

## UMOWA

### POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu ..... r. pomiędzy:

.....

reprezentowaną przez:

.....

zwaną dalej „**Administratorem**”

a

.....

reprezentowaną przez:

.....

zwanym dalej „**Podmiotem przetwarzającym**”,

zaś wspólnie „**Stronami**”

W związku z zawarciem w dniu ..... r. Umowy .. zwanej dalej „Umową główną”, której przedmiotem są czynności związane z .....

Strony postanawiają, co następuje:

#### § 1

##### Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 *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* (zwane dalej „Rozporządzeniem”) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Administrator oświadcza, że jest Administratorem danych, które powierza Podmiotowi przetwarzającemu do przetwarzania.
3. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający w celu .....

K-GT-43-232-4/2022

Załącznik nr 3 do Umowy

4. 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.
5. Podmiot przetwarzający oświadcza, że stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.
6. Podmiot przetwarzający oświadcza, że przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

## § 2

### Zakres i cel przetwarzania danych

1. Dane osobowe dotyczą następujących kategorii osób: .....
2. Podmiot przetwarzający będzie przetwarzać, powierzone na podstawie Umowy głównej dane w następującym zakresie: .....
3. Administrator oświadcza, że charakter danych osobowych, powierzanych Umową główną, nie obejmuje szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 Rozporządzenia.
4. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji Umowy głównej z dnia ..... r.

## § 3

### Sposób wykonania umowy w zakresie przetwarzania danych osobowych

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.
2. Wdrażając środki organizacyjne i techniczne, o których mowa powyżej, Podmiot przetwarzający:

K-GT-43-232-4/2022

Załącznik nr 3 do Umowy

- 1) przestrzega wytycznych Administratora w zakresie sposobu zabezpieczenia procesów przetwarzania danych osobowych zgodnie z przepisami Rozporządzenia oraz innymi obowiązującymi przepisami prawa. Minimalne gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych wymaganych przez Administratora stanowi załącznik nr 1 do Umowy;
- 2) powinien uwzględnić stan wiedzy technicznej oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, których dane osobowe będzie przetwarzał na podstawie Umowy.
3. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
4. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, których dostęp jest niezbędny do wykonania usług określonych w Umowie głównej, w związku z którą przetwarzane są dane osobowe.
5. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy (o której mowa w art. 28 ust. 3 lit. b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji Umowy głównej, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
6. Podmiot przetwarzający biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia.
7. Podmiot przetwarzający uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32–36 Rozporządzenia.
8. Podmiot przetwarzający po zakończeniu realizacji Umowy głównej niezwłocznie, jednak nie później niż w ciągu 10 dni, zwraca powierzone dane Administratorowi oraz trwale usuwa wszelkie ich istniejące kopie.
9. Podmiot przetwarzający ma obowiązek powiadomić Administratora za pośrednictwem poczty elektronicznej, w przypadku stwierdzenia nieprawidłowości w terminie 48 godzin od wystąpienia zdarzenia o wszelkich incydentach dotyczących przetwarzania powierzonych danych osobowych,

K-GT-43-232-4/2022

Załącznik nr 3 do Umowy

w tym przypadkowego lub nieupoważnionego dostępu do powierzonych danych osobowych, przypadkach utraty, zmiany powierzonych danych.

**10.** Zgłoszenie, o którym mowa w ust. 9 musi co najmniej:

- 1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- 2) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- 3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
- 4) opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

**11.** Podmiot przetwarzający jest obowiązany do dokumentowania wszelkich okoliczności i zebrania wszelkich dowodów, które pomogą Administratorowi wyjaśnić szczegóły naruszenia, w tym jego charakter, skalę, skutki, czas zdarzenia, osoby odpowiedzialne oraz osoby poszkodowane.

**12.** Podmiot przetwarzający odpowiada za szkody, jakie powstaną u Administratora lub osób trzecich w wyniku niezgodnego z niniejszą Umową przetwarzania danych.

