GKK GUMULARZ KOZIEŁ KOZIK

Zasady prowadzenia audytu przez Administratora Bezpieczeństwa Informacji

radca prawny Patrycja Kozik
audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji wg normy ISO 27001:2013

Lublin, 18.11.2017

Agenda

1. Audyt – definicje najważniejszych pojęć
2. Specyfika audytu ochrony danych osobowych
3. Status prawny i zadania ABI a status i zadania IOD
4. Sposób i zasady przeprowadzania audytu przez ABI
5. Rodzaje audytu dokonywanego przez ABI

a. Sprawdzenia doraźne
b. Sprawdzenia na wniosek GIODO
c. Sprawdzenia planowe
d. Weryfikacja dokumentacji
e. Audyt u procesora

Kluczowe akty prawne

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
2. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015, poz. 745)
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
4. 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 (ogólne rozporządzenie o ochronie danych)

Wytyczne dotyczące audytowania systemów zarządzania (I S O 19011):

Audyt – systematyczny, niezależny i udokumentowany **proces uzyskiwania dowodów z audytu** oraz **jego obiektywnej oceny** w celu określenia **kryteriów audytu.**

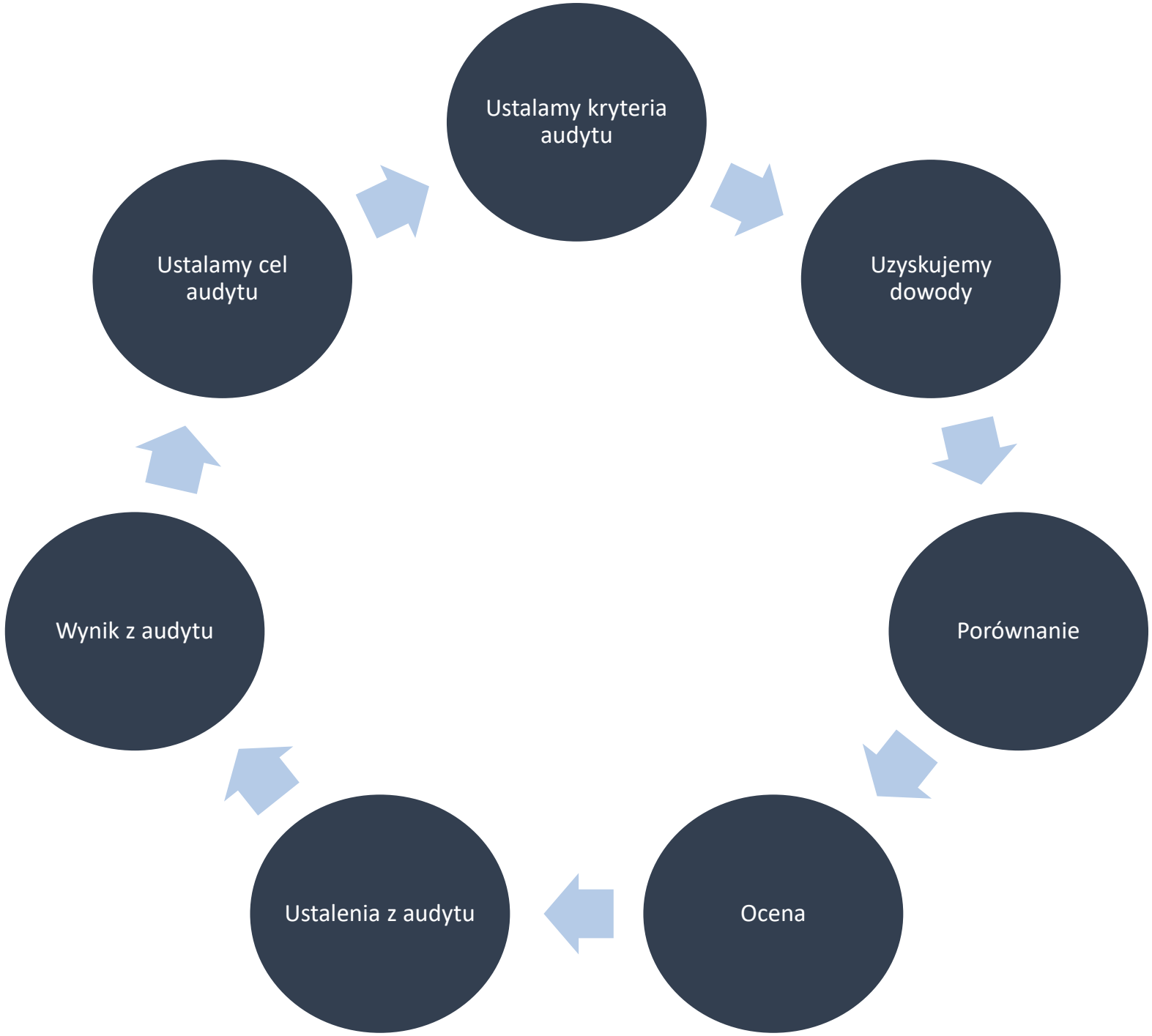
Kryteria audytu – zestaw polityk, procedur lub wymagań **używanych jako odniesienie**, do których porównuje się dowody z audytu.

Dowód z audytu – zapisy, stwierdzenia faktu lub inne informacje, które są istotne ze względu na kryteria audytu.

