pracownia badań
i innowacji
społecznych
stocznia

KATARZYNA
SZYMIELEWICZ
FUNDACJA
PANOPTYKON

OCHRONA DANYCH OSOBOWYCH W BADANIACH NAD BEZDOMNOŚCIĄ METODĄ AGREGACJI ZINDYWIDUALIZOWANYCH DANYCH GROMADZONYCH PRZEZ PLACÓWKI UDZIELAJĄCE WSPARCIA.

OPINIA PRAWNA.

Konsultacja ekspercka: dr Dominika Dőrre-Nowak, (Kancelaria Prawna A. Sobczyk i Współpracownicy)

Dokument powstał w ramach projektu: Wolski pilotaż badania „Retrospektywna analiza zbiorów danych o osobach bezdomnych z terenu Warszawy z lat 2005-2009”

Warszawa, sierpień 2010 r.

WSTĘP

Opinia prawna z zakresu ochrony danych osobowych w badaniach nad bezdomnością metodą agregacji zindywidualizowanych danych gromadzonych przez placówki wspierające została opracowana przez zespół Fundacji Panoptykon na zlecenie Pracowni Badań i Innowacji Społecznych STOCZNIA w ramach projektu wolskiego pilotażu badania „Retrospektywna analiza zbiorów danych o osobach bezdomnych z terenu Warszawy z lat 2005-2009".

Opinia powstała w oparciu o ustawę o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (zwaną dalej „**UODO**" lub „**ustawą**"), dostępne komentarze[1] i orzecznictwo oraz oficjalne porady publikowane w serwisie edu-GIODO (https://edugiodo.giodo.gov.pl/), prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych (zwanego dalej „**GIODO**"). Konsultacji eksperckiej udzieliła dr Dominika Dőrre-Nowak.

Metoda agregacji zindywidualizowanych danych pobieranych z instytucji udzielających wsparcia i gromadzących informacje o swoich klientach na potrzeby świadczonej pomocy jest z powodzeniem wykorzystywana w wielu miejscach na świecie min. w USA (Homelessness Management Information System), Wielkiej Brytanii (system zarządzany przez Homeless LINK) czy Holandii (system Federatie Opvang). Do tej pory nie była jednak stosowana w Polsce, co było w dużym stopniu uwarunkowane potocznie przekazywanymi wątpliwościami dotyczącymi jej zgodności z regulacjami zawartymi w UODO. Nigdy jednak nie przeprowadzono dokładnej analizy przepisów pozwalającej na pozytywne bądź negatywne zweryfikowanie owych wątpliwości.

Niniejsza ekspertyza właśnie to ma na celu. Zjawisko bezdomności jest bardzo wymagającym przedmiotem wszelkich badań w szczególności ilościowych ze względu na niewielki rozmiar badanej populacji w porównaniu do populacji ogólnej, jej rozproszenie i wewnętrzną mobilność. Dlatego każda metodologia pozwalająca na jego lepsze poznanie powinna być przetestowana, dostosowana do lokalnego kontekstu i jak najszybciej stosowana.

We wstępnej części opinii wyjaśnione zostały podstawowe terminy m.in. dane osobowe, dane wrażliwe, przetwarzanie danych, zbiór danych osobowych, administrator zbioru oraz powierzenie przetwarzania danych. W zasadniczej części opinii autorzy starali się udzielić odpowiedzi na pytanie o warunki, na jakich placówka wspierająca ludzi bezdomnych np. noclegownia, schronisko czy poradnia zdrowia, prowadząca rejestr osób, którym udziela wsparcia, może przekazać gromadzone dane osobowe (elektronicznie lub na papierze) badaczowi lub instytucji chcącej na ich podstawie przeprowadzić badania naukowe, których efekty mogą się przyczynić do poprawy jakości polityki społecznej. Zidentyfikowano trzy takie możliwości: (1) przekazanie danych innej instytucji (np. organizacji pozarządowej), (2) powierzenie zbioru danych innemu podmiotowi w celu przetwarzania w zakresie i celu, jaki wyznacza sam administrator, (3) upoważnienie konkretnej osoby (w tym wypadku badacza) do przetwarzania danych w ramach zawartej umowy (np. zlecenia, pracy, o dzieło). Każda z opcji została szczegółowo opisana. W dalszej części opinii przedstawiono zagadnienie anonimizacji danych, która okazuje się niezbędną procedurą, w sytuacji gdy żadna z trzech opcji przedstawionych nie ma zastosowania. Opisano także warunki przechowywania powierzonych danych, możliwości ich publikowania oraz procedurę rejestracji zbiorów danych.

[1] Komentarz do art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.02.101.926), [w:] J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych. Komentarz, LEX, 2007, wyd. IV.

Opinia została wzbogacona o przykłady konkretnych sytuacji, z jakimi mogą mieć do czynienia badacze i organizacje pozarządowe angażujące się w tego rodzaju przedsięwzięcia badawcze. Autorzy opinii przeanalizowali wskazane sytuacje pod kątem UODO, zastrzegają jednak, iż interpretacje umieszczone w sekcjach „Przykłady" nie mają charakteru oficjalnych wykładni i nie zostały oparte na istniejącym orzecznictwie (z powodu braku analogicznych spraw), a stanowią jedynie próbę wypracowania najbardziej prawdopodobnych odpowiedzi w oparciu o doświadczenia i wiedzę autorów.

Opinia prawna powstała dzięki dotacji przyznanej Pracowni Badań i Innowacji Społecznych Stocznia na realizację projektu o nazwie Wolski pilotaż badania „Retrospektywna analiza zbiorów danych o osobach bezdomnych z terenu Warszawy z lat 2005-2009" w konkursie Wojewody Mazowieckiego dla Organizacji Pozarządowych w 2010 roku.

OCHRONA DANYCH OSOBOWYCH: PODSTAWOWE TERMINY

DANE OSOBOWE

Za dane osobowe uważa się - według ustawy - "**wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej** " (art. 6 UODO).

Możemy zatem wyróżnić trzy elementy (przesłanki) definicji „danych osobowych":

1) **informacja**

Pojęcie informacji oznacza komunikat wyrażony i zapisany w jakikolwiek sposób: znakami graficznymi, symbolami, w języku komputerowym, na fotografii itd.), niezależnie od sposobu ich udostępniania i pozyskania. Użycie zwrotu "**wszelkie** informacje" służy podkreśleniu, że w grę wchodzą informacje odnoszące się do każdego aspektu osoby, tj. jej stosunków osobistych i rzeczowych, jej życia zawodowego, prywatnego, wykształcenia, wiedzy czy cech charakteru[2].

2) **dotycząca osoby fizycznej**

Ta przesłanka rozstrzyga, że nie są danymi osobowymi zbiory informacji dotyczące podmiotów innych niż osoby fizyczne, a więc wszelkich osób prawnych (spółek prawa handlowego, organizacji pozarządowych, jednostek organizacyjnych, organów administracji państwowej czy samorządowej).

3) **zidentyfikowanej lub możliwej do zidentyfikowania**

Zgodnie z tą przesłanką, za dane osobowe uznaje się tylko te informacje, które "umożliwiają ustalenie tożsamości osoby fizycznej".[3] Imię i nazwisko są (same w sobie) takimi informacjami tylko, jeśli są to dane unikatowe (tzn. nie ma drugiej osoby o tym samym zastawie imienia i nazwiska), a w pozostałych przypadkach dopiero w połączeniu z dodatkowymi informacjami (np. data i miejsce urodzenia, miejsce pracy, wykonywany zawód, tytuł naukowy czy cechy zewnętrzne). Za dane z zasady „jednoznacznie identyfikujące" uznaje się np. numer PESEL i strukturę DNA.

Wątpliwości co do tego, jakie informacje i w jakim kontekście pozwalają na ustalenie tożsamości osoby (a przez to stanowią jej dane osobowe) w dużej mierze rozstrzyga sama ustawa. Według art. 6 ust. 2 UODO, za „**osobę możliwą do zidentyfikowania** uważana jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jego cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne".

Numerami identyfikacyjnymi, o których mowa w komentowanym przepisie, są: numer powszechnego elektronicznego systemu ewidencji ludności (PESEL); numer identyfikacji podatkowej (NIP), a także numer dokumentu tożsamości (dowodu osobistego oraz paszportu). Czynnikami określającymi cechy osoby mogą być m.in.: wygląd zewnętrzny, wzór siatkówki oka; struktura kodu genetycznego, grupa

[2] Komentarz …, Art. 6 UODO, par. 4

[3] Komentarz … Art. 6 UODO, par. 11

krwi; status majątkowy; pochodzenie, poglądy polityczne, przekonania religijne lub filozoficzne oraz przynależność wyznaniowa, partyjna lub związkowa[4].

Pojęcie danych osobowych obejmuje także informacje, które dopiero w połączeniu z danymi spoza zbioru umożliwiają identyfikację danej osoby. Art. 6 ust. 3 UODO wprowadza jednak w tym zakresie istotne ograniczenie: **nie mają charakteru danych osobowych informacje, przy których ustalenie tożsamości osoby wymaga nieproporcjonalnie dużego nakładu czasu, pracy czy kosztów**. A zatem za dane osobowe uważa się tylko informacje które bez nadzwyczajnego wysiłku i bez nieproporcjonalnie dużych nakładów dają się "powiązać" z określoną osobą, zwłaszcza przy wykorzystaniu powszechnie dostępnych źródeł informacji (np. Internet).

Wobec powyższego nie ulega wątpliwości, że **nie są danymi osobowymi wszelkie informacje anonimowe**, czyli niedające się powiązać z indywidualnymi osobami. W tej kategorii mieszczą się przede wszystkim dane pozyskiwane do celów statystycznych.

Przykłady:

(1) Zeszyt meldunkowy prowadzony w schronisku w którym pod datą wpisane są wyłącznie imiona i nazwiska osób znajdujących się danej nocy w placówce może być zbiorem danych osobowych, jeśli przynajmniej niektóre z zestawów danych imię + nazwisko + data noclegu pozwala na identyfikację konkretnych osób. Może się zdarzyć tak, że niektóre dane nie będą możliwe do powiązania z konkretnymi osobami, czyli nie będą uważane za dane osobowe w rozumieniu ustawy; to jednak nie uchyla obowiązku ochrony wobec pozostałych danych i całego zbioru (zeszytu meldunkowego). Wreszcie, wydaje się, że w przypadku takim jak zeszyt meldunkowy schroniska osoby mające dostęp do zbioru danych (zeszytu) posiadają dodatkową wiedzę na temat osób, których dane zostają w nim zapisane, i z zasady będą w stanie takie osoby zidentyfikować (wskazać) na podstawie samego imienia, nazwiska i daty noclegu. Z uwagi na tę okoliczność skłanialibyśmy się do wniosku, że zeszyt meldunkowy w schronisku dla bezdomnych z zasady należy traktować jak zbiór danych osobowych.

(2) Elektroniczny rejestr prowadzony w placówce dla bezdomnych, w którym znajdują się imiona i nazwiska mieszkańców oraz numer identyfikacyjny za pomocą którego można odnajdywać karty z szerszymi danymi o osobie znajdujące się w zbiorze papierowym, jest bez wątpienia zbiorem danych osobowych ponieważ pełny zestaw danych, do którego dostęp daje numer identyfikacyjny, pozwala bez problemu zidentyfikować poszczególne osoby. Jest to klasyczny przykład zbioru danych, które swój charakter „danych osobowych" zyskują dopiero w połączeniu z danymi spoza zbioru. Ponieważ istnieje w tym wypadku możliwość łatwego i szybkiego zidentyfikowania osoby za pomocą dodatkowych informacji (tj. zbioru papierowego, do którego pracownicy mają stały dostęp) nie ma wątpliwości, że mamy do czynienia ze zbiorem danych osobowych.

DANE WRAŻLIWE

Katalog danych wrażliwych został określony w art. 27 ust. 1. UODO. Jest to katalog zamknięty, tzn. tylko kategorie danych wprost wymienione w tym przepisie uznaje się za dane wrażliwe.

[4] Komentarz … Art. 6 UODO, par. 13

Są to następujące kategorie danych:

(1) dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową;

(2) dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym; oraz

(3) dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Z powyższego wynika, że inne rodzaje informacji o osobie, np. fakt bycia bezdomnym, samotną matką czy osobą korzystającą z pomocy społecznej, nie stanowią danych wrażliwych.

A. Przetwarzanie danych

Zgodnie z art. 7 pkt. 2 UODO przez „przetwarzanie" rozumie się przez 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**.

A zatem terminem tym objęte są wszelkie działania, jakie możemy wykonać na danych osobowych (poza wymienionymi wprost w przepisie, np.: łączenie, zestawianie, wywoływanie, rozpowszechnianie, przesyłanie). Przy czym wystarczy, że realizowana jest którakolwiek z tych operacji (np. samo zbieranie danych), abyśmy mieli do czynienia z "przetwarzaniem danych". Można nawet, tak jak autorzy komentarza do ustawy, twierdzić, że już samo czytanie danych osobowych przez administratora danych lub jego pracownika stanowi ich przetwarzanie.[5]

Przykład:

Jeśli organizacja daje zeszyt meldunkowy lub pozwala obejrzeć komputerową bazę danych np. wolontariuszowi czy badaczowi, którzy je przeglądają, uzupełniają, sortują itd. to, zgodnie z powyżej przedstawioną interpretacją pojęcia „przetwarzania", mamy do czynienia z przetwarzaniem danych. Najbezpieczniej jest przyjąć, że nawet samo uzyskanie wglądu do bazy, bez sporządzania notatek czy dokonywania jakichkolwiek operacji na danych, stanowi przetwarzanie danych osobowych.

ZBIÓR DANYCH OSOBOWYCH

Art. 7 pkt. 1 zbiór danych to **każdy posiadający strukturę zestaw danych o charakterze osobowym**, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Zawartość zbioru tworzyć mogą **dane** (informacje) **wyrażone w różny sposób:** słowem, dźwiękiem (np. zbiory nagranych wypowiedzi), obrazem (np. zbiory zdjęć używane do identyfikacji sprawców przestępstw) itd. Można przy tym uznać, że zbiorem danych osobowych jest zarówno zestaw danych odnoszących się do wielu osób, jak i do jednej osoby.

Zbiór musi wykazywać się strukturą **uporządkowaną**. Nie powinien być zatem luźnym zestawem, samą tylko sumą elementów składowych. Cechę zbioru danych stanowi "**dostępność** [zawartości danych] **według określonych kryteriów**". Chodzi tu o kryteria pozwalające na w miarę szybki i bezpośredni

[5] Komentarz … Art. 7 pkt 1.

dostęp do danych. Rezultatem uporządkowania powinna być sytuacja, w której po to, aby znaleźć pewne dane, nie jest potrzebne przeglądanie wszystkich składników zbioru. Można przyjąć, że "dostępność według określonych kryteriów" zapewnia np. indeks (skorowidz) alfabetyczny. Takie stanowisko zajmuje GIODO, który stwierdza: "Każdy zestaw danych osobowych, który umożliwia dostęp do poszczególnych danych przez jakiekolwiek kryterium, jest zbiorem danych w rozumieniu art. 7 pkt 1 ustawy. Alfabetyczne ułożenie danych osobowych według nazwiska lub nazwiska i imienia pozwala na szybkie odnalezienie informacji o osobie bez potrzeby przeglądania całego zestawu". [6]

UODO stosuje się w niektórych przypadkach przetwarzania danych bez względu na to, czy dane są przechowywane w formie zbioru czy też nie. Ustawa wyraźnie rozstrzyga, że przewidziane w niej **zasady przetwarzania danych osobowych stosuje się do danych przechowywanych w systemach informatycznych, kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych** (art. 2 ust. 2 UODO).

Przykłady:

(1) Zeszyt meldunkowy prowadzony w schronisku w którym pod datą wpisane są imiona i nazwiska osób znajdujących się danej nocy (lub w danym miesiącu) w placówce, gdzie na liście z danego dnia (miesiąca) jest od 50 do 120 imion i nazwisk oraz daty przyjęcia i opuszczenia placówki natomiast nazwiska są wpisywane tylko według kolejności przyjęcia do placówki (a nie alfabetycznie) nie jest uporządkowanym zbiorem danych, ponieważ nie da się danych poszczególnych osób wyszukać bez przejrzenia całego zeszytu. Nie mniej jednak należy pamiętać, że taki zeszyt zawiera dane osobowe (jak omówiono w przykładzie powyżej), które podlegają ochronie prawnej.

(2) Elektroniczny rejestr w placówce, w którym znajdują się imiona i nazwiska mieszkańców oraz numer identyfikacyjny za pomocą którego można odnajdywać karty z szerszymi danymi o osobie znajdujące się w zbiorze papierowym, jest zbiorem danych osobowych ze względu na elektroniczny charakter. Przyjmuje się, że każde zestawienie danych osobowych w formie elektronicznej jest zbiorem danych, ponieważ specyfika elektronicznych baz pozwala na wyszukiwanie wedle dowolnie wybranego kryterium (np. numeru identyfikacyjnego, imienia, nazwiska).

ADMINISTRATOR DANYCH

Zgodnie z ustawową definicją (art. 7 pkt. 4 UODO) za administratora danych uznaje się:

a) organ państwowy lub samorządowy,

b) państwową lub komunalną jednostkę organizacyjną,

c) podmiot niepubliczny realizujący zadania publiczne,

d) osobę prawną, jednostkę organizacyjną nieposiadającą osobowości prawnej lub osobę fizyczną, przetwarzającą dane w związku ze swą działalnością zarobkową, zawodową albo dla realizacji celów statutowych,

- który (która) decyduje o celach i środkach przetwarzania danych osobowych.

[6] *Wystarczy ułożyć alfabetycznie*, Rzeczpospolita z 20 lipca 2000 r., nr 168.

Jak wynika z powyższego, administratorami danych osobowych mogą być także **podmioty prywatne** (podmioty niepubliczne realizujące zadania publiczne, osoby fizyczne, osoby prawne takie jak organizacje pozarządowe), jeśli tylko przetwarzają dane osobowe w związku ze swoją działalnością zarobkową, zawodową lub dla realizacji celów statutowych, i które decydują o celach i środkach przetwarzania danych osobowych. To właśnie te podmioty mają status administratora danych, natomiast **nie jest administratorem osoba lub osoby pełniące funkcje kierownicze** (dyrektor, prezes, zarząd itd.), podobnie jak **nie jest administratorem oznaczony pracownik, któremu powierzono wykonywanie obowiązków związanych z ochroną i operacjami na danych osobowych**. Funkcji administratora danych nie można na takie osoby scedować.[7] Nie jest również administratorem danych **osoba, której administrator powierzył przetwarzanie danych**.

Przykład:

Jeśli organizacja pozarządowa prowadzi kilka placówek, a w każdej z nich oddzielny zbiór danych kierujący się innymi zasadami (np. inne są cele i zakres przetwarzania danych), dane wciąż mają jednego administratora, którym jest ta organizacja pozarządowa (oczywiście, organizacja działa przez swój zarząd, jednak to ona, a nie jej organy, pozostaje administratorem danych). Zasady przetwarzania czy ilość zbiorów danych są bez znaczenia: jeden administrator może zarządzać wieloma zbiorami, każdym na innych zasadach.

POWIERZENIE PRZETWARZANIA DANYCH

Instytucja powierzenia przetwarzania danych jest wprost uregulowana w ustawie (Art. 31 UODO). Zgodnie z tym przepisem, **administrator danych może powierzyć przetwarzanie danych innemu podmiotowi, w drodze umowy zawartej na piśmie**. Przedmiotem zlecenia mogą być też tylko niektóre procedury składające się na pojęcie "przetwarzania" (patrz I. C). Na przykład zlecić można jedynie usunięcie danych (zniszczenie kartotek, usunięcie zawartości z elektronicznych nośników danych itp.).[8]

Powierzenie przetwarzania danych wymaga **umowy zawartej na piśmie**. Umowa powinna zawierać następujące elementy:

(i) wskazanie kto i komu powierza przetwarzanie danych;

(ii) określenie jakie dane są przedmiotem powierzenia (jaki zbiór; czy cały zbiór, czy części zbioru);

(iii) określenie dokładnego celu i zakresu przetwarzania (np. przetwarzanie w celu przeprowadzenia badań naukowych; usuwanie danych; segregowanie itp.);

(iv) określenie czasu trwania umowy

(v) zobowiązanie podmiotu, któremu dane są powierzane do ich odpowiedniego zabezpieczenia i ochrony.

Umowę powierzenia podpisuje, zgodnie z ogólnymi zasadami prawa cywilnego, osoba umocowana zgodnie ze statutem organizacji / placówki do jej reprezentowania, np. dyrektor.

7 Komentarz … Art. 7 par. 4

8 Komentarz, Art. 31, par. 2

Podmiot przyjmujący od administratora "zlecenie przetwarzania danych" może to **przetwarzanie prowadzić wyłącznie w przewidzianym umową zakresie** (chodzi tu głównie o rodzaj danych) **oraz w określonym umową celu** (chodzi tu głównie o przeznaczenie danych). Zakres i cel mogą być doprecyzowane przez wskazówki i polecenia udzielane ze strony administratora (zlecającego). A zatem niedozwolone byłoby w takiej sytuacji przetwarzanie danych poza ramami upoważnienia wynikającego z umowy (tj. w szerszym niż to umowa przewiduje zakresie czy dla innego niż wynikającego z umowy celu).

Co istotne, podmiot któremu powierzono dane jest **zobowiązany do podjęcia wymaganych prawem środków zabezpieczenia zbioru danych przed rozpoczęciem przetwarzania**. Chodzi tu o środki techniczne i organizacyjne zabezpieczające dane przede wszystkim przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (patrz punkt II. C)

ZAGADNIENIA SZCZEGÓŁOWE

A. Na jakich warunkach placówka może przekazać zbiory danych osobowych elektroniczne/ papierowe badaczowi do badań naukowych czy badań, które mają się przyczynić do poprawy jakości polityki społecznej?

Są trzy podstawowe scenariusze, według których można przekazać zbiory danych osobowych do celów badań naukowych lub społecznych:

1) przekazanie danych przez administratora bazy innej instytucji prowadzącej badania;

2) powierzenie zbioru danych innemu podmiotowi w celu przetwarzania w zakresie i celu, jaki wyznacza sam administrator;

3) upoważnienie konkretnej osoby (w tym wypadku badacza) do przetwarzania danych w ramach zawartej umowy (np. zlecenia, pracy, o dzieło).

Poniżej przedstawiamy każdy z tych scenariuszy, analizując przesłanki przetwarzania danych oraz możliwości ich zastosowania do sytuacji objętej niniejszą analizą.

PRZEKAZANIE DANYCH INNEJ INSTYTUCJI (ORGANIZACJI POZARZĄDOWEJ)

Przekazanie danych innej instytucji, np. organizacji prowadzącej badania naukowe lub społeczne (w tym organizacji pozarządowej) może nastąpić tylko w oparciu o przesłanki z UODO, których katalog jest zamknięty. Nie będziemy omawiać każdej przesłanki przewidzianej w ustawie (jest ich kilkanaście), a jedynie te, które mogłyby znaleźć zastosowanie w analizowanej sytuacji.

W sytuacji przekazania danych przez instytucję/organizację udzielającą pomocy osobom bezdomnym innej organizacji pozarządowej, która w oparciu o te dane prowadzi niezależne badania, można rozważać następujące przesłanki:

(a) Art. 23 ust. 1 pkt. (1), zgodnie z którym przetwarzanie danych jest dopuszczalne, jeśli osoba, której dane dotyczą, wyrazi na to zgodę.

Uzyskanie zgody osoby, której dane dotyczą jest podstawową i najbezpieczniejszą przesłanką przetwarzania danych przez podmioty niepubliczne. Ta przesłanka będzie spełniona tylko, jeśli każda

osoba, której dane mają być przetwarzane (w tym przypadku przekazane organizacji prowadzącej badania) wyrazi **świadomą, dobrowolną i skonkretyzowaną** zgodę na takie działanie. Aby zgoda spełniała wymienione powyżej warunki, administrator danych (tj. organizacja prosząca o udzielenie zgody) **musi poinformować** osobę, której dane dotyczą, o: (i) swojej **nazwie i adresie**; (ii) **rodzaju danych**, jakie mają być przetwarzane; (iii) oraz **celu i zakresie przetwarzania**.

Oświadczenie woli, jakim jest zgoda na przetwarzanie danych, musi być udzielone w sposób zupełnie **dobrowolny**, a zatem bez presji czy warunków stawianych osobie, której dane dotyczą. Zgoda nieskonkretyzowana czy wymuszona jest z mocy prawa nieskuteczna. Jednym słowem, wyrażający zgodę musi mieć pełną świadomość tego, na co się godzi.[9]

Jak wynika z powyższego, skutecznie zgodzić się można tylko na przekazanie danych **konkretnej instytucji, czyli wskazanej co do nazwy i adresu.** Taka zgoda może obejmować wielokrotne przekazanie danych w przyszłości, preferowane jest natomiast wskazanie czasu (np. przez okres 10 lat). Przyjmuje się natomiast, że nie można skutecznie zgodzić się na przekazanie danych w przyszłości nieokreślonej bliżej instytucji, w nieokreślonym celu.

Zgoda na przetwarzanie danych zwykłych nie musi być wyrażona na piśmie, jednak jest to zalecane dla celów dowodowych. Natomiast w przypadku danych wrażliwych (por. punkt I. B) ustawa wprost wymaga zgody wyrażonej na piśmie.

Co istotne, zgodnie z ogólnymi zasadami ochrony danych osobowych, także w przypadku przetwarzania danych w oparciu o tę przesłankę **zakres i czas przetwarzania musi być z góry określony przez administratora i adekwatny do celu**. A zatem nie można wykorzystywać przesłanki zgody w sposób blankietowy, tj. w celu uzyskania dostępu do danych, które następnie będą wykorzystywane w dowolny sposób. Np. jeśli osoba, której dane dotyczą, zgadza się na wykorzystywanie jej danych osobowych na potrzeby konkretnego badania naukowego lub społecznego, organizacja prowadząca projekt badawczy nie może zatrzymać tych danych po zrealizowaniu projektu ani wykorzystywać ich do innych celów w trakcie jego trwania.

Przesłanka adekwatności dotyczy także **rodzajów przetwarzanych danych**: nawet na podstawie zgody nie można przetwarzać takich rodzajów danych, które nie są obiektywnie niezbędne do zrealizowania celu, o którym była mowa w klauzuli zgody. Np. jeśli na potrzeby przeprowadzenia konkretnego badania potrzebne są podstawowe dane identyfikujące osobę oraz informacje o jej stanie zdrowia i miejscu pobytu, natomiast nie ma znaczenia płeć czy wyznanie, organizacja prowadząca badania nie ma prawa przetwarzać takich danych nawet jeśli uzyskała na to formalną zgodę.

Przykłady:

(1) To, czy organizacja prowadzi wyłącznie zbiór w formie elektronicznej, czy papierowej nie ma żadnego znaczenia dla formy uzyskiwania zgody od osoby, której dane dotyczą. A zatem w każdej konfiguracji można poprosić o zgodę na piśmie, w formie papierowej, lub zgodę w formie elektronicznej („tick box" na formularzu internetowym itp.). Ważna jest tylko treść klauzuli zgody, która musi wskazywać cel i zakres przetwarzania danych. Z jednym zastrzeżeniem: tak jak

[9] Wyrok Naczelnego Sądu Administracyjnego z dnia 4 kwietnia 2003 r. (sygn. akt II SA 2135/2002)

wyjaśniamy powyżej, w przypadku przetwarzania danych wrażliwych ustawa nakłada obowiązek uzyskania zgody w formie pisemnej. To oznacza, że konieczna jest albo zgoda na papierze, z klasycznym podpisem osoby udzielającej zgody, albo oświadczenie woli w formie elektronicznej potwierdzone tzw. kwalifikowanym podpisem elektronicznym.

(2) Jeśli mieszkaniec schroniska w momencie przyjęcia do schroniska wypełnia kwestionariusz „kartę mieszkańca" zawierającą następującą formułę „Wyrażam zgodę na przetwarzanie przez (miejsce na pieczątkę placówki/organizacji) moich danych osobowych w systemach informatycznych i innych zbiorach ewidencyjnych. Potwierdzam otrzymanie informacji, że moje dane osobowe są zbierane w związku z udzieleniem mi pomocy, przysługuje mi prawo wglądu do moich danych prawo ich poprawiania." to zgodnie z przeważającą interpretacją nie udziela skutecznej zgody na przetwarzanie danych. Tak sformułowana klauzula zgody nie jest kompletna i nie spełnia ustawowych wymogów, ponieważ nie zawiera określenia celów i zakresu przetwarzania danych.

Klauzula powinna wyraźnie wskazywać w jakim celu i zakresie dane będą przetwarzane – tylko wtedy jest kompletna i zapewnia możliwość udzielenia poinformowanej zgody. Np. „Wyrażam zgodę na przetwarzanie przez (miejsce na pieczątkę placówki/organizacji) moich danych osobowych w systemach informatycznych i innych zbiorach ewidencyjnych ww. organizacji w zakresie niezbędnym, do udzielenia mi pomocy oraz przeprowadzenia na podstawie moich danych uzasadnionych badań naukowych lub społecznych".

Ponadto, jeśli w celu zwiększenia jakości świadczonej pomocy, dana placówka ma zamiar przekazywać dane innym organizacjom, takie działanie **musi** być wyraźnie przewidziane w klauzuli zgody, najlepiej ze wskazaniem podmiotu, któremu dane mają być przekazane: „Wyrażam zgodę na przetwarzanie przez (miejsce na pieczątkę placówki/organizacji) moich danych osobowych w systemach informatycznych i innych zbiorach ewidencyjnych ww. organizacji w zakresie niezbędnym, do udzielenia mi pomocy oraz na przekazywanie moich danych [nazwa i adres organizacji] w celu przeprowadzenia uzasadnionych badań naukowych lub społecznych".

Niezwykle istotne w tym kontekście jest to, aby zapewnić dobrowolność zgody. Placówka w żadnym razie nie może uzależniać udzielenia pomocy od faktu wyrażenia zgody na przetwarzanie danych ani wywierać nacisku innego typu (np. psychologicznego) na osoby pytane o zgodę. W innym wypadku uzyskana zgoda będzie uważana za wymuszoną, a przez to nieskuteczną.

(3) Klauzula zawarta w karcie mieszkańca może przewidywać zgodę osoby, której dane dotyczą, na przetwarzanie jej danych osobowych do celów badawczych także w przyszłości (a zatem bez konieczności uzyskiwania zgody na każde prowadzone badanie/analizę) pod warunkiem, że będzie w niej określony cel i zakres przetwarzania danych oraz nazwa i adres organizacji, której dane mają zostać przekazane (dokładnie tak, jak w powyższym przykładzie). Optymalnie byłoby również wskazać w takim przypadku czas, przez jaki dane mogą być przetwarzane w ten sposób, np. „przez okres 10 lat od momentu uzyskania zgody".

(b) Art. 27 ust 2 pkt. (9) zgodnie z którym przetwarzanie danych jest dopuszczalne, jeśli jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego.

Aby dane mogły być przekazane organizacji prowadzącej badania w oparciu o tę przesłankę, muszą zostać spełnione łącznie następujące warunki:

(i) Prowadzone badania muszą mieć **charakter naukowy**

Kwestia, czy badania społeczne prowadzone przez organizację pozarządową na potrzeby projektowania polityki społecznej mogą być uznane za „naukowe" nie była przedmiotem orzeczeń sądu ani oficjalnych interpretacji. Dlatego nie możemy w tym zakresie udzielić wiążącej interpretacji. Wydaje się jednak, że mogą pojawić się na tym tle poważne wątpliwości w sytuacji, gdy badania prowadzone są przez organizację, która nie ma statusu jednostki badawczej ani naukowej, a tym samym nie jest poddana analogicznym wymogom co do metodologii badań. Z drugiej strony, ważnym argumentem na rzecz charakteru naukowego prowadzonych badań może być fakt, że są one zaprojektowane i prowadzone przez osoby posiadające stopień naukowy. Nie byłoby wątpliwości w tym zakresie, gdyby badania realizowała jednostka akademicka, pracownik akademicki w ramach swoich badań, student na potrzeby uzyskania dyplomu czy doktorant na potrzeby uzyskania stopnia naukowego. To, czy dana organizacja pozarządowa ma przewidziane w swoich celach statutowych prowadzenie badań naukowych, nie wpływa na jej ocenę z punktu widzenia ustawy. Tzn. wciąż pojawiają się te same wątpliwości, na ile można uznać za „naukowe" badania prowadzone przez jednostkę, która nie ma charakteru akademickiego.

Gdyby dana organizacja chciała z tej przesłanki skorzystać w ramach realizowanych projektów badawczych, aby rozstrzygnąć powyższe wątpliwości zalecalibyśmy wystąpienie z prośbą o wiążącą interpretację do GIODO.

(ii) Przetwarzanie danych musi być **konieczne do przeprowadzenia badań** naukowych **(dotyczy wyłącznie danych wrażliwych)**

Ten warunek odnosi się do **rodzajów danych oraz zakresu i czasu ich przetwarzania**. W żadnym wypadku nie można zakładać, że organizacja, która w oparciu o tę przesłankę uzyskała dane na potrzeby badań naukowych może je wykorzystywać swobodnie w ramach takiej działalności i przechowywać bez ograniczeń. Zgodnie z ogólnymi zasadami przetwarzania danych, które zostały podkreślone w cytowanym przepisie, przetwarzanie jest dopuszczalne tylko w zakresie koniecznym do uzyskania założonego rezultatu. A zatem organizacja prowadząca badania może wykonywać tylko takie działania na danych, jakie są obiektywnie potrzebne do zrealizowania celu badań (i jest to w stanie wykazać w przypadku kontroli). Dane powinny zostać usunięte natychmiast po zrealizowaniu celu badań. To ograniczenie dotyczy także rodzajów przetwarzanych danych – organizacja nie ma prawa przetwarzać takich rodzajów danych, które nie są obiektywnie konieczne do zrealizowania celu badawczego. Do problematyki publikacji wyników badań odnosimy się poniżej (punkt II.D).

Wreszcie, co bardzo istotne, **omawiana przesłanka dotyczy jedynie przetwarzania danych wrażliwych**. A zatem organizacja może z niej skorzystać jedynie w sytuacji, w której zbiór danych, który ma zostać jej przekazany dla celów badawczych, zawiera dane wrażliwe (definicja danych wrażliwych została omówiona w punkcie I. B).

POWIERZENIE ZBIORU DANYCH INNEMU PODMIOTOWI

Zasady i procedura powierzenia przetwarzania danych zostały uregulowane w art. 31 UODO i opisane szczegółowo powyżej (punkt I. F). Podsumowując, powierzenie przetwarzania tym się różni

od przekazania danych innemu pomiotowi, który następnie będzie takie dane sam przetwarzał, że w przypadku powierzenia w ogóle nie dochodzi do samodzielnego przetwarzania danych przez inny podmiot (tj. ten, któremu dane powierzono). Jest tak dlatego, że **pełną kontrolę nad celami oraz środkami przetwarzania danych zachowuje podmiot powierzający** (formalnie wciąż administrator danych). Innymi słowy, z prawnego punktu widzenia to **organizacja powierzająca dane wciąż je przetwarza,** tyle że nie „własnymi rękami", ale wykorzystując do tego inny podmiot.

Dla uproszczenia pojęć i odróżnienia tej sytuacji od opisanej w powyższym punkcie sytuacji przekazania danych organizacji do samodzielnego przetwarzania, poniżej będziemy posługiwać się samym pojęciem „powierzenie danych", bez wspominania o „przetwarzaniu" danych przez organizację, której powierzono dane.

W praktyce oznacza to, że organizacja pozarządowa, której powierzono dane (ale nie przekazano do samodzielnego przetwarzania), mogłaby dokonywać na nich wyłącznie takie działania, jakie zostały wprost przewidziane **w umowie powierzenia**. Jeśli zatem organizacja (placówka) powierzająca dane (i, z punktu widzenia ustawy wciąż je przetwarzająca, tzn. decydująca o celach i zakresie przetwarzania danych) nie zawrze u umowie takiego celu, jak użycie danych w celu przeprowadzenia określonych badań naukowych czy społecznych, takie działanie na danych nie będzie możliwe. Co więcej, **organizacja, której dane zostały powierzone** (w analizowanej sytuacji organizacja pozarządowa realizująca badania) **nie może włączyć powierzonych danych do własnego zbioru.** Jej rola ogranicza się do **dokonywania zleconych operacji na danych** (zgodnie z zawartą umową powierzenia), **w ramach powierzonego jej zbioru**.

Tym samym, jeśli celem badań miałoby być porównanie lub zintegrowanie zbiorów danych pochodzących z kilku różnych organizacji (placówek) wydaje się, że w ramach stosunku powierzenia (nawet zawartego z kilkoma organizacjami jednocześnie) **takie działanie nie będzie możliwe,** ponieważ z definicji oznaczałoby to przetwarzanie danych poza poszczególnymi powierzonymi zbiorami oraz w celach szerszych, niż cele poszczególnych administratorów danych (tj. organizacji lub placówek powierzających dane). Na gruncie istniejącej doktryny wydaje się, że jednoczesne zawarcie kilku umów powierzenia, z których każda przewidywałaby zintegrowanie zbiorów pochodzących od różnych administratorów w jeden duży zbiór, byłoby potraktowane jak obejście prawa (tj. ustawowych przesłanek dla przekazania danych innemu podmiotowi – patrz punkt (1)).

Umowę powierzenia zawiera podmiot będący administratorem danych (czyli odpowiednia organizacja / placówka, do której należy baza danych). W jej imieniu działa osoba upoważniona (np. na podstawie statutu) do składania oświadczeń woli w jej imieniu, czyli stosujemy ogólne zasady reprezentacji w stosunkach cywilnoprawnych. W praktyce najczęściej osobą umocowaną do składania oświadczeń woli jest prezes lub dyrektor, ewentualnie inne osoby zarządzające, jeśli mają takie prawne umocowanie. Zasady reprezentacji oraz umocowanie konkretnych osób można zweryfikować w Krajowym Rejestrze Sądowym (każdy może uzyskać odpis z rejestru prowadzonego dla danej organizacji).

UPOWAŻNIENIE KONKRETNEJ OSOBY (BADACZA) DO PRZETWARZANIA DANYCH W RAMACH ZAWARTEJ UMOWY

Organizacja (placówka) będąca administratorem danych może upoważnić konkretną osobę (np. badacza) do pracy ze zbiorami w takiej wersji, w jakiej przechowywane są one w organizacji (placówce). Wymaga to jednak spełnienia dwóch warunków:

(i) istnienia stosunku umownego między organizacją (placówką) a badaczem

Badacz nie może być osobą zewnętrzną wobec organizacji. Pomiędzy nim a organizacją **musi istnieć stosunek umowny** – niekoniecznie umowa pracy, może to być umowa zlecenia, umowa o dzieło czy nawet umowa wolontariacka – który uzasadnia fakt pracy z danymi. Nie ma przy tym znaczenia fakt uzyskiwania wynagrodzenia za świadczoną pracę, tj. umowa zlecenia mogłaby opiewać na symboliczna kwotę.

W praktyce, organizacja (placówka) mogłaby np. zlecić konkretnemu badaczowi przeprowadzenie analizy gromadzonych przez nią danych na potrzeby realizowanego przez organizację (placówkę) programu pomocowego czy kampanii społecznej. Istotne jest, aby treść zlecenia uzasadniała potrzebę pracy z danymi oraz aby było to zlecenie na rzecz organizacji. Tym samym trudno sobie wyobrazić zlecenie, które faktycznie nie służy organizacji (placówce), a tylko celom własnym badacza (np. analiza danych, która *de facto* nie będzie wykorzystana przez organizację). Zawarcie takiej umowy wraz z upoważnieniem do przetwarzania danych mogłoby być uznane za ominięcie prawa. Klasyczną sytuacją, która powinna być traktowana jako punkt odniesienia, jest upoważnienie do przetwarzania danych stałego pracownika organizacji (placówki), któremu dostęp do danych jest obiektywnie niezbędny w ramach wykonywanej pracy (np. pracownik socjalny pracujący z klientami ośrodka świadczącego pomoc).

Przykład:

Organizacja (placówka) i badacz mogą dość dowolnie ukształtować stosunek pracy czy zlecenia. To organizacja (placówka) decyduje o tym, jaki produkt z pracy badacza chciałaby otrzymać. Np. strony mogą się umówić, że badacz w oparciu pracę nad zbiorem danych osobowymi przygotuje dla organizacji np. raport statystyczny o mieszkańcach lub formularz bazy danych (do którego będzie można dane wpisywać w przyszłości). Tego typu zlecenie można uznać za służące organizacji, a zatem uzasadniające upoważnienie do przetwarzania danych.

Nie mniej jednak, odrębną kwestią jest to, czy badacz może dane, na których pracuje wykorzystać do innych, własnych celów badawczych. W oparciu o interpretację ustawy nie jest to możliwe. Badacz może przetwarzać dane (przypominamy, że to pojęcie zawiera w sobie wszelkie czynności, w tym sam wgląd do zbioru) wyłącznie w takim celu i zakresie, jaki wynika z treści upoważnienia od organizacji (placówki). Treść upoważnienia powinna wynikać z zdań, jakie realizuje sama organizacja (placówka). Można sobie jednak wyobrazić taką sytuację, że organizacja (placówka), która normalnie świadczy tylko doraźną pomoc osobom bezdomnym dochodzi do wniosku, że potrzebny jest jej raport statystyczny i w tym celu zatrudnia pracownika lub wolontariusza. Treść takich „dodatkowych zleceń" musi oczywiście pozostawać w granicach prawdopodobieństwa i mieć zawsze związek z realnymi potrzebami organizacji (placówki).

Bez wątpienia do relacji organizacja – badacz nie można zastosować logiki umowy barterowej „coś za coś" (np. badacz korzysta z danych dla własnych celów, a „w zamian" przygotowuje dla organizacji raport).

(ii) upoważnienia udzielonego przez odpowiednio umocowaną osobę

Każda osoba, która ma dostęp do danych w ramach danej organizacji (placówki) musi posiadać odpowiednie upoważnienie. **Dotyczy to wszystkich osób, bez względu na ich rolę, stanowisko służbowe czy podstawę prawną świadczenia usług na rzecz organizacji.** Wyraźnie stwierdza to art. 37 UODO: „Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych." Upoważnieniem powinny się wykazać nie tylko osoby, które na stałe zajmują się przetwarzaniem danych (czyli pracownicy administratora), ale też osoby czasowo wykonujące czynności w tym zakresie (np. osoby dokonujące przeglądów serwisowych sprzętu czy oprogramowania z tego względu, że mają one dostęp do danych osobowych, a zatem można uznać, iż przetwarzają dane).[10] W praktyce zatem, takie upoważnienie muszą posiadać zarówno osoby pracujące bezpośrednio z danymi, nawet jeśli wykonują czysto mechaniczne czynności (np. wprowadzanie danych do zbioru), jak i kierownictwo organizacji, o ile tylko chce mieć możliwość dostępu do danych. Pierwsze osoby w organizacji upoważnione do przetwarzania danych to te, które zostają zgłoszone do GIODO w momencie rejestrowania zbioru danych.

Ustawa nie przesądza ani treści, ani formy upoważnienia do przetwarzania danych wydanego przez administratora danych. Ze względów dowodowych zaleca się jednak, żeby upoważnienie takie miało formę pisemną. Upoważnienie powinno mieć charakter imienny, powinno też określać dozwolony zakres przetwarzania danych. W praktyce nadanie upoważnienia powinno być związane z podpisaniem przez osobę odbierającą upoważnienie **oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych oraz o przyjęciu do wiadomości obowiązku zachowania tajemnicy.**[11]

Upoważnienia może dokonać każda osoba, która w ramach organizacji (placówki) posiadającej zbiór danych i będącej administratorem danych ma uprawnienia do przetwarzania danych oraz udzielania dalszych upoważnień. Wyznaczenie takich osób w pełni zależy od wewnętrznej struktury organizacji: osoby upoważnione do przetwarzania danych można wyznaczyć dowolnie, w zależności od wewnętrznych potrzeb i modelu pracy. Umocowanie danej osoby do przetwarzania danych i udzielania dalszych upoważnień musi jednak jasno wynikać z **dokumentacji**, którą opracowuje organizacja (placówka) w związku z przetwarzaniem danych.

Ustawa określa dokładnie zasady prowadzenia ewidencji osób upoważnionych do przetwarzania danych**.** Zgodnie z art. 39 ust. 1 **organizacja będąca administratorem danych musi prowadzić ewidencję osób upoważnionych do przetwarzania danych**. Taka ewidencja zawiera:

1) imię i nazwisko osoby upoważnionej,

2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,

10 Komentarz … Art.37, par. 1

11 Komentarz … Art. 37, par 3

3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

A zatem w celu uzyskania upoważnienia do przetwarzania danych, badacz również musiałby zostać wpisany do ewidencji prowadzonej przez organizację (placówkę).

Co bardzo istotne w kontekście analizowanej sytuacji, **osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia** (art. 26 ust. 2 UODO). Oznacza to, że pod groźbą odpowiedzialności karnej badaczowi nie wolno ujawniać danych, do których uzyskał dostęp ani wykorzystywać ich poza ramami udzielonego mu zlecania (stosunku pracy).

Dane mogą być **przenoszone poza miejsce wykonywania zlecania** (świadczenia pracy) – np. na przenośnym komputerze czy nośniku pamięci – o ile takie urządzenie zostanie odpowiednio zabezpieczone zgodnie z ogólną polityką ochrony danych (patrz punkt II. C).

Badacz, który został upoważniony do przetwarzania danych zyskuje do nich pełny dostęp w zakresie swojego upoważnienia. Np. badacz upoważniony do przetwarzania zbioru danych osobowych osób, którym organizacja udzielała pomocy w ciągu ostatnich pięciu lat zyskuje pełny dostęp do tego zbioru w takiej formie, w jakiej przechowuje dane organizacja (placówka). Upoważnienie nie oznacza jednak dostępu do wszelkich danych posiadanych przez organizację, a jedynie do tych, które zostały wskazane w upoważnieniu (np. badacz upoważniony tylko do przetwarzania danych klientów nie uzyska dostępu do danych pracowników organizacji itp.).

Procedura upoważnienia jest taka sama bez względu na rodzaj przetwarzanych danych. Nie ma w tym wypadku znaczenia, czy w zbiorze znajdują się dane zwykłe czy wrażliwe, imię i nazwisko czy numer PESEL, tak długo jak z upoważnienia (i ewidencji) wyraźnie wynika, jaki zakres danych został udostępniony danej osobie.

ANONIMIZOWANIE DANYCH

"Kodowanie" danych to określenie potoczne, czynność, o której będzie mowa w tym punkcie, w języku prawniczym określana jest terminem "anonimizacja".

(1) Kiedy potrzebne jest anonimizowanie danych?

Co do zasady żadne dane **nie muszą** być anonimizowane. Prawo nie przewiduje obowiązku anonimizowania danych; ustawa nie zawiera nawet definicji anonimizacji. Natomiast można uznać, że **anonimizacja jest potrzebna**, a nawet konieczna, w przypadku, gdy **nie ma podstawy prawnej do przetwarzania danych osobowych, a mimo to dana osoba lub podmiot chciałaby uzyskać dostęp do danych**.

Zgodnie z definicją danych osobowych – jako informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (por. punkt I. A) – **po przeprowadzeniu anonimizacji dane tracą charakter danych osobowych,** a zatem można je przetwarzać bez ograniczeń, jakie nakłada UODO.

W odniesieniu do analizowanej sytuacji, jeśli nie mogą być spełnione przesłanki umożliwiające przekazanie danych osobowych organizacji prowadzącej badania naukowe lub społeczne (patrz punkt II. A), wówczas jedynym sposobem na przeprowadzenie analizy danych jest ich zanonimizowanie.

(2) Jakie warunki musi spełniać procedura anonimizowania?

Ani ustawa, ani orzecznictwo ani GIODO nie precyzują warunków przeprowadzenia skutecznej anonimizacji. Wydaje się, że w takiej sytuacji trzeba się odwołać do zasad logiki ogólnej.

Dane są zanonimizowane wtedy, kiedy nikt (osoba fizyczna czy podmiot) kto uzyskał je w takiej postaci **nie jest w stanie odtworzyć połączenia pomiędzy zestawem danych a konkretną osobą, do której pierwotnie ten zestaw danych był przypisany.** Nie oznacza to, że nigdzie nie może istnieć klucz łączący te dwa zbiory: zbiór osób, do których dane były pierwotnie przypisane i zbiór danych zanonimizowanych. Taki klucz może być przechowywany przez administratora danych. Natomiast **klucz ten nie może być ani dostępny ani możliwy do odtworzenia dla osób / podmiotów, które nie są uprawnione do przetwarzania** (w tym odczytywania informacji z) **pierwotnego zbioru** danych osobowych.

Brak możliwości odtworzenia powiązania pomiędzy zbiorem danych zanonimizowanych a pierwotnie z nim powiązanymi danymi osobowymi jest warunkowany rodzajem użytego klucza czy algorytmu szyfrującego. Wydaje się, że zbyt prosty algorytm, który łatwo złamać z pomocą powszechnie dostępnej technologii nie spełniałby tego kryterium. Nie spełnia też wymogów anonimizacji tzw. pseudo-anonimizacja, czyli zastąpienie pierwotnych danych osobowych swoistym pseudonimem. Rodzajem takiego pseudonimu może być np. identyfikator zbudowany na zasadzie zestawienia pierwszych lister imienia i nazwiska osoby, której dotyczy zestaw danych oraz jej daty urodzenia. Tak skonstruowany pseudonim jest możliwy do "rozszyfrowania" dla osoby z odpowiednią wiedzą kontekstową i dlatego nie wydaje się być bezpieczną formą anonimizowania danych.

Natomiast spełnia warunki anonimizacji zwykły klucz szyfrujący (tj. ciąg cyfr używanych jako podstawa do przekształcenia innego ciągu znaków), który generuje identyfikatory oparte wyłącznie na cyfrach, kompletnie oderwane od informacji źródłowej. Zasadą działania klucza jest, że przypisuje unikalny identyfikator danemu zestawowi danych, tzn. dla danej kombinacji imienia, nazwiska, daty urodzenia i miejsca pobytu osoby system wygeneruje identyfikator właściwy tylko dla tej kombinacji. Jeśli taka kombinacja się powtórzy, system ponownie wygeneruje identyczny identyfikator. Oderwanie od informacji źródłowej oznacz tylko brak „śladów" w identyfikatorze zaczerpniętych z oryginalnego zbioru danych, np. numeru z daty urodzenia czy litery z imienia lub nazwiska.

C. PRZECHOWYWANIE POWIERZONYCH/PRZETWARZANYCH DANYCH

W kwestii przechowywania i zabezpieczania danych obowiązują takie same zasady, bez względu na to w jaki sposób (tj. na jakiej podstawie prawnej) dana organizacja uzyskała dostęp do danych. Zgodnie z ustawą, te same zabezpieczenia w stosunku do przechowywanych danych musi zastosować administrator (tj. podmiot/osoba, która decyduje o celach i środkach przetwarzania danych), co organizacja pozarządowa, której dane zostały jedynie powierzone przez administratora (por. art. 31 UODO oraz Rozdział 5 UODO). Badacz czy inna osoba fizyczna, która przetwarza dane z upoważnienia swojego pracodawcy/zleceniodawcy musi się do takich zabezpieczeń stosować, natomiast nie ponosi osobistej odpowiedzialności za ich wprowadzenie w miejscu pracy. Środki zabezpieczenia danych zostaną bardziej szczegółowo przedstawione poniżej.

Zgodnie z art. 36 ust. 2 UODO administrator danych (tj. każda organizacja przetwarzająca dane) musi posiadać dokumentację opisującą sposób przetwarzania danych oraz ich zabezpieczania.

Administrator danych musi także wyznaczyć **administratora bezpieczeństwa informacji** (ABI), nadzorującego przestrzeganie zasad ochrony.

Szczegółowe zasady prowadzenia takiej dokumentacji określa Rozporządzenie **Ministra Spraw Wewnętrznych i Administracji** z dnia 29 kwietnia 2004 r, stanowiące aneks do niniejszej opinii.

(1) W jakich warunkach dane powierzone/przetwarzane muszą być przechowywane?

Zgodnie z art. 36 ust 1 UODO administrator danych jest zobowiązany do **zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do rodzaju zagrożeń oraz kategorii danych objętych ochroną**.

W szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Te wymogi są interpretowane jako obowiązek zastosowania **odpowiednich**, a więc skutecznych, **środków technicznych i organizacyjnych, które umożliwią administratorowi ochronę danych przed ww. zagrożeniami.** Mogą to być środki różnego rodzaju, od rozwiązań architektonicznych, poprzez systemy alarmowe i służby ochroniarskie, aż po środki techniczne i informatyczne (chip-karty, kody dostępu, systemy kodujące i przeciwdziałające włamaniom).

Przy stosowaniu zabezpieczeń powinno się także uwzględniać zmieniające warunki oraz postęp techniczny, co może prowadzić do konieczności zmiany czy modernizowania wprowadzonych wcześniej systemów ochrony.[12]

Zgodnie z art. 37 UODO **do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych**. Konsekwencją tego wymogu jest kolejny obowiązek: zgodnie z art. 38 UODO, administrator danych musi zapewnić **kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane**.

W przypadku systemów informatycznych dostęp do danych musi być zabezpieczony poprzez konieczność logowania się indywidualnym identyfikatorem, a informacje o tym kto i kiedy uzyskał dostęp do systemu muszą być zapisywane i analizowane. W przypadku przetwarzania danych w formie papierowej ewidencji czy kartoteki standardowym zabezpieczeniem jest przechowywanie dokumentów w zamykanym pomieszczeniu lub szafie, do której dostęp mają tylko upoważnione osoby.

Przykład

Szafa pancerna lub skrzynka zamykana na klucz (np. na zeszyty meldunkowe) z zasady spełniają wymóg skutecznej ochrony danych przed dostępem osób nieuprawnionych, zakładając że klucz do szafy / skrzynki mają tylko osoby upoważnione do przetwarzania danych i właściwie go chronią (np. trzymając w zamkniętej szufladzie, a nie luzem na biurku).

[12] Komentarz … Art. 36, par. 1

Bardzo pomocne w ustaleniu jakie środki i zabezpieczenia należy podjąć w celu ochrony danych jest **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji** z dnia 29 kwietnia 2004 r., które określa:

- środki techniczne i organizacyjne, jakie zapewniają ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych;
- podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych; oraz
- wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

Ze względu na wagę, kazuistyczny charakter i szczegółowość tej regulacji załączamy ją w całości, jako aneks do niniejszej opinii. Próby opisania w formie opinii wszystkich wymogów zawartych w tym Rozporządzeniu tylko zaciemniły by ich treść i nadmiernie rozciągnęły objętość[13].

(2) Czy dane mogą być przechowywane na laptopie badacza?

Dane osobowe **mogą być przenoszone poza miejsce wykonywania zlecania** (świadczenia pracy) przez upoważnioną do ich przetwarzania osobę (np. badacza) **na różnych nośnikach pamięci**, takich jak laptopy, dyski przenośne, urządzenia typu USB itp., **pod warunkiem, że te urządzenia są odpowiednio zabezpieczone**. Według ww. Rozporządzenia urządzenia i nośniki zawierające dane osobowe trzeba zabezpieczyć w **sposób zapewniający poufność i integralność danych**.

Rozporządzenie nie precyzuje, jaka technologia powinna zostać to zastosowana. Wydaje się jednak, że powinno to być przede wszystkim **hasło** uniemożliwiające dostęp do samego urządzenia osobie nieuprawnionej (standardowa opcja w przypadku wszystkich laptopów, możliwa do zainstalowania także w przypadku nośników pamięci). Zalecanym dodatkowym środkiem bezpieczeństwa jest **zabezpieczenie pliku**, który zawiera dane poprzez jego **zaszyfrowanie**.. Proste szyfrowanie treści można wprowadzić przy użyciu ogólnodostępnego oprogramowania.

To drugie zabezpieczenie chroni przede wszystkim integralność danych. Ochrona integralności pliku oznacza, że plik powinien być zabezpieczony przed otwarciem i zmodyfikowaniem przez osobę nieuprawnioną, przy czym wymóg ten nie jest zależny od wielkości pliku (zbioru danych). Jest to jednak zabezpieczenie dodatkowe i można argumentować, że w przypadku niewielkich baz, których zagubienie nie wiąże się z dużym ryzykiem dla osób, których dane dotyczą, samo hasło jako środek zabezpieczenia danych powinno wystarczyć.

D. PUBLIKOWANIE DANYCH

(1) W jakiej formie dane można publikować?

Rozumiemy to pytanie jako odnoszące się do tego, czy można publikować dane osobowe, czy tylko dane zanonimizowane.

[13] Polecam także publikację GIODO: *ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych* [http://www.giodo.gov.pl/plik/id_p/1057/j/pl/]

Odpowiedź zależy od okoliczności: podobnie jak w przypadku dostępu do danych (osobowych bądź zanonimizowanych) przez badacza, **możliwość publikacji danych zależy od tego, czy istnieje odpowiednia podstawa prawna**. O ile dla zwykłego przetwarzania danych (np. zbierania danych, uzyskania dostępu do istniejącego zbioru, łączenia czy analizowania danych) nie zawsze jest wymagana zgoda osoby, której dane dotyczą (ustawa przewiduje kilka przesłanek przetwarzania bez zgody, także dla podmiotów prywatnych – por. punkt II.A (1)), o tyle wydaje się, że dla opublikowania danych osobowych przez podmiot prywatny czy osobę fizyczną taka zgoda jest niezbędna. Żadna przesłanka ustawowa – inna niż wyraźna zgoda osoby, której dane dotyczą – nie uzasadnia tak dalece idącej ingerencji w prywatność. Wynika to, w naszej opinii, z ogólnych zasad przetwarzania danych: celowości i adekwatności (opisane w punkcie II. A (1)).

Potwierdzając tę linię rozumowania, art. 27 ust. 2 pkt. (9) UODO, wyraźnie wyklucza możliwość publikowania danych, mimo że zezwala na ich przetwarzanie bez zgody osób, których dane dotyczą do celów przeprowadzenia badań naukowych (por. punkt II.A (1)).

Zgodnie z tym przepisem, **publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone**. Ponieważ jest to w naszej opinii jedyna przesłanka w oparciu o którą organizacja mogłaby uzyskać dane osobowe bez zgody osób, których one dotyczą, ten przepis kategorycznie zamyka także możliwość publikowania danych osobowych bez uzyskania odpowiedniej zgody.

A zatem **jedyną podstawą dla publikacji danych osobowych, czyli nie zanonimizowanych, jest zgoda osób, których dane dotyczą**. Co więcej, w przypadku danych wrażliwych, ustawa wymaga uzyskania wyraźnej **zgody na piśmie** (art. 27 ust. 1 UODO).

Odrębną kwestią jest możliwość uzyskania skutecznej – tj. dobrowolnej i świadomej – zgody na publikację danych osobowych, szczególnie wrażliwych oraz przestrzegania zasady adekwatności. Zgodnie z zasadami przedstawionymi powyżej (punkt II. A (1)), oświadczenie woli, jakim jest zgoda na przetwarzanie danych, musi być udzielone w sposób zupełnie **dobrowolny**, a zatem bez presji czy warunków stawianych osobie, której dane dotyczą. Zgoda na publikację wymuszona okolicznościami lub zmanipulowana będzie nieskuteczna. Podobnie jak zgoda nieskonkretyzowana: osoba udzielająca zgody musi być w pełni **poinformowana** (powinno to zostać zapisane w treści tzw. klauzuli zgody) o tym w jakim celu i w jaki sposób jej dane mają zostać przetworzone, w tym wypadku w związku z publikacją. Wreszcie, zakres przetwarzania danych i w tym wypadku musi być **adekwatny do celu przetwarzania**. A zatem nie można opierając się na przesłance zgody wykorzystać danych w szerszym zakresie – np. na potrzeby kolejnych publikacji czy równoległej publikacji o innym charakterze.

Odrębną kwestią, której tu nie będziemy analizować, jest potencjalna odpowiedzialność publikującego za zniesławienie lub naruszenie dóbr osobistych, o której także należy pamiętać.

(2) <u>Jakich danych bezwzględnie nie można publikować?</u>

Z zastrzeżeniem powyższych warunków, nie ma zakazu publikowania jakichkolwiek danych. Jeśli publikujący jest w stanie uzyskać świadomą i dobrowolną zgodę na to od osoby, której dane dotyczą, może opublikować nawet dane wrażliwe.

(3) Czy historię osoby bez podawania jej imienia i nazwiska można opublikować?

Tak, ale tylko **pod warunkiem, że tożsamość osoby, o której mowa w publikowanej historii nie jest możliwa do ustalenia** poprzez łączenie innych informacji dostępnych w tekście oraz kontekstu.

Do tej sytuacji stosuje się analogiczna logika, jak w przypadku ustalenia, jakie informacje już stanowią dane osobowe (por. punkt I. A). Jak wyjaśnialiśmy powyżej, daną osobową może być w zasadzie każda informacja – na temat okoliczności życiowych, cech charakteru, miejsca pobytu itp. – jeżeli w danym kontekście umożliwia identyfikację osoby. A zatem przed publikacją tekstu trzeba się upewnić, że wśród odbiorców tekstu nie ma osób, które korzystając ze swojej wiedzy ogólnej w połączeniu z informacjami zawartymi w tekście byłyby w stanie ustalić o kim mowa.

Jak widać na powyższym przykładzie, to czy dana informacja jest „daną osobową" w ogromnej mierze zależy od kontekstu oraz od okoliczności, w jakich się ją ujawnia. Dlatego też przy projektowaniu historii „anonimowej osoby" trzeba przewidzieć wiele możliwych okoliczności i dobrze zbadać kontekst.

E. REJESTROWANIE ZBIORÓW DANYCH

Zasadą wyrażoną w ustawie (art. 40 UODO) jest, że **administrator danych ma obowiązek zgłosić zbiór danych do rejestracji GIODO**. Procedura rejestracji zbioru danych jest określona w ustawie (art. 41 UODO), natomiast formularz rejestracyjny można znaleźć w Rozporządzeniu MSWiA z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Nieco przystępniej procedura i wymagania dotyczące zgłoszenia rejestracyjnego zostały opisane na stronie GIODO. GIODO uruchomił bardzo wygodny elektroniczny system rejestrowania baz danych, w którym użytkownik jest instruowany i prowadzony krok po kroku. Instrukcje oraz interaktywny formularz rejestracyjny są dostępne na stronie http://www.giodo.gov.pl/148/.

Czas trwania procedury rejestrowania zbioru zależy od okoliczności, szczególnie od ilości wniosków, jakie w danym momencie otrzymał GIODO, jednak z zasady **nie powinien przekroczyć 30 dni**. Co istotne, tylko w przypadku rejestrowania zbioru zawierającego dane wrażliwe ten czas oczekiwania jest istotny, ponieważ dane można przetwarzać dopiero po skutecznym zarejestrowaniu zbioru w biurze GIODO. W przypadku przetwarzania danych zwykłych, czas trwania procedury jest bez znaczenia, ponieważ administrator danych (organizacja czy placówka) może legalnie przetwarzać dane już od momentu złożenia wniosku o zarejestrowanie zbioru danych.

Od zasady, jaką jest obowiązek rejestracji, jest kilka wyjątków, które zostały enumeratywnie wskazane w art. 43 ust. 1. UODO. Z tego katalogu wymienimy tylko te, które mogą mieć zastosowanie do działalności organizacji pozarządowych lub ich pracowników i klientów.

A zatem, **z obowiązku rejestracji zbioru danych zwolnieni są** administratorzy danych:

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

(ii) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej – ale już nie w przypadku, gdy dane te mają być

wykorzystywana także w innych celach;

(iii) powszechnie dostępnych – za takie dane GIODO uznaje dane udostępnione „nieograniczonemu kręgowi podmiotów, np. w sieci Internet”[14];

(iv) przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; oraz

(v) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego – nie istnieje ustawowa definicja „drobnych bieżących spraw”, a zatem jest to kwestia otwarta do każdorazowej interpretacji GIODO lub sądu rozstrzygającego ew. spór. Na podstawie dotychczasowego doświadczenia można jednak przyjąć, że w tej kategorii mieszczą się np. zbiory wizytówek, osobiste listy adresowe (np. w telefonie) czy zbiory danych gromadzone w osobistych notatnikach.

Ponadto, z art. 2 UODO wynika kolejne istotne wyłączenie z obowiązku rejestrowania zbioru danych. Otóż, w odniesieniu do **zbiorów danych osobowych sporządzanych doraźnie**, **wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką** w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, mają zastosowanie jedynie przepisy rozdziału 5 (tj. o zabezpieczeniu danych), a więc nie ma tu zastosowania obowiązek zgłoszenia zbioru do rejestracji GIODO. W tej kategorii znajdą się wszelkiego typu zbiory tymczasowe (np. lista osób sporządzona tylko na potrzeby wysyłki korespondencji), listy uczestników lub zbiory danych tworzone w celach szkoleniowych, a następnie niszczone.

Według naszej wiedzy oraz przepisów ustawy nie istnieje procedura pozwalająca na uzyskanie zwolnienia z obowiązku rejestracji dla konkretnego zbioru, który nie spełnia żadnego wymogu przewidzianego w ustawie, na podstawie indywidualnej oceny czy konsultacji z GIODO. Natomiast nic nie stoi na przeszkodzie, żeby wystąpić do GIODO z prośbą o interpretację, czy dany zbiór podpada pod którąś z kategorii zbiorów zwolnionych z tego obowiązku.

Przykład:

Zbiór kart mieszkańca prowadzony na potrzeby pracy socjalnej/udzielania pomocy mieszkańcowi placówki dla bezdomnych nie mieści się żadnym z powyższych wyłączeń i dlatego powinien być zarejestrowany w GIODO jako zbiór danych osobowych.

14 *Pytania i odpowiedzi*, www.giodo.gov.pl

ANEKS

ROZPORZĄDZENIE

MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

z dnia 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 dnia 1 maja 2004 r.)

Na podstawie art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1)sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;

2)podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;

3)wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

§ 2. Ilekroć w rozporządzeniu jest mowa o:

1)ustawie - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej "ustawą";

2)identyfikatorze użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

3)haśle - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

4)sieci telekomunikacyjnej - rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.[2)])

5)sieci publicznej - rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne;

6)teletransmisji - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

7)rozliczalności - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

8)integralności danych - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

9)raporcie - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

10)poufności danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

11)uwierzytelnianiu - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 3. 1. Na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej "instrukcją".

2. Dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej.

3. Dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

§ 4. Polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności:

1)wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

2)wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

3)opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;

4)sposób przepływu danych pomiędzy poszczególnymi systemami;

5)określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 5. Instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności:

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.

§ 6. 1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym:

1) podstawowy;

2) podwyższony;

3) wysoki.

2. Poziom co najmniej podstawowy stosuje się, gdy:

1)w systemie informatycznym nie są przetwarzane dane, o których mowa w art. 27 ustawy, oraz

2)żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

3. Poziom co najmniej podwyższony stosuje się, gdy:

1)w systemie informatycznym przetwarzane są dane osobowe, o których mowa w art. 27 ustawy, oraz

2)żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

4. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

5. Opis środków bezpieczeństwa stosowany na poziomach, o których mowa w ust. 1, określa załącznik do rozporządzenia.

§ 7. 1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym - z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - system ten zapewnia odnotowanie:

1)daty pierwszego wprowadzenia danych do systemu;

2)identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;

3)źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;

4)informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;

5)sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§ 8. System informatyczny służący do przetwarzania danych, który został dopuszczony przez właściwą służbę ochrony państwa do przetwarzania informacji niejawnych, po uzyskaniu certyfikatu wydanego na podstawie przepisów ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.[3)]) spełnia wymogi niniejszego rozporządzenia pod względem bezpieczeństwa na poziomie wysokim.

§ 9. Administrator przetwarzanych w dniu wejścia w życie niniejszego rozporządzenia danych osobowych jest obowiązany dostosować systemy informatyczne służące do przetwarzania tych danych do wymogów określonych w § 7 oraz w załączniku do rozporządzenia w terminie 6 miesięcy od dnia wejścia w życie niniejszego rozporządzenia.

§ 10. Rozporządzenie wchodzi w życie z dniem uzyskania przez Rzeczpospolitą Polską członkostwa w Unii Europejskiej[4)].

---

1) Minister Spraw Wewnętrznych i Administracji kieruje działem administracji rządowej - administracja publiczna, na podstawie § 1 ust. 2 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 14 marca 2002 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji (Dz. U. Nr 35, poz. 325 i Nr 58, poz. 533).

[2)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 122, poz. 1321 i Nr 154, poz. 1800 i 1802, z 2002 r. Nr 25, poz. 253, Nr 74, poz. 676 i Nr 166, poz. 1360 oraz z 2003 r. Nr 50, poz. 424, Nr 113, poz. 1070, Nr 130, poz. 1188 i Nr 170, poz. 1652.

[3)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2000 r. Nr 12, poz. 136 i Nr 39, poz. 462, z 2001 r. Nr 22, poz. 247, Nr 27, poz. 298, Nr 56, poz. 580, Nr 110, poz. 1189, Nr 123, poz. 1353, Nr 154 poz. 1800, z 2002 r. Nr 74, poz. 676, Nr 89, poz. 804 i Nr 153, poz. 1271, z 2003 r. Nr 17, poz. 155 oraz z 2004 r. Nr 29, poz. 257.

[4)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 80, poz. 521 oraz z 2001 r. Nr 121, poz. 1306), które utraci moc z dniem wejścia w życie ustawy z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz. U. Nr 33, poz. 285).

ZAŁĄCZNIK

A. Środki bezpieczeństwa na poziomie podstawowym

I

1. Obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.

2. Przebywanie osób nieuprawnionych w obszarze, o którym mowa w § 4 pkt 1 rozporządzenia, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.

2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;

b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1)działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;

2)utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.

3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

4. Kopie zapasowe:

a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;

b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1)likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

2)przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

3)naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

VII

Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.

B. Środki bezpieczeństwa na poziomie podwyższonym

VIII

W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

IX

Urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

X

Instrukcja zarządzania systemem informatycznym, o której mowa w § 5 rozporządzenia, rozszerza się o sposób stosowania środków, o których mowa w pkt IX załącznika.

XI

Administrator danych stosuje na poziomie podwyższonym środki bezpieczeństwa określone w części A załącznika, o ile zasady zawarte w części B nie stanowią inaczej.

C. Środki bezpieczeństwa na poziomie wysokim

XII

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:

a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;

b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

XIII

Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

XIV

Administrator danych stosuje na poziomie wysokim środki bezpieczeństwa, określone w części A i B załącznika, o ile zasady zawarte w części C nie stanowią inaczej.