KAMSOFT S.A.

OSWAJAMY ŚWIAT
INFORMATYKI

Od 35 lat rozwijamy profesjonalne
rozwiązania IT dla sektora ochrony zdrowia

Medycyna | Farmacja | E-zdrowie | Diagnostyka | Wterynaria | Ubezpieczenia

Numer: Z03-05-02-6 Data wydania: 2019-11-18

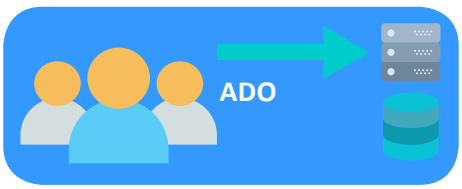
Dobre praktyki w zabezpieczaniu danych osobowych

Istotą wszystkich działań związanych z utrzymaniem odpowiedniego poziomu bezpieczeństwa jest świadomość, że bezpieczeństwo to proces, który należy doskonalić oraz monitorować w sposób ciągły. Błędnym podejściem jest traktowanie bezpieczeństwa jako np. jeden z etapów w ramach projektowania systemu – wytworzony raz na zawsze. Na bezpieczeństwo należy patrzeć kompleksowo starając się przewidzieć różne scenariusze zagrożeń i ataków prowadzących do naruszenia bezpieczeństwa w tym naruszeń związanych z ochroną danych osobowych co przedstawia poniższy diagram.

Celem dokumentu jest wskazanie elementów związanych z zabezpieczeniem przetwarzania danych osobowych, uświadomienie zagrożeń oraz wskazanie dostępnych zabezpieczeń, które powinien wdrożyć Administrator Danych Osobowych (ADO) w celu ochrony swoich zasobów, w tym danych osobowych. Celem dokumentu jest również uświadomienie faktu, że to na ADO spoczywa konieczność wdrożenia skutecznych zabezpieczeń wynikających z przeprowadzonej analizy ryzyka. Zakup systemu informatycznego nie zwalnia ADO z odpowiedzialności za dane oraz z konsekwencji zmaterializowania się zagrożeń w tym ich utraty lub kradzieży czy nieautoryzowanego dostępu do danych. ADO jest odpowiedzialny za wdrożenie odpowiednich środków technicznych i organizacyjnych, które podniosą bezpieczeństwo danych osobowych.

1. Relacja ADO – dostawca oprogramowania

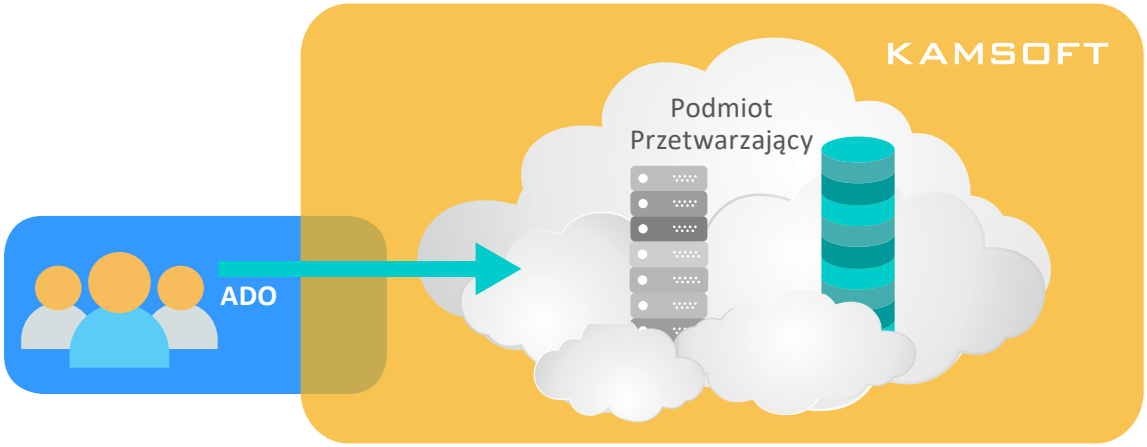
1.1 Model korzystania z oprogramowania „na miejscu” (on premise)



W modelu „na miejscu” - ADO samodzielnie użytkuje system informatyczny, zainstalowany na własnej infrastrukturze, samodzielnie go utrzymując i serwisując.

UWAGA! W MODELU „NA MIEJSCU”, ADO W CAŁOŚCI ODPOWIADA ZA UTRZYMANIE I ADMINISTRACJĘ SYSTEMEM, OCENĘ RYZYKA I WPROWADZENIE ZABEZPIECZEŃ ADEKWATNYCH DO ZAGROŻEŃ.

1.2 Model „chmurowy” korzystania z oprogramowania jako usługi (Software as a Service – SaaS)

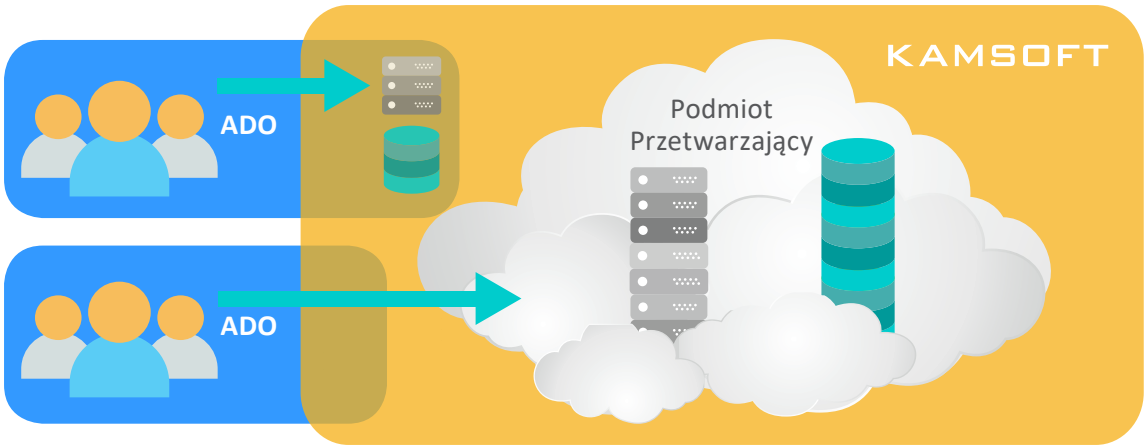


ADO użytkuje system informatyczny udostępniany jako usługę, zarządzaniem infrastrukturą, utrzymaniem i zabezpieczeniem systemu opiekuje się dostawca oprogramowania (Podmiot Przetwarzający) na mocy i na zasadach zawartej umowy korzystania z usługi oraz umowy powierzenia danych osobowych.

W MODELU OPROGRAMOWANIA JAKO USŁUGI, W ZNACZNEJ CZĘŚCI PODMIOT PRZETWARZAJĄCY WSPIERA ADO W UTRZYMANIU I ADMINISTRACJI SYSTEMEM, ANALIZIE RYZYKA I WPROWADZENIU ODPOWIEDNICH ZABEZPIECZEŃ.

W MODELU OPROGRAMOWANIA JAKO USŁUGI, ADO NADAL ODPOWIADA ZA CAŁOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH, W SZCZEGÓLNOŚCI W ZAKRESIE ORGANIZACJI I PROCESÓW PRZETWARZANIA DANYCH OSOBOWYCH.

1.3 Świadczenie usług serwisowych



W obu poprzednio wymienionych modelach może zachodzić również powierzenie danych w celu świadczenia usług serwisowych – np. diagnozowanie i rozwiązywanie zgłoszonych problemów z eksploatacją systemu. Powierzenie danych jest tutaj dokonywane wyłącznie w celu i możliwości uzyskania dostępu do systemu i danych celem weryfikacji, diagnozy i ewentualnego rozwiązywania problemów.

KORZYSTANIE Z USŁUG POWIERZENIA DANYCH OSOBOWYCH W CELU ŚWIADCZENIA USŁUG SERWISOWYCH NIE OZNACZA AUTOMATYCZNIE PRZEJĘCIA ODPOWIEDZIALNOŚCI ZA UTRZYMANIE, ZARZĄDZANIE I ADMINISTRACJĘ SYSTEMEM JAK RÓWNIEŻ NIE ZWALNIA ADO Z ANALIZY RYZYKA I WDROŻENIA ZABEZPIECZEŃ.

2. Obowiązki wynikające z RODO

Motyw 22 RODO

Przetwarzanie danych osobowych *w kontekście* ***działalności prowadzonej przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego*** *w Unii powinno odbywać się zgodnie z niniejszym rozporządzeniem, niezależnie od tego, czy samo przetwarzanie ma miejsce w Unii.*

Należy tutaj podkreślić, że wymagania RODO odnoszą się do przetwarzania danych osobowych przez ADO lub Podmiot Przetwarzający i to głównie na tych podmiotach spoczywa zadanie przygotowanie się do wypełniania obowiązków wynikających z rozporządzenia RODO. Przepisy RODO są neutralne technologicznie i nie wskazują w jaki sposób podmioty mają dane przetwarzać ani z jakich narzędzi korzystać – ważne aby to było zgodnie z rozporządzeniem.

Częste pytanie jakie pojawia się ze strony klientów – to czy system jest zgodny z RODO? – zasadniczo rozporządzenie dotyczy czynności przetwarzania i obowiązków ADO. Organizacja i procesy przetwarzania mogą być zgodne z RODO, nie systemy informatyczne. System może co najwyżej być przygotowanym i wspierać ADO w spełnianiu obowiązków RODO.

ZDECYDOWANA WIĘKSZOŚĆ ZOBOWIĄZAŃ WYNIKAJĄCYCH Z RODO DOTYCZY BEZPOŚREDNIO ADO, ORGANIZACJI I PROCESÓW, A NIE TECHNOLOGII CZY SYSTEMÓW INFORMATYCZNYCH.

3. Podmiot Przetwarzający

Osobną część RODO stanowią przepisy dot. funkcjonowania Podmiotu Przetwarzającego, czyli podmiotu, któremu ADO powierza przetwarzanie danych osobowych w konkretnym celu i zakresie.

Do obowiązków ADO należy weryfikacja i odpowiedni wybór Podmiotu Przetwarzającego.

Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.

Klienci, którzy powierzyli lub powierzą dane osobowe do przetwarzania przez KAMSOFT mają potwierdzenie w postaci wdrożonego, stosowanego i certyfikowanego systemu zarządzania bezpieczeństwem informacji i jakości zgodnego z ISO/IEC 27001 oraz ISO 9001 w obszarze całej organizacji.

Normy z rodziny 27001 stanowią międzynarodowy, niekwestionowany wzorzec postępowania w celu zapewnienia bezpieczeństwa informacji. Jest to również planowany kierunek regulacji w Kodeksie Branżowym Sektora Ochrony Zdrowia.

KAMSOFT S.A. mając świadomość konieczności zapewnienia bezpieczeństwa informacji – zarówno naszych klientów, danych osób które przetwarzamy jak również powierzonych nam przez klientów danych, od wielu lat posiada wdrożony, utrzymywany, doskonalony i certyfikowany SZBI zgodny z wymaganiami normy ISO/IEC 27001.

Tłumaczenie certyfikatu HU11/5573

System zarządzania funkcjonujący w

KAMSOFT S.A.

ul. 1 Maja 133, 40-235 Katowice, Polska

został oceniony i certyfikowany jako spełniający wymagania zawarte w

ISO/IEC 27001:2013

Zakres rejestracji

Projektowanie i instalowanie nowych systemów informatycznych i nadzorowanie baz danych. Produkcję, dostarczanie, uruchamianie, szkolenia i wdrażanie systemów informatycznych KAMSOFT. Utrzymywanie systemów informatycznych i realizację stałego serwisu eksploatacyjnego. Projektowanie, wykonywanie i serwis sieci strukturalnych oraz instalacji niskoprądowych. Prowadzenie sprzedaży hurtowej i detalicznej sprzętu i oprogramowania. Świadczenie usług doradczych w zakresie IT. Zgodnie z deklaracją stosowania z dnia 02.2016, wersja 5.0.

Certyfikat ważny od 10 maja 2019 do 26 kwietnia 2021 oraz pozostaje ważny z zastrzeżeniem uzyskiwania pozytywnych wyników auditów nadzoru.

Audit recertyfikacyjny należy przeprowadzić minimum 60 dni przed datą wygaśnięcia certyfikatu.

Wydanie 8. Certyfikowany od 12 stycznia 2011

Certyfikacja obejmuje wiele lokalizacji. Informacje o dodatkowych lokalizacjach są wyszczególnione na kolejnej stronie.

Authorised by

SGS United Kingdom Ltd
Rossmore Business Park Ellesmere Port Cheshire CH65 3EN UK
t +44 (0)151 350 6666 f +44 (0)151 350 6600 www.sgs.com

HC SGS 27001 2013 0818 M2

Page 1 of 2

UKAS MANAGEMENT SYSTEMS 0005

DO OBOWIĄZKÓW ADO NALEŻY WERYFIKACJA I ODPOWIEDNI WYBÓR PODMIOTU PRZETWARZAJĄCEGO. CERTYFIKAT ISO27001 STANOWI NIEKWESTIONOWANY WZORZEC ODPOWIEDZIALNEGO I BEZPIECZNEGO PODEJŚCIA DO KWESTII OCHRONY INFORMACJI I DANYCH OSOBOWYCH.

4. Analiza Ryzyka

Motyw 76 RODO

Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, ***należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.***

ADO ZOBOWIĄZANY JEST DO REGULARNEGO SZACOWANIA, OCENY I PODEJMOWANIA DZIAŁAŃ MINIMALIZUJĄCYCH RYZYKO. OCHRONY INFORMACJI I DANYCH OSOBOWYCH.

Rozporządzenie RODO - nie stanowi w jaki sposób należy chronić dane osobowe – przesądza jednak, że dane osobowe mają być chronione - należycie, adekwatnie do zagrożeń, przed wszelkimi możliwymi do zidentyfikowania zagrożeniami.

Każdy ADO musi indywidualnie oszacować ryzyko związane z przetwarzaniem danych oraz ryzyko utraty, zniszczenia czy wycieku danych. Pod uwagę powinny być brane zarówno prawdopodobieństwo wystąpienia oraz skutek w przypadku, gdy ryzyko się zmaterializuje.

Każdy ADO musi również indywidualnie oszacować środki minimalizujące to ryzyko adekwatne do zagrożeń, ale również biorące pod uwagę koszty ich wprowadzenia.

Wsparcie w ocenie ryzyka niosą normy z rodziny ISO/IEC 27001 odnośnie metodologii szacowania ryzyka, wyboru dobrych praktyk związanych z szacowaniem ryzyka oraz zabezpieczania informacji.

PRODUKT KS-BDO RODO UMOŻLIWIA WSPARCIE ADO W OCENIE I SZACOWANIU RYZYKA W OPARCIU O METODOLOGIĘ I DOBRE PRAKTYKI WSKAZYWANE M.IN. W NORMIE ISO 27005. WIĘCEJ O KS-BDO RODO W DALSZEJ CZĘŚCI MATERIAŁU.

5. Dobre praktyki w zabezpieczaniu danych osobowych

Rozdział ten poświęcony jest dobrym praktykom w zabezpieczeniu danych osobowych. Przedstawione poniżej praktyki i zabezpieczenia nie stanowią katalogu zamkniętego, czy katalogu minimalnych zabezpieczeń, gdyż taki katalog w praktyce nie istnieje. Każdy ADO musi samodzielnie przeprowadzić analizę ryzyka, rozważyć i zastosować stosowne do zagrożeń zabezpieczenia.

Niemniej jednak lektura poniższych przykładów zabezpieczeń i dobrych praktyk, pozwoli zapewne na identyfikację wybranych zagrożeń i zweryfikowanie ich w ramach prowadzonych przez ADO procesów przetwarzania danych osobowych.

5.1 Zabezpieczenia fizyczne

5.1.1 Lokalizacja serwera (danych) uniemożliwiająca kradzież,

Systemy informatyczne, niezależnie od zastosowanej architektury, czy to w modelu oprogramowania zainstalowanego na miejscu, czy w modelu oprogramowania jako usługi przechowują dane (w tym dane osobowe) na serwerze lub systemach pamięci masowej. W modelu oprogramowania na miejscu serwer jest w lokalizacji klienta **w modelu usługowym serwer jest w lokalizacji dostawcy usługi, który dba o jego bezpieczeństwo fizyczne**. W obu przypadkach w zdecydowanej większości przypadków systemy (w tym systemy KAMSOFT) nie przechowują danych osobowych na końcówkach (komputerach użytkowników) łączących się do serwera.

W przypadku gdy serwer zlokalizowany jest u klienta, bezwzględnie powinien się on znajdować w miejscu niedostępnym dla osób postronnych i odpowiednio zabezpieczonym przed dostępem fizycznym (m. in. wytrzymałe drzwi, zamki, kraty w oknach, ochrona, systemy alarmowe monitoring). Pomieszczenie dedykowane (serwerownia) powinno być wyposażone w odpowiednie systemy gwarantujące bezpieczne środowisko eksploatacji sprzętu: zasilanie awaryjne, klimatyzacja, monitoring.

Szczególną uwagę na zabezpieczenia fizyczne powinny zwrócić uwagę małe podmioty – np. indywidualne praktyki lekarskie, w których system eksploatowany jest często na jednym komputerze, będącym równocześnie serwerem, lub w sytuacji w której serwer jest jednocześnie komputerem użytkownika. Sprzęt taki powinien być objęty szczególną ochroną. O możliwych zabezpieczeniach można przeczytać w sekcji 5.1.2 Zniszczenie sprzętu w przypadku kradzieży oraz 5.1.3 Szyfrowanie dysków na wypadek kradzieży.

Należy pamiętać, że konsekwencje utraty danych osobowych (np. kradzieży serwera wraz z danymi) są dla ADO bardzo dotkliwe:

Zgodnie z Art.33 RODO, w przypadku utraty danych osobowych ADO zobowiązany jest do powiadomienia Urzędu Ochrony Danych Osobowych (UODO).

*Artykuł 33 - **Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu***

1.W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

(…)

Dodatkowo, zgodnie z Art. 34 RODO , ADO zobowiązany jest również do powiadomienia o utracie danych WSZYSTKICH osób, których dane dotyczą.

*Artykuł 34 - **Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych***

1.Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

(…)

Dodatkowo UODO może nałożyć na ADO dotkliwe kary finansowe o których mowa w RODO.

Niezależnie od tego w przypadku wystąpienia tego rodzaju sytuacji ADO zobowiązany będzie do wdrożenia środków naprawczych przeciwdziałających wystąpieniu tego rodzaju sytuacji, dlatego nie warto oszczędzać na zabezpieczeniach i warto wdrożyć stosowne zabezpieczenia już teraz.

Niezależnie również od zastosowanych środków ochrony i podjętych przez ADO starań może dojść do kradzieży sprzętu (wraz z danymi). O tym jak przeciwdziałać skutkom kradzieży sprzętu i danych można przeczytać w sekcji 5.1.2 Zniszczenie sprzętu w przypadku kradzieży oraz 5.1.3 Szyfrowanie dysków na wypadek kradzieży.

Jedną z możliwych form zabezpieczenia przed fizyczną kradzieżą serwera i danych może być również migracja do rozwiązań typu usługa SaaS, gdzie serwer i dane chronione są w sposób profesjonalny, a zabezpieczenia fizyczne po stronie ADO mogą być dużo mniejsze.

MODEL SAAS (OPROGRAMOWANIE JAKO USŁUGA) MINIMALIZUJE KOSZTY ZWIĄZANE Z POSIADANIEM WŁASNEJ INFRASTRUKTURY SPRZĘTOWEJ, MINIMALIZUJE RYZYKO KRADZIEŻY I OGRANICZA KOSZTY ZABEZPIECZEŃ FIZYCZNYCH.

Oczywistą konsekwencją utraty sprzętu i danych jest również konieczność ich odtworzenia z kopii zapasowej. O kopii zapasowej przeczytać można w rozdziale: 5.1.4 Zasilanie awaryjne oraz 5.6 Kopia zapasowa.

5.1.2 Zniszczenie sprzętu w przypadku kradzieży

Jeżeli już do kradzieży dojdzie, dzisiejsze rozwiązania technologiczne pozwalają zabezpieczyć sprzęt w taki sposób aby zarówno sam sprzęt jak i dane na nim zgromadzone były dla przestępcy bezużyteczne lub niemożliwe do wykorzystania.

Jednym z możliwych zabezpieczeń do zastosowania, zarówno w przypadku części serwerów zainstalowanych lokalnie u klienta jak również komputerów pełniących jednocześnie funkcję serwera dla małych podmiotów są zabezpieczenia typu „Kensington Lock" pozwalających na trwałe przymocowanie sprzętu do miejsca w którym został umieszczony. W przypadku kradzieży sprzętu i wyrwania zabezpieczenia, sprzęt jest trwale uszkadzany i nie nadaje się do dalszego użytkowania.

Zabezpieczenie tego rodzaju potrafi również skutecznie zniechęcić do kradzieży z uwagi na świadomość uszkodzenia sprzętu w przypadku wyrwania zabezpieczenia.

W MODELU USŁUGOWYM SERWER ZLOKALIZOWANY JEST W SERWEROWNI Z ZABEZPIECZONYM DOSTĘPEM FIZYCZNYM I CAŁODOBOWĄ OCHRONĄ.

Pozostaje jednak problem utraty (kradzieży wraz ze sprzętem) danych zgromadzonych na nośnikach. O tym jak zabezpieczyć się przed tego rodzaju problemami można przeczytać w kolejnym rozdziale.

Oczywistą konsekwencją utraty sprzętu i danych jest również konieczność ich odtworzenia z kopii zapasowej. O kopii zapasowej przeczytać można w rozdziale: 5.1.4 Zasilanie awaryjne oraz 5.6 Kopia zapasowa.

5.1.3 Szyfrowanie dysków na wypadek kradzieży

Pomimo wszystkich zastosowanych zabezpieczeń fizycznych i organizacyjnych zawsze może dojść jednak do kradzieży i konieczności zmierzenia się z jej skutkami. Poza kosztami związanymi z zakupem nowego sprzętu, konsekwencją kradzieży jest również utrata danych zgromadzonych na dyskach i potencjalna możliwość ich ujawnienia i wykorzystania.

Zabezpieczeniem, które należy rozważyć i które jest rekomendowane jest zaszyfrowanie całej przestrzeni dyskowej na poziomie systemu operacyjnego lub minimalnie jeżeli jest taka możliwość na poziomie bazy danych. W sytuacji kradzieży sprzętu istnieje duże prawdopodobieństwo że dane umieszone na takim nośniku są niemożliwe do odszyfrowania i tym samym nigdy nie zostaną ujawnione czy wykorzystane.

*Artykuł 34 - **RODO przewiduje również odstępstwa od wymogu zawiadamiania osób których dane dotyczą w przypadku naruszenia ochrony danych osobowych.***

(...)

*3.Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach: a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, **w szczególności środki takie jak szyfrowanie**, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;*

(...)

ZASTOSOWANIE SZYFROWANIA DANYCH ZGROMADZONYCH NA NOŚNIKACH SKUTECZNIE UNIEMOŻLIWIA WYKORZYSTANIE TAKICH DANYCH W PRZYPADKU KRADZIEŻY ORAZ OGRANICZA OBOWIĄZEK ADO DO ZAWIADOMIENIA OSÓB, KTÓRYCH DANE DOTYCZĄ O NARUSZENIU OCHRONY DANYCH OSOBOWYCH.

Oczywistą konsekwencją utraty sprzętu i danych jest również konieczność ich odtworzenia z kopii zapasowej. O kopii zapasowej przeczytać można w rozdziale - 5.6 Kopia zapasowa.

5.1.4 Zasilanie awaryjne

Zdecydowana większość systemów operacyjnych oraz baz danych posiada już zabezpieczenia na wypadek niekontrolowanego zaniku napięcia w serwerze. Zabezpieczenia te nie są jednak w 100% doskonałe i w praktyce osób serwisujących systemy informatyczne na wiele tysięcy instalacji nierzadko zdarzają się sytuacje w których baza danych uległa uszkodzeniu na skutek takiego zaniku napięcia.

Konsekwencją takiego zaniku jest konieczność odtwarzania bazy danych z kopii zapasowej i nierzadko częściowa utrata danych (od momentu, w którym utworzona była kopia zapasowa).

Zabezpieczeniem, które można w tej sytuacji zastosować jest **zasilacz awaryjny (UPS)**, który w zależności od wielkości (pojemności akumulatora) pozwoli na podtrzymanie napięcia na serwerze w przypadku krótkotrwałego zaniku napięcia jak również po upływie określonego czasu w przypadku długotrwałego zaniku napięcia wyśle sygnał do serwera pozwalający poprawnie i bezpiecznie zamknąć bazę danych oraz wyłączyć serwer, eliminując ryzyko uszkodzenia bazy wskutek zaniku napięcia.

MODEL SAAS (OPROGRAMOWANIE JAKO USŁUGA) ZAPEWNIA BEZPIECZEŃSTWO ZWIĄZANE Z ZASILANIEM AWARYJNYM, JAK RÓWNIEŻ KOPIĄ ZAPASOWĄ.

5.1.5 Zabezpieczenie fizycznego dostępu do serwerów

Grono pracowników posiadających fizyczny dostęp do serwera powinno być maksymalnie ograniczone, wyłącznie do osób, które muszą taki dostęp posiadać – administratorzy, serwisanci.

Dlaczego jest to takie istotne?

Pierwszym czynnikiem jest sam fakt, że dużo łatwiej zadbać jest o bezpieczeństwo fizyczne sprzętu (zamknięte pomieszczenie, monitoring) w sytuacji, w której znajduje się ono w pomieszczeniu do którego fizycznie dostęp ma tylko wąska grupa pracowników. Nie jest możliwe zapewnienie takiego bezpieczeństwa w przypadku, gdy sprzęt jest w pomieszczeniu ogólnodostępnym dla wszystkich pracowników. Ograniczenie dostępu minimalizuje również ryzyko sabotażu czy nieumyślnego lub przypadkowego zniszczenia sprzętu.

Drugim istotnym czynnikiem jest minimalizacja możliwych błędów np. na skutek działania osób o mniejszym doświadczeniu informatycznym i przypadkowe uszkodzenie czy zniszczenie sprzętu – np. zalanie kawą czy herbatą.

MODEL SAAS (OPROGRAMOWANIE JAKO USŁUGA) ZAPEWNIA BEZPIECZEŃSTWO ZWIĄZANE BARDZO OGRANICZONYM DOSTĘPEM FIZYCZNYM DO SERWERÓW.

5.1.6 Zabezpieczenie zdalnego dostępu do serwerów

W praktyce, zdecydowana większość infekcji oprogramowaniem wymuszającym okup (ransomware), spowodowana jest przez uruchomienie zainfekowanego oprogramowania na tym komputerze lub na komputerze (serwerze) posiadającym udostępnione zasoby innego komputera (serwera).

Podstawowym zabezpieczeniem jest tutaj brak dostępu sieciowego (np. w postaci udostępnionych zasobów) do serwera na którym jest baza danych. W większości przypadków do zainfekowania złośliwym oprogramowaniem dochodzi w wyniku niefrasobliwości użytkownika i uruchomienia oprogramowania o nieznanym pochodzeniu z maila czy z podsuniętej strony internetowej. W przypadku gdy taki użytkownik ma dostęp do zasobów serwera, zostaną one również zainfekowane. Ograniczenie grona osób do absolutnego minimum zdecydowanie minimalizuje to ryzyko.

W MODELU SAAS (OPROGRAMOWANIE JAKO USŁUGA) UDOSTĘPNIANE SĄ TYLKO APLIKACJE I OPROGRAMOWANIE, NIE SĄ UDOSTĘPNIANE ZASOBY POZWALAJĄCE NA ZAINFEKOWANIE I ZASZYFROWANIE DANYCH ZŁOŚLIWYM OPROGRAMOWANIEM.

5.1.7 Konserwacja sprzętu

Wykorzystywany sprzęt powinien być regularnie poddawany konserwacji. Naprawa i konserwacja sprzętu może być wykonywana wyłącznie przez osoby uprawnione. Konserwacja i naprawa sprzętu powinny przebiegać zgodnie z zaleceniami producenta sprzętu. Naprawa i konserwacja sprzętu poza placówką powinna być realizowana jedynie przez dział serwisu z zachowaniem m.in. następujących zasad:

- W przypadku gdy naprawa sprzętu nie wymaga obecności dysku twardego należy go wymontować przed przekazaniem do naprawy
- W przypadku, gdy nie jest możliwe wymontowanie nośnika danych, należy wcześniej usunąć z niego wszelkie dane osobowe, medyczne w sposób uniemożliwiający ich odzyskanie lub przy naprawie sprzętu powinna uczestniczyć osoba uprawniona przez ADO

5.1.8 Bezpieczeństwa sprzętu poza siedzibą,

Zaleca się aby wykorzystanie sprzętu, na którym mogą być przetwarzane dane osobowe poza siedzibą było autoryzowane przez Kierownictwo organizacji/placówki. W celu ochrony sprzętu i danych poza siedzibą należy rozważyć następujące zasady:

- Nie należy pozostawiać sprzętu w miejscach publicznych bez nadzoru,
- Zastosowanie zabezpieczeń zmniejszających ryzyko dostępu do danych osób nieuprawnionych, poza siedzibą wynikające z przeprowadzonej analizy ryzyka.

5.2 Zabezpieczenia sieciowe

5.2.1 Zabezpieczenie sieci bezprzewodowej WiFi

Podstawowym zabezpieczeniem sieci bezprzewodowej jest włączenie uwierzytelnienia hasłem przy wykorzystaniu szyfrowania na poziomie protokołu WPA2. Należy unikać stosowania urządzeń sieciowych korzystających ze starych protokołów zabezpieczeń WEP oraz WPA. Sieć bezprzewodowa nie może pozostać otwarta bez zabezpieczeń.

Dodatkowo można rozważyć filtrowanie dostępu do WiFi na podstawie adresu MAC bezprzewodowej karty sieciowej urządzenia, które korzysta z sieci.

Udostępnianie Internetu pacjentom / klientom należy wykonać za pomocą odseparowanej sieci WiFi, z której nie ma dostępu do zasobów placówki.

5.2.2 Zabezpieczenie urządzeń sieciowych

Praktycznie w każdym podmiocie istnieje wewnętrzna sieć komputerowa i/lub sieć wifi, podłączenie się do takiej sieci przez nieupoważnionego użytkownika (znacznie ułatwione w przypadku sieci WiFi), pozwala uzyskać połączenie z innymi komputerami w sieci i może być potencjalnym miejscem z którego przeprowadzony będzie atak lub włamanie do systemów komputerowych.

Podstawowym i absolutnie minimalnym zabezpieczeniem wewnętrznej sieci komputerowej jest zabezpieczenie urządzeń sieciowych – routerów, punktów dostępowych oraz przełączników (switchy), odpowiednio silnym hasłem znanym tylko administratorowi i właścicielowi podmiotu. Nie należy pozostawiać urządzeń z domyślnym hasłem fabrycznym lub całkowicie bez zabezpieczeń. Hasła powinny być odpowiednio silne, trudne do odgadnięcia.

Kolejnym zabezpieczeniem, które można rozważyć jest ograniczenie możliwości podłączenia do sieci komputerowej wyłącznie dla wskazanych i użytkowanych przez podmiot komputerów (np. na podstawie adresów kart sieciowych MAC).

Urządzenia sieciowe, podobnie jak serwery, powinny być umieszczone w miejscu niedostępnym dla osób postronnych, najlepiej zabezpieczone przed fizycznym dostępem w szafie serwerowej lub dedykowanym pomieszczeniu. Należy zadbać o ich ukrycie, ale mając na uwadze odpowiednie warunki pracy i przepisy ppoż.

KAŻDE URZĄDZENIE SIECIOWE TO MIEJSCE KTÓRYM MOŻE BYĆ PRZEPROWADZONY ATAK NA INFRASTRUKTURĘ I DANE, NIE NALEŻY POZOSTAWIAĆ TYCH URZĄDZEŃ NIEZABEZPIECZONYCH.

5.3 Dostęp i uwierzytelnianie

Podstawowym zabezpieczeniem dostępu jest autoryzacja i uwierzytelnianie użytkowników w systemie informatycznym z wykorzystaniem kont i haseł. Jest to rozwiązanie skuteczne pod warunkiem stosowania się do dobrych praktyk związanych z użyciem kont i haseł. Poniżej zamieszczono wykaz podstawowych i zalecanych praktyk związanych z postępowaniem z kontami i hasłami w systemach informatycznych.

- Każdy użytkownik systemu (osoba) powinien posiadać indywidualne konto, co zapewnia pełną kontrolę i rozliczalność działań użytkowników w systemie. W żadnym wypadku nie jest dopuszczalne współdzielenie kont i haseł pomiędzy różnych użytkowników.
- Konta nieaktywnych użytkowników (np. po zakończeniu współpracy z daną osobą) powinny być natychmiast blokowane/dezaktywowane i w żadnym wypadku nie mogą być ponownie używane.
- Hasła są tak skuteczne jak prawdopodobieństwo ich odgadnięcia przez intruza. Systemy informatyczne pozwalają na wymuszenie odpowiedniej długości hasła, wielkości liter, stosowania cyfr lub znaków specjalnych. W interesie ADO jest zadbanie o odpowiednie bezpieczeństwo haseł. Siła hasła powinna być dostosowano do poziomu istotności przetwarzanych danych, zidentyfikowanych ryzyk i zagrożeń, co powinno wynikać z przeprowadzonej analizy ryzyka.
- Systemy informatyczne pozwalają również na wymuszenie regularnej zmiany haseł z określonym interwałem, co utrudnia skuteczny atak poprzez wielokrotne próby odgadnięcia hasła. System może dbać o uniknięcie powtarzania haseł w danym okresie.
- Hasła w żadnym wypadku nie mogą być nigdzie zapisywane, czy to w miejscu ogólnodostępnym (na monitorze, biurku czy tablicy) jak również w miejscach trudniej dostępnych – notatniki, szuflady itp. Należy rozważyć użycie tzw. menedżerów haseł np. KeePass.
- Bezwzględnie należy unikać używania wspólnych danych autoryzacyjnych w systemach zintegrowanych takich jak usługi NFZ: eWUŚ, KOLCE, DILO. Prowadzi to nie tylko do naruszania regulaminów takich usług, ale także do braku możliwości zidentyfikowania osoby odpowiedzialnej za potencjalne naruszenia.

WŁAŚCIWA POLITYKA ZARZĄDZANIA KONTAMI I HASŁAMI MINIMALIZUJE SKUTECZNIE RYZYKO WŁAMANIA DO SYSTEMU Z WYKORZYSTANIEM JEDNEGO Z KONT UŻYTKOWNIKÓW.

5.4 Uprawnienia

Użytkownikom powinny być nadawane tylko i wyłącznie minimalne wymagane uprawnienia do prowadzenia działań operacyjnych. Każde dodatkowo i nadmiarowo nadane uprawnienie oznacza potencjalnie możliwość popełnienia błędu przez użytkownika, nieumyślnego wykorzystania uprawnienia i w konsekwencji naruszenia bezpieczeństwa danych osobowych.

Nadmiarowe uprawnienia to również zwiększenie pola rażenia w przypadku skutecznego włamania na konto użytkownika i możliwość wykorzystania dodatkowych uprawnień.

Należy okresowo weryfikować nadane uprawnienia oraz w razie potrzeby dokonywać korekty adekwatnej do potrzeb użytkownika.

NALEŻY MINIMALIZOWAĆ ZAKRES PRZYZNAWANYCH UŻYTKOWNIKOM UPRAWNIEŃ. DZIĘKI TEMU, MINIMALIZUJEMY MIĘDZY INNYMI RYZYKO BŁĘDÓW I PRZYPADKOWYCH DZIAŁAŃ UŻYTKOWNIKA.

5.5 Zabezpieczenia systemowe

Podstawowymi zabezpieczeniami systemowymi jakie powinny być stosowane i wdrożone, to stosowanie tylko rozwiązań wspieranych przez producentów i regularne ich aktualizowanie. Producenci na bieżąco publikują poprawki, które likwidują zidentyfikowane luki bezpieczeństwa w swoich systemach.

Dotyczy to zarówno komputerów (serwery, komputery użytkowników), urządzeń sieciowych (routery, przełączniki itp.) ale też systemów operacyjnych, oprogramowania bazodanowego czy oprogramowania narzędziowego.

Konieczne jest regularne wgrywanie aktualizacji oprogramowania wydawanego przez producentów.

Również minimalnym zabezpieczeniem jest stosowanie znanych i sprawdzonych rozwiązań antywirusowych na każdym stanowisku, zapewniających kontrolę i prewencyjne wykrywanie możliwości zainfekowania złośliwym oprogramowaniem.

ZALECANE JEST STOSOWANIE SPRAWDZONYCH ROZWIĄZAŃ ZNANYCH PRODUCENTÓW, REGULARNIE AKTUALIZUJĄCYCH OPROGRAMOWANIE I WYDAJĄCYCH POPRAWKI DOT. BEZPIECZEŃSTWA.

5.6 Kopia zapasowa

Kluczowym elementem pozwalającym na przywrócenie sprawności systemu zarówno po kradzieży sprzętu czy też uszkodzeniu bazy danych **jest kopia zapasowa**. Jest to jedno z podstawowych zabezpieczeń o którym wszyscy wiedzą i które w teorii wszyscy stosują. Jest to również zabezpieczenie stanowiące absolutne minimum na liście możliwych zabezpieczeń chroniących dane osobowe. W praktyce osób serwisujących systemy informatyczne spotyka się jednak wiele sytuacji, w których zabezpieczenie to jest nieskuteczne. Zdarzają się sytuacje, w których kopia zapasowa w praktyce nie jest możliwa do wykorzystania, poniżej lista najczęstszych przyczyn:

- kopia umieszczona jest na tym samym sprzęcie/nośniku co baza, jest więc skradziona razem ze sprzętem lub ulega uszkodzeniu razem z bazą w przypadku awarii sprzętu,
- brakuje miejsca na kopię, przez co nie jest ona wykonywana,
- mechanizm kopii nie ma dostępu do miejsca gdzie powinna być składowana, przez co nie jest ona wykonywana,
- kopia jest wykonywana incydentalnie lub zbyt rzadko, przez co jest bezużyteczna,
- kopia wprawdzie się wykonuje jednak na skutek błędnej konfiguracji nie jest możliwe jej odtworzenie.

