Polityka Bezpieczeństwa

TDIKM Anna Jabłońska - Schmidt

Bydgoszcz 2018

Spis treści

Rozdział 1. Deklaracja firmy TDIKM

Ochrona danych osobowych oraz systemów informatycznych jest priorytetem w funkcjonowaniu firmy TDIKM. Ma także zasadnicze znaczenie dla jej działalności, klientów oraz pracowników. Informacje podlegające ochronie stanowią istotny składnik majątku firmy TDIKM.

Osiągnięcie pożądanego, zgodnego z prawem, bezpieczeństwa danych osobowych wymaga zaangażowania wszystkich pracowników firmy TDIKM. Właściciel firmy TDIKM zobowiązany jest do inicjowania i wdrażania wszelkich działań zmierzających do zapewnienia optymalnego poziomu ochrony przetwarzanych danych.

Celem zapewnienia bezpieczeństwa danych osobowych wszyscy pracownicy i współpracownicy firmy TDIKM zobowiązani są do przestrzegania i stosowania zasad wynikających z Polityki Bezpieczeństwa.

Polityka Bezpieczeństwa jest zgodna z obowiązującymi przepisami prawa.

Realizując Politykę bezpieczeństwa informacji zapewnia się ich:

- poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
- integralność – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany,
- dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot,
- rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom,
- autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
- niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
- niezawodność – zamierzone zachowania i skutki są spójne.

Poniższy dokument określa założenia i jednolitą strategię ochrony informacji. Definiuje cele ochrony informacji, zakres tej ochrony, przypisuje odpowiedzialność i kompetencje oraz okre-

śla strukturę mająca za zadanie realizację programu ochrony informacji, a także określa zadanie dla poszczególnych jednostek tej struktury.

Celem Systemu Zarządzania Bezpieczeństwem Informacji jest zapewnienie ochrony danych osobowych oraz innych przetwarzanych w Firmie TDIKM informacji przed wszelkiego rodzaju zagrożeniami zarówno wewnętrznymi jak i zewnętrznymi. Zagwarantowanie dostępności, integralności, poufności, rozliczności oraz autentyczności i niezaprzeczalności danych.

Rozdział 2. Postanowienia ogólne

1. Celem Polityki Bezpieczeństwa jest określenie warunków dla zarządzania i wykorzystywania danych osobowych w sposób zapewniający ich bezpieczeństwo oraz opracowanie strategii niezbędnej dla zapewnienia w firmie TDIKM właściwego poziomu ochrony danych osobowych.

2. Polityka Bezpieczeństwa ma zastosowanie w stosunku do informacji przetwarzanych w systemach informatycznych, oraz, w stosownej części, do informacji przetwarzanych w formie tradycyjnej (papierowej), których administratorem bądź gestorem jest TDIKM.

3. Realizując Politykę bezpieczeństwa w zakresie ochrony danych osobowych Firma TDIKM dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia warunki, aby dane te określały:

    a. zasady związane z przetwarzaniem danych osobowych,

    b. organizacyjno – techniczne zabezpieczenie danych osobowych,

    c. zasady tworzenia, wykorzystywania i usuwania zbiorów danych osobowych,

    d. zasady powierzenia i udostępniania danych osobowych,

    e. zasady postępowania przy naruszeniu bezpieczeństwa danych osobowych.

4. Polityka Bezpieczeństwa jest zgodna z przepisami prawa, w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady 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 RODO z dnia 10 maja 2018r.).

5. W razie zmiany obowiązujących przepisów prawa powodujących niezgodność niniejszego dokumentu z nimi, Polityka Bezpieczeństwa zostanie dostosowana do obowiązujących przepisów.

6. Polityka Bezpieczeństwa na charakter nadrzędny w stosunku do innych aktów dotyczących bezpieczeństwa danych osobowych obowiązujących w firmie TDIKM takich jak: zarządzenia, procedury, regulaminy, protokoły, wytyczne itp.

7. W razie sprzeczności postanowień Polityki Bezpieczeństwa z postanowieniami aktów wewnętrznych dotyczących bezpieczeństwa danych osobowych obowiązujących w firmie TDIKM takich jak: zarządzenia, procedury, regulaminy, protokoły, wytyczne itp., pierwszeństwo mają postanowienia Polityki Bezpieczeństwa.

8. Polityka Bezpieczeństwa ma zastosowanie w stosunku do zarządu, wszystkich pracowników, osób zatrudnionych na innej podstawie niż umowa o pracę, zleceniobiorców, wykonawców, konsultantów, praktykantów, stażystów i innych pracowników firmy TDIKM.

