległy naruszeniu: np. w przypadku sklepu internetowego profil użytkownika, w skład którego wchodzi: nazwa użytkownika, imię, nazwisko, hasło (zapisane otwartym tekstem lub hashowane), adres e-mail, oraz historia transakcji - kwota, data i nazwa kupionego produktu.

2. Dane podstawowe

☐ Dane identyfikacyjne

np. imię, nazwisko, nr dowodu osobistego, adres IP

☐ Krajowy numer identyfikacyjny

np. PESEL, SSN

☐ Dane kontaktowe

np. e-mail, numer telefonu, adres korespondencyjny

☐ Dane ekonomiczne i finansowe

np. historie transakcji, faktury, dane o rachunkach bankowych, wnioski o wsparcie finansowe

☐ Oficjalne dokumenty

np. akty notarialne, dowody osobiste, prawa jazdy, karty pobytu, legitymacje

☐ Dane lokalizacyjne

np. GPS, dane o przemieszczaniu, miejsce zamieszkania

☐ Inne

Opisz poniżej kategorie danych:

3. Dane szczególnej kategorii

- ☐ Dane o pochodzeniu rasowym lub etnicznym
- ☐ Dane o poglądach politycznych
- ☐ Dane o przekonaniach religijnych lub światopoglądowych
- ☐ Dane o przynależności do związków zawodowych
- ☐ Dane dotyczące seksualności lub orientacji seksualnej
- ☐ Dane dotyczące zdrowia
- ☐ Dane genetyczne
- ☐ Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

4. Dane, o których mowa w art. 10 RODO

- ☐ Dane dotyczące wyroków skazujących
- ☐ Dane dotyczące czynów zabronionych
- ☐ Inne

Opisz poniżej kategorie danych:

5. Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie
Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

6. Kategorie osób

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

A. Kategorie osób, których dane dotyczą

- ☐ Pracownicy
- ☐ Użytkownicy
- ☐ Subskrybenci
- ☐ Studenci
- ☐ Uczniowie
- ☐ Służby mundurowe (np. wojsko, policja)
- ☐ Klienci (obecni i potencjalni)
- ☐ Klienci podmiotów publicznych

<input type="checkbox"/> Pacjenci <input type="checkbox"/> Dzieci <input type="checkbox"/> Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)	
Szczegółowy opis kategorii osób, których dotyczy naruszenie. Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie	
B. Liczba osób, których mogło dotyczyć naruszenie	
Przybliżona liczba osób, których mogło dotyczyć naruszenie	
7. Środki bezpieczeństwa zastosowane przed naruszeniem	
<u>Środki zastosowane lub proponowane <u>celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą</u></u>	
8. Możliwe konsekwencje	
A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą	
<input type="checkbox"/> Utrata kontroli nad własnymi danymi osobowymi <input type="checkbox"/> Ograniczenie możliwości realizowania praw z art. 15-22 RODO <input type="checkbox"/> Ograniczenie możliwości realizowania praw <input type="checkbox"/> Dyskryminacja <input type="checkbox"/> Kradzież lub sfalszowanie tożsamości <input type="checkbox"/> Strata finansowa <input type="checkbox"/> Naruszenie dobrego imienia <input type="checkbox"/> Utrata poufności danych osobowych chronionych tajemnicą zawodową <input type="checkbox"/> Nieuprawnione odwrócenie pseudonimizacji <input type="checkbox"/> Inne	
Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:	
B. Ryzyko naruszenia praw i wolności osób fizycznych	
<input type="checkbox"/> Niskie <input type="checkbox"/> Średnie <input type="checkbox"/> wysokie	
6. Środki zaradcze	
A. Środki w celu zaradzenia naruszeniu ochrony danych osobowych	
Opisz dodatkowe środki (poza poinformowaniem osób) zastosowane lub proponowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia i jego ponownego wystąpienia.	