Ustalenia z audytu – wyniki oceny dowodów z audytu w stosunku do kryteriów

Audyt – wprowadzenie i podstawowe pojęcia

1. **Ustalamy cel audytu –** co jest naszym głównym celem? Cele mogą wynikać np. z wymogów prawnych, zamierzeń biznesowych etc.
2. **Kryteria audytu –** wymagania tj. w odniesieniu do czego będziemy określać zgodność?
3. **Uzyskujemy dowody –** pod kątem ustalonych kryteriów
4. **Porównujemy kryteria do dowodów** – by dokonać oceny
5. **Dokonujemy oceny** – czynimy ustalenia z audytu
6. **Wynik audytu –** po rozważeniu celu i ustaleń


Ustalamy kryteria audytu
Uzyskujemy dowody
Porównanie
Ocena
Ustalenia z audytu
Wynik z audytu
Ustalamy cel audytu


GKK
GUMULARZ
KOZIEŁ
KOZIK

Audyt – wprowadzenie i podstawowe pojęcia

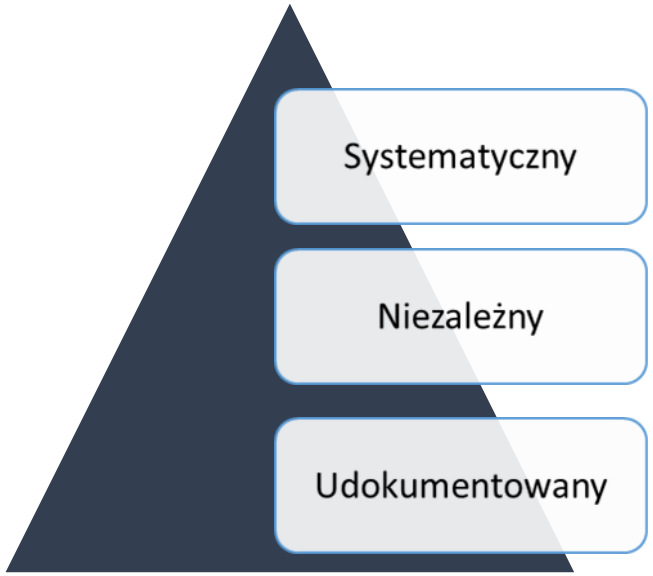
Co jeszcze? Harmonogram audytu

Harmonogram audytu – określający zakres, czas trwania audytu

- **Metody audytu** – jak będziemy audytować?
- **Wyznaczenie zespołu audytującego** – kto będzie audytował?
- **Wyznaczenie zespołu audytowanego** – kogo będziemy audytować?
- **Wskazanie niezbędnych zasobów –** kwestie organizacyjne

Audyt – cechy audytu wg ISO

1. **Systematyczny** – zaplanowany i przygotowany, przebiegający według określonego porządku
2. **Niezależny** – brak odpowiedzialności za działania będące przedmiotem audytu, brak uprzedzeń i konfliktu interesów
3. **Udokumentowany** – należy dokumentować wszelkie ustalenia, a audyt zakończyć sprawozdaniem.



Schemat audytu:

- Przygotowanie audytu
- Przeprowadzenie audytu
- Zakończenie
- Oddziaływanie

GKK GUMULARZ KOZIEŁ KOZIK

Audyt – wprowadzenie i podstawowe pojęcia

Schemat audytu:

1. Przygotowanie audytu

Poznanie kontekstu organizacji - analiza dostępnych informacji, schematu organizacyjnego, stron internetowych

Przygotowanie harmonogramu – kiedy, gdzie, o której, z kim i co będziemy audytować?

Przygotowanie członków zespołu audytującego, w tym dokumentów potrzebnych do przeprowadzenia audytu

Audyt – wprowadzenie i podstawowe pojęcia

2. Przeprowadzenie audytu

Spotkanie otwierające

Uzyskiwanie dowodów z audytu

Uzyskiwanie ustaleń i wniosków

Spotkanie zamykające

3. Zakończenie audytu

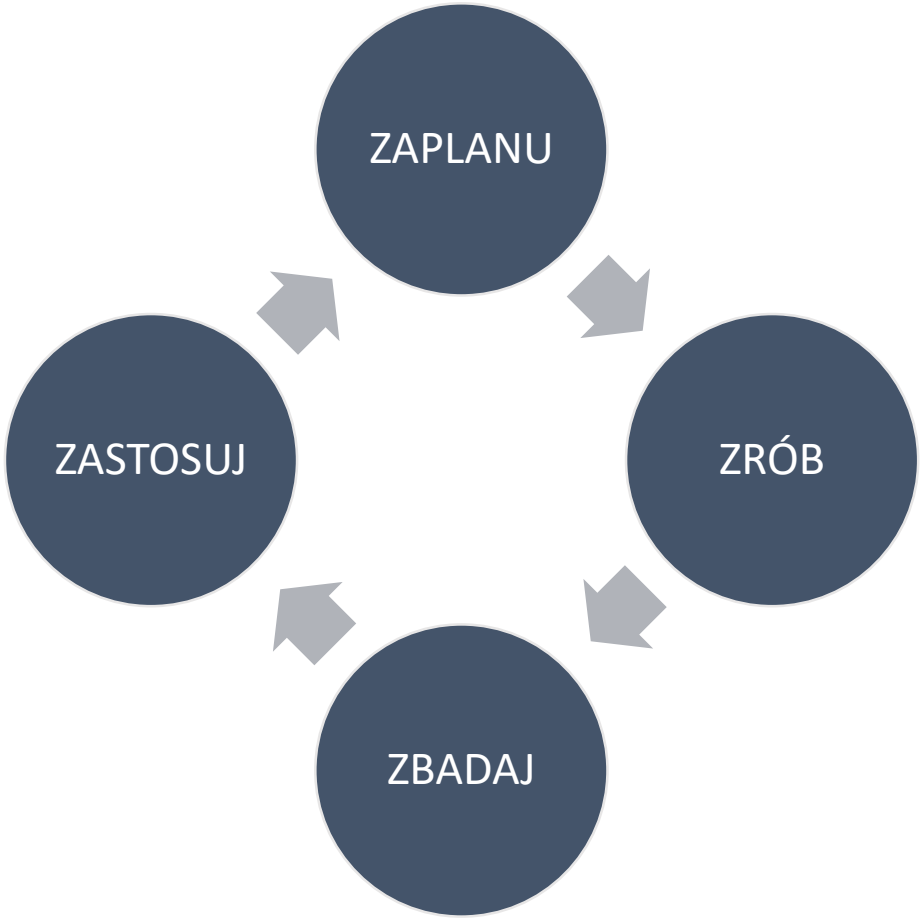
Przygotowanie raportu z audytu opisującego stan faktyczny, przebieg audytu, stwierdzone niezgodności

Audyt – wprowadzenie i podstawowe pojęcia

4. **Oddziaływanie**

Zalecenia, wnioski poaudytowe

Audyt jako proces – PDCA (cykl Deminga)



A jaki powinien być audytor?