**13.** Odpowiedzialność, o której mowa w ust. 11 obejmuje rzeczywiste szkody za niewykonanie, bądź nienależyte wykonanie niniejszej Umowy, będące następstwem okoliczności, za które Podmiot przetwarzający ponosi odpowiedzialność.

**14.** W przypadku, gdy osoba trzecia skieruje przeciwko Administratorowi roszczenia oparte na zarzucie niezgodnego z niniejszą Umową lub przepisami przetwarzania danych osobowych przez Podmiot przetwarzający, Strony ustalają poniższe zasady postępowania:

- 1) Administrator zobowiązany jest niezwłocznie, nie później niż w terminie 3 dni roboczych od powzięcia wiedzy w tym przedmiocie – powiadomić Podmiot przetwarzający i wezwać go do udziału w wyjaśnieniu sprawy,
- 2) Podmiot przetwarzający będzie brał czynny udział w wyjaśnieniu sprawy, w celu naprawienia powstałej szkody lub polubownego załatwienia sprawy w drodze negocjacji,
- 3) w przypadku, gdy Strony wspólnie z osobą trzecią dojdą do porozumienia, że roszczenie osoby trzeciej jest uzasadnione i uzgodnią sposób zadośćuczynienia, Podmiot przetwarzający będzie

K-GT-43-232-4/2022

Załącznik nr 3 do Umowy

zobowiązany do pokrycia roszczeń osoby trzeciej, chyba że naruszenie powstało z winy Administratora, wtedy do pokrycia roszczeń zobowiązany będzie Administrator,

- 4) w razie braku porozumienia, o którym mowa w lit. c i wystąpieniem osoby trzeciej na drogę postępowania sądowego, Administrator niezwłocznie jednak nie później niż w terminie 7 dni od powzięcia takiej wiadomości powiadomi Podmiot przetwarzający,
- 5) po rozpoczęciu postępowania sądowego Podmiot przetwarzający będzie w nim uczestniczył jako interwenient uboczny, po stronie pozwanej bądź w miejsce strony pozwanej, udzieli wszelkiej pomocy w celu obrony przed roszczeniami osoby trzeciej, w szczególności w zakresie dostarczenia informacji i dokumentów, w których jest w posiadaniu a związanych z dochodzonym roszczeniem.
- 6) w przypadku zawarcia ugody, Podmiot przetwarzający zwolni Administratora z obowiązku naprawienia szkody w takim zakresie w jakim wynika to z ugody.

15. Administrator odpowiada za szkody, jakie powstaną u Podmiotu przetwarzającego lub osób trzecich w wyniku przetwarzania danych niezgodnego z niniejszą umową, postanowieniami Rozporządzenia lub innych ogólnie obowiązujących przepisów prawa, o ile wynikają one z winy Administratora.

#### **§ 4**

##### **Prawo kontroli**

1. Administrator zgodnie z art. 28 ust. 3 lit. h Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia niniejszej Umowy.
2. Administrator realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 3-dniowym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybienia stwierdzonych podczas kontroli w terminie wskazanym przez Administratora nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
5. Podmiot przetwarzający umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

K-GT-43-232-4/2022

Załącznik nr 3 do Umowy

6. Administrator ma prawo dokonywać regularnej oceny Podmiotu przetwarzającego, za pomocą formularza stanowiącego załącznik nr 2 do Umowy.
7. W związku z obowiązkiem określonym w ust. 4 Podmiot przetwarzający niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie Rozporządzenia lub innych przepisów powszechnie obowiązujących o ochronie danych.

