POLITYKA BEZPIECZEŃSTWA INFORMACJI

SPORZĄDZONA PRZEZ:

P.U. Administracja Beata Kaczmarek
ul. Wielka 18/17 61-775 Poznań
[Administrator danych]

Poznań, dnia 1 grudnia 2021r.

1. Cel sporządzenia Polityki bezpieczeństwa informacji

Niniejsza *Polityka bezpieczeństwa informacji*, zwana dalej **Polityką,** została opracowana w celu potwierdzenia, że dane osobowe zbierane przez Administratora danych są przetwarzane i zabezpieczone zgodnie z przepisami *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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* (dalej **RODO**).

2. Postanowienia ogólne

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, Administrator danych wdrożył odpowiednie środki techniczne oraz organizacyjne opisane w niniejszej Polityce, aby przetwarzanie danych odbywało się zgodnie z RODO. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
2. Dodatkowo Administrator danych w ramach monitorowania zastosowanych środków ochrony dokonuje m.in. bieżącego monitorowania działań Użytkowników oraz integralności plików, ochrony przed atakami zewnętrznymi oraz wewnętrznymi, a także prowadzi rejestr naruszeń zasad dostępu do danych.
3. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora danych.

3. Definicje

1. **Administrator danych** Przedsiębiorstwo Usługowe „Administracja” Beata Kaczmarek, ul. Wielka 18/17, 61-775 Poznań
2. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
3. **Przetwarzanie danych** – oznacza operację lub zestaw operacji wykonywanych na Danych osobowych lub zestawach Danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
4. **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów.
5. **Użytkownik** – osoba upoważniona przez Administratora danych do Przetwarzania danych osobowych.
6. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów i narzędzi programowych zastosowanych w celu Przetwarzania danych.
7. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie Przetwarzania danych w takim systemie.

4. Podstawowe zasady dotyczące Przetwarzania danych

1. Wszyscy Użytkownicy zobowiązani są do Przetwarzania danych osobowych zgodnie z RODO , niniejszą Polityką, w tym Instrukcją Zarządzania Systemem Informatycznym, stanowiącą Załącznik nr 1 do Polityki, a także innymi procedurami związanymi z Przetwarzaniem danych obowiązującymi u Administratora danych.
2. Wszystkie Dane osobowe są przetwarzane z poszanowaniem zasad Przetwarzania danych przewidzianych w RODO:

a) w każdym przypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla Przetwarzania danych,
b) Dane osobowe przetwarzane są rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
c) Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
d) Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu Przetwarzania danych,
e) Dane osobowe są prawidłowe i w razie potrzeby uaktualniane,
f) wobec osoby, której Dane osobowe dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO,
g) Dane osobowe są zabezpieczone przed naruszeniami zasad ich ochrony.

3. Administrator danych prowadzi rejestr czynności przetwarzania, z uwagi na okoliczność, iż Przetwarzanie danych nie ma charakteru sporadycznego.
4. Administrator danych może powierzyć przetwarzanie Danych osobowych innemu podmiotowi w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.
5. Administrator danych nie będzie przekazywał Danych osobowych do państwa trzeciego, poza sytuacjami, w których następuje to na wniosek osoby, której dane dotyczą.
6. Administrator danych, po dokonaniu Szacowania ryzyka dla procesu przetwarzania danych, z uwagi na brak wystąpienia określonych przesłanek wskazanych w RODO nie jest zobowiązany do dokonania Oceny skutków dla ochrony danych tzw. DPIA oraz nie wyznaczył Inspektora ochrony danych tzw. DPO.

5. Cele Przetwarzania danych

Administrator danych przetwarza Dane osobowe, w szczególności aby:

1) zrealizować w sposób należyty wszystkie obowiązki lub uprawnienia wynikające z umowy łączącej Administratora danych z osobą, której Dane osobowe są przetwarzane,
2) sprawnie i rzetelnie zarządzać i administrować nieruchomościami,
3) zrealizować obowiązki wynikające z umów zawartych przez Administratora danych z podmiotami, z którymi Administrator danych współpracuje w ramach prowadzonej działalności gospodarczej,
4) zrealizować obowiązki lub uprawnienia wynikające z przepisów prawa dotyczące określonego stosunku prawnego,
5) zapewnić bezpieczeństwo osób i mienia na terenie nieruchomości,
6) dochodzić ewentualnych roszczeń,
7) zrealizować obowiązki związane z zamiarem zawarcia przez Administratora danych umów dotyczących grupowych świadczeń na rzecz pracowników.

6. Podstawa prawna Przetwarzania danych

Podstawą prawną Przetwarzania danych może być:

1) zgoda osoby, które Dane osobowe dotyczą - art. 6 ust. 1 lit. a) RODO,
2) konieczność realizacji przez Administratora danych obowiązków i uprawnień wynikających z umowy zawartej między Administratorem danych a osobą, której Dane osobowe dotyczą – art. 6 ust. 1 lit. b) RODO,
3) konieczność wypełnienia przez Administratora danych obowiązków prawnych wynikających z przepisów prawa, w szczególności ustawy Kodeks cywilny, ustawy z dnia 21 czerwca 2001 r. o ochronie praw lokatorów, mieszkaniowym zasobie gminy i o zmianie Kodeksu cywilnego, ustawy Kodeks pracy lub innej dotyczącej stosunku prawnego łączącego Administratora danych z osobą, której Dane osobowe dotyczą – art. 6 ust. 1 lit. c) RODO,

4) prawnie uzasadniony interes Administratora danych realizowany przez Administratora danych lub osobę trzecią, art. 6 ust. 1 lit. f) RODO, tj. w szczególności:
    a) konieczność zapewnienia bezpieczeństwa osób i mienia na terenie nieruchomości (monitoring wizyjny),
    b) realizacja przez Administratora danych obowiązków wynikających z umów zawartych przez Administratora danych z podmiotami, z którymi Administrator danych współpracuje w ramach prowadzonej działalności gospodarczej,
    c) zawarcie przez Administratora danych umów dotyczących grupowych świadczeń na rzecz pracowników związanych ze stosunkiem pracy,
    d) ustalenie, dochodzenie lub obrona roszczeń z tytułu prowadzonej przez Administratora danych działalności,
    e) archiwizacja Danych osobowych.

7. Odbiorcy danych

1. Administrator danych może przekazywać Dane osobowe podmiotom, które w imieniu Administratora danych realizować będą cele określone w pkt 5 powyżej, tj. w szczególności podmiotom, które:
    a) dokonują rozliczenia czynszów i innych opłat wynikających z umowy najmu,
    b) dokonują napraw lub remontów na nieruchomości,
    c) usuwają awarie,
    d) są dostawcami mediów do nieruchomości,
    e) są dostawcami usług IT,
    f) kancelarii prawnej,
    g) będą dokonywać przetwarzania danych osobowych zgodnie z RODO na wyraźne udokumentowane polecenie Administratora danych.
2. Dodatkowo Dane osobowe pracowników Administratora danych mogą być przekazywane:
    a) podmiotom, które dokonują rozliczenia wynagrodzenia za pracę lub innych świadczeń wynikających ze stosunku pracy (biuro rachunkowe),
    b) Zakładowi Ubezpieczeń Społecznych, Urzędowi Skarbowemu, innym organom administracji publicznej w wykonaniu obowiązku prawnego, bankom,
    c) Kontrahentom Administratora danych w celach związanych z zajmowanym przez pracownika stanowiskiem,
    d) podmiotom, które oferują Administratorowi danych świadczenia grupowe na rzecz pracowników.

