**UMOWA**

**powierzenia przetwarzania danych osobowych**

zawarta dnia ..................... pomiędzy:

**Skarbem Państwa reprezentowanym przez p.o. Wielkopolskiego Komendanta Wojewódzkiego Państwowej Straży Pożarnej**

**st. bryg. mgr inż. Jacka STRUŻYŃSKIEGO**

przy kontrasygnacie Głównego Księgowego mgr Wiesławy Nawrockiej

adres do korespondencji:

Komenda Wojewódzka Państwowej Straży Pożarnej

61-767 Poznań, ul. Masztalarska 3

NIP:778-12-09-832, REGON: 000684493,

zwanym w dalszej części umowy **"Administratorem danych" lub ,,Administratorem"**

a

……………………………………………………………….. , zwanym w dalszej części umowy  **,,Podmiotem przetwarzającym",** reprezentowanym przez: ……………………………………

łącznie zwanymi Stronami

Na podstawie art. 28 ust. 3 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 (zwanego w dalszej części umowy "Rozporządzeniem") mając na względzie zawartą w dniu ....................................... pomiędzy Stronami umowę   
o świadczenie usług. Strony postanawiają, co następuje:

**§ 1**

**Powierzenie przetwarzania danych osobowych**

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 Rozporządzenia,przetwarzanie danych osobowych, na zasadach i w celu określonym w niniejszej Umowie.

2. 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.

3. 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 osobowe zwykłe oraz szczególnej kategorii przesyłane pocztą elektroniczną*.* Przetwarzanie danych osobowych będzie miało charakter **ciągły** i **elektroniczny**.
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy z dnia .............................. dotyczącej **Technicznego utrzymania serwera pocztowego**.

**§ 3**

**Obowiązki podmiotu przetwarzającego**

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia. Podmiot przetwarzający przedstawi Administratorowi informacje o zapewnieniu przez podmiot przetwarzający odpowiednich środków ochrony (technicznych i organizacyjnych), umożliwiających należyte zabezpieczenie danych osobowych, wymaganych zgodnie z załącznikiem nr 1 do niniejszej umowy. Ponadto niezwłocznie jednak nie później niż w terminie 21 dni od wystąpienia zmian, Podmiot przetwarzający poinformuje Administratora o wszelkich zmianach, które zaistnieją w obszarze zapewnionych środków ochrony.

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 w celu realizacji niniejszej umowy.

4. Podmiot przetwarzający, zgodnie z art. 28 ust. 3 pkt b Rozporządzenia, zobowiązuje się zapewnić zachowanie w tajemnicy przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.

5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem zwraca Administratorowi wszelkie dane osobowe oraz usuwa ze swoich zasobów wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.

7. Podmiot przetwarzający będzie udzielał niezbędnego wsparcia Administratorowi danych przy ocenie skutków dla ochrony danych dokonywanych w myśl art. 35 i 36 RODO.

8. Podmiot przetwarzający zobowiązuje się do prowadzenia rejestru wszystkich kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu administratora danych.

9. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w ciągu 24 godzin. Powiadomienie o stwierdzeniu naruszenia, powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organ nadzoru. Podmiot przetwarzający dokonuje zgłoszenia naruszenia ochrony danych osobowych administratorowi danych na druku stanowiącym załącznik nr 2 do niniejszej umowy.

**§4**

**Prawo kontroli**

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Na żądanie Administratora Podmiot przetwarzający okaże Administratorowi dowody na zastosowanie zabezpieczeń, które zostały wcześniej zdeklarowane przez podmiot przetwarzający w załączniku nr 1.

3. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 7 dniowym jego uprzedzeniem.

4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.

5. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

**§ 5**

**Dalsze powierzenie danych do przetwarzania**

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy, po uzyskaniu uprzedniej pisemnej zgody Administratora danych.

2. Podwykonawca winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.

3. 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 tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

**§7**

**Czas obowiązywania umowy**

1. Niniejsza umowa obowiązuje przez czas trwania umowy zawartej w dniu ............................................... dotyczącej świadczenia usług.

2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem 1 miesięcznego okresu wypowiedzenia.

