INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W BEST LINGUA Monika Mazur

	Data	Podpis
Opracowanie:	Maj 2018	
Zatwierdzenie:	01.06.2018	
Aktualizacja:	01.03.2023	
Aktualizacja:	16.03.2026	
Aktualizacja		

§1

Ilekroć w niniejszym dokumencie jest mowa o:

a) Przedsiębiorstwo – należy przez to rozumieć BEST LINGUA Monika Mazur; Nazwa skrócona BEST LINGUA;
b) Administrator Danych Osobowych – należy przez to rozumieć przedsiębiorstwo BEST LINGUA Monika Mazur, ul. Reformacka 6, 35-026 Rzeszów, NIP: 8161405781.
c) Osoby przetwarzające dane – należy przez to rozumieć wszystkie osoby upoważnione do przetwarzania danych osobowych, czyli pracownika przedsiębiorstwa zatrudnionego na podstawie umowy o pracę, osobę wykonującą pracę na podstawie umowy cywilnoprawnej, osobę odbywającą staż, praktykę w przedsiębiorstwie;
d) Użytkownik systemu – należy przez to rozumieć osoby upoważnione przez Administratora Danych Osobowych do przetwarzania danych osobowych w systemie informatycznym przedsiębiorstwa. Użytkownikiem może być pracownik przedsiębiorstwa, osoba wykonująca pracę na podstawie umowy cywilnoprawnej lub osoba odbywająca staż, praktykę w przedsiębiorstwie, którzy zostali upoważnieni do dostępu do danych osobowych klientów, kontrahentów, współpracowników i pracowników przedsiębiorstwa;
e) Dane osobowe – wszelkie informacje umożliwiające zidentyfikowanie osoby fizycznej;
f) PUODO – Prezes Urzędu Ochrony Danych Osobowych;
g) RODO – przepisy dotyczące danych osobowych osób fizycznych, zgodnie z przepisami 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) (Dz. U. UE. L. 2016.119.1);
h) Ustawa – ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (t.j. Dz. U. 2018, poz. 1669).
i) Instrukcja zarządzania systemem informatycznym BEST LINGUA Monika Mazur – zwana dalej „Instrukcją" określa zasady i tryb postępowania przy przetwarzaniu w systemach informatycznych danych osobowych klientów, kontrahentów, współpracowników i pracowników przedsiębiorstwa BEST LINGUA, zgodnie z przepisami RODO i Ustawy.
j) Zewnętrzne nośniki – przenośne nośniki, na których są, bądź mogą znajdować się dane osobowe przetwarzane przez BEST LINGUA, m.in. laptopy, dyski twarde, PenDrive, pamięć flash (SD, SSD, MS, MMC i inne), płyty CD i inne.

§ 2

1. Celem niniejszej Instrukcji jest określenie procedur i odpowiednich warunków zarządzania systemem informatycznym dla ochrony zgromadzonych danych, jak również jednolitych i bezpiecznych zasad korzystania z przetwarzania danych osobowych w przedsiębiorstwie, zgodnie z wymaganiami określonymi w Ustawie oraz w RODO. Za priorytet uznano zagwarantowanie zgromadzonym danych osobowym, przez cały okres ich przetwarzania, charakteru poufnego wraz z zachowaniem ich integralności oraz integralności systemu przetwarzania danych.
2. Niniejsza Instrukcja dotyczy wszystkich zbiorów danych osobowych przetwarzanych w przedsiębiorstwie w postaci elektronicznej.
3. Zasady opisane w niniejszym dokumencie obowiązują wszystkie osoby przetwarzające dane osobowe w systemach informatycznych w przedsiębiorstwie.
4. Zasady opisane w niniejszym dokumencie obowiązują także podmioty przetwarzające dane osobowe na rzecz przedsiębiorstwa, w zakresie określonym umową zawartą w tym przedmiocie.

§ 3

1. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:
    a) dostęp do danych wyłącznie osób uprawnionych oraz wyeliminowanie ujawnienia i dostępu do nich osobom nieuprawnionym;
    b) niezmienność danych w sposób nieuprawniony;
    c) niezniszczalność danych w sposób nieuprawniony;
    d) integralność systemu rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

§ 4

1. Realizację zamierzeń określonych w § 3 powinna zagwarantować następująca strategia:
    a) wdrożenie procedur określających postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich odpowiedzialność za ochronę tych danych;
    b) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych, w zakresie odpowiedzialności użytkowników za ochronę tych danych oraz sposobów zabezpieczenia systemu informatycznego;
    c) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory) oraz zapewniających dostęp użytkowników do różnych poziomów bazy danych osobowych lub określonych aplikacji – stosownie do indywidualnych zakresów czynności;
    d) zaimplementowanie w systemie informatycznym zabezpieczeń zapewniających nienaruszoną pracę systemu, w tym najnowszych wersji oprogramowania antywirusowego;
    e) ocena ewentualnych zagrożeń bezpieczeństwa systemu informatycznego;
    f) stałe monitorowanie wdrożonych zabezpieczeń w celu identyfikacji podatnych na zagrożenia obszarów i słabości zabezpieczeń;
    g) podejmowanie niezbędnych działań dla likwidacji słabych ogniw w systemie zabezpieczeń;
    h) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych;
    i) opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii;
    j) śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych i – w miarę możliwości organizacyjnych i techniczno-finansowych – wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemem informatycznym, które mają służyć wzmocnieniu bezpieczeństwa danych osobowych.

§ 5

1. Dostęp/uprawnienia do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych w danym zbiorze danych.
2. Każdy użytkownik w systemie posiada zarejestrowany w procesie nadawania uprawnień odrębny, unikalny (niepowtarzalny w skali systemu) identyfikator i hasło do tych części systemu informatycznego, z którymi uprawniony jest pracować.
3. Dostęp do danych osobowych we wszystkich zidentyfikowanych systemach informatycznych możliwy jest po podaniu prawidłowego unikalnego identyfikatora użytkownika oraz prawidłowego hasła, który przekazywany jest użytkownikowi przez Administratora Danych Osobowych.

4. Identyfikator użytkownika nie podlega zmianie, z wyjątkiem sytuacji, gdy identyfikator zostanie ujawniony.
5. Identyfikator użytkownika podlega rejestracji w systemie informatycznym, a za jego ochronę w systemie odpowiada Administrator Danych Osobowych lub osoba przez niego upoważniona.
6. Hasło dostępu do systemu informatycznego stanowi tajemnicę i udostępnione jest wyłącznie użytkownikowi, któremu zostało nadane upoważnienie. Ustanowione hasło, Administrator przekazuje użytkownikowi w sposób bezpieczny i bezpośredni – indywidualnie, w sposób ustny.
7. Zmianę użytkownika komputera każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa liczba użytkowników wykorzystywała wspólnie jedno konto użytkownika.

§ 6

1. W przypadku zakończenia przetwarzania danych osobowych w systemie informatycznym spowodowanego zmianą zakresu dotychczasowych obowiązków bądź zakończeniem wykonywania obowiązków na rzecz przedsiębiorstwa (ustanie stosunku pracy, zakończenie odbywania stażu, praktyki itp.), Administrator zobowiązany jest do niezwłocznego dokonania zmiany bądź odebrania praw dostępu do systemu informatycznego.
2. Administrator Danych Osobowych prowadzi aktualną ewidencję użytkowników danego systemu, w której odnotowuje w szczególności identyfikator użytkownika systemu, nazwę systemu/modułu, rolę w systemie, datę nadania uprawnienia, datę ustania uprawnienia, datę zmiany uprawnienia itp.
3. Ewidencja użytkowników uprawnionych do przetwarzania danych, w tym w systemie informatycznym, prowadzona jest zgodnie ze wzorem, stanowiącym załącznik nr 5 do Polityki Bezpieczeństwa przetwarzania danych BEST LINGUA Monika Mazur.

§ 7

Zasady posługiwania się hasłami:

1) Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2) Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
3) W przypadku podejrzenia ujawnienia hasła osobie nieupoważnionej, podlega ono natychmiastowej zmianie.
4) Przy wpisywaniu hasło lub PIN nie może być wyświetlane na ekranie ani nigdzie utrwalane.
5) Hasła i PIN-y muszą odpowiadać następującym wymogom:
    a) hasła nie mogą być krótsze niż 10 znaków zawierające minimum 1 literę dużą, 1 cyfrę i 1 znak specjalny;
    b) PIN-y nie mogą być krótsze niż 4 cyfry;
    c) nie mogą być zapisywane w systemie w postaci jawnej;
    d) nie mogą być w nich używane numery telefonów użytkownika, numery rejestracyjne pojazdów, nazwy firmy lub skrótu i innych kombinacji znaków mogących doprowadzić do łatwego odgadnięcia hasła lub PIN-u przez osoby nieupoważnione;
    e) nie mogą być w nich stosowane znaki następujące po sobie na klawiaturze bądź te same cyfry.

§ 8

Raz wykorzystany identyfikator nie może być ponownie przydzielony.

§ 9

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym:

1) Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora, PIN-u oraz hasła.
2) Przy opuszczeniu stanowiska komputerowego należy je zablokować w sposób wymagający podanie hasła lub PIN-u w celu odblokowania.
3) Osoba udostępniająca stanowisko komputerowe innej upoważnionej osobie zobowiązana jest do wylogowania się z systemu.
4) Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wylogować się z sieci komputerowej.
5) Niedopuszczalne jest wyłączenie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

§ 10

1. Użytkownik systemu informatycznego ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
2. Użytkownik systemu informatycznego ponosi pełną odpowiedzialność za wszystkie operacje wykonywane przy użyciu jego identyfikatora i hasła dostępu.
3. Wszystkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
4. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia w przedsiębiorstwie.
5. Identyfikator użytkownika systemu informatycznego, który utracił uprawnienia dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jego hasło.

§ 11

1. Przed przystąpieniem do pracy z systemem informatycznym, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie dostępu do danych osobowych.
2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie systemu, użytkownik obowiązany jest dokonać czynności, określonych w Instrukcji postępowania w sytuacji naruszenia bezpieczeństwa przetwarzania danych.

§ 12

1. Każda osoba przetwarzająca dane osobowe jest odpowiedzialna za zabezpieczenie danych wyświetlanych przez system oraz wydruków zawierających dane osobowe przed osobami trzecimi, nie posiadającymi uprawnień.
2. Dane osobowe powinny być przesyłane wyłącznie jako przesyłki polecone/dokumenty papierowe lub przesyłane w formie zaszyfrowanej z użyciem środków teleinformatycznych.
3. Każdy nośnik powinien być odpowiednio oznakowany i opisany oraz posiadać stosowne zabezpieczenia kodowane.
4. Administrator Danych Osobowych prowadzi ewidencję zewnętrznych nośników zawierających dane osobowe.

§ 13

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.
2. Za wykonywanie kopii zapasowych danych osobowych przetwarzanych w plikach zapisanych na danym komputerze (stacji roboczej) odpowiedzialny jest użytkownik tego komputera.

Nadzór nad realizacją tego obowiązku sprawuje Administrator. Kopie zapasowe danych osobowych przetwarzanych w plikach zapisanych na danym komputerze (stacji roboczej) należy wykonywać nie rzadziej niż raz na miesiąc.

3. Zbiory zapisywane na zewnętrznych nośnikach powinny być odpowiednio oznakowane i przechowywane w miejscach wyznaczonych i odpowiednio zabezpieczonych, poza pomieszczeniami, w których przetwarzane są dane osobowe, za co odpowiedzialny jest Administrator.
4. Kopie zapasowe danych osobowych przechowuje się przez okres nie dłuższy niż niezbędny do zrealizowania celu, w jakim dane osobowe zapisane na tych nośnikach zostały zebrane, chyba że odrębne przepisy przewidują inny okres archiwizacji danych.
5. Kopia zapasowa danych osobowych może zostać usunięta dopiero po wykonaniu kolejnej kopii zapasowej tych danych i sprawdzeniu prawidłowości wykonania tej kopii zapasowej. Zasada określona w zdaniu pierwszym nie dotyczy sytuacji, w których ustały przesłanki przechowywania danych osobowych.
6. Kopie zapasowe (awaryjne), które uległy uszkodzeniu lub zdezaktualizowały się podlegają natychmiastowemu zniszczeniu.
7. Usunięcia kopii zapasowej danych osobowych dokonuje się przez trwałe usunięcie danych z nośnika lub likwidację nośnika zawierającego kopię zapasową danych osobowych.
8. Nośniki z kopiami zapasowymi danych osobowych, których nie można pozbawić zapisu, należy trwale uszkodzić w sposób uniemożliwiający odczytanie zapisanych na nich danych.
9. Niszczenia kopii zapasowych, na nośnikach magnetycznych, półprzewodnikowych i optycznych dokonuje użytkownik w obecności Administratora.

§ 14

1. Dostęp do wszystkich serwerów i stacji roboczych, na których przetwarzane są dane osobowe, wymaga autoryzacji w formie hasła.
2. Na komputerach używanych przez Administratora instaluje się przynajmniej jeden program antywirusowy, który uruchamia się przy każdorazowym rozpoczęciu pracy komputera. Oprogramowanie antywirusowe powinno być tak zainstalowane, aby użytkownik nie był w stanie wyłączyć ochrony antywirusowej.
3. Wszystkie serwery i stacje robocze, na których przetwarzane są dane osobowe, powinny być wyposażone w oprogramowanie antywirusowe, chroniące zasoby informatyczne przed szkodliwym oprogramowaniem.
4. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych. półprzewodnikowych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych. Szczególnej kontroli podlegają nośniki przychodzące z zewnątrz.
5. Użytkownik systemu informatycznego służącego do przetwarzania danych osobowych zobowiązany jest do:
    a) skanowania przy użyciu oprogramowania antywirusowego zawartości dysków komputera – przynajmniej 1 raz dziennie;
    b) skanowania zawartości nośników wymiennych odczytywanych na komputerze – przy każdym odczycie.
6. Okresowych kontroli w zakresie instalowania najnowszych wersji oprogramowania antywirusowego dokonuje Administrator Danych Osobowych.
7. W razie stwierdzenia wystąpienia wirusa, użytkownik systemu obowiązany jest poinformować niezwłocznie o tym fakcie Administratora, który natychmiast go usuwa, jeśli automatycznie nie dokonał tego program antywirusowy.

8. Po usunięciu wirusa Administrator lub osoba przez niego wyznaczona sprawdza zainfekowany system informatyczny oraz przywraca go do pełnej funkcjonalności i sprawności.

§ 15

1. System informatyczny, w którym przetwarzane są dane osobowe powinien posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności system informatyczny powinien zapewnić odnotowanie:
    a) faktu udostępnienia danych osobowych;
    b) informacji o odbiorcach, którym dane osobowe zostały udostępnione;
    c) dacie i zakresie tego udostępnienia.
2. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą;
    b) osoby upoważnionej do przetwarzania danych;
    c) podmiotu, któremu powierzono przetwarzanie danych na podstawie umowy;
    d) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
3. Obowiązek odnotowania ww. informacji w systemie informatycznym spoczywa na użytkowniku systemu, który udostępnia dane.
4. Odnotowanie informacji w systemie informatycznym powinno nastąpić niezwłocznie po udostępnieniu danych.
5. Wymóg określony w ust. 1 nie dotyczy systemów informatycznych:
    a) służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie;
    b) używanych do przetwarzania danych zawartych w zbiorach jawnych.
6. W przypadku, gdy system informatyczny nie jest wyposażony w wewnętrzną funkcjonalność pozwalającą na zapewnienie odnotowania informacji, o których mowa w ust. 1, informacje te odnotowuje się w odrębnym pliku elektronicznym, który należy przechowywać i archiwizować łącznie z systemem informatycznym, dla którego plik ten został utworzony.

§ 16

1. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.
2. Oprogramowanie dostarczane bez opłat uznawane jest za nieautoryzowane, jeżeli nie otrzyma stosownej aprobaty Administratora Danych Osobowych.
3. Administrator Danych Osobowych odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelniania użytkownika.
4. Stacji robocza powinna być tak skonfigurowany, aby po upływie 3 minut od ostatniego użycia stanowiska roboczego następowała automatyczna blokada stanowiska roboczego, wymuszająca ponowne zalogowanie.
5. Ekrany monitorów powinny być ustawione w taki sposób, aby osoby nieupoważnione nie miały wglądu w informacje aktualnie wyświetlane na ekranie.

§ 17

1. Wszelkie prace związane z przeglądami, naprawami, konserwacją lub bieżącym serwisem systemu informatycznego służącego do przetwarzania danych osobowych (lub elementów tego systemu) wykonywane są przez przedsiębiorstwo informatyczne wyznaczone przez Administratora.
2. Administrator w takiej sytuacji zobowiązany jest do całkowitego i trwałego usunięcia danych osobowych zapisanych na sprzęcie, uniemożliwiając ich odczyt. Jeżeli nie jest to możliwe,

Administrator zobowiązany jest zawrzeć z przedsiębiorstwem informatycznym właściwą umowę powierzenia przetwarzania danych, na wypadek ich odczytu.

3. Prace konserwacyjne i przeglądy odbywają się w terminach określonych w zaleceniach dostawców sprzętu i systemu lub w razie pojawiających się potrzeb, nie rzadziej jednak niż raz w roku.
4. Nadzór nad instalowaniem, sprawnym funkcjonowaniem i wymianą uszkodzonych urządzeń oraz ich likwidacją sprawuje Administrator Danych Osobowych lub osoba przez niego upoważniona.

§ 18

1. Zasady korzystania z urządzeń przenośnych oraz elektronicznych nośników informacji, na których są przetwarzane dane osobowe określone zostały w §12 Polityki bezpieczeństwa danych BEST LINGUA Monika Mazur.
2. Pracodawca wyraża zgodę pracownikowi w uzasadnionych przypadkach na pracę na komputerze służbowym przenośnym poza budynkiem przedsiębiorstwa.
3. Komputer powinien być przygotowany do wykonywania przez użytkownika czynności służbowych poza budynkiem przedsiębiorstwa, tzn.:
   a) użytkownik powinien mieć możliwość połączenia się z sieciami WI-FI bez uprawnień administratora lokalnego;
   b) zapora sieciowa komputera oraz oprogramowanie antywirusowe powinno być aktywne;
   c) wygaszacz ekranu i automatyczna blokada komputera przenośnego powinna być włączona;
   d) komputer przenośny powinien mieć włączone zabezpieczenie BIOS-u hasłem i wyłączone bootowanie z nośników zewnętrznych.
4. Pracodawca musi każdorazowo wyrazić pracownikowi zgodę na jego pracę na własnym komputerze.

§ 19

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji:

1) Dane osobowe w postaci elektronicznej – zapisywane na dyskach twardych nie są wynoszone poza siedzibę przedsiębiorstwa z zastrzeżeniem §12 Polityki bezpieczeństwa danych BEST LINGUA Monika Mazur.
2) Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityki bezpieczeństwa danych BEST LINGUA Monika Mazur.
3) Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki są przechowywane w szafie zamykanej na klucz.
4) Nośniki zewnętrzne zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
5) Nośniki zewnętrzne zawierające dane osobowe, przeznaczone do naprawy pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

§ 20

1. W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie ogólne przepisy przeciwpożarowe.
2. Osoby biorące udział w akcji ratunkowej, mają prawo wejść do pomieszczeń w których przetwarzane są dane osobowe bez dopełniania obowiązków wynikających z zapisów

niniejszej Instrukcji oraz Polityki bezpieczeństwa przetwarzania danych BEST LINGUA Monika Mazur.

3. W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy systemu, przebywający w pomieszczeniach, w których przetwarzane są dane osobowe, obowiązani są do przerwania pracy – w miarę możliwości przed opuszczeniem tych pomieszczeń – do zamknięcia systemu.
4. W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Danych Osobowych i pozostali obecni użytkownicy systemu powinni, w miarę możliwości, zabezpieczać dane osobowe przed nieuprawnionym dostępem. Obowiązek ten ciąży w równym stopniu na innych pracownikach przedsiębiorstwa, obecnych przy akcji ratunkowej.

§ 21

1. Osobami bezpośrednio odpowiedzialnymi za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych używanych w przedsiębiorstwie, w tym za realizację obowiązków wynikających z niniejszej Instrukcji, są:
    a) osoby przetwarzające dane osobowe;
    b) Administrator Danych Osobowych.
2. Nadzór nad prawidłowym wykonywaniem obowiązków określonych w niniejszej Instrukcji sprawuje Administrator Danych Osobowych.
3. Nieprzestrzeganie zasad postępowania określonych w niniejszej Instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną pociągnięcia pracownika do odpowiedzialności dyscyplinarnej określonej w Kodeksie pracy.
4. Jeżeli skutkiem działania określonego w ust. 3 jest ujawnienie danych osobowych lub umożliwienie dostępu do nich osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów ustawy o ochronie danych osobowych i Kodeksu karnego.

Zatwierdzam
Monika Mazur
Administrator Danych Osobowych