Polityka bezpieczeństwa danych osobowych Stowarzyszenia Archiwistów Polskich

wersja 3.0

Historia dokumentu

Nr wersji	Sporządził	Opis zmian	Zatwierdził	Obowiązuje od
1.0	ENIGMA SOI Sp. z o.o.	wersja początkowa		
1.1	COMP Safe Support SA	uwzględnienie zbiorów pracowników, członków Stowarzyszenia uczestników kursów i szkoleń oraz klientów wydawnictw		
2.0	SAP	Aktualizacja dokumentu	Prezes Kazimierz Jaroszek	22.06.2017
3.0	Ultrasec Karol Górski	Aktualizacja uwzględniająca RODO		

Spis treści

1. Wstęp

Niniejszy dokument stanowi zestaw obowiązujących zasad i dobrych praktyk regulujących sposób przetwarzania i ochrony danych osobowych w Stowarzyszeniu Archiwistów Polskich (zwanym dalej SAP) zarówno metodami tradycyjnymi, jak i w systemach informatycznych.

Wszyscy pracownicy oraz inne osoby upoważnione do przetwarzania danych osobowych w SAP mają obowiązek zapoznania się z postanowieniami niniejszej polityki i postępowania zgodnie z jej postanowieniami a także zapoznania się i postępowania zgodnie z postanowieniami innych zatwierdzonych instrukcji i procedur dotyczących przetwarzania danych osobowych, w zakresie w jakim te instrukcje i procedury zostały im udostępnione. Udostępnienie instrukcji i procedur następuje na podstawie decyzji Dyrektora Biura Zarządu Głównego SAP. Pracownicy Archiwum SAP zobowiązani są do corocznego przeglądu i akceptacji w/w dokumentów.

Informacje zawarte w niniejszej polityce, instrukcjach i procedurach dotyczą sposobów zabezpieczenia danych osobowych w SAP. Pracownicy oraz inne osoby, którym te informacje udostępniono zobowiązane są do

zachowania ich w tajemnicy.

Postanowienia dot. przetwarzania i ochrony danych osobowych są elementem organizacji i porządku pracy w SAP.

2. Podstawa prawna

Podstawą prawną dla niniejszej polityki jest Rozporządzenie Parlamentu Europejskiego i Rady (UE)2016/679 z dnia 17.04.2016 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 (Dz. Urz. UE L Nr 119 s.1), zwane dalej RODO.

3. Podstawowe definicje

dane osobowe –informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (RODO, art. 4 pkt 1);

przetwarzanie danych - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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 (RODO, art. 4 pkt 2);

poufność danych - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;

integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione, ani zniszczone w sposób nieautoryzowany;

rozliczalność danych – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

odbiorca danych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców (RODO, art. 4 pkt 9);

strona trzecia – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe (RODO, art. 4 pkt 10);

udostępnianie danych – przekazywanie, ujawnianie lub umożliwianie wglądu w dane osobowe (nawet pojedynczych) odbiorcy danych;

naruszenie ochrony danych osobowych – 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 (RODO, art. 4 pkt 12)

system ochrony danych osobowych – całokształt działań SAP mających na celu zgodne z prawem przetwarzanie danych osobowych, zapewniające odpowiedni poziom bezpieczeństwa, ochronę interesów osób, których dane dotyczą oraz rozliczalność

4. System ochrony danych osobowych

4.1 Zakresy odpowiedzialności

Prezes SAP jest odpowiedzialny za wypełnienie przez SAP ustawowych obowiązków ciążących na Stowarzyszeniu Archiwistów Polskich jako administratorze danych.

Dyrektor Biura Zarządu Głównego SAP jest odpowiedzialny za całokształt zarządzania bezpieczeństwem informacji i zarządzanie ryzykiem, nadzór nad przetwarzaniem danych osobowych oraz realizowanie uprawnień osób, których dane są przetwarzane.

Administrator Systemów Informatycznych (ASI) jest odpowiedzialny za wdrożenie i utrzymanie zabezpieczeń informatycznych oraz bieżące zarządzanie systemami informatycznymi.

