

POLITYKA OCHRONY DANYCH OOBOWYCH

KLEIWO Biuro Rachunkowe Iwona Klemczak

NIP: 6991837942

Gołaszyn 65B/1, 63-940 Bojanowo

e-mail: kleiwo.biurorachunkowe@gmail.com

Nr telefonu: 661 843 142



Spis treści

I WPROWADZENIE	2
II REJESTRY	2
III NARUSZENIA OCHRONY DANYCH OSOBOWYCH	2
IV OBOWIĄZKI INFORMACYJNE	2
V UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH	3
VI UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH	3
VII WSPÓŁADMINISTROWANIE	Błąd! Nie zdefiniowano zakładki.
VIII ANALIZA RYZYKA	3
IX OCENY SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH	4
X ŚRODKI OCHRONY DANYCH OSOBOWYCH	4
XI INSPEKTOR OCHRONY DANYCH	4
XII MONITORING	4
XIV ZAŁĄCZNIKI	34

I WPROWADZENIE

- Niniejsza Polityka Ochrony Danych wraz z załącznikami stanowi obowiązującą w Podmiocie dokumentację w zakresie wdrażania, przestrzegania i weryfikacji zasad ochrony danych osobowych.
- Każda osoba odpowiedzialna za wdrażanie, utrzymanie lub monitorowanie zasad przetwarzania danych osobowych w Podmiocie, w szczególności przedstawiciele najwyższego kierownictwa oraz ewentualny Inspektor Ochrony Danych, mają obowiązek zapoznania się z niniejszą Polityką Ochrony Danych, obowiązek jej przestrzegania oraz egzekwowania stosowania w Podmiocie.
- Polityka Ochrony Danych wraz z załącznikami wchodzi w życie z dniem jej podpisania przez osoby uprawnione do reprezentacji Podmiotu.
- W przedmiocie spraw nieuregulowanych Polityką Ochrony Danych, zastosowanie znajdują przepisy prawa powszechnie obowiązującego.

II REJESTRY

Podmiot **prowadzi** niżej wymienione rejestry:

- Rejestr czynności przetwarzania danych osobowych – stanowiący ewidencję wykonywanych przez Podmiot czynności na danych osobowych, rozumianych jako zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane.
- Rejestr kategorii czynności przetwarzania danych osobowych – stanowiący ewidencję powierzonych Podmiotowi usług, realizowanych na zlecenie administratora związanej ze zleconymi czynnościami przetwarzania.
- Rejestr naruszeń ochrony danych osobowych – stanowiący ewidencję stwierdzonych w Podmiocie naruszeń ochrony przetwarzanych danych osobowych,
- Rejestr środków ochrony danych osobowych,
- Rejestr odbiorców danych osobowych,
- Rejestr osób upoważnionych do przetwarzania danych osobowych,

Podmiot przechowuje wymienione dokumenty: w załączeniu do niniejszej Polityki Ochrony Danych.

III NARUSZENIA OCHRONY DANYCH OSOBOWYCH

- **Podmiot wdraża procedurę naruszeniową**, znajdującą się w załączniku.
- Procedura obowiązuje wszystkie osoby pracujące lub świadczące usługi w Podmiocie.
- Procedura obowiązuje w przypadku stwierdzenia naruszenia ochrony danych osobowych lub naruszenia praw lub wolności osób, których dane osobowe są przetwarzane.

Podmiot przechowuje wymienione dokumenty: w załączeniu do niniejszej Polityki Ochrony Danych.

IV OBOWIĄZKI INFORMACYJNE

- Podmiot **wdraża stosowanie obowiązków informacyjnych**, wymienionych w załączniku.
- Zabrania się przetwarzania danych osobowych bez udzielenia obowiązku informacyjnego, chyba że indywidualnie stwierdzono podstawy wyłączenia tego obowiązku w danym przypadku.
- Przechowywanie wzorów: w załączeniu do niniejszej Polityki Ochrony Danych.
- Przechowywanie udzielonych obowiązków informacyjnych: wraz z dokumentacją właściwą (np. w załączeniu do umowy).

Podmiot przechowuje:

- szablony obowiązków informacyjnych w załączeniu do niniejszej Polityki Ochrony Danych,
- udzielone obowiązki informacyjne wraz z dokumentacją właściwą (np. w załączeniu do umowy).

V UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

- Podmiot **wdraża stosowanie upoważnień do przetwarzania danych osobowych**, znajdujących się w załączniku.
- Zabrania się przetwarzania danych osobowych przez osoby do tego nieupoważnione.
- Upoważnienia stosuje się względem pracowników.
- Upoważnienia można stosować względem osób fizycznych trzecich, świadczących na rzecz Podmiotu usługi z użyciem narzędzi Podmiotu (np. informatyk na umowie zlecenie), jednakże decyzję w tym zakresie należy podejmować indywidualnie.

Podmiot przechowuje:

- szablony upoważnień w załączeniu do niniejszej Polityki Ochrony Danych,
- udzielone upoważnienia w części B akt osobowych, a w przypadku osób niebędących pracownikami, w załączeniu do właściwych umów o współpracy,
- ewidencję upoważnień w rejestrze osób upoważnionych do przetwarzania danych osobowych.

VI UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

- Podmiot **wdraża stosowanie wzorców umów powierzenia przetwarzania danych osobowych** znajdujących się w załączniku.
 - Wzorzec dla administratora stosuje się w przypadku powierzenia przetwarzania danych osobowych zewnętrznym podmiotom przetwarzającym.
 - Wzorzec dla podmiotu przetwarzającego stosuje się w przypadku, gdy Podmiot wykonuje czynności przetwarzania danych osobowych, powierzone przez ich zewnętrznych administratorów.
- Dopuszcza się stosowanie wzorców umów dostarczonych przez kontrahentów, pod warunkiem ich udokumentowanej akceptacji przez najwyższe kierownictwo lub osobę przez nie wyznaczoną.
- Zabrania się powierzenia przetwarzania danych osobowych bez odpowiedniej umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego, zgodnego z art. 28 RODO.
- Zawarcie umowy powierzenia przetwarzania danych osobowych należy poprzedzić badaniem podmiotu przetwarzającego na podstawie **ankiety dla podmiotu przetwarzającego**.
- Umów powierzenia nie stosuje się względem pracowników.

Podmiot przechowuje szablony umów powierzenia i zawarte umowy powierzenia, a także uzupełnione ankiety dla podmiotu przetwarzającego, w załączeniu do niniejszej Polityki Ochrony Danych.

VIII ANALIZA RYZYKA

- **Podmiot wdraża zasadę analizowania ryzyka** naruszenia praw lub wolności osób, których dane osobowe podlegają przetwarzaniu.
- Szacowanie ryzyka odbywać się będzie na warunkach ustanowionych w załączniku.
- Zabrania się wdrażania nowych czynności przetwarzania danych osobowych, wdrażania nowych zasobów służących do ich przetwarzania, a także zmian środków ochrony danych osobowych, bez uprzedniego wykonania analizy ryzyka lub jej aktualizacji.

- Podmiot zobowiązuje się do aktualizacji analizy ryzyka, znajdującej się w załączniku.

Podmiot przechowuje dokumentację szacowania ryzyka w załączeniu do niniejszej Polityki Ochrony Danych.

IX OCENY SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH

- Podmiot wdraża zasadę, aby **monitorować czynności przetwarzania danych osobowych, w celu stwierdzenia, czy wymagają one wykonania OSOD-u** (oceny skutków dla ochrony danych osobowych).
- W przypadku gdy dana czynność wymaga przeprowadzenia OSOD-u, stosuje się szablon znajdujący się w załączniku.
- Zabrania się wdrażania nowych czynności przetwarzania danych osobowych bez uprzedniego wykonania analizy ryzyka lub jej aktualizacji, a w przypadku gdy potwierdzi ona takową zasadność, bez przeprowadzenia OSOD-u.

Podmiot przechowuje szablon oceny skutków dla ochrony danych osobowych oraz dokumentację wykonanych ocen w załączeniu do niniejszej Polityki Ochrony Danych.

X ŚRODKI OCHRONY DANYCH OSOBOWYCH

Uwzględniając zalecenia z przeprowadzonej analizy ryzyka oraz wymogi ustanowione w art. 32 RODO:

- **Podmiot wdraża środki ochrony danych osobowych** wymienione w załączniku – Rejestrze środków ochrony danych. Zabrania się wdrażania zmian środków ochrony danych osobowych, bez ich zewidencjonowania. Ponadto zobowiązuje się do ich aktualizacji.
- **Podmiot wdraża procedury** (organizacyjne środki ochrony danych osobowych), wymienione w załączniku – Procedury. Zabrania się wdrażania zmian wdrożonych procedur, bez ich uchwalenia zgodnie z zasadami reprezentacji. Ponadto zobowiązuje się do ich aktualizacji.

Podmiot przechowuje wymienioną dokumentację w załączeniu do niniejszej Polityki Ochrony Danych.

XI INSPEKTOR OCHRONY DANYCH

Podmiot nie powołał Inspektora Ochrony Danych z powodu braku spełniania kryteriów określonych w art. 37 ust. 1 RODO, tj:

- Podmiot nie jest podmiotem publicznym,
- główna działalność Podmiotu nie polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,
- główna działalność Podmiotu nie polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.

