SPIS TREŚCI

SPIS ZAŁĄCZNIKÓW

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w Systemach informatycznych stosowanych w spółce SerwisPrawa.pl Sp zo.o z siedzibą we Wrocławiu. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń. Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym. Dokument „Polityka bezpieczeństwa", wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych i przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych. Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1).
Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:

1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

Polityka bezpieczeństwa obowiązuje wszystkich pracowników. Realizacja postanowień tego dokumentu ma zapewnić ochronę danych osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych.

Rozdział I

Przepisy wprowadzające

§ 1

1. Użyte w niniejszym dokumencie określania oznaczają:
   1) **Administrator danych** – SerwisPrawa.pl Sp.z o.o,
   2) **Administrator Bezpieczeństwa Informacji** (ABI) – osoba wyznaczona przez Administratora danych, a gdy osoba taka nie została wyznaczona – Administratora danych;

3) **Identyfikator** - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
4) **Hasło** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym;
5) **Sieć telekomunikacyjna** - sieć telekomunikacyjna w rozumieniu art. 2 pkt. 23 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
6) **Internet** - sieć publiczna w rozumieniu art. 2 pkt. 22 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne;
7) **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
8) **RODO** – oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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.Urz. UE L 119, s. 1);
9) **Dane** – oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.;
10) **Dane wrażliwe** – oznaczają dane specjalne i dane karne.;
11) **Dane specjalne** – oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
12) **Dane karne** – oznaczają dane wymienione w art. 10 RODO tj.dane dotyczące wyroków skazujących i naruszeń prawa.;
13) **Dane dzieci** – oznaczają dane osób poniżej 16 roku życia.;

14) **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
15) **Integralności danych** - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
16) **IOD lub inspektor** – oznacza inspektora Ochrony Danych Osobowych;
17) **Raport** - przygotowane przez System informatyczny zestawienia zakresu i treści przetwarzanych danych;
18) **Polityka bezpieczeństwa** – niniejszy dokument;

19) **Poufności danych** - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
20) **Uwierzytelnianie** - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
21) **Baza danych osobowych** – każdy posiadający strukturę zbiór danych o charakterze osobowym, dostępnych według określonych kryteriów,
22) **Przetwarzanie danych** – 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,
23) **Usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
24) **System zarządzania bazą danych** – system oprogramowania zawierający mechanizmy zapewniające spójność i bezpieczeństwo danych, sprawny dostęp do danych, środki programistyczne służące do przetwarzania danych, jednoczesny dostęp do danych dla wielu użytkowników, środki pozwalające na regulację dostępu do danych, środki pozwalające na odtworzenie zawartości bazy danych po awarii,
25) **System informatyczny** – zbiór powiązanych ze sobą elementów: serwerów z systemami operacyjnymi, systemu zarządzania bazą danych, baz danych, oprogramowania (programów użytkowych), urządzeń końcowych (komputerów, terminali, drukarek) oraz urządzeń służących do komunikacji między sprzętowymi elementami systemu,

§ 2

1. Administrator danych, wyznacza Administratora Bezpieczeństwa Informacji oraz osobę upoważnioną do zastępowania Administratora Bezpieczeństwa Informacji.
2. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:
   1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Administratora,
   2) podejmowania stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych,
   3) niezwłocznego informowania Administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   4) nadzoru i kontroli Systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,
   5) fizycznego zabezpieczenia danych osobowych oraz obiektów, w których są gromadzone i przetwarzane.

3. Osoba zastępująca Administratora Bezpieczeństwa Informacji powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa Informacji.
4. Osoba zastępująca składa Administratorowi Bezpieczeństwa Informacji relację z podejmowanych działań w czasie jego zastępstwa.
5. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych osobowych, a w szczególności poprzez następujące działania:
   1) prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych,
   2) nadzoruje funkcjonowanie mechanizmów uwierzytelniania użytkowników w Systemie Informatycznym przetwarzającym dane osobowe oraz kontroli dostępu do danych osobowych,
   3) nadzoruje wykonywanie kopii zapasowych (awaryjnych), ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
   4) nadzoruje przeglądy, konserwacje oraz uaktualnienia Systemu Informatycznego służącego do przetwarzania danych osobowych,
   5) podejmuje stosowne działania zgodnie z niniejszą Polityką Bezpieczeństwa oraz Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych, w przypadku otrzymania informacji o naruszeniu zabezpieczeń Systemu informatycznego lub informacji o zmianach w sposobie działania Systemu informatycznego, programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych,
   6) przegląda niniejszą Politykę Bezpieczeństwa pod kątem aktualności i stosowalności nie rzadziej niż raz w roku.

Rozdział II

Podstawowe zasady związane z przetwarzaniem danych osobowych

§ 3

1. Ochrona danych osobowych przetwarzanych w SerwisPrawa.pl Sp zo.o obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych w SerwisPrawa.pl Sp zo.o, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy.
2. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.
3. Zachowanie tajemnicy w zakresie danych osobowych obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu.

4. Administrator Bezpieczeństwa Informacji jest odpowiedzialna za tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji, standardów, zaleceń oraz procedur dotyczących ochrony danych osobowych w SerwisPrawa.pl Sp zo.o Polecenia Administratora Bezpieczeństwa Informacji a także innych osób delegowanych i wyznaczonych do działań związanych z ochroną w zakresie ochrony informacji i bezpieczeństwa systemu informatycznego muszą być bezwzględnie wykonywane przez wszystkich pracowników i użytkowników systemu.

§ 4

1. Przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych. W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych), jednak wymaga to zgody indywidualnej administratora bezpieczeństwa informacji. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe oraz do pomieszczeń, w których znajdują się serwery baz danych lub przechowywane są kopie zapasowe mogą mieć wyłącznie osoby, które posiadają do tego upoważnienie nadane przez Administratora Bezpieczeństwa Informacji.
2. Kontrolą dostępu do pomieszczeń przeznaczonych do przetwarzania danych osobowych zajmuje się ochrona obiektu na podstawie upoważnień wydanych przez Administratora Bezpieczeństwa Informacji.
3. Przetwarzać dane osobowe może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych.
4. Wydanie upoważnienia następuje na wniosek przełożonego pracownika, który otrzymuje upoważnienie. Wniosek o wydanie upoważnienia składany jest w formie pisemnej do Administratora Bezpieczeństwa Informacji.

§ 5

1. Administrator dopuszcza możliwość przekazania danych osobowych innym administratorom. W takim przypadku, przetwarzanie danych osobowych odbywa się na podstawie umowy pomiędzy Administratorem a osobom trzecią jako administratorem, zawartej w formie pisemnej.
2. Umowa ta musi zawierać ściśle określony zakres przetwarzanych danych.
3. Przetwarzanie danych osobowych możliwe jest tylko w ustalonym przez umowę zakresie.
4. Powierzone dane podlegają przetwarzaniu i ochronie na takich samych zasadach jak te, które dotyczą Administratora, chyba, że umowa określi inne zasady ochrony danych osobowych.

5. Zmiana zasad związana z ochroną danych osobowych oraz ich przetwarzaniem przez administratora, któremu Administrator udostępnił dane osobowe, nie może:
   a) naruszać praw osób, których dane są przetwarzane;
   b) naruszać zasad związanych z ochrona danych osobowych przewidzianych we właściwych przepisach prawa;
   c) zmieniać celu przetwarzania danych osobowych;
   d) udostępniać danych innym administratorom bez zgody Administratora.
6. Zmiana zasad związanych z przetwarzaniem danych osobowych może dotyczyć nadawania uprawnień do przetwarzania danych osobowych.
7. Dostęp do powierzonych danych osobowych z sieci zewnętrznej musi odbywać się z zachowaniem odpowiednich zabezpieczeń.
8. Dostęp do danych musi być chroniony identyfikatorem oraz hasłem, a połączenie sieciowe realizujące dostęp do danych musi być odpowiednio szyfrowane.

Rozdział III

Opis zdarzeń naruszających ochronę danych osobowych

§ 6

1. Podział zagrożeń:
   1) Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) - ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej Systemu informatycznego; ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
   2) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania) - może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
   3) Zagrożenia zamierzone - świadome i celowe działania powodujące naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
      - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
      - nieuprawniony dostęp do systemu z jego wnętrza,
      - nieuprawnione przekazanie danych,
      - bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).
2. Naruszenie lub podejrzenie naruszenia Systemu informatycznego, w którym przetwarzane są dane osobowe następuje w sytuacji:

1) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.,
2) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
3) awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,
4) pojawienia się odpowiedniego komunikatu alarmowego,
5) podejrzenia nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,
6) naruszenia lub próby naruszenia integralności systemu lub bazy danych w tym systemie,
7) pracy w systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych - np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,
8) ujawnienia nieautoryzowanych kont dostępu do systemu,
9) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych np.
   - niezabezpieczone pomieszczenia,
   - nienadzorowane, otwarte szafy, biurka, regały,
   - niezabezpieczone urządzenia archiwizujące,
   - pozostawianie danych w nieodpowiednich miejscach – kosze, stoły itp.

Rozdział IV

Zabezpieczenie danych osobowych

§ 7

1. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych, a w szczególności:
   1) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobieganie przed pobraniem danych przez osobę nieuprawnioną,
   3) zapobieganie zmianie, utracie, uszkodzeniu lub zniszczeniu danych,
   4) zapewnianie przetwarzanie danych zgodnie z obowiązującymi przepisami prawa.

2. Zadania określone w pkt. 2 wykonuje w imieniu Administratora danych osobowych Administrator Bezpieczeństwa Informacji.

§ 8

1. Zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe:
   1) wszystkie pomieszczenia, w których przetwarza się dane osobowe, są zamykane na klucz,
   2) w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy, dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (na zewnętrznych nośnikach np. pendirve, płyta CD/DVD, dyskietka) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe – w szafach metalowych lub pancernych. Klucze od szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych,
   3) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach,
   4) budynek, w którym zlokalizowane są zbiory danych osobowych, jest nadzorowany przez pracowników ochrony fizycznej oraz posiada instalację alarmową.
2. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych następuje poprzez:
   1) podłączenie urządzenia końcowego (komputera, terminala, drukarki) do Sieci informatycznej dokonywane jest przez Administratora Bezpieczeństwa Informacji,
   2) udostępnianie użytkownikowi zasobów sieci (programów i baz danych), następuje na podstawie upoważnienia do przetwarzania danych osobowych,
   3) identyfikacja użytkownika w systemie następuje poprzez zastosowanie podwójnego uwierzytelnienia,
   4) przydzielenie indywidualnego identyfikatora każdemu użytkownikowi Systemu Informatycznego i rejestrowanie przez system czasu logowania użytkownika i rodzaju wprowadzonych przez niego danych,
   5) udostępnianie kluczy od centrum przetwarzania danych (serwerowni) tylko upoważnionym pracownikom,
   6) przechowywanie kopii zapasowych w zamykanej szafie metalowej, ognioodopornej umiejscowionej poza pomieszczeniami Administratora,
   7) stosowanie programu antywirusowego z zaporą antywłamaniową na komputerach ze środowiskiem operacyjnym MS Windows,
   8) zabezpieczenie hasłami kont na komputerach, używanie kont z ograniczonymi uprawnieniami do ciągłej pracy,

9) ustawienie monitorów stanowisk przetwarzania danych osobowych w sposób uniemożliwiający wgląd w dane osobom nieupoważnionym.

3. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych poprzez Internet:
   1) logiczne oddzielenie Sieci informatycznej (lokalnej), uniemożliwiające uzyskanie połączenia z bazą danych spoza Systemu Informatycznego, jak również uzyskanie dostępu z Systemu do sieci rozległej Internet,
   2) zastosowanie dwustopniowego zabezpieczenia Sieci lokalnej:
      a) pierwszy stopień ochrony stanowią listy dostępu ACL (Acces Control List) na głównym routerze uniemożliwiające nawiązanie połączenia z jakimkolwiek niewskazanym jawnie komputerem w sieci,
      b) drugi stopień ochrony stanowi lokalna brama sieciowa z zainstalowanym systemem typu firewall z funkcją analizy charakteru ruchu sieciowego, uniemożliwiającym nawiązanie połączenia do chronionych komputerów i blokującym ruch o charakterystyce niepożądanej lub mogącej zostać uznanej za szkodliwą.
4. Zabezpieczenia przed utratą danych osobowych w wyniku awarii:
   1) odrębne zasilanie sprzętu komputerowego,
   2) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,
   3) ochrona przed utratą zgromadzonych danych poprzez cykliczne wykonywanie kopii zapasowych, z których w przypadku awarii odtwarzane są dane i system operacyjny,
   4) ochrona przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych,
   5) zapewnienie właściwej temperatury i wilgotności powietrza dla pracy sprzętu komputerowego, poprzez zastosowanie klimatyzatorów,
   6) zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w serwerowni gaśnic, okresowo kontrolowanych przez specjalistę,
   7) zwiększenie niezawodności serwerów i urządzeń sieciowych poprzez logiczne rozmieszczenie ich w szafach serwerowych.

Rozdział V

Kontrola przestrzegania zasad zabezpieczenia danych osobowych

§ 9

1. Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikający z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

2. Administrator Bezpieczeństwa Informacji sporządza roczne plany kontroli zatwierdzone przez Administratora danych osobowych i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.
3. Na podstawie zgromadzonych materiałów, o których mowa w pkt. 2, Administrator Bezpieczeństwa Informacji sporządza roczne sprawozdanie i przedstawia je Administratorowi danych osobowych.

Rozdział VI

Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 10

1. W przypadku stwierdzenia naruszenia:
   a. zabezpieczenia systemu informatycznego,
   b. technicznego stanu urządzeń,
   c. zawartości zbioru danych osobowych,
   d. jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   e. innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, kradzież itp.)

   każda osoba jest zobowiązana do niezwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji i bezpośredniego przełożonego.
2. Po wykonaniu czynności określonych w pkt. 1 należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę zdarzenia,
   4) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego lub aplikacji użytkowej,
   5) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
   6) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej.
3. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa Informacji lub osoba go zastępująca:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy,
2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
3) w razie potrzeby powiadamia o zaistniałym naruszeniu Administratora danych,
4) jeżeli zachodzi taka potrzeba zleca usuniecie występujących naruszeń, oraz powiadamia odpowiednie instytucje,

4. Raport, o którym mowa w ust. 4, Administrator Bezpieczeństwa Informacji niezwłocznie przekazuje Administratorowi danych osobowych, a w przypadku jego nieobecności osobie uprawnionej.
5. Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez zespół powołany przez Administratora danych.
6. Analiza, o której mowa w pkt. 6, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rodział VII

Minimalizacja

Spółka dba o minimalizację przetwarzania danych pod kątem : (I) adekwatności danych do celów (ilości danych i zakresu przetwarzania), (II) dostępu do danych , (III) czasu przechowywania danych.

1. **Minimalizacja zakresu** - Spółka zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilości przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrążenia RODO.
   Spółka dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.
   Spółka przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (privacy by design)
2. **Minimalizacja dostępu** – Spółka stosuje ograniczenia dostępu do danych, osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).
   Spółka stosuje kontrolę dostępu fizycznego.

Spółka dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.

Spółka doonuje okresowego przeglądu ustawionych użytkowników systemów i aktualizacje ich nie rzadziej niż raz na rok.

Szczegółowe zasady kontroli dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Spółki.

3. **Minimalizacja czasu** – Spółka wdąza mechanizmy kontroli cyklu życia danych osobowych w Spółce, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze. Dane,których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów produkcyjnych Spółki, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Spółkę. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

Rozdział VIII

Postanowienia końcowe

§ 11

4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, wszczyna się postępowanie dyscyplinarne.
5. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.