## **§ 5**

### **Podpowierzenie**

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umowa do dalszego przetwarzania osobie trzeciej jedynie w celu wykonania umowy po uzyskaniu uprzedniej zgody Administratora.
2. Podmiot przetwarzający zapewnia, że będzie korzystał wyłącznie z usług takich dalszych podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz przepisów obowiązującego prawa z zakresu ochrony danych osobowych, a także zapewniało ochronę praw osób, których dane dotyczą.
3. Podwykonawca winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podwykonawca winien zapewniać wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom Rozporządzenia.
5. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

## **§ 6**

### **Czas obowiązywania umowy**

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas obowiązywania umowy głównej, o której mowa w § 2 ust. 4 oraz po zakończeniu realizacji tej umowy – do dnia realizacji § 3 ust. 7.
2. Wszelkie zmiany niniejszej Umowy i jej warunków mogą być dokonywane za zgodą obu Stron wyrażoną na piśmie pod rygorem nieważności.
3. Treść Umowy może być zmieniana m.in. w przypadku zmiany przepisów prawa i konieczności dostosowania treści Umowy do tych przepisów lub zmiany regulacji wewnętrznych dotyczących przetwarzania danych osobowych obowiązujących u Administratora.

## § 7

### **Rozwiązanie umowy**

1. Każda ze stron może rozwiązać niniejszą Umowę w trybie natychmiastowym w przypadku, gdy druga Strona rażąco naruszy postanowienia niniejszej Umowy lub Umowy głównej, a w szczególności zasad dotyczących ochrony powierzonych danych osobowych.
2. W przypadku rozwiązania Umowy Podmiot przetwarzający zobowiązany jest niezwłocznie, jednak nie później niż w terminie 7 dni, zwrócić Administratorowi dane osobowe powierzone do przetwarzania oraz dokonać trwałego zniszczenia wszelkich kopii zawierających powierzone dane osobowe. Zwrot zostanie potwierdzony protokołem przekazania danych podpisanym przez obie Strony.

## § 8

### **Zasady zachowania tajemnicy**

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych, o których mowa w ust. 1, nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy głównej, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy głównej.
3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych, o których mowa w ust. 1, gwarantowały zabezpieczenie danych w tym w szczególności danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

## § 9

### **Postanowienia końcowe**

1. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego, Rozporządzenia oraz inne przepisy prawa powszechnie obowiązującego.



K-GT-43-232-4/2022

Załącznik nr 3 do Umowy

2. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy dla siedziby Podmiotu przetwarzającego.
3. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednej dla każdej ze Stron.

**ADMINISTRATOR**

**PODMIOT PRZETWARZAJĄCY**

---

---



| <b>WERYFIKACJA/ANALIZA<br/>ŚRODKÓW ZABEZPIECZEŃ ORGANIZACYJNYCH I TECHNICZNYCH ZASTOSOWANYCH PRZEZ<br/>PODMIOT PRZETWARZAJĄCY</b> |   |                                      |
|---|---|--------------------------------------|
| <b>ADMINISTRATOR DANYCH</b>   |   |                                      |
| <b>PODMIOT PRZETWARZAJĄCY</b>   |   |                                      |
| <b>Grupa zabezpieczeń</b>   | <b>Opis zabezpieczeń</b>  | <b>Uzupełnia<br/>Przetwarzający:</b> |
| Środki organizacyjne  | 1. Zapewniono kontrolę nad dostępem do Danych osobowych, w szczególności poprzez:   |                                      |
|   | 1) wyznaczenie osób upoważnionych do przetwarzania danych osobowych na polecenie Administratora i wydanie imiennych upoważnień do przetwarzania danych osobowych, |                                      |
|   | 2) zapewnienie, że osoby posiadające upoważnienia, o których mowa w pkt 1 zobowiązały się do zachowania tajemnicy.  |                                      |
|   | 2. Zapewniono szkolenia z zakresu bezpieczeństwa przetwarzania danych osobowych dla osób biorących udział w procesie przetwarzania.                               |                                      |
|   | 3. Przyjęto i wdrożono polityki ochrony danych, w tym polityki bezpieczeństwa danych w systemach informatycznych.   |                                      |
|   | 4. Prowadzony jest rejestr kategorii czynności przetwarzania danych.  |                                      |
|   | 5. Przyjęto i wdrożono procedurę związaną z reagowaniem na naruszenia ochrony danych, w tym prowadzony jest rejestr naruszeń ochrony danych osobowych.            |                                      |
| 6. Prowadzona jest analiza ryzyka w zakresie przetwarzania danych osobowych.  |   |                                      |
| Środki ochrony fizycznej i  | 1. Zapewniono kontrolę dostępu fizycznego do budynku oraz pomieszczeń, w których przetwarzane są dane osobowe.  |                                      |

