Polityka Bezpieczeństwa Informacji w „LekSeek Polska Spółka z ograniczoną odpowiedzialnością” Spółce komandytowej

LekSeek Polska 2018

§ 1

Polityka bezpieczeństwa w „LekSeek Polska Spółka z ograniczoną odpowiedzialnością" Spółce komandytowej (dalej LekSeek lub LekSeek Polska) została wprowadzona zgodnie z aktami prawnymi obowiązującymi na terytorium Rzeczypospolitej Polskiej w szczególności:

1. Konstytucji Rzeczypospolitej Polskiej (art. 47 i 51 Konstytucji Rzeczypospolitej Polskiej).
2. Ustawy z dnia 10 maja 2018 roku. o ochronie danych osobowych.
3. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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).

§ 2

1. Podczas realizacji polityki bezpieczeństwa informacji zapewnia się ich:
   - **poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
   - **integralność** – dane nie mogą być modyfikowane i niszczone w sposób nieautoryzowany
   - **rozliczalność** – każde działanie na danych może być jednoznacznie przypisane konkretnej osobie
   - **autentyczność** – zapewnienie, że tożsamość podmiotu jest taka, jak zadeklarowana
   - **niezaprzeczalność** – uczestnictwo w całości lub części wymiany informacji przez jeden z podmiotów uczestniczących w wymianie jest niepodważalne
   - **niezawodność** – zamierzone zachowania mają prowadzić do określonych skutków
   - **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu

§ 3

1. Polityka bezpieczeństwa informacji w LekSeek Polska ma na celu zniwelowanie, bądź maksymalną redukcję możliwości negatywnych konsekwencji w zakresie:
   - naruszeń danych osobowych przetwarzanych przez LekSeek Polska
   - naruszeń litery prawa
   - utraty bądź naruszenia dobrego imienia firmy
   - zakłóceń organizacji pracy spowodowanych niepożądanymi zdarzeniami
   - strat finansowych w wyniku nałożonych kar, bądź spowodowanych zakłóceniami w systemie przepływu informacji

2. Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych LekSeek dokłada szczególnej staranności w celu dbania o interesy osób, których dane dotyczą, a w szczególności zapewnia warunki, by dane były:
   - przetwarzane zgodnie z prawem,
   - zbierane do jasno określonych i zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   - przechowywane były w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celów przetwarzania.

§ 4

1. Jeżeli w tekście padnie określone pojęcie rozumiemy je, jako:

Firma, LekSeek lub LekSeek Polska – „LekSeek Polska Spółka z ograniczoną odpowiedzialnością” Spółka komandytowa z siedzibą w Warszawie ul. Puławska 465 02-844 Warszawa.
Administrator (Administrator Danych Osobowych/ ADO) - LekSeek Polska zarówno jako Administrator w odniesieniu do własnych zasobów danych osobowych, jak i w charakterze podmiotu, któremu powierzono przetwarzanie danych osobowych z zasobów innych podmiotów.
IOD (Inspektor Ochrony Danych) – osoba powołana przez ADO do nadzorowania przestrzegania zasad określonych w niniejszym dokumencie oraz wymagań w zakresie określonym poprzez obowiązujące w tej kwestii przepisy prawne.
Polityka – Polityka bezpieczeństwa informacji w skład, której wchodzą środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych informacji a w szczególności danych osobowych. Zawiera procedury nadawania i zabierania uprawnień pracownikom przetwarzających dane osobowe, spis pomieszczeń gdzie zachodzi wyżej wymieniony proces, opis środków bezpieczeństwa zastosowanych w Firmie, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, a także tryb postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa informacji w systemach informatycznych lub kartotekach albo w sytuacji powzięcia podejrzenia o takim naruszeniu. Wszelkie postanowienia Polityki odnoszą się zarówno do własnych zasobów danych osobowych Administratora, jak i danych, dla których Administrator jest podmiotem, któremu powierzono przetwarzanie danych osobowych z zasobów innych podmiotów.

Bezpieczeństwo informacji – określony poprzez politykę i przepisy prawne stan rzeczy w firmie, w którym przepływ informacji jest niezagrożony żadną zewnętrzną, nieautoryzowaną ingerencją. W szczególności rozumie się go poprzez zgodny z prawem i poufny sposób przetwarzania danych osobowych, ale także utrzymany w poufności przepływ informacji w firmie niedotyczący tych danych. Inaczej ujmując: bezpieczeństwo informacji to stan, w którym każda informacja, która jest w firmie niejawna, pozostaje bez nieautoryzowanego wglądu dla osób do tego nieuprawnionych.
Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.
Dane osobowe –. oznaczają wszelkie 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.
Ograniczenie przetwarzania – oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania..
Profilowanie – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów

dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
Pseudonimizacja – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
Zbiór danych – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
Przetwarzanie 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.
Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
Dane genetyczne – oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.
Dane biometryczne – oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne..
Dane dotyczące zdrowia – oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia.
System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych używanych w firmie podczas procesu przetwarzania danych.
Dział Firmy - rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, na czele której stoi zwierzchnik.
Pracownik – osoba zatrudniona poprzez jakąkolwiek formę umowy w firmie LekSeek Polska .
Użytkownik Systemu – rozumie się przez to osobę wyznaczoną przez ADO lub IOD albo Osobę przez nich upoważnioną, uprawnioną do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz kartotekach, posiadającą ustalony identyfikator i hasło.
Login – ustalony przez ADO/IOD identyfikator (ciąg znaków) pozwalający na jednoznaczne określenie jego indywidualnego właściciela.
Osoba upoważniona – osoba upoważniona przez ADO/IOD do wykonywania czynności przetwarzania danych osobowych w zakresie określonym w upoważnieniu.
Pomieszczenia - pomieszczenia lub części pomieszczeń określone przez Administratora tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz w formie papierowej.

W celu optymalizacji poziomu bezpieczeństwa informacji szereg wdrożonych zabezpieczeń funkcjonuje równolegle do siebie. Ochrona danych realizowana jest poprzez połączenie zabezpieczeń fizycznych, realizacji odpowiednich procedur organizacyjnych, aplikacje systemowe, oraz poprzez świadomość użytkowników.

§ 5

1. **Administrator** zakres odpowiedzialności:
   - Formułowanie i wdrażanie zakresu warunków technicznych mających realizować ochronę danych w zakresie bezpieczeństwa informacji w tym ochrony danych osobowych.
   - Decyduje o zakresie, celach i metodach przetwarzania danych osobowych.
   - Odpowiada za zgodne z prawem przetwarzanie danych osobowych w LekSeek Polska.

2. **IOD** zakres obowiązków i uprawnień:
   - Egzekucja zgodnego z prawem przetwarzania danych osobowych w LekSeek.
   - Wydaje upoważnienia do przetwarzania danych osobowych określając w nich zakres i czas obowiązywania. (Załącznik nr 1).
   - Odwołuje upoważnienia (Załącznik nr 2).
   - Prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych (zał. nr 3).
   - Ewidencjonuje oświadczenia osób upoważnionych o zapoznaniu się z zasadami bezpieczeństwa informacji w LekSeek.
   - Prowadzi szkolenia pracowników, podejmuje działania na rzecz podnoszenia świadomości pracowników w zakresie ochrony danych osobowych.
   - Może wydawać pracownikom LekSeek polecenia i wyznaczać zadania, które mają na celu utrzymanie bądź korektę stanu zachowania bezpieczeństwa informacji.
   - Zarządzanie bezpieczeństwem przetwarzania danych osobowych w systemach informatycznych.
   - Wdrażanie i doskonalenie metod zabezpieczania danych w systemach komputerowych.
   - Przydzielanie loginów i haseł użytkownikom systemów komputerowych.
   - Nadzorowanie prac związanych z rozwojem, modyfikacją, konserwacją i serwisowaniem systemów.
   - Zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych.
   - Jest odpowiedzialny za nadzór nad wykonywaniem i przechowywaniem cyfrowych kopii danych w Firmie.

4. Za przestrzeganie polityki bezpieczeństwa informacji w odpowiednich działach odpowiedzialni są zwierzchnicy tychże działów, którzy (w swoim dziale) odpowiadają także za zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia.

5. Realizację wyżej zamieszczonych zamierzeń powinny zagwarantować następujące założenia:

   - Wdrożenie procedur określające postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych, oraz ich odpowiedzialność za bezpieczeństwo tych danych.
   - Przeszkolenie pracowników w zakresie bezpieczeństwa informacji, a w

szczególności w zakresie bezpieczeństwa przetwarzania danych osobowych.

- Przypisanie użytkownikom określonych systemów informatycznych indywidualnych atrybutów (hasło, login), które w jednoznaczny sposób pozwolą na identyfikację danego użytkownika a także na pełen rejestr jego działań w tychże systemach.
- Monitoring i podejmowanie działań wykluczających słabe ogniwa w systemie zabezpieczeń.
- Okresowe kontrole przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.
- Opracowanie procedur przywracania systemu w przypadku wystąpienia awarii.
- Wdrożenie procedur zatrudniania i zwalniania osób, które będą uwzględniały bezpieczeństwo informacji w firmie, w szczególności bezpieczeństwo przetwarzania danych osobowych.

§ 6

1. Za naruszenie bezpieczeństwa informacji uważa się w szczególności:

- Nieautoryzowany dostęp, lub próba nieautoryzowanego dostępu do danych osobowych lub obszarów, w których są one przechowywane.
- Wszelkie nieuprawnione modyfikacje danych osobowych, bądź ich próby (zmian wartości danych, utrata całości lub części danych).
- Zmianę lub utratę danych zapisanych na kopiach zapasowych.
- Naruszenie lub próbę naruszenia poufności danych lub ich części.
- Nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu).
- Udostępnienie osobom nieupoważnionym danych osobowych lub ich części.
- Zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w systemy informatyczne i zbiory dokumentów zmierzające do zakłócenia ich działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemach informatycznych lub kartotekach.
- Inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy.
- Włamanie lub jego próba do budynku lub pomieszczeń, w których przetwarzane są dane osobowe.

§ 7

Przedsięwzięcia zabezpieczające przed naruszeniem bezpieczeństwa informacji, w szczególności ochrony danych osobowych.

1. Każdy nowozatrudniony pracownik podlega szkoleniu w dziedzinie przepisów o ochronie danych osobowych, obowiązków w tym zakresie do niego należących a także zapoznawany jest z polityką bezpieczeństwa firmy. Szkolenia nowych pracowników odbywane są na wniosek osoby kierującej daną komórką, w której zostaje ona zatrudniona na podstawie dowolnej formy umowy, w tym praktyki, czy staż.

2. Wszyscy pracownicy podlegają szkoleniom okresowym w dziedzinie zmian przepisów w

kwestii ochrony danych osobowych, zmian w polityce bezpieczeństwa, czy też sytuacji, gdy IOD oceni, że takie szkolenia należy przeprowadzić.

3. Za szkolenia odpowiedzialny jest IOD, lub osoba wyznaczona na zastępstwo podczas jego nieobecności.

§ 8

1. Osoby przetwarzające dane osobowe posiadają stosowne upoważnienia do pracy na tychże. Upoważnienia wydaje ADO lub IOD w imieniu ADO na wniosek przełożonego działu, gdzie pracuje dana osoba.

2. ADO lub IOD odwołuje upoważnienia na wniosek przełożonego działu, gdzie pracuje dana osoba, np. w przypadku rozwiązania umowy współpracy. IOD ma prawo do natychmiastowego odwołania upoważnienia w sytuacji, gdy dana osoba rażąco nie stosuje się do dyrektyw zawartych w polityce firmy. Odwołanie upoważnienia wiąże się z utratą uprawnień wykonywania obowiązków służbowych związanych z przetwarzaniem danych osobowych.

3. IOD prowadzi ewidencję upoważnień.

§ 9

1. Pracownicy powinni mieć świadomość zaistnienia sytuacji, w których może zostać naruszone bezpieczeństwo informacji.
Pod tym kątem zaleca się:

- Zwracanie szczególnej uwagi na osoby niezatrudnione przebywające na terenie LekSeek.
- Przestrzeganie procedur wchodzenia i wychodzenia z budynku.
- Przestrzeganie zasad i procedur ochrony danych osobowych podczas wykonywania obowiązków służbowych.
- Zgłaszanie wszelkich podejrzanych i nietypowych sytuacji IOD, bądź w przypadku ich nieobecności przełożonemu.

2. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba, która tej czynności dokonuje.

3. Osoby zarządzające poszczególnymi działami, osoby zajmujące samodzielne stanowiska a także użytkownicy są zobowiązani, na podstawie dokonanej identyfikacji poszczególnych zagrożeń o informowaniu o nich IOD, do tego zwierzchnicy działów zobowiązani są do przedkładania stosownych dla specyfiki działu propozycji niwelowania owych zagrożeń.

4. Do zabezpieczeń przed naruszeniem bezpieczeństwa informacji należą:

- Ochrona w holu firmy.
- Monitoring przy wejściach do budynku.
- Zabezpieczenie wejść odpowiednimi zamkami.
- Przechowywanie ważnej dokumentacji w szafach z zamkami.
- Do kluczy mają dostęp osoby upoważnione.
- Do obsługi systemów informatycznych stosuje się instrukcję, która minimalizuje ryzyko naruszenia bezpieczeństwa.
- Plomby stosowane na szafach w których nie ma bezpośredniego nadzoru

personelu.

5. IOD prowadzi ewidencję kluczy do firmy pomieszczeń zajmowanych przez LekSeek wraz z osobami, którym je udostępniono.

6. Osoby, które mają dostęp do danych zobowiązane są do rzetelnego prowadzenia dokumentacji, kompletność wprowadzanych danych, a także ich rzetelność.

7. Opuszczenie stanowiska pracy związanego z przetwarzaniem danych osobowych obowiązkowo powinno się wiązać z odpowiednim zabezpieczeniem danych, na których wykonywano działania. Dokumenty należy odłożyć do miejsca przechowywania, system komputerowy należy odpowiednio zabezpieczyć.

8. Klucze do szaf, gdzie przechowywane są dane osobowe posiadają tylko pracownicy do tego upoważnieni.

9. Dostęp do pomieszczeń firmowych poza godzinami pracy monitorowany jest przez personel ochrony budynku.

10. Dokumentacji, która zawiera zbiory danych osobowych nie można wynosić poza teren LekSeek. Wyjątki stanowi uzasadniona potrzeba, za akceptacją IOD.

11. Osoby pracujące przy dokumentacji są zobowiązane do niezwłocznego poinformowania IOD o sytuacji, w której miał miejsce nieupoważniony dostęp do dokumentów, bądź zaszło podejrzenie takiego dostępu.

12. Zabrania się pozostawiania dokumentów zawierających dane osobowe w drukarkach, skanerach, kopiarkach bez nadzoru.

13. Dokumenty zawierające dane osobowe utylizuje się za pomocą niszczarki.

14. Ostatnia osoba opuszczająca zajmowane pomieszczenie jest odpowiedzialna za sprawdzenie:

- Czy wszystkie okna w pomieszczeniu są zamknięte.
- Czy wszystkie komputery w pomieszczeniu są wyłączone/wylogowane.
- Czy w innych otwartych pomieszczeniach nie są obecne osoby postronne.

Po wykonaniu tych czynności pracownik podpisuje się na odrębnej liście.

§ 10

1. Osoby postronne wchodzące do Firmy przebywają na jej obszarze pod nadzorem pracowników.

2. Prace konserwacyjne w obszarach, gdzie odbywa się przetwarzanie danych mogą być wykonywane wyłącznie w obecności pracowników Firmy.

3. Na czas obecności osób postronnych w obszarze przetwarzania danych pracownik powinien w miarę możliwości upewnić się, czy owe osoby nie mają wglądu w przetwarzane dane. Jeżeli tak, to należy podjąć działania zapobiegawcze (przestawienie monitora, laptopa, przeniesienie dokumentów). Jeżeli takie działanie nie przyniesie skutków, pracownik zobowiązany jest do przerwania pracy na danych i zabezpieczenia ich przed wglądem.

§ 11

1. Podczas pracy na komputerze każdy użytkownik powinien stosować się do **Instrukcji zarządzania systemem informatycznym (zał 1)**

2. Każdy użytkownik systemu informatycznego ma dostęp do instrukcji poprzez drogę mailową, a także może wnioskować o nią u IOD.

3. Osobiste urządzenia mobilne – dopuszcza się ich używanie, jednakże zakazuje się rejestracji na nich jakichkolwiek informacji związanych z danymi osobowymi.

§ 12

1. Struktura informatyczna firmy składa się z komputerów połączonych siecią LAN. Komputery i urządzenia mobilne mają dostęp do Internetu.

2. W ramach tej struktury funkcjonują systemy informatyczne:
- DistroCRM sprzedaż – służy do przechowywania danych firm i osób korzystających z usług marketingowych LekSeek Polska
- DistroCRM lekarze – służy do przechowywania danych lekarzy korzystających z subskrypcji publikacji firmy i kontaktów marketingowych z nimi.
- Pakiet Microsoft Office
- Mozilla Thunderbird – klient poczty elektronicznej

Programy są niezależne i posiadają samodzielne bazy danych wprowadzane do systemów manualnie.

§ 13

Na podstawie dostępnej wiedzy i dotychczasowych doświadczeń związanych z działalnością firmy LekSeek Polska, a także w związku z zastosowanymi zabezpieczeniami, poziom ryzyka naruszenia bezpieczeństwa informacji ocenia się na niski.

§ 14

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznego zgodnie z wymogami przepisów, stosuje się wysoki poziom bezpieczeństwa. Inspektor Ochrony Danych przeprowadza okresową analizę ryzyka (minimalnie raz na 2 lata) dla poszczególnych systemów i na tej podstawie przedstawiają ADO propozycje dotyczące środków technicznych i organizacyjnych służących zapewnieniu właściwej ochrony danych.

§ 15

1. Podsumowanie postępowania w przypadku naruszenia bezpieczeństwa informacji.

2. Każdy pracownik LekSeek, który stwierdzi fakt naruszenia bezpieczeństwa informacji w Firmie bądź posiadający informację mogącą mieć wpływ na owe bezpieczeństwo, jest zobowiązany do niezwłocznego poinformowania o tym fakcie IOD bądź przełożonego, zaraz po wykonaniu czynności uwzględnionych w ust. 3.

3. Przy stwierdzeniu faktu naruszenia bezpieczeństwa informacji, każdy pracownik jest zobowiązany do podjęcia natychmiastowych czynności niezbędnych do zniwelowania skutków tego naruszenia, oraz w miarę możliwości ustalenia przyczyny i identyfikacji sprawcy tego naruszenia.

4. W przypadku naruszenia bezpieczeństwa informacji należy przerwać wszelkie działania mogące utrudnić analizę wystąpienia naruszenia i udokumentowania zdarzenia. Należy też bez uzasadnionej przyczyny nie opuszczać miejsca takiego zdarzenia.

5. Formy potencjalnych naruszeń bezpieczeństwa danych osobowych/bezpieczeństwa informacji i działań zapobiegawczych określa odrębny dokument.

6. Niezależnie od sformułowania dokumentu określającego potencjalne naruszenia bezpieczeństwa, każdy pracownik zobowiązany jest do samodzielnej oceny czy zdarzenie, którego jest świadkiem/uczestnikiem jest formą naruszenia bezpieczeństwa, mimo iż nie zostało ono uwzględnione w tabeli.

7. Po wykonaniu czynności zawartych w ustępie trzecim pracownik, bądź jego przełożony, zobowiązany jest do spisania wstępnego raportu z incydentu naruszenia bezpieczeństwa, który niezwłocznie przedkładany jest IOD.

§ 16

1. W przypadku stwierdzenia incydentu naruszającego bezpieczeństwo informacji IOD podejmuje następujące kroki:

- Zapoznanie się z bieżącą sytuacją i podjęcie wyboru co do schematu postępowania, który uwzględnia przede wszystkim dobro osób, których zostało naruszone bezpieczeństwo danych osobowych. Następnie działania mają w miarę możliwości zabezpieczać prawidłowe funkcjonowanie LekSeek.
- Ma prawo wydawać polecenia każdemu pracownikowi LekSeek, jeżeli służą one zniwelowaniu skutków naruszenia bezpieczeństwa, czy zapobieżeniu dalszym incydentom naruszenia bezpieczeństwa.
- Ma prawo zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa od każdej osoby, wobec której będzie zachodziło prawdopodobieństwo tego, że posiada jakiekolwiek informacje mogące tego zdarzenia dotyczyć. Osoba zobowiązana jest udzielić wyjaśnień niezwłocznie.
- Rozważa celowość i potrzebę powiadomienia o tym zdarzeniu osób zarządzających LekSeek.

2. Następnie IOD raportuje dane zdarzenie w księdze incydentów naruszenia bezpieczeństwa informacji.

3. IOD poprzez analizę incydentu/incydentów i zebranie opinii przedstawia plan działań naprawczych i zaradczych, tak by w przyszłości zniwelować bądź zminimalizować ryzyko wystąpienia kolejnych incydentów.

§ 17

1. Wobec pracownika LekSeek, który w sposób świadomy i celowy narusza bezpieczeństwo informacji LekSeek, bądź też w taki sam sposób zataja informacje o takim naruszeniu, bądź świadomie i celowo uniemożliwia działania zapobieżenia naruszeń

bezpieczeństwa może zostać wszczęte natychmiastowe postępowanie dyscyplinarne.

2. W razie celowego i rażącego narażenia firmy na straty pracownik może być obciążony karą finansową w wysokości miesięcznego wynagrodzenia wyliczonego na podstawie średniej z trzech ostatnich otrzymanych wynagrodzeń. Dodatkowo LekSeek może obciążyć taką osobę kosztami poniesionych przez firmę strat.

3. Kara dyscyplinarna i/lub finansowa w takim wypadku, nie wyklucza odpowiedzialności karnej, jaka wynika z powszechnie obowiązujących przepisów o ochronie danych osobowych.

Warszawa, dnia 25.05.2018 roku

zatwierdzam:

Piotr Pajek – Prezes Zarządu „LekSeek Polska Spółka z ograniczoną odpowiedzialnością”

Spis załączników:

1. Instrukcja zarządzania systemem informatycznym
2. Wzór upoważnienia do przetwarzania danych osobowych
3. Ewidencja osób upoważnionych – imię, nazwisko – zakres upoważnienia
4. Ewidencja użytkowników systemów – imię, nazwisko – login – program
5. Spis pomieszczeń, w których przetwarzane są dane osobowe
6. Indeks incydentów naruszenia bezpieczeństwa informacji
7. Wzór raportu z incydentu naruszenia bezpieczeństwa informacji
8. Ewidencja baz danych osobowych
9. Tabela form naruszeń danych osobowych.
10. Wzór oświadczenia pracownika o zachowaniu poufności informacji.