W przypadku kopii zapasowej, należy pamiętać o kilku niezbędnych i wymaganych dobrych praktykach, zapewniających skuteczność takiego zabezpieczenia:

- kopia zapasowa **powinna być wykonywana na odrębnym nośniku, odrębnym sprzęcie i najlepiej w odrębnej lokalizacji**, celem zapewnienia bezpieczeństwa na wypadek kradzieży lub zniszczenia fizycznego sprzętu.
- **Zalecane jest dodatkowo wykonywanie kopii w tzw. „chmurze”**, czyli kopii zapasowej przechowywanej w przestrzeni dyskowej wynajętej od dostawcy – zabezpieczonej i chronionej w serwerowni geograficznie oddalonej od klienta. Kopia ta nie jest podatna na większość zagrożeń czyhających na dane klienta.
- Kopia zapasowa powinna być wykonywana **regularnie, nie rzadziej niż raz dziennie**, a w miarę możliwości częściej i przyrostowo aby zachować minimalny okres w którym dane mogą być utracone.
- **Fakt wykonania kopii zapasowej powinien być weryfikowany regularnie, nie rzadziej niż raz dziennie**, aby uniknąć sytuacji, w której kopia z różnych możliwych powodów nie została wykonana.
- **Kopia zapasowa powinna być okresowo odtwarzana i testowana** celem weryfikacji poprawności jej wykonania, możliwości jej odtworzenia oraz zachowania jej integralności.
- **Zalecane jest zachowywanie wielu kolejnych kopii zapasowych** zgodnie z przyjętym planem zachowania kopii, pozwala to uniknąć sytuacji, w której np. w wyniku działania złośliwego oprogramowania szyfrującego (ransomware) jedyna poprawna kopia zostanie nadpisana zaszyfrowanym plikiem danych. Kilka kopii zapasowych pozwoli też na odtworzenie danych w przypadku nieumyślnych błędów użytkowników, które zostają zdiagnozowane po dłuższym okresie i są powielane w aktualnej kopii.

ZASTOSOWANIE WYTYCZNYCH I DOBRYCH PRAKTYK ZARZĄDZANIA KOPIĄ ZAPASOWĄ W TYM POSIADANIE RÓWNIEŻ KOPII W CHMURZE, ZNACZĄCO PODNOSI BEZPIECZEŃSTWO I POZIOM OCHRONY DANYCH OSOBOWYCH. W MODELU USŁUGOWYM, TO DOSTAWCA USŁUGI OPIEKUJE SIĘ I ZARZĄDZA KOPIĄ ZAPASOWĄ

5.7 Korespondencja

Bardzo istotnym elementem związanym z bezpieczeństwem danych osobowych, jest stosowanie bezpiecznych form komunikacji przy przesyłaniu danych osobowych. W żadnym wypadku dane osobowe (zwłaszcza duże ilości danych osobowych) nie powinny być przesyłane w otwarty sposób z wykorzystaniem komunikacji mailowej.

Minimalnym zabezpieczeniem jest zaszyfrowanie danych osobowych i przekazanie hasła do zaszyfrowanego archiwum osobnym kanałem (np. SMS).

NIE NALEŻY PRZEKAZYWAĆ DANYCH OSOBOWYCH (ZWŁASZCZA DUŻYCH ILOŚCI DANYCH) Z WYKORZYSTANIEM POCZTY E-MAIL BEZ UPRZEDNIEGO ZASZYFROWANIA TYCH DANYCH I PRZEKAZANIA HASŁA INNYM BEZPIECZNYM KANAŁEM.

5.8 Odpowiedzialność użytkowników

Każdy użytkownik systemu może mieć wpływ na bezpieczeństwo eksploatowanego systemu, w związku tym należy zapoznać użytkowników z podstawowymi zasadami bezpieczeństwa:

- Nie należy otwierać załączników/klikać w łącza danych otrzymanych pocztą elektroniczną, a budzących jakiekolwiek wątpliwości. Należy pamiętać, że może być to wiadomość typu phishing, która może doprowadzić do zainfekowania systemów oprogramowaniem typu malware.
- Monitory należy ustawić w taki sposób, aby osoby niepowołane nie miały w nie wglądu.
- Nie należy wynosić bez autoryzacji nośników danych zawierających dane osobowe.
- Nie należy wyrzucać zbędnych wydruków zawierających dane osobowe – wydruki takie należy niszczyć w przeznaczonych do tego urządzeniach.
- Nie należy pozostawiać bez nadzoru osób postronnych w pomieszczeniach, w których przetwarzane są dane osobowe.
- Nie należy otwierać załączników/klikać w łącza danych otrzymanych pocztą elektroniczną, a budzących jakiekolwiek wątpliwości że może być to wiadomość typu phishing.

6. Bezpieczeństwo Danych Osobowych – „KS–BDO RODO”

KAMSOFT od wielu lat oferuje klientom rozwiązanie pozwalające na wytworzenie dokumentacji bezpieczeństwa danych osobowych – polityki bezpieczeństwa i związanych z nią dokumentów wymaganych w aktualnym stanie prawnym.

Jest również grono konsultantów, którzy świadczą usługę wdrożenia rozwiązania, które to oczywiście zostało dostosowane do RODO i aktualnie oferuje nowe możliwości:

- Inwentaryzacja bieżącej sytuacji i zabezpieczeń,
- Identyfikacja procesów przetwarzania danych osobowych,
- Weryfikacja spełnienia wymogów dla każdego z procesów przetwarzania,
- Analiza ryzyka dla każdego z procesów przetwarzania,
- Wytworzenie niezbędnych dokumentów, m.in. Rejestry np. czynności przetwarzania,
- Upoważnienia, powołania, itp..

7. Słownik Pojęć

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

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

Administrator Danych Osobowych (ADO) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

Powiernik, Podmiot Przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora

KS-BDO RODO – oprogramowanie dostarczane przez KAMSOFT wspomagające realizowanie procesów obejmujących ochronę danych osobowych w placówkach opieki zdrowotnej. Rozwiązanie ma na celu ułatwienie osiągnięcia zgodności z wymogami prawa i zostało przygotowane oraz jest rozwijane w kontekście wymagań rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. dotyczącego ochrony danych osobowych (RODO)