K-GT-43-232-4/2022

Załącznik nr 3 do Umowy

|   |   |  |
|---|---|--|
| środowiskowej stosowane w celu zabezpieczenia budynków oraz pomieszczeń, w których przetwarzane są dane osobowe | 2. Zabezpieczono miejsca przetwarzania danych osobowych od zdarzeń losowych (np. pożar, zalanie).   |  |
|   | 3. Zapewniono ochronę danych osobowych przed dostępem osób postronnych, uszkodzeniem lub zniszczeniem przez nie.  |  |
|   | 4. Przyjęto i wdrożono procedurę niszczenia danych.   |  |
| Zabezpieczenia techniczne i systemów teleinformatycznych  | 1. Zapewniono bezpieczeństwo danych osobowych, w tym poufność danych poprzez:   |  |
|   | 1) stosowanie unikalnych identyfikatorów użytkowników,  |  |
|   | 2) stosowanie złożonych haseł dostępowych użytkowników (co najmniej 8 znaków, w tym przynajmniej 1 wielka litera, 1 mała litera, 1 cyfra lub znak specjalny),   |  |
|   | 3) stosowanie wymuszonej okresowej zmiany haseł użytkowników (nie rzadziej niż co 30 dni),  |  |
|   | 4) legalne i aktualne oprogramowanie, wspierane przez producenta, w tym oprogramowanie antywirusowe lub inne oprogramowanie identyfikujące podejrzane aktywności w systemach, na stacjach roboczych oraz serwerach mailowych, w szczególności filtrowanie poczty: antyspam, antywirus i anti-malware. |  |
|   | 5) kontrola i nadzór ruchu w sieci wewnętrznej, tj. monitoring aktywności użytkowników, blokowanie zewnętrznych nośników.   |  |
|   | 6) kontrolę oraz monitorowanie styku sieci wewnętrznej z siecią Internet (zapory ogniowe, proxy),   |  |

K-GT-43-232-4/2022

Załącznik nr 3 do Umowy

|                       |   |  |
|-----------------------|---|--|
|                       | 7) środki kryptograficznej ochrony na poziomie transmisji danych przesyłanych z wykorzystaniem sieci Internet, tj. szyfrowanie informacji zawierających Dane osobowe wysyłanych lub udostępnianych elektronicznymi kanałami wymiany informacji, |  |
|                       | 8) przetwarzanie informacji zawierających dane osobowe na zabezpieczonych nośnikach w postaci szyfrowanych dysków urządzeń mobilnych, w tym przenośnych pamięci masowych,   |  |
|                       | 10) mechanizmy identyfikacji i uwierzytelniania użytkowników (co najmniej identyfikator i hasło) w przypadku udostępniania aplikacji dostępnych przez sieć Internet.  |  |
|                       | 2. Zapewniono bezpieczeństwo danych osobowych, w tym ich dostępność i odporność systemów poprzez:   |  |
|                       | 1) sformalizowane zasady zgłaszania incydentów związanych z bezpieczeństwem systemów,   |  |
|                       | 2) systemy wykonywania i przechowywania kopii zapasowych,   |  |
|                       | 3) systemy podtrzymania napięcia (UPS),   |  |
|                       | 4) ograniczanie pojedynczych punktów awarii lub minimalizowanie ryzyka związanego z wystąpieniem awarii,  |  |
|                       | 3. Zapewniono bezpieczeństwo danych osobowych, w tym ich integralność i realizację zasady rozliczalności poprzez:   |  |
|                       | 1) logowanie działalności użytkowników (repozytorium z logami),   |  |
|                       | 2) logowanie wykonanych zmian na danych osobowych przez użytkowników,   |  |
| <b>WYMAGANIA RODO</b> | Czy podmiot przetwarzający spełnia wymagania RODO z art. 24 RODO?   |  |

K-GT-43-232-4/2022

Załącznik nr 3 do Umowy

|  |   |  |
|--|---|--|
|  | Czy podmiot przetwarzający spełnia wymagania RODO z art. 32 RODO? |  |
|  | Czy podmiot przetwarzający spełnia wymagania RODO z art. 27 RODO? |  |

**PODPIS OSOBY REPREZENTUJĄCEJ PROCESORA**

---

***MINIMALNE GWARANCJE WDROŻENIA ODPOWIEDNICH ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH PRZEZ ZLECENIOBIORCĘ***

1. Obszar, w którym przetwarzane są dane osobowe, należy zabezpieczyć przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. W przypadku realizacji usług poza wskazanym obszarem z wykorzystaniem urządzeń przenośnych, należy zabezpieczać je, stosując środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.
2. System informacyjny należy chronić przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, obejmującym przykładowo:
  - 1) kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną,
  - 2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
3. System powinien zostać wyposażony w mechanizm filtrowania połączeń wchodzących i wychodzących (firewall – zaporę sieciową).

K-GT-43-232-4/2022

Załącznik nr 3 do Umowy

4. System informatyczny musi zostać wyposażony w mechanizmy ochrony antywirusowej. Wszystkie pliki muszą być testowane oprogramowaniem antywirusowym.
5. Każdy komputer powinien mieć założone zabezpieczenie uniemożliwiające osobom nieupoważnionym zmianę konfiguracji komputera.
6. Załączniki do poczty elektronicznej nie powinny być otwierane, jeśli zachodzi podejrzenie, że zostały wysłane z niezauważanego źródła.
7. Należy stosować środki ochrony kryptograficznej wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.
8. W systemie informatycznym służącym do przetwarzania danych osobowych muszą istnieć odpowiednie mechanizmy kontroli dostępu do danych. Należy wziąć pod uwagę stosowanie: tworzenie i usuwanie kont, ich czasowe lub trwałe blokowanie, nadawanie haseł i ich zmianę oraz nadawanie i wycofywanie uprawnień, raportowanie wszystkich istotnych operacji związanych z zarządzaniem uprawnieniami, generowane z perspektywy czasu, konta, roli lub operacji.
9. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas należy zapewnić, aby:
  - 1) w systemie rejestrowany był dla każdego użytkownika odrębny identyfikator,
  - 2) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
10. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
11. W przypadku, gdy do uwierzytelnienia użytkowników używa się hasła, zaleca się jego cykliczną zmianę.
12. Systemy informatyczne muszą być zabezpieczone w szczególności przed:
  - 1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
  - 2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
13. Dane osobowe przetwarzane w systemie informatycznym muszą być zabezpieczane przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
14. Kopie zapasowe:

K-GT-43-232-4/2022

Załącznik nr 3 do Umowy

- 1) należy przechowywać w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem,
  - 2) muszą być usuwane niezwłocznie po ustaniu ich użyteczności.
15. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
- 1) likwidacji – pozbawia się wcześniej zapisu danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
  - 2) przekazanie innemu podmiotowi – pozbawia się wcześniej zapisu danych, w sposób uniemożliwiający ich odzyskanie,
  - 3) naprawy – pozbawia się wcześniej zapisu danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej.
16. Przetwarzający zobowiązany jest do monitorowania wdrożonych środków zabezpieczenia systemu informatycznego.
17. Przetwarzający posiada wiedzę z zakresu przepisów regulujących przetwarzanie danych osobowych i jest zobowiązany do uzupełniania swojej wiedzy z tego zakresu w przypadku zmian w przepisach.
18. Przetwarzający ma obowiązek zapoznania swoich pracowników, którzy mają być uprawnieni do przetwarzania danych osobowych, z przepisami dotyczącymi danych osobowych i odpowiedzialnością za ochronę tych danych.
19. Należy prowadzić dokumentację ustalającą zasady ochrony danych osobowych.

**Administrator**

**Przetwarzający**

.....

.....