**§ 8**

**Rozwiązanie umowy**

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

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;

b) przetwarza dane osobowe w sposób niezgodny z umową;

c) 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 ze 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.

**§ 10**

**Inspektor Ochrony Danych**

1. Inspektorem Ochrony Danych powołanym przez Administratora Danych jest:

Lucyna Rudzińska

email: iod@psp.wlkp.pl tel.: 47 771 61 89

2. Inspektorem Ochrony Danych powołanym przez Podmiot Przetwarzający jest:

……………………………………………………………………………………….

email: ………………………………….. tel.: …………………………………….

3. O zmianie osoby pełniącej funkcję Inspektora Ochrony Danych strony będą się informowały niezwłocznie bez konieczności zmiany niniejszej umowy.

**§ 11  
Kontakt roboczy**

W celu zapewnienia prawidłowej realizacji niniejszej umowy Strony wskazują osoby kontaktowe w sprawach związanych z jej realizacją, po jednej osobie dla każdej   
ze Stron:

a. dla Administratora danych:

Grzegorz Lewicz

naczelnik Wydziału Informatyki i Łączności KW PSP w Poznaniu

e-mail: wil@psp.wlkp.pl,

tel. 47 771 60 50

b. dla Podmiotu przetwarzającego

……………………………………………………………..

……………………………………………………………..

e-mail: …………………….............,

tel. ………………………..

**§ 12**

**Postanowienia końcowe**

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

2. W sprawach nieuregulowanych w niniejszej umowie zastosowanie będą miały odpowiednie przepisy Kodeksu cywilnego oraz Rozporządzenia.

3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Administratora danych.

4. Umowa zastępuje wszelkie wcześniej obowiązujące umowy powierzenia przetwarzania danych osobowych oraz inne postanowienia umowne dotyczące powierzenia przetwarzania danych osobowych, na mocy których Administrator powierzał Podmiotowi przetwarzającemu przetwarzanie danych osobowych w związku z realizacją Umowy głównej, które w związku z powyższym wygasają.

Administrator danych Podmiot przetwarzający

Załącznik nr 1

do umowy powierzenia

**Ankieta - zakres informacji o zapewnieniu przez podmiot przetwarzający odpowiednich środków ochrony (technicznych i organizacyjnych), umożliwiających należyte zabezpieczenie danych osobowych, wymaganych art. 24 ust. 1 i 2 oraz art. 32 RODO**

□ został wyznaczony inspektor ochrony danych osobowych, nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych, należy podać dane kontaktowe (imię i nazwisko, numer telefonu oraz adres poczty elektronicznej):

□ do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie w przedmiotowym zakresie,

□ prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,

□ została opracowana i wdrożona dokumentacja w zakresie ochrony danych osobowych, spełniająca wymagania określone dla środków organizacyjnych, o których mowa w art. 24 ust. 2 RODO; należy ją wyszczególnić poniżej:

1. Polityka ochrony danych osobowych,

2. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,

3. Metodyka szacowania ryzyka naruszenia praw lub wolności osób fizycznych w PSP,

4. Wytyczne zabezpieczeń dla systemów informatycznych,

5. Wytyczne Komendanta Głównego PSP w sprawie organizacji ochrony danych osobowych w jednostkach organizacyjnych PSP.

|  |  |  |
| --- | --- | --- |
| **Środki ochrony fizycznej danych** | | |
| W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do fizycznego zabezpieczenia przetwarzanych danych osobowych. | | |
| 1 | □ | Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi). |
| 2 | □ | Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej >= 30 min. |
| 3 | □ | Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C. |
| 4 | □ | Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej. |
| 5 | □ | Pomieszczenia, w których przetwarzany jest zbiór danych osobowych, wyposażone są w system alarmowy przeciwwłamaniowy. |
| 6 | □ | Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, objęte są systemem kontroli dostępu. |
| 7 | □ | Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych. |
| 8 | □ | Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony. |
| 9 | □ | Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych, przez całą dobę jest nadzorowany przez służbę ochrony. |
| 10 | □ | Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie. |
| 11 | □ | Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej metalowej szafie. |
| 12 | □ | Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętym sejfie lub kasie pancernej. |
| 13 | □ | Kopie zapasowe / archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie. |
| 14 | □ | Kopie zapasowe / archiwalne zbioru danych osobowych przechowywane są w zamkniętej metalowej szafie. |
| 15 | □ | Kopie zapasowe / archiwalne zbioru danych osobowych przechowywane są w zamkniętym sejfie lub kasie pancernej. |
| 16 | □ | Zbiór danych osobowych przetwarzany jest w kancelarii tajnej, prowadzonej zgodnie z wymogami określonymi w odrębnych przepisach. |
| 17 | □ | Pomieszczenie, w którym przetwarzany jest zbiór danych osobowych, zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i / lub wolnostojącej gaśnicy. |
| 18 | □ | Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów. |
| **Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej** | | |
| W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do:   * technicznych środków zabezpieczenia komputerów przed skutkami awarii zasilania, * opisu infrastruktury sieci informatycznej, w której użytkowane są komputery wykorzystywane do przetwarzania danych osobowych, * sprzętowych i programowych środków ochrony przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji, * sprzętowych i programowych środków ochrony poufności danych przesyłanych drogą elektroniczną (środków ochrony transmisji), * sprzętowych i programowych środków ochrony przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych. | | |
| 1 | □ | Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego. |
| 2 | □ | Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową. |
| 3 | □ | Zastosowano urządzenia typu UPS, generator prądu i / lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania. |
| 4 | □ | Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej / komputerze przenośnym, zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS. |
| 5 | □ | Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. |
| 6 | □ | Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena. |
| 7 | □ | Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej. |
| 8 | □ | Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych. |
| 9 | □ | Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł. |
| 10 | □ | Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych. |
| 11 | □ | Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji. |
| 12 | □ | Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia. |
| 13 | □ | Zastosowano procedurę oddzwonienia (*callback*) przy transmisji realizowanej za pośrednictwem modemu. |
| 14 | □ | Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej. |
| 15 | □ | Zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity. |
| 16 | □ | Użyto system Firewall do ochrony dostępu do sieci komputerowej. |
| 17 | □ | Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej. |
| **Środki ochrony w ramach narzędzi programowych i baz danych** | | |
| W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do technicznych i programowych środków bezpieczeństwa zastosowanych w procedurach, aplikacjach i programach oraz innych narzędziach programowych wykorzystywanych do przetwarzania danych osobowych. | | |
| 1 | □ | Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych. |
| 2 | □ | Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych. |
| 3 | □ | Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. |
| 4 | □ | Dostęp do zbioru danych osobowych wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN lub tokena. |
| 5 | □ | Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem technologii biometrycznej. |
| 6 | □ | Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego. |
| 7 | □ | Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych. |
| 8 | □ | Zastosowano kryptograficzne środki ochrony danych osobowych. |
| 9 | □ | Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe. |
| 10 | □ | Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika. |
| **Środki organizacyjne** | | |
| W tej grupie środków należy zaznaczyć te pozycje, które odnoszą się do innych środków organizacyjnych zastosowanych przez administratora w celu ochrony danych, takich jak: instrukcje, szkolenia, zobowiązania. | | |
| 1 | □ | Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych. |
| 2 | □ | Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego. |
| 3 | □ | Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy. |
| 4 | □ | Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane. |
| 5 | □ | Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco. |

Jeżeli zastosowane zostały dodatkowo inne środki nie wymienione w udostępnionych listach, należy je wyszczególnić poniżej: ……………………………………………………………………………………………………………  
……………………………………………………………………………………………………………  
………………………………………………………………………………………………………

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu realizacji zadań wynikających z Umowy głównej.

.................................................

