Polityka bezpieczeństwa przetwarzania danych osobowych w SCANIX Sp. z o.o. w restrukturyzacji

Rozdział 1
Postanowienia ogólne

§ 1

Celem Polityki bezpieczeństwa przetwarzania danych osobowych w SCANIX Sp. z o.o. w restrukturyzacji, zwanej dalej „Polityką bezpieczeństwa", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

§ 2

Polityka bezpieczeństwa została utworzona w związku z wymaganiami zawartymi 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, Ustawie z 29 sierpnia 1997 r. o ochronie danych osobowych oraz Rozporządzeniu ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

§ 3

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników.

§ 4

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w SCANIX Sp. z o.o. w restrukturyzacji rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   a) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   b) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   c) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   d) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
   e) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   f) zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 5

1. Administratorem danych osobowych przetwarzanych w SCANIX Sp. z o.o. w restrukturyzacji, z siedzibą 40-057 Katowice, ul. Polskiego Czerwonego Krzyża 10.
2. Administrator danych osobowych powołuje Inspektora Ochrony Danych w osobie Bartłomieja Gasińskiego (adres e-mail: bartłomiej.gasinski@scanix.pl), którego zadania określa § 17.

Rozdział 2
Definicje

§ 6

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

a) **administrator danych osobowych –** SCANIX Sp. z o.o. w restrukturyzacji;
b) **RODO –** Rozporządzenie 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;
c) **ustawa** – rozumie się przez to Ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2016 r. poz. 922);
d) **rozporządzenie** – Rozporządzenie ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. nr 100, poz. 1024);
e) **dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak – **imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej**;
f) **zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
g) **przetwarzane danych –** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak **zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie**;
h) **system informatyczny –** rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
i) **system tradycyjny** – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze;
j) **zabezpieczenie danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

k) **administrator systemu informatycznego** – rozumie się przez to osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi;
l) **użytkownik** – rozumie się przez to upoważnionego przez administratora danych osobowych lub administratora bezpieczeństwa informacji (o ile został powołany), wyznaczonego do przetwarzania danych osobowych pracownika;
m) **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
n) **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Rozdział 3
Zakres stosowania

§ 7

1. W SCANIX Sp. z o.o. w restrukturyzacji przetwarzane są w szczególności dane osobowe klientów, pracowników, kontrahentów zebrane w zbiorach danych osobowych.
2. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
3. Polityka bezpieczeństwa zawiera dokumenty dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 8

Politykę bezpieczeństwa stosuje się w szczególności do:
a) danych osobowych przetwarzanych w systemach: SimpleRIS, SimplePACS, RAKS, Płatnik, LogicalDOC. Zbiory danych zostały określone w załączniku nr 1;
b) wszystkich informacji dotyczących danych pracowników, klientów, kontrahentów;
c) wszystkich danych które identyfikują lub umożliwiają identyfikację osoby fizycznej;
d) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych;
e) rejestru osób dopuszczonych do przetwarzania danych osobowych;
f) innych dokumentów zawierających dane osobowe.

§ 9

1. Zakresy ochrony danych osobowych określone przez dokumenty Polityki bezpieczeństwa mają zastosowanie do systemów informatycznych, w których są przetwarzane dane osobowe, a w szczególności do:
    a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;
    b) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
    c) wszystkich pracowników, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez dokumenty Polityki bezpieczeństwa zobowiązani są wszyscy pracownicy, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

Rozdział 4
Wykaz zbiorów danych osobowych

Szczegółowo zbiory danych zostały określone w załączniku nr 2.

Rozdział 5
Wykaz budynków, pomieszczeń i stref do przetwarzania danych osobowych

§ 10

Dane osobowe przetwarzane są w budynkach określonych w załączniku nr 3.

Rozdział 6
Środki techniczne i organizacyjne zabezpieczenia danych osobowych

§ 11

1. Opis środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych szczegółowo opisano w załączniku nr 4;.

2. Zabezpieczenia organizacyjne:
   a) sporządzono i wdrożono Politykę bezpieczeństwa;
   b) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w SCANIX Sp. z o.o. w restrukturyzacji;
   c) wyznaczono Inspektora Ochrony Danych*;*
   d) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych bądź osobę przez niego upoważnioną – wzór upoważnienia stanowi załącznik nr 5;

      Wyjątek stanowią osoby wykonujące zawód medyczny. Osobą wykonującą zawód medyczny jest, zgodnie z art. 2 ust. 1 pkt 2 Ustawy z 15 kwietnia 2011 r. o działalności leczniczej, osoba uprawniona na podstawie odrębnych przepisów do udzielania świadczeń zdrowotnych oraz osoba legitymująca się nabyciem fachowych kwalifikacji do udzielania świadczeń zdrowotnych w określonym zakresie lub w określonej dziedzinie medycyny. Zgodnie z art. 24 ust. 2 Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta do przetwarzania danych zawartych w dokumentacji medycznej w celu ochrony zdrowia, udzielania oraz zarządzania udzielaniem świadczeń zdrowotnych, utrzymania systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnienia bezpieczeństwa tego systemu, są uprawnione osoby wykonujące zawód medyczny. **W SCANiX Sp. z o.o. w restrukturyzacji są to: lekarze, technicy elektroradiolodzy, pielęgniarki.**

   e) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;
   f) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
   g) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;

h) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
i) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
j) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.

3. Zabezpieczenia techniczne:
   a) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą systemu Firewall, NAT oraz dzięki zastosowaniu na każdym z komputerów klienckich programu przeciwdziałającego szkodliwemu oprogramowaniu i wykradaniu danych z aktualna bazą antywirusową;
   b) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową;
   c) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła przez system Active Directory.
4. Środki ochrony fizycznej:
   a) obszary, na których przetwarzane są dane osobowe, poza godzinami pracy, chronione są zabezpieczeniami fizycznymi;
   b) urządzenia służące do przetwarzania danych osobowych umieszcza się w zamykanych pomieszczeniach.

Rozdział 9
Zadania administratora danych osobowych lub Inspektora Ochrony Danych

§ 16

Do najważniejszych obowiązków administratora danych osobowych lub Inspektora Ochrony Danych należy:

1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki,
3) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
5) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych, prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
6) nadzór nad bezpieczeństwem danych osobowych,
7) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
8) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

Rozdział 10
Zadania administratora systemów informatycznych

§ 17

1. Inspektor Ochrony Danych odpowiedzialny jest za:
    a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
    b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
    d) współpraca z organem nadzorczym;
    e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
    f) Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
2. Administrator systemów informatycznych odpowiedzialny jest za:
    a) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych;
    b) optymalizację wydajności systemu informatycznego, instalacji i konfiguracji sprzętu sieciowego i serwerowego;
    c) instalacje i konfiguracje oprogramowania systemowego, sieciowego;
    d) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem;
    e) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych;
    f) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych;
    g) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego;
    h) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie;
    i) przyznawanie na wniosek administratora danych osobowych lub administratora bezpieczeństwa informacji ściśle określonych praw dostępu do informacji w danym systemie;
    j) wnioskowanie do administratora danych osobowych lub administratora bezpieczeństwa informacji w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń;
    k) zarządzanie licencjami, procedurami ich dotyczącymi;
    l) prowadzenie profilaktyki antywirusowej.
3. Praca administratora systemu informatycznego jest nadzorowana pod względem przestrzegania ustawy o ochronie danych osobowych, rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim

powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz Polityki bezpieczeństwa przez administratora danych lub administratora bezpieczeństwa informacji.

Rozdział 11
Sprawozdanie roczne stanu systemu ochrony danych osobowych

§ 18

1. Corocznie, do dnia 31 marca, Inspektor Ochrony Danych przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych i przekazuje do administratora danych osobowych.
2. Sprawozdanie przygotowywane jest w formie pisemnej.

Rozdział 12
Szkolenia użytkowników

§ 19

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada administrator danych osobowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami Ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u administratora danych osobowych, a także o zobowiązaniu się do ich przestrzegania.
4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
5. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemów informatycznych przetwarzających dane osobowe.

Rozdział 13
Postanowienia końcowe

§ 20

1. Administrator danych osobowych lub Inspektor Ochrony Danych ma obowiązek zapoznać z treścią Polityki każdego użytkownika.
2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
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, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

5. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.