Piotr Czubaty

RODO
OBOWIĄZKI PRACODAWCY
PRAKTYCZNY PORADNIK ZE WZORAMI

Stan prawny na dzień 15 maja 2021 r.

Warszawa 2021

Spis treści

1. Wstęp

„Mężczyzna nie dba o pieniądze – pod warunkiem, że jest bogaty" – niezwykła, acz oczywista mądrość. Wiele jest obszarów w życiu, które uznajemy za mało istotne albo wręcz niepotrzebne, dopóki niespodziewany splot okoliczności nie przekona nas, że jest inaczej. Całkiem podobnie jest z ochroną danych osobowych.

Wśród przedsiębiorców, którzy podlegają przepisom RODO[1], bo przetwarzają dane osobowe w celach innych niż czynności o osobistym lub domowym charakterze (takiego przetwarzania danych Rozporządzenie nie obejmuje), najszczęśliwsi są chyba ci, do których wciąż nie dotarły obowiązki wynikające z przepisów o ochronie danych osobowych. Ta błoga nieświadomość, choć ryzykowna, daje poczucie zupełnej lekkości bytu. A ryzyko, z którego nie zdają sobie przecież sprawy, nie powoduje w związku z tym podwyższonego tętna. Podobny spokój panuje w organizacjach, w których osoby zarządzające zadbały o odpowiednie i prawidłowe wdrożenie niezbędnych regulacji oraz standardów wewnętrznych – albo miały już te standardy przyjęte dużo wcześniej. Bo trzeba pamiętać, że ochrona danych nie zaczęła się w 2016 roku, w chwili uchwalenia RODO, ani też w maju 2018 roku, od kiedy rozpoczęliśmy stosowanie tych przepisów (i egzekwowanie obowiązków). Tak. Wiele firm dbało o ochronę danych, zanim to było modne. Ale jest też trzecia grupa organizacji, które co prawda mają świadomość – ale nie mają odpowiedniego wsparcia. To ogromny odsetek rynku, niestety. A poczucie braków w obszarze obarczonym potencjalnymi milionowymi karami nie należy do komfortowych.

Ta trzecia kategoria, a trzeba przyznać, że należą do niej zarówno podmioty z sektora prywatnego, jak i jednostki publiczne, wyrosła na gruncie chaosu związanego z pojawieniem się RODO w Polsce. Nowe obowiązki, komunikowane narastająco od przełomu lat 2017 i 2018, wprawiały przedsiębiorców w coraz większe zakłopotanie. Głównym powodem była oczywiście ich niejasność i nieprecyzyjność – co z kolei wynikało bezpośrednio z przyjętej przez ustawodawcę unijnego formuły przyjętego aktu. Przepisy Rozporządzenia wymagają interpretacji i to

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

wyzwanie z finezją i polotem zostało podjęte przez licznych specjalistów. Wyjaśnianie bardzo ogólnych zapisów nie wszystkim szło równie sprawnie, w związku z powyższym do różnych podmiotów trafiały czasem całkiem odmienne informacje, powodując jeszcze większy zamęt. Ilość wątpliwości mnożyła się, a osoby odpowiedzialne za ten aspekt w ramach organizacji dostawały niekonkretne – a czasem wręcz sprzeczne informacje na temat poszczególnych obowiązków.

Taki stan rzeczy trwa w niektórych organizacjach do dziś, ale coraz częściej powodem jest już tylko niefrasobliwość ich reprezentantów – bowiem dostęp do fachowej wiedzy nie jest trudny i poziom kwalifikacji profesjonalistów w branży na szczęście odbiega dziś znacznie od „punktu zero", czyli od 25 maja 2018. Przy minimum zaangażowania każdy szukający rozwiązań potrafi odnaleźć niezbędne informacje i dostosować się do wymogów, które obowiązują już przecież od kilku lat.