GKK GUMULARZ KOZIEŁ KOZIK

Audyt ochrony danych osobowych

- brak definicji i regulacji audytu w ustawie o ochrony danych osobowych
- audyt jako element kontroli przetwarzania

P. Fajgielski: *„najogólniej mianem audytu przetwarzania i ochrony danych osobowych można określić sprawdzenie stosowanych w danej jednostce organizacyjnej rozwiązań technicznych i organizacyjnych służących przetwarzaniu i ochronie danych osobowych pod kątem skuteczności oraz spełnienia wymogów wynikających z przepisów prawa, dokonywane z reguły przez niezależnych ekspertów”*

- definicja sprawdzenia w przepisach wykonawczych do uodo:

„sprawdzenie – czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (definicja z Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r.)

Sprawdzenie a audyt ochrony danych osobowych

ABI

- sprawdzenie – główne zadanie

ADO

- audyt

Powołanie ABI – kryteria ustawowe

administrator danych osobowych może powołać ABI (fakultatywność)

ABI może być osoba, która:

- ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych,
- posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,
- nie była karana za umyślne przestępstwo.

Administrator danych może powołać zastępców ABI którzy spełniają powyższe warunki.

GKK GUMULARZ KOZIEŁ KOZIK

ABI

Jeżeli administrator danych skorzysta z przysługującego mu uprawnienia i powoła administratora bezpieczeństwa informacji, zgodnie z art. 46b ust. 1 u.o.d.o., **ma 30 dni od dnia powołania ABI na zgłoszenie tego faktu do rejestracji Generalnemu Inspektorowi.**

ABI zgłoszeni do rejestracji GIODO są wpisywani do ogólnokrajowego, jawnego rejestru (art. 46c u.o.d.o.).

Administrator danych, który zgłosi ABI do rejestracji zobowiązany jest zgłaszać Generalnemu Inspektorowi każdą zmianę informacji objętych zgłoszeniem powołania ABI w terminie 14 dni, a także jego odwołanie w terminie 30 dni, odpowiednio od dnia dokonania zmiany lub odwołania**.**

Zgłoszenia powołania ABI do rejestracji Generalnemu Inspektorowi oraz zgłoszenia odwołania ABI należy dokonać przy użyciu wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji, które stanowią załączniki do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. (Dz. U. z 2014 r., poz. 1934).

ABI a IOD

Co się stanie z ABI po 25 maja 2018 roku?

ABI a IOD

Projekt nowej ustawy o ochronie danych osobowych

Powołanie Inspektora ochrony danych (IOD)

Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa

GKK GUMULARZ KOZIEŁ KOZIK

Powołanie Inspektora ochrony danych (IOD)

Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, **a w szczególności wiedzy fachowej** na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań

ABI posiada **odpowiednią wiedzę** w zakresie ochrony danych osobowych

Zadania ABI

1) **zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności** przez:

- **sprawdzanie zgodności** przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie **sprawozdania dla administratora danych,**
- nadzorowanie opracowania i aktualizowania dokumentacji przetwarzania oraz przestrzegania zasad w niej określonych,
- zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora – na warunkach określonych w przepisach.

Administrator danych **może powierzyć ABI wykonywanie innych obowiązków**, jeżeli nie naruszy to prawidłowego wykonywania zadań.

GKK GUMULARZ KOZIEŁ KOZIK

Audyty IOD vs. sprawdzenia ABI

monitorowanie przestrzegania przepis. rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz **powiązane z tym audyty**

zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez **sprawdzanie zgodności** przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie **sprawozdania dla administratora danych,**

Sprawdzenie a audyt ochrony danych osobowych – UODO i RODO

ABI	• sprawdzenie
IOD	• audyt

Kazus – oceń stan faktyczny

W Spółce ABC sp. z o.o. powołano na stanowisko ABIego Adama Bielskiego – pracownika działu IT. Adam Bielski bardzo ucieszył się ze zmiany zakresu obowiązków, gdyż uznał, że jako pracownik działu IT pełniący dotychczas funkcję ASI, pomaga na co dzień w zabezpieczaniu systemów służących do przetwarzania danych osobowych, więc idealnie sprawdzi się w tej dodatkowej roli. Adam Bielski, jako osoba będąca jednocześnie ABI i ASI, otrzymał stanowisko kierownika działu IT, podległego dyrektorowi ds. informatycznych. Adam Bielski bardzo wczuł się w swoją rolę. Już następnego dnia rozpoczął audyt umów z podwykonawcami Spółki. W czasie analizy umów spostrzegł, że umowa zawarta z firmą Host-Net nie porusza kwestii dotyczących ochrony danych osobowych choć w jego przekonaniu powinna, zatem odnotował, że należy uzupełnić umowę o wskazane kwestie. Przełożony Adama Bielskiego, gdy tylko się o tym dowiedział, stwierdził, że umowa jest w porządku, bo są w niej już kwestie dotyczące zachowania w poufności wszystkich informacji, w tym danych osobowych. Adam przyznał mu rację, uznając, że przełożony ma większą wiedzę i odnotował, że umowa jest prawidłowa.

ABI w wykonywaniu swoich zadań

- Komu podlega ABI?
- Czy ABI może podlegać dyrektorowi ds. informatycznych?
- Czy ABIego można audytować?
- Czy można wydawać mu polecenia dotyczące sposobu realizacji zadań ABI np. dotyczące przeprowadzanych sprawdzeń?
- Czy ABI może być jednocześnie ASI?
- Czy ABI może być kierownikiem działu IT?

GKK GUMULARZ KOZIEŁ KOZIK

Status ABI

- ABI podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych (art. 36a ust. 7 uodo)
- Administrator danych zapewnia **środki i organizacyjną odrębność ABI niezbędne do niezależnego wykonywania przez niego zadań** (art. 36a ust. 8 uodo)

Łączenie funkcji ABI z funkcją ASI (czy innym stanowiskiem kierowniczym) może powodować zagrożenia dla bezpieczeństwa przetwarzania danych osobowych i rodzić konflikt interesów (ta sama osoba decyduje i jednocześnie weryfikuje)

Odrębność organizacyjna i niezależność ABI w wykonywaniu zadań !!!

IOD

Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych **nie otrzymywał instrukcji dotyczących wykonywania tych zadań**.

Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. **Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.**

Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by **takie zadania i obowiązki nie powodowały konfliktu interesów.**

Administrator oraz podmiot przetwarzający zapewniają, by **inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych**.

Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

GKK GUMULARZ KOZIEŁ KOZIK

Zadania ustawowe ABI

- Zapewnianie przestrzeganie przepisów ODO (szeroko pojęte)
- **Przeprowadzanie sprawdzeń**
- Opracowywanie sprawozdania ze sprawdzenia dla ADO
- Nadzorowanie opracowania i aktualizowania dokumentacji
- Nadzorowanie zasad określonych w dokumentacji
- Zapoznanie osób upoważnionych do przetwarzania z przepisami ODO
- Prowadzenie rejestru zbiorów danych

+

- **GIODO może zwrócić się do ABI wpisanego do rejestru, o dokonanie sprawdzenia u administratora danych, który go powołał, wskazując zakres i termin sprawdzenia**. ABI przedstawia GIODO sprawozdanie ze sprawdzenia.

Rodzaje sprawdzeń dokonywanych przez ABI:

- dla administratora danych osobowych
- dla GIODO

Tryby dokonywania sprawdzeń przez ABI:

- **sprawdzenia planowe** – dokonywane wg planu sprawdzeń
- **sprawdzenia doraźne** – gdy ABI poweźmie wiadomość o naruszeniu ochrony danych osobowych lub uzasadnione podejrzenie jego wystąpienia
- sprawdzenia dokonywane **na wniosek GIODO**

Sprawdzenie doraźne

Sprawdzenie doraźne jest przeprowadzane niezwłocznie **po powzięciu wiadomości** przez administratora bezpieczeństwa informacji o naruszeniu ochrony danych osobowych **lub uzasadnionym podejrzeniu takiego naruszenia.**

Naruszenie ochrony danych – brak definicji w UODO

Definicja w RODO:

„naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Wiadomość lub podejrzenie – c.d.

Należy zawiadomić kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności **w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.**

Zawiadomienia nie przekazuje się w przypadku sprawdzenia doraźnego, **jeżeli niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy naruszenie miało miejsce.**

Należy powiadomić ADO przed podjęciem pierwszej czynności w toku sprawdzenia doraźnego.

Sprawdzenie doraźne - ćwiczenie

Zostałeś powołany jako ABI w spółce ABC sp. z o.o. Gdy przyszedłeś po tygodniowym urlopie do siedziby Spółki, w okolicach godziny 10:00 przy przyszedł do Ciebie pracownik działu obsługi klienta Krzysztof Nowak i powiedział, że dostał w nocy wiadomość e-mail od zdenerwowanego klienta spółki pana Marka Szumnego, który napisał, że jest oburzony tym, że w spółce ABC nie chroni się danych osobowych klientów, a pracownik Adam Kowalski powinien zostać zwolniony, za takiego maila (nie wyjaśniając przy tym o co chodzi).

Adam Kowalski to nowy pracownik, pracujący w spółce ABC sp. z o.o. od trzech dni. Jego praca polega na obsłudze klienta, w tym na przesyłaniu klientom ofert na produkty spółki (taką ofertę przesłał Panu Szumnemu).

Oceń stan faktyczny i powiedz jakie podejmiesz czynności.

Sprawdzenie doraźne – plan działania

Plan działania			
Wiadomość o naruszeniu lub podejrzenie naruszenia	Ustalenie jakie czynności muszą być podjęte • w przypadku naruszenia – **czynności naprawcze** • w przypadku podejrzenia – **weryfikacja czy doszło do naruszenia i ew. dalsze czynności**	Zawiadomienie kierownika jednostki, chyba że trzeba niezwłocznie działać	Powiadomienie ADO

GKK GUMULARZ KOZIEŁ KOZIK

Sprawdzenia – sposób i zakres dokumentowania

ABI dokumentuje czynności przeprowadzone w toku sprawdzenia, **w zakresie** niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych **oraz do opracowania sprawozdania**.

Dokumentowanie może polegać, w szczególności, na **utrwaleniu danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz** na:

1) **sporządzeniu notatki** z czynności, **w szczególności z** zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;

2) **odebraniu wyjaśnień osoby**, której czynności objęto sprawdzeniem;

3) **sporządzeniu kopii** otrzymanego dokumentu;

4) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;

5) sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

Sprawdzenia – sposób i zakres dokumentowania

Sprawozdanie, powinno zawierać:

1. oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania;
2. imię i nazwisko administratora bezpieczeństwa informacji;
3. wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach;
4. datę rozpoczęcia i zakończenia sprawdzenia;
5. określenie przedmiotu i zakresu sprawdzenia;

Sprawdzenia – sposób i zakres dokumentowania

Sprawozdanie, powinno zawierać:

6. opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;

7. **stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem**;

8. wyszczególnienie załączników stanowiących składową część sprawozdania;

9. podpis administratora bezpieczeństwa informacji, a w przypadku sprawozdania w postaci papierowej – dodatkowo parafy administratora bezpieczeństwa informacji na każdej stronie sprawozdania;

10. datę i miejsce podpisania sprawozdania przez administratora bezpieczeństwa informacji.

Sprawdzenia – sposób i zakres dokumentowania

Po zakończeniu sprawdzenia administrator bezpieczeństwa informacji przygotowuje sprawozdanie.

Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.

Administrator bezpieczeństwa informacji przekazuje administratorowi danych sprawozdanie:

1. ze sprawdzenia planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia;
2. ze sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia;
3. ze sprawdzenia, o którego dokonanie zwrócił się Generalny Inspektor – zachowując termin wskazany przez Generalnego Inspektora;

Sprawdzenie doraźne – ćwiczenia

W toku podjętych czynności okazało się, że Kowalski wysłał ofertę Panu Szumnemu, ale na liście mailingowej było także 250 innych adresatów (klientów) do wiadomości.

Jak należy ocenić powyższe?

Czy należy podjąć/rekomendować jakieś działania?

Wewnętrznie? Wobec klientów?

Sprawdzenia – ćwiczenia

Przygotuj sprawozdanie ☺

Sprawdzenie doraźne

1. Sporządzamy notatkę
2. Ustalamy zakres planowanych czynności:
   a. odebranie wyjaśnień od Krzysztofa Nowaka
   b. uzyskanie kopii wiadomości e-mail od klienta którą otrzymał
   c. odebranie wyjaśnień od Adama Kowalskiego
   d. sporządzenie kopii wiadomości wysłanej przez Kowalskiego do klienta Szumnego
   e. sprawdzenie podstaw prawnych wysyłki oferty
   f. sprawdzenie czy Kowalski został przeszkolony
3. Zawiadomienie kierownika jednostki – czy w tym konkretnym przypadku?
4. Zawiadomienie ADO

Sprawdzenie doraźne – ćwiczenia

Co należałoby przygotować?

1. Notatkę z uzyskania informacji o podejrzeniu naruszenia
2. Wzór protokołu z odebrania wyjaśnień
3. Wzór zawiadomienia ADO
4. Wzór zawiadomienia kierownika jednostki
5. Wniosek do ADO o podjęcie działań

Sprawdzenie doraźne – ćwiczenia

Netia wzorowo informuje osoby poszkodowane w wycieku

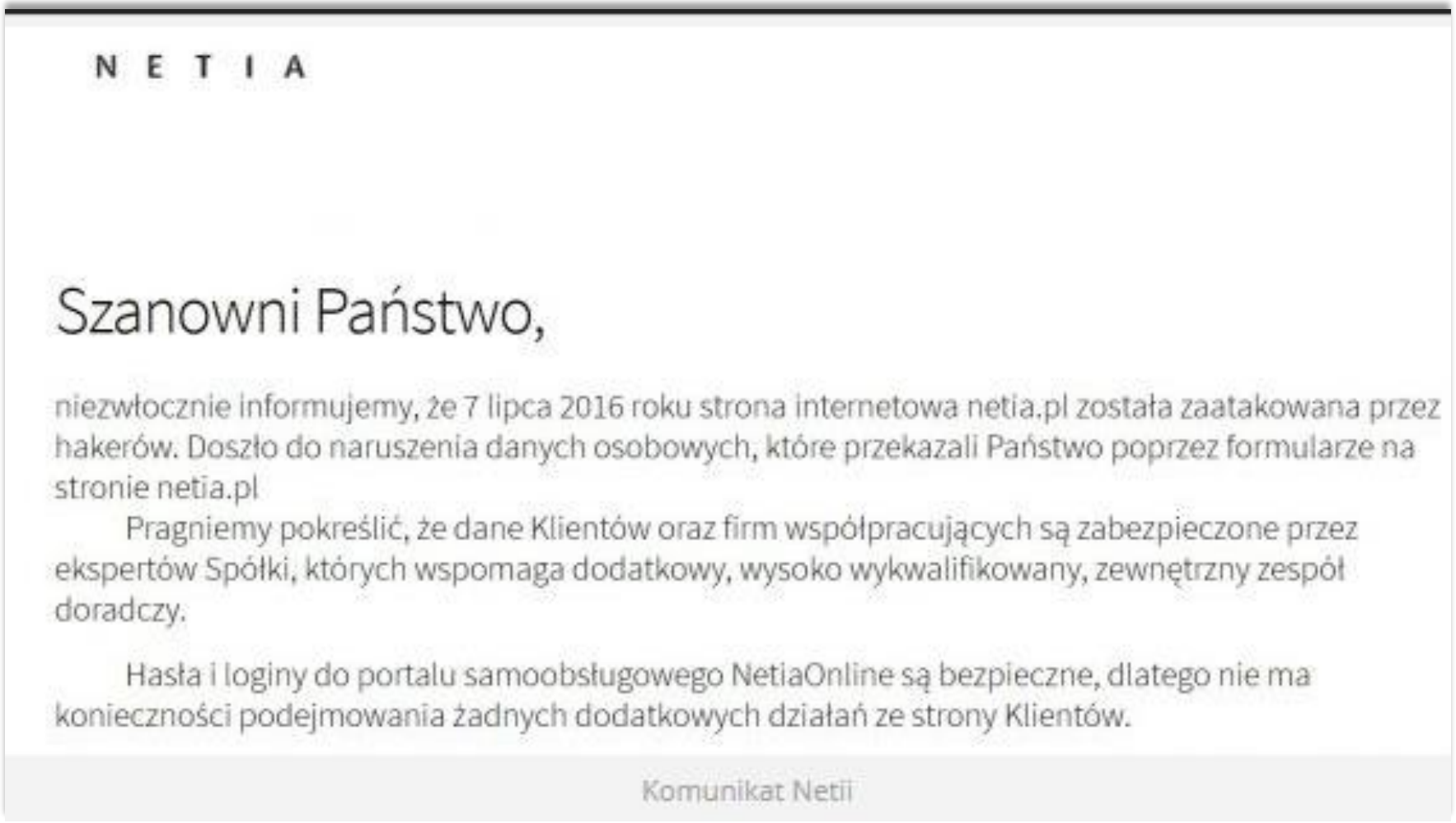
Adam dodał 9 lipca 2016 o 21:36 w kategorii Włamania z tagami: incydent • Netia

W przypadku incydentów bezpieczeństwa związanych z wyciekami danych rzadko można napisać coś dobrego o sposobie w jaki poszkodowana firma reaguje na incydent oraz jak informuje ofiary. Tym razem jest jednak inaczej.

Włamania i wycieki danych stają się chlebem powszednim firm i ich klientów. Miliardy wpisów z baz danych takich gigantów jak Adobe, LinkedIn czy Myspace krążą po sieci. W dzisiejszych czasach mówi się nawet, że incydentom nie można zapobiec – można jedynie skracać czas ich wykrycia i poprawiać sposób reakcji. Dzisiejszy artykuł będzie właśnie o reakcji – i to o reakcji właściwej i całkiem dojrzałej.

GKK GUMULARZ KOZIEŁ KOZIK

Reakcja na naruszenia



NETIA

Szanowni Państwo,

niezwłocznie informujemy, że 7 lipca 2016 roku strona internetowa netia.pl została zaatakowana przez hakerów. Doszło do naruszenia danych osobowych, które przekazali Państwo poprzez formularze na stronie netia.pl

Pragniemy pokreślić, że dane Klientów oraz firm współpracujących są zabezpieczone przez ekspertów Spółki, których wspomaga dodatkowy, wysoko wykwalifikowany, zewnętrzny zespół doradczy.

Hasła i loginy do portalu samoobsługowego NetiaOnline są bezpieczne, dlatego nie ma konieczności podejmowania żadnych dodatkowych działań ze strony Klientów.

Komunikat Netii

GKK GUMULARZ KOZIEŁ KOZIK

Incydenty na gruncie RODO

Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu

Art. 33 ust. 5 RODO: Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze**.**

Sprawdzenia na wniosek GIODO

GIODO może zwrócić się do administratora bezpieczeństwa informacji wpisanego do rejestru, o dokonanie **sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych** u administratora danych, który go powołał**, wskazując zakres i termin sprawdzenia**.

Po dokonaniu sprawdzenia, administrator bezpieczeństwa informacji, **za pośrednictwem administratora danych**, przedstawia Generalnemu Inspektorowi sprawozdanie.

Sprawdzenia na wniosek GIODO

Administrator bezpieczeństwa informacji zawiadamia administratora danych **o zakresie dokonywanych czynności** w ramach sprawdzenia na wniosek GIODO **przed podjęciem pierwszej czynności w toku sprawdzenia.**

Dokonanie przez administratora bezpieczeństwa informacji sprawdzenia, **nie wyłącza prawa Generalnego Inspektora do przeprowadzenia kontroli.**

Sprawdzenia na wniosek GIODO - ćwiczenie

Jesteś ABIm w spółce ABC sp. z o.o. W dniu dzisiejszym otrzymałeś pismo z GIODO, w którym zwraca się ono do Ciebie o dokonanie sprawdzenia w Spółce, w terminie 21 dni od dnia otrzymania pisma. Sprawdzenie ma dotyczyć **danych kandydatów do pracy w Spółce w zakresie realizacji wobec nich obowiązku informacyjnego (24 i 25 uodo).**

Spółka prowadzi rekrutacje zarówno przez portal pracuj.pl, jak też przez swoją stronę internetową – poprzez zakładkę „kariera", gdzie umieszcza ogłoszenia o pracę. W spółce funkcjonuje także adres e-mail kariera@abc.pl, na który można przesyłać CV nawet gdy Spółka nie prowadzi konkretnych rekrutacji. CV można także przynieść na portiernię i wówczas pracownik ochrony przekazuje je do działu HR. Spółka ABC sp. z o.o. otrzymuje także CV kandydatów do pracy od innej spółki z grupy, która przy prowadzeniu swoich rekrutacji zbiera zgody na udostępnienie danych kandydatów do Spółki ABC sp. z o.o.

Napisz jakie podejmiesz czynności.

Sprawdzenia na wniosek GIODO - ćwiczenie

1. Sporządzenie notatki – odnotowanie daty wpływu pisma!!!
2. Ustalenie zakresu czynności:
   a. Zweryfikowanie zakładki „kariera”
   b. Zweryfikowanie treści ogłoszeń na pracuj.pl
   c. Zweryfikowanie umowy z pracuj.pl
   d. Zweryfikowanie procedury prowadzenia rekrutacji
   e. Rozmowa z pracownikami działu HR odpowiedzialnymi za rekrutacje
   f. Rozmowa z pracownikami ochrony przyjmującymi CV
   g. Zweryfikowanie procedury przyjmowania CV
   h. Zweryfikowanie umowy ze spółką z grupy udostępniającą dane
   i. Zweryfikowanie sposobu i miejsca udostępnienia danych od spółki z grupy
   j. Zweryfikowanie zawartości dedykowanych skrzynek mailowych
3. Zawiadomienie kierownika jednostki
4. Powiadomienie ADO

Sprawdzenie na wniosek GIODO – plan działania

Plan działania			
Wniosek GIODO o dokonanie sprawdzenia	Ustalenie jakie czynności muszą być podjęte	Zawiadomienie kierownika jednostki, chyba że nie pozwala na to wyznaczony termin	Powiadomienie ADO

GKK GUMULARZ KOZIEŁ KOZIK

Sprawdzenia planowe

Plan sprawdzeń określa:

- Przedmiot sprawdzenia – jakie zbiory danych i systemy będziemy sprawdzać?
- Zakres sprawdzenia – w jakim zakresie będziemy je sprawdzać?
- Termin przeprowadzenia sprawdzeń – kiedy będziemy sprawdzać?
- Sposób i zakres dokumentowania sprawdzeń – jak będziemy dokumentować?

Administrator bezpieczeństwa informacji zawiadamia kierownika jednostki organizacyjnej objętej sprawdzeniem o **zakresie planowanych czynności** w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

GKK GUMULARZ KOZIEŁ KOZIK

Sprawdzenia planowe – przedmiot i zakres sprawdzenia

Administrator bezpieczeństwa informacji w planie sprawdzeń uwzględnia, w szczególności:

- **zbiory danych osobowych i systemy informatyczne** służące do przetwarzania danych osobowych, np. dane pracowników, system SAP

- **konieczność weryfikacji zgodności przetwarzania danych osobowych:**

  1) z zasadami, o których mowa w art. 23–27 i art. 31–35 uodo;

  2) z zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36, art. 37–39 uodo oraz przepisach wydanych na podstawie art. 39a uodo;

  3) z zasadami przekazywania danych osobowych, o których mowa w art. 47–48;

  4) z obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane, o których mowa w art. 27 ust. 1 uodo.

Sprawdzenia planowe – termin sprawdzenia

Plan sprawdzeń jest przygotowywany przez administratora bezpieczeństwa informacji **na okres nie krótszy niż kwartał i nie dłuższy niż rok**.

Plan sprawdzeń jest przedstawiany administratorowi danych **nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem**. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych **powinny być objęte sprawdzeniem co najmniej raz na pięć lat.**

ABI zawiadamia kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności **w terminie co najmniej 7 dni** przed dniem przeprowadzenia czynności.

Sprawdzenia planowe – jakich dokumentów potrzebujemy?

Zadanie – przygotuj plan sprawdzenia.

Jesteś ABIm w spółce Marketing ABC Polska sp. z o.o. z siedzibą w Warszawie przy ul. Warszawskiej 17. Spółka posiada także biura w Lublinie (sprzedaż) i Krakowie (marketing), a co więcej jest częścią grupy spółek Marketing ABC (spółka „matka" Marketing ABC Japan, ma siedzibę w Japonii).

W związku z tym, że spółka „matka" dostarczyła Spółce nowe narzędzia marketingowe, Spółka Marketing ABC Polska zaczęła właśnie przesyłać swoim klientom newsletter, za pośrednictwem systemu spółki Marketing ABC Japan (system Marketing PLUS). Spółka Marketing ABC Polska korzysta także z dwóch agencji marketingowych, które mają jej pomagać w wysyłce newslettera. Pracownicy działu marketingu i sprzedaży cieszą się z nowych możliwości promocji Spółki, gdyż nigdy wcześniej nie korzystali z adresów e-mail klientów dla celów marketingowych (dział marketingu w ogóle z nich nie korzystał, a dział sprzedaży korzystał z części z nich wyłącznie dla wykonywania umowy). Dział marketingu przed wysyłką newslettera zorganizował konkurs dla klientów, dzięki czemu zebrał dane potrzebne do wysyłki newslettera od klientów którzy wzięli udział w konkursie.

Sprawdzenia planowe – co sprawdzamy jakich dokumentów potrzebujemy?

1. Zbiór danych klientów – newsletter, system Marketing PLUS
2. Pomieszczenia działu sprzedaży i marketingu – Lublin i Kraków
3. Podstawy przetwarzania danych
4. Realizacja praw podmiotów danych np. spełnienie obowiązku informacyjnego
5. Zgodność z zasadami przetwarzania
6. Umowy powierzenia z agencjami marketingowymi
7. Przekazywanie danych do Japonii
8. Zabezpieczenie danych (środki techniczne i organizacyjne)
9. Upoważnienia – zakres (skoro dział m. wcześniej nie przetwarzał tych danych)
10. Dokumentacja

Jak będziemy sprawdzać i jak dokumentować?

Sprawdzenia planowe – co sprawdzamy jakich dokumentów potrzebujemy?

1. Zbiór danych klientów – newsletter, system Marketing PLUS
2. Pomieszczenia działu sprzedaży i marketingu – Lublin i Kraków
3. Podstawy przetwarzania danych
4. Realizacja praw podmiotów danych np. spełnienie obowiązku informacyjnego
5. Zgodność z zasadami przetwarzania
6. Umowy powierzenia z agencjami marketingowymi
7. Przekazywanie danych do Japonii
8. Zabezpieczenie danych (środki techniczne i organizacyjne)
9. Upoważnienia – zakres (skoro dział m. wcześniej nie przetwarzał tych danych)
10. Dokumentacja

Jak będziemy sprawdzać i jak dokumentować?

Sprawdzenia planowe – checklista - ćwiczenie

Przygotuj uniwersalną listę pytań audytowych, która pomoże Ci zweryfikować zgodność przetwarzania danych osobowych:

1) z zasadami, o których mowa w art. 23–27 i art. 31–35 uodo;

2) z zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36, art. 37–39 uodo oraz przepisach wydanych na podstawie art. 39a uodo;

3) z zasadami przekazywania danych osobowych, o których mowa w art. 47–48;

4) z obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane, o których mowa w art. 27 ust. 1 uodo.

Audyt dokumentacji

Administrator bezpieczeństwa informacji **dokonuje weryfikacji:**

1) opracowania i kompletności dokumentacji przetwarzania danych;

2) zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa;

3) stanu faktycznego w zakresie przetwarzania danych osobowych;

4) zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych;

5) przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych

GKK GUMULARZ KOZIEŁ KOZIK

Weryfikacja dokumentacji

Administrator bezpieczeństwa informacji przeprowadza weryfikację:

1) w sprawdzeniach

2) poza sprawdzeniami, na podstawie zgłoszenia osoby wykonującej obowiązki określone w dokumentacji przetwarzania danych oraz własnego udziału administratora bezpieczeństwa informacji w procedurach w niej określonych.

Administrator bezpieczeństwa informacji może przeprowadzić weryfikację poza sprawdzeniami, na podstawie zgłoszenia osoby trzeciej.

GKK GUMULARZ KOZIEŁ KOZIK

Wykrycie nieprawidłowości w dokumentacji

W przypadku wykrycia podczas weryfikacji nieprawidłowości administrator bezpieczeństwa informacji:

1) zawiadamia administratora danych **o nieopracowaniu lub brakach** w dokumentacji przetwarzania danych lub jej elementach oraz działaniach podjętych w celu doprowadzenia dokumentacji do wymaganego stanu, w szczególności może przedstawić mu do wdrożenia projekty dokumentów usuwające stan niezgodności;

2) zawiadamia administratora danych **o nieaktualności** dokumentacji przetwarzania danych oraz może przedstawić administratorowi danych do wdrożenia projekty dokumentów aktualizujących;

3) **poucza lub instruuje osobę nieprzestrzegającą zasad** określonych w dokumentacji przetwarzania danych o prawidłowym sposobie ich realizacji lub zawiadamia administratora danych, wskazując osobę odpowiedzialną za naruszenie tych zasad oraz jego zakres (w odrębnym dokumencie)

Zawiadomienia mogą być zawarte w sprawozdaniu albo w odrębnym dokumencie.

Wykrycie nieprawidłowości w dokumentacji

W przypadku wykrycia podczas weryfikacji nieprawidłowości administrator bezpieczeństwa informacji:

1) zawiadamia administratora danych **o nieopracowaniu lub brakach** w dokumentacji przetwarzania danych lub jej elementach oraz działaniach podjętych w celu doprowadzenia dokumentacji do wymaganego stanu, w szczególności może przedstawić mu do wdrożenia projekty dokumentów usuwające stan niezgodności;

2) zawiadamia administratora danych **o nieaktualności** dokumentacji przetwarzania danych oraz może przedstawić administratorowi danych do wdrożenia projekty dokumentów aktualizujących;

3) **poucza lub instruuje osobę nieprzestrzegającą zasad** określonych w dokumentacji przetwarzania danych o prawidłowym sposobie ich realizacji lub zawiadamia administratora danych, wskazując osobę odpowiedzialną za naruszenie tych zasad oraz jego zakres (w odrębnym dokumencie)

Zawiadomienia mogą być zawarte w sprawozdaniu albo w odrębnym dokumencie.

Wykrycie nieprawidłowości w dokumentacji

Polityka bezpieczeństwa, zawiera w szczególności:

1. wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
2. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4. sposób przepływu danych pomiędzy poszczególnymi systemami;
5. określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Wykrycie nieprawidłowości w dokumentacji

Instrukcja zarządzania systemem informatycznym, zawiera w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;

2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

Wykrycie nieprawidłowości w dokumentacji

Instrukcja zarządzania systemem informatycznym, zawiera w szczególności:

5) sposób, miejsce i okres przechowywania:

a) elektronicznych nośników informacji zawierających dane osobowe,

b) kopii zapasowych, o których mowa w pkt 4,

6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;

7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 (odnotowywanie informacji w systemie)

8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Wykrycie nieprawidłowości w dokumentacji

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym:

1) podstawowy;

2) podwyższony;

3) wysoki.

Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

Opis środków bezpieczeństwa stosowany na poziomach, o których mowa w ust. 1, określa załącznik do rozporządzenia.

Wykrycie nieprawidłowości w dokumentacji – wybrane środki

Obszar przetwarzania, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze przetwarzania, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni

Wykrycie nieprawidłowości w dokumentacji – wybrane środki

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

3) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.Kopie zapasowe:

a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;

b) usuwa się niezwłocznie po ustaniu ich użyteczności

Wykrycie nieprawidłowości w dokumentacji - ćwiczenia

Jesteś ABIm w spółce ABC. Spółka posiada Politykę Bezpieczeństwa i Instrukcję zarządzania systemem informatycznym, ale masz wątpliwości czy pracownicy znają ich treść (w zakresie wskazanym powyżej).

Przygotuj listę pytań kontrolnych do pracowników mających na celu sprawdzenie ich znajomości dokumentacji.

Audyt u procesora

1. Co do zasady ABI prowadzić tzw. audyt pierwszej strony – wewnętrzny
2. Możliwe jest także przeprowadzenie audytu tzw. drugiej strony – podmiotowi któremu powierzono dane do przetwarzania, gdy to wynika z umowy:

„Administrator ma prawo do kontroli sposobu wykonywania umowy przez procesora w zakresie……”

RODO:

Umowa stanowi, że podmiot przetwarzający: (…) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Dziękuję za uwagę

r.pr. Patrycja Kozik
p.kozik@gkklegal.pl

GKK
GUMULARZ
KOZIEŁ
KOZIK