Uwzględnia nowelizację
ustawy i rozporządzenia

JAK W PRAKTYCE I ZGODNIE Z PRAWEM PRZETWARZAĆ

DANE OSOBOWE

autor: Leszek Kępa

ODO24.pl

› Spis treści

Patron poradnika

ODO 24 sp. z o.o. specjalizuje się w ochronie danych osobowych dostarczając nowoczesne, elastyczne i kompleksowe rozwiązania, pomagające zapewnić zgodność z ustawą o ochronie danych osobowych. Na ofertę ODO 24 składają się m. in.: outsourcing funkcji administratora bezpieczeństwa informacji (ABI), wsparcie ABI, szkolenia administratorów i pracowników, bezpłatne porady prawne oraz opiniowanie umów z zakresu ochrony danych osobowych. Poprzez swoją stronę internetową firma bezpłatnie udostępnia Biuletyn informacyjny, ten poradnik w formie liku PDF, oraz aplikację ABIeye, wspierającą sprawne zarządzanie systemem ochrony danych osobowych w każdej organizacji.

ODO 24 kompleksowo dostosowuje podmioty do wymogów prawa, ze szczególnym uwzględnieniem bezpieczeństwa przetwarzanych przez nie danych. Swoją działalność dedykuje wszystkim tym, którzy chcą poznać, zrozumieć i wdrożyć zasady ochrony danych osobowych.

Autor poradnika

Leszek Kępa – ekspert bezpieczeństwa informacji, autor książki „Ochrona danych osobowych w praktyce" oraz współautor książki „Bezpieczeństwo systemu e-commerce, czyli jak bez ryzyka prowadzić biznes w Internecie". Posiada, uznane na całym świecie, certyfikaty CISA (Certified Information Security Auditor) i CISM (Certified Information Security Manager). Jest członkiem ISACA oraz Podkomisji Ochrony Danych i Standaryzacji Informacji Polskiej Izby Ubezpieczeń. Absolwent Szkoły Głównej Handlowej, Politechniki Częstochowskiej oraz Akademii Podlaskiej.

Ilustracje

Agnieszka Śliwczyńska (www.kel.com.pl)

Projekt

Radosław Zbytniewski (www.zbytniewski.com.pl)

Skład

Radek Zgódka (www.radekzgodka.pl)

Korekta

Małgorzata Korólczyk-Rabek (www.gkrconsulting.pl)

Wydanie VI – Warszawa, październik 2015 r.

Wszelkie prawa zastrzeżone.

Zarówno publikacja w całości jak też każdy jej fragment nie mogą być powielane ani rozpowszechniane w żadnej formie i w żaden sposób bez uprzedniego pisemnego zezwolenia ODO 24 sp. z o.o. Wszelkie znaki towarowe, znaki graficzne, nazwy własne, logotypy i inne dane są chronione prawem autorskim i należą do ODO 24 sp. z o.o.

Ignorantia iuris nocet
– nieznajomość prawa szkodzi.

Wstęp

Wydawałoby się, że ustawa o ochronie danych osobowych jest tylko jedna, powinna być w związku z tym łatwa do przyswojenia. W praktyce okazuje się jednak, że zasady ochrony danych osobowych reguluje ponad sto rozmaitych aktów prawnych! Naprawdę można się w tym pogubić. Co więcej, wszystkie te przepisy bardzo często się zmieniają – największą zmianą jest najnowsza nowelizacja ustawy o ochronie danych osobowych. której przepisy weszły w życie 1 stycznia 2015 r. Zdaję sobie sprawę, że niezmiernie trudno jest na bieżąco śledzić, co się dzieje w prawie, dlatego przygotowałem dla Państwa kolejne, już piąte, wydanie Poradnika, w którym wyjaśniam zmiany, a także przedstawiam pokrótce, czym są dane osobowe oraz jak je przetwarzać i zabezpieczać zgodnie z obowiązującym prawem. Prezentuję również najważniejsze praktyczne zastosowania ustawy o ochronie danych osobowych.

Przede wszystkim warto pamiętać, że nieznajomość prawa utrudnia prowadzenie działalności gospodarczej. Weźmy przykład sklepów internetowych. Prawie każdy z nich powinien mieć zarejestrowany zbiór danych osobowych (no chyba, że powołał ABI), ale nie zawsze ma to odzwierciedlenie w praktyce. W efekcie, zdarza się, że niezadowoleni klienci (np. po otrzymaniu towaru z opóźnieniem), chcąc zaszkodzić sprzedawcy, zgłaszają do GIODO brak zarejestrowania przez niego takiego zbioru danych. Zgodnie z art. 53 ustawy o ochronie danych osobowych, niezgłoszenie, wbrew obowiązkowi, zbioru danych do rejestracji, grozi grzywną, karą ograniczenia wolności, a nawet pozbawienia wolności do roku.

Warto podkreślić, że jest to przestępstwo ścigane z urzędu, co oznacza, że organy ścigania, po uzyskaniu informacji o podejrzeniu popełnienia przestępstwa, zobowiązane są do niezwłocznego podjęcia działań, mających na celu wykrycie sprawcy i zebranie dowodów jego winy. Gdyby przedsiębiorca był świadomy wymogów stawianych przez ustawę o ochronie danych osobowych, zgłosiłby zapewne zbiór danych do rejestracji w GIODO, co pozwoliłoby mu na uniknięcie kłopotów.

Czy to jedyny powód, dla którego warto znać ustawę o ochronie danych osobowych? Oczywiście, że nie. Ustawa stanowi również o tym, jak odpowiednio sformułować treści poszczególnych zgód na przetwarzanie danych osobowych, a także jak wypełnić tzw. obowiązek informacyjny. Przykładowo, art. 54 ustawy określa obowiązki administratora danych osobowych wobec osoby, której dane dotyczą – poinformowanie osoby o wejściu w posiadanie jej danych oraz o przysługujących jej, w związku z tym, prawach. Niedopełnienie tego obowiązku grozi grzywną, karą ograniczenia wolności lub karą pozbawienia wolności do roku. W praktyce oznacza to, że zbierając dane, np. na stronie internetowej, zobligowani jesteśmy do zamieszczenia na tej stronie stosownego komunikatu, informującego m.in. o tym, kto zbiera dane (kto jest administratorem tych danych) oraz w jakim celu je gromadzi. Co więcej, jeśli przedsiębiorca chce prowadzić marketing przez telefon, musi zebrać zupełnie odrębne zgody na takie działanie.

Świadomość społeczna zasad ochrony danych osobowych jest w Polsce coraz większa, a w związku z tym, coraz więcej nieprawidłowości zgłaszanych jest do GIODO. Efektem takich skarg, poza wspomnianymi już sankcjami karnymi, jest spadek zaufania do firmy, która dopuściła się uchybień w zakresie ochrony danych. Nakładane kary czy kosztowne procesy sądowe, zdecydowanie nie wpływają korzystnie na wizerunek organizacji.

Tym z Państwa, których lektura Poradnika zachęci do dalszego zgłębienia tematu, odsyłam do książki „Ochrona danych osobowych w praktyce", której jestem autorem.

Leszek Kępa

Wpływ ustawy na działalność podmiotów

Znakomita większość podmiotów przetwarza dane osobowe – już samo zebranie danych pracownika w celu zatrudnienia podlega ustawie o ochronie danych osobowych. Trzeba przyznać, że ustawa, narzucając wiele obowiązków i ograniczeń, stanowi niemałe wyzwanie. Przykładowo, nawet jeśli osoby, których dane dotyczą, wyrażą na to zgodę, nie możemy swobodnie przetwarzać ich danych. Aby być w zgodzie z prawem, musimy dokładnie uzasadnić cel tego przetwarzania. Co więcej, w wielu przypadkach cel ten podlega dodatkowo kontroli państwowej. Ograniczenia[1)] dotyczą również danych osobowych zebranych z publicznie dostępnych źródeł, takich jak strony internetowe czy katalogi adresowe. Aby móc z nich skorzystać, należy wcześniej poinformować osoby, których dane dotyczą, o pozyskaniu ich danych i przysługujących im w związku z tym prawach. Warto pamiętać, że osoby te mają prawo sprzeciwić się przetwarzaniu swoich danych.

Takie uregulowania mogą utrudniać polskim przedsiębiorcom konkurowanie z zagranicznymi firmami,

1) - Co ciekawe, na tle innych krajów europejskich prawo polskie jest najbardziej wymagające, a jednak te ograniczenia nie zahamowały rozwoju polskiej gospodarki.

Zadania w związku z ustawą

Ustawa oznacza konieczność wykonania wielu zadań i wdrożenia w organizacji określonych procesów. Poniższa lista obrazuje najistotniejsze zagadnienia wynikające z ustawy.

Zadania wewnętrzne:

- **określenie, jakie dane i od kogo będą zbierane oraz w jakim celu będą przetwarzane,**
- **ustalenie, czy wymagana jest rejestracja zbioru danych osobowych,**
- **rejestracja zbiorów danych osobowych lub powołanego w organizacji administratora bezpieczeństwa informacji,**
- **przygotowanie treści informacji dla osób, których dane będą zbierane oraz treści zgód na przetwarzanie danych,**
- **wydawanie i odbieranie upoważnień do przetwarzania danych osobowych, prowadzenie ewidencji wydanych upoważnień,**
- **zabezpieczenie danych osobowych w formie tradycyjnej i w systemach informatycznych,**
- **stworzenie i aktualizowanie stosownej dokumentacji (polityka bezpieczeństwa i instrukcja zarządzania systemem),**
- **nadzór nad zgodnością z przepisami o ochronie danych osobowych i ewentualne powołanie administratora bezpieczeństwa informacji, który będzie pełnić ten nadzór,**
- **zapoznawanie pracowników z przepisami o ochronie danych osobowych,**
- **usuwanie zbędnych danych osobowych.**

Zadania dotyczące osób, których dane są przetwarzane:

- **zbieranie, aktualizowanie i usuwanie danych,**
- **spełnianie tzw. obowiązku informacyjnego, w tym informowanie osób m.in. o tym, jakie mają prawa, jaki jest cel przetwarzania ich danych, kto będzie dane przetwarzał i komu będą przekazywane,**
- **rejestrowanie sprzeciwów i odwoływanych zgód na przetwarzanie danych osobowych.**

Zadania zewnętrzne:

- **zawarcie umowy powierzenia danych osobowych do przetwarzania (w przypadku, gdy dane osobowe przetwarzają w naszym imieniu podmioty zewnętrzne),**
- **kontrolowanie podmiotów zewnętrznych,**
- **poddawanie się kontroli Generalnego Inspektora Danych Osobowych (GIODO),**
- **poddawanie się kontroli podmiotu, w imieniu którego przetwarzamy dane.**

Zadania realizowane w przypadku powołania administratora bezpieczeństwa informacji:

- **sprawdzenie czy administrator bezpieczeństwa informacji spełnia wymagania, w szczególności czy nie był karany,**
- **prowadzenie i udostępnianie rejestru zbiorów danych osobowych wszystkim zainteresowanym,**
- **dokonywanie kontroli na żądanie GIODO,**
- **udokumentowane przeprowadzanie wewnętrznych kontroli zgodności z przepisami administratora bezpieczeństwa informacji .**

których te zapisy nie dotyczą. Przykładowo, nie mogą oni zbierać przez internet wszystkich rodzajów danych, na przetwarzanie danych, które posiadają, muszą posiadać podstawę prawną (np. zgodę), a niektórych rodzajów usług w ogóle nie mogą świadczyć przez internet. Niezależnie jednak od oceny poszczególnych przepisów, wszystkie podmioty przetwarzające dane osobowe zobligowane są do ich przestrzegania. Warto przy tym wiedzieć, jak, stosując się do zapisów ustawy o ochronie danych osobowych, efektywnie prowadzić swoją działalność biznesową.

Co składa się na ustawę?

Na zestaw aktów prawnych dotyczących danych osobowych składają się:

- **ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. 2014 poz. 1182) oraz akty wykonawcze do niej, tj.:**
- **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. z 2008 r., nr 229, poz. 1536), Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. 2011, nr 225, poz. 1350),**
- **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 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 (Dz.U. z 2004 r., nr 100, poz. 1024),**
- **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2004 r., nr 94, poz. 923) i Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 11 maja 2011 r. zmieniające rozporządzenie w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2011 r., nr 103, poz. 601)**
- **Rozporządzenie Ministra Administracji i Cyfryzacji z 29 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz.U. 2014 r. poz. 1934),**
- **Rozporządzenie Ministra Administracji i Cyfryzacji z 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. z 29 grudnia 2014, poz. 1934)**
- **Rozporządzenie Ministra Administracji i Cyfryzacji z 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 25 maja 2015, poz. 719)**
- **Rozporządzenie Ministra Administracji i Cyfryzacji z 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 29 maja 2015, poz. 745)**

Dla większości podmiotów przetwarzających dane osobowe najistotniejsza będzie sama ustawa oraz rozporządzenie w sprawie dokumentacji i wymagań dotyczących systemów informatycznych. Przedmiotem ustawy są wszystkie dane dotyczące osób fizycznych. Osoba fizyczna to określenie człowieka w prawie cywilnym – od chwili narodzenia do śmierci. W konsekwencji ustawa chroni dane osobowe jedynie osób żyjących. Warto też podkreślić, że dla stosowania ustawy nie ma znaczenia narodowość osób, których dane są przetwarzane.[2)]

2) -W sprawozdaniu GIODO za 2009 r., s. 91, Generalny Inspektor podkreśla, że narodowość użytkowników projektowanego portalu nie ma żadnego znaczenia z uwagi na fakt, że ustawa przyznaje ochronę danym osobowym każdej osoby (art. 1 ustawy).

Podmiotami ustawy czyli tymi, którzy zobowiązani są stosować się do opisanych w niej zasad, są w zasadzie wszyscy, za wyjątkiem:

- **osób fizycznych przetwarzających dane w celach osobistych i domowych (nie zarobkowych),**
- **podmiotów z terenu Europejskiego Obszaru Gospodarczego (EOG),**
- **podmiotów spoza tego obszaru, jeśli przez Polskę jedynie przesyłają dane.**

Podmioty z terenu Europejskiego Obszaru Gospodarczego, dzięki konieczności implementacji zasad Dyrektywy 95/46/WE, posiadają własne akty prawne chroniące dane osobowe. Tranzyt danych nie podlega ustawie. Gdyby było inaczej, nie byłoby możliwe np. internetowe przesyłanie danych przez Polskę. Polska ustawa została przyjęta w konsekwencji uchwalenia Dyrektywy 95/46/WE, stanowiącej akt prawa europejskiego. Wszystkie państwa członkowskie Unii Europejskiej zobowiązane zostały do zaimplementowania zapisów dyrektywy do przepisów krajowych, przy czym sposób, w jaki to zrobią, pozostawiono do ich decyzji. W Polsce wymagania dyrektywy wdrożono w 1997 r. przyjmując ustawę o ochronie danych osobowych.