Poradnik, który Państwo czytacie, powstał, by umożliwić względnie swobodne poruszanie się po materii związanej z przepisami o ochronie danych osobowych. Ideą było stworzenie prostej w odbiorze i zrozumiałej check-listy, która krok po kroku pozwala na zweryfikowanie wdrożonych już działań i uzupełnienie tych, które umknęły lub zostały pominięte. Prawidłowe wykonywanie obowiązków prawnych leży w dobrze pojętym interesie każdej firmy, organizacji pozarządowej, czy też jednostki samorządowej. I główną motywacją do utrzymania wysokich standardów ochrony danych wcale nie muszą być odczuwalne sankcje finansowe.

Wszystkie kraje, które obowiązuje RODO, cały czas ewoluują. I dzieje się to w różnym tempie. My w Polsce wciąż jeszcze jesteśmy na etapie „kija" – decydujemy się na wdrażanie obowiązków pod groźbą kar. Owszem, nie można tego pominąć – wszak Prezes Urzędu Ochrony Danych Osobowych wcale nie unika kategorycznych decyzji a górny pułap dwudziestu milionów Euro kary pobudza wyobraźnię. Poza tym, wszelkiej maści naruszenia, wycieki danych czy zaniedbania przy realizowaniu obowiązków informacyjnych, rodzą jednocześnie ryzyko roszczeń cywilnych. Nie bez znaczenia są również zapisy o odpowiedzialności karnej, którą (ciekawostka) zaprojektowano m.in. za „utrudnianie lub udaremnianie przeprowadzenia kontroli". O stratach wizerunkowych nie wspominając… Tymczasem równie istotny jest element „marchewki" – wzmacniania pozytywnego wymiaru „compliance" w obszarze ochrony danych osobowych, a także budowanie wizerunku organizacji o najwyższych możliwych standardach. Niezależnie od wielkości podmiotu. Jakość jest sprzymierzeńcem dobrego wizerunku. Wdrożenie wysokiego poziomu zgodności – nazwijmy to ogólnie, z RODO – wzmacnia konkurencyjność firmy, gminy, NGO's – u. Takie podejście do poziomu wdrożenia obowiązków w zakresie ochrony danych jest zapewne dopiero przed nami – rola pionierów na tym polu jest zatem wciąż otwarta.

Proces jest w toku. Czasy, w których posiadanie systemu zarządzania bezpieczeństwem informacji zgodnego z normą ISO 27001, certyfikacja na zasadach opisanych w RODO lub inna forma standaryzacji tego obszaru dla wyróżnienia i podniesienia konkurencyjności rynkowej podmiotu – z całą pewnością są przed nami. Kiedyś będzie to wymóg dla oferentów przystępujących do zamówień publicznych, a z pewnością atut przy podejmowaniu współpracy. Pierwszym krokiem niech będzie właściwe wdrożenie zasad, procedur i dobrych praktyk, w czym ma pomóc niniejszy Poradnik.

Powodzenia!

2. RODO w organizacji – istota ochrony danych, dobre praktyki, faktyczne obowiązki

2.1. Istota ochrony danych

Pełna nazwa RODO brzmi: Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Już na tej podstawie można wywnioskować, że ustawodawca zamierzał uregulować i usankcjonować ochronę osób fizycznych wówczas, gdy przetwarzane są ich dane. Każdy, kto w ramach swojej działalności zbiera, utrwala, organizuje, porządkuje, przechowuje, adaptuje, pobiera, przegląda, wykorzystuje, ujawnia poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowuje, ogranicza, usuwa lub niszczy dane osobowe[2], podlega przepisom i jest zobligowany do ich ochrony. Jednakże, Rozporządzenie poza ochroną danych osobowych, w swojej nazwie zawiera również element wskazujący na „swobodny przepływ takich danych". Należy więc uważać, że ustawodawcy – obok oczywistego aspektu ochrony – zależało także na podkreśleniu, iż RODO nie służy w żaden sposób blokowaniu przepływów danych, ani na paraliżowaniu jakiejkolwiek działalności w związku z koniecznością przetwarzania danych osobowych. Warto to podkreślić, ponieważ jest to bardzo często spotykana praktyka – zwłaszcza u zarania wdrażania przepisów w 2018 roku niezrozumienie idei powodowało niezwykłe absurdy, jak odmowa udzielania informacji „bo RODO".