XII MONITORING

Podmiot nie stosuje żadnych form monitoringu.

Z komentarzem [WW1]: Należy pozostawić, w przypadku gdy Podmiot nie stosuje żadnych form monitoringu. Wówczas drugi akapit należy usunąć.

PROCEDURA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

I. WSTĘP

Ustanawia się poniższą procedurę postępowania z naruszeniami ochrony danych osobowych w Podmiocie.

Celem procedury jest ustalenie jednolitych zasad postępowania w przypadku, gdy:

1. stwierdzono naruszenie lub istnieje podejrzenie naruszenia zasad ochrony danych osobowych przetwarzanych w Podmiocie,
2. stan urządzenia, zawartość baz danych osobowych, ujawnione metody pracy, sposób działania programu lub obniżona jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zasad ochrony danych osobowych.

II. DOKUMENTY POWIĄZANE

- *Procedura postępowania z naruszeniami ochrony danych osobowych*
- *Rejestr naruszeń ochrony danych osobowych*
- *Polityka Ochrony Danych Osobowych*

III. NARUSZENIE OCHRONY DANYCH OSOBOWYCH

1. Naruszenie ochrony danych osobowych może być skutkiem:
 - a) szkodliwego wpływu środowiska na system przetwarzania danych osobowych,
 - b) zewnętrznych zdarzeń losowych,
 - c) zamierzonych lub niezamierzonych czynności osób upoważnionych do przetwarzania danych osobowych,
 - d) nieuprawnionych działań osób nieupoważnionych do przetwarzania danych osobowych.
2. Naruszeniem ochrony danych osobowych jest każdy stwierdzony fakt naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem:
 - a) zniszczenia,
 - b) utracenia,
 - c) zmodyfikowania,
 - d) nieuprawnionego ujawnienia,
 - e) nieuprawnionego dostępu do danych osobowych, przesyłanych, przechowywanych lub w inny sposób przetwarzanych,
 - f) a także naruszenia praw lub wolności osób, których dane osobowe są przetwarzane.

IV. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. **Obowiązki osoby upoważnionej do przetwarzania danych osobowych, identyfikującej naruszenie:**

W przypadku podejrzenia naruszenia ochrony danych osobowych, każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana niezwłocznie:

- a. poinformować o tym fakcie IOD albo Administratora poprzez wysłanie wiadomości e-mail pod adres: kleiwo.iwonaklemczak@gmail.com
- b. określić sytuację i czas, w jakim zauważono naruszenie,
- c. podać wszelkie istotne informacje, mogące pomóc w ustaleniu przyczyny naruszenia,
- d. do czasu otrzymania informacji zwrotnej, powstrzymać się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
- e. w miarę możliwości zabezpieczyć elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych,
- f. wówczas należy oczekiwać udokumentowanej informacji zwrotnej od osoby poinformowanej.

Osoby upoważnione do przetwarzania danych osobowych, zobowiązane są przestrzegać tych zasad w przypadku stwierdzenia naruszenia zasad ochrony danych osobowych.

2. Obowiązki IOD/Administratora:

- a. zapoznanie się z sytuacją wystąpienia naruszenia i wybór dalszego postępowania uwzględniającego zagrożenie związane z przerwaniem ciągłości i prawidłowości pracy,
- b. przeprowadzenie dokładnego wywiadu z zaistniałego naruszenia z osobą powiadamiającą, jak również z każdą inną osobą, która może posiadać informacje w związku z zaistniałym naruszeniem,
- c. jeżeli zachodzi taka potrzeba skorzystanie ze wsparcia zewnętrznych specjalistów,
- d. dokumentowanie zaistniałego przypadku naruszenia ochrony danych osobowych poprzez prowadzenie *Rejestru naruszeń ochrony danych osobowych*,
- e. IOD/Administrator po zasięgnięciu potrzebnych opinii wdraża działania naprawcze oraz zaradcze, tak aby zminimalizować wystąpienie naruszeń w przyszłości.

3. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu:

- a. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki, w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych (PUODO), chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
- b. Zgłoszenie, o którym mowa powyżej, dokonuje się za pomocą formularza zgłoszenia naruszenia do UODO, dostępnego na stronie internetowej Urzędu.

4. Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych:

- a. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
- b. Zawiadomienie, o którym mowa powyżej, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz co najmniej:
 - zawiera imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,

- opisuje możliwe konsekwencje naruszenia ochrony danych osobowych,
 - opisuje 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.
- c. Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, nie jest wymagane, w następujących przypadkach:
- Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
 - Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
 - wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

PROCEDURA PRIVACY BY DEFAULT

I. WSTĘP

Ustanawia się poniższą procedurę Privacy by default w Podmiocie.

II. DOKUMENTY POWIĄZANE

- *Polityka Ochrony Danych Osobowych*

III. DOMYŚLNE ZACHOWANIE PRYWATNOŚCI

Już na etapie projektowania i opracowywania sposobów przetwarzania danych, a ponadto także na każdym kolejnym etapie przetwarzania, należy uwzględniać obowiązek wdrożenia domyślnych ustawień prywatności.

Jego istotą jest wdrożenie przez Administratora odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Zasada ta oznacza, że ustawienia prywatności stosowane przez Administratora mają mieć na celu maksymalną ochronę użytkownika.

Wprowadzenie zasady domyślnej ochrony danych jest równoznaczne z koniecznością podjęcia przez użytkownika dodatkowych kroków w przypadku, gdyby chciał swoją prywatność w jakikolwiek sposób ograniczyć, np. poprzez udostępnianie swoich danych większej liczbie osób fizycznych.

Zatem zmiana domyślnie stosowanej maksymalnej ochrony prywatności będzie następować jedynie na wyraźne żądanie użytkownika danego systemu czy oprogramowania.

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są przestrzegać zasad domyślnego zachowania prywatności przy przetwarzaniu danych osobowych.

PROCEDURA KORZYSTANIA Z INTERNETU

I. WSTĘP

Ustanawia się poniższą procedurę korzystania z internetu w Podmiocie przez osoby upoważnione do przetwarzania danych osobowych.

Celem procedury jest ustalenie jednolitych zasad postępowania w przypadku korzystania z internetu tak, aby zabezpieczyć wszystkie nośniki informacji przed nieuprawnionym dostępem z sieci zewnętrznej za pomocą wszelkiego oprogramowania mającego działać szkodliwie (malware), a także za pomocą stosowanych socjotechnik: phishing, pharming.

II. DOKUMENTY POWIĄZANE

- *Polityka Ochrony Danych Osobowych*

III. OBOWIĄZKI UŻYTKOWNIKA

1. Użytkownicy systemu informatycznego mają prawo korzystać z internetu wyłącznie w celu wykonywania obowiązków służbowych.
2. Zabrania się w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
3. Zabrania się zgrywania na nośniki pamięci używane w urządzeniach informatycznych oraz uruchamiania na nich jakichkolwiek programów lub aplikacji niezatwierdzonych do użytku.
4. Zabrania się uruchamiania plików pobranych z pominięciem skanowania przez program antywirusowy lub oznaczonych przez ten program jako niebezpieczne lub potencjalnie niebezpieczne.
5. Zabrania się przysyłania danych osobowych przy użyciu nieszyfrowanych stron internetowych. W tym celu przed rozpoczęciem przesłania tych danych, należy sprawdzić czy w pasku adresu strony internetowej widoczna jest informacja o odpowiednim zabezpieczeniu (zielona kłódka, protokół https).
6. Zabrania się przysyłania danych osobowych do krajów spoza EOG (Europejskiego Obszaru Gospodarczego, w zakres którego wchodzi wszystkie kraje Unii Europejskiej, Islandia, Liechtenstein oraz Norwegia), bez uprzedniej zgody IOD lub Administratora.
7. Zabrania się przeglądania treści o charakterze przestępczym, hakerskim lub innym zakazanym przez prawo.
8. Przy korzystaniu z internetu, użytkownicy systemu informatycznego mają obowiązek przestrzegać prawa własności przemysłowej i praw autorskich.

Osoby upoważnione do przetwarzania danych osobowych, zobowiązane są przestrzegać tych zasad podczas korzystania z internetu.

PROCEDURA KORZYSTANIA Z KOMPUTERA SŁUŻBOWEGO

I. WSTĘP

Ustanawia się poniższą procedurę korzystania z komputera służbowego w Podmiocie. Celem procedury jest ustalenie jednolitych zasad użytkowania komputera służbowego.