Ustawę o ochronie danych osobowych należy traktować jako swego rodzaju akt generalny, definiujący podstawowe wymogi dotyczące przetwarzania danych osobowych. Jeżeli inna ustawa odnosi się do przetwarzania danych o osobie i nakazuje je chronić bardziej restrykcyjnie, należy stosować te surowsze wymogi. Wynika to z art. 5 ustawy:

Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw.

Obecnie trwają intensywne prace nad przyjęciem rozporządzenia unijnego, które ma zastąpić Dyrektywę 95/46/WE. Różnica między dyrektywą i rozporządzeniem jest taka, że dyrektywę należało zaimplementować (dlatego powstała ustawa o ochronie danych osobowych), natomiast rozporządzenie unijne stosuje się bezpośrednio. W efekcie rozporządzenie zastąpi obecną ustawę o ochronie danych osobowych.

Podmioty prywatne i publiczne

Ustawa o ochronie danych osobowych dotyczy zarówno podmiotów prywatnych jak i publicznych. Warto jednak zauważyć, że w jej praktycznym stosowaniu istnieje pewna subtelna różnica. W publikacji GIODO zatytułowanej „ABC Ochrony danych osobowych" podkreśla się, że podmioty publiczne, w myśl zasady praworządności, wyrażonej w art. 7 Konstytucji Rzeczypospolitej Polskiej, działają wyłącznie na podstawie i w granicach prawa. Oznacza to, że mogą one przetwarzać dane osobowe jedynie wtedy, gdy służy to wypełnieniu określonych prawem zadań, obowiązków i upoważnień.

Zasadę tę podkreśla wyraźnie art. 51 Konstytucji Rzeczypospolitej:

1. *Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.*
2. *Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.*
3. *Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.*
4. *Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.*
5. *Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.*

Piotr Waglowski w swoim serwisie internetowym prawo.vagla.pl pisze, że *państwo kieruje się innymi zasadami, niż obywatele. Obywatele [...] mogą robić to, co nie jest im zabronione przez prawo, muszą robić to, co prawo im nakazuje. Organy władzy publicznej odwrotnie – mogą robić tylko to, co prawo wyraźnie dopuszcza.*[3)]

Wynika z tego, że podmioty publiczne nie powinny zbierać danych osobowych jedynie na podstawie zgody. Musi istnieć przepis prawa, który zezwala im na zbieranie i przetwarzanie danych osobowych. Podmioty prywatne mogą natomiast zbierać w zasadzie dowolne dane, o ile będą mieć np. zgodę osób, których dane dotyczą i dane będą odpowiednie do celu, w jakim mają być przetwarzane.

3) -http://prawo.vagla.pl/node/9936

GIODO i ABI

Nad prawidłowym stosowaniem przepisów o ochronie danych osobowych czuwa Generalny Inspektor Ochrony Danych Osobowych, w skrócie GIODO. Jego kompetencje wyznaczają przepisy art. 12 ustawy o ochronie danych osobowych. Należą do nich m.in.:

- **przeprowadzanie kontroli,**
- **wydawanie decyzji administracyjnych (np. o zarejestrowaniu zbioru, nakazujące usunięcie danych, albo przywrócenie zgodności z ustawą),**
- **rozpatrywanie skarg osób, których dane dotyczą na przetwarzanie ich danych,**
- **prowadzenie rejestru zbiorów danych osobowych,**
- **prowadzenie rejestru administratorów bezpieczeństwa informacji**

Można stwierdzić, że GIODO pełni nadzór nad ochroną danych osobowych w skali makro. W mniejszej skali ustawodawca, uznając wagę danych osobowych, nakazuje pełnić nad nimi nadzór każdemu, kto je przetwarza.[4)]

Każdy podmiot, przetwarzający dane osobowe zobowiązany jest nadzorować ich bezpieczeństwo. Nadzór ten pełnić ma **administrator danych osobowych** – „właściciel" zebranych danych, zwany w skrócie **ADO**. ADO może powołać osobę, która będzie pełniła ten nadzór w jego imieniu (art. 36a) – **administratora bezpieczeństwa informacji**, w skrócie **ABI** – należy wówczas pamiętać o zgłoszeniu takiej osoby GIODO do rejestracji (art. 46b):

Administrator danych jest obowiązany zgłosić do rejestracji Generalnemu Inspektorowi powołanie i odwołanie administratora bezpieczeństwa informacji w terminie 30 dni od dnia jego powołania lub odwołania.

GIODO prowadzi jawny rejestr zgłoszonych administratorów bezpieczeństwa informacji, co oznacza, że takie dane jak imię, nazwisko, dane organizacji w której ABI wykonuje zadania, będą dla wszystkich powszechnie dostępne.

Podkreślmy, że są to zmiany, które obowiązują od 1 stycznia 2015 r. – wcześniej powołanie ABI nie zawsze było opcjonalne, uważano, że w niektórych przypadkach jest taki obowiązek, organizacje nie miały też żadnych korzyści z powołania ABI.

Ministerstwo Gospodarki podkreśla, że *„możliwość wyboru optymalnego rozwiązania jest dla przedsiębiorców bardziej korzystnym rozwiązaniem, niż obowiązujące unormowania. Zgodnie z proponowanymi zmianami po stronie administratora danych istnieć będzie dobrowolność w zakresie powołania ABI".*[5)]

Skoro jesteśmy przy zmianach, to trzeba zauważyć, że podmiot, który powołał i zgłosił do rejestracji ABI jest zwolniony z obowiązku rejestracji zbiorów da-

4) - Z 1 stycznia 2015 r. podmioty, które powołają administratora bezpieczeństwa informacji zwolnione są z rejestracji zbiorów danych osobowych, jednak powinny upublicznić informacje o nich w formie (prawdopodobnie) podobnej, jak robi to GIODO.

5) -Jest to odpowiedź Ministerstwa Gospodarki na uwagi zgłoszone w ramach uzgodnień międzyresortowych i konsultacji społecznych projektu ustawy o ułatwieniu wykonywania działalności gospodarczej.

nych osobowych. Jest to więc bez wątpienia zdecydowana korzyść. Zwolnienie nie dotyczy jednak tych zbiorów, w których przetwarza się dane sensytywne (wrażliwe).

Ustawa określa, że ABI:

- **musi posiadać pełną zdolność do czynności prawnych (a więc musi być pełnoletni, nie może być ubezwłasnowolniony),**
- **musi korzystać w pełni praw publicznych,**
- **nie może być karany za umyślne przestępstwo,**
- **ma podlegać bezpośrednio kierownikowi podmiotu np. zarządowi (art. 36a, ust. 7),**
- **musi posiadać odpowiednią wiedzę z zakresu ochrony danych osobowych.**

Główne zadania ABI to:

- **zapewnianie, że przestrzega się przepisów o ochronie danych osobowych (a więc już nie tylko sam nadzór nad ich zabezpieczeniem – a tak było do tej pory),**
- **nadzór nad opracowaniem dokumentacji i przestrzegania zasad w niej opisanych,**
- **zapewnianie, że osoby zostaną zapoznane z przepisami (np. przeszkolone),**
- **prowadzenie rejestru zbioru danych osobowych.**

Jedna ze zmian jest szczególnie istotna – przed zmianami ABI nadzorował jedynie zabezpieczenia danych osobowych. Po wprowadzeniu zmian w prawie zakres nadzoru jest znacznie szerszy, bo chodzi o zapewnianie przestrzegania przepisów o ochronie danych osobowych.

Ustawodawca nie wskazał, w jaki sposób ustalić, czy wiedza ABI jest odpowiednia. Można jednak poprosić kandydata o udokumentowanie swojego doświadczenia, np. przedstawienie certyfikatów branżowych, informacji o szkoleniach, w których brał udział lub referencji z pracy na podobnym stanowisku,

Warto wiedzieć, że funkcję ABI można powierzyć firmie zewnętrznej. Należy wówczas pamiętać, aby wskazać ABI-ego z imienia i nazwiska, sprawdzić, czy spełnia wymagania określone w ustawie oraz zgłosić go do rejestracji GIODO. Co istotne, ta sama osoba może pełnić rolę ABI w kilku podmiotach. ABI może mieć także wskazanych zastępców.

› Dane osobowe

W rozumieniu ustawy o ochronie danych osobowych za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Nie istnieje jednak żaden ustawowy katalog informacji, które można za takie dane uznać. W praktyce, dowolna informacja dotycząca osoby fizycznej, może stanowić dane osobowe.

Aby odpowiedzieć na pytanie, czy określone dane są danymi osobowymi, należy wziąć pod uwagę kontekst danych. Przykładowo, informacja „zarabia 5 tys. zł miesięcznie" albo „właściciel czarnego Porsche" nic nie mówi o konkretnej osobie, ale nabierze charakteru danych osobowych, gdy zostanie połączona z danymi:

- **dotyczącymi zidentyfikowanej osoby (np.:** *zarabia 5 tys. zł miesięcznie + Jan Kowalski, mieszkający przy ul. Stawki w Radomiu***),**
- **umożliwiającymi łatwe zidentyfikowanie osoby (np.:** *właściciel czarnego Porsche + wojewoda mazowiecki***).**

Dane, które wcześniej nie miały charakteru danych osobowych, nabrały ich po dodaniu informacji, identyfikujących osobę (imię, nazwisko i adres) lub pozwalających na identyfikację (piastowanie urzędu w określonej miejscowości lub regionie).

Najważniejszym składnikiem danych osobowych są informacje umożliwiające identyfikację konkretnej osoby, ustalenie jej tożsamości. Będą one jednak danymi osobowymi tylko dla tych, którzy mają możliwość powiązania ich z danymi konkretnej osoby – znają jej tożsamość lub są w stanie ją ustalić. Te same informacje nie będą danymi osobowymi dla tych, którzy takiej możliwości nie mają.

Ustawa kategoryzuje dane dzieląc je na **dane osobowe zwykłe i dane wrażliwe**, zwane też **sensytywnymi**. Przez dane wrażliwe rozumiemy informacje o osobie opisane w art. 27 ust. 1 ustawy, tj. informacje ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. W ramach ciekawostki warto dodać, że informacja o tym, że osoba nigdy nie była karana również stanowi dane wrażliwe. Wszystkie pozostałe informacje to dane zwykłe.

Przetwarzanie danych osobowych

Przetwarzanie danych jest bardzo szerokim pojęciem. Definicja przetwarzania, zawarta w art. 7 pkt 2 ustawy o ochronie danych osobowych mówi o tym, że są to **jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych**.

Szczególną uwagę należy zwrócić na wyrazy:

- **jakiekolwiek (dowolne),**
- **operacje (działania),**
- **na danych osobowych (wykonywane na danych).**

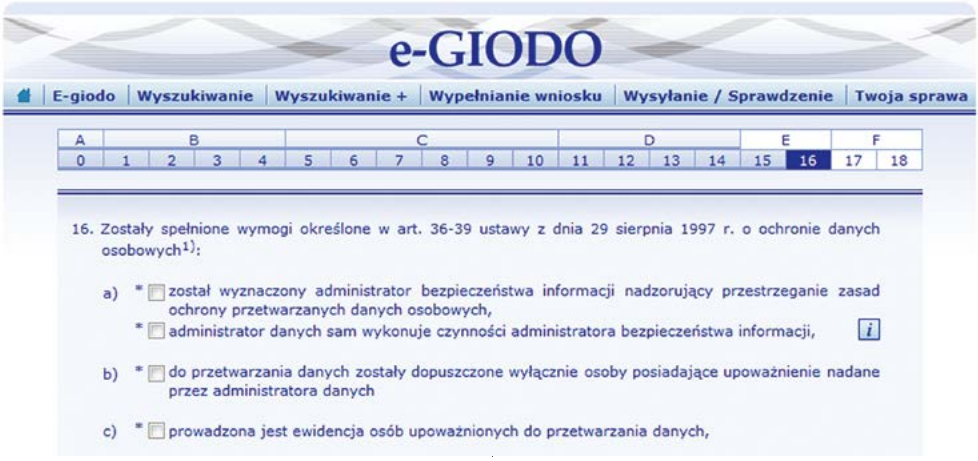
Powyższy wykaz operacji jest jedynie przykładowy. Przetwarzaniem mogą być dowolne działania, wystarczy, że są wykonywane na danych osobowych. Uwagę w definicji zwraca określenie: **zwłaszcza te, które wykonuje się w systemach informatycznych**, co podkreśla szczególną rolę systemów informatycznych w procesie przetwarzania danych osobowych.

Jeśli operacje nie są wykonywane bezpośrednio na danych osobowych, nie występuje przetwarzanie. Przykładowo, kurier transportujący zamkniętą paczkę dokumentów nie będzie przetwarzał danych osobowych zawartych w tych dokumentach, ale firma prowadząca archiwum i sortująca dokumenty w formie papierowej – już tak.

Administrator danych osobowych

W bardzo dużym uproszczeniu **administratora danych osobowych (ADO)** można określić jako właściciela zebranych danych, który decyduje o tym, co się z nimi dzieje – po co je zbiera, co z nimi robi, komu przekazuje, itp. Pojęcie to zdefiniowane jest w art. 7 pkt 4 ustawy: jest to **organ, jednostka organizacyjna, podmiot lub osoba, [...] decydujące o celach i środkach przetwarzania danych osobowych.**

W ustawie, a szczególnie w jej przepisach karnych, pojawia się dodatkowe pojęcie – **administrujący**



danymi. Zgodnie z art. 50, 51, 52 i 54 ustawy o ODO, jest to podmiot, który zarządza, zawiaduje zbiorem danych lub danymi w procesie ich przetwarzania, w tym i powierzonego mu w trybie wskazanym w art. 31 tej ustawy. [6)]

Pojęcie administrującego danymi jest pojęciem szerszym niż administrator danych osobowych. Administrującym danymi jest każdy kto włada danymi – a więc może to być:

- **administrator danych osobowych,**
- **podmiot przetwarzający dane na zlecenie, któremu powierzono dane osobowe do przetwarzania, tzw. procesor,** [7)]
- **ten, który decyduje o celach lub środkach bezprawnie (kto przetwarza dane osobowe nielegalnie).**

Udostępnianie danych osobowych

Udostępnianie, w związku ze znaczeniem potocznym, może się kojarzyć z pożyczaniem, np. można komuś udostępnić samochód albo książkę. W przypadku danych osobowych, mówiąc o udostępnieniu rozumiemy jednak przekazywanie, oddawanie danych podmiotom, które w ustawie nazywane są odbiorcami danych. W wyniku pozyskania danych odbiorcy stają się ich właścicielami – administratorami danych osobowych. Dane możemy również udostępnić innym podmiotom w celu wykonania określonego zlecenia, mówimy wówczas o powierzeniu danych lub upoważnieniu do przetwarzania.

W rozumieniu ustawy, nie każdy jest odbiorcą danych. Będzie nim ten:

[...] komu udostępnia się dane osobowe, z wyłączeniem:
a) osoby, której dane dotyczą,
b) osoby upoważnionej do przetwarzania danych,
c) przedstawiciela, o którym mowa w art. 31a,
d) podmiotu, o którym mowa w art. 31,
e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Zatem, przykładowo, odbiorcami danych nie są:

- **pracownicy upoważnieni do przetwarzania danych,**
- **zleceniobiorcy przetwarzający dane w ramach zlecenia,**
- **osoby, których dane dotyczą (mimo iż mogą te dane odbierać),**
- **komornik, który pozyskuje dane w postępowaniu windykacyjnym.**

Ale już ten, kto dane osobowe kupił, jest ich odbiorcą, a następnie ich właścicielem, czyli administratorem danych osobowych.

Przekazywanie danych do państwa trzeciego

Przekazywanie danych poza kraj należy podzielić na dwa rodzaje:

- **przekazywanie danych do państw Europejskiego Obszaru Gospodarczego,**
- **przekazywanie danych do pozostałych państw (tzw. państw trzecich).**

Przekazywanie danych do państw z terenu Europejskiego Obszaru Gospodarczego w zasadzie nie różni się niczym od przekazywania danych na terytorium Polski. Sytuacja nieco się komplikuje w przypadku pozostałych państw. Przed rozpoczęciem przetwarzania danych należy przede wszystkim określić, co rozumie się jako przekazywanie danych poza kraj. Po pierwsze, dane muszą się znaleźć pod władzą innego państwa – bezpośrednio lub pośrednio, tj. wtedy, gdy podmiot, który ma je przetwarzać, np. zagraniczny przedsiębiorca, będzie podlegał władzy innego państwa. Po drugie, musi istnieć także zamiar przekazywania tych danych.

Dane osobowe udostępnione na polskiej stronie internetowej, bez intencji przetwarzania ich poza krajem, pomimo możliwości dostępu do nich z całego świata, nie będą przekazywane, w rozumieniu

6) -Wyrok NSA z 10 listopada 2009 (I OSK 1379/08)

7) -Termin „procesor" pochodzi z Dyrektywy 95/46/WE, w której tak się określa podmiot, który przetwarza dane osobowe na zlecenie. W projekcie rozporządzenia unijnego jest określany terminem „przetwarzający". Najczęściej chodzi o różnego rodzaju zleceniobiorców.

ustawy, do innego państwa[8]). Podobnie w przypadku laptopa z danymi osobowymi zabranego w podróż zagraniczną – dane znajdą się co prawda na terytorium innego państwa, ale ani laptop ani dane nie wchodzą w jego władanie. Nie jest to więc, w rozumieniu ustawy, przekazywanie danych poza kraj.

Aby móc przekazywać dane poza terytorium Polski i poza Europejski Obszar Gospodarczy (EOG) należy spełnić co najmniej jeden z poniższych warunków:

- **państwo docelowe daje gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązują na terytorium Rzeczypospolitej Polskiej (art. 47 ust. 1),**
- **przesłanie danych osobowych wynika z obowiązku nałożonego przepisami prawa (ustawą) lub postanowieniami ratyfikowanej umowy międzynarodowej,**
- **spełniona zostanie co najmniej jedna z przesłanek określonych w art. 47 ust. 3 (np. zgoda osoby, której dane dotyczą),**
- **zastosowano specjalne zabezpieczenia w zakresie ochrony prywatności, np. tzw. klauzule umowne lub wiążące reguły korporacyjne (art. 48 ust. 2),**
- **na przekazanie danych osobowych wyrazi zgodę GIODO.**

Jeśli gwarancje ochrony nie są „odpowiednie", ale administrator zapewnia właściwe zabezpieczenia korzystając ze specjalnych wzorców umów lub klauzul (w ustawie „standardowe klauzule umowne" oraz „wiążące reguły korporacyjne"), wówczas dane można przekazać bez uzyskania zgody GIODO.

Należy podkreślić, że posiadanie oddziałów firmy na całym świecie, w tym w państwach trzecich, nie usprawiedliwia transferu danych pomiędzy tymi oddziałami bez spełnienia odpowiednich warunków.

8) -por. wyrok Europejskiego Trybunału Sprawiedliwości z 6 listopada 2003 r., sygn. C-101/01 Bodil Lindqvist v. Aklagarkammaren I Jönköping.

Kiedy dane są „osobowe", a kiedy nie

W zasadzie każdy zestaw informacji o osobie może stanowić dane osobowe. Wszystko zależy od tego, czy ten, kto jest w ich posiadaniu, będzie mógł ustalić tożsamość osoby, której dane dotyczą i jak szybko albo przy jakim nakładzie pracy będzie w stanie to zrobić.

Imię i nazwisko oraz adres

Pięć najczęściej spotykanych w Polsce nazwisk nosi prawie 700 tysięcy osób. Samo imię i nazwisko nie stanowi danych osobowych, dopóki nie zostaną one powiązane z informacją dodatkową, pozwalającą na

identyfikację osoby. Czasami wystarczy nazwa miejscowości (np. Stefan Żeromski ze Strawczyna) albo inna informacja uzupełniająca (Bronisław Komorowski – prezydent). Samo imię i pierwsza litera nazwiska (np. Janusz Z.) nie stanowią danych osobowych, chociaż już Mariusz O. z Woli Gułowskiej może identyfikować osobę.

Sam adres także nie identyfikuje konkretnej osoby, a jedynie określone miejsce. Pod jednym adresem może bowiem przebywać czy mieszkać wiele osób. Jednak w połączeniu z dodatkową informacją, adres mógłby już konkretną osobę zidentyfikować. Taką dodatkową informacją jest z pewnością imię i nazwisko. W takim połączeniu dane stają się już danymi osobowymi – znajdziemy je np. w dowodzie osobistym, prawie jazdy, dowodzie rejestracyjnym, itp.

W niektórych sklepach sprzedawcy proszą klientów dokonujących zakupów o podanie kodu pocztowego. Pozwala im to na określenie miejscowości albo regionu, a w dużych miastach nawet nazwy ulicy, przy której mieszka klient. Wiążąc kody pocztowe ze sprzedażą, można określić w jakich regionach kraju, jakie towary sprzedają się najlepiej. Sam kod pocztowy nie jest daną osobową[9].

Numer IP

Numer IP identyfikuje urządzenia w sieci Internet. GIODO na swojej stronie internetowej w sekcji poświęconej odpowiedziom na najczęściej zadawane pytania podkreśla, że *adres IP może być w pewnych przypadkach uznany za dane osobowe*. Jest to oczywiście w zgodzie z generalną zasadą, że za dane osobowe może zostać uznana dowolna informacja, dotycząca osoby fizycznej, umożliwiająca jej zidentyfikowanie.

Sam numer IP jest daną osobową głównie dla operatorów telekomunikacyjnych, którzy są w stanie powiązać ten numer z danymi konkretnego użytkownika sieci. Numer IP powiązany z innymi danymi osobowymi stanie się automatycznie danymi osobowymi.

Numer PESEL

Numer PESEL nadaje się głównie obywatelom polskim, chociaż mogą go otrzymać także cudzoziemcy, zameldowani w Polsce na dłuższy pobyt. PESEL jest swojego rodzaju identyfikatorem osoby. Zakłada się, że nie ma dwóch takich samych numerów PESEL, więc jest to identyfikator unikalny, co w ustawie o ewidencji ludności i dowodach osobistych zostało podkreślone słowem „jednoznacznie"– art. 31a ust. 1:

Numer Powszechnego Elektronicznego Systemu Ewidencji Ludności, zwany w niniejszej ustawie „numerem PESEL", jest to 11-cyfrowy, stały symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, w którym sześć pierwszych cyfr oznacza datę urodzenia (rok, miesiąc, dzień), kolejne cztery – liczbę porządkową i płeć osoby, a ostatnia jest cyfrą kontrolną służącą do komputerowej kontroli poprawności nadanego numeru ewidencyjnego.

W społeczeństwie zwykło się przykładać dużą uwagę do zachowywania numeru PESEL w tajemnicy, podczas gdy, w gruncie rzeczy, numer ten jest niczym innym, jak tylko identyfikatorem. Szczególnie wrażliwe są w tej kwestii kobiety, bo numer PESEL ujawnia ich wiek. Upraszczając można powiedzieć, że poszczególne osoby są w naszym kraju ponumerowane, a PESEL jest po prostu numerem danej osoby. Numer PESEL stanowi dane osobowe – takie jest stanowisko GIODO, który zauważa: **„sam numer PESEL stanowi dane osobowe w rozumieniu ustawy o ochronie danych osobowych"**[10].

Numer telefonu

Jeszcze nie tak dawno jeden telefon służył całej rodzinie. Telefonia komórkowa szybko zmieniła ten stan rzeczy i dzisiaj numer telefonu związany jest raczej z konkretną osobą, niż z miejscem. Mimo że, w rozumieniu ustawy, sam numer telefonu (jako ciąg cyfr) nie jest daną osobową, jednak, podobnie jak adres e-mail, stanowi wyjątkową informację, umożliwiającą bezpośredni kontakt z konkretną osobą. Ustawa, skupiając się na ochronie danych, silnie podkreśla konieczność ustalenia tożsamości osoby. Dane kontaktowe nieco się jej wymykają, gdyż sama możliwość skontaktowania się z daną osobą nie musi (chociaż oczywiście może!) prowa-

9) -Warto odnotować, że ta zasad nie musi obowiązywać we wszystkich krajach. Przykładowo, w Wielkiej Brytanii kod pocztowy jednoznacznie może identyfikować określony adres. Bywa nawet, że Brytyjczycy zamiast adresu podają sam kod pocztowy.

10) - http://www.giodo.gov.pl/317/id_art/973/j/pl/

dzić do ustalenia jej tożsamości. Pomimo faktu, że numer telefonu nie jest samodzielnie daną osobową, stanowi jednak informację, która może umożliwiać naruszenie prywatności.

Art. 172 ustawy Prawo telekomunikacyjne w dotychczasowym brzmieniu, obowiązującym do 25 grudnia 2014 r., zakazywał używania „automatycznych systemów wywołujących" dla celów marketingu bezpośredniego bez uprzedniej zgody abonenta. Poprzez dodanie trzech niepozornych słów – „telekomunikacyjnych urządzeń końcowych" – ustawodawca wprowadził szerokie ograniczenia w zakresie wykonywania marketingu bezpośredniego. Przez urządzenia końcowe rozumie się telefony, smartfony, a nawet tablety i komputery. W rezultacie, nielegalne jest wykonywanie połączeń telefonicznych w celach marketingowych, jeżeli osoba, do której dzwonimy, nie wyraziła wcześniej na to odpowiedniej zgody.

Numer telefonu w połączeniu z imieniem albo nazwiskiem należy uznawać za dane osobowe.

Numer telefonu zestawiony z innymi informacjami o osobie, mimo iż nie zawsze będą to dane osobowe, należy traktować bardzo ostrożnie, np. numer telefonu i wysokość wynagrodzenia. Grupa robocza art.29[11)] w opinii 4/2007 stwierdza, że sam numer telefonu stanowi dane osobowe – po to się go przetwarza, aby ostatecznie ustalić tożsamość konkretnej osoby i do niej dotrzeć.

Danych, które samodzielnie, w rozumieniu ustawy, nie będą danymi osobowymi, bo nie pozwalają na ustalenie tożsamości, umożliwiają jednak kontakt z konkretną osobą, będzie więcej. Będą to np.: numery Gadu-Gadu, identyfikator Skype oraz prywatne adresy poczty elektronicznej.

Adres e-mail

Adres poczty elektronicznej, podobnie jak numer telefonu, pozwala na kontakt z konkretną osobą. Różni się jednak nieco większą zawartością informacji, może bowiem ujawniać np. miejsce zatrudnienia, przynależność do określonej organizacji lub pewne cechy danej osoby. Firmowe adresy poczty elektronicznej zawierają w sobie najczęściej imię i nazwisko oraz nazwę firmy. Możliwość kontaktu połączona z identyfikacją osoby z imienia i nazwiska oraz miejscem jej pracy pozwala na ustalenie tożsamości użytkownika danego adresu. To powoduje, że **firmowy adres e-mail uznawany jest za dane osobowe**. Nie ma przy tym znaczenia, czy taki adres jest powszechnie dostępny czy też nie.

W przypadku prywatnych, najczęściej darmowych, adresów poczty elektronicznej, nawet jeżeli zawierają imię i nazwisko, nie zwykło się uważać ich za dane osobowe. Każdy może założyć sobie konto pocztowe o dowolnej nazwie (np. leszek.kepa@gmail.com), oczywiście o ile nie jest ona już zajęta. To sprawia, że adres nie identyfikuje jednoznacznie konkretnej osoby. Należy jednak pamiętać, że adres poczty elektronicznej wciąż pozwala na kontakt z jego właścicielem, a więc jego nieuprawnione wykorzystanie może spowodować naruszenie sfery prywatności danej osoby.

Warto wiedzieć, że gdy pracownik odchodzi z pracy, należy usunąć, a przynajmniej zablokować jego adres poczty elektronicznej. Przetwarzanie imienia i nazwiska w ramach służbowego adresu e-mail osoby, która już nie pracuje *jest niezgodne z celem, dla którego dane te były zbierane. […] ciągła aktywność przedmiotowego adresu poczty elektronicznej, a zarazem możliwość przesyłania wiadomości na ten adres, pośrednio jednak nadal wpływało na utożsamianie osoby […] ze spółką, co w obecnej sytuacji dawało fałszywy obraz jej*

11) - Zespół roboczy ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych – niezależny podmiot o charakterze doradczym, powołany na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. W skrócie określany jako „Grupa robocza art. 29".

aktywności zawodowej. Ponadto osoba, do której, zgodnie z jej identyfikatorem zawartym w adresie, kierowana była korespondencja nie miała możliwości zapoznania się z nią, co z kolei stanowiło przejaw naruszenia wolności tej osoby do prawa komunikowania się oraz ochrony jej korespondencji[12].

Numer rachunku bankowego

Numer rachunku bankowego (NRB) składa się z 26 cyfr. W numerze rachunku, w cyfrach od 3 do 10, zaszyta jest informacja o banku. Jest to tzw. numer rozliczeniowy jednostki organizacyjnej banku. Sam numer rachunku w zasadzie nie prowadzi do identyfikacji konkretnej osoby i dla przeciętnej osoby nie stanowi danej osobowej, podobnie jak kwoty i daty przelewów. Jednak w przypadku banków, a w szczególności macierzystego banku posiadacza rachunku, taka identyfikacja jest możliwa poprzez wprowadzenie numeru rachunku do systemu komputerowego.

Podobnie więc jak w innych przypadkach dane stają się „osobowe" dopiero wówczas, gdy zostaną połączone z innymi danymi osobowymi, identyfikującymi osobę. W podobny sposób można traktować także numer dowodu osobistego, legitymacji, czy nawet numer rejestracyjny samochodu.

Kiedy dane są „osobowe"?

Jak można już było zauważyć, to czy informacje są danymi osobowymi, czy też nie, zależy przede wszystkim od kontekstu, w jakim się znajdują, tj. od tego, z jakimi innymi danymi występują lub z jakimi są zestawiane. Te same informacje, w zależności od sytuacji, mogą być lub nie być danymi osobowymi. Przykładowo, studenci mogą otrzymać mailem wyniki egzaminu w formie tabeli, w której znajduje się numer studenta, przedmiot i ocena. Takie informacje to dane osobowe dla studenta oraz pracowników uczelni. Dla innych te informacje nie będą danymi osobowymi, gdyż nie będą oni w stanie ustalić tożsamości osób, których dane dotyczą.

Ma to ogromne znaczenie w przypadku zabezpieczania przesyłania lub transportu danych osobowych. Dane osobowe przesyłane przez internet, powinny być przesyłane w zabezpieczonej formie, np. szyfrowane. Jednak jeśli przesyłane informacje nie stanowią danych osobowych (dla osób innych niż nadawca i odbiorca), nie ma takiego obowiązku.

Nr studenta	przedmiot	ocena
2697	ochrona danych osobowych	3+
2698	ochrona danych osobowych	4+
2699	ochrona danych osobowych	5

Przykład publikowania informacji o wynikach egzaminów

Warto zapamiętać, że niektóre informacje, wewnątrz organizacji mogą być danymi osobowymi, a poza organizacją już nie. W efekcie, poza organizacją, nie będą wymagały takiej ochrony, jak nakazuje ustawa.

› Zbieranie danych

Nie można zbierać większej ilości danych, niż jest to niezbędne do realizacji określonego celu przetwarzania. Dane muszą być adekwatne do celu ich zbierania (art. 26 ust. 1 pkt 3) i przetwarzania. Cel przetwarzania danych przez organizację musi być zgodny z prawem i z jej profilem działalności. Warto podkreślić, że adekwatność podlega kontroli GIODO, np. na etapie rejestrowania zbioru danych.

Czym jest adekwatność? Według słownika języka polskiego „adekwatny" to „dokładnie odpowiadający czemuś, zgodny z czymś". W łacinie „adaequatus" oznacza dostosowany.

Zdaniem GIODO adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swymi danymi a interesem administratora danych. Równowaga będzie zachowana, jeżeli administrator przetwarza dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane.[13]

Przykładem braku adekwatności jest opisana w sprawozdaniu GIODO za 2010 r. usługa wypoży-

12) - Sprawozdanie GIODO za 2011 r., s. 75-76

13) -Sprawozdanie GIODO za 2012r., s. 190

czania w hipermarketach wózków-samochodzików dla dzieci. Świadczący usługi, w ramach zastawu za wypożyczany wózek, zatrzymywał za zgodą wypożyczających ich dokumenty (legitymacje studenckie, prawa jazdy, dowody rejestracyjne samochodów, itp.), a następnie pozyskiwał z nich dane. Generalny Inspektor Danych Osobowych uznał, że *w związku z realizacją takiej umowy administrator danych pozyskiwał szerszy zakres danych niż ten, który był niezbędny dla realizacji ww. umowy, naruszając tym samym zasadę adekwatności wyrażoną w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych*. Konsekwencją była decyzja nakazująca przywrócenie stanu zgodnego z prawem, a więc zaprzestanie pozyskiwania danych osób wypożyczających wózki w zakresie szerszym, niż jest to niezbędne dla realizacji umowy wypożyczenia wózka.

Przykładem braku adekwatności jest kodowanie na biletach okresowych numeru PESEL, podczas gdy imię, nazwisko i wizerunek posiadacza są wystarczające dla umożliwienia weryfikacji, czy daną kartą, jako nośnikiem imiennego biletu komunikacji miejskiej, posługuje się osoba upoważniona do jej używania. Zdaniem GIODO umieszczanie numeru PESEL na legitymacjach szkolnych także nie jest adekwatne do celu, jakim jest oświadczenie faktu uczęszczania ucznia do szkoły oraz jego uprawnienia do korzystania ze zniżek ustawowych przy przejazdach środkami publicznego transportu kolejowego i autobusowego.

Adekwatny i niezbędny nie oznaczają tego samego.

Podczas starania się o pożyczkę, przekazujemy bankowi wiele informacji, które nie są niezbędne do jej udzielenia, są jednak adekwatne, bo pozwalają bankowi ocenić naszą wiarygodność i zdolność kredytową.

Gdy Generalny Inspektor Danych Osobowych uzna, że dane nie są odpowiednie w stosunku do celu w jakim je zebrano, może np. nakazać usunięcie nadmiarowych danych i zażądać zaprzestania ich zbierania. Cel przetwarzania zbieranych danych osobowych musi być zgodny z prawem i profilem organizacji. Zakup bazy danych klientów, mimo że danych nie zbiera się w rozumieniu ustawy, także oznacza zbieranie danych, tyle że nie bezpośrednio od osób, których one dotyczą. Ustawowo „zbieranie danych" oznacza wszystkie przypadki, w których administrator uzyskuje nowe, ze swej perspektywy, dane osobowe[14)].

Zbierając dane należy spełnić tzw. obowiązek informacyjny tj. poinformować osobę, której dane dotyczą, m.in. o tym, kto będzie przetwarzał jej dane i w jakim celu. Bardzo istotne, aby zdefiniować cel przetwarzania danych jeszcze przed rozpoczęciem ich przetwarzania. Zmiana celu w trakcie przetwarzania wiąże się z dodatkowymi obowiązkami, w tym m.in. z obowiązkiem poinformowania wszystkich osób, których dane zostały już zebrane (art. 26 ust. 2) o nowym celu przetwarzania ich danych. Może się okazać, że właściciele danych nie zgodzą się na ten nowy cel (zgłaszając tzw. sprzeciw) i wówczas zmuszeni będziemy do usunięcia ich danych z naszej bazy.

Dane osobowe można pozyskiwać:

- *bezpośrednio od osoby, której dane dotyczą,*
- *z innych źródeł (niebezpośrednio), np. ze stron internetowych, książki telefonicznej bądź od osób trzecich.*

Niezależnie od źródła pozyskania danych, osobę, której dane dotyczą, należy poinformować:

- *o tym, kto będzie przetwarzał jej dane (kto będzie administratorem danych),*
- *w jakim celu jej dane są zbierane,*
- *o prawie dostępu do treści danych i możliwości ich poprawiania,*
- *o innych przysługujących jej prawach.*

14) -P. Barta, P. Litwiński, Ustawa o ochronie danych osobowych. Komentarz, C.H.Beck, Warszawa 2009, s. 238.

Szczegółowa treść informacji będzie się różnić w zależności od tego, z jakiego źródła pochodzą dane.

Osoba, której dane dotyczą, musi być poinformowana o ich pozyskaniu najpóźniej w chwili ich zbierania. Informacje te bardzo często przekazuje się wraz z uzyskiwaniem zgody na przetwarzanie danych osobowych. Jest to bardzo ważny obowiązek, a jego niespełnienie karane jest z art. 54 ustawy o ochronie danych osobowych.

› Przesłanki legalności, upoważnienia i powierzenia.

Aby można było przetwarzać dane osobowe, należy spełnić tzw. przesłanki legalności przetwarzania danych osobowych – mowa o nich w art. 23 i 27 ustawy o ochronie danych osobowych. Przetwarzanie danych jest dopuszczalne gdy:

- **osoba, której dane dotyczą wyrazi na to zgodę,**
- **jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,**
- **jest to konieczne do 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,**
- **jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,**
- **jest to niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych [...], a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.**

Należy pamiętać, że w przypadku przetwarzania danych osobowych wrażliwych należy spełnić dodatkowe warunki, opisane w art. 27 ustawy o ochronie danych osobowych.

Bardzo interesującym tematem jest wyrażanie zgody na przetwarzanie danych osobowych przez dzieci. Należy przyjąć, że dziecko do ukończenia 13 roku życia nie może wyrazić zgody, gdyż nie ma zdolności do czynności prawnych – musi to zrobić jego rodzic. Zgodę na przetwarzanie danych wrażliwych może dać wyłącznie osoba pełnoletnia.

W kontekście przesłanek legalności przetwarzania danych osobowych warto zauważyć, że Wojewódzki Sąd Administracyjny w Warszawie w wyroku II SA/Wa 892/12 z 26 lipca 2012 r. stwierdza, że *na wstępie rozważań należy wskazać, że ochrona danych osobowych polega przede wszystkim na określeniu kiedy dozwolone, a kiedy zabronione jest ich przetwarzanie.*

Upoważnienia do przetwarzania danych osobowych

Każdy pracownik, który będzie przetwarzał dane osobowe powinien zostać upoważniony do ich przetwarzania przez administratora danych osobowych (ADO). Upoważnienie pełni kilka istotnych funkcji, m.in. stanowi uprawnienie do przetwarzania danych i spełnia wymóg ustawy określony w art. 37:

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

Nie ma znaczenia forma zatrudnienia ani stosunek prawny między przedsiębiorcą a osobą przetwarzającą dane. Może to być pracownik danego przedsiębiorcy, osoba na umowie zlecenie, pracownik firmy zewnętrznej, np. serwisu komputerowego, itp. **W przypadku osób fizycznych uprawnieniem do przetwarzania danych może być zwykłe upoważnienie, w innych przypadkach, np. osób prawnych (spółek akcyjnych i spółek z o.o.) będą to stosowne umowy powierzenia**[15)].

15) - W przypadku osoby fizycznej prowadzącej działalność gospodarczą możliwe są oba rozwiązania tj. upoważnienie właściciela do przetwarzania danych osobowych albo zawarcie umowy powierzenia. Zalecamy zawieranie takich umów.

Przykładowe upoważnienie do przetwarzania danych osobowych

Każdy, kto przetwarza dane osobowe musi mieć ku temu jakąś prawną przesłankę. Administrator danych musi spełnić tzw. przesłanki legalności przetwarzania danych osobowych, pracownik – otrzymuje stosowne upoważnienie, zleceniobiorca – umowę powierzenia. Bez tego nie powinno być mowy o przetwarzaniu danych.

Upoważnienie należy wydać, zanim dana osoba zacznie przetwarzać dane osobowe. Nie można zakładać, że skoro została zatrudniona na określonym stanowisku, np. jako doradca klienta, może już przetwarzać dane klientów. Upoważnienie należy przekazać tak, jak nakazuje ustawa. Należy też pamiętać, aby przed dopuszczeniem danej osoby do przetwarzania przeszkolić ją z zasad ochrony danych osobowych.

Upoważnienia wydaje administrator danych. Może on też ustanowić pełnomocnictwo do wystawiania upoważnień i wówczas upoważnienia może wystawiać np. pracownik działu personalnego lub administrator bezpieczeństwa informacji (ABI). Warto zaznaczyć, że upoważnienia nie muszą mieć formy papierowej, można wydawać je elektronicznie, np. wysyłając mailem[16]. Generalny Inspektor akceptuje taki sposób stwierdzając: *nie wydaje się, aby upoważnienie nadane w formie e-maila pozostawało w sprzeczności z przepisami ustawy o ochronie danych osobowych, jeśli spełnia wszelkie inne ww. wymogi z tej ustawy*[17].

16) - GIODO akceptuje upoważnienia wydawane w formie elektronicznej: http://www.giodo.gov.pl/317/id_art/3442/j/pl/

17) - GIODO akceptuje upoważnienia wydawane w formie elektronicznej: http://www.giodo.gov.pl/317/id_art/3442/j/pl/

Informacje o wydanych upoważnieniach należy zamieszczać w stosownym rejestrze, zawierającym dane wszystkich osób aktualnie upoważnionych do przetwarzania danych osobowych. Choć nie ma oficjalnie takiego obowiązku, wydane upoważnienia, jako dodatkowy dowód ich nadania, warto przechowywać, np. w odrębnym segregatorze.

Oświadczenia o ochronie danych osobowych

Osoby zatrudnione przy przetwarzaniu danych osobowych muszą zostać zapoznane z zasadami ochrony danych osobowych (art. 36a ust. 2 oraz art. 36b). Zapoznanie takie ma najczęściej charakter szkolenia, często także w formie elektronicznej. Jako dowód

Upoważnienie do przetwarzania danych osobowych

Firma X, na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz.U. 2014 poz. 1182 i 1662), niniejszym upoważnia Pana /Panią Y do przetwarzania danych osobowych w następującym zakresie:

[x] dane przetwarzane w formie papierowej,
[x] dane przetwarzane w systemie informatycznym,

w tym dane osobowe objęte zbiorami:

1. „Nazwa zbioru A" w zakresie modyfikacja, odczyt, wprowadzanie i usuwanie danych,
2. „Nazwa zbioru B" w zakresie odczyt,

Niniejsze upoważnienie obowiązuje od daty wystawienia i traci moc najpóźniej z dniem zakończenia pracy przez Pana / Panią Y w Firmie X.

warto zebrać od osób stosowne oświadczenia, m. in.: o przejściu szkolenia, zapoznaniu się z dokumentami wymaganymi przez ustawę oraz o zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia.

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

Warto zauważyć, że podczas zgłaszania zbioru danych osobowych do rejestracji należy opisać, jakie środki organizacyjne przedsięwzięto w celu zabezpieczenia danych osobowych. Wśród nich wymienia się następujące zabezpieczenia:

- **zaznajomienie (przeszkolenie) osób zatrudnionych przy przetwarzaniu danych z przepisami dotyczącymi ochrony danych osobowych,**
- **zobowiązanie osób zatrudnionych przy przetwarzaniu danych osobowych do zachowania ich w tajemnicy.**

Obowiązek przeszkolenia osób upoważnionych do przetwarzania danych osobowych wynika wprost z ustawy:

Do zadań administratora bezpieczeństwa informacji należy:

1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez: [...]

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

Art. 36b. W przypadku niepowołania administratora bezpieczeństwa informacji zadania określone w art. 36a ust. 2 pkt 1 [...], wykonuje administrator danych.

Oświadczenia o zapoznaniu się z regulacjami stanowią jeden z organizacyjnych elementów ochrony danych osobowych. Można je przechowywać w aktach pracowniczych albo razem z kopiami wydanych upoważnień do przetwarzania danych osobowych.

Jak przygotować zgodę na przetwarzanie danych osobowych?

Zgodą, w rozumieniu ustawy o ochronie danych osobowych, jest oświadczenie woli pochodzące od osoby, której dane dotyczą, którego treścią jest zgoda na przetwarzanie jej danych. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Może być za to w każdym czasie odwołana.

Są jednak przypadki, kiedy forma pisemna jest wymagana:

- **wówczas, gdy przetwarzane mają być dane wrażliwe (sensytywne),**
- **wówczas, gdy dane mają być przekazywane do państwa trzeciego.**

Zawarcie umowy z osobą jest odpowiednikiem zgody na przetwarzanie jej danych, nie należy wtedy zbierać odrębnej zgody na przetwarzanie danych w celu realizacji umowy.

Na stronie GIODO można znaleźć opinię, że **podmiot, który przy okazji zawierania umowy zamierza również pozyskać zgodę na przetwarzanie danych osobowych kontrahenta, zobligowany jest do wyodrębnienia oświadczenia, którego treścią jest zgoda na przetwarzanie danych osobowych, od oświadczenia wyrażającego chęć związania się postanowieniami umowy. Nie można bowiem utożsamiać woli zawarcia umowy ze złożeniem oświadczenia woli, na podstawie którego osoba, której dane dotyczą, zgadza się na wykorzystywanie jej danych osobowych do innych celów**[18].

Zgoda na przetwarzanie danych osobowych może być także „zapłatą" za usługę lub towar. W literaturze można spotkać opinie, że **uzależnianie świadczenia usługi od zgody na przetwarzanie danych dopuszczalne jest jedynie wyjątkowo, gdy usługa świadczona jest nieodpłatnie, a zgoda traktowana jest jedyne jako swoiste świadczenie wzajemne**[19].

Doskonałym tego przykładem są serwisy oferujące darmowe konta poczty elektronicznej w zamian za zgodę na przetwarzanie danych osobowych. Należy przy tym pamiętać, że taka zgoda musi być dobrowolna i nie można w żaden sposób przymuszać osób do jej wyrażenia. W przypadku serwisów internetowych rekomenduje się, aby pole do wyrażenia zgody, np. tzw. checkbox, domyślnie nie było zaznaczone, a dopiero samodzielne jego zaznaczenie oznaczać ma dobrowolne i świadome wyrażenie zgody.

18) - O ile marketing własnych towarów i usług jest dopuszczalny, to inne akty prawa mogą ograniczać pewne formy marketingu, np. marketing za pomocą telefonu czy poczty elektronicznej reguluje znowelizowane niedawno prawo telekomunikacyjne.

19) - Dodatek specjalny do Monitora Prawniczego nr 3/2011, Nowelizacja ustawy o ochronie danych osobowych 2010, „Nowelizacja ustawy o ochronie danych osobowych – zakładane cele i przewidywane skutki", dr hab. P. Fajgielski, s. 4.

Powierzenie przetwarzania danych

Zlecenie innemu podmiotowi przetwarzania danych osobowych w celu realizacji określonego zadania w ustawie o ochronie danych osobowych określa się jako *powierzenie przetwarzania*. Zgodnie z art. 31 ust. 1: *Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych*. W Dyrektywie 95/46/WE taki podmiot określa się mianem „procesora", natomiast nasza ustawa nie wprowadziła krótszego terminu i jest to po prostu „podmiot, któremu powierzono przetwarzanie danych osobowych".

Sytuacji, w których dane osobowe będą niezbędne do realizacji zlecenia może być wiele. Można z góry założyć, że zawarcia umowy powierzenia będą wymagały następujące usługi:

- **prowadzenie ksiąg rachunkowych,**
- **przygotowanie i wysyłanie korespondencji na zlecenie (niezależnie od formy),**
- **prowadzenie archiwum dokumentów papierowych,**
- **niszczenie dokumentów,**
- **usługa centrum telefonicznego (call center),**
- **prowadzenie spraw pracowniczych (kadry),**
- **windykacja należności.**

Z definicji ustawowej przetwarzania danych osobowych wynika, że przetwarzanie to operacje na danych osobowych. Jeśli celem zlecenia nie są operacje na danych, to nie należy zawierać umowy powierzenia, lecz np. umowę o zachowaniu poufności.

Powierzenie jest w pewnym sensie uzupełnieniem podstaw prawnych do przetwarzania. Każdy, kto przetwarza dane osobowe, musi mieć jakąś podstawę do ich przetwarzania:

- **administrator danych osobowych musi spełniać tzw. przesłanki legalności z art. 23 ust. 1 lub art. 27 ust. 2 ustawy o ochronie danych osobowych;**

» **pracownik może przetwarzać dane osobowe na podstawie wydanego upoważnienia;**

» **zleceniobiorca przetwarza dane osobowe na podstawie umowy powierzenia.**

Ustawa wymaga, aby umowa powierzenia została zawarta na piśmie, jednak brak formy pisemnej nie oznacza jeszcze, że umowa jest nieważna, może to jednak prowadzić do sankcji w postaci decyzji administracyjnej Generalnego Inspektora Ochrony Danych Osobowych. Ustawa o ochronie danych osobowych nie nakłada żadnych ograniczeń na powierzanie danych – jeśli administrator ma prawo je przetwarzać, może również powierzyć ich przetwarzanie każdemu innemu podmiotowi. Ograniczenia mogą jednak wynikać z innych aktów prawa.

Obowiązki zleceniobiorcy

Przyjmujący dane osobowe do przetwarzania w imieniu administratora danych osobowych zobowiązany jest do spełnienia związanych z tym wymagań wynikających z ustawy. Musi je spełnić zanim zacznie przetwarzać dane, a więc zanim otrzyma je od zleceniodawcy. Wymagania te wynikają z treści art. 31 ust. 3:

Podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.

Zleceniobiorca zobowiązany jest m.in. do:

» **zabezpieczenia danych osobowych (art. 36 ust. 1),**

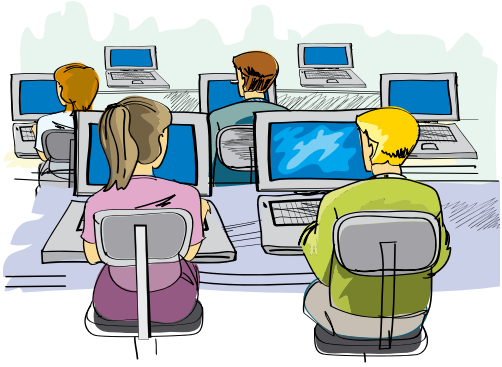
» **wydania swoim pracownikom upoważnień do przetwarzania danych osobowych (art. 37),**

» **przeszkolenia pracowników z zasad ochrony danychprowadzenia ewidencji osób upoważnionych do przetwarzania danych,**

» **zastosowania wymogów przewidzianych w rozporządzeniach.**

Jak widać, zleceniobiorcy dotyczy niemal cała ustawa o ochronie danych osobowych. Wyjątkiem jest spełnienie przesłanek legalności, obowiązku informacyjnego i prawa do informacji oraz rejestracja i aktualizacja zbiorów danych osobowych (zbiór może zarejestrować tylko administrator danych).

Zleceniobiorca biorąc na siebie przetwarzanie „cudzych" danych osobowych w celu realizacji umowy zobowiązuje się w zasadzie do stosowania całej ustawy o ochronie danych osobowych.



Obowiązki zleceniodawcy

Obowiązkiem zleceniodawcy, czyli administratora danych osobowych, jest zgłoszenie aktualizacji zbiorów danych osobowych i ujawnienie informacji dotyczących podmiotu, któremu powierzono przetwarzanie (o ile powierzono do przetwarzania dane osobowe ze zbioru podlegającego rejestracji w GIODO). Wynika to z treści art. 41 ust. 1 pkt 2:

Zgłoszenie zbioru danych do rejestracji powinno zawierać [...] oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru, a w przypadku powierzenia przetwarzania danych podmiotowi,

o którym mowa w art. 31 [...] oznaczenie tego podmiotu i adres jego siedziby lub miejsca zamieszkania.

W konsekwencji tego zapisu informacja o współpracujących z przedsiębiorstwem podmiotach przestaje być tajemnicą. Warto zapamiętać, że jeśli w umowie o współpracy znajduje się zapis „zleceniodawca powierza zleceniobiorcy przetwarzanie danych osobowych", stanowi on jednocześnie powierzenie przetwarzania danych osobowych. Z pozoru wydaje się to mało znaczące, jednak oznacza to, że przyjmujący zlecenie, zobowiązany jest do spełnienia wszystkich wymagań ustawowych związanych z ochroną danych osobowych. I to jeszcze zanim otrzyma dane osobowe od zleceniodawcy! Taki sposób nie jest to, co prawda, rekomendowany jako zawarcie umowy powierzenia, ale trzeba wiedzieć, że jest wiążący. Między innymi z tego powodu należy bardzo dokładnie czytać umowy, zwracając uwagę nawet na z pozoru mało istotne zapisy.

Jak bezpiecznie prowadzić marketing?

Względem własnych klientów nie trzeba zbierać żadnych dodatkowych zgód na działalność marketingową – jest ona dozwolona. Jednak, wykorzystując posiadane dane, można promować jedynie własne produkty lub usługi.

Jeśli klient zawarł z przedsiębiorcą umowę, kupił towar lub usługę, prawo zezwala przedsiębiorcy (administratorowi danych) na marketing bezpośredni własnych produktów i usług. Takie działanie traktowane jest jako tzw. usprawiedliwiony prawnie cel administratora danych (art. 23 ust. 1 pkt 5 oraz art. 23 ust. 4 pkt 1)[20]. Sformułowanie „własnych produktów" nie oznacza, że podmiot musi być producentem wszystkich oferowanych artykułów, ważne, że znajdują się one bezpośrednio w jego ofercie i można je od niego kupić.

20) - O ile marketing własnych towarów i usług jest dopuszczalny, to inne akty prawa mogą ograniczać pewne formy marketingu, np. marketing za pomocą poczty elektronicznej reguluje art. 10 ustawy o świadczeniu usług drogą elektroniczną.

Działania marketingowe na podstawie ww. artykułów można prowadzić do czasu, gdy osoba, której dane wykorzystujemy (klient) wyrazi wobec tego sprzeciw. Taki sprzeciw należy odnotować i w przyszłości respektować. Mimo coraz większej świadomości przepisów o ochronie danych osobowych,

nadal nie wszyscy klienci zdają sobie sprawę, że taki marketing jest zgodny z przepisami. Czasem są wręcz przekonani, że jest to naruszenie ustawy, bo nie wyrażali żadnej odrębnej zgody marketingowej.

Przez „marketing bezpośredni" rozumie się przekaz spersonalizowany, skierowany do konkretnej osoby. Nie będą nim zatem np. ulotki wkładane do skrzynek pocztowych.

Cudze towary i usługi, czyli te, które sprzedaje lub świadczy inny podmiot, można promować tylko za zgodą klienta. W zasadzie powinna być to zgoda na prowadzenie marketingu. Umowa zawarta z inną firmą w sprawie wzajemnej promocji nie będzie wystarczającą podstawą do uznania, że wysyłanie oferty marketingowej firmy współpracującej jest prawnie usprawiedliwionym celem administratora danych. Przykładowo, jeśli podmiot świadczący usługi pośrednictwa w obrocie nieruchomościami zawrze z bankiem umowę o współpracy w celu promowania jego oferty produktowej i chciałby tę ofertę przesyłać kupującym mieszkania, musiałby mieć na to zgodę swoich klientów. Informacja o ofercie banku jest bowiem informacją marketingową banku, a nie pośrednika.

Należy jednak być tutaj świadomym ograniczeń, jakie nakładają inne przepisy prawa. Przykładowo, przedsiębiorca może mieć podstawę do prowadzenia marketingu, np. wspomniany wcześniej usprawiedliwiony cel administratora lub zgoda osoby, a mimo to nie

będzie mógł prowadzić marketingu przez telefon, gdyż staną mu na drodze przepisy art. 172 prawa telekomunikacyjnego. Aby móc prowadzić marketing przez telefon należy uzyskać uprzednią zgodę osoby.

Marketing w grupach kapitałowych

Grupa kapitałowa to co najmniej dwa przedsiębiorstwa, które pozostają ze sobą w związku kapitałowym. Grupa składa się z jednostki dominującej i jednostek zależnych (kontrolowanych przez jednostkę dominującą) lub stowarzyszonych. Jednostką dominującą może być spółka akcyjna, spółka z o.o. lub inna spółka kapitałowa (jawna lub komandytowa), która ma jedną bądź więcej spółek zależnych (stowarzyszonych). Obowiązujące prawo precyzuje obowiązki grupy kapitałowej w rozdziale 6. ustawy o rachunkowości.

Ustawa o ochronie danych osobowych w ogóle nie zauważa istnienia grup kapitałowych. Jedna firma może być właścicielem innej firmy w części lub całości (powiązania kapitałowe), ale nie oznacza to automatycznie, że jest także właścicielem lub współwłaścicielem danych osobowych przetwarzanych przez podmiot zależny.

W praktyce **wymiana danych osobowych w grupie kapitałowej odbywa się tak, jakby były to zupełnie obce sobie podmioty**.

› Jak i kiedy rejestrować zbiory danych osobowych?

W Polsce funkcjonuje prawie 2 mln aktywnych przedsiębiorców[21]. Bez wątpienia większość z nich posiada zbiory danych podlegające rejestracji, jednak w rejestrze GIODO znajduje się jedynie ok. 150 tys. zbiorów.

21) - Wraz z nieaktywnymi przedsiębiorcami liczbę tę szacuje się na ok. 4 mln.

Warto wiedzieć, że niezgłoszenie zbioru do rejestracji stanowi przestępstwo i jest karane z art. 53 ustawy o ochronie danych osobowych. Natomiast brak aktualizowania zgłoszonego zbioru może prowadzić do wszczęcia postępowania administracyjnego przez GIODO. Dlatego też podmiot, który przetwarza dane osobowe powinien wiedzieć, czym jest zbiór danych oraz kiedy i jak go rejestrować.

Niezależnie od tego, czy dane są rozproszone (znajdują się w różnych miejscach) czy też podzielone funkcjonalnie (w różnych modułach systemu informatycznego lub firmowych departamentach), zbiorami danych osobowych są:

- **zestawy danych dotyczących osób fizycznych (pewna ilość informacji),**
- **zestawy danych, posiadające strukturę (określoną budowę) i określone kryteria dostępu (np. możliwość wyszukiwania według określonego klucza).**

Zbiory różnią się od siebie trzema głównymi czynnikami:

- **celem przetwarzania danych,**
- **podstawą prawną pozwalająca przetwarzać dane,**
- **zakresem przetwarzanych danych.**

Zbiór danych nie jest tożsamy z bazą danych. Jest pojęciem znacznie szerszym – może obejmować wiele systemów i baz informatycznych, a także papierowe formy dokumentów.

Zgłoszenie zbioru danych i jego aktualizacje można wysyłać do GIODO na trzy sposoby:

- **tradycyjnie – w formie papierowej,**
- **za pomocą internetowej aplikacji e-GIODO,**

» **za pomocą internetowego programu e-GIODO (wypełnienie i wysyłka w pełni elektronicznie).**

Najwygodniej jest wypełnić i wysłać wniosek elektronicznie, a w ramach potwierdzenia skorzystać również z formy tradycyjnej, wysyłając do GIODO podpisaną wersję papierową. Tak składa wnioski większość podmiotów.

Ustawa rozróżnia dwa rodzaje zbiorów:

» **zbiór z danymi zwykłymi,**

» **zbiór, zawierający dane wrażliwe.**

Jeśli mamy do czynienia ze zwykłymi danymi osobowymi, możemy je przetwarzać od razu po wysłaniu zgłoszenia rejestracyjnego. W przypadku danych wrażliwych musimy poczekać na zarejestrowanie tego zbioru (art. 46 ustawy).

Każdy zbiór danych osobowych należy zarejestrować, chyba że stanowi on wyjątek opisany w art. 43 ust. 1:

Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych: (...)

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, (...)*

8. *przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,*

9. *powszechnie dostępnych, (...)*

10. *przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.*
11. *przetwarzanych wyłącznie w formie papierowej (jeśli nie ma w nich danych wrażliwych)*

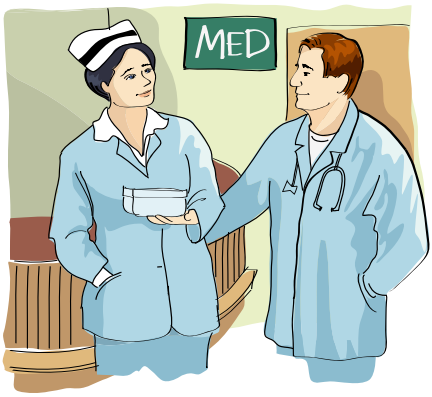
Dane osób przetwarzane w związku z ich zatrudnieniem stanowią zbiór danych osobowych. Zbiór ten jest jednak zwolniony z rejestracji na podstawie art. 43 ust 1 pkt 4.

Zwolnienie z rejestracji obejmuje zbiór zawierający dane mające związek z zatrudnieniem, a więc także dane kandydatów do pracy i dane osób już niepracujących. Obejmuje też dane osób zatrudnionych na podstawie umów cywilnoprawnych (umowa zlecenie, umowa o dzieło, umowa agencyjna, praktykanci).

Z rejestracji zbioru zwolnieni są też m.in. administratorzy danych powszechnie dostępnych. Chodzi tu o dane, które w wyniku przetwarzania stają się powszechne, nie zaś o dane, które w momencie zbierania były powszechnie dostępne. Na swojej stronie internetowej GIODO zauważa, że **zwolnienie to miałoby zastosowanie tylko w przypadku, gdyby wszystkie dane przetwarzane w danym zbiorze były powszechnie dostępne u danego administratora danych, tj. upubliczniane przez tego administratora**[22].

22) - http://www.giodo.gov.pl/560/id_art/4627/j/pl/

W efekcie zbiór danych osobowych zebranych z Internetu, różnego rodzaju katalogów, czy nawet rejestrów publicznych należy zgłosić do rejestracji.



Zbiór z informacjami pobranymi z Centralnej Ewidencji i Informacji o Działalności Gospodarczej należy zarejestrować, chyba że ten zbiór jest upubliczniony tj. gdy dane w nim zawarte są w całości powszechnie dostępne.

Nowością jest brak obowiązku zgłaszania zbiorów do rejestracji, jeśli w organizacji powołano ABI i zgłoszono go GIODO do rejestracji (art. 34 ust. 1a). Wówczas jednak ABI musi prowadzić rejestr zbiorów i udostępniać go wszystkim zainteresowanym. Trzeba także pamiętać, że zwolnienie z rejestracji dotyczy wyłącznie zbiorów, które nie zawierają danych wrażliwych.

› Polityka bezpieczeństwa i instrukcja

Wymagane ustawą politykę i instrukcję bezpieczeństwa możemy porównać do wewnętrznych aktów prawa – ustawy i rozporządzenia.

Wyobraźmy sobie ekskluzywną restaurację. Co dla jej właściciela będzie szczególnie ważne? Jakie istotne zasady postępowania chciałby przekazać swoim pracownikom? Pierwsza myśl to taka, aby przygotowanie posiłków odbywało się w higienicznych

warunkach, wnętrze pozostawało czyste oraz aby zachowano pewną estetykę. Ważne byłoby też na pewno stosowanie odpowiednich receptur potraw, aby zawsze smakowały i były przygotowane tak samo dobrze. Zapewne ważny byłby także określony standard obsługi klienta i postępowanie w przypadku reklamacji, a także wiele innych zasad, zapewniających bezproblemowe prowadzenie restauracji. Wszystkie te elementy to sposoby właściciela na uzyskanie i utrzymanie określonego poziomu usług, a także wyraz jego woli stosowania się do ustalonych założeń. Takie kluczowe założenia można określić mianem polityki.

W kolejnym kroku ustalone założenia przekładają się na szczegółowe zasady. Przykładowo, posiłki należy przygotowywać w czystej kuchni, ze świeżych składników, a pracownicy powinni stosować odpowiednie ubranie robocze (czepek, fartuch), etc. Te zasady, ze względu na szczegółowość, dzielą się na tzw. standardy i procedury. W tym konkretnym przypadku standard określa, że przed rozpoczęciem pracy należy umyć ręce, procedura zaś uszczegóławia, jak i czym je umyć (np. płynem Impuls 10 SD). Taka szczegółowa dokumentacja to po prostu instrukcja utrzymania czystości i higieny.

Ustawa o ochronie danych osobowych wymaga, aby podmiot przetwarzający dane osobowe przygotował politykę bezpieczeństwa i instrukcję zarządzania systemem. Rola tych dokumentów jest bardzo istotna i warto, aby były to praktyczne regulacje nie tylko spełniające wymogi ustawy, ale dobrze służyły organizacji. Z tego powodu polityka i instrukcja nie powinny być tworzone jedynie na potrzeby ewentualnej kontroli GIODO.

W przypadku braku wymaganej przez rozporządzenie dokumentacji administratorowi danych grozi najczęściej postępowanie administracyjne, nie jest jednak wykluczone również postępowanie karne. Dokumentacja uznawana jest za formę zabezpieczenia danych osobowych, a brak odpowiednich zabezpieczeń może być karany na podstawie art. 52 ustawy o ochronie danych osobowych.

Polityka bezpieczeństwa powinna odnosić się całościowo do problemu zabezpieczenia danych, tj. obejmować swoim zakresem dane przetwarzane tradycyjnie i dane przetwarzane w systemach informatycznych. Rozporządzenie obejmuje ogólnie zabezpieczenie danych, szczególnie uwzględniając przetwarzanie danych osobowych z pomocą komputerów. Należy się stosować do opisanych w nim zasad, nawet jeśli do przetwarzania danych nie używa się systemów informatycznych.

Obowiązek przygotowania polityki bezpieczeństwa dotyczy każdego, kto przetwarza dane osobowe, nawet jeśli nie używa do tego celu komputerów.

Celem polityki jest **wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonywać obowiązki w zakresie zabezpieczenia danych osobowych**. Dokument polityki bezpieczeństwa powinien deklarować zaangażowanie kierownictwa i wyznaczać podejście instytucji do zarządzania bezpieczeństwem informacji.

Instrukcja zarządzania systemem informatycznym

Instrukcja stanowi uszczegółowienie zasad opisanych w polityce bezpieczeństwa. O ile politykę bezpieczeństwa musi posiadać każdy administrator danych oraz podmiot, któremu powierzono przetwarzanie danych osobowych, o tyle instrukcję muszą przygotować tylko te podmioty, które przetwarzają dane osobowe z wykorzystaniem komputerów.

Na instrukcję będzie składać się wiele odrębnych dokumentów, m.in.:

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

Instrukcja stanowi udokumentowanie zastosowanych środków bezpieczeństwa. Administrator danych zobowiązany jest zapewnić, że jest taka dokumentacja, no chyba że powołał administratora bezpieczeństwa informacji – wtedy zadanie to będzie ciążyło na ABI. Podkreślmy, że zapewnienie oznacza nadzór nad tym, że ta dokumentacja jest przygotowana (nie ma znaczenia kto ją przygotuje), kompletna i aktualna.

Sprawozdanie

Jeśli w organizacji powołano ABI i zgłoszono go do rejestracji w GIODO jest on zobowiązany przygotować sprawozdanie na temat zgodności przetwarzania z przepisami o ochronie danych osobowych (art. 36a ust. 2 pkt 1 lit. a). Ustawa określa co powinno zawierać sprawozdanie (art. 36c) – są to m.in.:

- **wykaz kontroli dokonanych przez ABI,**
- **informacje o tym, kto brał udział w tych kontrolach,**
- **przedmiot i zakres sprawdzenia,**
- **opis stanu faktycznego,**
- **stwierdzone przypadki naruszenia przepisów w okresie objętym sprawozdaniem.**

W rozporządzeniu przewiduje się, że sprawdzenia mają być planowane – na okres nie krótszy niż kwartał i nie dłuższy niż rok. ABI powinien więc zaplanować, kiedy i jakie kontrole będzie w ciągu całego roku przeprowadzał w organizacji. Bez wątpienia ABI będzie miał znacznie więcej pracy, niż do tej pory, ale z pewnością będzie to z korzyścią dla organizacji, gdyż w końcu sprecyzowano, jakie informacje kierownictwo powinno otrzymywać od ABI, zaś kierownictwo będzie wiedzieć, czego może się spodziewać.

Zakres sprawdzenia jest dość szeroki, bo obejmuje m.in.:

- **wszystkie zbiory danych osobowych,**
- **zgodność z przepisami art. 23-27 i 31-35 ustawy (m.in. przesłanki legalności oraz obowiązki informacyjne)zabezpieczenie danych.**

Pewną niedogodnością może być zlecenie kontroli przez GIODO – zgodnie z przepisami, może ją zlecić w każdej chwili. W praktyce sprowadza się to do tego, że ABI będzie wykonywał kontrolę w swojej organizacji, w pewnym sensie, zamiast GIODO. Nie oznacza to jednak, że na takiej kontroli nie zjawi się GIODO. Taką możliwość daje mu art. 19b ust. 3 ustawy.

› Zabezpieczenie danych osobowych

O zabezpieczenie danych osobowych warto zadbać z wielu powodów. Po pierwsze, nieodpowiednie zabezpieczenie danych jest karane przepisami karnymi – przykładowo, art. 52 ustawy o ochronie danych osobowych podkreśla, że **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.** Po drugie, jeśli osoby, których dane dotyczą, na skutek słabych zabezpieczeń ich danych osobowych (albo braku tych zabezpieczeń) doznają szkody albo krzywdy, mogą dochodzić swoich praw w postępowaniu cywilnym. Jest to zazwyczaj problematyczne i może zaburzyć działalność organizacji.

Zabezpieczenia danych osobowych to tak obszerna materia, że na ten temat można napisać odrębną książkę, dlatego też poniżej przedstawię jedynie niektóre przykłady zabezpieczeń.

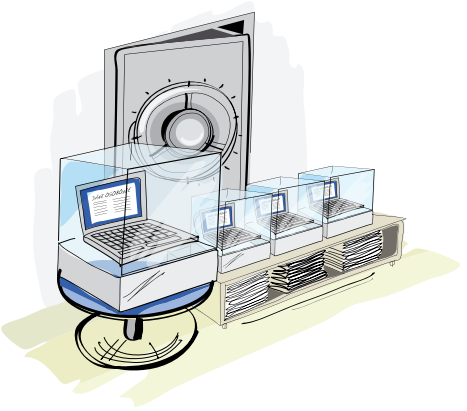
Ustawienie monitora

Wydawałoby się, że ustawienie monitora nie ma większego znaczenia dla ochrony danych osobowych. A jednak! O odpowiednim ustawieniu monitorów należy pamiętać pracując, przykładowo, w dużym budynku biurowym. Takie biurowce są czę-

sto całkowicie przeszklone, co może spowodować niezamierzone udostępnienie danych. Może się zdarzyć, że ktoś, wykorzystując aparat z dużym przybliżeniem (zoomem), sfotografuje zawartość ekranu komputera nawet z budynku naprzeciwko. Jeśli więc na komputerze są przetwarzane poufne dane, warto się przed tym zabezpieczyć. Szczególną uwagę należy zwrócić na ustawienie monitorów kadry kierowniczej, która ma dostęp do najbardziej poufnych informacji.

Zasadę odpowiedniego ustawienia monitorów podkreśla się także w poradach GIODO. Ważne jest, aby danych osobowych nie odczytała (nie zapoznała się z nimi) osoba nieupoważniona.

Warto też, aby komputer był zabezpieczony wygaszaczem ekranu na hasło – jeśli pracownik zapomni zablokować ekran, po określonym czasie wygaszacz uruchomi się samoistnie. W ten sposób nie będą wyświetlane na ekranie dane osobowe, a także uniemożliwi to dostęp do komputera osobom do tego nieupoważnionym.



Niszczenie dokumentów w niszczarce

Dokumenty zawierające ważne informacje nie powinny być wyrzucane do kosza ani na śmietnik. Aby mieć pewność, że przed zutylizowaniem nie trafią w niepowołane ręce, przed wyrzuceniem warto zadbać o ich zniszczenie. Zdarzały się przecież sytuacje, gdy dokumenty zawierające dane osobowe znajdowano na śmietnikach. Co więcej, portal Gazeta.pl opisał przypadek wypadnięcia dokumentów z ciężarówki przewożącej makulaturę: **Jezdnia, pas zieleni, przystanek – w Alejach Jerozolimskich po południu wszędzie fruwała makulatura. Jedna z ciężarówek pogubiła ładunek. [...] Wśród papierów można znaleźć zeszyty, faktury, książki szkolne oraz ulotki**[23]. Wystarczy w wyszukiwarce internetowej wpisać „dokumenty na śmietniku", aby przekonać się, że nie był to odosobniony przypadek.

Dokumenty należy niszczyć skutecznie. Najłatwiej użyć niszczarki dokumentów. Pracują one w trzech klasach ochrony (oraz siedmiu poziomach bezpieczeństwa) wg normy DIN 66399. Niszczarkę pracującą w klasie drugiej można kupić już za mniej niż 100 zł.

Niszczenie nośników danych

Elektronicznych i magnetycznych nośników danych, tak jak dokumentów papierowych, nie powinno się tak po prostu wyrzucać na śmietnik. Nawet jeśli dane zostały usunięte, należy też pamiętać aby utylizować elektronikę zgodnie z ustawą o zużytym sprzęcie elektrycznym i elektronicznym.

W przypadku taśmowych magnetycznych nośników danych (podobne do dawnych kaset wideo i magnetofonowych), na których zazwyczaj tworzy się kopie zapasowe, najlepszym sposobem utylizacji będzie rozwinięcie i pocięcie taśmy na kawałki. Szansa na to, że ktoś to poskłada jest w zasadzie żadna.

Płyty CD i DVD najlepiej zniszczyć w niszczarce (wiele z nich oferuje taką funkcjonalność) lub też po prostu przeciąć na pół nożyczkami.

Nie będzie skuteczne zniszczenie płyty przez jej porysowanie albo pomazanie flamastrem – ponieważ rysy można wypolerować, a ślady flamastra zmyć.

W przypadku odsprzedaży lub przekazania w formie darowizny firmowego komputera należy wcześniej pozbawić go danych. Niekiedy wyjmuje się w tym celu dyski i przekazuje urządzenia bez nośników, częściej jednak usuwa się z nich dane wykorzystując do tego specjalne programy.

Należy zapamiętać, że zwykłe usunięcie danych (plików i folderów), a nawet

23) - http://m.warszawa.gazeta.pl/warszawa/1,106541,11532970,Aleje_pelne_dokumentow__Rozsypany_transport_makulatury.html

sformatowanie dysku nie usuwa w rzeczywistości plików (a więc i danych osobowych) z powierzchni dysku.

Czy tzw. pełne formatowanie usuwa dane? Niestety, także nie. Jedyna różnica między formatowaniem szybkim a pełnym jest taka, że przy pełnym formatowaniu dysk jest dodatkowo sprawdzany w poszukiwaniu uszkodzonych sektorów. Aby mieć pewność, że z dysku nie da się już nic odczytać, warto skorzystać z programu **sdelete.exe**, który można za darmo pobrać z internetu[24]. Po usunięciu plików, zamiast nadpisywania dysku danymi wystarczy uruchomić ten program wydając polecenie:

sdelete.exe -p 2 -c c:\.

Cyfra „2" oznacza ile razy to samo miejsce ma zostać nadpisane, a parametr „c" określa, że na dysku należy „wyczyścić" miejsce zwolnione po usuniętych plikach[25].

› Rola szkoleń z ochrony danych osobowych

Szkolenia stanowią niezwykle istotny element ochrony danych osobowych. Przede wszystkim są wymagane przez obowiązujące prawo, gdyż zadaniem administratora danych (bądź administratora bezpieczeństwa informacji – jeśli został powołany) jest *zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.*

Szkolenia pełnią głównie funkcję zapobiegawczą, bo ataki takie jak phishing, czy wyłudzanie haseł bądź danych, odnoszą sukces głównie z braku wiedzy o podstawowych zasadach bezpieczeństwa. Można się przed nimi bronić odpowiednio szkoląc użytkowników, pokazując im, co wolno robić, jak przetwarzać dane, jakie działania są dozwolone, a co jest absolutnie niedopuszczalne.

W sytuacji naruszenia przepisów, kiedy firma zechce pociągnąć pracownika do odpowiedzialności, może się on po prostu bronić się niewiedzą. Jeśli faktycznie nie został odpowiednio przeszkolony, to wyłącza jego odpowiedzialność. Dlatego też warto szkolić pracowników z zasad bezpiecznego przetwarzania danych osobowych i każdorazowo dokumentować ten fakt stosownym zaświadczeniem.

Istotnym jest, aby przeszkolenie odbyło się przed rozpoczęciem przetwarzania danych osobowych przez pracownika. W niedużej organizacji może to być szkolenie tradycyjne. W dużych firmach lub tam, gdzie istnieje znaczna rotacja pracowników (np. centra telefoniczne) można z powodzeniem skorzystać z oferty szkoleń elektronicznych, tzw. e-learningu.

Na koniec warto podkreślić wagę polityki bezpieczeństwa danych osobowych. Właściwie przygotowana może stanowić bardzo ważny element, budujący świadomość bezpieczeństwa przetwarzania danych. Pracownicy często poszukują informacji o tym, co im wolno w zakresie przetwarzania danych, a czego nie. Czasem, mimo odbytych szkoleń, nie pamiętają o wszystkim. Warto więc, aby dokument polityki bezpieczeństwa szczegółowo omawiał wszelkie zagadnienia związane z ochroną danych osobowych oraz był powszechnie dostępny dla wszystkich zatrudnionych w danym przedsiębiorstwie czy organizacji.

24) - http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx

25) - Program należy uruchomić z tzw. terminala (Start › Uruchom › cmd.exe)

Usuwanie danych osobowych

Dane można przetwarzać do czasu, kiedy istnieje aktualna przesłanka legalności ich przetwarzania, a więc cel tego przetwarzania jest nadal aktualny. Co do zasady dane osobowe można przetwarzać, dopóki cel ich przetwarzania nie zostanie osiągnięty, co znalazło swój wyraz w art. 26 ust. 1 pkt 4 ustawy:

Administrator danych [...] w szczególności jest obowiązany zapewnić, aby dane te były: [...]

4. *przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.*

Uwagę zwraca określenie: *umożliwiającej identyfikację osób*. Nie chodzi więc o pozbywanie się wszystkich danych, a tylko tych danych, które umożliwiają identyfikację osób. Uniemożliwienie identyfikacji osób sprawia, że wszystkie pozostałe dane utracą charakter danych osobowych. O ile do większości operacji na danych potrzebna jest przesłanka legalności, o tyle dane usuwać można swobodnie, bez zgody osoby, której dane dotyczą (art. 23 ust. 1 pkt 1).

Dane osobowe przetwarzane na podstawie zgody osoby można przetwarzać, dopóki nie wygaśnie cel, dla którego zostały zebrane lub do czasu odwołania zgody. Biorąc to pod uwagę, uzyskawszy odpowiednią zgodę od osoby, dotyczące jej dane można przetwarzać bez ograniczeń czasowych.

Możliwe jest nakazanie usunięcia danych osobowych przez GIODO w drodze decyzji administracyjnej. Dzieje się tak w sytuacji, gdy GIODO uzna, że nastąpiło naruszenie przepisów o ochronie danych osobowych (art. 18 ust. 1 pkt 6).

Co zrobić gdy dane osobowe wycieką?

Co jakiś czas słychać o różnych wyciekach danych osobowych – ich przypadkowym lub celowym udostępnieniu, kradzieży, itp.. Przypadki te obejmują takie sytuacje jak:

- **kradzież lub zagubienie laptopa, tabletu, smartfona, firmowych dokumentów,**
- **włamanie do systemu komputerowego,**
- **udostępnienie danych w internecie,**
- **kradzież danych przez pracownika;**
- **udostępnienie danych w wyniku pomyłki (np. przesłanie maila do innej osoby, niż się zamierzało).**

Skutki takich zdarzeń mogą być przeróżne, w tym np.:

- **naruszenie przepisów prawa (ochrona danych osobowych, inne regulacje),**
- **negatywny wpływ na reputację organizacji,**
- **narażenie prywatności osób,**
- **zakłócenie czynności biznesowych,**
- **straty finansowe,**
- **odpowiedzialność prawna, administracyjna lub cywilna.**

Każdy pracownik i każdy podmiot współpracujący (zleceniobiorca przetwarzający dane osobowe) powinien wiedzieć, do kogo i jak zgłaszać incydenty., Czas ma w takich sytuacjach ogromne znaczenie – szybka reakcja to mniejsze straty.

Dużą wagę warto też przykładać do odpowiedniej komunikacji w sprawie naruszenia bezpieczeństwa informacji. Osoba za nią odpowiedzialna (rzecznik prasowy, ekspert ds. public relations) powinna więc ściśle współpracować z administratorem bezpieczeństwa informacji i innymi zaangażowanymi działami. Brak takiej współpracy może spowodować poważny kryzys zaufania do firmy.

Na koniec warto przypomnieć, że przestępstwa dotyczące ochrony danych osobowych są ścigane z urzędu. W związku z tym każdy, kto dowiedział się o popełnieniu takiego przestępstwa (nie tylko pokrzywdzony bądź świadek) zobowiązany jest zawiadomić o tym fakcie prokuratora lub policję. Wynika to z treści art. 304 kodeksu postępowania karnego.

Kontrola GIODO

Generalny Inspektor Ochrony Danych Osobowych ma możliwość kontrolowania nawet tych podmiotów, które nie przetwarzają żadnych danych osobowych – choćby po to, aby się upewnić, że rzeczywiście tak jest.

Generalny Inspektor może skontrolować każdy podmiot.

Oczywiste w tym świetle wydaje się, że GIODO może kontrolować też podmioty, które przetwarzają dane osobowe w imieniu przedsiębiorcy, tzw. procesorów. Wynika to zresztą bezpośrednio z art. 31 ust. 5 ustawy.

Kontrola GIODO ma miejsce najczęściej wówczas, gdy do urzędu trafią sygnały o naruszaniu przez dany podmiot przepisów ustawy o ochronie danych osobowych. Najczęstszymi sygnałami są skargi poszczególnych osób. Warto przy tym zwrócić uwagę, że złożenie skargi do GIODO wiąże się z koniecznością wniesienia stosownej opłaty, więc bardzo prawdopodobne, że najpierw taka skarga zostanie skierowana do podmiotu naruszającego ustawę, a dopiero w dalszej kolejności – gdy nie przyniesie to oczekiwanego efektu – do GIODO. Generalny Inspektor podkreśla, że skupia się przede wszystkim na kontrolowaniu podmiotów, na które wpływają skargi, bo jest to sygnał, że może w nich dochodzić do poważnego naruszania przepisów. Wynika z tego, że dbając o rzetelne podejście do skarg i reklamacji klientów w zakresie przetwarzania danych osobowych, przedsiębiorcy mogą skutecznie zmniejszyć ryzyko wpłynięcia na nich skarg i, w konsekwencji, kontroli GIODO.

Niezależnie od wpływających skarg, każdego roku GIODO wybiera różne branże lub sektory działalności, którym chce się lepiej przyjrzeć. Bodźce inicjujące kontrolę mogą pochodzić od podmiotów, z którymi GIODO podpisał stosowne porozumienia. Przykładowo, w 2012 r. zostało podpisane porozumienie z Państwową Inspekcją Pracy (PIP), która zobowiązała się m.in. do zawiadamiania GIODO o stwierdzonych, w czasie swoich kontroli, nieprawidłowościach w zakresie zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Rok wcześniej zawarto porozumienie z Najwyższą Izbą Kontroli (NIK), na mocy którego strony zobowiązały się do wzajemnego przekazywania sobie informacji o nieprawidłowościach, które mogą stanowić przedmiot ich zainteresowania[26].

Kontrole, jakie mogą wystąpić to:

- **kontrola z urzędu (własna inicjatywa GIODO, rozpatrywanie zgłoszeń rejestracyjnych zbiorów, skargi poszczególnych osób),**
- **kontrola sprawdzająca (jeśli GIODO nakazał wcześniej usunięcie uchybień),**
- **kontrola na wniosek (np. prokuratury, Państwowej Inspekcji Pracy, osoby pokrzywdzonej).**

Kontrole mogą różnić się zakresem:

- **kontrola kompleksowa – dotyczy wszystkich zbiorów danych osobowych i wszystkich wymogów ustawy o ochronie danych osobowych,**
- **kontrola częściowa – dotyczy określonych zagadnień, np. wybranego obszaru funkcjonowania organizacji lub, w opcji bardziej zawężonej, np. sprawdzenia legalności pozyskiwania danych czy sposobu realizacji obowiązku informacyjnego wobec osób, których dane są przetwarzane.**

Jeśli chodzi o formę, można wyróżnić dwa rodzaje kontroli:

- **kontrola na miejscu – tradycyjna forma kontroli,**
- **kontrola korespondencyjna („zdalna") – udzielanie pisemnych wyjaśnień GIODO.**

Zazwyczaj podmiot kontrolowany informowany jest o planowanej kontroli z pewnym wyprzedzeniem telefonicznie. Następnie na piśmie (czasem faksem) przedstawiany jest przedmiot kontroli, potwierdzenie terminu i prośba o przygotowanie określonych materiałów[27].

Nie ma obowiązku odpisywania

26) - http://www.giodo.gov.pl/259/id_art/5767/j/pl25) http://www.giodo.gov.pl/597/id_art/4451/j/pl

27) - Generalny Inspektor Ochrony Danych Osobowych, ABC zasad kontroli przetwarzania danych osobowych, Wydawnictwo Sejmowe, Warszawa 2007, s. 19.

Przepisy o ochronie danych osobowych, przewidujące kary

Art. 49 – przetwarzanie danych przez nieuprawnionego.

Przestępstwo opisane w artykule 49 jest przestępstwem umyślnym, dokonanym z rozwagą, celowo. Nieuprawniony to ten, który przetwarza dane bez spełnienia tzw. przesłanek legalności przetwarzania. Będzie to mieć miejsce, przykładowo, gdy żaden przepis prawa nie zezwala na przetwarzanie danych, nie została też uzyskana zgoda osoby, której dane dotyczą. Grozi za to grzywna, kara ograniczenia, a nawet pozbawienia wolności do 3 lat, jeśli w grę wchodzą dane wrażliwe.

Art. 51 – udostępnianie danych osobom nieuprawnionym.

Bardzo ważny przepis, stanowiący ochronę przed udostępnianiem lub umożliwianiem dostępu do danych osobom nieupoważnionym. Czyn ten może być popełniony zarówno umyślnie, jak też nieumyślnie, np. przez niedbalstwo lub niewiedzę. Artykuł dotyczy wszystkich, którzy powinni chronić dane osobowe w procesie ich przetwarzania – administratora zbioru danych osobowych i procesora jako administrujących zbiorem oraz osoby upoważnione do przetwarzania jako osoby zobowiązane do ochrony danych osobowych. Karą za złamanie tego przepisu może być grzywna, kara ograniczenia wolności, pozbawienia wolności do roku w przypadku działania nieumyślnego i do 2 lat w przypadku działania umyślnego.

Art. 52 – naruszenie obowiązku zabezpieczenia danych.

Ustawodawca odróżnia udostępnienie lub umożliwienie dostępu do danych od braku zabezpieczenia danych. Art. 51 nakierowany jest na nieumożliwianie dostępu do danych osobowych, zaś art. 52 ochronę kieruje na bezpieczne i niezakłócone przechowywanie danych, co podkreśla użycie słów „zabranie", „uszkodzenie", „zniszczenie".

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.

Złamaniem tego przepisu jest niezabezpieczenie danych zgodnie z wymogami art. 36 ustawy, w tym na przykład: brak hasła do systemu informatycznego, hasła niespełniające wymagań rozporządzenia, niezabezpieczenie dokumentów zawierających dane osobowe w szafie, sejfie lub niezamknięcie pomieszczenia, w którym znajdują się dane osobowe.

Art. 53 – niezgłoszenie danych do rejestru.

Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Przepis ten ma zastosowanie, gdy nie zostanie zgłoszony do rejestracji zbiór danych osobowych. Nie ma znaczenia, czy zbiór został zgłoszony poprawnie, czy nie. Dla sprawy istotny jest sam fakt zgłoszenia, tj. jego wysłanie.

Art. 54 – niedopełnienie obowiązku poinformowania.

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.

Obowiązek informacyjny wobec osoby, której dane dotyczą powstaje na skutek zapisów art. 24 i 25 ustawy, które zobowiązują administratora danych do informowania m.in. o adresie swojej siedziby, celu zbierania danych, prawie dostępu do swoich danych, itd. Jest on też elementem art. 32 i 33, które zobowiązują administratora danych osobowych do udzielenia informacji osobie na jej wniosek. Czyn zabroniony, opisany w tym artykule, można popełnić nie informując, przy zbieraniu danych osobowych, o tym kto zbiera dane (informacja o ADO), gdzie ma swoją siedzibę, a także o tym, że osoba, której dane są przetwarzane ma prawo wglądu do nich i ich modyfikowania.

na zawiadomienie o kontroli. Wyjątkiem jest sytuacja, gdy kontrolowanemu podmiotowi, z uzasadnionych przyczyn, nie odpowiada ustalony przez GIODO termin. Można wówczas wnioskować o jego zmianę.

Przygotowując się do kontroli, należy przede wszystkim zacząć od przeanalizowania zagadnień z art. 49 – 54 ustawy o ochronie danych osobowych, których niedopełnienie grozi postępowaniem karnym. W pierwszej kolejności należy zadbać m.in. o posiadanie prawa do przetwarzania danych, właściwe zabezpieczenie danych (tak, aby osoby nieupoważnione nie miały do nich dostępu), rejestrację zbiorów oraz dopełnianie obowiązków informacyjnych względem osób, których dane są przetwarzane. Wszystkie pozostałe wymagania można uznać za mniej groźne, bo konsekwencją ich nierealizowania jest postępowanie administracyjne, mniej dotkliwe od karnego.

W czasie kontroli inspektorzy GIODO zobowiązani są posiadać stosowne upoważnienie – imienne, terminowe (ważne na okres danej kontroli) i dotyczące kontroli w konkretnym przedsiębiorstwie. Upoważnienie powinni okazać wraz z legitymacjami służbowymi inspektorów. Nie należy obawiać się legitymowania kontrolerów i sprawdzania ich upoważnień. Takie działanie należy przyjąć za dobrą praktykę, zaś inspektorzy powinni do nich podejść z wyrozumiałością.

Prawa kontrolerów są bardzo szerokie. Mają oni m.in. prawo wstępu do pomieszczeń firmy, mogą żądać udzielenia wyjaśnień, a także uzyskiwać dostęp do wszelkich danych, mających związek z kontrolą i przeprowadzania oględzin (art. 14 ustawy).

Podstawowym obowiązkiem przedsiębiorcy jest umożliwienie przeprowadzenia kontroli. Nie można jej utrudniać ani uniemożliwiać, bo to jest karane z art. 54a ustawy.

Po okazaniu ważnej legitymacji służbowej i upoważnienia, należy umożliwić inspektorom przeprowadzenie kontroli, tj.:

- **składać niezbędne wyjaśnienia pisemne albo ustne,**
- **udostępnić żądane dokumenty do wglądu albo ich kopie,**
- **pozwolić na dokonanie oględzin systemów informatycznych, urządzeń i nośników służących do przetwarzania danych osobowych,**
- **umożliwić wgląd w dane osobowe.**

Kontrola kończy się sporządzeniem protokołu (art. 16 ust.1 ustawy), przy czym kontrolowany może wnieść do protokołu umotywowane zastrzeżenia i uwagi.

Jeśli w trakcie kontroli stwierdzono nieprawidłowości, zgodnie z art. 61 § 4 Kodeksu postępowania administracyjnego, następuje wszczęcie postępowania administracyjnego. Kontrolowany zostaje o tym poinformowany pisemnie, otrzymuje również opis uchybień stwierdzonych w trakcie kontroli. W wyniku postępowania wydawana jest decyzja administracyjna, która może nakazać „przywrócenie stanu zgodnego z prawem" (usunięcie niezgodności z ustawą) lub umorzyć (zamknąć) postępowanie.

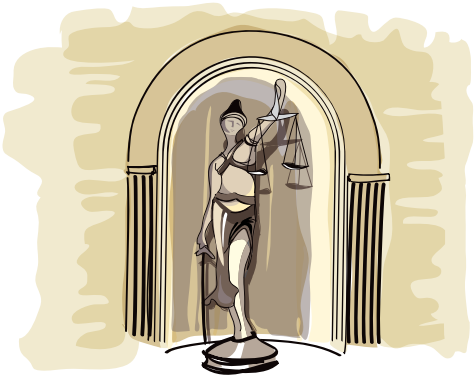
Jak wynika z przepisów prawa, czynności kontrolne są dla ustawodawcy niezwykle ważne. Art. 15 ust. 1 ustawy o ochronie danych osobowych nakazuje podmiotowi umożliwienie przeprowadzenia kontroli. Utrudnianie lub uniemożliwienie przeprowadzenia kontroli od 2012 r. jest karane nowymi przepisami karnymi. Udaremnianie i utrudnianie kontroli oznacza, odpowiednio, całkowite uniemożliwienie wykonania kontroli oraz doprowadzenie do tego, że kontrola napotka na przeszkody, uniemożliwiające jej osiągnięcie celu. Przykładem takiego działania może być zlecenie służbom ochrony niewpuszczenia inspektorów GIODO na teren przedsiębiorstwa. Utrudnianiem kontroli będzie też odmówienie udzielenia wyjaśnień czy niedopuszczenie do oględzin urządzeń, nośników danych, itp. Jeśli kontrolowany doprowadzi do udaremnienia albo utrudnienia kontroli niechcący, nie mając takiego zamiaru, nie będzie wówczas odpowiadał z art. 54a.

Nowością od 1 stycznia 2015 r. jest możliwość żądania przez GIODO dokonanie przez administratora bezpieczeństwa informacji „sprawdzenia" na ile organizacja zapewnia zgodność z przepisami dotyczącymi ochrony danych osobowych (art. 19b ust. 1). Po jego dokonaniu należy przygotować sprawozdanie i przesłać je do GIODO.

Gdy nie zastosujesz się do poleceń GIODO...

Jeśli po kontroli, w ramach postępowania administracyjnego, Generalny Inspektor Danych Osobowych nakaże przywrócić stan zgodny z prawem, a kontrolowany się nie zastosuje do tego nakazu, GIODO ma prawo podjąć działania egzekucyjne – wystawia tytuł wykonawczy i kieruje do właściwego organu wniosek o wszczęcie postępowania egzekucyjnego. Środki egzekucyjne, jakie mogą zostać zastosowane, to:

- **grzywna,**
- **wykonanie zastępcze,**
- **przymus bezpośredni.**



Grzywna jest karą najprostszą do zastosowania. Organ egzekucyjny wystawia postanowienie o zastosowaniu grzywny, a gdy nie zostanie ona uiszczona, kieruje tytuł wykonawczy do właściwego urzędu skarbowego, w wyniku czego zasądzona kwota zostanie zajęta z rachunku bankowego ukaranego. W przypadku osoby fizycznej maksymalna wysokość grzywny wynosi 10 tys. zł, w przypadku osób prawnych i jednostek organizacyjnych, nieposiadających osobowości prawnej (spółki z o.o., spółki akcyjne) – 50 tys. zł.

Grzywny można nakładać wielokrotnie. W jednym postępowaniu egzekucyjnym ich łączna kwota wynosi do 50 tys. zł w przypadku osób fizycznych i do 200 tys. zł w przypadku osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej.

Odpowiedzialność karna, administracyjna i cywilna

W przypadku naruszenia ustawy o ochronie danych osobowych należy się liczyć z odpowiedzialnością administracyjną, cywilną i karną. Postępowanie administracyjne to wszystkie działania, jakie wobec administrującego danymi podejmować będzie bezpośrednio Generalny Inspektor Ochrony Danych Osobowych. Postępowanie cywilne będzie mieć miejsce, gdy w wyniku niedopełnienia obowiązków ustawowych zostaną poszkodowane osoby, których dane przetwarzano – poszkodowani mogą wówczas dochodzić swoich praw na drodze postępowania cywilnoprawnego. Postępowanie karne wynika z opisanych powyżej zapisów ustawy o ochronie danych osobowych – warto więc je znać i stosować w praktyce.

› Planowane zmiany w prawie

Obecnie zasady ochrony danych osobowych w Unii Europejskiej reguluje Dyrektywa Parlamentu Europejskiego i Rady z 24 października 1995 r. (95/46/WE) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Dyrektywa jest w pewnym sensie matką europejskich, w tym polskiej, ustaw o ochronie danych osobowych.

Niedługo minie 20 lat od kiedy obowiązuje, nie dziwi więc, że wymaga nowelizacji – głównie ze względu na globalizację i rozwój nowoczesnych technologii, w tym szczególnie rosnącą popularność i dostępność technologii mobilnych.

4 listopada 2010 r. Komisja Europejska przedstawiła strategię zwiększenia skuteczności unijnych przepisów dotyczących ochrony danych. Następnie przez dwa lata zbierano uwagi do tych propozycji, również w formie konsultacji społecznych. W rezultacie 25 stycznia 2012 r. Komisja Europejska przedstawiła projekt kompleksowej reformy unijnych przepisów o ochronie danych, w tym także dokument **Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)**.[28)]

Według Komisji Europejskiej, wdrożenie przepisów z 1995 r. przez każde z 27 państw członkowskich na swój sposób, doprowadziło do rozbieżności w ich egzekwowaniu i kosztownymi obciążeniami administracyjnymi. Rozwiązaniem miałby być jeden spójny akt prawny – rozporządzenie europejskie.

12 marca 2014 r. Parlament Europejski 621 głosami za, 10 przeciw i 22 wstrzymującymi się od głosu przyjął wniosek Komisji.

Największa zmiana polegać będzie na zastąpieniu Dyrektywy 95/46/WE rozporządzeniem. Dyrektywa stanowi swojego rodzaju wytyczne, które każde państwo członkowskie Unii Europejskiej musi wdrożyć za pomocą wewnętrznych aktów prawa (w Polsce są to ustawy). Rozporządzenie europejskie jest natomiast aktem, który bezpośrednio obowiązuje w każdym z państw członkowskich. Proponowana zmiana oznaczała, że ochrona danych osobowych w każdym kraju Unii Europejskiej będzie na identycznym poziomie.

Wiele zaproponowanych zmian ma charakter rewolucyjny. Przykładowo, w przypadku naruszenia bezpieczeństwa danych osobowych, administrator miałby obowiązek zgłoszenia takiego naruszenia organowi nadzorczemu (w Polsce – GIODO) bez nieuzasadnionej zwłoki i, jeśli jest to możliwe, nie później niż w ciągu 24 godzin od momentu uzyskania informacji o tym naruszeniu. Jeśli organ nadzorczy nie zostanie zawiadomiony w ciągu 24 godzin, do zgłoszenia należy dołączyć umotywowane wyjaśnienie. Za brak zgłoszenia przewiduje się bardzo wysokie kary.

Rozporządzenie wprowadza także **obowiązek powołania inspektora ochrony danych osobowych** (**odpowiednik administratora bezpieczeństwa informacji**) dla sektora publicznego, dużych firm w sektorze prywatnym oraz wszędzie tam, gdzie główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, wymagających regularnego i systematycznego monitorowania. Co ważne, pracodawca nie będzie mógł zwolnić inspektora w okresie jego kadencji (4 lata na podstawie umowy o pracę, 2 lata na podstawie umowy zlecenia), chyba że nie wywiązywałby się on ze swoich obowiązków. Inspektor będzie podlegał bezpośrednio kierownictwu firmy. **Bardzo interesujący jest fakt, że dane inspektora** (**imię i nazwisko oraz dane kontaktowe**) **mają być publicznie dostępne**. Należy je również zgłosić GIODO – inspektor będzie stanowił dla GIODO punkt kontaktowy. Co więcej, w zakresie obowiązków inspektora znajdzie się również komunikacja z klientami w zakresie ochrony danych.

Innym **ciekawym wymogiem jest wdrożenie przez administratora danych osobowych mechanizmów służących zapewnieniu przestrzegania terminów usunięcia danych osobowych** lub okresowego przeglądu, dokonywanego w celu ustalenia potrzeby przechowywania danych. Osoby, których dane będą zbierane, będą musiały być poinformowane o tym, jak długo ich dane będą przetwarzane.

28) - http://europa.eu/rapid/press-release_IP-12-46_pl.htm

Bardzo interesujące są też **kary za niezgodność z przepisami. Mogą one wynieść do 100 mln EUR lub do 5% rocznego światowego obrotu przedsiębiorstwa. Na szczęście w przypadku pierwszego naruszenia można liczyć jedynie na ostrzeżenie pisemne**.

Wydaje się, że na efekt tych zmian będzie trzeba jeszcze trochę poczekać, warto jednak na bieżąco monitorować propozycje i dyskusje na ten temat a, przede wszystkim, zadbać o zgodność z obecną (znowelizowaną) ustawą o ochronie danych osobowych. Dzięki temu łatwiej będzie, za jakiś czas, dostosować się do nowego prawa.

› Zakończenie

I tak doszliśmy do końca poradnika. **Miał on za zadanie dostarczenie Państwu podstawowej wiedzy z zakresu ochrony danych osobowych** – jak przetwarzać dane osobowe oraz jak je zabezpieczać, aby być w zgodzie z obowiązującym prawem. Przedstawiliśmy także zmiany, które obowiązują od 1 stycznia 2015 r. Materiał uzupełniały praktyczne rady, wskazujące najważniejsze aspekty stosowania ustawy o ochronie danych osobowych. Wierzę, że była to dla Państwa cenna lektura.

Leszek Kępa

– autor książki **„Ochrona danych osobowych w praktyce”** oraz współautor książki **„Bezpieczeństwo systemów e-commerce, czyli jak bez ryzyka prowadzić biznes w internecie”**. Ekspert ds. ochrony danych osobowych, zawodowo zajmujący się przede wszystkim zagadnieniami dotyczącymi ochrony danych osobowych, zarządzaniem bezpieczeństwem informacji, badaniami bezpieczeństwa systemów i aplikacji, a także zarządzaniem ciągłością działania. Posiada, uznane na całym świecie, certyfikaty CISA (Certified Information Security Auditor) i CISM (Certified Information Security Manager). Jest członkiem ISACA oraz Podkomisji Ochrony Danych i Standaryzacji Informacji Polskiej Izby Ubezpieczeń. Absolwent Szkoły Głównej Handlowej, Politechniki Częstochowskiej i Akademii Podlaskiej.

Książka „Ochrona danych osobowych w praktyce“

wyczerpująco przedstawia wszystkie istotne zagadnienia dotyczące przetwarzania danych osobowych. Materiał w niej zawarty adresowany jest przede wszystkim do przedsiębiorców, ale także wszystkich innych osób, które decydują o zbieraniu, przetwarzaniu i zabezpieczaniu danych osobowych. Opisane w książce zasady mogą być stosowane przez każdy podmiot, zarówno prywatny jak i publiczny, przetwarzający dane osobowe, bez względu na rodzaj i charakter prowadzonej działalności.

Z książki czytelnik dowie się m.in.:

- *jak racjonalnie stosować się do wymagań ustawy,*
- *co robić, gdy dane osobowe wyciekną,*
- *w jaki sposób przygotować zgodę na przetwarzanie danych,*
- *jak, krok po kroku, zarejestrować zbiory danych,*
- *jak zabezpieczać dane,*
- *jak wygląda kontrola GIODO,*
- *co grozi za nieprzestrzeganie przepisów,*
- *jak przygotować się na przyszłe zmiany w prawie.*

Książka dostępna jest w wielu księgarniach w całej Polsce, można także kupić ją w internetowej księgarni wydawnictwa — *https://www.facebook.com/dane.osobowe*

Ochrona Danych Osobowych

BEZPIECZEŃSTWO INFORMACJI

AUDYT

Zakończony raportem zawierającym niezależną ocenę stanu faktycznego, opis niezgodności oraz praktyczne rekomendacje.

DOKUMENTACJA

Zestaw indywidualnie przygotowanych procedur i wymaganych dokumentów, uwzględniających strukturę organizacyjną oraz spełniających szczegółowe wymagania przepisów prawa.

SZKOLENIA

Administratorów (ABI, ADO i ASI) w formule otwartej - szkolenia i warsztaty. Dla pracowników w formie szkoleń zamkniętych lub e-learning.

EGZAMIN

Potwierdzający kompetencje w zakresie praktycznego stosowania przepisów oraz projektowania, budowania i nadzoru nad systemem ochrony danych osobowych.

WSPARCIE

Aktywna pomoc w wypełnianiu obowiązków nałożonych na ABI lub ADO.

ODO24.pl

tel. 22 740 99 99

Nasza firma przekazuje 1% przychodu na rzecz szlachetna PACZKA