**data, imię, nazwisko, podpis  
osoby/osób uprawnionych**

Załącznik nr 2.

do umowy powierzenia przetwarzania

**Zgłoszenie naruszenia ochrony danych osobowych**

**Zgłoszenia naruszenia danych osobowych należy dokonać na adres administratora danych osobowych:**

Nazwa administratora: **Wielkopolski Komendant Wojewódzki PSP**

Adres e-mail: **kancelaria@psp.wlkp.pl** telefon: **47 771 60 00**

Fax: **61 222 05 00** E-puap: **/KWPSPPOZNAN/skrytka**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Typ zgłoszenia** | | | | | | | | | | | | | | | | | | | | | | | |
| Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie. | | | | | | | | | | | | | | | | | | | | | | | |
| Podaj swoją sygnaturę sprawy (opcjonalnie) (np. sygnatura w Twoim wewnętrznym rejestrze naruszeń) | | | | | | | | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | |
|  | | | | | | | |  | | | | | | | | | | | |  | | | |
|  | | | | | | | | Podaj przybliżoną datę uzupełnienia zgłoszenia (opcjonalnie)  Kliknij tutaj, aby wprowadzić datę. | | | | | | | | | | | | Podaj datę poprzedniego zgłoszenia  (opcjonalnie)  Kliknij tutaj, aby wprowadzić datę.  Podaj sygnaturę sprawy UODO  Kliknij tutaj, aby wprowadzić datę. | | | |
| 1. **Podmiot zgłaszający** | | | | | | | | | | | | | | | | | | | | | | | |
| **2A. Dane administratora danych** | | | | | | | | | | | | | | | | | | | | | | | |
| Pełna nazwa administratora | | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | | | | | | | |
| REGON (opcjonalnie) | | | | | | Podaj numer. | | | | | | | | NIP  (opcjonalnie) | | | Podaj numer. | | | KRS  (opcjonalnie) | | Podaj numer. | |
| Sektor (opcjonalnie) | | | | | | Dla sektora publicznego:  Wpisz nazwę sektora | | | | | | | | | | Dla sektora prywatnego:  Wpisz nazwę sektora | | | | | | | |
| **2B. Adres siedziby administratora danych** | | | | | | | | | | | | | | | | | | | | | | | |
| Ulica | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | Numer domu | | | | | Podaj numer | | Numer lokalu | Podaj numer |
| Miejscowość | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | Kod pocztowy | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | |
| Gmina | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | Powiat | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | |
| Województwo | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | Państwo | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | |
| **2C. Osoby uprawnione do reprezentowania administratora** | | | | | | | | | | | | | | | | | | | | | | | |
|  | Imię i nazwisko | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | | Stanowisko | | | | Kliknij tutaj, aby wprowadzić tekst. | | | |
|  | Imię i nazwisko | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | | Stanowisko | | | | Kliknij tutaj, aby wprowadzić tekst. | | | |
|  | Imię i nazwisko | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | | Stanowisko | | | | Kliknij tutaj, aby wprowadzić tekst. | | | |
|  | Imię i nazwisko | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | | Stanowisko | | | | Kliknij tutaj, aby wprowadzić tekst. | | | |
|  | Imię i nazwisko | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | | Stanowisko | | | | Kliknij tutaj, aby wprowadzić tekst. | | | |
| **2D. Pełnomocnik** | | | | | | | | | | | | | | | | | | | | | | | |
| ☐ Wniosek wypełniany przez pełnomocnika(opcjonalnie)  Jeśli zgłoszenie przesyłane jest w formie elektronicznej, należy załączyć pełnomocnictwo **udzielone w formie elektronicznej** (zgodnie z art. 33a KPA) oraz dowód uiszczenia opłaty skarbowej | | | | | | | | | | | | | | | | | | | | | | | |
| **2E. Inspektor ochrony danych** | | | | | | | | | | | | | | | | | | | | | | | |
| Imię i nazwisko | | | imię i nazwisko. | | | | | | Numer telefonu | | | | | Numer telefonu. | | | | | | | Adres e-mail | E-mail. | |
| **☐** Inspektor nie został wyznaczony | | | | | | | | | | | | | | | | | | | | | | | |
| Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.  Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | | | | | | | | | | | | | |
| **2F. 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 (np. podmiot przetwarzający, współadministratora, operator pocztowy itp.) | | | | | | | | | | | | | | | | | | | | | | | |
| 1. | | Nazwa i dane kontaktowe | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | Rola | Kliknij tutaj, aby wprowadzić tekst. | | | | |
| 2. | | Nazwa i dane kontaktowe | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | Rola | Kliknij tutaj, aby wprowadzić tekst. | | | | |
| 3. | | Nazwa i dane kontaktowe | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | Rola | Kliknij tutaj, aby wprowadzić tekst. | | | | |
| 4. | | Nazwa i dane kontaktowe | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | Rola | Kliknij tutaj, aby wprowadzić tekst. | | | | |
| 1. **Czas naruszenia** | | | | | | | | | | | | | | | | | | | | | | | |
| **3A. Wykrycie naruszenia i powiadomienie organu nadzorczego** | | | | | | | | | | | | | | | | | | | | | | | |
| Data stwierdzenia naruszenia Wskaż kiedy dowiedziałeś/aś się o naruszeniu. Jeśli nie znasz dokładnego terminu, podaj czas przybliżony. | | | | | | | | | | Kliknij tutaj, aby wprowadzić datę. | | | | | | | | | | | | | |
| Sposób stwierdzenia naruszenia Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa  Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | | | | | | | | | | | | | |
| Data powiadomienia przez podmiot przetwarzający (opcjonalnie)  Jeśli nie znasz dokładnego terminu, podaj czas przybliżony. | | | | | | | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | | |
| Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h  Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | | | | | | | | | | | | | |
| **3B. Czas naruszenia** | | | | | | | | | | | | | | | | | | | | | | | |
| Data i czas zaistnienia/rozpoczęcia naruszenia Jeśli nie znasz dokładnego terminu, podaj czas przybliżony. | | | | | | | | | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | |
| Data i czas zakończenia naruszenia (opcjonalnie) Jeśli nie znasz dokładnego terminu, podaj czas przybliżony. | | | | | | | | | | | | | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | |

|  |  |
| --- | --- |
| 1. **Charakter naruszenia** | |
| **4A. Opisz szczegółowo na czym polegało naruszenie** | |
| Kliknij tutaj, aby wprowadzić tekst. | |
| **4B. Na czym polegało naruszenie?** | |
| **☐** Zgubienie lub kradzież nośnika/urządzenia  **☐** Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji  **☐** Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy  **☐** Nieuprawnione uzyskanie dostępu do informacji  **☐** Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń  **☐** Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych  **☐** Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing) | **☐** Nieprawidłowa anonimizacja danych osobowych w dokumencie  **☐** Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora  **☐** Niezamierzona publikacja  **☐** Dane osobowe wysłane do niewłaściwego odbiorcy  **☐** Ujawnienie danych niewłaściwej osoby  **☐** Ustne ujawnienie danych osobowych |
| **4C. Przyczyna naruszenia** | |
| **☐** Wewnętrzne działanie niezamierzone  **☐** Wewnętrzne działanie zamierzone  **☐** Zewnętrzne działanie niezamierzone  **☐** Zewnętrzne działanie zamierzone | |
| **4D. Charakter** | |
| **☐** Naruszenie poufności danych  Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych  **☐** Naruszenie integralności danych  Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania  **☐** Naruszenie dostępności danych  Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną | |
| **4E. Dzieci** | |
| **☐** Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.  (opcjonalnie) | |

