płk rez. mgr inż. Dariusz Kilian

Autor artykułu — jest ekspertem Instytutu Bezpieczeństwa i Rozwoju Międzynarodowego SDirect24, a ponadto absolwentem m.in. studiów podyplomowych w Wyższej Szkole Bankowej w Toruniu – kierunek: „Ochrona danych osobowych w praktyce", auditorem wewnętrznym systemu zarządzania bezpieczeństwem informacji lSO/lEC 27001:2017 oraz wykładowcą ochrony danych osobowych w wyższej uczelni na kierunku Kadry i prawo pracy. Prowadzi działalność gospodarczą dotyczącą szkoleń i wdrożeń w zakresie RODO.

KARY ZA RODO

Kary w systemie prawnym zawsze wzbudzają emocje, które w przypadku ochrony danych osobowych wzmacnia przekonanie części społeczeństwa, że jest to w Polsce temat nowy, wymagający wdrażania, informowania i mniej restrykcyjnego podejścia. Z niektórymi z tych twierdzeń zgadzam się z innymi zaś nie. Zapraszam do lektury artykułu i powszechnej dyskusji na temat ochrony danych, nie tylko osobowych, w Polsce.

W społecznym odczuciu, z jakim spotykam się stosunkowo często – ochrona danych osobowych w Polsce jest czymś nowym, niepotrzebnym, a wręcz w ocenie części osób, zupełnie szkodliwym. W tym miejscu należy przypomnieć, iż ochrona danych osobowych (ODO) została w Polsce uregulowana ustawą już w **1997 roku** (ustawa z 29 sierpnia 1997 r. Dz.U. 1997 nr 133 poz. 883). Mimo, że ustawa ta przestała obowiązywać (została zastąpiona ustawą o ochronie danych osobowych z 10 maja 2018 r. Dz. U. 2018 poz. 1000 z późniejszymi zmianami) (UODO) – nader często spotykam się z dokumentami, w których jako podstawę prawną przetwarzania danych nadal wykazuje się tę z 1997 roku!

28 stycznia br. obchodziliśmy 14. Europejski Dzień Ochrony Danych Osobowych.

W ustawie z 1997 roku istniały już zapisy (artykuły od 49 do 54a), które przewidywały katalog kar takich jak: grzywna, kara ograniczenia wolności albo pozbawienia wolności

w maksymalnym wymiarze do trzech lat. Jednocześnie należy zauważyć, że wymiar grzywny (na podstawie ustawy z 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji) nie mógł przekroczyć kwoty 10 tys. zł w stosunku do osób fizycznych, a w stosunku do osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej - kwoty 50 tys. zł. Grzywny nakładane wielokrotnie nie mogły łącznie przekroczyć kwoty 50 tys. zł, a w stosunku do osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej – kwoty 200 tys. zł.

Obywatele mieli zatem wystarczająco dużo czasu, aby „oswoić" się z nowymi przepisami i dostosować swoje postępowanie, a firmy, instytucje, przedsiębiorstwa, urzędy i inne podmioty, aby zapoznać się i swoich pracowników z przepisami, sporządzić i wdrożyć niezbędną dokumentację oraz zawrzeć stosowne umowy powierzenia przetwarzania danych osobowych.

W obecnie obowiązującej ustawie z 2018 r. kary opisano w rozdziale 11 (artykuły od 101 do 108). Najistotniejszy jest zapis z Art. 101. (UOODO) -

„Prezes Urzędu może nałożyć na podmiot obowiązany do przestrzegania przepisów rozporządzenia 2016/679, inny niż:

1) jednostka sektora finansów publicznych,

2) instytut badawczy,

3) Narodowy Bank Polski

– w drodze decyzji, administracyjną karę pieniężną na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679" (RODO).

Pod rządami UODO i RODO kara pieniężna w maksymalnej wysokości może wynieść nawet 20 000 000 Euro (art. 83 ust. 5 RODO). Jest więc o czym dyskutować, gdyż wysokość kar może być nie tylko dotkliwa dla podmiotu przetwarzającego ale wręcz spowodować upadłość nawet dużego przedsiębiorstwa.

Zgodnie ze stanowiskiem Urzędu Ochrony Danych Osobowych - kary pieniężne mają być nie tylko skuteczne i odstraszające, ale i proporcjonalne. Dlatego przy ich wymierzaniu Prezes UODO (PUODO) musi brać pod uwagę wiele różnych czynników.

„1. charakter, wagę i czas trwania naruszenia;

2. umyślny lub nieumyślny charakter naruszenia;

3. działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;

4. stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem wdrożonych środków technicznych i organizacyjnych;

5. wszelkie wcześniejsze naruszenia, zatem czy to było pierwsze naruszenie czy kolejne;

6. stopień współpracy z Prezesem UODO w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;

7. kategorie danych osobowych, których dotyczyło naruszenie;

8. sposób, w jaki Prezes UODO dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie (np. czy sam zgłosił „wyciek danych")

Wysokość kary

Prezes UODO bierze pod uwagę ww. czynniki zarówno wtedy, gdy decyduje o zasadności nałożenia administracyjnej kary pieniężnej, jak i wtedy, gdy określa jej wysokość. Przepisy przewidują górne limity wysokości kar. Prezes UODO nakłada karę pieniężną za naruszenie w wysokości:

- do 10 000 000 euro lub do 2% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego (zastosowanie ma kwota wyższa) za np.: nieprawidłowości w zakresie powierzenia przetwarzania danych; niewłaściwe prowadzenie rejestru czynności przetwarzania lub jego brak; czy niezgłoszenie naruszenia ochrony danych lub niezawiadomienie o naruszeniu osoby, której dane dotyczą;
- do 20 000 000 euro, a w przypadku przedsiębiorstwa - w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, np. za przetwarzanie danych osobowych niezgodnych z zasadami RODO, niedotrzymanie warunku wyrażenia zgody na przetwarzanie danych, niedotrzymanie warunków przetwarzania szczególnych kategorii danych osobowych (tj. np. danych o stanie zdrowia, wyznaniu, orientacji seksualnej), niedopełnienie obowiązku informacyjnego, czy prawa do sprostowania;
- do 100 000 złotych na jednostki sektora finansów publicznych, instytuty badawcze, czy Narodowy Bank Polski;
- do 10 000 złotych na państwowe i samorządowe instytucje kultury"[1].

Dodatkowo PUODO wskazuje na podstawę do ewentualnego wymierzenia kary za nieprzestrzeganie ochrony danych - art. 29 Grupy Roboczej ds. ochrony danych.

Z informacji dostępnych na stronie Urzędu Ochrony Danych Osobowych (UODO) wynika, że Prezes Urzędu wydał dotąd ponad 130 decyzji (na dzień 16.01.2020 r.) w części z nich nakładając kary na podmioty kontrolowane w tym kary finansowe.

[1] https://uodo.gov.pl/pl/138/1244

Warto zastanowić się, za co takie kary zostały nałożone, aby podjąć działania zapobiegawcze, jeśli ktoś jeszcze tego nie uczynił.

W tabeli poniżej przedstawiam aktywność własną Urzędu Ochrony Danych Osobowych oraz reagowanie na zgłoszenia obywateli, firm, instytucji odnośnie ewentualnych naruszeń w zakresie ochrony danych osobowych. Dane na podstawie strony internetowej UODO https://uodo.gov.pl/pl/p/decyzje

Decyzje Prezesa Urzędu Ochrony Danych Osobowych.	Rok 2018	Rok 2019
Decyzja Prezesa UODO stwierdzająca naruszenie m.in. zasady przetwarzania zgodnie z prawem i zasady poufności oraz nakazująca dostosowanie operacji przetwarzania do przepisów o ochronie danych osobowych.	0	4
Decyzja Prezesa UODO umarzająca postępowanie	6	27
Decyzja Prezesa UODO odmawiająca uwzględnienia skargi/wniosku	19	46
Decyzja Prezesa UODO dotycząca przetwarzania danych osobowych przez związek wyznaniowy	0	1
Decyzja Prezesa UODO utrzymująca w mocy zaskarżoną decyzję	1	3
Decyzja Prezesa UODO nakazująca usunięcie danych osobowych	0	3
Decyzja Prezesa UODO nakazująca ponowne zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych	1	0
Decyzja nakazująca dopełnienie obowiązku informacyjnego oraz nakładająca karę	1	5
Decyzja Prezesa UODO nakazująca zaprzestania przetwarzania danych osobowych	2	0
Decyzja Prezesa UODO nakazująca udostępnienie danych	0	5
Decyzja Prezesa UODO nakazująca ubezpieczycielowi ponowne zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych i wskazanie jej możliwych konsekwencji zdarzenia, a także powiadomienie jej o podjętych działaniach zaradczych i proponowanych środkach, które osoba ta może zastosować, by zminimalizować ewentualne negatywne skutki naruszenia.	11	1
Upomnienie	0	1

Źródło: opracowanie własne autora

Do najbardziej znanych decyzji PUODO należą te dotyczące firmy (M…... Sp. z o. o.) z siedzibą w Krakowie (Decyzja PUODO nr ZSPR.421.2.2019), czy Urząd Miasta w Aleksandrowie Kujawskim (Decyzja PUODO nr ZSPU.421.3.2019) – przyjrzyjmy się tym przypadkom.

Odnośnie firmy M……. – Prezes UODO w decyzji z września 2019 r. stwierdził naruszenie przez ww. firmę przepisów art. 5 ust. 1 lit. a oraz lit. f, art. 5 ust 2, art. 6 ust. 1, art. 7 ust. 1, art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 lit. b, lit. d, art. 32 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. i nałożył na tę firmę karę pieniężną w wysokości **2 830 410 PLN.**

Dlaczego tak wysoka kara i za jakie nieprawidłowości?

Szczegółowy opis przypadku zająłby zbyt wiele miejsca, a poza tym jest dostępny na stronie internetowej UODO (adres w przypisie nr 2). Dlatego pozwolę sobie przytoczyć jedynie najbardziej interesujące fragmenty.

Co ustalił UODO?

„Na podstawie zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Spółka, jako administrator, naruszyła przepisy o ochronie danych osobowych. Uchybienia te polegały na: naruszeniu przez Spółkę zasady poufności danych wyrażonej w art. 5 ust 1 lit. f „ … „ (RODO – przypis autora)", odzwierciedlonej w postaci obowiązków określonych w art. 24 ust 1, art. 25 ust. 1 oraz art. 32 ust. 1 lit. b oraz d, art. 32 ust. 2 rozporządzenia 2016/679 polegającym na niezapewnieniu bezpieczeństwa i poufności przetwarzanych danych osobowych co spowodowało, że dostęp do danych osobowych klientów Spółki uzyskały osoby nieuprawnione oraz na naruszeniu zasady legalności, rzetelności i rozliczalności wyrażonych w art. 5 ust 1 lit. a oraz art. 5 ust. 2 rozporządzenia 2016/679, uszczegółowionych w art. 7 ust. 1 oraz art. 6 ust. 1 rozporządzenia 2016/679, poprzez niewykazanie, że dane osobowe z wniosków ratalnych zbierane przed 25 maja 2018 r. były przetwarzane przez (……) na podstawie zgody osoby, której dane dotyczyły"[2].

Za najpoważniejsze uchybienia i nieprawidłowości uznano naruszenie przez Spółkę zasady poufności określonej w art. 5 ust 1 lit. f rozporządzenia 2016/679. Przemawiał za tym poważny charakter naruszenia oraz ilość osób jakich to dotyczyło (około dwóch milionów dwustu tysięcy użytkowników sklepów internetowych, których administratorem jest Spółka). Co istotne, jak podkreślił PUODO „w stosunku do ww. liczby osób w dalszym ciągu istnieje wysokie ryzyko niezgodnego z prawem posłużenia się ich danymi osobowymi, albowiem nieznany jest cel, dla którego osoba nieuprawniona podjęła działania zmierzające do uzyskania dostępu do tychże informacji" (źródło – przypis nr 2).

Decydując się na wysokość kary PUODO wyszedł z założenia, że administracyjna kara pieniężna spełni w tych konkretnych okolicznościach funkcję represyjną, ale i prewencyjną,

[2] Źródło: https://uodo.gov.pl/decyzje/ZSPR.421.2.2019

jako że sama Spółka, jak i inni administratorzy będą skutecznie zniechęceni do naruszania przepisów o ochrony danych osobowych w przyszłości.

Takie stwierdzenie w decyzji PUODO powinno dać do myślenie wszystkim administratorom danych, ponieważ i oni w razie udowodnienia im nieprawidłowości mogą stać się w przyszłości swego rodzaju ofiarami „prewencyjnego" działania UODO.

Kazus Aleksandrowa Kujawskiego.

Sprawę ukarania Urzędu Miasta w Aleksandrowie Kujawskim nazywam kazusem, ponieważ jest to pierwszy przypadek nałożenia kary finansowej na podmiot administracji samorządowej.

Sentencja decyzji PUODO.

„I. stwierdzając naruszenie przez Burmistrza Aleksandrowa Kujawskiego przepisów:

a) art. 5 ust. 1 lit. a) oraz f) w zw. z art. 5 ust. 2 ogólnego rozporządzenia o ochronie danych, tj. zasady zgodności z prawem i zasady poufności oraz art. 28 ust. 3 ogólnego rozporządzenia o ochronie danych osobowych poprzez udostępnianie danych osobowych na rzecz T. Sp. z o.o. z siedzibą w T. oraz na rzecz konsorcjum podmiotów: W. S.A. z siedzibą w G. oraz C. S.A. z siedzibą w K. bez podstawy prawnej, tj. bez uprzedniego zawarcia z ww. podmiotami umów powierzenia danych osobowych, o której mowa w art. 28 ust. 3 ogólnego rozporządzenia o ochronie danych, w związku z prowadzeniem strony internetowej Biuletynu Informacji Publicznej Urzędu Miejskiego w Aleksandrowie Kujawskim,

b) art. 5 ust. 1 lit. e) w zw. z art. 5 ust. 2, tj. zasady ograniczenia przechowywania, oraz art. 24 ogólnego rozporządzenia o ochronie danych poprzez brak odpowiednich polityk dotyczących przetwarzania danych osobowych w Biuletynie Informacji Publicznej Urzędu Miejskiego w Aleksandrowie Kujawskim pod kątem ich aktualności i celowości publikacji oraz określających terminy usunięcia danych osobowych,

c) art. 5 ust. 1 lit. f) w zw. z art. 5 ust. 2 ogólnego rozporządzenia o ochronie danych, tj. zasady integralności i poufności, zasady prawidłowości, oraz art. 24 ogólnego rozporządzenia o ochronie danych poprzez nieprzeprowadzenie analizy ryzyka związanego z korzystaniem przez Burmistrza Aleksandrowa Kujawskiego z kanału YouTube w celu transmisji nagrań z obrad Rady Miasta Aleksandrowa Kujawskiego,

d) art. 5 ust. 1 lit. f) w zw. z art. 5 ust. 2 ogólnego rozporządzenia o ochronie danych, tj. zasady integralności i poufności, oraz art. 32 ogólnego rozporządzenia o ochronie danych poprzez niewdrożenie odpowiednich środków technicznych i organizacyjnych mających na celu zabezpieczenie danych osób fizycznych w związku z przechowywaniem nagrań sesji Rady Miasta Aleksandrowa Kujawskiego wyłącznie na serwerach YouTube, bez wykonywania i przechowywania kopii zapasowych tych nagrań w zasobach własnych Urzędu Miejskiego w Aleksandrowie Kujawskim,

e) art. 5 ust. 2 ogólnego rozporządzenia o ochronie danych, tj. zasady rozliczalności, oraz art. 30 ust. 1 lit. d) oraz f) ogólnego rozporządzenia o ochronie danych poprzez niewskazanie w rejestrze czynności przetwarzania danych osobowych, dla czynności związanych z publikacją informacji na stronie Biuletynu Informacji Publicznej Urzędu Miasta w Aleksandrowie Kujawskim, wszystkich odbiorców danych oraz niewskazanie dla tych czynności przetwarzania planowanego terminu usunięcia danych w sposób zapewniający przetwarzanie danych zgodnie z zasadą ograniczonego przechowywania,

nakazuje Burmistrzowi Aleksandrowa Kujawskiego dostosowanie operacji przetwarzania danych osobowych do przepisów ogólnego rozporządzenia o ochronie danych, w terminie 60 dni od dnia, w którym niniejsza decyzja stanie się ostateczna, poprzez:

1) zaprzestanie udostępniania danych osobowych na rzecz T. Sp. z o.o. z siedzibą w T. oraz na rzecz konsorcjum podmiotów: W. S.A. z siedzibą w G. oraz C. S.A. z siedzibą w K., bez podstawy prawnej, tj. bez uprzedniego zawarcia umów powierzenia danych osobowych z ww. podmiotami, o której mowa w art. 28 ust. 3 ogólnego rozporządzenia o ochronie danych osobowych, w związku z prowadzeniem strony internetowej Biuletynu Informacji Publicznej Urzędu Miejskiego w Aleksandrowie Kujawskim,

2) wdrożenie polityk:

- określających okresy przetwarzania danych w Biuletynie Informacji Publicznej Urzędu Miejskiego w Aleksandrowie Kujawskim zgodne z przepisami prawa lub niezbędne do realizacji celów, dla których dane są przetwarzane,

- zapewniających przestrzeganie terminów usuwania danych,

3) przeprowadzenie analizy ryzyka w związku z publikacją nagrań sesji rady miejskiej i wdrożenie odpowiednich środków organizacyjnych i technicznych w związku z przetwarzaniem danych osobowych na kanale YouTube w związku z transmisją nagrań sesji rady miejskiej oraz przechowywaniem nagrań na serwerach YouTube,

4) wdrożenie odpowiednich środków organizacyjnych i technicznych mających na celu zabezpieczenie danych osób fizycznych pochodzących z nagrań sesji Rady Miasta Aleksandrowa Kujawskiego poprzez zapewnienie dostępności kopii zapasowych w zasobach własnych Urzędu Miejskiego w Aleksandrowie Kujawskim,

5) ujęcie w rejestrze czynności przetwarzania danych osobowych, dla czynności przetwarzania związanych z prowadzeniem Biuletynu Informacji Publicznej, informacji:

a) o wszystkich odbiorcach danych, którym dane zostały lub zostaną ujawnione, zgodnie z art. 30 ust. 1 lit. d) ogólnego rozporządzenia o ochronie danych,

b) o planowanych terminach usunięcia danych, zgodnie z art. 30 ust. 1 lit. f) ogólnego rozporządzenia o ochronie danych.

II. za naruszenie przepisów art. 5 ust. 1 lit. a), e) i f), art. 5 ust. 2, art. 28, art. 30 ust. 1 lit. d) i f) oraz art. 32 ogólnego rozporządzenia o ochronie danych nakłada na Burmistrza Aleksandrowa Kujawskiego karę pieniężną w kwocie **40.000 zł (słownie: czterdziestu tysięcy złotych i 00/100)"[3].**

Cały tekst decyzji dostępny jest na stronie UODO – należy jednak zauważyć, że do nałożenia kary na Urząd Miasta przyczyniło się kilka okoliczności ujawnionych przez UODO w treści decyzji, a są to takie okoliczności jak:

1. Czas trwania naruszeń,
2. Umyślny charakter naruszenia,
3. Wysoki stopień odpowiedzialności administratora,
4. **Brak współpracy administratora po wszczęciu postępowania,**

Należy domniemywać, że punkty 1. i 4., czyli uporczywe niestosowanie się do zaleceń kontrolujących oraz brak chęci współpracy ze strony Burmistrza Aleksandrowa Kujawskiego w głównej mierze przyczyniły się do nałożenia kary pieniężnej oraz do jej wysokości.

Uzasadnienie PUODO.

„Nakładając niniejszą decyzją administracyjną karę pieniężną za naruszenie przepisów o ochronie danych osobowych Prezes Urzędu Ochrony Danych Osobowych wziął pod uwagę oba aspekty: po pierwsze - **charakter represyjny**, Burmistrz naruszył przepisy ogólnego rozporządzenia o ochronie danych, po drugie - **charakter prewencyjny**, zarówno Burmistrz, jak i inni administratorzy, będą skutecznie zniechęceni do naruszania w przyszłości prawa ochrony danych osobowych, jednocześnie dokładając większej staranności przy realizacji swoich obowiązków wynikających z ogólnego rozporządzenia o ochronie danych"[4].

Jak widzimy z powyższego cytatu – Urząd Ochrony Danych Osobowych wydając decyzje w prowadzonych przez siebie sprawach – po raz kolejny akcentuje kwestie związane z represja i prewencją.

Podsumowanie.

Patrząc z punktu widzenia podmiotu kontrolowanego podejście oparte na prewencji może wyglądać na odpowiedzialność zbiorową, jednak z drugiej strony mamy prawa i wolności obywateli, którym należy się ochrona, zwłaszcza, że naruszenie przepisów może skutkować konkretnymi i dotkliwymi stratami. Straty te mogą być zarówno finansowe jak i psychiczne, moralne itp. Warto czasem postawić się w roli osoby, na której dane osobowe zaciągnięto wysoki kredyt lub ujawniono publicznie informacje o jej stanie zdrowia, preferencjach seksualnych lub inne, których nie życzymy sobie ujawniać.

[3] Źródło: https://uodo.gov.pl/decyzje/ZSPU.421.3.2019
[4] Źródło: https://uodo.gov.pl/decyzje/ZSPU.421.3.2019

Kwestie kar związanych z ochrona danych osobowych budzą i zapewne jeszcze długo będą budziły spore emocje i ożywione dyskusje. Swoim klientom i słuchaczom w uczelni porównuję opór przy wprowadzaniu przepisów z tym, dotyczącym uregulowań prawnych związanych chociażby z bezpieczeństwem i higieną pracy. Obecnie nie spotyka się powszechnie opinii, że szkolenia BHP, dokumentacja BHP czy ocena ryzyka na stanowisku pracy są czymś nadzwyczajnym. Podobnie społeczeństwo musi się przyzwyczaić do ochrony danych osobowych. Nawiasem mówiąc był na to czas, ponieważ przypominam, że ustawa o ochronie danych osobowych w Polsce została wprowadzona w 1997 roku. Dopiero wdrożenie bezpośrednio do stosowania w polskiej praktyce prawnej Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. o ochronie danych osobowych spowodowało, że instytucje, przedsiębiorcy, ale także i obywatele zainteresowali się tą dziadziną.

Kar finansowych w Polsce było na razie niewiele, ale jeśli już są nakładane, to najczęściej są surowe, ponieważ jak sam PUODO stwierdza maja być: „represyjne i prewencyjne".

Co zatem należy zrobić, aby nie narażać się na kary ze strony PUODO?

Jeśli przepisy wymagają od Ciebie wdrożenia ochrony danych osobowych, jeszcze tego nie uczyniłeś, to masz do realizacji szereg przedsięwzięć, do których należą w szczególności:

- przeprowadzenie audytu zgodności firmy z RODO,

- zapoznanie wszystkich pracowników przetwarzających dane osobowe łącznie z kierownictwem ze stanem prawnym dotyczącym tegoż zagadnienia,

- zatrudnienie Inspektora Ochrony Danych (IOD) - jeśli jest wymagany,

- opracowanie dokumentacji RODO (zdecydowanie odradzam kupowania „gotowych zestawów" z internetu). Nie ma czegoś takiego jak uniwersalna dokumentacja RODO. Tylko dokumentacja sporządzona na podstawie audytu i realiów firmy, instytucji (przez specjalistę w tej dziedzinie) – może być rzetelna i zgodna z wymogami prawa,

- upoważnienie pracowników do przetwarzania danych,

- powierzenie przetwarzania danych podmiotom zewnętrznym,

- wdrożenie rozwiązań we wszelkich dziedzinach funkcjonowania firmy, instytucji łącznie z papierowym, elektronicznym przetwarzaniem danych oraz w każdej innej postaci,

- ciągłe aktualizowanie rozwiązań systemowych oraz dokumentacji związanej z ochroną danych w związku ze zmianami prawnymi, organizacyjnymi, technologicznymi itp.

- cały szereg innych czynności wynikających z przepisów prawa oraz zaleceń dostępnych na stronie Urzędu Ochrony Danych Osobowych.

Jak wynika z przedstawionego wyżej przypadku Urzędu Miasta – rozsądnym rozwiązaniem jest współpraca z organem nadrzędnym kontrolnym czyli UODO oraz stosowanie się do jego zaleceń.

Instytut Bezpieczeństwa i Rozwoju Międzynarodowego SDirect24 na stronie internetowej https://www.sdirect24.org/informacjaniejawna oferuje szkolenia dla wszystkich, którzy zamierzają wdrażać RODO lub poszerzyć swoją wiedzę na ten temat. Przekazywany zakres materiału dostosowywany jest każdorazowo do specyfiki i profilu firmy, instytucji, urzędu itp.