II. DOKUMENTY POWIĄZANE

- *Polityka Ochrony Danych Osobowych*

III. OBOWIĄZKI UŻYTKOWNIKA

Komputer stacjonarny

1. Przed rozpoczęciem przetwarzania danych osobowych osoba upoważniona powinna sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń, a także czy komputer jest podłączony do UPS (urządzenia zabezpieczającego przed awarią zasilania lub zakłóceniami w sieci zasilającej), jeżeli jest ona na stanowisku stosowany.
2. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić IOD lub Administratora. W szczególności osoba upoważniona jest zobowiązana powiadomić o stwierdzonym usiłowaniu załogowania się do systemu informatycznego służącego do przetwarzania danych osobowych przez osobę nieuprawnioną.
3. Przystępując do pracy z komputerem służącym do przetwarzania danych osobowych, osoba upoważniona jest zobowiązana wprowadzić swoje hasło dostępu lub odblokować urządzenie przy użyciu danych biometrycznych.
4. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora, hasła dostępu lub danych biometrycznych innej osoby upoważnionej.
5. Ustawienie monitorów komputerów służbowych muszą zapewniać ograniczenie możliwości podglądania wyświetlanych danych osobom trzecim.
6. Osoba upoważniona jest zobowiązana dochowywać należytej staranności w celu uniemożliwienia nieuprawnionym osobom trzecim wglądu w informacje obejmujące dane osobowe przetwarzane w ramach systemu, które wyświetlane są na ekranie komputera.
7. W przypadku konieczności przerwania lub zakończenia pracy przy komputerze służbowym służącym do przetwarzania danych osobowych, należy zablokować dostęp do komputera.
8. Zabrania się wnoszenia komputerów stacjonarnych z lokalizacji Podmiotu.
9. Zabrania się wyłączania programów antywirusowych oraz uniemożliwiania wykonania kopii zapasowych przez system informatyczny.
10. Zabrania się odłączania komputera od urządzenia zabezpieczającego przed awarią zasilania lub zakłóceniami w sieci zasilającej.
11. Kopie zapasowe danych osobowych w systemie informatycznym wykonuje wyłącznie osoba wyznaczona przez Administratora.

12. W przypadku przechowywania na komputerze danych osobowych lub stanowiących tajemnicę Administratora, użytkownik jest zobowiązany do ich przechowywania na dysku szyfrowanym, zabezpieczonym hasłem lub w plikach szyfrowanych zabezpieczonych hasłem.

Komputer przenośny

1. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Administratora, użytkownik jest zobowiązany do ich przechowywania na dysku szyfrowanym, zabezpieczonym hasłem lub w plikach szyfrowanych zabezpieczonych hasłem.
2. Na komputerze przenośnym przeznaczonym do zewnętrznych prezentacji multimedialnych nie powinny, o ile to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Administratora.
3. W przypadku kradzieży lub zagubienia komputera przenośnego, użytkownik powinien natychmiast powiadomić o tym IOD albo Administratora, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
4. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności poprzez:
 - przenoszenie go w specjalnym futerale,
 - niepozostawianie w samochodzie podczas postoju w miejscu publicznym bez nadzoru,
 - przechowywanie komputera w bagażniku podczas jazdy samochodem.
5. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania odpowiednich zabezpieczeń. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów, itp.
6. W przypadku pozostawienia komputerów przenośnych w siedzibie zaleca się umieszczenie ich po zakończeniu pracy w zamykanych szafkach.
7. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
8. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.
9. Zabrania się logowania do otwartych sieci (hotspotów, otwartych Wi-Fi).
10. Zabrania się wywożenia komputera przenośnego służącego do przetwarzania danych osobowych do krajów spoza EOG (Europejskiego Obszaru Gospodarczego, w zakres którego wchodzi wszystkie kraje Unii Europejskiej, Islandia, Liechtenstein oraz Norwegia) bez uprzedniej zgody IOD lub Administratora.

Osoby upoważnione do przetwarzania danych osobowych, zobowiązane są przestrzegać tych zasad podczas korzystania z komputerów służbowych.

PROCEDURA KORZYSTANIA Z TELEFONU SŁUŻBOWEGO

I. WSTĘP

Ustanawia się poniższą procedurę korzystania z telefonu służbowego w Podmiocie. Celem procedury jest ustalenie jednolitych zasad użytkowania telefonu służbowego.

II. DOKUMENTY POWIĄZANE

- *Polityka Ochrony Danych Osobowych*

III. OBOWIĄZKI UŻYTKOWNIKA

13. Przystępując do użytkowania telefonu służbowego, osoba upoważniona jest zobowiązana wprowadzić swoje hasło dostępu lub odblokować urządzenie przy użyciu danych biometrycznych.
14. Osoba upoważniona jest zobowiązana dochowywać należytej staranności w celu uniemożliwienia nieuprawnionym osobom trzecim wglądu w informacje obejmujące dane osobowe przetwarzane w ramach systemu, które wyświetlane są na ekranie telefonu.
15. Osoba upoważniona zobowiązana jest do przechowywania i zabezpieczenia telefonu służbowego w sposób utrudniający jego uszkodzenie, zagubienie lub kradzież.
16. Osoba upoważniona jest zobowiązana do należytej dbałości o telefon służbowy oraz jego eksploatację zgodnie z przekazaną instrukcją obsługi.
17. Zabrania się udostępniania telefonu służbowego osobom nieupoważnionym.
18. Zabrania się korzystania z telefonu służbowego w celach prywatnych.
19. Zabrania się instalowania oprogramowania bez wiedzy Administratora, chyba, że jest to konieczne do wykonania obowiązków związanych z umową i prawidłowego działania poszczególnych programów i aplikacji lub poprawia funkcjonowanie i wydajność telefonu służbowego, w takim wypadku obce oprogramowanie powinno pochodzić z legalnego źródła.
20. Zabrania się wyłączania programów antywirusowych oraz uniemożliwiania wykonania kopii zapasowych przez system operacyjny.
21. Zabrania się logowania do otwartych sieci (hotspotów, otwartych sieci Wi-Fi).
22. Zabrania się wywożenia telefonu służbowego służącego do przetwarzania danych osobowych do krajów spoza EOG (Europejskiego Obszaru Gospodarczego, w zakres którego wchodzi wszystkie kraje Unii Europejskiej, Islandia, Liechtenstein oraz Norwegia) bez uprzedniej zgody IOD lub Administratora.
23. Za zabezpieczenie telefonu służbowego odpowiedzialna jest osoba wyznaczona przez Administratora.

Osoby upoważnione do przetwarzania danych osobowych, zobowiązane są przestrzegać tych zasad podczas korzystania z telefonu służbowego.

PROCEDURA KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

I. WSTĘP

Ustanawia się poniższą procedurę korzystania z poczty elektronicznej w Podmiocie przez osoby upoważnione do przetwarzania danych osobowych.

Celem procedury jest ustalenie jednolitych zasad postępowania w przypadku korzystania z poczty elektronicznej tak, aby zabezpieczyć wszystkie nośniki informacji przed nieuprawnionym dostępem z sieci zewnętrznej za pomocą wszelkiego oprogramowania mającego działać szkodliwie (malware), a także za pomocą stosowanych socjotechnik: phishing, pharming.

II. DOKUMENTY POWIĄZANE

- *Polityka Ochrony Danych Osobowych*

III. OBOWIĄZKI UŻYTKOWNIKA

1. Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę. Dopuszcza się taką możliwość wyłącznie po uprzedniej pozytywnej weryfikacji adresu e-mail nadawcy (gdy np. stwierdzimy, że jest to kontrahent Podmiotu).
2. Przy rozsyłaniu wszelkiej korespondencji wielu adresatom należy używać funkcji UDW, pozwalającej na ukrycie adresów e-mail adresatów. W takim przypadku adresy e-mail adresatów należy wprowadzić w polu UDW, a jako jej odbiorcę wprowadzić np. własny adres e-mail.
3. W przypadku przesyłania wszelkich danych osobowych za pośrednictwem poczty elektronicznej, należy wykorzystywać mechanizmy kryptograficzne (np. pakowanie i zabezpieczanie hasłem wysyłanych plików). W takim przypadku hasło dostępowe do pliku należy przesłać innym środkiem komunikacji (np. w wiadomości SMS).
4. Przed wysłaniem wiadomości zawierającej dane osobowe, należy przynajmniej jednokrotnie zweryfikować poprawność adresu e-mail adresata.
5. Zabrania się korzystania z poczty elektronicznej służbowej, w celach prywatnych. Wszelkie wiadomości o charakterze prywatnym utworzone lub odebrane za pośrednictwem poczty elektronicznej przetwarzane są wyłącznie na własną odpowiedzialność. W przypadku kontroli poczty Administrator nie będzie odpowiadać za przypadkowe naruszenie dóbr osobistych Użytkownika w postaci naruszenia tajemnicy korespondencji.
6. Zabrania się wysyłania wiadomości zawierających informacje poufne dotyczące Administratora, jego pracowników, zleceniobiorców, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.
7. Przy korzystaniu z poczty elektronicznej należy przestrzegać prawa własności przemysłowej i prawa autorskiego.

Osoby upoważnione do przetwarzania danych osobowych, zobowiązane są przestrzegać tych zasad podczas korzystania z poczty elektronicznej.

PROCEDURA KORZYSTANIA Z URZĄDZEŃ PRZENOŚNYCH

I. WSTĘP

Ustanawia się poniższą procedurę korzystania z innych niż komputery i telefony urządzeń przenośnych (w szczególności USB) w Podmiocie, przez osoby upoważnione do przetwarzania danych osobowych.

Niniejsza procedura nie dotyczy telefonów służbowych oraz przenośnych komputerów służbowych, w zakresie których sformułowano odrębne procedury.

Celem procedury jest ustalenie jednolitych zasad postępowania w przypadku korzystania z urządzeń przenośnych tak, aby zabezpieczyć wszystkie urządzenia przenośne przed nieuprawnionym dostępem oraz kradzieżą.

II. DOKUMENTY POWIĄZANE

- *Polityka Ochrony Danych Osobowych*

III. OBOWIĄZKI UŻYTKOWNIKA

24. Przystępując do pracy z urządzeniem służącym do przetwarzania danych osobowych, osoba upoważniona jest zobowiązana zweryfikować, czy jego pamięć jest zaszyfrowana. Zabrania się umieszczania plików na nośnikach niezasyfrowanych.
25. W przypadku konieczności przerwania lub zakończenia pracy na urządzeniu przenośnym służącym do przetwarzania danych osobowych, należy zablokować dostęp do tego urządzenia, jeżeli istnieje taka możliwość.
26. Użytkownik jest zobowiązany do należytej dbałości o urządzenie przenośne w sposób utrudniający jego uszkodzenie, zagubienie lub kradzież.
27. Zabrania się pozostawiania urządzeń przenośnych służących do przetwarzania danych osobowych bez nadzoru, poza lokalizacją Podmiotu.
28. Zabrania się wywożenia urządzeń przenośnych służących do przetwarzania danych osobowych do krajów spoza EOG (Europejskiego Obszaru Gospodarczego, w zakres którego wchodzi wszystkie kraje Unii Europejskiej, Islandia, Liechtenstein oraz Norwegia) bez uprzedniej zgody IOD lub Administratora.
29. Zabrania się wyłączania programów antywirusowych oraz uniemożliwiania wykonania kopii zapasowych przez system informatyczny.
30. W przypadku stwierdzenia pojawienia się szkodliwego oprogramowania lub stwierdzenia zaburzeń w funkcjonowaniu urządzenia, osoba upoważniona jest zobowiązana powiadomić o tym fakcie Administratora.
31. Za odpowiednie zabezpieczenie urządzenia przenośnego, a w szczególności jego zaszyfrowanie, odpowiedzialny jest Administrator.
32. Kopie zapasowe danych osobowych w systemie informatycznym wykonuje wyłącznie Administrator.
33. W przypadku korzystania z komputera przenośnego należy postępować zgodnie z *Procedurą korzystania z komputera służbowego*.
34. W przypadku korzystania z telefonu służbowego należy postępować zgodnie z *Procedurą korzystania z telefonu służbowego*.

Osoby upoważnione do przetwarzania danych osobowych, zobowiązane są przestrzegać tych zasad podczas korzystania z urządzeń przenośnych.

PROCEDURA POSTĘPOWANIA Z HASŁAMI I PLIKAMI DOSTĘPOWYMI

I. WSTĘP

Ustanawia się poniższą procedurę postępowania z hasłami i plikami dostępowymi w Podmiocie.

II. DOKUMENTY POWIĄZANE

- *Polityka Ochrony Danych Osobowych*

III. OBOWIĄZKI UŻYTKOWNIKA

Każda osoba upoważniona jest zobowiązana do ochrony swoich danych dostępowych do systemów informatycznych służących do przetwarzania danych osobowych. W zakres danych dostępowych włącza się w szczególności

1. hasła dostępowe,
2. klucze softwareowe (pliki umożliwiające dostęp – np. certyfikaty do VPN),
3. klucze sprzętowe,
4. inne mechanizmy umożliwiające dostęp do systemów IT.

Podstawowe metody ochrony danych dostępowych:

1. nieprzekazywanie danych dostępowych innym osobom (np. przekazywanie swojego hasła dostępowego osobom trzecim),
2. nieprzechowywanie danych dostępowych w miejscach publicznych (np. zapisywanie haseł dostępowych w łatwo dostępnych miejscach),
3. ochrona danych dostępowych przed pozyskaniem przez osoby trzecie.

Osoby upoważnione do przetwarzania danych osobowych, zobowiązane są przestrzegać tych zasad.

PROCEDURA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

I. WSTĘP

Ustanawia się poniższą procedurę powierzenia przetwarzania danych osobowych w Podmiocie.

II. DOKUMENTY POWIĄZANE

- *Umowa powierzenia przetwarzania danych osobowych dla Administratora*
- *Umowy powierzenia przetwarzania danych osobowych - zawarte*
- *Polityka Ochrony Danych Osobowych*

III. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

W przypadku konieczności przetwarzania danych osobowych przez odrębne podmioty świadczące usługi dla Administratora, może on powierzyć ich przetwarzanie.

Powierzenie nie polega na udostępnieniu danych. Udostępnienie jest przekazaniem danych innemu podmiotowi (odbiorcy danych), który staje się ich Administratorem w zamiarze realizacji własnych celów. Powierzenie polega na przetwarzaniu danych przez podmiot przyjmujący w powierzenie, w zamiarze realizacji celów Administratora. Powierzeniem jest np. ujawnienie danych osobowych do zewnętrznego biura rachunkowego. Udostępnieniem jest np. ujawnienie danych osobowych Urzędowi Skarbowemu.

Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i Administratora, określają w szczególności przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Rekomenduje się posługiwanie wzorem *Umowy powierzenia przetwarzania danych osobowych dla Administratora*.

W przypadku, gdy stosowana jest inny wzorzec umowny, odmienny od wzorca umowy pozostającego w dyspozycji Administratora, konieczna jest szczegółowa weryfikacja zgodności tego innego wzorca z przepisami powszechnie obowiązującego prawa, w szczególności Rozporządzenia UE.

Administrator przechowuje zawarte Umowy powierzenia przetwarzania danych osobowych w zbiorze *Umowy powierzenia przetwarzania danych osobowych - zawarte*.

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do powierzenia danych osobowych tylko z uwzględnieniem powyższych wymogów. W przypadku wątpliwości należy skontaktować się z Administratorem.

PRECEDURA PRIVACY BY DESIGN

I. WSTĘP

Ustanawia się poniższą procedurę privacy by design.

II. DOKUMENTY POWIĄZANE

- *Polityka Ochrony Danych Osobowych*

III. PROJEKTOWANIE PROCESÓW PRZETWARZANIA:

Już na etapie projektowania i opracowywania sposobów przetwarzania danych, a ponadto także na każdym kolejnym etapie przetwarzania, należy uwzględniać obowiązujące zasady ochrony danych osobowych.

W szczególności należy zadbać o zachowanie zasad:

- minimalizacji przetwarzania danych osobowych,
- jak najszybszej pseudonimizacji danych osobowych,
- przejrzystości co do funkcji i przetwarzania danych osobowych,
- umożliwienia osobie, której dane dotyczą, monitorowania przetwarzania danych,

- umożliwienia Administratorowi tworzenia i doskonalenia zabezpieczeń.

Do obowiązków Administratora należy zapewnienie, by stosowane rozwiązania były zgodne z przepisami rozporządzenia i chroniły prawa osób, których przetwarzane dane dotyczą. Niemniej osoby upoważnione, przy wykonywaniu czynności służbowych, powinny mieć tę zasadę na względzie.

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są przestrzegać powyższych zasad na etapie projektowania i opracowywania sposobów przetwarzania danych osobowych.

PROCEDURA PRZEGLĄDÓW I KONSERWACJI SYSTEMU INFORMATYCZNEGO

I. WSTĘP

Ustanawia się poniższą procedurę przeglądów i konserwacji systemu informatycznego. Celem procedury jest zapewnienie realizacji przeglądów, napraw i konserwacji systemu informatycznego, służącego do przetwarzania danych osobowych.

II. DOKUMENTY POWIĄZANE

- *Rejestr przeglądów i konserwacji systemu informatycznego*
- *Polityka Ochrony Danych Osobowych*

III. ZGŁASZANIE ZAPOTRZEBOWANIA NA PRZEPROWADZENIE PRZEGLĄDU, NAPRAWY LUB KONSERWACJI URZĄDZEŃ INFORMATYCZNYCH

1. W przypadku wystąpienia zapotrzebowania na przeprowadzenie przeglądu, naprawy lub konserwacji urządzeń informatycznych służących do przetwarzania danych osobowych, osoba upoważniona jest zobowiązana zgłosić ten fakt do informatyka wyznaczonego przez Administratora.
2. Osoba upoważniona jest zobowiązana udostępnić urządzenie informatyczne dla celu wykonania przeglądu, naprawy lub konserwacji.
3. Zabronione jest wykonywanie przeglądów, napraw i konserwacji systemów informatycznych służących do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych samodzielnie przez pracownika.

IV. REALIZACJA PRZEGLĄDÓW, NAPRAW I KONSERWACJI SYSTEMU INFORMATYCZNEGO

Przeglądy, naprawy i konserwacje urządzeń informatycznych służących do przetwarzania danych osobowych, przeprowadzane są w lokalizacji Podmiotu, z zastrzeżeniem poniższych warunków:

1. naprawy i konserwacje urządzeń informatycznych służących do przetwarzania danych osobowych mogą być wykonywane przez przedsiębiorstwa lub wykonawców zewnętrznych wyłącznie na podstawie zawartych umów,
2. w przypadku przekazywania do naprawy urządzeń informatycznych służących do przetwarzania danych osobowych:
 - a. jeśli uszkodzenie nie dotyczy nośników pamięci, należy je wymontować i do naprawy przekazać urządzenie nie zawierające nośników, na których są dane osobowe,

- b. jeśli uszkodzenie dotyczy nośników pamięci, należy zniszczyć je, przywracając pliki zawierające dane osobowe z kopii zapasowej,
 - c. jeśli uszkodzenie dotyczy nośników pamięci a jednocześnie brak jest plików zawierających dane osobowe, wówczas należy zrealizować naprawę pod bezpośrednim nadzorem osoby upoważnionej albo po zawarciu umowy powierzenia danych osobowych,
3. w przypadku przeprowadzania naprawy zdalnej, w szczególności przy użyciu środków teletransmisji podglądu ekranu osoby upoważnionej do przetwarzania danych, przed rozpoczęciem tej czynności osoba upoważniona jest zobowiązana wyłączyć wszelkie programy służące do przetwarzania danych osobowych, których użycie nie jest niezbędne podczas wykonywania czynności, a także ukryć ikony pulpitu,
4. Administrator jest zobowiązany zapewnić wykonywanie przynajmniej wyrywkowych przeglądów technicznych urządzeń służących do przetwarzania danych osobowych nie rzadziej niż raz w roku,
5. W Podmiocie prowadzi się *Rejestr przeglądów i konserwacji systemu informatycznego*.

PRECEDURA PRZETWARZANIA DANYCH OSOBOWYCH W FORMIE PAPIEROWEJ

I. WSTĘP

Ustanawia się poniższą procedurę przetwarzania danych osobowych w formie papierowej. Celem procedury jest ustalenie jednolitych zasad postępowania z danymi osobowymi w wersji papierowej.

II. DOKUMENTY POWIĄZANE

- *Polityka Ochrony Danych Osobowych*

III. OBOWIĄZKI OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

8. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są wszystkie osoby upoważnione do przetwarzania danych osobowych.
9. Rozpoczynając pracę należy rozeznaczyć czy stanowisko pracy jest w stanie nienaruszonym od dnia poprzedniego.
10. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych, w szafach, biurkach i szufladach. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do zabezpieczenia dokumentów (zamykanie biurek, szuflad i szaf na klucz) podczas swojej nieobecności w pomieszczeniach i po zakończeniu pracy – tzw. „zasada czystego biurka”.
11. W trakcie pracy w zasięgu wzroku osób nieupoważnionych nie mogą znaleźć się dokumenty zawierające dane osobowe.
12. W przypadku chwilowego opuszczenia stanowiska pracy, w zasięgu wzroku i w zasięgu ręki nie można pozostawić dokumentów zawierających dane osobowe. Dokumenty należy wcześniej schować do biurka/szuflady.
13. Po zakończeniu pracy należy wykonać następujące czynności:
- uporządkować stanowisko pracy, nie pozostawiając na nim dokumentacji zawierającej dane osobowe,

- schować do biurka lub zamykanej na klucz szafy pieczętki służbowe,
 - zamknąć biurko i szafy zawierające dokumentację,
 - upewnić się, czy nie pozostawiono żadnych kluczy na stanowisku pracy.
14. Drukarki nie mogą znajdować się w zasięgu dostępu osób nieupoważnionych. Za prawidłowość ustawienia urządzeń odpowiada Administrator.
15. Zabrania się pozostawiania wydruków w i na drukarkach i kserokopiarkach.
16. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przewożenia dokumentów w sposób zapobiegający kradzieży, zgubieniu lub utracie.
17. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

Osoby upoważnione, przy przetwarzaniu danych osobowych w formie papierowej, zobowiązane są do przestrzegania powyższych zasad.

PROCEDURA PRZYJMOWANIA DANYCH OSOBOWYCH W POWIERZENIE

I. WSTĘP

Ustanawia się poniższą procedurę przyjmowania danych osobowych w powierzenie przez Podmiot.

II. DOKUMENTY POWIĄZANE

- *Umowa powierzenia przetwarzania danych osobowych dla podmiotu przetwarzającego*
- *Rejestr kategorii czynności przetwarzania danych osobowych*
- *Polityka Ochrony Danych Osobowych*

III. PRZYJMOWANIE DANYCH OSOBOWYCH:

Podmiot w charakterze podmiotu przetwarzającego (procesora) może przyjąć do przetwarzania dane osobowe powierzone przez odrębnych administratorów.

Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają w szczególności przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

W pierwszej kolejności Podmiot zobowiązany jest korzystać ze wzoru *Umowy powierzenia przetwarzania danych osobowych dla podmiotu przetwarzającego*.

W przypadku, gdy stosowana jest inny wzorzec umowny, odmienny od wzorca umowy pozostającego w dyspozycji Podmiotu, konieczna jest szczegółowa weryfikacja zgodności tego innego wzorca z przepisami powszechnie obowiązującego prawa, w szczególności RODO.

W przypadku przyjmowania czynności na danych osobowych w powierzenie, podmiot jest zobowiązany ewidencjonować ich kategorie w *Rejestrze kategorii czynności przetwarzania danych osobowych*.

Wyłączenie obowiązku prowadzenia rejestru kategorii czynności przetwarzania stosuje się w przypadkach określonych w art. 30 pkt 5 Rozporządzenia UE.

Powierzenie nie polega na udostępnieniu danych. Udostępnienie jest przekazaniem danych innemu podmiotowi (odbiorcy danych), który staje się ich Administratorem w zamiarze realizacji własnych celów. Powierzenie polega na przetwarzaniu danych przez podmiot przyjmujący w powierzenie, w zamiarze realizacji celów Administratora. Powierzeniem jest np. ujawnienie danych osobowych do zewnętrznego biura rachunkowego. Udostępnieniem jest np. ujawnienie danych osobowych Urzędowi Skarbowemu.

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przyjmowania danych osobowych w powierzenie tylko z uwzględnieniem powyższych wymogów. W przypadku wątpliwości należy skontaktować się z Administratorem.

PROCEDURA REALIZACJI OBOWIĄZKU INFORMACYJNEGO

I. WSTĘP

Ustanawia się poniższą procedurę realizacji obowiązku informacyjnego.

II. DOKUMENTY POWIĄZANE

- *Obowiązki informacyjne*
- *Polityka Ochrony Danych Osobowych*

III. REALIZACJA OBOWIĄZKU INFORMACYJNEGO

W przypadku zbierania danych osobowych, zwykle należy czytelnie udzielić informacji zgodnych z właściwym *Obowiązkiem informacyjnym*.

W odniesieniu do procesów zbierania danych **od osób, których one dotyczą**, podanych w załączniku zasad nie stosuje się, jeżeli:

1. przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania lub jeżeli
2. osoba, której dane dotyczą, posiada już te informacje.

W odniesieniu do procesów zbierania danych **nie od osób, których one dotyczą**, podanych w załączniku zasad nie stosuje się, jeżeli:

1. przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,
2. poinformowanie wymaga niewspółmiernie dużego wysiłku – w szczególności, gdy dane przetwarzane są w celach archiwizacyjnych, statystycznych, badań naukowych,
3. przekazanie informacji okazuje się niemożliwe,
4. utrwalenie lub ujawnienie danych jest wyraźnie nakazane prawem UE lub prawa krajowego,
5. dotyczy to tajemnicy zawodowej wynikającej z prawa UE lub prawa krajowego.

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przestrzegania powyższych zasad przy zbieraniu danych osobowych.

PROCEDURA USUWANIA DANYCH OSOBOWYCH

I. WSTĘP

Ustanawia się poniższą procedurę usuwania danych osobowych w Podmiocie przez osoby upoważnione do przetwarzania danych osobowych.

Celem procedury jest ustalenie jednolitych zasad postępowania w przypadku usuwania danych osobowych.

II. DOKUMENTY POWIĄZANE

- *Rejestr czynności przetwarzania danych osobowych*
- *Procedura usuwania urzędzeń i nośników informacji*
- *Procedura przetwarzania danych osobowych w formie papierowej*
- *Polityka Ochrony Danych Osobowych*

III. OGÓLNE ZASADY

18. Niszczenie dokumentów zawierających dane osobowe powinno być dokonywane w sposób uniemożliwiający identyfikację osoby, której dane dotyczą.
19. Dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, dla realizacji których dane te są przetwarzane.
20. Dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
21. Podczas ustalania zasad i okresów usuwania danych osobowych powinno uwzględniać się przepisy obowiązującego prawa oraz cele administratora.
22. Dane osobowe powinny zatem być usuwane wtedy, gdy:
 - przepisy szczególne regulują obowiązek przetwarzania danych osobowych przez ustalony okres, np. przepisy prawa pracy, prawa podatkowego, ustawa o rachunkowości,
 - jeżeli ustawodawca krajowy lub unijny nie reguluje okresu przechowywania danych osobowych, wówczas należy kierować się zasadą ograniczenia celu.
23. Terminy retencji danych osobowych zostały ustanowione w *Rejestrze czynności przetwarzania danych osobowych*. Niniejsze terminy są wykorzystywane przy opracowaniu treści obowiązku informacyjnego, który należy spełnić wobec osób, których dane przetwarza Administrator. Jednym z jego elementów jest konieczność wskazania okresu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe kryteria ustalania tego okresu.
24. Ustalając okres przechowywania danych osobowych należy wziąć pod uwagę obecną i przyszłą wartość informacji, koszty, ryzyko i zobowiązania związane z przetwarzaniem danych osobowych.

25. Administrator wyznacza osoby odpowiedzialne w Podmiocie za przestrzeganie niniejszej Procedury.
26. Osoby odpowiedzialne regularnie sprawdzają czy dane są niezbędne do realizacji określonych celów.
27. Osoby odpowiedzialne dokonują okresowych przeglądów ustalonych okresów przechowywania danych osobowych, lokalizacji danych osobowych, a także faktycznej weryfikacji realizacji obowiązku usuwania danych osobowych.

IV. USUWANIE DANYCH OSOBOWYCH

Usuwanie danych osobowych w formie papierowej.

1. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach, niezwłocznie po ustaniu celu ich przetwarzania, zgodnie z *Rejestrem czynności przetwarzania danych osobowych*.
2. Dokumenty powinny być niszczone tak, aby nie sposób było odczytać zawartych w nich informacji.

Usuwanie danych osobowych w formie elektronicznej

1. Usuwanie danych osobowych ma charakter zautomatyzowany – poprzez odpowiednią konfigurację systemów informatycznych.
2. Systemy informatyczne powinny pozwalać na ustalanie okresów przechowywania danych osobowych, a także umożliwić sprawne usuwanie całości lub części danych.
3. Usuwanie urządzeń i nośników informacji odbywa się zgodnie z *Procedurą usuwania urządzeń i nośników informacji*.

Osoby upoważnione do przetwarzania danych osobowych, zobowiązane są przestrzegać tych zasad podczas usuwania danych osobowych.

PROCEDURA USUWANIA DANYCH OSOBOWYCH

I. WSTĘP

Ustanawia się poniższą procedurę usuwania danych osobowych w Podmiocie przez osoby upoważnione do przetwarzania danych osobowych.

Celem procedury jest ustalenie jednolitych zasad postępowania w przypadku usuwania danych osobowych.

II. DOKUMENTY POWIĄZANE

- *Rejestr czynności przetwarzania danych osobowych*
- *Procedura usuwania urządzeń i nośników informacji*
- *Procedura przetwarzania danych osobowych w formie papierowej*
- *Polityka Ochrony Danych Osobowych*

III. OGÓLNE ZASADY

28. Niszczenie dokumentów zawierających dane osobowe powinno być dokonywane w sposób uniemożliwiający identyfikację osoby, której dane dotyczą.
29. Dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, dla realizacji których dane te są przetwarzane.
30. Dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
31. Podczas ustalania zasad i okresów usuwania danych osobowych powinno uwzględniać się przepisy obowiązującego prawa oraz cele administratora.
32. Dane osobowe powinny zatem być usuwane wtedy, gdy:
 - przepisy szczególne regulują obowiązek przetwarzania danych osobowych przez ustalony okres, np. przepisy prawa pracy, prawa podatkowego, ustawa o rachunkowości,
 - jeżeli ustawodawca krajowy lub unijny nie reguluje okresu przechowywania danych osobowych, wówczas należy kierować się zasadą ograniczenia celu.
33. Terminy retencji danych osobowych zostały ustanowione w *Rejestrze czynności przetwarzania danych osobowych*. Niniejsze terminy są wykorzystywane przy opracowaniu treści obowiązku informacyjnego, który należy spełnić wobec osób, których dane przetwarza Administrator. Jednym z jego elementów jest konieczność wskazania okresu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe kryteria ustalania tego okresu.
34. Ustalając okres przechowywania danych osobowych należy wziąć pod uwagę obecną i przyszłą wartość informacji, koszty, ryzyko i zobowiązania związane z przetwarzaniem danych osobowych.
35. Administrator wyznacza osoby odpowiedzialne w Podmiocie za przestrzeganie niniejszej Procedury.
36. Osoby odpowiedzialne regularnie sprawdzają czy dane są niezbędne do realizacji określonych celów.
37. Osoby odpowiedzialne dokonują okresowych przeglądów ustalonych okresów przechowywania danych osobowych, lokalizacji danych osobowych, a także faktycznej weryfikacji realizacji obowiązku usuwania danych osobowych.

IV. USUWANIE DANYCH OSOBOWYCH

Usuwanie danych osobowych w formie papierowej.

3. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach, niezwłocznie po ustaniu celu ich przetwarzania, zgodnie z *Rejestrem czynności przetwarzania danych osobowych*.
4. Dokumenty powinny być niszczone tak, aby nie sposób było odczytać zawartych w nich informacji.

Usuwanie danych osobowych w formie elektronicznej

4. Usuwanie danych osobowych ma charakter zautomatyzowany – poprzez odpowiednią konfigurację systemów informatycznych.

5. Systemy informatyczne powinny pozwalać na ustalanie okresów przechowywania danych osobowych, a także umożliwić sprawne usuwanie całości lub części danych.
6. Usuwanie urządzeń i nośników informacji odbywa się zgodnie z *Procedurą usuwania urządzeń i nośników informacji*.

Osoby upoważnione do przetwarzania danych osobowych, zobowiązane są przestrzegać tych zasad podczas usuwania danych osobowych.

PRECEDURA REALIZACJI ŻĄDAŃ PODMIOTU DANYCH

I. WSTĘP

RODO zapewnia podmiotowi danych szereg praw w zakresie przetwarzania danych osobowych. Podmiot danych może żądać od Administratora realizacji tych praw zgodnie z Rozdziałem III RODO. Ustanawia się poniższą procedurę realizacji żądań podmiotu danych. Celem niniejszej procedury jest określenie zasad obsługi żądań podmiotu danych, dotyczących realizacji praw podmiotu danych.

II. DOKUMENTY POWIĄZANE:

- *Obowiązki informacyjne*
- *Polityka Ochrony Danych Osobowych*

III. OGÓLNE ZASADY

W przypadku zwrócenia się przez osobę, której dane są przetwarzane z żądaniem realizacji jej praw, osoba która powzięła o tym wiedzę, ma obowiązek natychmiastowego poinformowania o tym fakcie IOD albo Administratora. Osoba upoważniona nie podejmuje samodzielnych działań w tym zakresie.

Ogólne zasady udzielania informacji i realizacji praw podmiotu danych opisuje art. 12 Rozporządzenia UE.

1. Podawanie informacji w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje kierowane są do dziecka. Podmiot udziela informacji zgodnie ze wzorami *Obowiązków informacyjnych*.
2. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – drogą elektroniczną.
3. Administrator jest zobowiązany udzielić podmiotowi danych odpowiedzi na żądanie, chyba że nie jest w stanie zidentyfikować osoby, której dane dotyczą.
4. Administrator udziela informacji podmiotowi danych bez zbędnej zwłoki – nie później niż maksymalnie w ciągu miesiąca od otrzymania żądania.
5. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.

6. Jeżeli osoba, której dane dotyczą, przekazała swoje żądanie drogą elektroniczną, w miarę możliwości informacje także przekazywane są drogą elektroniczną, chyba że osoba, której dane dotyczą, zażąda innej formy.
7. Jeżeli Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego.
8. Odpowiedzi na żądania są wolne od opłat. Wyjątkiem jest realizacja prawa dostępu do danych (wydania ich kopii), realizowana po raz kolejny.
9. Jeżeli Administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

IV. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Prawo do wycofania zgody.

- a. Podmiot danych ma prawo do wycofania zgody, jeżeli podstawą przetwarzania ich danych osobowych jest zgoda.
- b. Administrator jest zobowiązany ustalić, czy zgoda jest podstawą przetwarzania (czy nie występują inne podstawy np. Umowa, obowiązek wynikający z przepisów prawa) nim zaprzestanie przetwarzania danych.
- c. Jeśli Administrator ustali, że zgoda nie jest (jedyną) podstawą przetwarzania danych osobowych podmiotu danych, odrzuca żądanie informując podmiot danych o powodach odrzucenia.
- d. Jeśli zgoda dotyczy dziecka (które nie ukończyło 16 r.ż.) wycofanie zgody musi być potwierdzone przez rodzica lub opiekuna prawnego.
- e. W przypadku skorzystania z możliwości wycofanie zgody drogą elektroniczną (np. odznaczenie checkboxa w systemie informatycznym), niniejsza procedura może zostać pominięta.

2. Prawo do informacji

Administrator udziela osobie, której dane dotyczą informacji dotyczących przetwarzania jej danych osobowych zarówno wtedy, gdy dane te pozyskuje bezpośrednio od osoby, której dane dotyczą (art. 13 RODO), jak i w sytuacji, gdy dane pozyskuje z innych źródeł (art.14 RODO).

3. Prawo dostępu przysługujące osobie, której dane dotyczą

Administrator na żądanie osoby, której dane dotyczą, udziela jej informacji, czy przetwarza jej dane. Gdy ma to miejsce, Administrator jest zobowiązany udzielić tej osobie dostępu do tych danych oraz następujących informacji:

- a. cele przetwarzania,
- b. kategorie danych osobowych,
- c. odbiorcy lub kategorie odbiorców danych, w szczególności odbiorcy w państwach trzecich lub organizacjach międzynarodowych,

- d. planowany okres przechowywania danych (lub kryteria ustalania tego okresu),
- e. informacja o prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, które go dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
- f. informacja o prawie wniesienia skargi do organu nadzorczego,
- g. informacja o źródle danych, jeśli nie zostały one zebrane bezpośrednio od pomiotu danych,
- h. informacja o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą (ma zastosowanie w przypadku gdy zautomatyzowane podejmowanie decyzji wywołuje wobec osoby skutki prawne lub w podobny sposób istotnie na nią wpływa lub gdy opiera się na szczególnych kategoriach danych osobowych),
- i. w przypadku gdy dane są przekazywane do państwa trzeciego lub organizacji międzynarodowej, należy podać informacje o stosowanych zabezpieczeniach,

Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie Administrator może pobrać rozsądną opłatę.

4. Prawo do sprostowania danych

W przypadku nieprawidłowości lub niekompletności przetwarzanych danych osobowych, osoba, której dane dotyczą, ma prawo żądać ich sprostowania lub uzupełnienia.

5. Prawo do usunięcia danych („prawo do bycia zapomnianym”)

Administrator na żądanie osoby, której dane dotyczą usuwa jej dane, jeśli zachodzi jedna z poniższych okoliczności:

- a. dane osobowe nie są już niezbędne do celów, w których zostały one zebrane,
- b. osoba, której dane dotyczą wycofała zgodę, na której przetwarzanie było oparte i nie ma innej podstawy prawnej przetwarzania,
- c. podmiot danych wnosi sprzeciw wobec przetwarzania,
- d. dane osobowe były przetwarzane niezgodnie z prawem,
- e. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego (prawo Unii lub krajowe),
- f. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, oferowanych dziecku, które nie ukończyło 16 lat.

Jeśli dane osobowe zostały upublicznione, Administrator zobowiązany jest podjąć rozsądne działania (uwzględniające dostępną technologię i koszty realizacji), aby poinformować innych administratorów przetwarzających te dane, o żądaniu podmiotu danych dotyczącym usunięcia tych danych, ich kopii i łączy do nich.

Administrator ma prawo odmówić realizacji tego żądania, jeśli oceni, że przetwarzanie danych jest niezbędne:

- a. do korzystania z praw do wolności wypowiedzi i informacji,

- b. do wywiązania się z obowiązków prawnych (narzuconych prawem Unii, prawem krajowym lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
- c. ze względu na interes publiczny w dziedzinie zdrowia publicznego,
- d. do celów archiwalnych w interesie publicznym,
- e. do ustalenia, dochodzenia lub obrony roszczeń.

6. Prawo do ograniczenia przetwarzania

Osoba, której dane dotyczą może żądać ograniczenia przetwarzania jej danych osobowych w następujących przypadkach:

- a. osoba, której dane dotyczą kwestionuje prawidłowość danych. W takim przypadku Administrator ogranicza przetwarzanie na okres pozwalający mu sprawdzić ich prawidłowość,
- b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
- c. osoba, której dane dotyczą potrzebuje danych do ustalenia, dochodzenia lub obrony roszczeń, a nie są one już potrzebne Administratorowi,
- d. rozpatrywany jest sprzeciw wobec przetwarzania danych.

Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

7. Prawo do przenoszenia danych

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, np. CSV, JSON, XHTML, dane osobowe jej dotyczące, które dostarczyła Administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:

- a. Przetwarzanie odbywa się na podstawie zgody,
- b. Przetwarzanie odbywa się na podstawie umowy,
- c. Przetwarzanie odbywa się w sposób zautomatyzowany.

Osoba, której dane dotyczą ma prawo żądania, by jego dane osobowe były przesłane przez Administratora bezpośrednio innemu Administratorowi.

Rozpatrując żądanie przeniesienia danych należy rozważyć, czy ta operacja nie ma negatywnego wpływu na prawa i wolności innych.

8. Prawo do sprzeciwu

Osoba, której dane dotyczą ma prawo wnieść sprzeciw wobec przetwarzania danych z przyczyn związanych z jej szczególną sytuacją, jeśli przetwarzanie jest niezbędne:

- a. do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi,
- b. do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.

Administrator zaprzestaje przetwarzania danych, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą.

W przypadku, gdy dane osobowe przetwarzane są w celu prowadzenie marketingu bezpośredniego, Administrator musi bezwzględnie zaprzestać przetwarzania danych.

9. Prawo, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu w tym profilowaniu.

Osoba, której dane dotyczą ma prawo nie podlegać decyzji opartych wyłącznie o zautomatyzowane przetwarzanie (w tym profilowanie) i decyzja taka wywołuje wobec osoby skutki prawne lub w podobny sposób istotnie wpływa na podmiot.

Wyjątkiem są sytuacje, w których ta decyzja:

- a. jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a Administratorem;
- b. jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
- c. opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

W przypadku, gdy zautomatyzowane podejmowanie decyzji jest niezbędne do zawarcia umowy lub opiera się na wyraźnej zgodzie podmiot danych może żądać interwencji człowieka, a także ma prawo do wyrażenia własnego stanowiska i do zakwestionowania decyzji.

V. ETAPY REALIZACJI PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Wpłynięcie żądania – drogą elektroniczną, listownie lub telefonicznie.
2. IOD albo Administrator odpowiedzialny jest za realizację praw osób, których dane dotyczą lub koordynację działań związanych z ich realizacją oraz podejmuje decyzje w tej kwestii.
3. IOD albo Administrator potwierdzają tożsamość podmiotu danych. Jeżeli jest to wymagane, wówczas można wystąpić o dodatkowe informacje, jeżeli istnieją uzasadnione wątpliwości co do tożsamości osoby fizycznej.
4. IOD albo Administrator ocenia zasadność żądania:
 - czy żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, w takim przypadku podejmowana jest decyzja, czy odrzucić wniosek, czy zastosować opłatę, podmiot danych zostaje poinformowany o powodzie odrzucenia wniosku,
 - w przypadku wniosków o sprostowanie, usunięcie, ograniczenie lub sprzeciw wobec przetwarzania danych osobowych zostaje przeprowadzona analiza, czy wniosek jest uzasadniony i zgodny z prawem. Po analizie podjęta zostaje decyzja o przyjęciu bądź

odrzuconiu wniosku. Podmiot danych zostaje poinformowany o powodzie odrzucenia wniosku.

5. Jeżeli wniosek został przyjęty IOD albo Administrator przystępują do opracowania żądania. W zależności od rodzaju żądania podejmowane są odpowiednie działania, np. opracowanie stosownych informacji, opracowanie metody usunięcia/udostępnienia danych osobowych. Czynności te mogą zająć maksymalnie miesiąc czasu (uwzględniając czas jaki upłynął od wpłynięcia żądania i czas potrzebny na jego realizację). W uzasadnionych przypadkach czas ten może zostać wydłużony do dwóch miesięcy. O opóźnieniu i jego powodach należy poinformować podmiot danych.
6. IOD albo Administrator realizują żądanie – żądane informacje zostają przekazane osobom, których dane dotyczą.
7. IOD albo Administrator zamykają żądanie podmiotu danych.

PROCEDURA TWORZENIA KOPII ZAPASOWYCH

I. WSTĘP

Ustanawia się poniższą procedurę wykonywania kopii zapasowych w Podmiocie.

II. DOKUMENTY POWIĄZANE

- *Polityka Ochrony Danych Osobowych*

III. TWORZENIE KOPII ZAPASOWYCH:

Ustanawia się poniższe wymogi dotyczące wykonywania kopii zapasowych danych osobowych przetwarzanych w systemie informatycznym Podmiotu. Osoba wyznaczona przez Administratora jest zobowiązana do bezpośredniej realizacji ich przestrzegania.

1. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych tych danych.
2. Za system sporządzania kopii zapasowych danych osobowych odpowiedzialna jest osoba wyznaczona przez Administratora.
3. Kopie zapasowe danych osobowych w systemie informatycznym wykonuje wyłącznie osoba wyznaczona przez Administratora.
4. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
5. Kopie zapasowe powinny być cyklicznie kontrolowane przez osobę wyznaczoną przez Administratora, w szczególności pod kątem prawidłowości ich wykonania oraz możliwości odtworzenia, poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.
6. Nośniki zawierające kopie danych osobowych przetwarzanych w systemie informatycznym Podmiotu są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.

7. Kopie zapasowe przechowuje się w odrębnej lokalizacji względem oryginału zabezpieczonych danych.
8. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.

PROCEDURA UDOSTĘPNIANIA DANYCH OSOBOWYCH

I. WSTĘP

Ustanawia się poniższą procedurę udostępniania danych osobowych w Podmiocie.

II. DOKUMENTY POWIĄZANE

- *Rejestr odbiorców danych osobowych*
- *Polityka Ochrony Danych Osobowych*

III. UDOSTĘPNIANIE DANYCH OSOBOWYCH:

Udostępnianie danych osobowych, jest jedną z form ich przetwarzania. Udostępnianie danych osobowych można określić, jako wszelkie działania umożliwiające innym niż Administrator podmiotom, zapoznanie się z nimi, z wyłączeniem opisanych wcześniej powierzeń. Udostępnianie nie odnosi się również do pracowników Podmiotu, którzy działają na podstawie udzielonych upoważnień.

1. Nie jest istotne czy udostępnianie danych ma charakter odpłatny czy nie, aby czynność była uznana za udostępnianie.
2. Nie jest istotne, czy udostępnianie następuje w formie przekazu ustnego, pisemnego, za pomocą powszechnych środków przekazu lub poprzez sieć komputerową itd., aby czynność była uznana za udostępnianie.
3. Udostępnianie danych osobowych osobom lub podmiotom uprawnionym do ich otrzymania odbywa się na mocy przepisów prawa.
4. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

Administrator lub osoba przez niego upoważniona może prowadzić *Rejestr odbiorców danych osobowych*. Dokument zawiera informacje o ujawnieniach danych osobowych, z wyłączeniem:

1. osób upoważnionych do przetwarzania danych osobowych,
2. osób, których dane dotyczą.

Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do udostępniania danych osobowych tylko z uwzględnieniem powyższych wymogów. W przypadku wątpliwości należy skontaktować się z Administratorem.

PROCEDURA DOSTĘPU DO KLUCZY I OBIEKTÓW

I. WSTĘP

1. Ustanawia się niniejszą Procedurę dostępu do kluczy i obiektów.

2. Celem procedury jest ustanowienie zasad postępowania z kluczami do budynków, pomieszczeń oraz obszarów, w których przetwarzane są dane osobowe, a także zasad przebywania w nich.
3. Obowiązujący czas pracy wyszczególniony jest w aktualnym regulaminie pracy ~~– układzie zbiorowym pracy / obwieszczeniu.~~

II. DOKUMENTY POWIĄZANE

- *Polityka Ochrony Danych Osobowych*
- *Ewidencja osób upoważnionych do dostępu do kluczy do budynków i pomieszczeń zwykłych – załącznik nr 1*
- *Ewidencja pobrań i zdań kluczy - załącznik nr 2*

III. ZASADY DOSTĘPU DO KLUCZY

1. Dostęp do kluczy do budynków i pomieszczeń zwykłych, w których przetwarzane są dane osobowe, mają wyłącznie osoby upoważnione, tj. wpisane są do *Ewidencji osób upoważnionych do dostępu do kluczy do budynków i pomieszczeń zwykłych – załącznik nr 1* do niniejszej Procedury.
2. Osoby upoważnione do dostępu do kluczy mają obowiązek potwierdzania codziennego pobierania i zdawania kluczy w *Ewidencji pobrań i zdań kluczy - załącznik nr 2* do niniejszej Procedury.
3. Zabrania się udostępniania kluczy osobom nieupoważnionym do dostępu do kluczy.
4. Zabrania się pozostawiania w czasie pracy kluczy do budynków i pomieszczeń w zamkach.
5. Zabrania się pozostawiania kluczy w szafach, szufladach i biurkach podczas nieobecności w pomieszczeniu osób upoważnionych do przetwarzania danych osobowych.
6. Poza godzinami pracy, klucze do szaf, szuflad oraz biurek przechowuje się w kasetach lub skrzynkach zamykanych na szyfr.
7. Poza godzinami pracy, klucze do pomieszczeń przechowuje się w kasetach lub skrzynkach zamykanych na szyfr.

IV. ZASADY DOSTĘPU DO KLUCZY ZAPASOWYCH

1. Klucze zapasowe przechowywane są w kasetce.
2. Wydawanie kluczy zapasowych do budynków i pomieszczeń zwykłych może odbywać się tylko (łącznie):
 - w uzasadnionych sytuacjach lub przypadkach awaryjnych,
 - na rzecz osób wpisanych do *Ewidencji osób upoważnionych do dostępu do kluczy do budynków i pomieszczeń zwykłych – załącznik nr 1* do niniejszej Procedury,
 - za zgodą Administratora.
3. Po użyciu kluczy zapasowych, należy je niezwłocznie zwrócić.

V. ZASADY PRZEBYWANIA W POMIESZCZENIACH ZWYKŁYCH

1. Przebywanie w budynkach lub pomieszczeniach Podmiotu, jest dozwolone w godzinach pracy, przez osoby upoważnione do przetwarzania danych osobowych, przetwarzanych w tych budynkach lub pomieszczeniach.
2. Z zastrzeżeniem punktu poniżej, zabrania się przebywania w budynkach lub pomieszczeniach zwykłych Podmiotu poza godzinami pracy.
3. Przebywanie w budynkach lub pomieszczeniach zwykłych Podmiotu poza godzinami pracy, wymaga zgody Administratora.
4. Przebywanie osób nieupoważnionych do przetwarzania danych osobowych, wewnątrz pomieszczeń zwykłych, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych lub za zgodą Administratora.
5. Po zakończeniu pracy, poprzez użycie kluczy, osoby sprawujące nadzór nad nimi, zobowiązane są zabezpieczyć miejsca przechowywania dokumentów z danymi osobowymi (budynki, pomieszczenia, szafy, biurka, szuflady) i inne zbiory ewidencyjne przed dostępem osób trzecich, a także przed zniszczeniem i kradzieżą.

Ewidencja osób upoważnionych mających dostęp
do kluczy do budynków i pomieszczeń zwykłych

Imię i nazwisko osoby upoważnionej	Budynek- nazwa pomieszczenia, nr piętra	Limity czasowe (w godz. od-do)	Data przyznania dostępu	Data anulowania dostępu

Ewidencja pobrań i zdań kluczy

Imię i nazwisko osoby upoważnionej	Data	Godzina pobrania kluczy	Czytelny podpis	Godzina zdania kluczy	Czytelny podpis

PROCEDURA KONTROLI DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

I. WSTĘP

Ustanawia się poniższą procedurę wykonywania kontroli dostępu do systemu informatycznego, służącego do przetwarzania danych osobowych.

II. DOKUMENTY POWIĄZANE

- *Polityka Ochrony Danych Osobowych*

III. KONTROLA DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

Ustanawia się poniższe wymogi dotyczące kontroli dostępu do systemu informatycznego, służącego do przetwarzania danych osobowych w Podmiocie. Osoba odpowiedzialna za IT jest zobowiązana do monitorowania i zapewnienia ich przestrzegania.

1. W systemie informatycznym służącym do przetwarzania danych osobowych w Podmiocie, stosuje się mechanizmy kontroli dostępu do tych danych.
2. Jeżeli dostęp do danych osobowych przetwarzanych w systemie informatycznym (w szczególności do urządzenia, aplikacji lub programu), posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
 - a. w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator,
 - b. dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia lub z użyciem danych biometrycznych.
3. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, nie może być przydzielony innej osobie.

W przypadku, gdy do uwierzytelniania użytkowników w systemie informatycznym służącym do przetwarzania danych osobowych używa się hasła, wdraża się środki wymuszające stosowanie haseł składających się co najmniej z 8 znaków, w tym małych i wielkich liter oraz cyfr lub znaków specjalnych

PROCEDURA ZABEZPIECZENIA ANTYWIRUSOWEGO

I. WSTĘP

Ustanawia się poniższą procedurę zabezpieczenia antywirusowego w Podmiocie. Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem malware (np. typu robaki, wirusy komputerowe, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe. Ustanawia się poniższe wymogi dotyczące ochrony antywirusowej. Osoba wyznaczona przez Administratora jest zobowiązana do monitorowania i zapewnienia ich przestrzegania.

II. DOKUMENTY POWIĄZANE

- *Polityka Ochrony Danych Osobowych*

III. OBOWIĄZKI UŻYTKOWNIKA

1. Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych stosowane jest oprogramowanie antywirusowe.
2. Za zaplanowanie i zapewnienie ochrony antywirusowej, w tym za zapewnienie odpowiedniej ilości licencji odpowiada osoba wyznaczona przez Administratora.
3. Każdy plik wczytywany do urządzenia informatycznego, w tym także wiadomość e-mail, podlega przetestowaniu programem antywirusowym.
4. W każdym urządzeniu informatycznym wyposażonym w dostęp do internetu, musi być zainstalowane oprogramowanie antywirusowe.
5. Aktualizacja definicji wirusów odbywa się automatycznie przez system.

XIV ZAŁĄCZNIKI

Załączniki do niniejszej Polityki Ochrony Danych stanowią jej integralną część:

A - LISTA ZAŁĄCZNIKÓW:

1. Rejestr czynności przetwarzania danych osobowych,
2. Rejestr kategorii czynności przetwarzania danych osobowych,
3. Rejestr naruszeń ochrony danych osobowych,
4. Rejestr środków ochrony danych osobowych,
5. Rejestr odbiorców danych osobowych,
6. Obowiązki informacyjne - szablon,
7. Upoważnienie dla pracowników - szablon,
8. Upoważnienie dla osób zatrudnionych na podstawie umów cywilnoprawnych - szablon,
9. Umowa powierzenia przetwarzania danych osobowych dla administratora - szablon,
10. Umowa powierzenia przetwarzania danych osobowych dla podmiotu przetwarzającego – szablon,
11. Analiza ryzyka – dokument przewodni,
12. Matryce ryzyk,
13. Ocena skutków dla ochrony danych - szablon,
14. Umowy powierzenia przetwarzania danych osobowych (należy przechowywać w załączeniu),
15. Oceny skutków dla ochrony danych osobowych (należy przechowywać w załączeniu).
16. Rejestr osób upoważnionych do przetwarzania danych osobowych,
17. Ankieta dla podmiotu przetwarzającego,
18. Wzór - Nieodpłatne zezwolenie na rozpowszechnienie wizerunku,
19. Wzór - Odpłatne zezwolenie na rozpowszechnienie wizerunku.