|  |  |
| --- | --- |
| 1. **Liczba osób i wpisów** | |
| Przybliżona liczba osób, których mogło dotyczyć naruszenie  Kliknij tutaj, aby wprowadzić tekst. | 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)  Kliknij tutaj, aby wprowadzić tekst. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Kategorie danych osobowych**   **UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.** | | | | | | |
| **6A. Dane podstawowe** | | | | | | |
| **☐** Nazwiska i imiona  **☐** Imiona rodziców  **☐** Data urodzenia  **☐** Numer rachunku bankowego  **☐** Adres zamieszkania lub pobytu  **☐** Numer ewidencyjny PESEL  **☐** Adres e-mail | | | | **☐** Nazwa użytkownika i/lub hasło  **☐** Dane dotyczące zarobków i/lub posiadanego majątku  **☐** Nazwisko rodowe matki  **☐** Seria i numer dowodu osobistego  **☐** Numer telefonu  **☐** Wizerunek  **☐** Inne, wskaż jakie:  Kliknij tutaj, aby wprowadzić tekst. | | |
| **6B. 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 | | |
| **6C. Dane, o których mowa w art. 10 RODO** | | | | | | |
| **☐** Dane dotyczące wyroków skazujących | | **☐** Dane dotyczące czynów zabronionych | | | **☐** Inne  Kliknij tutaj, aby wprowadzić tekst. | |
| 1. **Kategorie osób** | | | | | | |
| **☐** Pracownicy  **☐** Użytkownicy  **☐** Subskrybenci  **☐** Studenci  **☐** Uczniowie  **☐** Służby mundurowe (np. wojsko, policja) | | | **☐** Klienci (obecni i potencjalni)  **☐** Klienci podmiotów publicznych  **☐** Pacjenci  **☐** Dzieci  **☐** 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 **W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.** | | | Kliknij tutaj, aby wprowadzić tekst. | | | |
| 1. **Możliwe konsekwencje** | | | | | | |
| **8A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą** | | | | | | |
| **☐** Utrata kontroli nad własnymi danymi osobowymi  **☐** Ograniczenie możliwości realizowania praw z art. 15-22 RODO  **☐** Ograniczenie możliwości realizowania praw  **☐** Dyskryminacja  **☐** Kradzież lub sfałszowanie tożsamości | | | | **☐** Strata finansowa  **☐** Naruszenie dobrego imienia  **☐** Utrata poufności danych osobowych chronionych tajemnicą zawodową  **☐** Nieuprawnione odwrócenie pseudonimizacji  **☐** Inne  Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:  Kliknij tutaj, aby wprowadzić tekst. | | |
| **8B. Ryzyko naruszenia praw i wolności osób fizycznych** | | | | | | |
|  |  | | | | |  |
| 1. **Środki bezpieczeństwa i środki zaradcze** | | | | | | |
| **9A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych** | | | | | | |
| Kliknij tutaj, aby wprowadzić tekst. | | | | | | |
| **9B. Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowana ryzyka ponownego wystąpienia naruszenia** | | | | | | |
| Kliknij tutaj, aby wprowadzić tekst. | | | | | | |
| **9C. Środki zastosowane lub proponowane celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą** | | | | | | |
| Kliknij tutaj, aby wprowadzić tekst. | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **Zawiadamianie osób, których dane dotyczą** | | | | |
| Czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu? | | | | |
|  | Pamiętaj, że po zawiadomieniu osób, należy przesłać treść zawiadomienia do UODO. | |  |  |
| Czy indywidualnie? | | | Powód niezawiadomienia osób, których dane dotyczą: | Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić osoby, których dane dotyczą, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające. |
| Wskaż datę kiedy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu  Kliknij tutaj, aby wprowadzić datę. | | Wskaż datę kiedy zamierzasz zawiadomić osoby, których dane dotyczą, o naruszeniu  Kliknij tutaj, aby wprowadzić datę.  **☐** Nie znam jeszcze daty kiedy zamierzam powiadomić osoby, których dane dotyczą |
| Liczba zawiadomionych osób, których dane dotyczą  Kliknij tutaj, aby wprowadzić tekst. | |
| Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą  Kliknij tutaj, aby wprowadzić tekst. | | |
| Umieść zanonimizowaną treść zawiadomienia, którą przesłałeś bądź zamierzasz przesłać do osób, których dane dotyczą.  Pamiętaj, że zawiadomienie powinno:   * opisywać jasnym i prostym językiem charakter naruszenia ochrony danych osobowych, * zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji, * opisywać możliwe konsekwencje naruszenia ochrony danych osobowych, * opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.   Kliknij tutaj, aby wprowadzić tekst. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Przetwarzanie transgraniczne i inne powiadomienie** | | | |
| **☐** Naruszenie ma charakter transgraniczny  Zaznacz kraje Europejskiego Obszaru Gospodarczego, których dotyczy naruszenie: | | | |
| **☐** Austria  **☐** Cypr  **☐** Finlandia  **☐** Holandia  **☐** Litwa  **☐** Niemcy  **☐** Słowacja  **☐** Wielka Brytania | **☐** Belgia  **☐** Czechy  **☐** Francja  **☐** Irlandia  **☐** Luksemburg  **☐** Norwegia  **☐** Słowenia  **☐** Włochy | **☐** Bułgaria  **☐** Dania  **☐** Grecja  **☐** Islandia  **☐** Łotwa  **☐** Portugalia  **☐** Szwecja | **☐** Chorwacja  **☐** Estonia  **☐** Hiszpania  **☐** Liechtenstein  **☐** Malta  **☐** Rumunia  **☐** Węgry |
| **☐** Naruszenie zostało lub zostanie zgłoszone innemu organowi ochrony danych osobowych (opcjonalnie)  Wymień inne organy nadzorcze ochrony danych osobowych, którym naruszenie zostało lub zostanie zgłoszone  Kliknij tutaj, aby wprowadzić tekst. | | | |
| **☐** Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu z powodu innych zobowiązań prawnych (opcjonalnie)  Np. obowiązek zgłoszenia incydentu wynikający z ustawy o krajowym systemie cyberbezpieczeństwa. Wymień inne organy, którym naruszenie zostało lub zostanie zgłoszone z powodu innych zobowiązań prawnych.  Kliknij tutaj, aby wprowadzić tekst. | | | |

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

Data, miejscowość

(dla zgłoszenia w formie papierowej)

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

Podpis osoby lub osób upoważnionych   
do reprezentowania administratora[[1]](#footnote-1)

(dla zgłoszenia w formie papierowej)

Informacja:

**Administrator danych osobowych.**

Administratorem Państwa danych osobowych będzie Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stawki 2.

Można się z nami kontaktować w następujący sposób:

a) listownie: ul. Stawki 2, 00-193 Warszawa

b) przez elektroniczną skrzynkę podawczą dostępną na stronie https://www.uodo.gov.pl/pl/p/kontakt

c) telefonicznie: (22) 531 03 00

**Inspektor ochrony danych.**

Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych pod adresem email IOD@uodo.gov.pl

**Cele i podstawy przetwarzania.**

Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu w celu przyjmowania zgłoszeń o naruszeniu ochrony danych osobowych zgodnie z art. 33 ust 1 , 3 i 4 RODO, podejmowania działań określonych w art. 34 ust. 4 oraz art. 58 ust. 2 RODO1, a także prowadzenia przez organ wewnętrznego rejestru naruszeń na podstawie art. 57 ust. 1 lit. u RODO. Następnie Państwa dane będziemy przetwarzać w celu wypełnienia obowiązku archiwizacji dokumentów wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

**Odbiorcy danych osobowych.**

Odbiorcami Państwa danych osobowych będą Minister Cyfryzacji w związku z zamieszczeniem formularza na platformie E-PUAP bądź Minister Przedsiębiorczości i Technologii w związku z zamieszczeniem formularza na platformie biznes.gov.pl

**Okres przechowywania danych.**Będziemy przechowywać Państwa dane przez czas realizacji uprawnień Prezesa UODO wskazanych w art. 34 ust. 4 i art. 58 ust. 2 RODO, a następnie - zgodnie z obowiązującą w Urzędzie Prezesa UODO Instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów - przez okres 10 lat od końca roku, w którym zgłoszono naruszenie ochrony danych, lub - w przypadku skierowania wystąpienia lub wydania decyzji administracyjnej – wieczyście.

**Prawa osób, których dane dotyczą.**

Zgodnie z RODO przysługuje Państwu:

1. prawo dostępu do swoich danych oraz otrzymania ich kopii;
2. prawo do sprostowania (poprawiania) swoich danych;
3. prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
4. prawo do ograniczenia przetwarzania danych;
5. prawo do wniesienia skargi do Prezesa UODO (na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)

**Informacja o wymogu podania danych.**

Podanie przez Państwa danych osobowych w niniejszym formularzu jest obowiązkiem wynikającym z art. 33 ust. 3 RODO oraz z art. 63 § 2-3a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego.

1 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 (RODO) oraz podjętych działań.

1. Jeżeli zgłoszenie podpisuje pełnomocnik, należy pamiętać o załączeniu pełnomocnictwa [↑](#footnote-ref-1)