Rozdział 3. Słownik terminów

Użyte w Polityce definicje bądź skróty oznaczają:

1. Administrator Danych Osobowych – firma TDIKM reprezentowana przez Właściciela, tj. Annę Jabłońską – Schmidt.

    a) formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przed nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,

    b) decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,

    c) odpowiada za zgodne z prawem przetwarzanie danych osobowych w firmie TDIKM,

2. Administrator Bezpieczeństwa Informacji (ABI) – od 25 maja 2018 roku Inspektor Ochrony Danych – osoba odpowiedzialna za nadzór i kontrolę przestrzegania w TDIKM zasad ochrony danych osobowych zgodnie z Ustawą o ochronie danych osobowych wraz z procedurami wewnętrznymi. W firmie TDIKM funkcję pełni właściciel – Anna Jabłońska - Schmidt.

3. Administrator Systemu Informatycznego (ASI) – wskazani pracownicy Firmy odpowiedzialni za poprawne wdrażanie, zabezpieczanie i funkcjonowanie systemu informatycznego i urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych.

4. Bezpieczeństwo informacji – to zachowanie atrybutów poufności, dostępności i integralności przetwarzanych informacji.

5. Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

6. Dane osobowe wrażliwe – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

7. Dostępność - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne.

8. Instrukcja zarządzania - Instrukcja zarządzania systemem informatycznym – wymagany Rozporządzeniem formalny dokument opisujący techniczne i eksploatacyjne aspekty zarządzania danymi osobowymi w systemie informatycznym.

9. Integralność - zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania.

10. Odbiorca danych – każdy, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, podmiotu, któremu powierzono przetwarzanie danych oraz organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

11. Poufność - zapewnienie, że informacja jest dostępna tylko dla osób do tego upoważnionych.

12. Pracownik - osoba współpracująca z firmą TDIKM w tym na podstawie umowy o pracę, na innej podstawie niż umowa o pracę, prowadząca działalność gospodarczą, zleceniobiorca, przyjmujący dzieło, konsultant, praktykant lub stażysta.

13. Przetwarzanie danych – to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

14. Ewidencja osób upoważnionych do przetwarzania danych osobowych – zestawienie informacji o wydanych i odwołanych upoważnieniach do przetwarzania danych osobowych.

15. System informatyczny (SI) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

16. Upoważnienie – pisemna zgoda Administratora Danych lub osoby działającej w jego imieniu, upoważniająca do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.

17. 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.

18. Zbiór danych osobowych doraźny – zbiór danych osobowych tworzony ze względów technicznych lub szkoleniowych, w celu realizacji określonego zadania, a po wykorzystaniu niezwłocznie usuwany lub anonimizowany.

Rozdział 4. Zasady przetwarzania informacji

1. Zasada ograniczenia celu – dane osobowe muszą być zbierana w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Cel ten musi być określony w momencie ich pozyskiwania. (art. 5 ust.1 lit. B RODO).

2. Zasada zgodności z prawem, rzetelności i przejrzystości – dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą. Wszelkie informacje i komunikaty związane z przetwarzaniem muszą być łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem (art. 5 ust. 1 lit. a i motyw 39 RODO).

3. Zasada minimalizacji danych - pozyskiwane mogą być jedynie dane adekwatne i niezbędne dla osiągnięcia celów konkretnych, uzasadnionych i określonych w momencie zbierania danych. Nie można zbierać danych osobowych, które nie mają związku z celem przetwarzania, są nadmiarowe lub już nieprzydatne (np. ze względu na ich nieaktualność) (art. 5 ust. 1 lit. c i motyw 39 RODO).

4. Zasada prawidłowości danych - dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Należy podejmować wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (art. 5 ust. 1 lit. d RODO).

5. Zasada ograniczenia czasowego - dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, dla których dane te są przetwarzane. Przechowywanie danych zgromadzonych np. w celu realizacji umowy powinno być zakończone w momencie przedawnienia roszczeń czy innych praw i obowiązków wynikających z przepisów prawa (art. 5 ust. 1 lit. e RODO).

6. Zasada integralności i poufności - dane osobowe muszą być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (art. 5 ust. 1 lit. f RODO).

7. Zasada ograniczonego przetwarzania - podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora,

przez co rozumie się przetwarzanie na podstawie i w zakresie udzielonego upoważnienia lub zawartej umowy powierzenia przetwarzania danych osobowych. (art. 29 RODO).

8. Zasada rozliczalności – wszelkie czynności i decyzje związane z Systemem Bezpieczeństwa Informacji muszą być dokumentowane. Działania związane z przetwarzaniem danych (w szczególności decyzje dotyczące zarządzania dostępem do informacji lub zasobów służących do jej przetwarzania) muszą być dokumentowane lub powodować tworzenie zapisów pozwalających na ocenę zgodności podejmowanych działań z przyjętymi zasadami.

9. Zasada odpowiedzialności – odpowiedzialność za czynności przetwarzania, podejmowanie decyzji o dostępie do informacji, dokumentację, procesy i środki przetwarzania musi być jednoznacznie przypisana do pracowników lub komórek organizacyjnych.

10. Zasada wiedzy koniecznej – możliwość uzyskania dostępu do informacji wyłącznie w zakresie i w ramach realizowanych obowiązków służbowych lub zapisów umowy.

11. Zasada identyfikowalności – osoby, procesy, urządzenia uzyskujące dostęp do informacji lub zasobów służących do jej przetwarzania muszą być w sposób jednoznaczny identyfikowalne.

12. Zasada uwierzytelnienia – mechanizmy kontroli dostępu osoby, procesu, urządzenia do informacji lub zasobów służących do jej przetwarzania muszą wykorzystywać właściwe środki uwierzytelniające oraz zapewniać bezpieczeństwo informacji uwierzytelniających.

13. Rozdzielenie obowiązków – rozdzielenie obowiązków związanych z podejmowaniem decyzji związanych z dostępem do informacji oraz zasobów wykorzystywanych do jej przetwarzania od obowiązków związanych z techniczną ich realizacją.

14. Zasada uwzględnienia ochrony danych w fazie projektowania – wdrożenie nowej czynności przetwarzania (w szczególności z wykorzystaniem narzędzi informatycznych) musi być poprzedzone fazą planowania obejmującą analizę związanych z nią ryzyk oraz uwzględnienie odpowiednich zabezpieczeń.

15. Zasada domyślnej ochrony - domyślnie przetwarzane mogą być wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.

Rozdział 5. Jednostki realizujące zasady zawarte w Polityce Bezpieczeństwa

1. Administratorem danych osobowych decydującym o celach i środkach przetwarzania danych osobowych jest firma TDIKM reprezentowana przez Właściciela.

2. Właściciel TDIKM obok kierowania bieżącą działalnością firmy, akceptuje założenia i priorytety Polityki Bezpieczeństwa.

3. Właściciel TDIKM zobowiązany jest do zorganizowania bezpiecznego przetwarzania danych osobowych, a ponadto do opracowywania planów rozwoju zabezpieczeń ochrony przedmiotowych danych osobowych.

4. Administrator Bezpieczeństwa Informacji /zwany dalej ABI – od 25 maja 2018 roku Inspektor Ochrony Danych / jest osobą odpowiedzialną za bezpieczeństwo danych osobowych w tym nadzór nad przestrzeganiem zasad zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

5. W związku z zakresem odpowiedzialności ABI, do jego zadań należą w szczególności:

    a. opracowywanie projektu i aktualizacja Polityki Bezpieczeństwa oraz innych dokumentów dotyczących bezpieczeństwa i ochrony danych,

    b. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, - wzór upoważnienia oraz ewidencja osób stanowi załącznik nr 1 do Polityki Bezpieczeństwa,

    c. prowadzenie spisu obszaru przetwarzania danych osobowych – wzór spisu stanowi załącznik nr 2 do Polityki Bezpieczeństwa,

    d. prowadzenie wykazu zbiorów danych osobowych oraz programów stosowanych do ich przetwarzania – wzór wykazu stanowi załącznik nr 3 do Polityki Bezpieczeństwa,

    e. prowadzenie opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi – wzór opisu stanowi załącznik nr 4 do Polityki Bezpieczeństwa,

    f. prowadzenie opisu środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych – wzór opisu stanowi załącznik nr 5 do Polityki Bezpieczeństwa,

    g. nadzór nad udostępnianiem danych osobowych innym podmiotom,

h. nadzór nad procedurami upoważniania do przetwarzania danych osobowych w firmie TDIKM,

i. podejmowanie działań w zakresie ustalania identyfikatorów dostępu do systemu informatycznego oraz dopuszczanie do systemów informatycznych,

j. zatwierdzanie i kontrola projektów umów powierzenia przez firmę TDIKM przetwarzania danych osobowych innemu podmiotowi oraz umów przyjmowania przez TDIKM do przetwarzania zbiorów innych podmiotów,

k. nadzór na zabezpieczeniami fizycznymi, organizacyjnymi, programowymi oraz sprzętowymi oraz przeprowadzanie okresowych testów tych zabezpieczeń,

l. podnoszenie świadomości dotyczącej bezpieczeństwa danych wśród pracowników, organizowanie odpowiednich szkoleń,

m. analiza incydentów związanych z naruszeniem ochrony danych i sporządzanie w tym zakresie raportów,

n. przeprowadzanie okresowych przeglądów nośników informacji,

o. analiza osiągnięć w dziedzinie zabezpieczania systemów informatycznych i wdrażanie takich narzędzi, metod pracy oraz sposobów zarządzania systemem informatycznym, które bezpieczeństwo to wzmocnią.

6. Administrator Systemu Informatycznego (ASI) – pracownik Firmy wyznaczony przez Właściciela Firmy (osoba odpowiedzialna za wdrażanie i utrzymanie zabezpieczeń technicznych i organizacyjnych dotyczących systemów informatycznych służących do przewarzania danych osobowych).

7. Do najważniejszych zadań Administratora Systemu Informatycznego należy:

a. realizacja napraw, konserwacja oraz likwidacja urządzeń komputerowych, na których zapisane są dane osobowe,

b. wykonywanie kopii zapasowych, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtwarzania danych,

c. zapewnianie bezpiecznej wymiany danych w wewnętrznej sieci telekomunikacyjnej oraz zapewnienie bezpiecznego styku z zewnętrzną siecią telekomunikacyjną,

d. zapewnianie niezawodności zasilania urządzeń teleinformatycznych,

e. współpraca i nadzór nad stronami trzecimi realizującymi zadania w zakresie systemów informatycznych na rzecz firmy TDIKM,

f. bieżące informowanie Administratora Bezpieczeństwa Informacji o stanie zabezpieczeń danych osobowych przetwarzanych w systemie informatycznym oraz nowych systemach wykorzystywanych do przetwarzania danych osobowych.

8. Jeżeli właściciel nie wyznaczy osób pełniących funkcje ABI oraz ASI, zadania wskazane powyżej są realizowane przez właściciela firmy TDIKM osobiście.

9. Wszyscy pracownicy, przed dopuszczeniem do przetwarzania danych, muszą zostać przeszkoleni w zakresie ochrony danych osobowych oraz zasad wynikających z Polityki Bezpieczeństwa.

10. Wszyscy pracownicy, przed dopuszczeniem do przetwarzania danych, muszą otrzymać upoważnienie wskazujące zakres działań przy przetwarzaniu danych, do którego bedą uprawnieni. Upoważnienia do przetwarzania danych osobowych wydaje Administrator Danych Osobowych.

11. Administrator Danych Osobowych prowadzi rejestr osób upoważnionych do przetwarzania danych osobowych, który zawiera następujące dane:

    a. imię i nazwisko pracownika,

    b. nazwę stanowiska pracownika,

    c. opis systemu (zbioru danych osobowych), do którego wnioskowany jest dostęp,

    d. określenie stopnia przetwarzania danych osobowych:

        - odczyt danych,
        - zapis,
        - drukowanie,
        - modyfikowanie danych,
        - administrowanie zbiorem,
        - wszystkie uprawnienia,

12. Administrator Systemu Informatycznego dokonuje nadania uprawnień, a w przypadku nadawania uprawnień po raz pierwszy, dokonuje wygenerowania identyfikatora użytkownika.

13. Identyfikator użytkownika musi być unikalny. Nie może być to identyfikator, który w przeszłości był już stosowany w danym systemie informatycznym.

14. Wszyscy pracownicy dopuszczeni do przetwarzania danych zobowiązani są do zapoznania się z treścią przeznaczonych dla nich dokumentów zawierających zasady bezpiecznego przetwarzania.

15. Wszyscy pracownicy mający dostęp do danych osobowych zobowiązani są do:

    a. zachowania tych danych w tajemnicy, również po ustaniu zatrudnienia w firmie TDIKM

    b. przestrzegania bezwzględnego zakazu udzielania informacji wewnętrznych w tym danych osobowych innym podmiotom,

    c. bezzwłocznego zawiadamiania bezpośredniego przełożonego o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych i systemu informatycznego przetwarzającego te dane.

16. Wszyscy pracownicy mający dostęp do danych podpisują Oświadczenie o:

    a. znajomości obowiązujących przepisów prawa, Polityki Bezpieczeństwa oraz innych aktów dotyczących bezpieczeństwa i ochrony informacji obowiązujących w firmie TDIKM

    b. zobowiązaniu się do przestrzegania i stosowania przepisów ww. aktów,

    c. zachowaniu w tajemnicy treści danych i sposobów ich zabezpieczenia podczas zatrudnienia i po jego ustaniu,

którego wzór stanowi załącznik nr 1 do Polityki Bezpieczeństwa.

Rozdział 6. Organizacyjno – techniczne zabezpieczenie danych osobowych

1. Wymagania dotyczące pomieszczeń, w których przetwarzane są dane osobowe w firmie TDIKM

    a. pomieszczenia, w których przetwarzane są dane osobowe, tworzące obszar przetwarzania danych osobowych, powinny być zabezpieczone przed: niepowołanym dostępem, pożarem i powodzią;

    b. przebywanie w tych pomieszczeniach osób nieuprawnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych;

    c. budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności osób zatrudnionych przy przetwarzaniu danych osobowych, w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym.

2. Wymagania dotyczące przechowywania zbiorów danych osobowych w postaci papierowej np. kartotek, ksiąg, wykazów i innych postaci papierowych:

    a. zbiory danych osobowych w postaci kartotek, ksiąg, wykazów czy innych postaci papierowych powinny być przechowywane w warunkach uniemożliwiających dostęp osobom nieuprawnionym, w tym pracownikom nieupoważnionym do przetwarzania określonego rodzaju zbioru danych osobowych;

    b. zbiory danych osobowych należy przechowywać w zamykanych na klucz szafach, pojemnikach do tego przeznaczonych lub w sejfach;

    c. biurka, szafy i inne pojemniki, w których przechowuje się zbiory danych osobowych powinny być po zakończeniu pracy zamykane na klucz lub w inny, skuteczny sposób zabezpieczone przed dostępem do nich osób niepowołanych;

    d. wszelkie błędne dokumenty zawierające dane osobowe należy niszczyć w niszczarkach. Zabrania się wyrzucania jakichkolwiek dokumentów do koszów na śmieci.

3. Wymagania dotyczące przechowywania zbiorów danych w postaci elektronicznej (m. in. pliki pochodzące z edytorów, arkuszy kalkulacyjnych):

a. wszystkie zbiory danych w postaci elektronicznej powinny być przechowywane w specjalnie do tego przeznaczonych i zabezpieczonych przed dostępem osób nieupoważnionych folderach na serwerze plików;

b. niedopuszczalne jest przechowywanie zbiorów danych w postaci elektronicznej jedynie na dyskach lokalnych stacji roboczych bez wykonania kopii danych w folderach sieciowych,;

4. Wymagania dotyczące systemów, aplikacji i urządzeń informatycznych wykorzystywanych w procesie przetwarzania danych osobowych w firmie TDIKM:

a. przetwarzanie danych osobowych jest dopuszczalne na komputerach zabezpieczonych identyfikatorem użytkownika oraz hasłem;

b. przetwarzanie danych osobowych jest dopuszczalne na serwerze aplikacyjnym zlokalizowanym w pomieszczeniu zabezpieczonym przed nieautoryzowanym dostępem osób nieupoważnionych;

c. urządzenia i systemy informatyczne powinny być zabezpieczone przed utratą danych osobowych spowodowaną awarią zasilania oraz zakłóceniami w sieci zasilającej i powinny umożliwiać poprawne odtworzenie danych osobowych po awarii systemu informatycznego;

d. urządzenia, dyski lub inne informatyczne nośniki przeznaczone do likwidacji lub zbycia, a zawierające dane osobowe, powinny być wcześniej pozbawione zapisu danych;

e. nośniki informatyczne zawierające dane osobowe powinny być przechowywane w pomieszczeniach, do których dostępu nie mają osoby nieuprawnione do przetwarzania danych osobowych;

f. system informatyczny musi być wyposażony w mechanizm uwierzytelnienia użytkownika poprzez identyfikator i hasło oraz mechanizm administracyjny zarządzania dostępem do funkcji,

g. system informatyczny powinien umożliwiać odnotowanie informacji daty pierwszego wprowadzenia danych do systemu, identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba, źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą, informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia. Jeśli system nie spełnia powyższych wymagań,

wymagane informacje należy odnotowywać ręcznie w specjalnie utworzonym w tym celu polu uwagi.

Rozdział 7. Tworzenie, wykorzystywanie i usuwanie zbiorów danych osobowych

1. Zakazuje się tworzenia zbiorów danych osobowych bez wiedzy Administratora Danych Osobowych. Pracownicy firmy TDIKM zgłaszają potrzebę utworzenia nowego zbioru danych osobowych Administratorowi Danych Osobowych, który podejmuje decyzję w tym przedmiocie.

2. Przetwarzanie danych osobowych z nowego zbioru danych osobowych może nastąpić dopiero po opracowaniu jego struktury i identyfikacji w załącznika do Polityki Bezpieczeństwa.

3. Wyjątkowo, gdy zachodzi potrzeba utworzenia doraźnego zbioru danych osobowych, np. w związku z utworzeniem listy uczestników szkolenia, bądź zapisaniem danych do nowego pliku lub utworzenie pliku w innym formacie (np. dokumenty Worda, arkusze kalkulacyjne Excel) celem opracowania raportu, sprawozdania, można tego dokonać w tzw. doraźnym zbiorze danych pod warunkiem, że zapisane dane będą należycie chronione, a po wykorzystaniu niezwłocznie usunięte. O utworzeniu takiego zbioru jego twórca informuje Administratora Bezpieczeństwa Informacji.

4. Za bezpieczeństwo doraźnego zbioru danych osobowych odpowiada jego twórca, który uniemożliwia dostęp do danych osobom nieuprawnionym.

5. Doraźny zbiór danych osobowych należy usunąć z nośnika danych, na którym został utworzony lub zniszczyć nośnik, nie później niż 3 dni po wykorzystaniu danych,

6. Dane w zbiorach doraźnych mogą być przetwarzane wyłącznie w pomieszczeniach stanowiących obszar przetwarzania danych osobowych w systemie informatycznym, oraz na stacjach komputerowych osób, które zbiór utworzyły.

7. Decyzję o usunięciu każdego - poza doraźnym - zbioru danych osobowych podejmuje Administrator Danych Osobowych. O podjętej decyzji Administrator Danych Osobowych niezwłocznie informuje Administratora Bezpieczeństwa Informacji.

8. Usunięcie zbioru danych odbywa się komisyjnie z obowiązkiem sporządzenia protokołu zniszczenia zbioru. W skład komisji wchodzi obligatoryjnie Administrator Bezpieczeństwa Informacji oraz Administrator Danych Osobowych.

Rozdział 8. Powierzenie oraz udostępnianie danych osobowych

1. Na zasadzie wyjątku dopuszczalne jest powierzenie przetwarzania danych. Decyzję o powierzeniu przetwarzania danych osobowych podejmuje Administrator Danych Osobowych po zasięgnięciu opinii ABI.

2. Powierzenie przetwarzania danych może mieć miejsce na podstawie pisemnej umowy określającej w szczególności zakres i cel przetwarzania danych. Umowa musi określać też zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy.

3. Powierzenie przetwarzania danych osobowych musi uwzględniać ponadto wymogi określone w przepisach prawa. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych do podjęcia środków zabezpieczających zbiór danych.

4. W umowach stanowiących podstawę powierzenia przetwarzania danych albo eksploatacji systemu informatycznego lub części infrastruktury należy umieścić zobowiązanie podmiotu zewnętrznego do przestrzegania Polityki Bezpieczeństwa, w tym zastosowanie odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo i odpowiedni poziom ochrony danych.

5. Powierzenie przetwarzania danych osobowych nie oznacza zwolnienia z odpowiedzialności firmy TDIKM za zgodne z prawem przetwarzanie powierzonych danych, co wymaga w umowach stanowiących podstawę powierzenia przetwarzania danych umieszczenia prawa firmy TDIKM do kontroli wykonania przedmiotu umowy w siedzibie podmiotu zewnętrznego m. in. w zakresie przestrzegania Polityki Bezpieczeństwa i właściwych przepisów prawa.

6. Powierzenie przetwarzania danych i nie ma zastosowania do przekazywania danych podmiotom upoważnionym do ich przetwarzania na mocy przepisów prawa, w tym ZUS, Prokuraturze oraz Policji.

7. TDIKM może udostępnić dane osobowe na pisemny, umotywowany wniosek, chyba, że przepis prawa stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres, przeznaczenie oraz podstawę prawną upoważniającą do żądania udostępnienia.

8. Wszystkie wnioski o udostępnienie danych osobowych przekazywane są do Administratora Bezpieczeństwa Informacji, który rozpatruje wniosek oraz nadzoruje proces udostępniania danych osobowych wskazanych we wniosku.

9. Odpowiedź na wniosek o udostępnienie danych osobowych udzielana jest przez Administratora Bezpieczeństwa Informacji. Administrator Bezpieczeństwa Informacji prowadzi w formie elektronicznej lub papierowej Rejestr Udostępnień danych obejmujący, co oznaczenie podmiotu, któremu udostępniono dane, rodzaju udostępnianych danych, sposobu udostępnienia danych, daty udostępnienia oraz oznaczenie zbioru, z którego pochodzą udostępniane dane osobowe.

10. Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom:

    a. listem poleconym za potwierdzeniem odbioru,

    b. w drodze teletransmisji danych, zgodnie z procedurami ochrony danych,

    c. osobiście za potwierdzeniem odbioru,

    d. w inny sposób określony przepisami prawa lub umową.

11. Udostępnianie danych osobowych w trybie uregulowanym w § 19 Polityki Bezpieczeństwa Informacji nie ma zastosowania do przekazywania danych podmiotom upoważnionym do ich przetwarzania na mocy przepisów prawa, którym dane są udostępniane w związku z prowadzonym postępowaniem, w tym w szczególności ZUS, Prokuraturze, Policji, a także nie ma zastosowania do udostępniania danych osobom, których te dane dotyczą.

Rozdział 9. Sposób postępowania w przypadku stwierdzenia naruszenia, lub powzięcia podejrzenia naruszenia zabezpieczenia danych osobowych

1. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

    a. nieautoryzowany dostęp do danych,

    b. nieautoryzowane modyfikacje lub zniszczenie danych,

    c. udostępnienie danych nieautoryzowanym podmiotom,

    d. nielegalne ujawnienie danych,

    e. pozyskiwanie danych z nielegalnych źródeł,

2. Pracownik, który stwierdził naruszenie zabezpieczenia danych w systemie informatycznym bądź w dokumentacji papierowej lub zaistnienie okoliczności, wskazujących na takie naruszenie, ma obowiązek niezwłocznego powiadomienia o tym fakcie wyznaczonych osób funkcyjnych zgodnie z niniejszą procedurą.

3. Niniejsza procedura określa sposób postępowania w przypadku stwierdzenia naruszenia, lub powzięcia podejrzenia o naruszeniu zabezpieczenia danych osobowych.

4. Naruszenie zabezpieczenia systemu informatycznego oznacza jakiekolwiek naruszenie poufności, integralności, dostępności, autentyczności danych osobowych lub niezawodności i bezpieczeństwa systemu informatycznego spowodowane awarią sprzętu lub oprogramowania, bądź działaniami dokonanymi przez osoby nieuprawnione lub uprawnione, lecz działające w złej wierze albo omyłkowo. Za naruszenie zabezpieczenia systemu informatycznego uważa się również włamanie do pomieszczeń firmy TDIKM a także próby takich działań.

5. Naruszenie zabezpieczenia dokumentów papierowych zawierających dane osobowe oznacza jakiekolwiek naruszenie poufności, integralności, dostępności, autentyczności danych osobowych zawartych w tych dokumentach spowodowane m.in oddziaływaniem czynników zewnętrznych lub klęsk żywiołowych, bądź działaniami dokonanymi przez osoby nieuprawnione lub uprawnione, lecz działające w złej wierze albo omyłkowo. Za naruszenie zabezpieczenia dokumentów papierowych uważa się również włamanie do pomieszczeń firmy TDIKM a także próby takich działań.

6. Za naruszenie ochrony danych osobowych uważa się w szczególności:

    a. nieuprawniony dostęp lub próbę dostępu do systemu informatycznego przetwarzającego dane osobowe,

    b. nieuprawniony dostęp lub próbę dostępu do dokumentów papierowych, w których przetwarzane są dane osobowe,

    c. nieprzewidziane oddziaływanie czynników zewnętrznych lub klęski żywiołowe mogące oddziaływać negatywnie lub zniszczyć zasoby systemu informatycznego bądź dokumenty papierowe takie jak: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, niepożądana ingerencja ekipy remontowej itp,

    d. naruszenie lub próby naruszenia integralności danych osobowych rozumiane jako wszelkie modyfikacje, zniszczenia lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jako błąd działania osoby uprawnionej (np. zmianę zawartości danych osobowych, utratę całości lub części tych danych),

    e. naruszenie lub próby naruszenia integralności systemu informatycznego, w którym przetwarzane są dane osobowe, bądź dokumentów papierowych zawierających dane osobowe,

    f. zmianę lub utratę danych osobowych zapisanych na kopiach zapasowych lub archiwalnych,

    g. naruszenie lub próby naruszenia poufności danych osobowych lub ich części,

    h. sytuację, w której jakość danych osobowych w systemie wskazuje na działanie wirusa lub inną nadzwyczajną i niepożądaną modyfikację w systemie, w którym przetwarzane są dane osobowe,

    i. nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu, w którym przetwarzane są dane osobowe),

    j. udostępnienie osobom nieupoważnionym danych osobowych lub ich części, znajdujących się w systemie, w którym przetwarzane są dane osobowe,

    k. zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w system informatyczny zmierzające do zakłócenia jego działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych osobowych objętych ochroną zawartych w zbiorach systemu,

l. inny stan systemu lub pomieszczeń niż pozostawiony przez osoby przetwarzające dane osobowe po zakończeniu lub po przerwie w pracy z systemem, w którym przetwarzane są dane osobowe, bądź dokumentami papierowymi zawierającymi dane osobowe,

m. rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się z systemu, w którym przetwarzane są dane osobowe przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w formie wydruku na drukarce, na ksero, nie wykonywanie w terminie kopii bezpieczeństwa zgodnie z Instrukcją zarządzania systemem w którym przetwarzane są dane osobowe, prace na danych osobowych w celach prywatnych, itp.).

7. Tryb postępowania w przypadku naruszenia lub podejrzenia naruszenia zabezpieczenia danych osobowych:

a. osoba upoważniona do przetwarzania danych osobowych, w przypadku stwierdzenia lub uzyskania informacji o naruszeniu zabezpieczenia przetwarzanych danych osobowych w systemie informatycznym bądź dokumentacji papierowej zobowiązana jest do natychmiastowego powiadomienia Administratora Bezpieczeństwa Informacji;

b. w przypadku niemożności zawiadomienia Administratora Bezpieczeństwa Informacji należy powiadomić bezpośredniego przełożonego, a gdy to nie jest możliwe innych członków kierownictwa firmy TDIKM

c. do czasu przybycia Administratora Bezpieczeństwa Informacji osoba upoważniona do przetwarzania danych osobowych, która ujawniła fakt naruszenia ochrony danych osobowych powinna powstrzymać się od rozpoczęcia lub kontynuowania jakiejkolwiek czynności lub pracy mogącej spowodować zatarcie śladów lub dowodów naruszenia oraz podjąć niezbędne działania celem zapobieżenia dalszym zagrożeniom, a w szczególności:

d. zabezpiecza elementy systemu informatycznego bądź dokumentacji papierowej oraz ślady lub dowody naruszenia ochrony danych osobowych,

e. podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować naruszeniem ochrony danych osobowych, jak: określenie symptomów naruszenia bezpieczeństwa, określenie sytuacji i czasu, w jakim stwierdzono naruszenie bezpieczeństwa oraz określenie wszelkich istotnych informacji mogących wskazać na przyczynę naruszenia.

8. Administrator Bezpieczeństwa Informacji a podczas jego nieobecności osoba z kierownictwa firmy TDIKM poinformowana o zdarzeniu w sytuacji naruszenia ochrony danych osobowych w szczególności dokonują:

    a. oceny zaistniałej sytuacji, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe, stan urządzeń i dokumentów zawierających dane osobowe oraz identyfikacji i rozmiarów negatywnych następstw incydentu,

    b. wysłuchują relacji osoby dopuszczonej do przetwarzania danych osobowych, która dokonała powiadomienia,

    c. podejmują decyzję o toku dalszego postępowania stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

9. Administrator Bezpieczeństwa Informacji a podczas jego nieobecności osoba z kierownictwa firmy TDIKM poinformowana o zdarzeniu sporządza raport z przebiegu zdarzenia. Raport powinien zostać utrwalony na piśmie albo na innym trwałym nośniku informacji.

10. Raport, o którym mowa w punkcie 9 winien zawierać opis istotnych dla powstałego zdarzenia faktów, a w szczególności:

    a. krótki opis zastanej sytuacji i faktów wskazujących na naruszenie lub prawdopodobieństwo naruszenia ochrony danych osobowych,

    b. opis zastosowanych środków i podjętych działań w celu wskazania i likwidacji skutków naruszenia,

    c. opis stanu systemu po zakończeniu działań zabezpieczających,

    d. wstępny szacunek powstałej szkody.

11. Administrator Bezpieczeństwa Informacji na podstawie raportu oraz faktów ustalonych w wyniku własnego postępowania, sporządza informacje dla Administratora danych Osobowych zawierające opis zaistniałego incydentu wraz z propozycją działań naprawczych.

12. Administrator Bezpieczeństwa Informacji, stosownie do potrzeb, postuluje wprowadzenie nowych form zabezpieczenia systemu bądź dokumentów.

13. Postępowanie pracowników upoważnionych do przetwarzania danych osobowych oraz Administratora Bezpieczeństwa Informacji (a podczas jego nieobecności osoby z kie-

rownictwa firmy TDIKM poinformowanej o zdarzeniu) w związku z naruszeniem ochrony danych osobowych winno zmierzać do:

a. zachowania ciągłości działania systemów informatycznych,

b. zabezpieczenia danych przed utratą,

c. wykrycia sprawców zdarzenia.

Rozdział 10. Postanowienia końcowe

1. Politykę Bezpieczeństwa oraz zmiany Polityki Bezpieczeństwa wprowadza się w życie w formie zarządzenia Administratora Danych Osobowych.

2. Zapoznanie się z zasadami Polityki (zmianami do Polityki) pracownik potwierdza na piśmie, które składa się do akt osobowych pracownika, przy czym zapoznanie nie obejmuje załączników do Polityki Bezpieczeństwa, do których dostęp mają wyłącznie ADO oraz ABI.

3. Odmowa potwierdzenia będzie traktowana na równi z odmową przestrzegania postanowień Polityki i może być uznana za ciężkie naruszenie obowiązków pracowniczych z winy pracownika.

4. ABI jest obowiązany przechowywać co najmniej jeden egzemplarz Polityki Bezpieczeństwa.

5. Integralną część niniejszej Polityki stanowią następujące załączniki:

    a. Załącznik nr 1 – wzór upoważnienia, oświadczenia oraz ewidencja osób upoważnionych do przetwarzania danych osobowych

    b. Załączniki nr 2 - spis obszaru przetwarzania danych osobowych

    c. Załącznik nr 3 - wykaz zbiorów danych osobowych oraz programów stosowanych do ich przetwarzania

    d. Załącznik nr 4 – opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,

    e. Załącznik nr 5 - opis środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych