OCHRONA DANYCH OSOBOWYCH OD 1 STYCZNIA 2015

Poradnik przetwarzania danych osobowych dla przedsiębiorstw oraz innych jednostek organizacyjnych

RBDO

REJESTRACJA I BEZPIECZEŃSTWO DANYCH OSOBOWYCH

NAJWAŻNIEJSZE OBOWIĄZKI PRZETWARZANIA DANYCH OSOBOWYCH

- Każde przedsiębiorstwo lub inna jednostka organizacyjna zatrudniająca choćby 1 pracownika lub posiadająca w jakiejkolwiek formie dane Klientów będącymi osobami fizycznymi, przetwarza dane osobowe w rozumieniu ustawy o ochronie danych osobowych.

- Sklepy internetowe, biura rachunkowe, hotele, spółdzielnie, urzędy, stowarzyszenia, placówki edukacyjne, medyczne i inne podmioty przetwarzają dane osobowe. Podmioty przetwarzające dane osobowe swoich Klientów, podlegają ustawie o ochronie danych osobowych.

- Podmiot przetwarzający dane osobowe musi posiadać odpowiednią dokumentację, w tym szczególnie dokument Polityki Bezpieczeństwa, Instrukcję Zarządzania Systemem Informatycznym oraz Ewidencję osób upoważnionych do przetwarzania danych osobowych.

KARY ZA UCHYBIENIA ZWIĄZANE Z OCHRONA DANYCH OSOBOWYCH

Od dnia 7 marca 2011 r. zgodnie ze znowelizowanym art. 12 pkt 3 ustawy o ochronie danych osobowych, GIODO może nakładać na podmioty, które nie wykonują jego decyzji administracyjnych (np. decyzji nakazującej usunięcie wybranych naruszeń), grzywny w celu przymuszenia.

Grzywny egzekwowane są w trybie ustawy o postępowaniu egzekucyjnym w administracji. Zgodnie z art. 121 ustawy o postępowaniu egzekucyjnym w administracji, wysokość grzywny wynosi:

- dla osób prawnych do 50 000 zł za każde uchybienie, ale nie więcej niż 200 tys. zł w jednym postępowaniu egzekucyjnym

- dla osób fizycznych do 10 000 zł za każde uchybienie, ale nie więcej niż 50 tys. zł w jednym postępowaniu egzekucyjnym

Oprócz powyższych sankcji możliwych do nałożenia w trybie administracyjnym, przetwarzanie danych osobowych poza trybem określonym w ustawie jako przestępstwo jest zagrożone karą nawet do 2 lat pozbawienia wolności, zgodnie z art. 49 ust. 1.

ZMIANY PRZEPISÓW OD 1 STYCZNIA 2015 ROKU

Zgodnie w nowymi przepisami firmy i jednostki organizacyjne przetwarzające zbiory podlegające zgłoszeniu do GIODO (np. dane Klientów, rejestry korespondencji) będą musiały wybrać wariant wdrożenia systemu ochrony danych z funkcją Administratora Bezpieczeństwa Informacji lub rejestrując zbiory w GIODO. Możliwe są zatem następujące warianty:

1. Pełnienie funkcji nadzorcy ochrony danych przez administratora danych (właściciela, Zarząd, Dyrekcję) z wdrożeniem dokumentacji i rejestracją zbiorów do GIODO, albo

2. Wyznaczenie i zgłoszenie do rejestru – Administratora Bezpieczeństwa Informacji (ABI), który będzie czuwał nad dokumentacją i zbiorami wewnątrz podmiotu.

UWAGA! Rejestracja zbiorów danych podlegających zgłoszeniu do GIODO pozwoli na uniknięcie wyznaczenia Administratora Bezpieczeństwa Informacji (ABI) w podmiocie – co wiąże się z dodatkowymi obowiązkami i sprawozdaniami ABI względem GIODO – jest to bardzo korzystne rozwiązanie.

Rekomendujemy jak najszybsze wdrożenie dokumentacji z instrukcją zgłoszenia zbioru do GIODO i wsparciem prawnym, niniejsza oferta jest dostępna ***tutaj >***

SPIS TREŚCI:

I. Czym są "dane osobowe"

Zgodnie z art. 6 ust. 1 ustawy o ochronie danych osobowych, za dane osobowe uważa się: "wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej". Sformułowanie to oznacza, iż za dane osobowe uważa się w szczególności dane osobowe pracowników – co znajduje oparcie w art. 22 [1] § 5 kodeksu pracy stanowiącym wprost, że danych pracowników zatrudnianych przez pracodawcę „stosuje się przepisy o ochronie danych osobowych".

Co więcej, tezę o zakwalifikowaniu danych pracowników, jako danych osobowych w rozumieniu ustawy potwierdza brzmienie art. 43 ust. 3 pkt 4 ustawy o ochronie danych osobowych, stanowiącego o zwolnieniu z obowiązku rejestracji zbioru danych przetwarzanych w związku z zatrudnieniem świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się - skoro zatem ustawa w wyżej wspomnianym przepisie uznaje dane przetwarzane w związku z zatrudnieniem za zbiór danych, to, zgodnie z art. 7 pkt 1 ustawy który definiuje pojęcie zbioru danych jako „zestawu danych o charakterze osobowym", należy uznać dane zatrudnianych pracowników za dane osobowe w rozumieniu ustawy o ochronie danych osobowych, a w konsekwencji, poddanych wymogom związanym z prowadzeniem dokumentacji, o jakiej mowa w rozdziale 5 ustawy o ochronie danych osobowych, przez co należy rozumieć w szczególności dokumentację wymaganą przez rozporządzenie, o którym mowa w art. 39a ustawy o ochronie danych osobowych.

Również dane klientów – nawet jeżeli ich zakres ogranicza się do numerów telefonów należy uznać za dane osobowe, interpretację taką potwierdzają: GIODO w decyzji DIS-DEC-42/1511, oraz Wojewódzki Sąd Administracyjny w Warszawie w wyroku II SA/Wa 1598/09 gdzie przyjęto pogląd, iż pomimo faktu, że informacje o numerze telefonu nie określają bezpośrednio tożsamości osoby, to jednak dają możliwość określenia tożsamości tych osób np. poprzez bezpośredni kontakt z osobą, która jest jego posiadaczem. Opowiedziano się zatem w sposób zdecydowany za zakwalifikowaniem tego typu informacji jako danych osobowych w rozumieniu ustawy. Powyższe uwagi zachowują aktualność również w odniesieniu do adresów e-mail, co zostało wprost potwierdzone w stanowisku rzecznika prasowego GIODO z dnia 7 maja 2010 r. (http://www.giodo.gov.pl/330/id_art/3529/j/pl/).

I. Czym są "dane osobowe"

Nie podlegają natomiast regulacjom przewidzianym w ustawie o ochronie danych osobowych dane, przetwarzane przez osoby fizyczne, które przetwarzają je „wyłącznie w celach osobistych lub domowych", o czym stanowi wprost art. 3a pkt 1.

Natomiast, jeżeli dane osobowe przetwarzane są przez osoby fizyczne, prawne lub jednostki organizacyjne niebędące osobami prawnymi, które przetwarzają je w związku z działalnością zarobkową lub zawodową – ustawa będzie miała do nich zastosowanie, co wynika wprost z art. 3 ust. 2 pkt 2 wyżej wspominanej ustawy.

Należy również zwrócić uwagę na odrębną kategorię danych osobowych, ujętą w art. 27 ustawy o ochronie danych osobowych, a mianowicie tzw. „danych wrażliwych". Zgodnie z przytoczonym powyżej przepisem, dane obejmujące „pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń postępowaniu sądowym lub administracyjnym" można przetwarzać wyłącznie, gdy zrealizowana jest określona co z przesłanek ujęta w art. 27 ust. 2 pkt 1-10, w szczególności zalicza się do nich zgoda osoby której dane są przetwarzane wyrażona na piśmie.

II. Zmiany w ustawie o ochronie danych osobowych od 1 stycznia 2015

Dnia 7 listopada 2014 do podpisu Prezydenta została przekazana ustawa o ułatwieniu wykonywania działalności gospodarczej, która weszła w życie od dnia 1 stycznia 2015 roku. W art. 9 tej ustawy znajdują się przepisy nowelizujące ustawę o ochronie danych osobowych. Na nowe przepisy można patrzeć z dwóch stron – w zależności od przyjętego wariantu postępowania dla konkretnego podmiotu może to być albo zniesienie obowiązku zgłaszania zbioru do GIODO, albo zniesienie obowiązku wyznaczenia ABI.

Nowelizacja znosi w aktualny dziś obowiązek wyznaczania ABI (którego w myśl poprzednio obowiązujących przepisów nie musieli wyznaczać jedynie jednoosobowi administratorzy danych, czyli tacy, którzy osobiście mogą pełnić funkcję ABI np. w przypadku jednoosobowej działalności gospodarczej). W przypadku np. spółki z ograniczoną odpowiedzialnością, przetwarzającej np. dane osobowe klientów w myśl starych przepisów zarząd miał obowiązek wyznaczenia ABI oraz zgłoszenia zbioru do GIODO (chyba że jest zwolniony z obowiązku zgłaszania na podstawie art. 43 ust. 1 uodo).

Nowelizacją dokonano uchylenia art. 36 ust. 3 który stwierdzał: Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności. Dodano w zamian art.. 36a ust. 1 ustalający że: *"Administrator danych może powołać administratora bezpieczeństwa informacji"*.

W myśl nowych przepisów administrator danych będzie miał obowiązek zgłoszenia zbioru do GIODO, chyba że wyznaczy ABI, zgłosi go do rejestru ABI prowadzonego przez GIODO oraz będzie zapewniał ABI możliwość realizacji swoich czynności z zapewnieniem odrębności organizacyjnej.

Nowe przepisy utrzymują obowiązek prowadzenia dokumentacji przetwarzania danych (Polityka Bezpieczeństwa, Instrukcja Zarządzania Systemem Informatycznym itd.).

II. Zmiany w ustawie o ochronie danych osobowych od 1 stycznia 2015

Warto dobrze zastanowić się nad wyborem wariantu odpowiedniego w konkretnym przypadku – rejestracja zbioru danych w GIODO, w przypadku gdy funkcję związane z ochroną danych będzie osobiście sprawował administrator danych (kierownik jednostki organizacyjnej – np. prezes zarządu), będzie co do zasady generowała znacznie mniej biurokratycznych obowiązków niż wyznaczenie ABI wpisanego do rejestru.

Zmiany od 1 stycznia 2015 będą polegały w szczególności na:

1. Zniesieniu obowiązku wyznaczania ABI, jeśli funkcję tą będzie osobiście sprawował Administrator Danych (kierownik jednostki organizacyjnej np., prezes zarządu, dyrektor placówki)

2. Zniesieniu obowiązku zgłaszania zbiorów danych dla tych administratorów danych, którzy wyznaczą i zarejestrują ABI w GIODO oraz dla tych, którzy przetwarzają zbiory danych osobowych wyłącznie w formie papierowej (chyba że przetwarzają „dane wrażliwe").

3. Prowadzeniu przez GIODO rejestru ABI.

4. Prowadzeniu przez ABI jawnych rejestrów zbiorów danych osobowych swoich administratorów danych, które nie są zwolnione z obowiązku zgłaszania do GIODO na podstawie art. 43 ust. 1 ustawy o ochronie danych osobowych.

5. Obowiązku sporządzania przez ABI cyklicznych sprawozdań, z których będzie on musiał sporządzać raporty dla ADO. Raporty ze sprawozdań dokonywanych przez ABI, będą musiały zawierać informacje o najdrobniejszych uchybieniach.

II. Zmiany w ustawie o ochronie danych osobowych od 1 stycznia 2015

Jaki wariant spowoduje najmniejsze obciążenie administracyjne?

Paradoksalnie – największym „ułatwieniem" jakie daje nowelizowana wersja ustawy o ochronie danych osobowych jest możliwość pozwalająca na uniknięcie „dobrodziejstw" płynących z nowelizacji, czyli nie wyznaczanie ABI i zgłaszanie przetwarzanych zbiorów danych zwykłym trybem – eliminuje to takie obowiązki jak:

1. Zgłaszanie powoływania i odwoływania ABI do GIODO.
2. Obowiązek sporządzania przez ABI szczegółowych raportów z przeprowadzanych sprawozdań wedle zasad ustalonych w ustawie i rozporządzeniu, co może w niektórych przypadkach stanowić biurokratyczną przeszkodę w funkcjonowaniu firmy.
3. Obowiązek prowadzenia wewnętrznego jawnego rejestru przetwarzanych zbiorów danych osobowych.
4. W samej dokumentacji wewnętrznej (Polityka Bezpieczeństwa itd.) nie przewidziano zmian. Dla zbiorów, które już zostały zgłoszone do GIODO na ten moment nic się nie zmienia – nie zmienia się bowiem treść rozporządzenia do art. 39a ustawy o ochronie danych osobowych z 2004 roku.

UWAGA! Rejestracja zbiorów danych podlegających zgłoszeniu do GIODO pozwoli na uniknięcie wyznaczenia Administratora Bezpieczeństwa Informacji (ABI) w podmiocie – co wiąże się z dodatkowymi obowiązkami i sprawozdaniami ABI względem GIODO – jest to bardzo korzystne rozwiązanie.

Rekomendujemy jak najszybsze wdrożenie dokumentacji z instrukcją zgłoszenia zbioru do GIODO i wsparciem prawnym, niniejsza oferta jest dostępna tutaj >

II.Zmiany w ustawie o ochronie danych osobowych od 1 stycznia 2015

Jak zatem optymalnie spełnić obowiązki?

Po pierwsze wdrożyć dokumentację ochrony danych osobowych. Każda firma lub jednostka organizacyjna bezwzględnie musi posiadać dokumentację przetwarzania danych osobowych, zgodną z rozporządzeniem do art. 39a ustawy, w tym szczególnie dokument polityki bezpieczeństwa, instrukcje zarządzania systemem informatycznym, wykazy ewidencyjne czy umowy powierzenia przetwarzania danych osobowych.

Brak dokumentacji może łączyć się z karami grzywien sięgających do 10.000 dla os. fizycznych oraz do 50.000 zł dla os. prawnych za każde uchybienie w związku z niewykonaniem decyzji administracyjnych.

JAK SPEŁNIĆ OBOWIĄZKI?

W celu spełnienia najważniejszego obowiązku wdrożenia dokumentacji warto skorzystać z kompletnej ***dokumentacji przetwarzania danych RBDO >>***
Następnie do wyboru: Rejestracja zbiorów do GIODO lub wyznaczenie ABI i jego imienne zgłoszenie do rejestru GIODO.

Jeśli podmiot wdrożył już dokumentację, na spełnienie reszty obowiązków od 1 stycznia 2015 można wybrać, albo zgłoszenie zbiorów danych podlegających pod rejestrację do GIODO (np. zbiory Klientów, newslettery, rejestry korespondencji, monitoring) albo wyznaczyć Administratora Bezpieczeństwa Informacji.

W przypadku rejestracji zbiorów danych do GIODO, można skorzystać z ***dokumentacji przetwarzania danch osobowych z instrukcją zgłoszenia zbioru do GIODO i wsparciem prawnym >>***

III.Stanowisko Administratora Bezpieczeństwa Informacji - ABI

Co zmiany oznaczają w praktyce?

Warto podkreślić, że zgłoszenie ABI do rejestru administratorów bezpieczeństwa informacji prowadzonego od 1 stycznia 2015 roku przez GIODO, oznacza brak konieczności rejestracji zbiorów do GIODO (chyba, ze przetwarzane są tzw. dane wrażliwe, czyli dane, o których mowa w art. 27 ustawy o ochronie danych osobowych). Administrator danych (kierownik jednostki organizacyjnej), który wyznaczy ABI nie będzie miał obowiązku, aby zgłaszać zbiory do rejestracji w GIODO.

Jednak ABI będzie miał obowiązek prowadzenia jawnego rejestru zbiorów danych wg. zasad ustalonych w rozporządzeniu w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych osobowych oraz prowadzenia cyklicznych sprawdzeń z których będzie musiał sporządzać raporty zawierające informacje o wszelkich stwierdzonych uchybieniach. Szczegółowe zasady przeprowadzania sprawdzeń przez ABI zawarte są w rozporządzeniu w sprawie trybu i sposobu realizacji zadań przez administratora bezpieczeństwa informacji.

Zniesienie obowiązku rejestracji zbiorów danych jak dotychczas do GIODO, w związku ze zgłoszeniem Administratora Bezpieczeństwa informacji nie będzie dotyczyć zbiorów danych tzw. wrażliwych (określonych w art. 27 uodo, czyli np. stan zdrowia, nałogi, poglądy polityczne itp.), chyba że wynika to z brzmienia art. 43 ust. 1

Podmiot ma zatem wybór – albo wyznacza Administratora Bezpieczeństwa Informacji albo zgłasza zbiory danych do GIODO.

Jeśli firma zdecyduje się na wyznaczenia ABI, warto zapewnić niniejszej osobie odpowiednie wsparcie, np. poprzez kompleksowe wdrożenie systemu ochrony danych oraz właściwe szkolenie z opieką prawną.

Z tego względu rekomendujemy usługę ***kompleksowego wdrożenia ze szkoleniem ABI z 12 miesięcznym wsparciem prawnym >***

Usługa zapewnia pogłębione szkolenie wyznaczonej osoby na ABI podczas kilkutygodniowego wdrożenie systemu ochrony danych oraz zapewnienie 12 miesięcznego wsparcia prawnego dla ABI przez wyspecjalizowanego prawnika.

III. Stanowisko Administratora Bezpieczeństwa Informacji - ABI

Powołany ABI będzie miał obowiązek raportowania do GIODO wszelkich uchybień Znowelizowana ustawa przede wszystkim wprowadza rozszerzenie kompetencji GIODO m. in. do prowadzenia rejestru Administratorów Bezpieczeństwa Informacji (ABI). To nie wszystko, GIODO, posiada od możliwość zwrócenia się do ABI w celu zlecenie kontroli zastępczej w imieniu GIODO wskazując zakres i termin takiej kontroli. W rzeczywistości zatem ABI będzie pierwszym organem kontrolnym w przypadku wszelkich incydentów związanych z ochroną danych.

Dotychczas kontroli dokonywał wyłącznie GIODO lub w zakresie pracowników PIP (który jedynie zgłaszał te uchybienia do GIODO). Nowe przepisy zobowiązuję do przeprowadzenie kontroli wewnętrznego ABI, który następnie będzie miał obowiązek wysłać wyniki kontroli do GIODO. Nie zmienia to faktu, że GIODO dalej będzie miał możliwość bezpośredniej kontroli administratora danych poprzez wysłanie inspekcji.

Kto może zostać ABI ?

Warunki, jakie spełniać musi osoba pełniąca funkcję ABI od 1 stycznia 2014 roku zostały określone w art. 36a ust. 5 znowelizowanej ustawy o ochronie danych osobowych - w rozumieniu tego przepisu administratorem bezpieczeństwa informacji może być osoba, która:

1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;
3) nie była karana za umyślne przestępstwo.

Na ABI będą spoczywały przede wszystkim obowiązki:

- Prowadzenia jawnego rejestru zbiorów danych osobowych przetwarzanych w firmie według wzoru określonego przez rozporządzenie.
- Wykonywania przez administratora bezpieczeństwa informacji sprawdzenia zgodności
- Przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Sprawdzenia będą wykonywane na podstawie opracowanego przez ABI i zatwierdzonego przez ADO rocznego programu sprawdzeń, na żądanie GIODO, lub doraźnie po powzięciu informacji o zaistniałych incydentach
- Opracowania sprawozdań dla administratora danych z dokonywanych działań
- Nadzorowania przez administratora bezpieczeństwa informacji opracowywania i aktualizowania dokumentacji wewnętrznej (Polityka Bezpieczeństwa, Instrukcja Zarządzania Systemem Informatycznym itd.)

IV. Jakie obowiązki wiążą się z przetwarzaniem danych osobowych?

Obowiązkiem, jaki przede wszystkim musi spełnić podmiot przetwarzający dane osobowe (inaczej mówiąc Administrator Danych Osobowych), jest legitymowanie się odpowiednią podstawą prawną, uzasadniającą sam fakt przetwarzania przez ten podmiot określonych danych osobowych. Podstawową i najczęściej funkcjonującą podstawą jest prawidłowo uzyskana zgoda na przetwarzanie danych konkretnej osoby przez konkretny podmiot, w określonym celu (lub celach) – zgodnie z art. 23 ust. 1 pkt 1 oraz art. 7 pkt 5 ustawy o ochronie danych osobowych, należy przy tym pamiętać, iż zgodnie z drugim z wymienionych wyżej przepisów, „zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści", podkreślenia wymaga również fakt, iż zgoda może być odwołana w każdym czasie.

Innymi ujętymi w art. 23 ust. 1 podstawami przetwarzania danych osobowych są: konieczność zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 23 ust. 1 pkt 2), konieczność realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą (art. 23 ust. 1 pkt 3), konieczność wykonania określonych prawem zadań realizowanych dla dobra publicznego, (art. 23 ust. 1 pkt 4), konieczność wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, pod warunkiem, że przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą (art. 23 ust. 1 pkt 5).

Jednym z obowiązków związanym z przetwarzaniem danych osobowych jest posiadanie zgody na ich przetwarzanie. Uwaga! Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

Przetwarzanie danych Klientów w celu sprzedaży nie wymaga zgody, ponieważ przetwarzane są w celu realizacji umowy, art. 23 ust. 1 pkt 3.

Jako „prawnie usprawiedliwiony cel", który może stanowić podstawę przetwarzania danych – ustawa uznaje „marketing własnych produktów lub usług".

Administrator Danych Osobowych jest zobowiązany do poinformowania danych osób, których dane przetwarza, m.in. o siedzibie, pełnej nazwie oraz prawie dostępu do treści oraz prawie do ich poprawiania

IV. Jakie obowiązki wiążą się z przetwarzaniem danych osobowych?

Jeżeli chodzi o podstawę przetwarzania opartą na „konieczności wypełnienia prawnie usprawiedliwionych celów" - istotną rzeczą jest fakt, że w art. 23 ust. 4 ustawy o ochronie danych osobowych znajdują się dwa przykłady wskazujące na to, w jaki sposób interpretować można „prawnie usprawiedliwiony cel" – ustawa rozumie przez to w szczególności „marketing bezpośredni własnych produktów lub usług administratora danych" oraz „dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej" – jest to wyliczenie przykładowe, na co wskazuje posłużenie się przed nim sformułowaniem „w szczególności" – oznacza to że nie jest wykluczone inne rozumienie zwrotu „prawnie usprawiedliwiony cel", jednak dopuszczalność zakwalifikowania innych sytuacji jako „prawnie usprawiedliwiony cel" będzie w każdym przypadku oceniana w odniesieniu do indywidualnych okoliczności towarzyszących określonej sytuacji.

Art. 24 przewiduje wymagania w stosunku do Administratora Danych Osobowych (może nim być przedsiębiorca przetwarzający dane klientów, kontrahentów, pracowników lub współpracowników) w sytuacji, kiedy uzyskuje on dane osobowe od osoby, której one dotyczą – jest to standardowa, najczęściej występująca w praktyce sytuacja, a obowiązki przewidziane w wyżej wymienionym przepisie mają charakter informacyjny – nie należy ich jednak lekceważyć, ponieważ niezastosowanie się do ich dyspozycji stanowi przestępstwo z art. 54 ustawy o ochronie danych zagrożone karą grzywny, ograniczenia wolności, lub pozbawienia wolności do roku.

Do obowiązków informacyjnych przewidzianych w art. 24 ustawy o ochronie danych osobowych należą: poinformowanie o adresie swojej siedziby i pełnej nazwie, a w przypadku, gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku (art. 24 ust. 1 pkt 1), poinformowanie o celu zbierania danych, a w szczególności o znanych Administratorowi Danych Osobowych " w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych (art. 24 ust. 1 pkt 2), poinformowanie o prawie dostępu do treści swoich danych oraz ich poprawiania (art. 24 ust. 1 pkt 3), poinformowanie o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej (art. 24 ust. 1 pkt 4).

IV. Jakie obowiązki wiążą się z przetwarzaniem danych osobowych?

Art. 27 ustawy o ochronie danych osobowych odnosi się do sytuacji, w której przetwarzane są tzw. „dane wrażliwe", przez co należy rozumieć: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych 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. W przypadku, gdy wyżej wymienione dane nie są przetwarzane, nie istnieje obowiązek stosowania się do postanowień art. 27.

Art. 27 ustawy o ochronie danych osobowych odnosi się do sytuacji, w której przetwarzane są tzw. „dane wrażliwe", przez co należy rozumieć: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych 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. W przypadku, gdy wyżej wymienione dane nie są przetwarzane, nie istnieje obowiązek stosowania się do postanowień art. 27.

Art. 31 ustawy o ochronie danych osobowych zawiera bardzo istotną z praktycznego punktu widzenia regulację dotyczącą umowy powierzenia przetwarzania danych osobowych. Regulacja ujęta w tym przepisie ma o tyle istotne znaczenie, że może dotyczyć wielu codziennych sytuacji (np. zlecenie usług księgowych biuru rachunkowemu), a odpowiedzialność za zgodne z prawem powierzenie danych spoczywać będzie na podmiocie będącym administratorem danych – zatem, w przypadku inspekcji we współpracującym z określonym przedsiębiorstwem biurem rachunkowym odpowiedzialność tak karna, jak i administracyjna spoczywać będzie na podmiocie powierzającym – co jednak nie wyklucza pociągnięcia przez powierzającego do odpowiedzialności na podstawie zawartej umowy podmiotu, któremu powierzono przetwarzanie danych osobowych

IV. Jakie obowiązki wiążą się z przetwarzaniem danych osobowych?

Art. 31 określa minimalne wymagania, jakie musi spełniać umowa powierzenia przetwarzania danych osobowych, umowa musi mieć formę pisemną oraz określać zakres i cel przetwarzania a podmiot przetwarzający, któremu powierzono dane nie może wykraczać poza oznaczony w umowie zakres oraz cel. Kolejną istotną rzeczą związaną z umową powierzenia przetwarzania danych osobowych jest fakt, że podmiot, któremu na mocy takiej umowy powierza się przetwarzanie danych osobowych musi mieć wdrożony system przetwarzania danych osobowych zgodny z art. 36 - 39a (w tym z rozporządzeniem do art. 39a wymagającym wdrożenia Polityki Bezpieczeństwa, oraz Instrukcji Zarządzania Systemem Informatycznym, jeżeli dane są przetwarzane w systemie informatycznym). Pewnym ułatwieniem, jeżeli chodzi o powierzenie przetwarzania danych jest fakt, że nie istnieje obowiązek informowania osób, których dane dotyczą, o fakcie przekazania danych – podmiot przetwarzający dane na podstawie takiej umowy nie jest bowiem odbiorcą danych w rozumieniu art. 7 pkt 6 lit. d ustawy o ochronie danych osobowych.

Rozdział 4 ustawy o ochronie danych osobowych, w art. 32 - 35 reguluje uprawnienia osób, których dane są przetwarzane, osoby takie mają prawo do kontroli przetwarzanych danych na ich temat. Co jest warte podkreślenia, w art. 32 ust. 1 pkt 8 zostało przyznane osobom, których na są przetwarzane prawo do wniesienia sprzeciwu, a nie zastosowanie się do prawidłowo wniesionego sprzeciwu i dalsze przetwarzanie danych stanowi przestępstwo określone w art. 49 zagrożone karą grzywny, ograniczenia wolności, albo pozbawienia wolności do lat 2.

Przychodnie zdrowia, gabinety stomatologiczne, szpitale, jako podmioty przetwarzające dane o stanie zdrowia swoich Pacjentów, są zobowiązane do szczególnie starannego przestrzegania przepisów ustawy o ochronie danych osobowych.

Umowa powierzenia danych osobowych może dotyczyć wielu codziennych sytuacji (np. zlecenie usług księgowych biuru rachunkowemu, hosting).

Każdy Administrator Danych Osobowych musi prowadzić dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne, które służyć mają ochronie danych osobowych, co zostało określone w rozporządzeniu do art. 39a ustawy, w szczególności: „Politykę Bezpieczeństwa", „Instrukcję Zarządzania Systemem Informatycznym" (jeżeli dane są wprowadzane do systemu informatycznego) oraz „Ewidencje osób upoważnionych do przetwarzania danych osobowych".

V.Czy zawsze potrzebna jest zgoda na przetwarzanie danych?

To, czy w danym przypadku konieczne będzie uzyskanie zgody osoby, której dane są przetwarzane zależy od dwóch głównych czynników – po pierwsze od tego, jakie dane będą przetwarzane, a po drugie – w jakim celu.

Np. pracodawca przetwarzający dane osobowe swoich pracowników nie potrzebuje odrębnej zgody na przetwarzanie ich danych – gdyż po pierwsze jest uprawniony do ich przetwarzania na podstawie 22 [1] § 5 kodeksu pracy, po drugie niezależnie od wyżej przywołanego przepisu kodeksu pracy, art. 23 ust. 1 pkt 3 ustawy o ochronie danych osobowych uznaje za wystarczającą podstawę do przetwarzania danych (co nie wymaga uzyskania dodatkowej zgody) „konieczność realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą".

Należy jednak pamiętać, że pracodawca, który zamierza przetwarzać dane osobowe pracowników lub kandydatów do pracy w oparciu o wyżej przytoczone przepisy – jest zobowiązany do wykazania, że przetwarzane prze niego dane są konieczne do realizacji umowy lub podjęcia działań mających zakończyć się jej zawarciem. Podobnie rzecz wygląda z przetwarzaniem danych klientów, którzy skorzystali z usługi np. sklepu który w konsekwencji stał się administratorem tych danych – zgoda nie jest konieczna, gdy przetwarzanie tych danych jest niezbędne do realizacji zawartej umowy.

Jednak gdy w wyżej wymienionym przypadku planowane jest np. wysyłanie mailingu z informacjami w nowościach o asortymencie sklepu, konieczne będzie uzyskanie dodatkowo zgody na otrzymywanie informacji handlowych drogą elektroniczną.

Dane pracowników nie wymagają zgody na przetwarzanie – chyba że pracodawca zamierza przetwarzać te dane w szerszym zakresie niż jest to wymagane do realizacji umowy stanowiącej podstawę zatrudnienia.

VI. Kiedy należy zgłosić zbiór do rejestracji?

Rozdział 6 ustawy o ochronie danych osobowych, w art. 40-46a, odnosi się do obowiązku rejestracji zbiorów danych osobowych, oprócz formalnych wymagań związanych ze zgłoszeniem zbioru do rejestracji istotne postanowienia zawiera art. 43 ust. 1 pkt 1-11 gdzie zawarto katalog wyłączeń spod obowiązku zgłoszenia zbioru danych osobowych do rejestracji. Na uwagę z praktycznego punktu widzenia zasługuje art. 43 ust.1 pkt 4, na podstawie którego zbiór danych osobowych osób zatrudnionych jest wyłączony spod obowiązku zgłoszenia do rejestracji.

Należy jednak mieć na uwadze, że zwolnienie z obowiązku zgłoszenia do rejestracji nie jest równoznaczne ze zwolnieniem od obowiązku zabezpieczenia danych osobowych, zgodnie z postanowieniami rozdziału 5 ustawy o ochronie danych osobowych – zatem nawet w przypadku, gdy jedynymi danymi osobowymi przetwarzanymi w przedsiębiorstwie są dane wyłączone spod obowiązku rejestracji (np. dane osobowe pracowników) będzie zachodziła konieczność wdrożenia dokumentacji, o jakiej mowa w rozporządzeniu wykonawczym do art. 39a ustawy o ochronie danych osobowych (Polityka Bezpieczeństwa oraz Instrukcja Zarządzania Systemem Informatycznym w przypadku, gdy dane przetwarzane są w systemie informatycznym).

Podobnie w przypadku szkół zwolnienie obejmuje zbiór danych uczniów, a w przypadku stowarzyszeń – dane członków w nim zrzeszonych.

Zbiory podlegające obowiązkowi zgłoszenia do rejestru GIODO:

- zbiory danych Klientów (zawierające dowolne dane teleadresowe)
- dane korespondencyjne Klientów
- rejestry korespondencji (szkół, firm, jednostek organizacyjnych)
- bazy Newsletter
- bazy konkursowe
- rejestry wysyłkowe towarów
- rejestry reklamacji
- beneficjenci działań stowarzyszenia/klubu
- zbiory danych darczyńców
- rejestry uczniów, którzy wypełniają obowiązek szkolny poza daną szkołą
- uczestnicy konkursów międzyszkolnych
- zbiór danych osobowych czytelników czytelni
- listy akcjonariuszy (jeśli są tam osoby fizyczne)
- księgi gości, księgi meldunkowe
- rezerwacje imienne usług
- wszelkie inne dane osobowe, które nie podlegają zwolnieniu

VI.Kiedy należy zgłosić zbiór do rejestracji?

Art. 43 ust. 1 ustawy o ochronie danych osobowych
(zawiera katalog danych wyłączonych spod obowiązku rejestracji)

Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych:

1) *zawierających informacje niejawne,*
1a) które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności,

2) *przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym, 2a) przetwarzanych przez Generalnego Inspektora Informacji Finansowej, 2b) przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym; 2c) przetwarzanych przez właściwie organy na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej,*

3) *dotyczących osób należących do kościoła lub innego związku wyznaniowego,* o *uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub* związku wyznaniowego.

4) *przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się,*

5) *dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta,*

6) *tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu,Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego,*

7) *dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnymdo wykonania tymczasowego aresztowania lub kary pozbawienia wolności,*

8) *przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej, przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu*

9) *powszechnie dostępnych,*

10) *ukończenia szkoły wyższej lub stopnia naukowego,*

11) *przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.*

VII. Sankcje administracyjne (grzywny nakładane przez GIODO)

art. 121 ustawy o postępowaniu egzekucyjnym w administracji

§ 1. Grzywna w celu przymuszenia może być nakładana kilkakrotnie w tej samej lub wyższej kwocie, z zastrzeżeniem § 4. § 2. Z zastrzeżeniem § 5 każdorazowo nałożona grzywna nie może przekraczać kwoty 10 000 zł, a w stosunku do osób prawnych i jednostek organizacyjnych nie posiadających osobowości prawnej kwoty 50 000 zł.

§ 3. Grzywny nakładane wielokrotnie nie mogą łącznie przekroczyć kwoty 50 000 zł, a w stosunku do osób prawnych i jednostek organizacyjnych nie posiadających osobowości prawnej kwoty 200 000 zł.(...)

art. 12 ustawy o ochronie danych osobowych

Do zadań Generalnego Inspektora w szczególności należy:

1)kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych,

2)wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych,

3)zapewnienie wykonania przez zobowiązanych obowiązków o charakterze niepieniężnymwynikających z decyzji, o których mowa w pkt 2, przez stosowanie środków egzekucyjnych przewidzianych w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954, z późn. zm.3). (...)

Od dnia 7 marca 2011 r. zgodnie ze znowelizowanym art. 12 pkt 3 ustawy o ochronie danych osobowych, GIODO może nakładać na podmioty, które nie wykonują jego decyzji administracyjnych (np. decyzji nakazującej usunięcie wybranych naruszeń), grzywny w celu przymuszenia. Grzywny egzekwowane są w trybie ustawy o postępowaniu egzekucyjnym w administracji.

Zgodnie z art. 121 ustawy o postępowaniu egzekucyjnym w administracji, wysokość grzywny wynosi:

- dla osób fizycznych do 10 000 zł za każde uchybienie, ale nie więcej niż 50 000 zł w jednym postępowaniu egzekucyjnym

- dla osób prawnych do 50 000 zł za każde uchybienie, ale nie więcej niż 200 000 zł w jednym postępowaniu egzekucyjnym

VIII. Odpowiedzialność karna

Zgodnie z art. 49 ust. 1 ustawy o ochronie danych osobowych, kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Jest to umyślne przestępstwo formalne ścigane z urzędu. Przestępstwo określone w powyższym artykule dotyczy po pierwsze sytuacji, w której przetwarza się dane osób, które nie wyraziły prawidłowej zgody, a brak jest ustawowej przesłanki legalizującej takie przetwarzanie (jak np. art. 23 ust. 4 pkt 1 dopuszczający przetwarzanie w celu marketingu bezpośredniego własnych produktów lub usług. Po drugie, ten sam przepis dotyczy sytuacji, w której istnieje przesłanka w postaci zgody lub ustawowego przepisu legalizującego przetwarzanie danych, lecz osoba która takiego przetwarzania dokonuje nie jest do tej czynności uprawniona (nie posiada odpowiedniego upoważnienia, lub nie jest administratorem danych a nie zawarła umowy powierzenia przetwarzania danych zgodnie z art. 31 ustawy o ochronie danych osobowych).

Odpowiedzialności karnej podlegać może w szczególności administrator bezpieczeństwa informacji, co nie wyklucza odpowiedzialności innych osób (w tym szeregowych pracowników), jeżeli dopuszczają się oni zachowań, które można określić mianem "przetwarzania". Nie zachodzi określone w powyższym przepisie przestępstwo, jeżeli dane osobowe są nieuporządkowane (nie posiadają struktury), ponieważ sankcja karna obejmuje jedynie przetwarzanie "zbioru" danych, natomiast nieuporządkowany zestaw danych nie jest "zbiorem" w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych. Powyższy przepis obejmuje również swym zakresem sytuację, w której dane osobowe są przetwarzane, pomimo niedopuszczalności ich przetwarzania.

Rozdział 8 ustawy o ochronie danych osobowych poświęcony jest odpowiedzialności karnej za naruszenie zasad bezpieczeństwa ochrony danych osobowych przewidzianych w ustawie.

Określone w art. 53 przestępstwo polegające na naruszeniu obowiązku zabezpieczenia danych osobowych przed zabraniem, uszkodzeniem lub zniszczeniem, może zostać popełnione także nieumyślnie.

Przestępstwa określone w rozdziale 8 ustawy o ochronie danych osobowych można popełnić zarówno poprzez działanie jak i zaniechanie.

VIII. Odpowiedzialność karna

Niedopuszczalność przetwarzania danych osobowych zachodzi w sytuacji, gdy w związku z brzmieniem art. 2 ustawy, dane są przetwarzane w zbiorze poza trybem przewidzianym w ustawie – natomiast za tryb przewidziany w ustawie należy rozumieć, oprócz wymagań w zakresie zabezpieczenia danych oraz uzyskania zgodnych z prawem przesłanek ich przetwarzania – także prowadzenie dokumentacji, o której mowa w art. 36 ust. 2 oraz rozporządzeniu wykonawczym do art. 39a o ochroniedanych osobowych.

Skoro zatem wyżej wymienione rozporządzenie wymaga wdrożenia polityki bezpieczeństwa oraz, w przypadku przetwarzania danych w systemie informatycznym, instrukcji zarządzania systemem informatycznym – to brak tych dokumentów w przedsiębiorstwie, w którym przetwarza się dane osobowe oznaczać będzie popełnienie przestępstwa opisanego w art. 49 ust. 1 ustawy o ochronie danych osobowych – polegającego na przetwarzaniu danych osobowych pomimo jego niedopuszczalności.

Zgodnie z art. 51 ust.1 ustawy o ochronie danych, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Przestępstwo powyżej określone jest przestępstwem formalnym, umyślnym, ściganym z urzędu - natomiast ust. 2 tego przepisu przewiduje wariant nieumyślny popełnienia tego przestępstwa (zagrożony karą pozbawienia wolności do roku). Popełnić je może w szczególności osoba, której przysługują kompetencje decyzyjne odnośnie zarządzania zbiorem, co nie wyklucza odpowiedzialności pracownika wykonującego polecenie służbowe w charakterze współdziałającego.

Zgodnie z art. 52 ustawy o ochronie danych osobowych, kto administrując danymi narusza, choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Jest to przestępstwo formalne, ścigane z urzędu, mogące zostać popełnione także nieumyślnie. Do jego zaistnienia dochodzi w momencie niezastosowania odpowiednich środków bezpieczeństwa dotyczących przetwarzanych danych. Odpowiedzialności z powyższego przepisu podlega jedynie administrator danych, co więcej, w odróżnieniu od odpowiedzialności przewidzianej w art. 49 oraz art. 51 nie jest konieczne istnienie zbioru danych (uporządkowanego zestawu danych) dla zaistnienia przestępstwa. Z powyższego przepisu wynika obowiązek dołożenia szczególnej staranności do zabezpieczenia danych osobowych.

VIII.Odpowiedzialność karna

Zgodnie z art. 53 ustawy o ochronie danych osobowych, kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Jest to przestępstwo umyślne, formalne, ścigane z urzędu, podmiotem obarczonym odpowiedzialnością jest w tym przypadku administrujący danymi osobowymi. Przestępstwo to następuje w wyniku zaniechania, jeżeli podmiot nie zgłaszając zbioru do rejestracji przetwarza dane osobowe, których obowiązek rejestracji nie jest wyłączony na mocy art. 43 ust. 1 ustawy o ochronie danych osobowych.

Zgodnie z art. 54 ustawy o ochronie danych osobowych, kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Jest to przestępstwo umyślne, formalne, ścigane z urzędu. Podobnie jak przy art. 51 ustawy o ochronie danych osobowych, odpowiedzialnością jest obarczona tu osoba administrująca zbiorem danych, zachowują więc aktualność uwagi poczynione odnoście podmiotu ponoszącego odpowiedzialność poczynione w odniesieniu do art. 51.

VIII.Odpowiedzialność karna

Odpowiedzialności będzie podlegać administrujący zbiorem, który nie wykonuje przewidzianych w art. 24 i art. 25 obowiązków informacyjnych - odpowiednim elementem na wyeliminowanie odpowiedzialności z tego przepisu będzie zawarcie wymaganych w art. 24 i art. 25 ustawy o ochronie danych osobowych informacji w dokumentach typu: "polityka prywatności", lub też "warunki korzystania z serwisu" itp. obowiązek informacyjny jest bowiem niezależny od obowiązku uzyskania przewidzianych prawem zgód.

Art. 54 dotyczy także sytuacji, w której administrujący zbiorem choćby ignoruje wniosek osoby, której dane osobowe są przetwarzane zgłoszony na podstawie art. 33 ustawy o ochronie danych. Podobnie odpowiedzialności z tego przepisu podlegać będzie administrujący zbiorem w przypadku zignorowania sprzeciwu wniesionego na podstawie art. 32 ust 1 pkt 8 ustawy. Należy zatem pamiętać, by odpowiednio reagować na wszelkie pisma składane przez osoby, których dane są przetwarzane.

Zgodnie z art. 54a ustawy o ochronie danych osobowych, kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Powyższy przepis odwołuje się do „czynności kontrolnej" natomiast, zgodnie z art.14 pkt 1 ustawy o ochronie danych osobowych inspektorowi przysługuje prawo wstępu, w godzinach od 6.00 do 22.00, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym zlokalizowany jest zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań oraz innych niezbędnych czynności. Chociaż w praktyce najczęściej kontrole GIODO są uprzednio zapowiedziane, to nie można wykluczyć sytuacji, w której kontrola jest niezapowiedziana.

Odnosząc się do przestępstwa ujętego w powyższym przepisie, wszelkie działania, które inspektor będzie miał prawo uznać za utrudnianie kontroli może skutkować powiadomieniem przez inspektora prokuratury, a w efekcie odpowiedzialnością karną z wyżej wymienionego przepisu.

IX.Ochrona danych w praktyce

Spis treści:

IX.Ochrona danych w praktyce w spółkach kapitałowych i jednostkach budżetowych

W odniesieniu do formy prawnej prowadzonej działalności, obowiązująca do 1 stycznia 2015 roku treść art. 36 ustawy o ochronie danych osobowych intepretowana była w praktyce w sposób obligujący organy spółek – czy to kapitałowych czy też osobowych- do wyznaczania administratora bezpieczeństwa informacji. W związku z wejściem w życie nowelizacji od dnia 1 stycznia 2015 roku wprowadzona została jedynie możliwość wyznaczenia ABI.

W przypadku zatem gdy np. w spółce z o.o. nie zostanie wyznaczony ABI, funkcje mu przypisane będzie pełnił kierownik jednostki organizacyjnej jako osoba działająca w imieniu administratora danych. W braku innych ustaleń za kierownika jednostki organizacyjnej odpowiadającego za przestrzeganie zasad ochrony danych osobowych będzie należało uznać prezesa zarządu jako osobę stojącą na czele organu kierującymi działaniami osoby prawnej.

Nieco bardziej skomplikowana sytuacja zajdzie w przypadku spółek osobowych, które ze swej istoty nie posiadają organów – gdy działaniami spółki osobowej kieruje kilku wspólników należy więc zadbać o przekazanie obowiązków administratora danych konkretnej osobie – np. w drodze pełnomocnictwa, które nie spowoduje konieczności uznania upoważnienia wskazanej osoby za ABI podlegającego wpisowi do rejestru.

Zbiory podlegające obowiązkowi zgłoszenia do rejestru GIODO:

- zbiory danych Klientów (zawierające dowolne dane teleadresowe)
- dane korespondencyjne Klientów
- rejestry korespondencji (szkół, firm, jednostek organizacyjnych)
- bazy Newsletter
- bazy konkursowe
- rejestry wysyłkowe towarów
- rejestry reklamacji
- beneficjenci działań stowarzyszenia/klubu
- zbiory danych darczyńców
- rejestry uczniów, którzy wypełniają obowiązek szkolny poza daną szkołą
- uczestnicy konkursów międzyszkolnych
- zbiór danych osobowych czytelników czytelni
- listy akcjonariuszy (jeśli są tam osoby fizyczne)
- księgi gości, księgi meldunkowe
- rezerwacje imienne usług
- wszelkie inne dane osobowe, które nie podlegają zwolnieniu

IX.Ochrona danych w praktyce w spółkach kapitałowych i jednostkach budżetowych

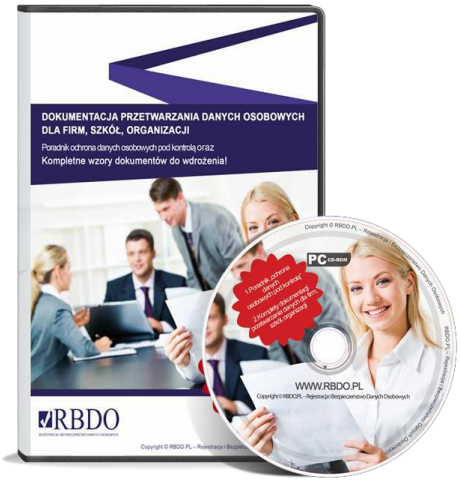
W przypadku przetwarzania zbiorów podlegających zgłoszeniu do GIODO, od 1 stycznia 2015 roku, administrator danych ma wybór zgłoszenia zbioru lub ABI do GIODO – poniżej możliwe warianty wdrożeń:

a) z powołaniem ABI – wówczas zamów kompleksowe wdrożenie ze szkoleniem ABI + 12 m-cy wsparcia prawnego – 2690 z ł netto + 23% VAT

b) bez powołanego ABI – wówczas zamów audyt z dokumentacją i rejestracją zbiorów do GIODO – 699 z ł netto + 23% VAT

c) bez powołanego ABI (*opcja ekonomiczna*) - zamów dokumentację z Instrukcją zgłoszenia do GIODO – w ofercie za 199 zł netto + 23% VAT

REKOMENDOWANY WARIANT:



Optymalnym rozwiązaniem regulującym wszystkie elementy przetwarzania danych w Państwa przypadku jest zamówienie i wdrożenie:

Dokumentacji przetwarzania danych osobowych dla firm z Instrukcj ą z gło sz enia zbiorów do GIODO – w cenie 199 zł netto + 23% VAT wraz z naszym pełnym wsparciem prawnym.

Zamówienie można złożyć na stronie sklepu lub przesyłając dane do Faktury na mail biuro@rbdo.pl

Istnieje także możliwość przeprowadzenia kompleksowego audytu z rejestracją zbiorów przez prawnika RBDO – w cenie 699 zł netto + 23% VAT

Szczegóły oferty na poniższej stronie: AUDYT Z DOKUMENTACJĄ I REJESTRACJĄ W CENIE 699 ZŁ NETTO + 23% VAT

IX.Ochrona danych w praktyce w przedsiębiorstwach jednoosobowych

Zarówno na podstawie poprzedniej wersji ustawy jak i po dniu 1 stycznia 2015 roku osoby fizyczne prowadzące działalność gospodarczą – jeżeli przetwarzały dane osobowe - nie musiały, a obecnie także nie muszą powoływać administratora bezpieczeństwa informacji.

W przypadku przetwarzania danych przez osoby fizyczne prowadzące działalność gospodarczą należy oprócz wdrożenia dokumentacji wewnętrznej (Polityki Bezpieczeństwa, oraz innych dokumentów) ustalić czy w konkretnym przypadku zachodzi konieczność zgłoszenia zbioru danych do GIODO – czy też z racji charakterystyki prowadzonej działalności lub samego zbioru zachodzi jedna z okoliczności określonych w art. 43 ustawy o ochronie danych osobowych wyłączająca obowiązek zgłoszenia zbioru do rejestru.

Zbiory podlegające obowiązkowi zgłoszenia do rejestru GIODO:

- zbiory danych Klientów (zawierające dowolne dane teleadresowe)
- dane korespondencyjne Klientów
- rejestry korespondencji (szkół, firm, jednostek organizacyjnych)
- bazy Newsletter
- bazy konkursowe
- rejestry wysyłkowe towarów
- rejestry reklamacji
- beneficjenci działań stowarzyszenia/klubu
- zbiory danych darczyńców
- rejestry uczniów, którzy wypełniają obowiązek szkolny poza daną szkołą
- uczestnicy konkursów międzyszkolnych
- zbiór danych osobowych czytelników czytelni
- listy akcjonariuszy (jeśli są tam osoby fizyczne)
- księgi gości, księgi meldunkowe
- rezerwacje imienne usług
- wszelkie inne dane osobowe, które nie podlegają zwolnieniu

IX.Ochrona danych w praktyce w przedsiębiorstwach jednoosobowych

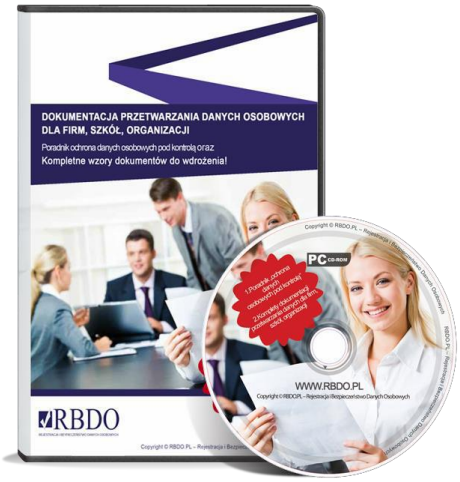
W przypadku przetwarzania zbiorów podlegających zgłoszeniu do GIODO, od 1 stycznia 2015 roku, administrator danych ma wybór zgłoszenia zbioru lub ABI do GIODO – poniżej możliwe warianty wdrożeń:

a) z powołaniem ABI – wówczas zamów kompleksowe wdroż enie ze sz koleniem ABI + 12 m-cy wsparcia prawnego – 2690 z ł netto + 23% VAT

b) bez powołanego ABI – wówczas zamów audyt z dokumentacją i rejestr acją zbiorów do GIODO – 699 z ł netto + 23% VAT

c) bez powołanego ABI (*opcja ekonomiczna*) - zamów dokumentację z Instrukcją zgłoszenia do GIODO – w ofercie za 199 zł netto + 23% VAT

REKOMENDOWANY WARIANT:



Optymalnym rozwiązaniem regulującym wszystkie elementy przetwarzania danych w Państwa przypadku jest zamówienie i wdrożenie:

Dokumentacji przetwarzania danych osobowych dla firm z Instrukcją zgłoszenia zbiorów do GIODO – w cenie 199 zł netto +23% VAT wraz z naszym pełnym wsparciem prawnym.

Zamówienie można złożyć na stronie sklepu lub przesyłając dane do Faktury na mail biuro@rbdo.pl

Istnieje także możliwość przeprowadzenia kompleksowego audytu z rejestracją zbiorów przez prawnika RBDO – w cenie 699 zł netto + 23% VAT

Szczegóły oferty na poniższej stronie: AUDYT Z DOKUMENTACJĄ I REJESTRACJĄ W CENIE 699 ZŁ NETTO + 23% VAT

IX.Ochrona danych w praktyce w biurze rachunkowym

Biura rachunkowe mają przede wszystkim obowiązek wdrożenia dokumentacji przetwarzania danych osobowych i ten obowiązek należy bezwzględnie spełnić.

Biura rachunkowe nie muszą zgłaszać zbiorów danych osobowych do GIODO – co wynika z faktu, że w większości przypadków dane, na jakich pracują są elementami zbiorów danych powierzonych przez klientów na podstawie umów powierzenia przetwarzania w rozumieniu art. 31 ustawy o ochronie danych osobowych. W przypadku, gdy przetwarzanie danych odbywa się na podstawie umowy powierzenia przetwarzania – przetwarzający, czyli biuro rachunkowe nie jest administratorem powierzonych danych osobowych a jedynie odpowiada tak jak administrator danych w ograniczonym zakresie, w szczególności w odniesieniu do odpowiedniego zabezpieczenia danych przed dostępem osób nieuprawnionych – ewentualny obowiązek dokonania zgłoszenia określonego zbioru będzie w tym przypadku mógł ciążyć na kliencie biura rachunkowego jako administratorze danych a nie na samym biurze.

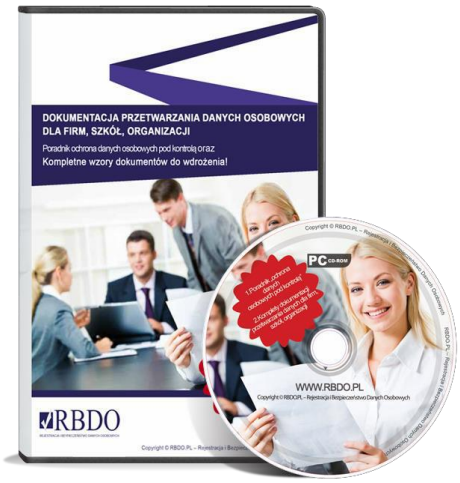
W odniesieniu do danych, w stosunku do których biuro bezpośrednie jest administratorem danych, czyli danymi klientów korzystających z usług biura należy rozróżnić sytuację, kiedy osoba prowadząca działalność biura posiada uprawnienia doradcy podatkowego – tej bowiem sytuacji dotyczy art. 43 ust. 1 pkt 5 wprost stanowiący, że zbiory danych osobowych osób korzystających z usług doradcy podatkowego w stosunku do których jest on ich administratorem są zwolnione z obowiązku zgłaszania do GIODO. Trudno jednoznacznie stwierdzić czy wąskie określenie jedynie zawodu doradcy podatkowego to celowy zabieg ustawodawcy czy przejaw błędu lub niedopatrzenia – jednak nawet jeżeli ktoś prowadzi biuro rachunkowe i nie posiada uprawnień doradcy podatkowego jako podstawę zwolnienia zgłaszania do GIODO zbiorów danych osobowych w stosunku do których jest on administratorem może wywodzić z art. 43 ust. 1 pkt 8 ustawy o ochronie danych osobowych – a więc na tej podstawie iż danych swoich klientów używa wyłącznie do wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej.

Biorąc powyższe pod uwagę - biuro rachunkowe, jako podmiot nie będący zobowiązany z racji specyfiki prowadzonej działalności do dokonania zgłoszenia do GIODO – w ograniczonym zakresie podlega także pod wchodzącą w życie z dniem 1 stycznia 2015 roku nowelizację ustawy o ochronie danych osobowych dotyczącą zagadnienia zgłaszania zbiorów do GIODO oraz stanowiska ABI.

Nowe przepisy największy wpływ mają na podmioty, które na mocy poprzednio obowiązujących przepisów musiały zgłaszać zbiory do GIODO i/lub musiały wyznaczać ABI, ponieważ istotną nowością jaką wprowadza ustawa to zastąpienie generalnego obowiązku wyznaczania ABI alternatywą w postaci wyznaczenia ABI i wpisania go do rejestru lub zgłoszenia do GIODO zbioru danych osobowych.

W przypadku biur rachunkowych ta alternatywa nie istnieje – co do zasady biuro rachunkowe nie musi ani wyznaczać ABI, ani zgłaszać zbioru do GIODO.

IX.Ochrona danych w praktyce w biurze rachunkowym



Optymalnym rozwiązaniem regulującym wszystkie elementy przetwarzania danych w Państwa przypadku jest zamówienie i wdrożenie: Dokumentacji przetwarzania danych osobowych dla firm – w cenie 99 zł netto + 23% VAT wraz z naszym pełnym wsparciem prawnym.

Zamówienie można złożyć na stronie sklepu lub przesyłając na biuro@rbdo.pl dane do Faktury Pro Forma.

Zapraszamy do współpracy wszystkie biura rachunkowe także do wdrożeń na rzecz Państwa Klientów !

IX.Ochrona danych w praktyce w stowarzyszeniach, spółdzielniach i fundacjach

Charakterystyczne dla tego typu podmiotów jest to, że przetwarzają one dane osób zrzeszonych u nich – co w związku z brzmieniem art. 43 ust. 1 pkt 4 wiąże się ze zwolnieniem zbiorów obejmujących te dane z obowiązku zgłoszenia do GIODO. Jednak w przypadku gdy po za osobami zatrudnionymi lub zrzeszonymi przetwarzane są inne dane osobowe np. najemców niebędących członkami spółdzielni lub beneficjentów/ darczyńców zachodził będzie obowiązek zgłoszenia zbiorów do GIODO - chyba że dane (od pierwszego stycznia 2015 roku) przetwarzane są wyłącznie w formie papierowej lub przetwarzanie następuje wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej – ewentualnie jeżeli zajdą inne okoliczności określone w art. 43 ust. 1 ustawy o ochronie danych osobowych.

Aktualności zachowują uwagi odnośnie spółek kapitałowych w kontekście wyznaczania ABI - jeżeli nie zostanie on wyznaczony, w braku innych postanowień za wdrożenie zasad zabezpieczenia zbiorów danych osobowych odpowiadać będzie kierownik jednostki organizacyjnej czyli prezes zarządu.

Jednostki organizacyjne mają przede wszystkim obowiązek wdrożenia dokumentacji przetwarzania danych osobowych i ten obowiązek należy bezwzględnie spełnić. Jeśli chodzi o rejestrację zbiorów lub ABI do GIODO, dotyczy to pewnej kategorii przetwarzanych zbiorów, np.:

- beneficjentów działań stowarzyszenia
- zbiorów danych darczyńców
- rejestrów korespondencji
- rejestry monitoringu
- wszelkie inne dane osobowe osób, które nie są członkami stowarzyszenia czy spółdzielni

IX.Ochrona danych w praktyce w stowarzyszeniach, spółdzielniach i fundacjach

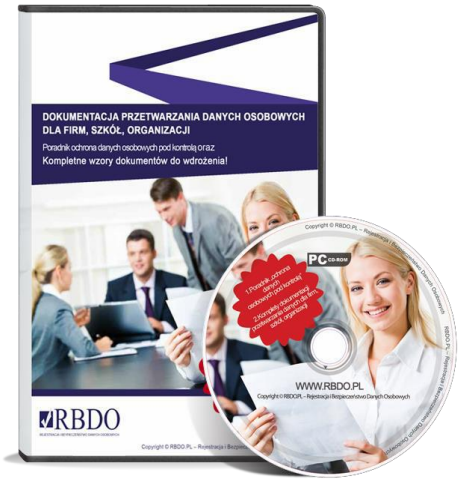
W przypadku przetwarzania zbiorów podlegających zgłoszeniu do GIODO, od 1 stycznia 2015 roku, administrator danych ma wybór zgłoszenia zbioru lub ABI do GIODO – poniżej możliwe warianty wdrożeń:

a) z powołaniem ABI – wówczas zamów kompleksowe wdrożenie ze szkoleniem ABI + 12 m-cy wsparcia prawnego – 2690 zł netto + 23% VAT

b) bez powołanego ABI – wówczas zamów audyt z dokumentacją i rejestracją zbiorów do GIODO – 699 z ł netto + 23% VAT

c) bez powołanego ABI (*opcja ekonomiczna*) - zamów dokumentację z Instrukcją z głoszenia do GIODO – w ofercie za 199 zł netto + 23% VAT

REKOMENDOWANY WARIANT:



Optymalnym rozwiązaniem regulującym wszystkie elementy przetwarzania danych w Państwa przypadku jest zamówienie i wdrożenie: Dokumentacji przetwarzania danych osobowych dla firm z Instrukcją zgłoszenia zbiorów do GIODO – w cenie 199 zł netto + 23% VAT wraz z naszym pełnym wsparciem prawnym.

Zamówienie można złożyć na stronie sklepu lub przesyłając dane do Faktury na mail biuro@rbdo.pl

Istnieje także możliwość przeprowadzenia kompleksowego audytu z rejestracją zbiorów przez prawnika RBDO – w cenie 699 zł netto + 23% VAT

Szczegóły oferty na poniższej stronie: AUDYT Z DOKUMENTACJĄ I REJESTRACJĄ W CENIE 699 ZŁ NETTO + 23% VAT

IX.Ochrona danych w praktyce w szkolnictwie

Jednostki oświatowe mają przede wszystkim obowiązek wdrożenia dokumentacji przetwarzania danych osobowych i ten obowiązek należy bezwzględnie spełnić. Jeśli chodzi o rejestrację zbiorów do GIODO, według przepisów do 2014 roku, co do zasady zbiory danych uczniów/wychowanków (a także rodziców uczniów) lub pracowników podmiotu realizującego zadania edukacyjne są zwolnione z obowiązku zgłoszenia do rejestru, nie dotyczy to jednak innej kategorii osób, których dane są przetwarzane w tego typu jednostkach, np.:

- rejestr korespondencji
- rejestr uczniów, którzy wypełniają obowiązek szkolny poza daną szkołą
- zbiór uczestników konkursów międzyszkolnych
- zbiór danych osobowych czytelników czytelni, jeśli nie są to uczniowie.

W przypadku przetwarzania wyżej wymienionych zbiorów, pojawiają się nowe elementy do spełnienia związane z wyznaczeniem ABI lub rejestracją zbiorów w GIODO.

W przypadku szkoły - to dyrektor placówki jako kierownik jednostki organizacyjnej jest osobą reprezentującą administratora danych osobowych, czyli szkołę jako odrębną jednostkę organizacyjną. W praktyce do dnia 1 stycznia 2015 roku przyjmowano obowiązek wyznaczenia w tego typu podmiotach tzw. ABI (administratora bezpieczeństwa informacji) ponieważ art. 36 ust. 3 stanowił że: Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego zasady ochrony, (...), chyba że sam wykonuje te czynności.

W praktyce interpretowane ten zapis w ten sposób, że dopuszczano brak wyznaczenia konkretnej osoby na tzw. ABI jedynie w tego typu podmiotach jak np. jednoosobowe działalności gospodarcze - gdzie jednoznacznie administrator danych osobowych zawsze był konkretną osobą fizyczną.

W przypadku struktury organizacyjnej takich podmiotów jak szkoły zawsze przy np. zgłoszeniu zbioru do GIODO wymagano oświadczenia, ze wyznaczono konkretną osobę na ABI - chodź nie istniał obowiązek podawania do GIODO informacji kto w konkretnym podmiocie pełni taką funkcję.

IX.Ochrona danych w praktyce w szkolnictwie

Zmiany od 1 stycznia, a szczególności uchylenie art. 36 ust. ustawy o ochronie danych osobowych w kontekście szkół oznaczają, że nie będzie trzeba wyznaczać ABI - jednak pozostanie w taki wypadku obowiązek dokonywania zgłoszeń przetwarzanych zbiorów danych do GIODO (chyba, że konkretne zbiory np. uczniów lub pracowników znajdują się w katalogu wyłączeń ujętym w art. 43 ust. 1 ustawy, który co do zasady pozostał niezmieniony).

Znowelizowana ustawa co prawda wprowadza możliwość skorzystania z dodatkowej przesłanki zwolnienia z obowiązku zgłaszania zbiorów do GIODO dla tych podmiotów, które dobrowolnie wyznaczą ABI i zgłoszą go do rejestru ABI - jednak wiąże się to z dużo większym obciążeniem administracyjnym niż samo zgłoszenie zbioru danych do GIODO.

W przypadku niewyznaczenia ABI - nad przestrzeganiem zasad ochrony danych osobowych czuwać będzie kierownik jednostki organizacyjnej, czyli w przypadku szkoły dyrektor.

IX.Ochrona danych w praktyce w szkolnictwie

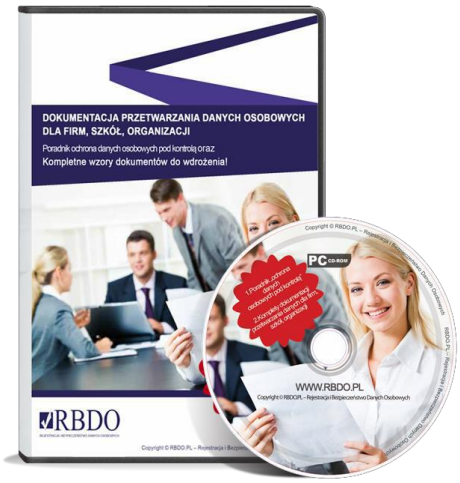
W przypadku przetwarzania zbiorów podlegających zgłoszeniu do GIODO, od 1 stycznia 2015 roku, administrator danych ma wybór zgłoszenia zbioru lub ABI do GIODO – poniżej możliwe warianty wdrożeń:

a) z powołaniem ABI – wówczas zamów kompleksowe wdrożenie ze szkoleniem A B I + 12 m-cy wsparcia prawnego – 2690 z ł netto + 23% VAT

b) bez powołanego ABI – wówczas zamów audyt z dokumentacją i rejestracją zbiorów do GIODO – 699 z ł netto + 23% VAT

c) bez powołanego ABI (*opcja ekonomiczna*) - zamów dokumentację z Instrukcją zgłoszenia do GIODO – w ofercie za 199 zł netto + 23% VAT

REKOMENDOWANY WARIANT:



Optymalnym rozwiązaniem regulującym wszystkie elementy przetwarzania danych w Państwa przypadku jest zamówienie i wdrożenie: Dokumentacji przetwarzania danych osobowych dla firm z Instrukcją zgłoszenia zbiorów do GIODO w cenie 199 zł netto + 23% VAT wraz z naszym pełnym wsparciem prawnym.

Zamówienie można złożyć na stronie sklepu lub przesyłając dane do Faktury na mail biuro@rbdo.pl

Istnieje także możliwość przeprowadzenia kompleksowego audytu z rejestracją zbiorów przez prawnika RBDO – w cenie 699 zł netto + 23% VAT

Szczegóły oferty na poniższej stronie: AUDYT Z DOKUMENTACJĄ I REJESTRACJĄ W CENIE 699 ZŁ NETTO + 23% VAT

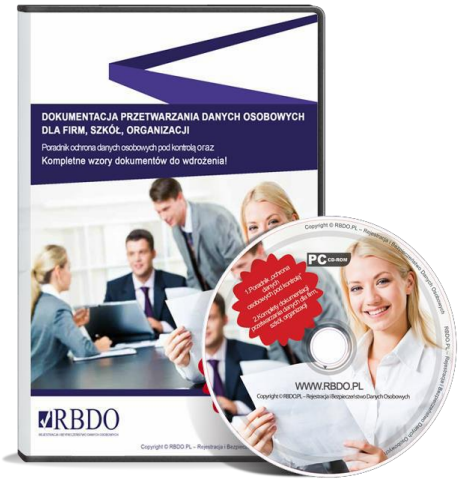
IX.Ochrona danych w praktyce w placówkach medycznych

Jednostki związane ze świadczeniem usług medycznych są administratorami danych osobowych przede wszystkim danych swoich pacjentów. Podkreślenia wymaga fakt, że w większości przypadków są to tzw. „dane wrażliwe" czyli w szczególności dane o stanie zdrowia.

Ustawa przewiduje w przypadku przetwarzania danych wrażliwych wyższy rygor związany także z obowiązkiem zgłoszenia zbioru do GIODO – jednak przewiduje wyjątek związany ze świadczeniem usług medycznych przez administratora tych danych. Zatem podmiot wykonujący usługi medyczne nie musi zgłaszać zbioru danych osobowych swoich pacjentów - pozostaje jednak ich administratorem, a zatem pozostają na nim obowiązki związane z prowadzeniem dokumentacji wewnętrznej oraz odpowiednim zabezpieczeniem tych danych.

W zależności od formy prawnej prowadzonej działalności gospodarczej za wdrożenie zasad ochrony danych odpowiadać będzie osoba prowadząca np. praktykę lekarską jako osoba prowadząca działalność gospodarczą lub prezes zarządu w przypadku prowadzenia działalności w formie spółki kapitałowej.

REKOMENDOWANY WARIANT:



Optymalnym rozwiązaniem regulującym wszystkie elementy przetwarzania danych w Państwa przypadku jest zamówienie i wdrożenie: Dokumentacji przetwarzania danych osobowych dla firm – w cenie 99 zł netto + 23% VAT wraz z naszym pełnym wsparciem prawnym.

Zamówienie można złożyć na stronie sklepu lub przesyłając na biuro@rbdo.pl dane do Faktury Pro Forma.

IX.Ochrona danych w praktyce w sklepach internetowych

W przypadku sklepów internetowych – zbiorem podlegającym zgłoszeniu do rejestru prowadzonego przez GIODO w standardowej sytuacji jest przede wszystkim zbiór danych osobowych klientów.

W art. 43 ust 1 pkt 8 znajduje się co prawda opisanie jako przesłanki zwolnienia z obowiązku zgłoszenia zbioru „przetwarzanie danych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej" jednak w przypadku z sklepu internetowego dokonuje się także samej czynności wysyłki towaru, co więcej sprzedawca ma też obowiązek zapewnić możliwość odstąpienia od umowy w określonym terminie do czego również konieczne jest wykonanie określonych operacji na danych osobowych klientów korzystających z tego prawa – nie można zapomnieć również o rozpatrywanych reklamacjach, gwarancjach itd.

Biorąc pod uwagę że w art. 43 ust. 1 pkt 8 użyto słowa wyłącznie, trudno uznać wykonywanie tych wszystkich czynności za mieszczące się w zakresie wymienionego zwolnienia.

Sklep internetowy powinien więc dokonać zgłoszenia do GIODO przynajmniej zbioru danych osobowych własnych klientów - a jeżeli np. prowadzi inne niestandardowe aktywności np. prowadzi wysyłkę newslettera do osób zapisanych do listy mailingowej - także inne zbiory danych (np. zbiór danych osób zapisanych na newsletter).

Zbiory podlegające obowiązkowi zgłoszenia do rejestru GIODO:

- zbiory danych Klientów (zawierające dowolne dane teleadresowe)
- dane korespondencyjne Klientów
- rejestry korespondencji (szkół, firm, jednostek organizacyjnych)
- bazy Newsletter
- bazy konkursowe
- rejestry wysyłkowe towarów
- rejestry reklamacji
- beneficjenci działań stowarzyszenia/klubu
- zbiory danych darczyńców
- rejestry uczniów, którzy wypełniają obowiązek szkolny poza daną szkołą
- uczestnicy konkursów międzyszkolnych
- zbiór danych osobowych czytelników czytelni
- listy akcjonariuszy (jeśli są tam osoby fizyczne)
- księgi gości, księgi meldunkowe
- rezerwacje imienne usług
- wszelkie inne dane osobowe, które nie podlegają zwolnieniu

IX.Ochrona danych w praktyce w sklepach internetowych

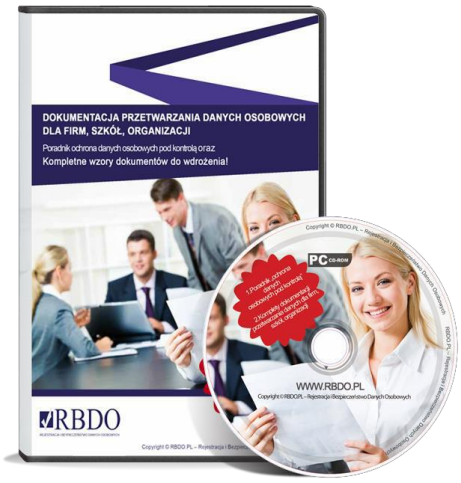
W przypadku przetwarzania zbiorów podlegających zgłoszeniu do GIODO, od 1 stycznia 2015 roku, administrator danych ma wybór zgłoszenia zbioru lub ABI do GIODO – poniżej możliwe warianty wdrożeń:

a) z powołaniem ABI – wówczas zamów kompleksowe wdrożenie ze szkoleniem ABI + 12 m-cy wsparcia prawnego – 2690 z ł netto + 23% VAT

b) bez powołanego ABI – wówczas zamów audyt z dokumentacją i rejestracją zbiorów do GIODO – 699 zł netto + 23% VAT

c) bez powołanego ABI (*opcja ekonomiczna*) - zamów dokumentację z Instrukcją zgłoszenia do GIODO – w ofercie za 199 zł netto + 23% VAT

REKOMENDOWANY WARIANT:



Optymalnym rozwiązaniem regulującym wszystkie elementy przetwarzania danych w Państwa przypadku jest zamówienie i wdrożenie: Dokumentacji przetwarzania danych osobowych dla firm z Instrukcją z głoszenia zbiorów do GIODO – w cenie 199 zł netto + 23% VAT z pełnym wsparciem prawnym.

Zamówienie można złożyć na stronie sklepu lub przesyłając dane do Faktury na mail biuro@rbdo.pl

Istnieje także możliwość przeprowadzenia kompleksowego audytu z rejestracją zbiorów przez prawnika RBDO – w cenie 699 zł netto + 23% VAT

Szczegóły oferty na poniższej stronie: AUDYT Z DOKUMENTACJĄ I REJESTRACJĄ W CENIE 699 ZŁ NETTO + 23% VAT

ZAPRASZAMY DO WSPÓŁPRACY

RBDO - Rejestracja i Bezpieczeństwo Danych Osobowych

ul. Kopalniana 22a /7
01-0321 Warszawa
tel.: (22) 487 86 70
biuro@rbdo.pl

Godziny pracy: 9.00 – 17.00

W celu usprawnienia kontaktu z RBDO, prosimy o kontakt na Infolinię Prawną – (22) 487 86 70.

Pod numerem Infolinii można uzyskać informacje o ustawie o ochronie danych osobowych, obowiązku rejestracji zbiorów danych, wdrożeniach RBDO.

Infolinia czynna jest od poniedziałku do piątku, w godzinach od 9:00 do 16:15.

Kierownictwo:

Łukasz Cieniak
Dyrektor Generalny Rejestracja i Bezpieczeństwo Danych Osobowych
Tel.:: +48 664 484 218
biuro@rbdo.pl

Zespół Prawny:

Dyrektor Działu Prawnego

Karol Cieniak
faq@rbdo.pl
Tel.: +48 666 335 207

Joanna Dobkowska
Adwokat
współpracujący