Ideą RODO jest zapewnienie ochrony danych osób fizycznych oraz zapewnienie swobodnego przepływu tych danych.

[2] Zgodnie z definicją przetwarzania, wyrażoną w art. 4 ust. 2 Rozporządzenia.

Niechlubnym przykładem jest historia wypadku w Tęczynie (małopolska) w czerwcu 2018 roku. W zderzeniu autokaru z samochodem ciężarowym ucierpiało 10 osób, w tym pięcioro dzieci. Ofiary zostały przetransportowane do kilku okolicznych szpitali. Rodzice jednego z dzieci próbowali uzyskać informację o tym, do której z placówek trafiła ich pociecha – i tu okazało się, że – mówiąc językiem młodzieżowym – „RODO weszło za bardzo". Telefoniczne pozyskanie informacji było niemożliwe, pracownicy szpitali kategorycznie odmawiali, powołując się na ochronę danych właśnie. Dopiero osobiste poszukiwania po kilku godzinach drogi skutkowały sukcesem – dziecko odnalazło się. Jest to przypadek często przytaczany jako jeden z absurdów, wynikających z niezrozumienia idei Rozporządzenia. Należy pamiętać, że oprócz przepisów (które oczywiście bywają nieprecyzyjne lub niejasne), jest też zdrowy rozsądek i dobra praktyka – jeżeli nie stoi w rażącej sprzeczności z regulacją prawną.

Na podkreślenie zasługuje fakt, iż na zrozumienie idei i wdrożenie wewnętrznych regulacji państwa członkowskie otrzymały od unijnego ustawodawcy dwa lata – od 27 kwietnia 2016 roku (moment uchwalenia) do 25 maja 2018 roku (moment rozpoczęcia stosowania). Okazało się, że w wielu przypadkach nie tylko owe regulacje wewnętrzne były przygotowywane w ostatniej chwili (polska ustawa o ochronie danych osobowych jest datowana na 10 maja 2018 roku, czyli na chwilę przed nałożonym przez UE deadlinem) – ale również samo zrozumienie idei nie wszystkim „weszło" do dziś.

Dla wielu będzie to odkrycie, ale ochrona danych osobowych nie zaczęła się w Polsce w 2018 roku. Jeszcze większym zdziwieniem będzie fakt, że RODO poluzowało nawet zasady związane z tym obszarem działalności biznesowej lub publicznej. Szczególnie pracownicy administracji publicznej powinni pamiętać Rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Ta regulacja z 2004 roku była niesamowicie konkretna, precyzyjna i dokładna. Nakazywała m.in. wdrożenie procedur wewnętrznych, ale nie jakichkolwiek procedur. Miały być to dokładnie „Polityka bezpieczeństwa" oraz „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych". Co poniektóre podmioty z sektora prywatnego, wdrażając wewnętrzne standardy, wzorowały się na kształcie i nazewnictwie przyjętym przez jednostki publiczne obligatoryjnie. Minister Spraw Wewnętrznych i Administracji wskazał nawet na obowiązkową zawartość tych procedur, a także np. na zasady zabezpieczania danych w systemach informatycznych – w zależności od poziomu bezpieczeństwa (podstawowy, podwyższony, wysoki). Obowiązkowe hasła składające się z minimum sześciu znaków, zmieniane co 30 dni, bezwzględne wykonywanie kopii zapasowych, stosowanie środków ochrony kryptograficznej

to standard w administracji publicznej przez długie lata przed wejściem w życie RODO. Sektor prywatny ocierał się gdzieniegdzie o te zasady, najczęściej wzorując się na nich. Oczywiście istniały również normy jakościowe, z kategorii ISO/IEC 27…, jednakże dla sektora prywatnego były to regulacje dobrowolne.

I przyszła regulacja unijna, i wprowadziła chaos… Wraz z rozpoczęciem stosowania RODO, ustawa z 1997 roku o ochronie danych osobowych i wszystkie rozporządzenia jej towarzyszące mają status „uchylony", lub „nieobowiązujący – uchylona podstawa prawna". Zamiast nich, obowiązuje nas unijne prawo – które na pytanie o to, w jaki sposób należy chronić dane osobowe w organizacji, odpowiada: „adekwatnie do ryzyka". I nic więcej. Nie ma przepisu nakazującego zmianę hasła w komputerze co 30 dni. Ba, nie ma nawet przepisu, który wprost nakazywałby zabezpieczanie systemu operacyjnego hasłem. Brak jasnych wytycznych dla jednych okazał się fantastycznym rozwiązaniem, dla innych oznaczał niesamowity kłopot. Prowadząc działalność ciężko jest poruszać się po obowiązkach, które nie są jasno uregulowane. Dodatkowo, ciężko jest żyć z poczuciem, że to na administratorze danych osobowych spoczywa obowiązek wykazywania zgodności z przepisami. Z nieprecyzyjnymi przepisami, które odpowiedzialność za właściwą (adekwatną do ryzyka) ochronę danych osobowych w całości przerzucają na przedsiębiorcę, który musi owo ryzyko oszacować i w oparciu o wynik projektować ochronę danych (zgodnie z zasadą „privacy by design"). I decydować – czy wdrażać polityki ochrony danych (i jakie), czy i jak zabezpieczać dane w formie papierowej i elektronicznej, czy kupować szafy pancerne, niszczarki, zamki szyfrowe i kubki zgodne z RODO. Wsparcie niosą najczęściej zewnętrzni specjaliści – chyba że firma czuje się zobligowana do wyznaczenia Inspektora Ochrony Danych. Jednostki publiczne mają ten obowiązek wpisany w przepisach, co bardzo ułatwiło sprawę. Sektor prywatny długo błądził w gąszczu domysłów, a Urząd Ochrony Danych Osobowych raz po raz wspierał nieboraków dobrą radą – lub też zaleceniem pokontrolnym w tym zakresie. Dziś już mniej więcej wiadomo, kto ma obowiązek, kto powinien, a kto może na własną rękę monitorować zgodność i poziom spełnienia obowiązków.

2.2. Dobre praktyki

Tak od istoty ochrony danych, którą trzeba traktować jako domyślną przy prowadzeniu działalności („privacy by default"), dochodzimy do dobrych praktyk. Wynikają one trochę z interpretacji przepisów prawa, których prawodawca nie raczył doprecyzować, a trochę z potrzeby ust.anowienia pewnych standardów – jednolicie dla określonej branży, czy też tylko w obrębie organizacji. Dobre praktyki ulegają ciągłej ewolucji, co jest absolutnie zgodne z duchem RODO – wszak

ochrona danych to nieust.anny proces. Czasem okazuje się, że przyjęte rozwiązania są niewystarczające lub wymagają korekty i system ochrony danych żyje wraz z organizacją. I tak jest dobrze. Dobre praktyki określają, w jaki sposób firma lub podmiot publiczny stosują przyjęte wewnętrznie zasady. To standard, który obowiązuje wszystkich tak samo i do stosowania którego zobligowani są wszyscy w równym stopniu. To zewnętrzna warstwa wdrożonych procedur, która bezpośrednio oddziałuje też na „klientów zewnętrznych" organizacji, czyli na osoby fizyczne, których dane są przetwarzane. Dobre praktyki określają, w jaki sposób realizowane są obowiązki informacyjne z art. 13 lub 14 RODO, jak wygląda proces realizacji praw osób, czy też jak zabezpiecza się dostęp do dokumentów i jakie są zasady dostępu do pomieszczeń. Z łatwością można zauważyć, że ten element systemu ochrony danych w organizacji wpływa istotnie na jej wizerunek. Firma jest postrzegana m.in. przez pryzmat jakości obsługi klienta – a chociażby sposób realizacji obowiązków informacyjnych, transparentność w komunikacji praw w związku z przetwarzaniem danych osobowych to obszar ewidentnie mieszczący się w kategorii PR.

Przyjęcie dobrych praktyk w obszarze ochrony danych w organizacji wpływa istotnie na jej wizerunek.

Dobre praktyki często są oczywiste, zrozumiałe i funkcjonują od lat. Niektóre z nich, siłą rzeczy, pojawiły się na etapie wdrażania przepisów o ochronie danych, zgodnie z wymogami unijnej regulacji. Niezależnie od stażu, stosunkowo łatwo je przyswoić, zapamiętać i stosować. Ważne, aby wypośrodkować dwie rzeczy: rutynę stosowania i zdrowy dystans – by wyłapać niedociągnięcia bądź też nowe potrzeby. Na pewnym etapie rozwoju firmy być może wystarczy papierowy formularz jako forma komunikacji z pracownikami, ale z czasem przydaje się wspólne miejsce na zewnętrznym serwerze, na którym lądują na przykład regulaminy lub procedury – w tym wewnętrzne zasady odnoszące się do przetwarzania danych klientów.

Przykłady dobrych praktyk? Oczywiście jest ich wiele i każdy podmiot powinien dobrać własne, adekwatnie do rodzaju prowadzonej działalności, skali przetwarzanych danych, istniejących ryzyk, stosowanych zabezpieczeń, poziomu świadomości pracowników. Do najpopularniejszych należą:

- zasada czystego biurka i czystego ekranu;
- szyfrowanie nośników zawierających dane osobowe;
- szyfrowanie załączników poczty e-mail, zawierających dane osobowe;
- regularna zmiana haseł dostępowych;
- zachowanie poufności przy wysyłaniu poczty do wielu odbiorców;
- zamykanie pomieszczeń pod nieobecność pracownika;

- korzystanie służbowo z bezpiecznych komunikatorów;
- korzystanie z wiarygodnego i aktualnego oprogramowania;
- ewidencjonowanie dostępów do systemów.

Powyższe zasady w swojej istocie są najczęściej jasne i nie wymagają w większości pogłębionej analizy – głównie dlatego, że były (albo powinny być) stosowane nawet wcześniej, zanim „przyszło RODO". Ale, jak pokazują chociażby kary administracyjne nałożone przez Prezesa Urzędu Ochrony Danych Osobowych, nie wszystkie są stosowane nawet w dużych organizacjach. Mowa na przykład o szyfrowaniu załączników poczty e-mail, co powinno dziś już stanowić absolutny elementarz w kodeksie dobrych praktyk. Wiele firm, a nawet jednostek publicznych, zabezpiecza systemy operacyjne hasłem – ale Windows nie wymusza cyklicznej jego zmiany, co jest przecież łatwe do skonfigurowania w ustawieniach systemowych. A taka praktyka to oczko wyżej do bezpieczeństwa danych. Z uwagi na skalę korespondencji prowadzonej drogą elektroniczną, pojawia się wiele błędów i pomyłek polegających na nieuprawnionym ujawnieniu danych adresatów w przypadku wysyłania wiadomości do wielu. Wynikają one z jednej strony z tempa, w jakim żyje większość organizacji i zwykłych przeoczeń w tym zakresie – ale równie często zdarza się, że powodem takich naruszeń jest po prostu niewiedza pracowników. Wszak człowiek jest w systemie ochrony danych najsłabszym ogniwem. Dlatego pracę nad świadomością kadr należałoby dopisać do check-listy dobrych praktyk, niezależnie od wielkości firmy.

Coraz więcej procesów przetwarzania danych osobowych odbywa się w systemach informatycznych, stąd rosnąca ilość oczekiwanych zachowań i stosowanych dobrych praktyk w tym zakresie. Tym niemniej, nie wolno zapominać o zasadach ochrony danych przetwarzanych w formie tradycyjnej (jakkolwiek to określenie w coraz mniejszym stopniu odnosić można do dokumentów papierowych, bo formą tradycyjną staje się już elektroniczny nośnik informacji). Zapewnienie bezpieczeństwa i poufności danych osobowych umieszczonych w dokumentach, formularzach, drukach, notatnikach, kalendarzach i innych odręcznych zapiskach również wymaga przyjęcia określonych standardów w zakresie ich odpowiedniego zabezpieczania. Dobre praktyki w tym zakresie – poza wspomnianą już zasadą czystego biurka – to między innymi:

- ewidencjonowanie dostępu do pomieszczeń;
- zabezpieczanie danych osobowych w szafach zamykanych na klucz;
- zapewnianie uprawnionego dostępu do kluczy;
- ewidencjonowanie obiegu dokumentów;
- standaryzacja w zakresie utylizacji dokumentów;
- możliwie precyzyjne określanie zasad retencji danych.

Oczywiście, zasad i dobrych praktyk jest o wiele więcej i każda organizacja, w oparciu o własne doświadczenia i oszacowane ryzyka podchodzić powinna

do nich indywidualnie. Niemniej, warto przyjmować jednolity standard nawet w małych podmiotach, dla zachowania zasady rozliczalności i zapewnienia poczucia bezpieczeństwa pracownikom, mogącym poruszać się w oparciu o jasno wyrażone zasady postępowania.

2.3. Faktyczne obowiązki

Zmiana patrzenia na ochronę danych, jaka przyszła wraz z unijnym rozporządzeniem, nie wpłynęła od razu na zmiany w codziennym funkcjonowaniu organizacji. Nie wpłynęła również na szybkie zrozumienie konieczności podjęcia określonych działań ani na uświadomienie obowiązków wynikających z RODO. Ba – nie wpłynęła na określenie, jakie te obowiązki faktycznie są. Nawet kiedy po pierwszych miesiącach stosowania RODO opadł już kurz i mniej więcej widoczne były kierunki niezbędnych zmian, dalej nie wszyscy potrafili odnaleźć się w treści aktu, który niektóre obowiązki komunikuje wprost, a inne jedynie sugeruje bez doprecyzowywania szczegółów. Na szczęście dziś wiemy już o wiele więcej, w czym niewątpliwa zasługa niestrudzonych mądrych głów, które poświęcają swój czas by z pasją dzielić się swoją wiedzą i nieść dobrą nowinę o prawidłowym stosowaniu obowiązujących przepisów. Kanon tych nazwisk jest zbyt szeroki by go w całości zaprezentować – aczkolwiek cytaty z niektórych z pewnością będzie można napotkać w treści poniżej.

Faktyczne obowiązki, jakie spoczywają na administratorze danych osobowych[3], można w wielkim uproszczeniu podzielić na dwa obszary:

a) Obowiązki względem osób fizycznych, których dane dotyczą;
b) Obowiązki związane z zapewnieniem bezpieczeństwa danych osobowych.

Oczywiście, tych podziałów może być o wiele więcej i z pewnością można by w inny sposób konfigurować zasady obowiązujące administratorów – ale dla zachowania możliwie największej prostoty w zrozumieniu przepisów – a jednocześnie bez przesadnej nadgorliwości – taki podział będzie zupełnie wystarczający. Zobowiązania, które wynikają z RODO, najwłaściwiej jest odnieść do wskazanych wyżej punktów. Pierwszym będzie relacja z osobami, których dane są w organizacji przetwarzane – niezależnie od źródeł ich pochodzenia, zakresu danych czy podstaw prawnych przetwarzania. Drugim – obowiązki wynikające z faktu, że dane osobowe są przetwarzane.

[3] Art. 4 ust. 7 Rozporządzenia: „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ust.ala cele i sposoby przetwarzania danych osobowych…"

2.3.1. Obowiązki względem osób fizycznych, których dane dotyczą:

a) Obowiązki informacyjne wynikające z art. 13 oraz art. 14 RODO
b) Obowiązek realizacji praw osób w związku z przetwarzaniem ich danych

2.3.1.1. Obowiązki informacyjne

Artykuł 13 i art. 14 RODO nakłada na administratora danych obowiązek przekazywania osobom fizycznym określonych informacji. W przypadku zbierania danych osobowych bezpośrednio od osoby (art. 13), należy dokonać swoistej wymiany informacji: ja zbieram dane od Ciebie, a jednocześnie Ty uzyskujesz konkretne dane ode mnie. Żeby wszystko było transparentne i obie strony miały jasność co do tej wymiany. Zgodnie z art 13 ust. 1 i 2 RODO, administrator podczas pozyskiwania danych osobowych podaje osobie fizycznej następujące informacje[4]:

1. Swoją tożsamość i dane kontaktowe;
2. Dane kontaktowe do Inspektora Ochrony Danych – jeśli został wyznaczony;
3. Cele przetwarzania danych osobowych oraz podstawy prawne ich przetwarzania;
4. Informacje o ewentualnych odbiorcach danych, jeżeli możliwe jest ich wskazanie;
5. Jeżeli przetwarzanie odbywa się w oparciu o uzasadniony prawnie interes, należy wskazać na czym on polega;
6. Okres przechowywania danych, jeżeli jest możliwy do określenia;
7. Informacje o możliwych do zrealizowania prawach, w zależności od rodzaju i podstawy przetwarzania: prawie dostępu do danych, sprostowania, usunięcia, ograniczenia przetwarzania, prawie do wniesienia sprzeciwu, prawie do przenoszenia danych;
8. Informację o możliwości wycofania zgody – jeżeli to zgoda jest podstawą przetwarzania;
9. Informację o możliwości wniesienia skargi do organu nadzorczego;
10. Informację o tym, czy podanie danych jest obowiązkowe, czy dobrowolne;
11. Informację o ewentualnym profilowaniu lub przekazywaniu danych do państw trzecich albo organizacji międzynarodowych.

Istotnym elementem tego obowiązku prawnego jest nakaz, by informacje przekazywane były „podczas pozyskiwania danych osobowych". W praktyce okazuje się to niezwykle trudne do zrealizowania – zwłaszcza w chwili pozyskiwania

[4] Wzory klauzul informacyjnych, skonstruowanych zgodnie z wytycznymi z art. 13 ust. 1 i 2 można znaleźć w rozdziale „Wzory dokumentów"

danych bezpośrednio – ale zdalnie. Obowiązek jednakowoż istnieje, wobec czego należy zajrzeć do dobrych praktyk i wykorzystać zdrowy rozsądek.

Obowiązek informacyjny powstaje w chwili zbierania danych osobowych bezpośrednio od osoby fizycznej.

Dobrą praktyką jest informowanie zawczasu, jeśli wiemy, że niezbędne będzie zbieranie danych osobowych – tak jest na przykład podczas rekrutacji, gdzie obowiązek informacyjny (najczęściej realizowany warstwowo)[5] pojawia się już na etapie publikacji ogłoszenia, zanim dane będą zbierane. Przykładem sytuacji, w której obowiązek informacyjny będzie realizowany wtórnie, już po uzyskaniu danych osobowych, może być korespondencja e-mail, w której umieszczona zostaje skrócona klauzula, wskazująca na przetwarzanie danych osobowych pozyskanych podczas wymiany korespondencji z osobą fizyczną (najczęściej w stopce). Idealną formułą jest zamieszczanie klauzul informacyjnych np. w kwestionariuszu osobowym pracownika – tu realizujemy obowiązek prawny dokładnie tak, jak sobie wymarzył ustawodawca, czyli podczas pozyskiwania danych.

Inaczej jest w przypadku pozyskiwania informacji o osobie nie bezpośrednio. Wówczas, jeżeli nie zachodzi wyłączenie opisane w art. 14 ust. 5[6], należy zrealizować obowiązek informacyjny „w rozsądnym terminie po uzyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych”[7] a w przypadku, gdy celem pozyskania danych jest nawiązanie kontaktu z osobą fizyczną – „najpóźniej przy pierwszej takiej komunikacji”[8].

[5] Warstwowe realizowanie obowiązku informacyjnego polega na przygotowaniu pełnej klauzuli i udostępnieniu jej na przykład na stronie www, a następnie klauzul skróconych które wskazywałyby na przykład tylko dane administratora danych i podstawę przetwarzania danych osobowych, zaś w zakresie uprawnień osoby oraz pozostałych elementów wymaganych przepisem odsyłałyby do pełnej treści, dostępnej w określonej zakładce na stronie www. O obowiązku informacyjnym wspomina UODO, chociażby relacjonując niezwykle bogate w treść spotkanie IOD w dniu 28 lutego 2019 roku (https://uodo.gov.pl/pl/138/727), a szukającym prostego w treści uzupełnienia tej materii polecam wpis dr Pawła Litwińskiego o tym, dlaczego nie tylko cebula i ogry mają warstwy: https://pl.linkedin.com/pulse/warstwowość-spełniania-obowiązku-informacyjnego-czyli-pawel-litwinski

[6] Przepis mówi, iż obowiązki informacyjne w chwili pozyskania danych w sposób inny niż bezpośrednio od osoby, której dane dotyczą nie muszą być realizowane wówczas, gdy:
a) osoba ta już dysponuje tymi informacjami;
b) udzielenie informacji jest niemożliwe albo wymagałoby niewspółmiernie dużego wysiłku;
c) pozyskiwanie lub ujawnianie danych jest wyraźnie uregulowane przepisami prawa i przepisy jasno przewidują środki chroniące dobra osobiste tych osób;
d) dane osobowe muszą pozostać poufne, co wiąże się z ustawowym obowiązkiem zachowania tajemnicy, w tym tajemnicy zawodowej

[7] Art. 14 ust. 3 lit a) RODO

[8] Art. 14 ust. 3 lit b) RODO

Zakres informacji, które należy przekazać w takiej klauzuli informacyjnej, jest analogiczny do zestawu, o którym wspomina art. 13 ust. 1 i 2 RODO, czyli:

1. Tożsamość administratora i jego dane kontaktowe;
2. Dane kontaktowe do Inspektora Ochrony Danych – jeśli został wyznaczony;
3. Cele przetwarzania danych osobowych oraz podstawy prawne ich przetwarzania;
4. Informacje o ewentualnych odbiorcach danych, jeżeli możliwe jest ich wskazanie;
5. Jeżeli przetwarzanie odbywa się w oparciu o uzasadniony prawnie interes, należy wskazać na czym on polega;
6. Okres przechowywania danych, jeżeli jest możliwy do określenia;
7. Informacje o możliwych do zrealizowania prawach, w zależności od rodzaju i podstawy przetwarzania: prawie dostępu do danych, sprostowania, usunięcia, ograniczenia przetwarzania, prawie do wniesienia sprzeciwu, prawie do przenoszenia danych;
8. Informację o możliwości wycofania zgody – jeżeli to zgoda jest podstawą przetwarzania;
9. Informację o możliwości wniesienia skargi do organu nadzorczego;
10. Informację o tym, czy podanie danych jest obowiązkowe, czy dobrowolne;
11. Informację o ewentualnym profilowaniu lub przekazywaniu danych do państw trzecich albo organizacji międzynarodowych.

Dodatkowo, w przypadku zbierania danych w inny sposób niż bezpośrednio od osoby, należy wskazać źródło pozyskania danych, a jeżeli pochodzą one ze źródeł publicznie dostępnych to również taką informację. Nie sposób nie wspomnieć tu niezwykle medialnej historii ukarania firmy kwotą 943 tysiące złotych za brak realizacji obowiązku informacyjnego. Firma gromadząc dane osobowe z publicznych baz, przetwarzała informacje dotyczące niemal 6,6 miliona osób, wobec których nie zrealizowano obowiązku z art. 14 RODO. Kara została co prawda nieprawomocnie uchylona, ale należy przyznać, że skala przetwarzanych danych i fakt gromadzenia ich w sposób zupełnie nietransparentny wobec osób fizycznych musi budzić zainteresowanie Urzędu Ochrony Danych Osobowych, całego środowiska i opinii publicznej.

2.3.1.2. Obowiązek realizacji praw

Drugim obowiązkiem prawnym, pochodzącym wprost z przepisu, jest konieczność prawidłowej realizacji praw osób fizycznych – co jest jednoznaczne z poszanowaniem tychże uprawnień na gruncie RODO. Każdy, kto przetwarza dane osobowe, realizując obowiązek informacyjny komunikuje przysługujące osobom prawa. Są to: