Polityka bezpieczeństwa
w sprawie ochrony danych osobowych

obowiązująca w WSRH spółce z ograniczoną odpowiedzialnością we Wrocławiu

***

W celu zapewnienia ochrony przetwarzanych danych osobowych administrator danych osobowych zgodnie z wymogami określonymi w Rozporządzeniu 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), dalej jako „RODO", WSRH sp. z o.o. we Wrocławiu wprowadza poniższą Politykę bezpieczeństwa w sprawie ochrony danych osobowych.

§ 1
Zakres przedmiotowy

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w WSRH sp. z o.o. we Wrocławiu zwana dalej „Polityką Bezpieczeństwa" określa przetwarzanie i zabezpieczanie danych osobowych w tej spółce.

§ 2
Definicje

Ilekroć w Polityce Bezpieczeństwa jest mowa o:

1) administratorze danych – rozumie się przez to WSRH sp. z o.o. we Wrocławiu, przy ul. Średzkiej 32-36, 54-017 Wrocław, wpisana do rejestru przedsiębiorców KRS prowadzonego przez Sąd Rejonowy dla Wrocławia - Fabrycznej we Wrocławiu, VI Wydział Gospodarczy, pod numerem KRS 0000378053, NIP 8943017685, kapitał zakładowy 610 000,00 zł, działająca przez zarząd, dalej jako „WSRH",
2) danych osobowych - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3) kontrahentach – rozumie się przez to podmioty, z którymi łączą WSRH stosunki gospodarcze w zakresie prowadzonych sklepów wykorzystywanych do detalicznej sprzedaży towarów,
4) najemcach – rozumie się przez to będących osobami fizycznymi najemców lub dzierżawców nieruchomości (ich wyodrębnionych części), co do których WSRH posiada tytuł prawny,
5) osobie nieuprawnionej – rozumie się przez to osobę niedopuszczoną do przetwarzania danych osobowych (z wyłączeniem osoby uprawnionej do ich przeglądania i przetwarzania na mocy odrębnych przepisów), a także osobę, której dane osobowe nie podlegają przetwarzaniu we właściwych zbiorach danych,
6) przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

7) placówkach – rozumie się przez to zarówno:
    a. siedzibę WSRH znajdującą się przy ul. Średzkiej 32-36 we Wrocławiu,
    b. sklepy WSRH wykorzystywane do detalicznej sprzedaży towarów, zlokalizowane we Wrocławiu:
        - przy ul. Średzkiej 32-36,
        - przy ul. Kominiarskiej 42,
        - przy ul. Stabłowickiej 55,
        - przy ul. Wałbrzyskiej 41,
        - przy ul. Piwnicznej 1,
        - przy ul. Maślickiej 191,
        - przy ul. P. Jasienicy 1,
        - przy ul. Miłoszyckiej 1a;
8) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
9) pracowniku – rozumie się przez to osobę zatrudnioną na podstawie umowy o pracę lub świadczącą usługi na podstawie umowy cywilnoprawnej nie zawartej w ramach prowadzonej przez nią działalności gospodarczej,
10) użytkowniku – rozumie się przez to pracownika dopuszczonego do przetwarzania danych osobowych w WSRH,
11) zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

§ 3
Cel Polityki Bezpieczeństwa

Celem wprowadzenia niniejszej Polityki Bezpieczeństwa jest:

1) ochrona danych osobowych przetwarzanych i gromadzonych w WSRH i dotyczy:
    a. zabezpieczenia przed dostępem do danych osób nieuprawnionych, na każdym etapie ich przetwarzania tj. wprowadzania, aktualizacji lub usuwania, wyświetlania lub drukowania zestawień i raportów, przemieszczania danych w sieci lokalnej pomiędzy programami i osobami je przetwarzającymi,
    b. metod archiwizacji oraz ochrony danych zarchiwizowanych na nośnikach zewnętrznych i wydrukach,
    c. procedur niszczenia niepotrzebnych wydruków lub nośników z danymi,
    d. ustalenia i wdrożenia zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia gromadzące i przetwarzające dane,
    e. określenia polityki i sposobów dostępu do tych pomieszczeń przez pracowników, personel pomocniczy oraz serwis naprawczy.
2) zmniejszenie ryzyka utraty informacji,
3) określenia zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych,
4) podnoszenie świadomości pracowników i ich pełne zaangażowanie w ochronę przetwarzanych danych.

§ 4

Zakres zastosowania

Zasady określone przez niniejszy dokument mają zastosowanie do całego systemu przetwarzania danych w tym do systemu informatycznego, a w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są lub będą informacje podlegające ochronie,
2) informacji będących własnością WSRH,
3) wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się informacje podlegające ochronie,
4) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
5) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, osób świadczących usługi na podstawie umów cywilnoprawnych, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

§ 5

Publikacja Polityki Bezpieczeństwa

1. Za rozpowszechnienie dokumentu i umożliwienie zapoznania się z nim przez wszystkich pracowników administracyjnych odpowiedzialny jest administrator danych.
2. Dokument powinien zostać umieszczony w formie elektronicznej, na wewnętrznych zasobach sieciowych, do których dostęp posiadają pracownicy WSRH lub w uzasadnionych przypadkach powinien zostać im przedłożony w formie papierowej.

§ 6

Cel przetwarzania danych osobowych

Administrator danych przetwarza dane osobowe w celu:

1) wykonywania obowiązków pracodawcy w zakresie zatrudnienia pracowników (dokumentacja i przebieg zatrudnienia oraz płace pracowników),
2) realizacji procesu rekrutacji w zakresie danych uzyskanych od kandydatów do pracy w WSRH,
3) wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej w zakresie danych uzyskanych od kontrahentów i najemców,
4) spełniania obowiązku, o którym mowa w art. 188 ustawy z dnia 15 września 2000 r. – Kodeks Spółek Handlowych (Dz.U. z 2013 r. poz. 1030 ze zm.) w zakresie danych identyfikujących poszczególnych wspólników WSRH,
5) prowadzenia nadzoru nad funkcjonowaniem i zabezpieczeniem placówek oraz gromadzenia materiałów dowodowych w sprawach karnych i o wykroczenia, jak również w kwestiach dotyczących dochodzenia świadczeń odszkodowawczych w przypadku wystąpienia szkody w mieniu WSRH sp. z o.o., w zakresie danych uzyskanych z monitoringu wizualnego.

§ 7

Dopuszczalność przetwarzania danych

1. Przetwarzanie danych osobowych przez WSHR może nastąpić, gdy:

1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

2. W przypadku, o którym mowa w ust. 1 pkt 2 - 6 nie jest wymagana dodatkowa zgoda osoby, której dane te dotyczą.
3. Zgoda na przetwarzanie danych osobowych może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.
4. WSRH stosuje ujednolicony wzór odbierania zgody osoby fizycznej na przetwarzanie danych osobowych, który stanowi **załącznik nr 1** do Polityki Bezpieczeństwa.
5. W celu uzyskania zgody na przetwarzanie danych osobowych od osób biorących udział w procesie rekrutacji wymaga się zamieszczenia w dokumentach, które takie dane zawierają, klauzuli o następującej treści:

„Zgadzam się na przetwarzanie przez WSRH sp. z o.o. we Wrocławiu danych osobowych zawartych w moim CV lub w innych dokumentach dołączonych do CV (moje zgłoszenie rekrutacyjne), dla celów prowadzenia rekrutacji na stanowisko wskazane w ogłoszeniu. Dodatkowo zgadzam się na przetwarzanie przez WSRH sp. z o.o. we Wrocławiu danych osobowych zawartych w moim zgłoszeniu rekrutacyjnym dla celów przyszłych rekrutacji.”

6. CV, listy motywacyjne, zgłoszenia konkursowe oraz inne dokumenty pochodzące od osoby biorącej udział w procesie rekrutacji, które nie zawierają przynajmniej pierwszego zdania ww. klauzuli zostaną bez merytorycznego rozpatrywania zniszczone (usunięte), chyba że osoba ta niezwłocznie uzupełni dany dokument w tym zakresie lub w treści przedłożonych przez nią dokumentów w inny sposób została wyrażona przez nią jednoznaczna zgoda na przetwarzanie danych osobowych.

§ 8
Obowiązek informacyjny

1. Przy pierwszej możliwej okazji WSRH informuje osobę fizyczną o konieczności, celu i sposobie przetwarzania danych osobowych.
2. Informacja o konieczności, celu i sposobie przetwarzania danych dotyczy w szczególności danych zawartych w art. 13 ust. 1 i 2 RODO.
3. W celu realizacji obowiązku informacyjnego WSRH przedstawia osobom fizycznym tzw. klauzule informacyjne pisemnie lub drogą mailową.
4. Wzory klauzul informacyjnych przeznaczonych dla kontrahenta, osoby uczestniczącej w rekrutacji do pracy, pracownika, osoby trzeciej stanowią odpowiednio **załączniki nr 2,3,4,5** do Polityki Bezpieczeństwa.

§ 9
Monitoring

1. Wszystkie placówki są objęte monitoringiem wizualnym.
2. Administrator danych ma obowiązek poinformować o prowadzonym monitoringu wizyjnym pracowników, których stanowiska pracy są takim monitoringiem objęte. Informacja o monitoringu wizyjnym powinna zostać przekazana najpóźniej w chwili rozpoczęcia pracy przez pracownika. Zgoda pracownika na stosowanie monitoringu wizyjnego jest odbierana na piśmie. Wzór zgody stanowi **załącznik nr 6** do niniejszej Polityki Bezpieczeństwa. Odmowa wyrażenia zgody na stosowanie monitoringu rodzi konieczność odmowy dopuszczenia pracownika do pracy.
3. Administrator danych ma obowiązek poinformować o prowadzonym monitoringu wizyjnym osoby trzecie poprzez wywieszenie w ogólnodostępnym miejscu przy wejściu do danej placówki informacji o stosowaniu monitoringu wizyjnego. Zgoda na stosowanie monitoringu wizyjnego jest wyrażana wejściem danej osoby na teren placówki.
4. Zapisów uzyskanych z monitoringu nie gromadzi się na zewnętrznych nośnikach pamięci i są one automatycznie usuwane (nadpisywane) z rejestratorów obrazów i dźwięków po 7 dniach pracy tych urządzeń z zastrzeżeniem ust. 5.
5. Zapisy uzyskane z monitoringu przetwarza się na zewnętrzne nośniki pamięci tylko na żądanie odpowiednich instytucji państwowych oraz w przypadku podejrzenia popełnienia przestępstwa w celu przekazania organom ścigania, jak też w przypadku wystąpienia szkody w mieniu WSRH sp. z o.o. na żądanie zakładów ubezpieczeń.
6. W razie przetwarzania zapisów uzyskanych z monitoringu nie tworzy się zapasowych kopii przechowywanych w placówkach. Ewidencjonuje się tylko fakt dokonania przetworzenia. Ewidencja przetworzenia zapisów z monitoringu stanowi **załącznik nr 7** do niniejszej Polityki Bezpieczeństwa.

§ 10
Informowanie o przetwarzaniu danych w trybie wnioskowym

1. Na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:
    1) jakie dane osobowe są przetwarzane,
    2) w jaki sposób zebrano dane,
    3) w jakim celu i zakresie dane są przetwarzane,
    4) w jakim zakresie oraz komu dane zostały udostępnione.
2. Na wniosek osoby, której dane dotyczą, ww. informacji udziela się na piśmie.
3. Osoba zainteresowana może skorzystać z prawa do informacji, o którym mowa powyżej, nie częściej niż raz na 6 miesięcy.

§ 11
Kontrola przetwarzania danych

Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

1) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji, dla którego zostały zebrane,
2) żądania zaprzestania przetwarzania jej danych.

§ 12
Obowiązek uaktualnienia danych

W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru.

§ 13
Upoważnienie do przetwarzania danych osobowych

1. Dostęp pracowników do systemu informatycznego, programów przetwarzających dane osobowe oraz urządzeń z nimi powiązanych, jak też do dokumentów zawierających dane osobowe, możliwy jest wyłącznie na podstawie upoważnienia do przetwarzania danych osobowych wydanego przez administratora danych. Wzór upoważnienia został określony w **załączniku nr 8** do niniejszej Polityki Bezpieczeństwa.
2. Przed dopuszczeniem do pracy związanej z przetwarzaniem danych osobowych, każda osoba powinna być zaznajomiona z procedurami dotyczącymi ochrony danych osobowych w szczególności z niniejszą Polityką Bezpieczeństwa.
3. Użytkownicy obowiązani są do zachowania w tajemnicy uzyskanych podczas wykonywania obowiązków pracowniczych danych osobowych dotyczących poszczególnych osób oraz do zachowania w tajemnicy informacji o ich zabezpieczeniu.
4. Przyjmując upoważnienie do przetwarzania danych osobowych, Użytkownik składa oświadczenie o zapoznaniu się z przepisami o odpowiedzialności karnej za naruszenie bezpieczeństwa danych osobowych.
5. Fakt zapoznania się z niniejszą Polityką Bezpieczeństwa potwierdza się własnoręcznym podpisem przy przyjęciu upoważnienia do przetwarzania danych osobowych.
6. Administrator danych prowadzi rejestr użytkowników, który stanowi **załącznik nr 9** do niniejszej Polityki Bezpieczeństwa.

§ 14
Przekazanie danych osobowych podmiotom przetwarzającym

1. WSRH w zakresie prowadzonego przez siebie przedsiębiorstwa może przekazywać dane osobowe podmiotom przetwarzającym w szczególności świadczącym usługi informatyczne, księgowe lub prawne.
2. Przekazywanie danych osobowych podmiotom przetwarzającym może nastąpić jedynie w zakresie niezbędnym do prawidłowego wykonania na rzecz WSRH sp. z o.o. usług przez te podmioty.
3. WSRH korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia danych osobowych.

4. WSRH dążyć będzie do zawarcia z każdym podmiotem przetwarzającym pisemnej umowy o powierzenie przetwarzania danych osobowych, której wzór stanowi **załącznik nr 10** do niniejszej Polityki Bezpieczeństwa.
5. WSRH prowadzi ewidencję podmiotów przetwarzających dane osobowe, z którymi współpracuje. Ewidencja ta stanowi **załącznik nr 11** do niniejszej Polityki Bezpieczeństwa.

§ 15

Wykaz budynków i pomieszczeń

1. Wszelkie dane, a zwłaszcza dane osobowe, które leżą w gestii administrowania i gromadzenia przez administratora danych, są przetwarzane w placówkach.
2. Szczegółowy wykaz pomieszczeń, w których dane osobowe są przetwarzane, ich usytuowanie, jak również rodzaj przechowywanych w nich zbiorów danych osobowych stanowi **załącznik nr 12** do niniejszej Polityki Bezpieczeństwa.
3. W uzasadnionych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych) wyłącznie za wiedzą administratora danych.

§ 16

Wykaz zbiorów danych osobowych

1. W WSRH utworzone zostały następujące zbiory danych osobowych:
   1) zbiór kadrowo – płacowy,
   2) zbiór kandydatów do pracy,
   3) zbiór danych osobowych kontrahentów,
   4) zbiór danych osobowych wspólników WSRH,
   5) zbiór danych osobowych najemców.
2. Zbiór kadrowo – płacowy prowadzony jest wyłącznie w celu, o którym mowa w § 6 pkt 1.
3. Zbiór kandydatów do pracy prowadzony jest wyłącznie w celu, o którym mowa w § 6 pkt 2.
4. Zbiory danych osobowych kontrahentów i najemców prowadzone są wyłącznie w celu, o którym mowa w § 6 pkt 3.
5. Zbiór danych osobowych wspólników WSRH prowadzony jest wyłącznie w celu, o którym mowa w § 6 pkt 4.
6. Administrator danych prowadzi rejestr czynności przetwarzania danych osobowych, które są zawarte w zbiorach wskazanych w ust.1 pkt 1, 3 i 5. Rejestr ten stanowi **załącznik nr 13** do niniejszej Polityki Bezpieczeństwa.
7. Administrator danych w związku z art. 30 ust.5 RODO nie prowadzi rejestru czynności przetwarzania danych osobowych, które są zawarte w zbiorze wskazanym w ust.1 pkt 2 i 4, z uwagi na fakt, że przetwarzanie tych danych następuje sporadycznie, a WSRH zatrudnia mniej niż 250 osób.

§ 17

Struktura zbiorów danych osobowych

1. Na strukturę zbioru kadrowo – płacowego składają się następujące dane osobowe:
   1) Imię i nazwisko, imiona rodziców, data urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie, przebieg dotychczasowego zatrudnienia;
   2) Imiona i nazwiska oraz daty urodzenia dzieci gdy jest to niezbędne do korzystania z uprawnień przewidzianych w prawie pracy;
   3) Nr PESEL;
   4) Dane kadrowe (wysługa lat pracy, stawka wynagrodzeń), dane o czasie pracy, przyznanych nagrodach, potrąceniach;
   5) Numery kont dla przelewów bankowych pracownika;
   6) Informacje o absencji (urlopy, zwolnienia lekarskie, rehabilitacyjne, szkoleniowe i inne), dane o zakresie obowiązków, stawce wynagrodzenia, karach i nagrodach oraz inne dane wymagane zgodnie z Kodeksem Pracy;
   7) Inne dane wymagane zgodnie z przepisami o ubezpieczeniu społecznym;
   8) Rejestry archiwum obejmujące akta osobowe pracowników;
   9) Rejestr związany z Zakładowym Funduszem Świadczeń Socjalnych lub środkami zgromadzonymi na tym funduszu;
   10) Rejestr wypadków pracowników;
   11) Ewidencja pracowników ze stwierdzonym stopniem niepełnosprawności;
   12) Ewidencja przynależności pracowników do poszczególnych organizacji związkowych.
2. Na strukturę zbioru kandydatów do pracy składają się dane przekazywane przez osoby biorące udział w procesie rekrutacji w szczególności imię, nazwisko, dane adresowe, adres email, nr telefonu, data i miejsce urodzenia, dane dotyczące wykształcenia i doświadczenia zawodowego kandydata.
3. Na strukturę zbioru danych osobowych kontrahentów składają się:
   1) dane adresowe kontrahentów, tj. imię, nazwisko, firma, adres zamieszkania/zameldowania, adres prowadzenia działalności (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), nr telefonu, adres email, NIP, nr PESEL, nr REGON.
   2) umowy (też aneksy) zawarte między WSRH a kontrahentem,
   3) dokumenty księgowe.
4. Na strukturę zbioru danych osobowych wspólników WSRH składają się:
   1) imiona, nazwiska, firma oraz miejsce zamieszkania wspólników,
   2) liczba i wartość nominalna ich udziałów,
   3) informacja o ustanowieniu zastawu lub użytkowania i wykonywania prawa głosu przez zastawnika lub użytkownika,
   4) wszelkie zmiany dotyczące osób wspólników i przysługujących im udziałów.
5. Na strukturę zbioru danych osobowych najemców składają się:
   1) dane adresowe najemców, tj. imię, nazwisko, firma, adres zamieszkania/zameldowania, adres prowadzenia działalności (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), nr telefonu, adres email, NIP, nr PESEL, nr REGON.
   2) umowy (też aneksy) zawarte między WSRH a najemcą,
   3) dokumenty księgowe.

§ 18

Wewnętrzna transmisja danych osobowych

Przepływ danych osobowych w WSRH następuje poprzez wykorzystanie:

1) poczty elektronicznej za pomocą służbowych skrzynek e-mail utworzonych w adresie domeny WSRH,
2) przenośnych nośników pamięci (m.in. USB, płyty CD, DVD) będących własnością WSRH z dostępem zabezpieczonym hasłem,
3) uporządkowanych i posegregowanych dokumentów papierowych.

§ 19

Rodzaje zabezpieczeń

W celu zapewnienia poufności, integralności i rozliczalności przetwarzanych danych ustanawia się następujące zabezpieczenia:

1) fizyczne,
2) informatyczne,
3) organizacyjne.

§ 20

Zabezpieczenia fizyczne

1. W poszczególnych placówkach montuje się niezależne zamki w drzwiach:
   a) archiwum i innych pomieszczeń, w których przechowywane są nośniki kopii zapasowych,
   b) pomieszczeń biurowych, w których odbywa się przetwarzanie danych.
2. W poszczególnych placówkach instaluje się antywłamaniowy system alarmowy.
3. Serwer znajduje się z zamykanej szafie typu Rack.
4. Bieżącą kontrolę dostępu do pomieszczeń przeznaczonych do przetwarzania danych osobowych sprawuje administrator danych.

§ 21

Zabezpieczenia informatyczne

Sposób i rodzaje zabezpieczeń informatycznych obowiązujące w WSRH zostały szczegółowo określone w Instrukcji zarządzania systemami informatycznymi, która stanowi **załącznik nr 14** do niniejszej Polityki Bezpieczeństwa.

§ 22

Zabezpieczenia organizacyjne

1. WSRH w celu zapewnienia optymalnego zabezpieczenia przetwarzanych danych osobowych zobowiązuje się stosować oraz na bieżąco uaktualniać niniejszą Politykę Bezpieczeństwa i jej załączniki.
2. Dostęp do szaf, sejfów, biurek, innego podobnego wyposażenia w pomieszczeniach placówek, w których znajdują się przetwarzane dane osobowe, a także archiwum oraz pomieszczeń, w których znajdują się serwery baz danych lub przechowywane są kopie zapasowe mogą mieć wyłącznie osoby, które posiadają upoważnienie do przetwarzania danych osobowych.

3. WSRH wprowadza Politykę czystego biurka określającą zasady przechowywania nośników danych osobowych na biurkach pracowniczych w trakcie pracy, która stanowi **załącznik nr 15** do niniejszej Polityki Bezpieczeństwa.
4. Klucze do pomieszczeń, o których mowa w §20 ust.1, posiadają tylko osoby zatrudnione w poszczególnych działach/pokojach.
5. Z wyłączeniem personelu sprzątającego i serwisów naprawczych, nikt nie może przebywać w pomieszczeniach placówek, o których mowa w § 15 ust. 2, jeżeli w pomieszczeniu tym nie znajduje się wówczas choć jeden użytkownik.
6. Po zakończeniu pracy osoba zamykająca pomieszczenie powinna dodatkowo sprawdzić, czy zostały w nim zamknięte wszystkie okna i wyłączone wszystkie komputery.

§ 23
Procedura postępowania w przypadku podejrzenia naruszeń

1. W przypadku uzasadnionego podejrzenia naruszenia Polityki Bezpieczeństwa lub powszechnie obowiązującego prawa dotyczącego danych osobowych, pracownik WSRH zobowiązany jest niezwłocznie poinformować o tym fakcie zarząd WSRH.
2. W celu ułatwienia dokonywania zgłoszeń, o których mowa powyżej, tworzy się wzór pisemnego zgłoszenia dostępnego dla wszystkich pracowników, który stanowi **załącznik nr 16** do niniejszej Polityki Bezpieczeństwa.
3. Po uzyskaniu informacji o możliwym naruszeniu Polityki Bezpieczeństwa administrator danych podejmie odpowiednie działania mające na celu jej zweryfikowanie.
4. W przypadku stwierdzenia naruszenia Polityki Bezpieczeństwa administrator danych podejmie niezbędne środki mające na celu wyeliminowanie naruszenia jak również środki zapobiegawcze, by podobna sytuacja nie powtórzyła się w przyszłości. Administrator danych powiadomi również o naruszeniu ochrony danych osobowych osobę, której one dotyczą. Powiadomienie sporządza się na piśmie, którego wzór stanowi **załącznik nr 17** do niniejszej Polityki Bezpieczeństwa.
5. WSRH prowadzi ewidencję naruszeń Polityki Bezpieczeństwa lub powszechnie obowiązujących aktów prawnych dotyczących danych osobowych, która stanowi **załącznik nr 18** do niniejszej Polityki Bezpieczeństwa.

§ 24
Załączniki

1. Wszystkie załączniki do Polityki Bezpieczeństwa stanowią jej integralną część, mogą być jednak w zależności od potrzeb modyfikowane i aktualizowane bez konieczności dokonywania zmian w samej Polityce Bezpieczeństwa.
2. Lista wszystkich załączników do Polityki Bezpieczeństwa jest następująca:
   1) Wzór zgody osoby fizycznej na przetwarzanie danych osobowych (załącznik nr 1),
   2) Klauzula informacyjna dla kontrahenta (załącznik nr 2),
   3) Klauzula informacyjna dla osoby ubiegającej się o pracę (załącznik nr 3),
   4) Klauzula informacyjna dla pracownika (załącznik nr 4),
   5) Klauzula informacyjna dla osoby trzeciej (załącznik nr 5),

6) Wzór zgody pracownika na stosowanie monitoringu wizyjnego (załącznik nr 6),
7) Ewidencja przetworzenia zapisów z monitoringu (załącznik nr 7),
8) Wzór upoważnienia do przetwarzania danych osobowych (załącznik nr 8),
9) Rejestr użytkowników (załącznik nr 9),
10) Wzór umowy o powierzenie przetwarzania danych osobowych (załącznik nr 10),
11) Ewidencja podmiotów przetwarzających dane osobowe (załącznik nr 11),
12) Wykaz pomieszczeń, gdzie przetwarzane są dane osobowe (załącznik nr 12),
13) Rejestr czynności przetwarzania danych osobowych (załącznik nr 13),
14) Instrukcja zarządzania systemami informatycznymi (załącznik nr 14),
15) Polityka czystego biurka (załącznik nr 15),
16) Wzór zgłoszenia naruszeń w zakresie przetwarzania danych osobowych (załącznik nr 16),
17) Wzór powiadomienia osoby poszkodowanej o naruszeniu ochrony jej danych osobowych (załącznik nr 17),
18) Ewidencja naruszeń Polityki Bezpieczeństwa (załącznik nr 18).

§ 25

Początek obowiązywania

Niniejsza Polityka Bezpieczeństwa wchodzi w życie w dniu ogłoszenia.