Inspektor Ochrony Danych (IOD) jest odpowiedzialny za monitorowanie przestrzegania przepisów

dotyczących przetwarzania i ochrony danych osobowych, nadzór nad wdrożonymi zabezpieczeniami, informowanie o spoczywających na administratorze i pracownikach obowiązkach z zakresu ochrony danych osobowych oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego i osób, których dane dotyczą.

Prezes Oddziału SAP jest odpowiedzialny za nadzór nad przestrzeganiem przepisów dotyczących przetwarzania i ochrony danych osobowych oraz wdrożenie i nadzór nad skutecznością zabezpieczeń w podległym mu Oddziale.

Pracownicy są odpowiedzialni za przestrzeganie postanowień niniejszej polityki a także innych przyjętych do stosowania w SAP instrukcji i procedur w zakresie w jakim zostały im udostępnione.

ASI oraz IOD są wyznaczani przez dyrektora Biura ZG SAP. Informacja o ich powołaniu jest komunikowana wszystkim pracownikom, a także władzom Oddziałów w sposób zwyczajowo przyjęty w SAP.

Do przetwarzania danych osobowych mogą być dopuszczone tylko osoby, którym nadano upoważnienie do przetwarzania takich danych i które zobowiązały się do zachowania tajemnicy. Upoważnienia w imieniu SAP nadaje Dyrektor Biura Zarządu Głównego SAP.

4.2 Zasady przetwarzania danych osobowych

Wszyscy pracownicy SAP oraz inne osoby, które przetwarzają dane osobowe w imieniu SAP, zobowiązani są do przestrzegania podstawowych zasad przetwarzania takich danych:

- zgodności z prawem, rzetelności i przejrzystości,
- związania celem przetwarzania,
- minimalizacji danych,
- adekwatności i prawidłowości,
- poufności i integralności,
- ograniczenia czasu przetwarzania,
- rozliczalności,
- uwzględnienia ochrony danych w fazie projektowania oraz domyślnej ochrony danych.

Tymi zasadami należy kierować się zarówno podczas projektowania systemów i procesów przetwarzania danych osobowych, negocjowania umów z klientami i wykonawcami jak i podczas codziennego wykonywania obowiązków, mając na względzie prawa i wolności osób, których dane będą lub są przetwarzane.

Szczegółowe sposoby implementacji niektórych z tych zasad znajdują się w odrębnych instrukcjach i procedurach przyjętych do stosowania w SAP.

4.2.1 Zgodność, rzetelność i przejrzystość

Zgodność z prawem wymaga aby każda czynność przetwarzania miała podstawę prawną. Rzetelność oznacza zachowanie szczególnej staranności przy przetwarzaniu danych, a przejrzystość – zapewnienie osobie, której dane są przetwarzane, informacji o celach i sposobie przetwarzania jej danych, tak na etapie zbierania jej danych jak i podczas dalszego przetwarzania.

Zebranie danych nowej osoby **dopuszczalne jest** dopiero po przekazaniu jej informacji m.in. o celach przetwarzania, administratorze i przysługujących jej prawach[1]. Wyjątek stanowią sytuacje, gdy osoba, której dane dotyczą, powyższe informacje już posiada. W przypadku zbierania danych za pośrednictwem osób trzecich, również konieczne jest poinformowanie osoby, której dane dotyczą, m.in. o nazwie i danych kontaktowych administratora danych, celu i zakresie zbierania danych, źródle danych, oraz przysługujących tej osobie prawach.

Dla zapewnienia, że osoby, których dane są zbierane otrzymują wszystkie niezbędne informacje, zwłaszcza przy wyrażaniu zgody na przetwarzanie danych, należy stosować opracowane na potrzeby SAP i znajdujące się we wzorach formularzy klauzule informacyjne. Wszelkie nowe lub zmieniane formularze wykorzystywane do zbierania danych osobowych muszą być uzgodnione z IOD pod kątem poprawności stosowanych klauzul informacyjnych.

[1] Obowiązek informacyjny dotyczy wprowadzania danych do zbiorów, wobec których SAP jest administratorem danych osobowych, nie dotyczy wprowadzania danych do zbiorów powierzonych SAP przez klientów, o ile nie zostanie to ustalone z tymi klientami.

4.2.2 Związanie celem

Osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać je tylko zgodnie z celem, dla którego dane zostały zebrane. Cele dla poszczególnych czynności przetwarzania są określone w odpowiednim rejestrze czynności lub kategorii czynności przetwarzania danych.

Zmiana celu jest dopuszczalna ale wymaga starannego rozważenia zgodności nowego celu z pierwotnym oraz poinformowania osoby, której dane dotyczą o nowym celu. Każde planowane przetwarzanie, którego cel jest inny niż cel, dla którego pierwotnie zebrano dane należy uzgodnić z IOD.

4.2.3 Minimalizacja danych

Procesy przetwarzania danych należy zaprojektować tak, aby korzystały z danych osobowych tylko w niezbędnym zakresie. Należy wystrzegać się niepotrzebnego powielania danych i zbierania danych na zapas. Nie należy zbierać dodatkowych danych potrzebnych tylko po to, aby móc wywiązać się z obowiązku informacyjnego lub innych obowiązków administratora określonych w przepisach prawa.

4.2.4 Poufność i integralność

Pracownicy upoważnieni do przetwarzania danych osobowych zobowiązani są do zachowania staranności w celu zachowania poufności i integralności przetwarzanych danych osobowych oraz do zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobu ich zabezpieczenia.

Wszyscy pracownicy zobowiązani są do przestrzegania postanowień dokumentacji systemu ochrony danych osobowych w zakresie, w jakim ta dokumentacja została im udostępniona. W szczególności zobowiązani są stosować i, w zakresie swoich kompetencji, dbać o właściwe funkcjonowanie środków organizacyjnych i technicznych służących ochronie danych osobowych, wdrożonych na ich stanowisku pracy i w otoczeniu tego stanowiska.

Wszyscy pracownicy zobowiązani są do nadzoru nad osobami znajdującymi się pod ich opieką w trakcie pobytu w SAP tak, aby nie dopuścić do naruszenia przez te osoby postanowień niniejszej polityki. W szczególności zakazane jest pozostawianie osób, którzy nie są upoważnienia do przetwarzania danych osobowych w SAP w obszarze przetwarzania danych osobowych pod nieobecność pracowników posiadających takie upoważnienie, jeżeli może w ten sposób dojść do ujawnienia danych osobowych osobom nieupoważnionym.

Zakazane jest kopiowanie, modyfikowanie, usuwanie, udostępnianie osobom spoza SAP lub innym pracownikom SAP danych osobowych lub ich zbiorów, do których dostęp pracownik uzyskał przypadkowo lub w sposób niepoprawnej konfiguracji mechanizmów kontroli dostępu lub w sposób nieuprawniony – np. w wyniku podszycia się pod pracownika upoważnionego do przetwarzania danych osobowych.

Szczegółowe zasady zachowania poufności i integralności danych osobowych w systemach informatycznych zawarte są w *Instrukcji Zarządzania Systemem Informatycznym* oraz *Instrukcji Użytkowania Systemu Informatycznego*.

4.2.5 Ograniczenie czasu przetwarzania

W przypadku, gdy dane są zbędne do realizacji celu, dla którego zostały zebrane, pracownicy upoważnieni do przetwarzania danych zobowiązani są do ich usunięcia. Dane powinny zostać usunięte w taki sposób, by zapewnić, że nie będą odtwarzalne np. poprzez pocięcie w niszczarce lub podarcie na bardzo drobne kawałki lub przekazanie do zniszczenia specjalistycznej firmie niszczącej dane. Usunięcie danych może też polegać na ich anonimizacji czyli usunięciu lub zmianie tych elementów danych, które pozwalały na identyfikację osoby.

W przypadku danych osobowych przetwarzanych w systemach informatycznych usunięcie danych może polegać na usunięciu pliku z takimi danymi lub wiadomości poczty elektronicznej przy pomocy dostępnych funkcji usuwania lub kasowania plików lub wiadomości, lub usunięciu danych przetwarzanych przy użyciu aplikacji za pomocą wbudowanych w tę aplikację funkcji. Niezależnie od użytego sposobu usunięcia danych należy zadbać, aby nośnik, na którym dane były zapisane przed usunięciem, został fizycznie zniszczony lub trwale wymazany, gdy nie będzie już dłużej używany do celów przetwarzania danych osobowych.

W szczególnych sytuacjach usunięcie danych może nie być w interesie osoby, której dane dotyczą, co może znaleźć swoje odzwierciedlenie w jej żądaniu ograniczenia przetwarzania danych.

4.2.6 Rozliczalność

Zasada rozliczalności oznacza, że administrator lub podmiot przetwarzający są w stanie wykazać przestrzeganie przepisów o ochronie danych. W tym celu powstają zapisy, odnoszące się do prowadzonych czynności

przetwarzania, komunikacji z osobami, których dane są przetwarzane, szacowania ryzyka i postępowania z ryzykami oraz analizy i oceny w przypadkach, gdy konieczne jest wyważenie interesów administratora oraz osób których dane są przetwarzane. Jest niezmiernie istotne, aby starannie i w sposób określony w szczegółowych procedurach dokumentować podejmowane działania w celu ochrony danych osobowych oraz interesów osób, których dane są przetwarzane.

W SAP przetwarzane są dane osobowe, w stosunku do których SAP posiada status administratora danych oraz dane osobowe, które SAP przetwarza na podstawie zawartych umów powierzenia przetwarzania danych. Szczegółowy wykaz czynności przetwarzania danych osobowych oraz kategorii czynności przetwarzania danych osobowych, zawierający charakterystykę tych czynności i kategorii czynności oraz opis sposobów przetwarzania danych zawierają rejestry prowadzone przez IOD. Zasady podejmowania nowych czynności przetwarzania danych osobowych, wprowadzania zmian w sposobie przetwarzania lub ochrony oraz wycofywania się z czynności przetwarzania opisane są w *Procedurach ochrony danych osobowych*.

Osoby upoważnione do przetwarzania danych osobowych mogą je przetwarzać tylko na polecenie administratora danych, co oznacza przetwarzanie zgodne z opisanym w odpowiednich rejestrach czynności lub kategorii czynności przetwarzania danych, instrukcjach, procedurach lub na podstawie polecenia otrzymanego drogą służbową, o ile nie jest sprzeczne z obowiązującym prawem.

4.2.7 Uwzględnienie ochrony danych osobowych w fazie projektowania oraz domyślna ochrona danych

Od początkowej fazy projektowania nowej usługi, sposobu lub procesu przetwarzania, w którym przetwarzane będą dane osobowe, a także przy planowaniu zmian w istniejących usługach, sposobach lub procesach przetwarzających dane osobowe, należy uwzględnić kwestie zabezpieczenia danych osobowych oraz narzędzia służące do realizacji praw przysługujących osobom, których dane będą przetwarzane. Właściwy poziom zabezpieczeń powinien być dobrany w oparciu o szacowanie ryzyka oraz wiedzę o wdrożonych już w SAP zabezpieczeniach. W przypadku planów użycia nowego systemu informatycznego należy dokładnie poznać oferowane mechanizmy zabezpieczeń, dążąc do tego, aby umożliwiały one skuteczną ochronę przetwarzanych danych, a w przypadku planów zatrudnienia podwykonawcy (dostawcy) należy ocenić, czy zapewnia on gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych, aby przetwarzanie spełniało wymogi przepisów prawa i odpowiednio chroniło przetwarzane dane. W każdym przypadku powierzenia podmiotowi zewnętrznemu przetwarzania danych osobowych należy zawrzeć umowę powierzenia przetwarzania danych osobowych.

We wszystkich przypadkach należy przyjąć zasadę umożliwiania dostępu do danych osobowych wyłącznie osobom, które mają uzasadnioną potrzebę ich przetwarzania. W wyjątkowych sytuacjach, kiedy dane mają być upubliczniane, należy zachować szczególną staranność, aby udostępnić właściwe dane i tylko w niezbędnym zakresie.

4.3 Udostępnianie danych osobowych

Dane osobowe mogą być udostępnione w następujących przypadkach:

a) odbiorcom wymienionym w rejestrze czynności przetwarzania lub należącym do kategorii odbiorców wymienionych w tym rejestrze,

b) na udokumentowane polecenie administratora lub podmiotu powierzającego, o ile nie jest on sprzeczny z prawem, w przypadku danych powierzonych SAP do przetwarzania,

c) na podstawie przepisu prawa Unii lub prawa państwa członkowskiego nakładającego obowiązek ich udostępnienia,

d) na żądanie osoby, której dane dotyczą lub na podstawie jej wyraźnej zgody.

W przypadku udostępniania, które wiąże się z przekazaniem danych do państwa trzeciego (leżącego poza obszarem Europejskiego Obszaru Gospodarczego) lub organizacji międzynarodowej należy dokonać oceny podstawy prawnej przekazania oraz stosowanych zabezpieczeń. Dopuszczalność i tryb takiego przekazania należy skonsultować z IOD.

Danych nie wolno udostępniać jeżeli złożone zostało żądanie ograniczenia ich przetwarzania, chyba że spełnione są przesłanki określone w art. 18 ust. 2 RODO.

Udostępnienie inne niż odbiorcom wymienionym w rejestrze czynności przetwarzania wymaga odnotowania w rejestrze udostępnień lub przy użyciu innego wdrożonego i udokumentowanego mechanizmu rejestrowania

odbiorcy danych.

4.4 Realizacja uprawnień osoby, której dane dotyczą (art. 12-22 RODO)

Obowiązek informacyjny dotyczy wyłącznie czynności przetwarzania, w których SAP jest administratorem danych, oraz czynności, w których SAP podjął się wykonywania obowiązku informacyjnego w umowie z administratorem danych lub podmiotem powierzającym.

O wszelkich żądaniach osób fizycznych składanych w trybie art. 15-22 RODO należy informować IOD. Standardowy sposób realizacji każdego z rodzajów żądań przysługujących osobom fizycznym jest opisany w przyjętych do stosowania *Procedurach ochrony danych osobowych*.

Każde żądanie i sposób jego spełnienia jest dokumentowany w *Rejestrze realizacji uprawnień*.

5. Zarządzanie systemem ochrony danych osobowych

5.1 Zarządzanie dokumentacją systemu ochrony danych osobowych

Na dokumentację systemu ochrony danych osobowych składa się:

- *Polityka ochrony danych osobowych* (niniejszy dokument),
- *Instrukcja zarządzania systemami informatycznymi*,
- *Instrukcja użytkowania systemów informatycznych*,
- *Procedury ochrony danych osobowych*.

W systemie ochrony danych osobowych utrzymywane są również następujące dokumenty wspomagające i ewidencje, służące realizacji zasady rozliczalności:

- rejestry (prowadzone przez IOD), w tym *Rejestr czynności przetwarzania*, *Rejestr kategorii czynności przetwarzania*, *Rejestr naruszeń*, *Rejestr udostępnień*, *Rejestr realizacji uprawnień*
- wyniki szacowania ryzyka i plany postępowania z ryzykiem (prowadzone przez ASI)
- ewidencja upoważnień i uprawnień (prowadzona przez IOD)
- ewidencja informatycznych nośników danych (prowadzona przez ASI)
- ewidencje kluczy (jedna w każdej lokalizacji, prowadzona przez: Dyrektora Biura w Biurze ZG SAP, przez Kierownika Archiwum w Archiwum)
- *Księga Administratora Systemu Informatycznego* (jedna w każdej lokalizacji, prowadzona przez ASI)
- wykaz aktów prawnych mających znaczenie dla systemu ochrony danych osobowych (prowadzony przez IOD)
- wykaz podmiotów, które należy zawiadomić w przypadku realizacji żądania bycia zapomnianym

Dodatkowo, w poszczególnych komórkach organizacyjnych utrzymywane są wzory formularzy stosowanych przy zbieraniu danych, zawierające klauzule informacyjne oraz wzory umów zawierające albo klauzule informacyjne albo klauzule powierzenia przetwarzania danych osobowych.

Za utrzymanie i właściwe udostępnianie dokumentacji odpowiedzialny jest Kierownik Działu Archiwalnego w Biurze Zarządu Głównego SAP.

5.1.1 Monitorowanie aktualności dokumentacji

W przypadku planowania zmian w systemach ewidencyjnych, systemie przetwarzania danych, systemach zabezpieczeń fizycznych i technicznych o zmianach informowany jest IOD, który sprawdza wpływ planowanych zmian na zgodność z prawem przetwarzania danych oraz na zawartość dokumentacji systemu ochrony danych osobowych oraz prowadzonych rejestrów i ewidencji.

W przypadku wprowadzania zmian w funkcjonowaniu SAP, obejmujących w szczególności:

- modyfikację systemu informatycznego służącego ewidencjonowania dokumentów (w tym zmianę programów lub ich wersji),
- modyfikację zabezpieczeń stosowanych do ochrony pomieszczeń,
- zmianę miejsc przetwarzania danych osobowych,

- zmianę zakresu i struktury zbiorów danych osobowych,

IOD jest odpowiedzialny za przegląd dokumentacji systemu ochrony danych osobowych pod kątem jej aktualności.

IOD monitoruje również zmiany w aktach prawnych, mających znaczenie dla systemu ochrony danych osobowych. W przypadku zmian, sprawdza, czy zmiany w aktach prawnych mają wpływ na sposób przetwarzania danych oraz na dokumentację systemu ochrony danych osobowych. W razie potrzeby informuje Dyrektora Biura Zarządu Głównego SAP o potrzebie wprowadzenia zmian w sposobie przetwarzania danych osobowych lub potrzebie aktualizacji dokumentacji.

Dodatkowo, IOD raz na 2 lata przeprowadza planowy przegląd dokumentacji systemu ochrony danych osobowych.

5.1.2 Zmiany w dokumentacji systemu ochrony danych osobowych

Do zmian w dokumentacji systemu ochrony danych osobowych stosuje się odpowiednio procedurę systemową PS-1 z Systemu Zarządzania Jakością.

5.2 Zarządzanie czynnościami przetwarzania danych

Zarządzanie czynnościami przetwarzania danych opisane jest w *Procedurach ochrony danych osobowych*.

5.3 Szacowanie ryzyka

Szacowanie ryzyka dla przetwarzanych danych osobowych prowadzone jest przez Dyrektora Biura Zarządu Głównego SAP z udziałem ASI oraz IOD oraz kierowników działów. W razie potrzeby w szacowaniu ryzyka biorą też udział Prezesi Oddziałów SAP.

Okresowe przeglądy szacowania ryzyka prowadzone są nie rzadziej niż raz w roku. Wyniki szacowania ryzyka służą do przygotowania planów postępowania z ryzykami. Decyzje o wyborze wariantów postępowania z ryzykami podejmuje Dyrektor Biura Zarządu Głównego SAP.

Szacowanie ryzyka powinno uwzględniać przy ocenie poziomu ryzyka potencjalne szkody dla SAP oraz potencjalne szkody dla osób, których dane są przetwarzane, w przypadku zmaterializowania się danego scenariusza zagrożenia.

Dokumentację wyników szacowania ryzyka prowadzi IOD. W ramach szacowania ryzyka prowadzone są rejestry aktywów i rejestry zabezpieczeń a także rejestry podatności i scenariuszy zagrożeń.

5.4 Obsługa incydentów i naruszeń ochrony danych osobowych

Pracownicy mają obowiązek niezwłocznego zgłaszania incydentów ASI, kierownikowi odpowiedniego działu lub Dyrektorowi Biura Zarządu Głównego SAP. Zgłoszenia mogą być przekazywane telefonicznie, za pośrednictwem poczty elektronicznej lub osobiście. W przypadku gdy zgłoszenie wpłynęło do ASI lub kierownika działu i ma poważny charakter informuje on niezwłocznie Dyrektora Biura Zarządu Głównego SAP, a jeżeli z analizy incydentu wynika, że doszło do naruszenia ochrony danych osobowych informuje również IOD.

Za poważne incydenty uznaje się takie, w wyniku których istnieje duże ryzyko szkód majątkowych lub wizerunkowych dla SAP lub znaczące zakłócenie działalności (powyżej 4 godzin przerwy w świadczeniu usług).

Dyrektor Biura Zarządu Głównego SAP jest odpowiedzialny za wyjaśnianie skutków i przyczyn zaistniałego incydentu. W przypadku incydentów mniejszej wagi wyjaśnienie skutków i przyczyn incydentu należy do obowiązków ASI lub kierownika działu. Z dokonanych ustaleń sporządzana jest notatka służbowa.

Wszyscy pracownicy zobowiązani są do niezwłocznego zgłaszania naruszeń ochrony danych osobowych IOD. Jeśli jest to potrzebne IOD, po poinformowaniu Dyrektora Biura Zarządu Głównego SAP oraz Prezesa Zarządu SAP, przygotowuje i przesyła do organu nadzorczego, o ile to możliwe nie później niż 72 godziny od chwili stwierdzenia naruszenia, zgłoszenie o naruszeniu ochrony danych osobowych.

IOD dokumentuje i ewidencjonuje zaistniałe incydenty dotyczące danych osobowych w rejestrze naruszeń, a ASI odnotowuje w Księdze Administratora Systemów Informatycznych incydenty dotyczące systemów informatycznych.

Dyrektor Biura Zarządu Głównego SAP jest odpowiedzialny za zaplanowanie, wdrożenie i nadzorowanie

działań naprawczych, korygujących i ew. zapobiegawczych eliminujących skutki i przyczyny zaistniałego incydentu, jeżeli takich działań wymagać będzie bezpieczeństwo danych osobowych. Na podstawie analizy przyczyn incydentów może wnioskować do Prezesa Zarządu o wdrożenie dodatkowych zabezpieczeń.

W przypadku wykrycia naruszenia przepisów o ochronie danych osobowych Dyrektor Biura Zarządu Głównego SAP może podjąć decyzję o ukaraniu pracowników winnych naruszeń. W przypadku, gdy incydent był spowodowany działaniem pracowników lub osób trzecich i skutkował szkodą dla SAP lub szkodą dla osób, których dane osobowe są przetwarzane przez SAP lub szkodą dla innych podmiotów, Prezez Zarządu SAP może powiadomić policję lub prokuraturę.

Wszyscy pracownicy są zobowiązani do niezwłocznego zgłaszania ASI podejrzenia istnienia podatności (słabości) w stosowanych systemach informatycznych oraz do niezłocznego zgłaszania Dyrektorowi Biura Zarządu Głównego SAP lub Kierownikowi Archiwum podejrzenia istnienia podatności w zabezpieczeniach fizycznych i technicznych. Zakazane są próby samodzielnego potwierdzenia istnienia takich podatności. Zgłoszone podejrzenia weryfikuje ASI, Dyrektor Biura Zarządu Głównego SAP lub Kierownik Archiwum, w zakresie swoich kompetencji. O potwierdzonych podatnościach informowany jest IOD.

5.5 Szkolenia pracowników

Pracownicy przyjmowani do pracy, upoważnieni do przetwarzania danych osobowych są szkoleni z zakresu swoich obowiązków wynikających z systemu ochrony danych osobowych, przed dopuszczeniem do przetwarzania danych osobowych. Szkolenie przeprowadza IOD. Odbycie szkolenia jest dokumentowane w teczkach osobowych pracowników lub przy umowach stanowiących podstawę ich zatrudnienia w SAP.

Nie rzadziej niż raz na 2 lata IOD przeprowadza szkolenie okresowe na temat ochrony danych osobowych dla wszystkich pracowników. IOD weryfikuje znajomość zasad przetwarzania danych osobowych wśród pracowników poprzez bezpośrednie rozmowy i testy wiedzy.

5.6 Kontrole przetwarzania danych osobowych

Raz do roku IOD przeprowadza planową kontrolę przetwarzania danych osobowych. Kontrola obejmuje co najmniej:

- wizje lokalne w archiwum SAP w Łubnej,
- ocenę zabezpieczenia systemów informatycznych przetwarzających dane osobowe (w tym aktualność uprawnień do systemów informatycznych, skuteczność tworzenia kopii zapasowych),
- ocenę stanu zabezpieczeń fizycznych i technicznych,
- kontrolę (audyt) u wybranych podmiotów przetwarzających dane w imieniu SAP.

W okresie 5 lat należy dokonać sprawdzenia wszystkich czynności przetwarzania danych osobowych i systemów informatycznych przetwarzających dane osobowe.

Z przeprowadzonych działań kontrolnych sporządzany jest protokół, który jest przedstawiany Prezesowi SAP. W przypadku wykrycia nieprawidłowości, poza podjęciem działań naprawczych w celu wyeliminowania skutków nieprawidłowości, Dyrektor Biura Zarządu Głównego SAP we współpracy z ASI i kierownikami komórek organizacyjnych oraz IOD przeprowadza analizę przyczyn wykrytej nieprawidłowości i rozważa potrzebę przeprowadzenia działań korygujących i/lub zapobiegawczych, mających na celu eliminację wystąpienia podobnych niezgodności w przyszłości.