Jak w praktyce i zgodnie z prawem przetwarzać

dane osobowe

Autor **Leszek Kępa**

› Spis treści

› 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. 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 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.

Przepisy prawa mogą utrudniać polskim przedsiębiorcom konkurowanie z zagranicznymi firmami.[3)]

3) 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 którego imieniu 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.

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.[7)]

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.

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".*[8)]

Podmiot, który powołał i zgłosił do rejestracji ABI jest zwolniony z obowiązku rejestracji zbiorów danych

7) Z dniem 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 podobnej, jak robi to GIODO.

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

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 mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.[10)] Wszystkie pozostałe informacje to dane zwykłe. W ramach ciekawostki warto dodać, że informacja o tym, że osoba nigdy nie była karana również stanowi dane wrażliwe.

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).**

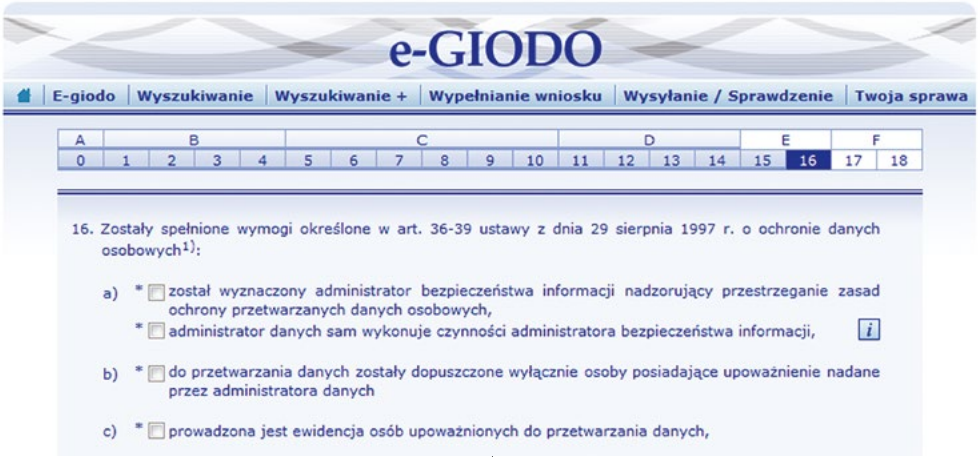
Powyższy wykaz operacji jest jedynie przykładowy. Przetwarzaniem mogą być dowolne działania, wystarczy, że są wykonywane na danych osobowych. Uwagę w definicji zwraca określenie: **zwłaszcza te, które wykonuje się w systemach informatycznych**, co podkreśla szczególną rolę systemów informatycznych w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

10) Dane biometryczne nie stanowią danych wrażliwych. Grupa robocza art. 29 rekomenduje, aby tak je traktować, jednak rekomendacje takie nie mają siły obowiązującego prawa. Unijne rozporządzenie zmieni ten stan rzeczy i dane biometryczne będą uznawane za dane wrażliwe.



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"**[17].

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

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

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, a właściwie kilku zgód.

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[18] 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

18) 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".

Zbieranie danych

Nie można zbierać większej ilości danych, niż jest to niezbędne do realizacji określonego celu przetwarzania. Dane muszą być adekwatne[21)] 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.

Nie można zbierać większej ilości danych, niż jest to niezbędne do realizacji określonego celu przetwarzania.

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.[22)]

Przykładem braku adekwatności jest opisana w sprawozdaniu GIODO za 2010 r. usługa wypożyczania 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 też zbieranie numeru PESEL podczas sprzedaży biletów przez internet. WSA uznał, że „wystarczające było pozyskiwanie przez przewoźnika danych osobowych

w następującym zakresie: imię, nazwisko, adres e-mail, numer telefonu komórkowego i hasło". Sprzedawca argumentował, że numery PESEL były potrzebne na wypadek ewentualnej kontroli skarbowej, ale sąd nie uznał tego argumentu.[23)]

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

21) Unijne rozporządzenie (RODO) w art. 5 ust. 1 podkreśla, że dane muszą być: „adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane – wprowadzając tym samym większe restrykcje jakie dane mogą być gromadzone.

22) Sprawozdanie GIODO za 2012r., s. 190

23) Sprawozdanie GIODO za 2015r., s. 266

siębiorcy, 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**.

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[25]. Generalny Inspektor akceptuje taki sposób stwierdzając: *nie widzi 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*[26].

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 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**

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

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

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

Za dobrą wiadomość należy uznać to, że grupy kapitałowe zostały w końcu zauważone i nowe przepisy (RODO) już je biorą pod uwagę, przykładowo ułatwiając im międzynarodową wymianę informacji o pracownikach.

Jak i kiedy rejestrować zbiory danych osobowych?

W Polsce funkcjonuje prawie ok. 2 mln aktywnych przedsiębiorców[32]. Bez wątpienia większość z nich posiada zbiory danych podlegające rejestracji, jednak w rejestrze GIODO znajduje się jedynie niewielka ich część .

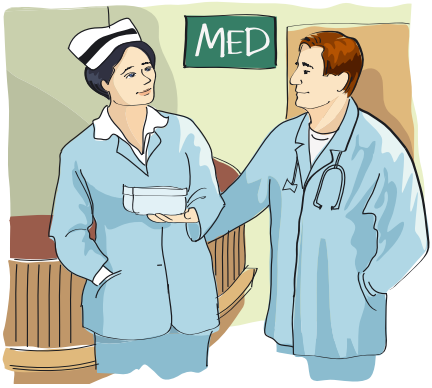
Warto wiedzieć, że niezgłoszenie zbioru do rejestracji stanowi przestępstwo i jest karane z art. 53 ustawy o ochronie danych osobowych. Natomiast brak aktualizowania zgłoszonego zbioru może prowadzić do wszczęcia postępowania administracyjnego przez GIODO. Dlatego też podmiot, który przetwarza dane osobowe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

- **tradycyjnie – w formie papierowej,**
- **za pomocą internetowej aplikacji e-GIODO,**
- **za pomocą internetowego programu e-GIODO (wypełnienie i wysyłka w pełni elektronicznie),**
- **za pomocą platformy ePK[33].**

Najwygodniej jest wypełnić i wysłać wniosek elektronicznie, a w ramach

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

33) 28 grudnia 2009 r. na mocy Dyrektywy usługowej oraz ustawy o swobodzie działalności gospodarczej utworzony został Pojedynczy Punk Kontaktowy, którego celem było wsparcie dla osób prowadzących lub planujących rozpocząć działalność gospodarczą. — https://www.biznes.gov.pl/o-nas/o-epk

nych, 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.

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.

Obecne przepisy nie nakazują informować osób o tym, jak długo ich dane bedą przetwarzane. Trzeba jednak pamiętać, że nowe przepisy taki obowiązek przewidują, dlatego już dzisiaj zbierając dane warto zastanowić się, do kiedy będą one przetwarzane.

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 wyciekną?

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.

Warto prowadzić rejestr wszystkich takich incydentów. Dzisiaj jest to obowiązkowe jedynie dla przedsiębiorców telekomunikacyjnych[38], ale za jakiś czas każdy przedsiębiorca będzie musiał taki rejestr prowadzić. Co ciekawe, przedsiębiorcy telekomunikacyjni, prócz prowadzenia rejestru, do GIODO zgłaszają przypadki naruszenia ochrony danych osobowych[39], mając na to 24 godziny, a gdy sprawa jest poważna, muszą także informować o tym swoich klientów.

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[40].

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,**

38) Ustawa prawo telekomunikacyjne, art 174a. zob. http://www.giodo.gov.pl/1520190/

39) Zawiadomienie o naruszeniu danych osobowych dla dostawców publicznie dostępnych usług komunikacyjnych można wysłać za pomocą platformy ePUAP oraz ePK — http://www.giodo.gov.pl/432/id_art/2096/ oraz http://www.giodo.gov.pl/1520190/

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

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.

Art. 54a. - utrudnianie kontroli

Kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

W sprawozdaniu GIODO za 2015 r. czytamy opis interesującej sytuacji, w której GIODO chciał dokonać kontroli pewnego przedsiębiorcy, ale ten nie odbierał korespondencji. Podjęto więc telefoniczną próbę kontaktu, ale telefon odbierała osoba, która nie była upoważniona do reprezentowania przedsiębiorcy. Ostatecznie pojawił się pełnomocnik, który udzielił pewnych wyjaśnień, ale też przedłożył „pisemne zawiadomienie kontrolujących o sprzeciwie przedsiębiorcy wobec prowadzenia kontroli GIODO". Przepychanki trwały pewien czas, ostatecznie GIODO uznał, że jest to utrudnianie kontroli.*

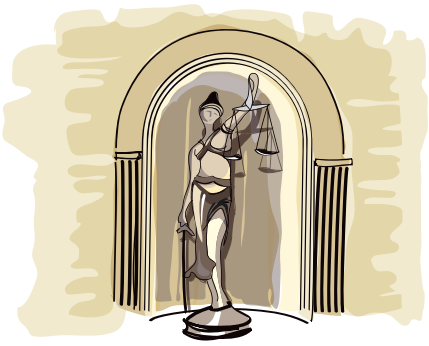
* *Sprawozdanie GIODO za 2015, str. 266-267 oraz postanowienie GIODO o sygnaturze DIS/POST-443/15/87481*

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 materiałów41).

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

Nie ma obowiązku odpisywania 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.

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.

Zmiany w prawie – unijne rozporządzenie o ochronie danych osobowych

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.

Minęło ponad 20 lat od kiedy ona 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.

W 2010 r. zapoczątkowano zmiany, które procesowały się dość długo, bo aż 6 lat, ale ostatecznie w maju 2016 r. przyjęto unijne przepisy, które zaczną obowiązywać od 25 maja 2018 r.[42]. Składają się na nie:

- **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)**
- **Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW**

Nas interesuje najbardziej Rozporządzenie (zwane RODO). Ogromne znaczenie ma fakt, że jest to rozporządzenie, a nie dyrektywa. Rozporządzenia europejskie są podobne do polskich ustaw, mają charakter wiążący i — co najważniejsze — obowiązują bezpośrednio. Oznacza to, że do rozporządzenia UE w Polsce (i w innych krajach Unii Europejskiej) należy stosować się tak samo, jakby to była polska ustawa. Tłumacząc obrazowo:

- **w przypadku Dyrektywy 95/46/WE każdy miał wybudować most na rzece, ale jego ostateczny kształt i rodzaj użytych materiałów pozostawiono decyzji każdego z państw.**

42) W polskiej literaturze spotyka się skrót RODO – Rozporządzenie o ochronie danych osobowych. W materiałach angielskojęzycznych natomiast GDPR – General Data Protection Regulation.

ODO 24

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.

WSPARCIE lub **PRZEJĘCIE**

Aktywna pomoc w wypełnianiu obowiązków nałożonych na ABI lub ADO.

ODO 24.pl

tel. 22 740 99 00

Wspieramy FUNDACJA WIEDZA TO BEZPIECZEŃSTWO

szlachetna PACZKA