UCHWAŁA ZARZĄDU NR 2 / 2020
SPÓŁDZIELNI MIESZKANIOWEJ „AR-MOCZYDŁO" W WARSZAWIE
z dnia 2.12.2020 r.
w sprawie uchwalenia Księgi Procedur
Spółdzielni Mieszkaniowej „AR –Moczydło" w Warszawie

Zarząd Spółdzielni Mieszkaniowej „AR-Moczydło" w Warszawie postanawia, co następuje:

§ 1.

Wprowadza się Księgę Procedur Spółdzielni Mieszkaniowej „AR-Moczydło" w Warszawie dotyczącą ochrony danych osobowych.

§ 2.

Treść Księgi Procedur Spółdzielni Mieszkaniowej „AR-Moczydło" w Warszawie stanowi załącznik do Uchwały.

§ 3.

Traci moc Uchwała Zarządu Nr 1/2018 Spółdzielni Mieszkaniowej „AR-Moczydło" w Warszawie z dnia 24 maja 2018 r. w sprawie przyjęcia polityki bezpieczeństwa przetwarzania danych osobowych.

§ 4.

Uchwała wchodzi w życie z dniem podjęcia.

PREZES ZARZĄDU
SM „AR-Moczydło"
Anna Skutkiewicz

WICEPREZES ZARZĄDU
SM „AR-Moczydło"
Zbigniew Furman

KSIĘGA PROCEDUR

SPÓŁDZIELNI MIESZKANIOWEJ „AR-MOCZYDŁO”

W WARSZAWIE

WARSZAWA, 2/12/ 2020 r.

SPIS TREŚCI

I. DEFINICJE I SKRÓTY

Poniżej przedstawiono specyficzne pojęcia, definicje i skróty przywołane w niniejszej Księdze Procedur:

Adekwatność przetwarzania danych – przetwarzanie danych osobowych w zakresie niezbędnym ze względu na cel zbierania danych

Administrator – podmiot decydujący o celach i sposobach przetwarzania danych osobowych. Administratorem danych osobowych objętych niniejszą Księgą Procedur jest Spółdzielnia Mieszkaniowa „AR-Moczydło" w Warszawie, ul. Mielczarskiego 8, 02-798 Warszawa wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy pod numerem 0000112158, NIP 5250011119, REGON 010143973. Administrator wykonuje swoje obowiązki za pośrednictwem swoich pracowników oraz osób, które z Administratorem łączy inny stosunek.

Dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można bezpośrednio lub pośrednio zidentyfikować.

Hasło – ciąg znaków literowych, cyfrowych lub innych.

Incydent – każde zdarzenie lub seria zdarzeń, które nie są częścią normalnego działania mogące grozić bezpieczeństwu przetwarzania danych osobowych.

IODO – Inspektor Ochrony Danych Osobowych.

Login – ciąg znaków literowych, cyfrowych lub innych.

Odbiorca danych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, którym ujawnia się dane osobowe.

Ograniczenie przetwarzania – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Operacje na danych osobowych – czynności podejmowane w związku z danymi osobowymi, w szczególności zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

Organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych.

Osoba, którą z Administratorem łączy inny stosunek – osoba współpracująca z Administratorem w ramach umowy cywilnoprawnej, umowy o współpracę lub innej umowy nienazwanej, w wyniku powołania innego niż określone w Kodeksie pracy, praktykant, stażysta, wolontariusz osoba skierowana przez agencję pracy tymczasowej.

Osoba Upoważniona – osoba upoważniona do dostępu lub przetwarzania danych osobowych przez Administratora na podstawie wewnętrznych uregulowań, posiadająca upoważnienie wydane przez Administratora lub osobę przez niego upoważnioną, w zakresie wskazanym w upoważnieniu oraz osoby sprawujące nadzór lub kontrolę. Wzór upoważnienia stanowi załącznik nr 1 do niniejszej Księgi Procedur.

Podejrzenie naruszenia bezpieczeństwa danych – uzasadnione przekonanie, iż doszło w szczególności do dostępu do danych osobowych, systemu informatycznego przez osoby nieupoważnione, nieuprawnionej modyfikacji lub zniszczenia danych osobowych, nieuprawnionego udostępnienia lub ujawnienia danych osobowych, pozyskiwania danych osobowych z nielegalnych źródeł, kradzieży nośników zawierających dane osobowe, zagrożenia spowodowanego wirusami komputerowymi lub programami o podobnym przeznaczeniu, wystąpienia zdarzeń losowych, nieprzestrzegania przepisów prawa lub wewnętrznych regulacji dotyczących ochrony danych osobowych i związanych z tym procedur.

Pracownik – osoba zatrudniona u Administratora na podstawie umowy o pracę, powołania lub wyboru.

Prawo spółdzielcze – ustawa z dnia 16 września 1982 r. Prawo spółdzielcze (Dz.U. z 2020 r., poz. 275 t.j. ze zm.).

Profilowanie – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które podlega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Przetwarzanie danych – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwiej do zidentyfikowania osoby fizycznej.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania danych osobowych i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.

Ustawa o spółdzielniach mieszkaniowych – ustawa z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (Dz.U. z 2020 r., poz. 1465 t.j. ze zm.).

Ustawa o własności lokali – ustawa z dnia 24 czerwca 1994 r. o własności lokali (Dz.U. z 2020 r., poz. 532 t.j. ze zm.).

Zabezpieczenia – wdrożenie i eksploatacja odpowiednich środków technicznych i organizacyjnych, mających na celu ochronę danych osobowych przed ich nieuprawnionym przetwarzaniem oraz dostępem osób nieupoważnionych.

Zbiór danych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie czy geograficznie.

II. POSTANOWIENIA OGÓLNE

§ 1 Definicja, zakres i cele bezpieczeństwa danych

1. Bezpieczeństwo danych ma na celu ich ochronę przed nieautoryzowanym dostępem lub zmianą. Polega na zabezpieczeniu informacji w zakresie:
   a) poufności – zapewnianie ciągłej poufności, dostęp do informacji jedynie dla osób posiadających upoważnienie oraz uniemożliwienie dostępu do informacji osobom nieupoważnionym,
   b) integralności – zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania, a także uniknięcie nieautoryzowanych zmian w danych,
   c) dostępności – zapewnienie Osobom Upoważnionym dostępu do informacji i związanych z nim aktywności,
   d) przejrzystości – zapewnienie aby wszystkie komunikaty związane z przetwarzaniem danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem,
   e) adekwatności – zapewnienie aby dane były zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach, w zakresie niezbędnym dla tych celów,
   f) rozliczalności operacji – zapewnienie możliwości wykazania przestrzegania obowiązujących regulacji, przetwarzanie danych w sposób rzetelny i przejrzysty.

2. Administrator stosuje adekwatne do sytuacji środki aby zapewnić bezpieczeństwo informacji.

§ 2 Zakres Księgi Procedur

1. Księga Procedur odnosi się do danych osobowych przetwarzanych w formie papierowej oraz w systemach informatycznych.
2. Księga Procedur obowiązuje Administratora, jego organy, członków, osoby, którym przysługują prawa do lokali oraz podmioty i osoby, z którymi Administrator współpracuje.
3. Administrator może zobowiązać do złożenia oświadczenia, które stanowi załącznik nr 2 do niniejszej Księgi Procedur.

§ 3 Cele Księgi Procedur i ich realizacja

1. Celami Księgi Procedur są:
   a) stworzenie i utrzymanie wysokiego poziomu bezpieczeństwa danych osobowych zgodnie z przepisami prawa,
   b) zapewnienie maksymalnej możliwej ochrony danych osobowych oraz wdrożenie zasad i procedur zapewniających odpowiedni poziom bezpieczeństwa danych osobowych,
   c) maksymalne ograniczenie ryzyka nieuprawnionego przetwarzania lub utraty danych osobowych,
   d) określenie zasad postępowania w sytuacjach zagrożenia, awarii i sytuacji kryzysowych,
   e) zwiększenie zdolności do zapobiegania i zwalczania zagrożeń,
   f) zmniejszenie skutków incydentów i sytuacji kryzysowych,
   g) stworzenie trwałego systemu kontroli bezpieczeństwa danych osobowych.
2. Wskazane powyżej cele realizowane zostaną poprzez:
   a) podejmowanie wszelkich działań niezbędnych do ochrony danych osobowych,
   b) stosowanie odpowiednich środków, urządzeń i oprogramowania wykorzystywanych do przetwarzania oraz zabezpieczania danych osobowych,
   c) stałe rozwijanie, modyfikowanie i dostosowywanie środków ochrony danych osobowych odpowiednich do niebezpieczeństw i zagrożeń.

III. ZASADY, STANDARDY I WYMAGANIA

§ 4 Zgodność z prawem

Dane osobowe chronione są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, w szczególności:

1. przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r., poz. 1781 t.j. ze zm.) oraz aktów wykonawczych, które zostały wydane na jej podstawie,
2. przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (RODO),
3. innych przepisów ustaw i rozporządzeń normujących przetwarzanie danych osobowych określonej kategorii.

§ 5 Zapewnienie odpowiedniego poziomu bezpieczeństwa

1. Administrator w celu osiągnięcia wysokiego poziomu bezpieczeństwa podejmuje aktywności w postaci w stałej identyfikacji zagrożeń, szacowania, analizy i oceny ryzyka w celu ustalenia prewencyjnych wytycznych zabezpieczenia przed wystąpieniem sytuacji kryzysowych, ograniczenia wystąpienia sytuacji awaryjnej oraz utrzymywaniu gotowości do natychmiastowej reakcji gdyby takowa zaistniała.
2. Dla tych celów Administrator w szczególności podejmuje działania:
   a) dokonuje cyklicznie kontroli zastosowanych środków bezpieczeństwa oraz przestrzegania instrukcji,
   b) każdego pracownika oraz osobę, którą z Administratorem łączy inny stosunek obowiązuje kontrola stanowiskowa, a więc działania polegające na kontroli przestrzegania obowiązujących przepisów prawa oraz wewnętrznych aktów sporządzonych przez Administratora dotyczących ochrony danych osobowych, a także funkcjonowania zastosowanych środków bezpieczeństwa, regularnym

badaniu czy doszło do naruszenia bezpieczeństwa danych osobowych oraz zastosowaniu się do procedur.

§ 6 Osoby wspierające Administratora

1. Administrator może w każdym czasie wyznaczyć IODO, który działa i realizuje zadania na zasadach określonych w RODO. Administrator niezwłocznie zawiadomi organ nadzorczy o wyznaczaniu IODO oraz przekaże jego dane.
2. W przypadku niewyznaczenia IODO, Administrator może powołać osobę odpowiedzialną za monitorowanie kwestii dotyczących przetwarzania danych osobowych (np. pełnomocnik do spraw przetwarzania danych osobowych). W dokumencie powołującym osobę odpowiedzialną za monitorowanie kwestii dotyczących przetwarzania danych osobowych wskazany zostanie przez Administratora zakres obowiązków i uprawnień.

§ 7 Wymagania dotyczące kształcenia w dziedzinie bezpieczeństwa danych

1. W celu podniesienia kwalifikacji istnieje konieczność przeprowadzenia cyklicznych szkoleń w zakresie bezpieczeństwa informacji przeznaczonych dla Osób Upoważnionych odpowiednio do zajmowanego stanowiska i ryzyka z nim związanego.
2. Administrator określi konieczność przeprowadzenia szkolenia oraz jego termin według własnego uznania, jednak nie rzadziej niż raz na 5 lat. Wyjątkiem jest wprowadzenie nowych regulacji prawnych, które wymaga przeprowadzenia szkolenia niezwłocznie w celu zapoznania Osób Upoważnionych z nowymi wymogami.

§ 8 Postępowanie w przypadku naruszenia Księgi Procedur

1. Wszelkie podejrzenia naruszenia Księgi Procedur należy niezwłocznie zgłaszać Administratorowi w formie pisemnej lub za pośrednictwem poczty elektronicznej na adres e-mail ..... W wyjątkowych i nagłych wypadkach takie zgłoszenie może zostać dokonane w formie ustnej, jednakże powinno ono zostać

potwierdzone przez zgłaszającego w formie pisemnej lub za pośrednictwem poczty elektronicznej, niezwłocznie po uzyskaniu takiej możliwości.

2. Każdy incydent jest odnotowywany, zaś Administrator podejmuje stosowne środki zaradcze, dokonuje analizy zaistniałego ryzyka oraz wprowadza procedury zapobiegające ponownemu zaistnieniu takiego incydentu.
3. Administrator może okresowo wykonywać wewnętrzną lub zewnętrzną kontrolę bezpieczeństwa mającą na celu wykrycie ewentualnych uchybień w realizacji niniejszej Księgi Procedur.
4. Naruszenie Księgi Procedur może powodować powstanie roszczeń odszkodowawczych lub poinformowanie organów ścigania w przypadku celowego naruszenia bezpieczeństwa.
5. Administrator może wyciągnąć konsekwencje przewidziane w Kodeksie Pracy i innych aktach prawnych w zależności od rodzaju stosunku łączącego Osoby Upoważnione i Administratora oraz od rodzaju skutków naruszeń.
6. Administrator w związku z naruszeniem Księgi Procedur może ze skutkiem natychmiastowym odebrać uprawnienia Osobom Upoważnionym. Formularz odebrania uprawnień przechowywany jest w aktach osobowych Osoby Upoważnionej.

IV. OBOWIĄZKI W ODNIESIENIU DO ZARZĄDZANIA BEZPIECZEŃSTWEM DANYCH

§ 9 Obowiązki w odniesieniu do zarządzania bezpieczeństwem danych

Do obowiązków Administratora należy w szczególności:

a) sporządzanie wewnętrznych aktów dotyczących ochrony danych osobowych i procedur z tym związanych,
b) nadzór nad przestrzeganiem przepisów prawa oraz wewnętrznych regulacji dotyczących ochrony danych osobowych i związanych z tym procedur,
c) zapewnienie środków organizacyjnych i technicznych zapewniających zabezpieczenie danych przed dostępem osób nieupoważnionych odpowiednich do zagrożeń oraz chronionych danych osobowych, a także monitorowanie ich funkcjonowania,
d) wydawanie i przechowywanie upoważnień dla Osób Upoważnionych,

e) weryfikacja zakresu przetwarzanych danych osobowych pod kątem adekwatności,
f) prowadzenie rejestru czynności przetwarzania, jeżeli jest to wymagane,
g) pseudonimizowanie przetwarzanych danych osobowych,
h) spełnianie obowiązku informacyjnego,
i) podejmowanie działań w przypadku wykrycia sytuacji zagrożenia, kryzysowych i awarii oraz innych incydentów, a także analiza sytuacji, ich okoliczności i przyczyn.

§ 10 Obowiązki i odpowiedzialność Osób Upoważnionych

1. Każda Osoba Upoważniona zobowiązana jest do:
   a) utrzymania w tajemnicy danych, które zostały jej udostępnione,
   b) ochrony danych osobowych oraz utrzymania właściwego poziomu bezpieczeństwa danych osobowych,
   c) zapoznania się z przepisami prawa, Księgą Procedur i innymi aktami dotyczącymi ochrony danych osobowych, a także złożenia oświadczenia, które stanowi załącznik nr 2 do niniejszej Księgi Procedur,
   d) przetwarzania danych osobowych zgodnie z Księgą Procedur i innymi aktami dotyczącymi bezpieczeństwa danych osobowych,
   e) niezwłocznego zgłaszania Administratorowi wszelkich podejrzeń naruszenia bezpieczeństwa danych osobowych, zgodnie z § 24.
   f) udziału w szkoleniach, o których mowa w § 7.
2. W przypadku niewykonania powyższych zobowiązań Administrator może wyciągnąć konsekwencje przewidziane w Kodeksie Pracy i innych aktach prawnych w zależności od rodzaju stosunku łączącego Osobę Upoważnioną i Administratora oraz od rodzaju skutków naruszeń.

V. ZBIORY DANYCH OSOBOWYCH I ZASTOSOWANE ŚRODKI

§ 11 Zbiory danych osobowych

1. Administrator przetwarza dane osobowe w szczególności członków, właścicieli, najemców, pracowników, osób których z Administratorem łączy inny stosunek oraz osób, z którymi Administrator zawarł inną umowę.
2. Administrator sprawuje nadzór nad rodzajami i zawartością zbiorów danych osobowych.
3. Administrator nie tworzy zbiorów danych osobowych i nie gromadzi innych danych osobowych niż niezbędne do realizacji celów.
4. Administrator przetwarza dane osobowe głównie w celu realizacji praw i obowiązków wynikających z Prawa spółdzielczego, Ustawy o spółdzielniach mieszkaniowych, Ustawy o własności lokali oraz obowiązków wynikających z innych powszechnie obowiązujących przepisów.
5. Administrator może także przetwarzać dane osobowe na podstawie prawnie uzasadnionego interesu, polegającego w szczególności na zapewnieniu bezpieczeństwa i ochrony osób i mienia, dbałości o zabezpieczenie i zgodne z przepisami korzystanie z nieruchomości zarządzanych przez Administratora, zapobieganie pogorszenia stanu nieruchomości oraz zapewnienie prawidłowej gospodarki finansowej.
6. Administrator w celu wykonania obowiązków wynikających z powszechnie obowiązujących przepisów prawa może przetwarzać dane o stanie zdrowia, dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym i administracyjnym.
7. Administrator może przetwarzać dane osobowe także na podstawie zgody osoby, której dane dotyczą. Wzór zgody stanowi załącznik nr 3 do niniejszej Księgi Procedur.

§ 12 Środki techniczne i organizacyjne niezbędne dla zapewnienia bezpieczeństwa danych

1. Środki techniczne i organizacyjne mają na celu w szczególności zabezpieczenie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez takie osoby, przetwarzaniem z naruszeniem przepisów prawa, a także nieuprawnioną zmianą, utratą uszkodzeniem lub zniszczeniem.
2. Wprowadzając środki techniczne i organizacyjne Administrator uwzględnia ryzyka wiążące się z przetwarzaniem danych osobowych.

3. Do potencjalnych zagrożeń dla bezpieczeństwa przetwarzania danych osobowych należą:
   a) zamierzone działania ludzkie mające na celu nieautoryzowane przetwarzanie danych osobowych – uszkodzenie zabezpieczeń fizycznych np. włamanie,
   b) działania Osoby Upoważnionej, które w sposób przypadkowy mogą doprowadzić do nieautoryzowanego przetwarzania danych osobowych – udostępnianie stanowisk pracy osobom nieuprawnionym, utrata dokumentu zwierającego dane osobowe, nieodpowiednie niszczenie dokumentów zawierających dane osobowe, pozostawienie dokumentów w ogólnodostępnych miejscach, niezastosowanie środków zabezpieczających pomieszczenie, w którym przetwarzane są dane osobowe, niezastosowanie się do powszechnie obowiązujących i wewnętrznych aktów dotyczących bezpieczeństwa danych osobowych,
   c) zdarzenia losowe – pożar, powódź, zalanie, włamanie, kradzież.
4. Jeżeli przetwarzanie danych osobowych ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania danych dokona oceny skutków planowanych operacji.

§ 13 Środki techniczne

1. Wszelka dokumentacja papierowa zawierająca dane osobowe oraz nośniki informacji zawierające dane osobowe muszą być przechowywane w zamykanych na klucz szafach lub stale przytwierdzonych sejfach.
2. Administrator dąży aby wejście do budynków lub pomieszczeń, w których przetwarza się dane osobowe lub przechowuje się wszelką dokumentację oraz nośniki informacji chronione były drzwiami otwieranymi kluczem.
3. Administrator może zabezpieczyć budynki, w których przetwarza się dane osobowe lub przechowuje się wszelką dokumentację oraz nośniki informacji zawierające dane osobowe poprzez monitoring, system alarmowy w postaci czujników ruchu lub czujniki przeciwpożarowych.
4. Dane osobowe zawarte w dokumentach papierowych zawsze muszą być usuwane za pomocą niszczarki.

5. Urządzenia elektroniczne ustawione są w sposób uniemożliwiający wgląd do danych osobowych przez osoby postronne.

§ 14 Środki organizacyjne

1. Administrator opracowuje wewnętrzne akty dotyczące ochrony danych osobowych oraz wdraża postanowienia w nich zawarte.
2. Administrator wyznacza osoby odpowiedzialne za nadzór i kontrolę nad bezpieczeństwem danych osobowych.
3. Osoby odpowiedzialne za nadzór i kontrolę nad bezpieczeństwem danych osobowych:
   a) dokonują cyklicznej kontroli budynków lub pomieszczeń, w których przetwarza się dane osobowe lub przechowuje się wszelkie nośniki informacji zawierające dane osobowe oraz monitorują zabezpieczenia systemów informatycznych.
   b) dokonują cyklicznej oceny ryzyk oraz rejestracji przypadków naruszeń i awarii.
4. Administrator ogranicza dostęp do danych tylko dla osób odpowiednio przeszkolonych oraz znających powszechnie obowiązujące i wewnętrzne akty dotyczące ochrony danych osobowych.
5. Administrator wydaje klucze uprawniające do wejścia do budynków lub pomieszczeń, w których wykonuje się operacje na danych osobowych lub przechowuje się wszelkie nośniki informacji zawierające dane osobowe jedynie Osobom Upoważnionym.
6. Zakazane jest przenoszenie danych osobowych poza obszar, na którym przetwarza się dane osobowe lub przechowuje się nośniki informacji zawierające dane osobowe. W przypadku upoważnionego przenoszenia danych osobowych poza wskazany obszar, konieczne jest ich zabezpieczenie.

§ 15 Udostępnianie i powierzanie danych osobowych

1. Zgromadzone w zbiorach dane osobowe są przekazywane lub powierzane przez Administratora podmiotom uprawnionym na mocy obowiązujących przepisów prawa.
2. Administrator powierza przetwarzanie danych osobowych na podstawie umowy, której wzór stanowi załącznik nr 4 do niniejszej Księgi Procedur lub innego instrumentu prawnego, które 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. Umowa lub inny instrument prawny mają formę pisemną lub formę elektroniczną.

3. Administrator jest uprawniony do kontroli podmiotu, któremu powierzył przetwarzanie danych osobowych.
4. Zgromadzone w zbiorach dane osobowe są przekazywane przez Administratora organom administracji państwowej i samorządowej w celu spełnienia obowiązków wynikających z obowiązujących przepisów prawa.
5. Zgromadzone w zbiorach dane osobowe mogą być przekazywane przez Administratora członkom oraz osobom posiadającym prawa do lokali, w niezbędnym zakresie, który nie utrudnia lub uniemożliwia realizacji obowiązków Administratora, w celu realizacji przez członków lub te osoby uprawnień wynikających z obowiązujących przepisów prawa. Dane te są przekazywane po zweryfikowaniu tożsamości albo uprawnień członków lub osób posiadających prawo do lokali. Dla zapewnienia bezpieczeństwa danych osobowych Administrator może określić terminy zapoznawania się z dokumentacją papierową lub elektroniczną oraz ograniczyć możliwość kopiowania i fotografowania. Wykonanie kserokopii następuje wyłącznie na koszt członka. Członek zobowiązany jest do złożenia oświadczenia o przestrzeganiu regulacji dotyczących ochrony danych osobowych oraz zachowania ich w poufności, którego wzór stanowi załącznik nr 5 do niniejszej Księgi Procedur.
6. Administrator sprawuje nadzór nad tym jakie dane i w jakim zakresie, a także komu zostały powierzone lub udostępnione poprzez prowadzenie rejestru udostępnionych danych osobowych, którego wzór stanowi załącznik nr 6 do niniejszej Księgi Procedur.
7. Administrator nie be□dzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których naste□puje to na wniosek osoby, której dane dotycza□.

VI. INSTRUKCJE POSTĘPOWANIA

§ 16 Instrukcja postępowania w kontaktach z osobami, których dane osobowe są przetwarzane oraz w przypadku zgłaszania żądań przez te osoby

1. Administrator niezwłocznie poinformuje osobę, której dane są przetwarzane między innymi o danych Administratora, podstawach przetwarzania, celach przetwarzania, okresie przetwarzania danych, przysługujących prawach. Informacja ta może być udzielona na pisemnie lub w inny sposób, także elektronicznie. Wzór informacji stanowi załącznik nr 7 do niniejszej Księgi Procedur.
2. Jeżeli dane osobowe przetwarzane są na podstawie zgody osoby, której dane dotyczą, zgoda ta musi być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, konkretne, świadome i jednoznaczne okazanie woli tej osoby. Wyrażona może zostać w formie pisemnej, elektronicznej, ustnej lub innej, która pozwala na wykazanie, że zgoda została wyrażona. Zgoda powinna dotyczyć wszystkich czynności przetwarzania. Zgoda ta może być w dowolnym momencie wycofana.
3. Przetwarzanie danych osobowych do celów innych niż cele, w których dane te zostały pierwotnie zebrane, dozwolone jest w przypadkach, gdy jest zgodne z celami, w których dane osobowe zostały pierwotnie zebrane.
4. Administrator zapewnia możliwość wnoszenia żądań także droga elektroniczną, w szczególności gdy dane osobowe są przetwarzane drogą elektroniczną.
5. Administrator powinien udzielić odpowiedzi na żądania bez zbędnej zwłoki, najpóźniej w terminie miesiąca, a jeżeli nie zamierza spełnić tego żądania, podać tego przyczyny.
6. Administrator bez zbędnej zwłoki, najpóźniej w terminie miesiąca od otrzymania żądania, udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem. Z uwagi na skomplikowany charakter żądania lub liczbę żądań, termin może zostać przedłużony o kolejne dwa miesiące, o czym należy poinformować z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądnie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.
7. W przypadku żądania osoby, której dane dotyczą, osoba ta ma dostęp do swoich danych w zakresie:
   a) potwierdzenia czy przetwarzane są jej dane,
   b) jakie są cele przetwarzania,
   c) jakie są kategorie danych,
   d) informacji o odbiorcach lub kategorii odbiorców,

e) w miarę możliwości planowany okres przechowywania danych lub kryteria ustalania tego okresu,
f) informacje o prawie do sprostowania, ograniczenia lub usunięcia,
g) informacji o prawie wniesienia skargi,
h) informacje o źródle danych, jeśli Administrator nie zostały zebrane od osoby, której dane dotyczą,
i) informacji czy decyzja podejmowana jest w formie zautomatyzowanej i zasadach oraz konsekwencjach takiego podejmowania decyzji
j) kopię danych osobowych podlegających przetwarzaniu (za kopie Administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych).

8. W przypadku żądania sprostowania, uzupełnienia, ograniczenia lub usunięcia danych, Administrator bez zbędnej zwłoki podejmuje odpowiednie czynności.
9. W przypadku wniesienia sprzeciwu przez osobę, której dane dotyczą, Administrator nie przetwarza tych danych osobowych, chyba że istnieją ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

§ 17 Instrukcja uzyskania dostępu do budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane lub przechowywane są nośniki informacji zawierające dane osobowe

1. Wstęp do budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane lub przechowywane są nośniki informacji zawierające dane osobowe mają wyłącznie Osoby Upoważnione, z zastrzeżeniem pkt 4 i 5.
2. Osoba Upoważniona, której przyznano klucz potwierdza jego otrzymanie oraz oświadcza, iż znane są jej konsekwencje jego utraty.
3. Osoby Upoważnione zobowiązane są zamykać pomieszczenia, w których przetwarza się dane osobowe lub przechowuje się wszelkie nośniki informacji zawierające dane osobowe każdorazowo podczas ich nieobecności (nawet czasowej) oraz po zakończeniu pracy, chyba że w pomieszczeniu pozostaje inna Osoba Upoważniona.

4. Osoby nieupoważnione, mające interes prawny w uzyskaniu dostępu do danych mogą przebywać w budynkach, pomieszczeniach i częściach pomieszczeń, w których przetwarzane są dane osobowe, wyłącznie w obecności Osoby Upoważnionej, poza wyjątkami wskazanymi poniżej.
5. Dostęp osób nieupoważnionych pod nieobecność Osoby Upoważnionej jest możliwy alternatywnie:
    a) jeżeli dane osobowe zostały odpowiednio zabezpieczone przed dostępem do nich osób nieupoważnionych w sposób nie budzący wątpliwości,
    b) w obecności osoby upoważnionej do dostępu do danych osobowych o innym zakresie upoważnienia niż nieobecna Osoba Upoważniona,
    c) w obecności osób, które zostały upoważnione przez Administratora wyłącznie do dostępu do budynków, pomieszczeń i części pomieszczeń, w których przetwarzane są dane osobowe.
6. Niezastosowanie się do powyższych regulacji skutkować może wyciągnięciem przez Administratora konsekwencji przewidzianych w Kodeksie Pracy i innych aktach prawnych w zależności od rodzaju stosunku łączącego Osobę Upoważnioną i Administratora oraz od rodzaju skutków naruszeń.

§ 18 Instrukcja postępowania z dokumentami w formie papierowej oraz nośnikami informacji zawierającymi dane osobowe

1. Wstęp do budynków, pomieszczeń lub części pomieszczeń, w których przechowywane są dokumenty w formie papierowej oraz nośniki informacji zawierające dane osobowe mają wyłącznie Osoby Upoważnione po zachowaniu procedury określonej w § 17.
2. Osoby Upoważnione, które przetwarzają dane w formie papierowej oraz na nośnikach informacji zobowiązane są do zabezpieczania ich przed dostępem osób nieupoważnionych poprzez przechowywanie ich w zamkniętych na klucz szafach bądź sejfach.
3. Nieużywane dokumenty oraz nośniki informacji należy niezwłocznie chować w zamkniętych na klucz szafach bądź sejfach.
4. Dokumenty papierowe i nośniki informacji zawierające dane osobowe pracowników Administratora oraz osób, które z Administratorem łączy inny stosunek przechowywane są w zamkniętych na klucz szafach lub sejfach.

5. Dokumenty papierowe zawierające dane osobowe przekazywane są w kopercie zabezpieczonej przed dostępem osób nieupoważnionych.
6. Zakazane jest pozostawienie niezabezpieczonych dokumentów lub nośników informacji bez nadzoru w trakcie pracy, a także po zakończonej pracy.
7. Zakazane jest pozostawianie wydruków w miejscu ogólnodostępnym. Wydruki zawierające dane osobowe po zakończeniu pracy należy chować do zamykanej na klucz szafy bądź sejfu.
8. Zakazane jest przenoszenie dokumentów i nośników informacji poza obszar, na którym przetwarza się dane osobowe lub przechowuje się nośniki informacji zawierające dane osobowe. W przypadku upoważnionego przenoszenia dokumentów, konieczne jest ich zabezpieczenie przed dostępem osób nieupoważnionych, zaś w przypadku nośników informacji konieczne jest ich pseudonimizowanie (a przynajmniej zabezpieczenie hasłem).
9. Niszczenie dokumentów wykonuje się za pomocą odpowiednich narzędzi (np. niszczarki) po ustaniu ich użyteczności. Do momentu zniszczenia dokumenty należy przechowywać w miejscu uniemożliwiającym dostęp osób nieupoważnionych.
10. Z nośników informacji, które zostały uznane za nieprzydatne, usuwa się zapisane na nich dane w sposób trwały (uniemożliwiający ich odtworzenie). Przez zniszczenie elektronicznego nośnika informacji rozumie się trwałe i nieodwracalne zniszczenie fizyczne do stanu niedającego możliwości ich rekonstrukcji i odzyskania danych.
11. W przypadku korzystania z podmiotu profesjonalnie zajmującego się niszczeniem dokumentów papierowych lub nośników informacji konieczne jest zawarcie odpowiedniej umowy, w której zostanie powierzone przetwarzanie danych osobowych oraz zwarte zobowiązanie do zachowania poufności.

§ 19 Instrukcja archiwizacji dokumentów papierowych i nośników informacji zawierających dane osobowe archiwalne

1. Dane osobowe archiwalne przechowywane są w zamkniętych szafach lub sejfach w budynkach, pomieszczeniach lub częściach pomieszczeń, innych niż, te w których przechowywane są dane aktualne.

2. Dokumenty papierowe oraz nośniki informacji zawierające dane osobowe archiwalne przechowuje się w oznaczonych pudłach lub segregatorach w miejscach zabezpieczonych przed dostępem osób nieupoważnionych (w szczególności w szafach, odrębnych pomieszczeniach).
3. Wydanie kopii archiwalnego dokumentu papierowego lub nośnika informacji zawierającego dane osobowe następuje na wniosek Osoby Upoważnionej. Od momentu wydania kopii wnioskująca Osoba Upoważniona jest za nią odpowiedzialna do chwili jej zniszczenia.
4. W wyjątkowych wypadkach istnieje możliwość wydania oryginału dokumentu papierowego lub nośnika informacji zawierającego dane osobowe archiwalne. Wnioskująca Osoba Upoważniona zobowiązana jest do zwrotu oryginału niezwłocznie po ustaniu konieczności jego posiadania.

§ 20 Instrukcja przetwarzania danych osobowych w formie elektronicznej

1. Przetwarzać dane osobowe w systemie informatycznym mogą Osoby Upoważnione wyłącznie po wprowadzeniu loginu oraz hasła.
2. Wszelkie hasła pozostają tajne. Każda Osoba Upoważniona jest zobowiązana do zachowania w tajemnicy swoich haseł, także po ich zmianie oraz do nieprzechowywania ich w formie zmaterializowanej w miejscu dostępnym dla osób nieupoważnionych.
3. Wprowadzanie hasła jest czynnością poufną, podczas wprowadzania hasło nie może być widoczne na ekranie monitora w postaci jawnej.
4. W przypadku podejrzenia, że hasło mogła poznać osoba nieuprawniona, Osoba Upoważniona zobowiązana jest do natychmiastowej zmiany hasła.
5. Zastosowane są mechanizmy automatycznej blokady dostępu do systemu informatycznego w przypadku nieaktywności Osoby Upoważnionej przez okres dłuższy niż 10 min.
6. W przypadku czasowego zawieszenia pracy Osoba Upoważniona powinna co najmniej aktywować wygaszacz ekranu z hasłem lub w inny sposób zablokować dostęp osób nieupoważnionych do urządzenia, z którego korzysta (np. wylogowanie się).
7. Osoba Upoważniona zobowiązana jest zabezpieczyć wszelkie elektroniczne nośniki danych przed dostępem osób nieupoważnionych.

8. Po zakończeniu pracy Osoba Upoważniona zobowiązana jest do zakończenia pracy w systemie informatycznym, wylogowania się z systemu informatycznego i wyłączenia urządzeń, z których korzystała.
9. Osoba Upoważniona zobowiązana jest do zabezpieczenia elektronicznych nośników danych w sposób uniemożliwiający dostęp osób nieupoważnionych.
10. Zakazane jest korzystanie z nośników wymiennych nieznanego pochodzenia.
11. Zakazane jest podłączanie urządzeń do obcych sieci Internet.
12. Zakazane jest wykorzystywanie urządzeń służbowych do celów prywatnych.
13. Wykorzystywać można programy pochodzące wyłącznie z legalnego źródła.
14. Zakazane jest dokonywanie zmian konfiguracji systemu oraz oprogramowania.
15. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.
16. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez zastosowanie oprogramowania zabezpieczającego przed oddziaływaniem szkodliwego oprogramowania.
17. W przypadku przekazywania danych osobowych w formie elektronicznej, muszą zostać zabezpieczone za pomocą jednorazowego hasła. Hasło to udostępniane jest poprzez przesłanie odrębnej wiadomości za pośrednictwem poczty elektronicznej lub wiadomości sms.
18. Ponadto każda Osoba Upoważniona zobowiązana jest w szczególności do:
    a) ochrony danych osobowych oraz utrzymania właściwego poziomu bezpieczeństwa danych osobowych,
    b) wskazywania konieczności zmian w funkcjonalności systemu informatycznego w celu poprawy bezpieczeństwa,
    c) niezwłocznego zgłaszania wszelkich podejrzeń naruszenia bezpieczeństwa systemu informatycznego,
    d) nieudostępniania osobom nieupoważnionym urządzeń wykorzystywanych do pracy oraz programów pracujących w systemie,
    e) nietworzenia nieautoryzowanych kopii danych osobowych.
19. W przypadku niewykonania powyższych zobowiązań Administrator może wyciągnąć konsekwencje przewidziane w Kodeksie Pracy i innych aktach prawnych w zależności od rodzaju stosunku łączącego Osobę Upoważnioną i Administratora oraz od rodzaju skutków naruszeń.

§ 21 Instrukcja postępowania w zakresie komunikacji elektronicznej

1. Wszelkie pliki zawierające kopie danych osobowych zawartych w systemie, wysyłane poza system, muszą być zabezpieczone hasłem. Hasło to udostępniane jest poprzez przesłanie odrębnej wiadomości za pośrednictwem poczty elektronicznej lub wiadomości sms.
2. Zakazane jest przesyłanie danych osobowych osobom, których tożsamość nie została zweryfikowana w zwyczajowo przyjęty sposób (np. zewidencjonowany e-mail).
3. Zakazane jest otwieranie plików nieznanego pochodzenia.
4. Nieuzasadnione kopiowanie danych jest zabronione.

§ 22 Monitoring

1. Administrator w celu zapewnienia bezpieczeństwa i ochrony osób i mienia, dbałości o zabezpieczenie i zgodne z przepisami korzystanie z nieruchomości zarządzanych przez Administratora oraz zapobiegania pogorszenia stanu nieruchomości wykorzystuje system monitoringu na terenie objętym działaniami Administratora, który rejestruje wizerunek osób fizycznych.
2. Strefa objęta monitoringiem została określona w załączniku nr 8 do niniejszej Księgi Procedur.
3. Osoby przebywające w strefie objętej monitoringiem zostaną poinformowane przez administratora o tym fakcie poprzez zamieszczone tablice informujące o prowadzonym monitoringu ze wskazaniem danych Administratora oraz określeniem miejsca, gdzie można zapoznać się z pełną treścią klauzuli informacyjnej.
4. Obsługę monitoringu prowadzą osoby upoważnione przez Administratora lub przez podmiot trzeci, z którym Administrator zawarł stosowną umowę.
5. Dane osobowe zawarte w nagraniach monitoringu są przekazywane przez Administratora organom administracji państwowej i samorządowej wyłącznie we wskazanym przez nich zakresie, w celu spełnienia obowiązków wynikających z obowiązujących przepisów prawa.
6. Dane osobowe zawarte w nagraniach monitoringu mogą zostać przekazywane przez Administratora innym osobom na zasadach określonych w § 15 Księgi

Procedur w celu spełnienia obowiązków wynikających z obowiązujących przepisów prawa lub obrony swoich praw.

7. Dane osobowe rejestrowane przez system monitoringu przechowywane będą maksymalnie przez zakres 3 miesięcy, a po tym okresie zostaną przez Administratora trwale usunięte. Wyjątkiem jest uzasadniona konieczne będzie zabezpieczenie określonego fragmentu nagrania w dłuższym terminie.
8. W celu ochrony danych stosowane są środki zabezpieczające na zasadach wskazanych w § 12, § 13 i § 14 niniejszej Księgi Procedur.

§ 23 Instrukcja prowadzenia rejestru czynności przetwarzania

1. Administrator może prowadzić rejestry czynności przetwarzania w formie papierowej lub elektronicznej. Wzór rejestru stanowi załącznik nr 9 do niniejszej Księgi Procedur.
2. Rejestry są na bieżąco aktualizowane.
3. W rejestrze czynności przetwarzania dokonywanego przez Administratora zamieszcza się informacje:
   a) nazwę oraz dane kontaktowe Administratora, wszelkich współadministratorów oraz IODO jeśli został powołany,
   b) cele przetwarzania,
   c) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych,
   d) kategorie odbiorców, którym dane zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
   e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a także dokumentacja odpowiednich zabezpieczeń, jeśli wymagają tego przepisy,
   f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
   g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
4. Jeżeli Administrator będzie przetwarzał dane na podstawie powierzenia przetwarzania, zobowiązany jest do prowadzenia rejestru kategorii czynności przetwarzania zawierający informacje:

a) nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz IODO,
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
c) gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej,a także dokumentacja odpowiednich zabezpieczeń, jeśli wymagają tego przepisy,
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

5. Rejestry udostępniane są organowi nadzorczemu na jego żądanie.

§ 24 Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych lub awarii

1. Wszelkie podejrzenia naruszenia bezpieczeństwa danych osobowych należy niezwłocznie (najpóźniej w terminie 1h od wykrycia) zgłaszać do Administratora w formie pisemnej lub za pośrednictwem poczty elektronicznej na adres ..... W wyjątkowych i nagłych wypadkach takie zgłoszenie może zostać dokonane w formie ustnej, jednakże powinno ono zostać potwierdzone przez zgłaszającego w formie pisemnej lub za pośrednictwem poczty elektronicznej, niezwłocznie po uzyskaniu takiej możliwości.
2. W razie stwierdzenia naruszenia bezpieczeństwa danych osobowych należy podjąć następujące działania:
   a) zaprzestać dalszej pracy,
   b) niezwłocznie poinformować o zaistniałym incydencie i zastosować się do otrzymanych z poleceń,
   c) nie wykonywać czynności, które mogłyby doprowadzić do zatarcia śladów lub dowodów,
   d) wykonać czynności przywracające normalne funkcjonowanie.
3. Odpowiedzialność za naruszenie bezpieczeństwa danych osobowych ponosi Osoba Upoważniona w zakresie naruszenia obowiązków lub zaniedbań wynikających z powszechnie obowiązujących i wewnętrznych aktów.

4. Administrator sporządza raport na formularzu, którego wzór znajduje się w załączniku nr 10 do niniejszej Księgi Procedur.
5. Skutki naruszenia:
   a) Administrator może wyciągnąć konsekwencje przewidziane w Kodeksie Pracy i innych aktach prawnych w zależności od rodzaju stosunku łączącego Osoby Upoważnione i Administratora oraz od rodzaju skutków naruszeń,
   b) naruszenie może powodować powstanie roszczeń odszkodowawczych,
   c) celowe naruszenie bezpieczeństwa może spowodować konieczność poinformowania organów ścigania,
   d) Administrator może ze skutkiem natychmiastowym odebrać uprawnienia Osobom Upoważnionym.
6. Po przywróceniu normalnego funkcjonowania Administrator lub Osoby Upoważnione dokonują analizy zaistniałego ryzyka oraz zlecają zastosowanie środków zaradczych.
7. W przypadku naruszenia bezpieczeństwa danych osobowych w wyniku nieświadomego działania Osoby Upoważnionej konieczne jest przeprowadzenie odpowiednich, dodatkowych szkoleń w celu wyeliminowania podobnych zdarzeń w przyszłości.
8. Awaria to niespodziewane, nagłe zdarzenie, które powoduje lub może spowodować szkodę oraz doprowadzić do narażenia bezpieczeństwa danych osobowych. W stosunku do awarii zastosowanie mają przepisy dotyczące naruszenia bezpieczeństwa danych osobowych.
9. W przypadku naruszenia bezpieczeństwa danych Administrator, bez zbędnej zwłoki, nie później niż w terminie 72h po stwierdzeniu naruszenia, zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W przypadku opóźnienia w zawiadomieniu, Administrator załącza wyjaśnienie przyczyn opóźnienia.
10. Zgłoszenie zawiera co najmniej:
    a) opis charakteru naruszenia bezpieczeństwa danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
    b) imię i nazwisko oraz dane kontaktowe IODO lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,

c) opis możliwych konsekwencji naruszenia ochrony danych osobowych,

d) opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

11. 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 opisując charakter naruszenia oraz informacje i środki z pkt 10 lit. b), c), d). Zawiadomienie nie jest wymagane, gdy Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony, uniemożliwiajace odczyt osobom nieuprawnionym lub zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności lub wymagałoby to niewspółmiernie dużego wysiłku (wtedy wystarczający jest komunikat publiczny lub inny podobny środek).

VII. POSTANOWIENIA KOŃCOWE

§ 25 Prawo właściwe

W sprawach nieuregulowanych w niniejszej Księdze Procedur zastosowanie mają przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000), przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) oraz inne przepisy ustaw i rozporządzeń normujących przetwarzanie danych osobowych określonej kategorii.

§ 26 Załączniki

Wskazane poniżej załączniki stanowią integralną część niniejszej Księgi Procedur:

1. załącznik nr 1 – upoważnienie do przetwarzania danych osobowych (wzór),
2. załącznik nr 2 – oświadczenie (wzór),
3. załącznik nr 3 – zgoda na przetwarzanie danych osobowych (wzór),

4. załącznik nr 4 – oświadczenie o przestrzeganiu regulacji dotyczących ochrony danych osobowych oraz zobowiązanie do zachowania poufności (wzór),
5. załącznik nr 5 – umowa powierzenia przetwarzania danych osobowych (wzór),
6. załącznik nr 6 – rejestr udostępnionych danych osobowych (wzór),
7. załącznik nr 7 – informacja o Administratorze (wzór),
8. załącznik nr 8 - strefa objęta monitoringiem,
9. załącznik nr 9 – rejestr czynności przetwarzania (wzór),
10. załącznik nr 10 – formularz odnotowywania naruszeń bezpieczeństwa danych (wzór).

SPÓŁDZIELNIA MIESZKANIOWA
„AR-MOCZYDŁO"
ul. Mielczarskiego 8
02-798 Warszawa
Regon 010143973

PREZES ZARZĄDU
SM „AR-Moczydło"
Anna Skutkiewicz

WICEPREZES ZARZĄDU
SM „AR-Moczydło"
Zbigniew Furman