8. Obszar Przetwarzania danych

1. Dane osobowe przetwarzane są w siedzibie Administratora danych, tj. w Poznaniu przy ul. Wielkiej 18/17, w pokojach zabezpieczonych systemem alarmowym. Dane osobowe znajdują się na następujących urządzeniach:
    a) serwerze Fujitsu Serwer TX1320M4 E-2234, znajdującym się w pokoju zamykanym na klucz,
    b) dysku sieciowym NAS (pamięć masowa) Qnap-TS-251D-2G, znajdującym się w pokoju zamykanym na klucz,
    c) komputerach Użytkowników w celu przetworzenia tych danych, w tym komputerach przenośnych,
    d) telefonach służbowych Użytkowników.
2. Dane osobowe gromadzone są również w formie papierowej (w szczególności umowy najmu, dzierżawy, umowy o pracę, faktury, rachunki, noty obciążeniowe, noty odsetkowe) i przechowywane na obszarze, o którym mowa w pkt 1 powyżej.

9. Zbiory danych

1. Dane osobowe przetwarzane przez Administratora danych gromadzone są w następujących zbiorach danych prowadzonych w programach i systemach informatycznych.

1) Program Symfonia Faktura

Dane przechowywane są w formie kartotek kontrahentów, tj. najemców lokali i współwłaścicieli nieruchomości w bazie danych Btrive.
Program Symfonia Faktura składa się z następujących pozycji:

- imię i nazwisko
- miejscowość
- kod
- ulica
- kraj
- rejon
- NIP
- REGON
- PESEL
- numer Telefonu
- numer Faksu
- adres e-mail
- adres strony www
- numer rachunku bankowego

2) Program Probit

Program Probit przechowuje kartoteki najemców lokali, korzystając z zaszyfrowanych plików tekstowych, które zawierają następujące elementy:

- imię i nazwisko
- adres
- NIP
- REGON
- telefon
- numer konta
- FAX

3) Program AGA – Archiwum – nie wpisujemy nowych danych

Program AGA przechowuje Dane osobowe pracowników i zleceniobiorców. Składa się z następujących pozycji:

- imię i nazwisko
- płeć
- data i miejsce urodzenia
- imię ojca i matki
- nazwisko rodowe
- nazwisko rodowe matki
- PESEL
- NIP
- stan cywilny
- numer telefonu
- dowód osobisty – seria, numer, przez kogo wydany

- wykształcenie
- numer rachunku bankowego
- adres zamieszkania – miejscowość, powiat, gmina, dzielnica, województwo, ulica, nr domu, mieszkania, kod pocztowy
- właściwy urząd skarbowy
- dane osobowe członków rodziny na utrzymaniu
- dane szczegółowe dotyczące zatrudnienia.

4) MS Office (Word i Excel)

Dane przechowywane są w formie dokumentów tekstowych oraz arkuszy kalkulacyjnych i zawierają następujące Dane osobowe:

- imię i nazwisko
- miejscowość
- kod
- ulica
- kraj
- rejon
- NIP
- REGON
- PESEL
- numer Telefonu
- numer Faksu
- adres e-mail
- adres strony www
- numer rachunku bankowego

5) MS Outlook

Dane osobowe przetwarzane są przez system informatyczny w celu wymiany korespondencji:

- imię i nazwisko
- miejscowość
- kod
- ulica
- kraj
- rejon
- NIP
- REGON
- PESEL
- numer Telefonu
- numer Faksu
- adres e-mail
- adres strony www
- numer rachunku bankowego

2. Administrator danych prowadzi także papierowe zbiory danych, w szczególności:
   a) akta osobowe
   b) zbiór umów najmu i dzierżawy,
   c) zbiór umów zlecenia, o dzieło, o roboty budowlane,
   d) zbiór dokumentów księgowych, tj. faktury, rachunki, noty obciążeniowe, noty odsetkowe.

10. Organizacyjne i techniczne środki bezpieczeństwa

1. Dla zapewnienia poufności, integralności i rozliczalności przetwarzanych Danych osobowych, Administrator danych podjął szereg środków technicznych i organizacyjnych.
2. Do organizacyjnych środków ochrony Danych osobowych należą w szczególności:
    a) dopuszczenie do Przetwarzania danych wyłącznie osób posiadających pisemne upoważnienia udzielone przez Administratora danych,
    b) przeszkolenie ww. osób w zakresie należytego Przetwarzania danych, w tym w szczególności w zakresie bezpieczeństwa sieciowego i systemowego oraz zobowiązane do zachowania w poufności wszystkich danych, do których mają dostęp,
    c) prowadzenie ewidencji osób upoważnionych do Przetwarzania danych,
    d) ograniczenie dostępu do pomieszczeń, w których przetwarzane są Dane osobowe, jedynie do osób odpowiednio upoważnionych,
    e) prowadzenie spotkań z osobami trzecimi wyłącznie w pomieszczeniu - sali konferencyjnej, w którym nie znajdują się żadne nośniki z Danymi osobowymi,
    f) przechowywanie dokumentacji archiwalnej w pomieszczeniach odosobnionych, zamkniętych na klucz, który jest w dyspozycji wyłącznie osoby upoważnionej przez Administratora danych,
    g) zabezpieczenie obszaru, na którym przetwarzane są Dane osobowe instalacją alarmową; system alarmowy zbudowany jest z następujących elementów:
        - centrali alarmowej SATEL, typ INTEGRA
        - klawiatury załączające/wyłączające system alarmowy (kod dostępu),
        - czujek alarmowych na podczerwień pasywną,
        - okablowanie obwodem sabotażowym (ingerencja w obwód sabotażowy powoduje natychmiastowe wyzwolenie alarmu bez względu na to, czy system jest załączony);

        system alarmowy posiada pamięć występujących zdarzeń (w pamięci zapisanych jest ok. 600 ostatnich zdarzeń w systemie: wejść, wyjść, alarmów, zaników zasilania i innych awarii),
    h) umieszczenie serwera oraz dysku sieciowego w pomieszczeniu odosobnionym, zamkniętym na klucz, który jest w dyspozycji wyłącznie osoby upoważnionej przez Administratora danych,
    i) wykorzystanie zamykanych szafek do zabezpieczenia dokumentów zawierających Dane osobowe,
    j) wykorzystanie niszczarki do skutecznego niszczenia i usuwania dokumentów zawierających Dane osobowe, w szczególności tymczasowych wydruków z Danymi osobowymi, zakaz wyrzucania dokumentów do pojemników śmietnikowych,
    k) korzystanie z drukarek w taki sposób, aby wszelkie wydruku były odbierane przez osoby korzystające z drukarek zaraz po wydrukowaniu dokumentu,
    l) opracowanie i wdrożenie Instrukcji Zarządzania Systemem Informatycznym służącym do Przetwarzania danych i zapoznanie z zasadami w niej określonymi Użytkowników,
    m) sprawdzanie zgodności Przetwarzania danych z przepisami RODO:
        - co dwa lata na podstawie Arkusza planu sprawdzeń stanowiącego Załącznik nr 2 do Polityki,
        - co trzy lata w zakresie systemów informatycznych służących do przetwarzania lub zabezpieczania Danych osobowych,
    n) aktualizowanie dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych, tj. w szczególności Polityki i Instrukcji zarządzania system informatycznym, oraz przestrzeganie zasad w nich określonych.

3. Do technicznych środków ochrony danych należą te rozwiązania, które zapewniają u Administratora danych bezpieczeństwo sieciowe i systemowe szczegółowo opisane w Instrukcji Zarządzania Systemem Informatycznym.

11. Naruszenia zasad ochrony Danych osobowych

1. Za naruszenie lub próbę naruszenia zasad Przetwarzania danych i ochrony Danych osobowych uważa się w szczególności:
    a) naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są Dane osobowe,
    b) udostępnianie lub umożliwienie udostępniania Danych osobowych podmiotom do tego nieupoważnionym,
    c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia Danym osobowym ochrony,
    d) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia,
    e) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania,
    f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych,
    g) naruszenie praw osób, których dane są przetwarzane.
2. W przypadku stwierdzenia naruszenia ochrony Danych osobowych Administrator danych dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
3. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator danych zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki, jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zgłoszenia określa Załącznik nr 3 do Polityki.
4. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator danych zawiadamia o incydencie także osobę, której dane dotyczą.

12. Prawa osób, których dane dotyczą

1. Administrator danych realizuje prawa osób, których dane dotyczą, w tym:
    a) Prawo do informacji (obowiązek informacyjny),
    b) Prawo dostępu do Danych osobowych lub otrzymania kopii Danych osobowych,
    c) Prawo do sprostowania Danych osobowych,
    d) Prawo do usunięcia Danych osobowych,
    e) Prawo do ograniczenia Przetwarzania danych,
    f) Prawo do przenoszenia Danych osobowych,
    g) Prawo do sprzeciwu.
2. W zakresie realizacji praw osoby, której Dane osobowe dotyczą, udzielanie tej osobie informacji oraz komunikacja z tą osobą powinna odbywać się w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem; informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie lub jeżeli osoba, której Dane osobowe dotyczą, tego żąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość tej osoby.
3. Administrator danych jest uprawniony do odmowy podjęcia działań w związku z żądaniami, o których mowa w pkt 1 powyżej, jeżeli wykaże iż nie jest w stanie zidentyfikować osoby, której Dane osobowe dotyczą, a ponadto w sytuacji, gdy:
    a) żądanie ma zostać zrealizowane w formacie lub na nośniku nieznanym lub niestosowanym przez Administratora danych,

b) wniosek jest niezrozumiały i osoba, której Dane osobowe dotyczą składając wniosek, mimo prośby Administratora danych nie wyjaśniła w sposób jednoznaczny niejasności związanych z wnioskiem,
c) tożsamość wnioskodawcy jest nieustalona i mimo prób, nie udało się potwierdzić tożsamości wnioskującego,
d) w przypadku, kiedy wnioskodawca zażąda wydania kopii Danych osobowych lub przeniesienia Danych osobowych w języku innym niż język, w jakim Dane osobowe są przetwarzane.

13. Okres przechowywania Danych osobowych

Dane osobowe będą przechowane do momentu całkowitego rozliczenia się stron ze wszystkich świadczeń wynikających z zakończonej umowy łączącej Administrator danych z osobą, której Dane osobowe dotyczą, lub do chwili przedawnienia wszystkich roszczeń wynikających z przedmiotowej umowy.

14. Zasady retencji Danych osobowych

1. Dane osobowe są usuwane w przypadku, gdy:
   a) cele, dla których Dane osobowe są przetwarzane zostały osiągnięte,
   b) upłynęły już okresy przechowywania Danych osobowych,
   c) osoba, której Dane osobowe dotyczą wystąpiła z wnioskiem o niezwłoczne usunięcie swoich Danych osobowych (zrealizowanie „prawa do bycia zapomnianym") i zachodzą przesłanki do ich usunięcia, tj.:
      - dane osobowe nie są niezbędne celów, dla których zostały zebrane lub w inny sposób przetwarzane,
      - osoba, której dane dotyczą cofnęła zgodę, na której opiera się przetwarzanie przez Administratora danych jej danych i nie ma innej podstawy prawnej Przetwarzania danych,
      - osoba, której dane dotyczą wnosi sprzeciw - z przyczyn dotyczących jej szczególnej sytuacji – wobec Przetwarzania danych i nie występują nadrzędnie prawnie uzasadnione podstawy Przetwarzania danych,
      - Dane osobowe były przetwarzane niezgodnie z prawem,
      - Dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub w obowiązujących przepisach prawa.
2. Usunięcie danych osobowych polega na:
   a) fizycznym niszczeniu dokumentów,
   b) likwidacji sprzętu lub nośników zawierających Dane osobowe,
   c) usuwaniu Danych osobowych z systemu,
   d) anonimizacji Danych osobowych,
3. Po usunięciu Danych osobowych Administrator danych ma prawo zachować rejestr usuniętych danych.

15. Postanowienia końcowe

1. Jakiekolwiek zmiany do Polityki wymagają formy pisemnej i są dokonywane jedynie przez Administratora danych.
2. Integralną część Polityki stanowią Załączniki wymienione w dokumencie.

.....
podpis Administratora danych

Załącznik nr 1
– INSTRUKCJA ZARZĄDZANIA SYSTEM INFORMATYCZNYM

Niniejsza *Instrukcja zarządzania systemem informatycznym*, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych Administratora danych przetwarzane są w sposób zgodny z przepisami RODO.

1. Nadawanie uprawnień

1. Nadawanie uprawnień Użytkownikom do Przetwarzania danych w Systemie informatycznym realizowane jest przez Administratora danych poprzez następujące czynności:
    a) umożliwienie wygenerowania Użytkownikowi własnego Hasła dostępu do komputera,
    b) wdrożenie Użytkownika do obsługi Systemu informatycznego oraz przeszkolenie Użytkownika w zakresie zabezpieczeń Systemu informatycznego.
2. Odebrania uprawnień Użytkownikom do Przetwarzania danych w Systemie informatycznym dokonuje Administrator danych poprzez:
    a) zablokowanie konta Użytkownika,
    b) usunięcie konta Użytkownika (z wyjątkiem informacji o jego działaniach na Zbiorze danych).

2. Hasła

1. Użytkownik przy pierwszym uruchomieniu nowego komputera określa własne Hasło składające się z minimum 8 znaków, w tym z dużych i małych liter oraz cyfr lub znaków specjalnych.
2. System wymusza zmianę Hasła przez Użytkownika na nowe co 30 dni.
3. Hasła zapisywane są do 18 zmian wstecz, co oznacza, że nie można tego samego Hasła użyć częściej niż raz na 1,5 roku. Zaleca się niekorzystanie z wcześniej użytych Haseł.

3. Praca Użytkownika w systemie

1. Przy rozpoczęciu pracy od Użytkownika wymaga się poprawnego zalogowania do systemu operacyjnego na komputerze lokalnym (login i hasło).
2. Zakończenie pracy polega na:
    a) wylogowaniu się Użytkownika z systemu,
    b) wyłączeniu komputera.
3. W przypadku braku możliwości zalogowania się bądź wylogowania z systemu, Użytkownik zobowiązany jest do niezwłocznego kontaktu z Administratorem danych lub z inną osobą wskazaną przez Administratora danych i podjęcia działań według jego wytycznych. Użytkownikowi zabrania się zakończenia pracy i opuszczenia stanowiska pracy bez wylogowania z systemu.
4. W przypadku tymczasowego zaprzestania pracy na skutek opuszczenia stanowiska, od Użytkownika wymaga się zablokowania ekranu, co skutkuje blokadą komputera. Podjęcie pracy na komputerze możliwe jest dopiero po wprowadzeniu Hasła. Automatyczna blokada następuje po 10 minutach nieaktywności Użytkownika (tj. bezczynności komputera).
5. W przypadku powzięcia przez Użytkownika uzasadnionego przypuszczenia naruszenia bezpieczeństwa systemu, tj. w przypadku stwierdzenia ingerencji w przetwarzane Dane osobowe lub użytkowane narzędzia programowe lub systemowe przez osobę nieuprawnioną, Użytkownik niezwłocznie powiadamia o tym drogą elektroniczną bądź

telefoniczną Administratora danych lub inną osobę wskazaną przez Administratora danych.

6. W przypadku, o którym mowa w pkt 5 powyżej, Administrator danych dokonuje fizycznego odłączenia serwera ze Zbiorem danych od wszystkich mediów transmisyjnych, dokonuje sprawdzenia dostępu do serwera i Zbioru danych sprzed ostatnich 24 godzin, porównuje aktualną wersję zbioru danych z ostatnio wykonaną kopią archiwalną.
7. Korzystanie z Internetu przez Użytkownika odbywa się wyłącznie do celów służbowych. Użytkowników obowiązuje zakaz stosowania funkcji zapamiętywania haseł w przeglądarkach internetowych.
8. W przypadku korzystania z poczty elektronicznej obowiązują następujące zasady:
    a) obowiązek korzystania z poczty elektronicznej tylko do celów służbowych,
    b) obowiązek rzetelnego zweryfikowania adresów mailowych w procesie wysyłania poczty, tj. kierowanie poczty do właściwych adresatów,
    c) zakaz korzystania z linków znajdujących się w mailach nieznanego pochodzenia,
    d) zakaz otwierania załączników znajdujących się w mailach nieznanego pochodzenia,
    e) wprowadzenie w stopce maila klauzuli poufności wraz z pouczeniem o skasowaniu wiadomości, jeśli nie trafiła ona do właściwego adresata.

4. Kopie zapasowe, nośniki

1. Celem zabezpieczenia Systemu informatycznego, Administrator danych tworzy kopie zapasowe Zbiorów danych – programów komputerowych i narzędzi programowych służących do ich Przetwarzania danych.
2. Kopie zapasowe są tworzone po każdym wylogowaniu się Użytkownika z systemu, z komputera lokalnego na serwer (kopia różnicowa).
3. Dysk sieciowy, na którym tworzone są kopie zapasowe, zabezpieczony jest Firewallem wbudowanym w router, który umożliwia dostęp do niego tylko z sieci lokalnej i blokuje kontakt z sieci Internet.
4. Każdy folder zabezpieczony dodatkowym Hasłem, które znane jest wyłącznie Administratorowi danych.
5. W przypadku uszkodzenia dysku twardego zawierającego kopie zapasowe, dokonuje się jego likwidacji poprzez przekazanie do zniszczenia odpowiedzialnemu za to podmiotowi, który wystawia certyfikat zniszczenia dysków.
6. Tymczasowe wydruki z Danymi osobowymi są po ich wykorzystywaniu niszczone w niszczarkach znajdujących się w pomieszczeniach, gdzie Dane osobowe są przetwarzane.

5. Zabezpieczenia systemu

1. Celem usunięcia niebezpieczeństwa przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do Systemu informatycznego, w szczególności wprowadzenia wirusów komputerowych do systemu informatycznego wprowadzono następujące środki:
    a) Firewall programowy systemu Windows filtrujący ruch pomiędzy systemem operacyjnym serwera i uruchomionymi aplikacjami, a siecią internet;
    b) Firewall wbudowany w router, pośredniczący w komunikacji z internetem, filtrujący dane przechodzące pomiędzy siecią lokalną i siecią publiczną oraz zabezpieczający poszczególne komputery przed atakami z zewnątrz;
    c) program antywirusowy z automatycznie aktualizowanymi bazami.
2. Dostęp do serwera zabezpieczony jest dodatkowym Hasłem, które znane jest wyłącznie Administratorowi danych.

3. Nie istnieje możliwość fizycznej obsługi serwera. Brak jest urządzeń wejścia/wyjścia, (klawiatury i myszy), brak podłączenia do monitora.
4. Serwer podłączony jest do systemu UPS, co oznacza, że w przypadku przerw lub zakłóceń dostawy energii elektrycznej z sieci energetycznej urządzenie zasila serwer, a w razie dłuższego braku zasilania bezpiecznie wyłączy serwer.
5. Komputery Użytkowników, z których możliwy jest dostęp do Danych osobowych zawartych w zbiorach danych, zabezpieczone są hasłem i loginem odrębnym dla każdego Użytkownika.
6. Użytkownicy mają dostęp do Zbiorów danych i zasobów udostępnionych (folderów sieciowych) tylko w takim zakresie, w jakim zostali upoważnieni przez Administratora danych.
7. W przypadku wykrycia i usunięcia wirusa komputerowego dokonuje się skanowania innym programem antywirusowym.
8. W przypadku gdy oprogramowanie zabezpieczające wskazuje zaistnienie zagrożenia, Użytkownik zobowiązany do natychmiastowego powiadomienia Administratora danych lub innej osoby wskazanej przez Administratora danych.

6. Przeglądy i konserwacje

1. Przeglądy i konserwacje Systemu informatycznego i Zbiorów danych dokonywane są okresowo poprzez sporządzanie zestawienia dostępu Użytkowników do zbiorów danych, sprawdzenie zmian dokonywanych przez Użytkowników oraz ich weryfikacja z przydzielonymi Użytkownikowi pracami.
2. Przeglądy realizowane są przez Administratora danych lub inną osobę przez niego wskazaną.

.....
podpis Administratora danych

Załącznik nr 2
– WZÓR ZGŁOSZENIA INCYDENTU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

. . . . . , dn. . . . . r.
[data sporządzenia]

Prezes Urzędu Ochrony Danych Osobowych

ZGŁOSZENIE INCYDENTU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 33 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych W związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych.

Dane Administratora danych do kontaktu	
Miejsce i dzień naruszenia	
Kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie	
Opis charakteru naruszenia ochrony danych osobowych	
Możliwe konsekwencje naruszenia ochrony danych osobowych	
Środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, lub w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych	

.....
podpis Administratora danych

Załącznik nr 3
– WZÓR ARKUSZU PLANU SPRAWDZEŃ

ARKUSZ PLANU SPRAWDZEŃ

1. DATA SPRAWDZENIA: …….. 201….R.

2. PRZEDMIOT SPRAWDZENIA:

- ZGODNOŚĆ PRZETWARZANYCH DANYCH Z PRZEPISAMI RODO

3. ZAKRES SPRAWDZENIA:
   1) PRZETWARZANIE DANYCH

      – ZGODNE CELAMI, DLA KTÓRYCH DANE OSOBOWE ZOSTAŁY ZEBRANE -- TAK/NIE*

   2) DO PRZETWARZANIA DANYCH

      - DOPUSZCZONE SĄ WYŁĄCZNIE OSOBY UPOWAŻNIONE PRZEZ ADMINISTRATORA DANYCH ----------TAK/NIE*

   3) EWIDENCJA OSÓB UPOWAŻNIONYCH

      – AKTUALIZOWANA JEST NA BIEŻĄCO ---------- TAK/NIE*

   4) OSOBY UPOWAŻNIONE

      - ZOSTAŁY PRZESZKOLONE ---------- TAK/NIE*
      - ZGŁASZAJĄ POTRZEBĘ POWTÓRZENIA SZKOLENIA ----------TAK/NIE*
      - PRZESTRZEGAJĄ ZASAD I OBOWIĄZKÓW OKREŚLONYCH W DOKUMENTACJI PRZETWARZANIA DANYCH ---------- TAK/NIE*

   5) WYKAZ ZBIORÓW DANYCH ORAZ ICH STRUKTURA

      – ZGODNE Z POLITYKĄ BEZPIECZEŃSTWA INFORMACJI ---------- TAK/NIE*

   6) ZABEZPIECZENIA DANYCH W ZAKRESIE ŚRODKÓW OCHRONY FIZYCZNEJ DANYCH ORAZ ŚRODKÓW ORGANIZACYJNYCH

      – ZGODNE Z RODO ORAZ POLITYKĄ BEZPIECZEŃSTWA INFORMACJI I INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMACTYCZNTYM -------TAK/NIE*

……
podpis Administratora danych

*właściwe zakreślić