OCHRONA DANYCH OSOBOWYCH

Drukuj

Kategoria: Prawo w służbie |

Dynamika rozwoju nowoczesnych technologii doprowadziła do przemian natury cywilizacyjnej. I nie sposób sprowadzić tego tylko do ułatwień w procesie komunikowania się, pozyskiwania i przetwarzania danych. Można już bowiem mówić o kształtowaniu się tzw. społeczeństwa informacyjnego.

Informacja (z łac. *informatio* – powiadomienie o czym, zakomunikowanie czegoś; wiadomość, pouczenie) [1] leży u źródeł **teorii informacji**, obejmującej kodowanie, przekształcanie, przekazywanie i przechowywanie informacji oraz ograniczanie czynników zakłócających je. W języku potocznym często zamiennie używa się pojęć: informacje, dane, dane osobowe, dane wrażliwe itp. Modyfikują one znaczenia zależnie od językowego lub sytuacyjnego kontekstu.

Pojęcie **dane** (z ang. *data*) ma niewiele wspólnego z pierwotnym łacińskim *datum* (czyli terminem, tj. kalendarzowym oznaczeniem dnia, miesiąca, roku) [2]. W naukach humanistycznych słowo dane oznacza np. cechy, właściwości. W naukach ścisłych, np. w informatyce, to zbiory liczb i tekstów w różnych formach (a więc znaki, mowa, wykresy i sygnały).

Metateoria TOGA wg Gadomskiego [3] definiuje dane jako wszystko, co jest/może być przetwarzane umysłowo lub komputerowo, a informację jako dane odnoszące się do określonej dziedziny działań człowieka lub sztucznej inteligencji. Zgodnie z tym informacja stanowi dane, ale nie każde dane są informacją. Same liczby są zawsze danymi, ale informacją stają się dopiero w połączeniu z określoną dziedziną. Przykładem danych są liczby 134 i 9612XXX6822. Określenie miejsca wypadku komunikacyjnego na 134 km autostrady A-4 to informacja. PESEL nr 9612XXX6822 to dana osobowa, czyli szczególny rodzaj informacji.

Implikacje i uwarunkowania rewolucji technologicznej wymagają podejmowania działań porządkujących w sferze przetwarzania i zabezpieczenia informacji, co wiąże się z wprowadzeniem stosownych regulacji. Zgodnie z zapisem art. 47 Konstytucji Rzeczypospolitej Polskiej każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Art. 51 ust. 1 i 2 ustawy zasadniczej wskazuje, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż te, które są niezbędne w demokratycznym państwie prawa, na co słusznie wskazują autorzy publikacji pt. „Ochrona informacji w stanach zagrożeń" [4].

Kolejnym istotnym, a zarazem nowym elementem systemu ochrony procesów przetwarzania danych są przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) [5]. Zastąpi ono przepisy dotychczasowej ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. DzU z 2016 r. poz. 922, dalej UODO) [6] wraz z aktami wykonawczymi do niej. Przepisy te zaczną być stosowane od 25 maja 2018 r., a okres przejściowy warto wykorzystać do uruchomienia odpowiednich procesów dostosowania do nowych wymogów.

Dane osobowe

Przepisy wyróżniają dwa rodzaje danych osobowych: zwykłe oraz szczególnie chronione (zwane również sensytywnymi lub wrażliwymi). Zgodnie z UODO za zwykłe dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Możliwa do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności powołując się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Ustawodawca nie zamknął katalogu informacji, które należy uważać za dane osobowe podlegające ochronie, tj. informacje takie jak numer telefonu, adres IP komputera, adres e-mail, pliki cookies, numer IMEI telefonu komórkowego, nick, login również mogą stanowić daną osobową. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Mianem danych wrażliwych (sensytywnych) potocznie określa się dane szczególnie chronione. Wymienia je art. 27 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, zgodnie z którym są to: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, dane o nałogach lub życiu seksualnym, skazaniach, orzeczeniach o ukaraniu i mandatach karnych, stanie zdrowia, kodzie genetycznym. Katalog ten uzupełnia także art. 29 Opinii Grupy Roboczej Rady Europy, który do danych szczególnie chronionych zalicza także odwzorowania danych biometrycznych i DNA, które mogą być wykorzystywane w celu ustalenia tożsamości osób.

Należy jednak zwrócić uwagę, że art. 4 RODO przedstawia nowe definicje. W rozumieniu tego przepisu danymi osobowymi są informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (której te dane dotyczą). Przy tym możliwą do zidentyfikowania osobą jest taka, którą można zidentyfikować bezpośrednio lub pośrednio, w szczególności na podstawie imienia i nazwiska, numeru identyfikacyjnego, danych o lokalizacji, identyfikatora internetowego lub jednego bądź kilku szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Z kolei dane genetyczne oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.

Dane biometryczne wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną

identyfikację tej osoby. To m.in. wizerunek twarzy lub dane daktyloskopijne. Dane dotyczące zdrowia są we wskazanym przepisie definiowane jako dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej (o stanie zdrowia), w tym informacje o korzystaniu z usług opieki zdrowotnej.

Dane osobowe cechuje różny stopień wrażliwości i krytyczności. Niektóre z nich mogą wymagać dodatkowego poziomu ochrony lub specjalnego traktowania. RODO umożliwia państwom członkowskim doprecyzowanie jego przepisów, w tym tych dotyczących przetwarzania szczególnych kategorii danych osobowych (zwanych danymi wrażliwymi). Rozporządzenie nie wyklucza możliwości określenia w prawie państwa członkowskiego konkretnych sytuacji związanych z przetwarzaniem danych, w tym dookreślenia warunków decydujących o zgodności przetwarzania z prawem.

Zasady przetwarzania danych osobowych

Zgodnie art. 7 Konstytucji Rzeczypospolitej Polskiej organy władzy publicznej działają na podstawie i w granicach prawa, a jego podstawy muszą znajdować się w treści przepisów. Przetwarzając dane osobowe na mocy obowiązującej UODO, jesteśmy zobligowani do stosowania odpowiednich zasad, zawartych w szczególności w art. 23 ust. 1 (dla danych zwykłych) i w art. 27 ust. 2 (dla danych wrażliwych). Mowa o zasadach: zgodności z prawem, ograniczenia celem, adekwatności i poprawności oraz niezbędności. Z kolei zgodnie z art. 5 RODO należy również uwzględnić zasadę integralności i poufności, a także rozliczalności.

Podstawy prawne przetwarzania danych osobowych

Zgoda

Jedną z przesłanek legalności przetwarzania danych jest zgoda osoby, której dane dotyczą, czyli jej oświadczenie woli w którym udziela pozwolenia na ich przetwarzanie. Co ważne, może być ono odwołane w każdym momencie. Należy pamiętać, że zgoda na przetwarzanie danych osobowych nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgody na przetwarzanie danych osobowych nie mogą też być łączone.

Realizacja obowiązku prawnego

Kolejną przesłanką legalizującą procesy przetwarzania danych osobowych może być realizacja obowiązku prawnego, np. wynikająca z ustawy z 24 sierpnia 1991 r. o ochronie przeciwpożarowej, w tym: obowiązki komendanta głównego Państwowej Straży Pożarnej, konieczność przyjmowania zgłoszeń alarmowych i obsługi numeru alarmowego 112 oraz związane z tym wszelkie procedury przetwarzania danych osobowych zgłoszenia alarmowego (art. 14h).

Państwowa Straż Pożarna może przetwarzać dane uzyskane w związku z obsługą zgłoszenia alarmowego, o której mowa w art. 2 pkt 2 ustawy z 22 listopada 2013 r. o systemie powiadamiania ratunkowego, w tym dane osoby zgłaszającej i innych osób, których zgłoszenie dotyczy.

Realizacja umowy

Przetwarzanie danych osobowych jest dopuszczalne również, gdy dochodzi do realizacji umowy. Podstawą takiego twierdzenia jest art. 23 ust. 1 pkt 3 ustawy. Przepis ten stanowi, że przetwarzanie danych osobowych jest dopuszczalne, gdy jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą. Zbędne jest w tym przypadku żądanie dodatkowego oświadczenia woli.

Zadania realizowane dla dobra publicznego

Przesłankę tę przeanalizuję na przykładzie. Wójt wysłał do sołtysów pismo nakazujące wstrzymanie toczącego się remontu dróg gruntowych z powodu skargi jednego z mieszkańców na degradację środowiska naturalnego. Podał przy tym dokładne dane skarżącego (imię i nazwisko oraz adres). Pismo to zawierało również polecenie poinformowania o tym fakcie mieszkańców. Jako podstawę prawną udostępnienia danych osobowych wójt wskazał art. 23 ust. pkt 4 UODO.
Zgodnie z nim przetwarzanie (w tym udostępnianie) danych osobowych jest dopuszczalne, gdy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego. W ocenie wójta opisane udostępnienie danych skarżącego było działaniem w interesie publicznym, gdyż zaspokajanie zbiorowych potrzeb wspólnoty należy do zadań własnych gminy, które w szczególności obejmują sprawy utrzymania i remontów gminnych dróg [7].
Jednak w ocenie generalnego inspektora ochrony danych osobowych powołana przez wójta podstawa prawna jest błędna. Przesłanka z art. 23 ust. 1 pkt 4 UODO dotyczy sytuacji, gdy brak jest odpowiednich przepisów prawa wprost upoważniających do przetwarzania danych, ale ze względu na konieczność wykonywania określonych przez prawo zadań realizowanych dla dobra publicznego dane te muszą być przetwarzane bez zgody osób, których dotyczą. Przetwarzanie danych osobowych musi więc być niezbędne w procesie realizacji określonych prawem zadań (bez tego nałożone w przepisach zadania konkretnego podmiotu nie będą mogły być zrealizowane) i służyć dobru publicznemu. W związku z tym art. 23 ust. 1 pkt 4 UODO nie uzasadnia udostępnienia przez wójta danych osobowych skarżącego, gdyż nie było ono niezbędne dla realizacji zadań gminy określonych w art. 7 ust. 1 pkt 2 ustawy o samorządzie gminnym, wskazującym zadania własne gminy, w tym zaspokojenie zbiorowych potrzeb wspólnoty, m.in. w sprawach dróg.
Działania wójta stanowiły także naruszenie art. 26 UODO, w myśl którego administrator danych (w tym przypadku wójt) ma obowiązek dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem oraz były adekwatne do celów, w jakich są przetwarzane.
Jak łatwo zauważyć, aby poinformować mieszkańców gminy o wstrzymaniu remontów dróg gminnych w związku ze skargą na degradację środowiska naturalnego możliwe było upublicznienie tej informacji, ale bez identyfikacji osoby, która złożyła przedmiotową skargę.
Prawnie usprawiedliwiony cel administratora
W art. 23 ust. 4 pkt 1 i 2 UODO znaleźć można wyjaśnienie, że za prawnie usprawiedliwiony cel uważa się w szczególności marketing bezpośredni własnych produktów lub usług administratora danych i dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej. Zgodnie z twierdzeniem doktryny cel taki musi mieć uzasadnienie gospodarcze oraz prawne i powinien mieścić się w granicach działalności prowadzonej przez administratora.
Ochrona żywotnych interesów podmiotu danych
Żywotne interesy osoby, której dane dotyczą, należy rozumieć jako interesy niezbędne dla życia tej osoby. Poza zakresem tego pojęcia znajdują się więc interesy ekonomiczne.
Przesłanka ta staje się szczególnie istotna, gdy podmiot danych nie może wyrazić zgody ze względu na swój stan psychofizyczny, a zachodzi konieczność przetwarzania danych na potrzeby np. ratowania życia jej lub innych. Można skorzystać z omawianej przesłanki jedynie w przypadku, gdy ewidentnie nie da się wykorzystać innej podstawy prawnej do uzasadnienia przetwarzania danych osobowych.

Niektóre rodzaje przetwarzania mogą służyć zarówno ważnemu interesowi publicznemu, jak i żywotnym interesom osoby, której dane dotyczą, na przykład gdy przetwarzanie jest niezbędne do szeroko pojętych celów humanitarnych, m.in.: monitorowania epidemii i ich rozprzestrzeniania się lub w przypadku klęsk żywiołowych i katastrof spowodowanych przez człowieka.

Obowiązek informacyjny

Przepisy prawa nakładają na administratorów danych zobowiązanie, aby przy zbieraniu danych osobowych tzw. obowiązek informacyjny, o którym mowa w art. 24 UODO, był spełniony [8], gdy dane zbierane są bezpośrednio od osoby, której one dotyczą i w przypadkach gromadzenia danych ze źródeł pośrednich, czyli np. od innych osób. Chodzi o to, by zainteresowany miał możliwość właściwej oceny sytuacji na podstawie uzyskanych informacji i podjęcia decyzji co do udostępnienia danych, a także mógł korzystać ze swoich praw podstawowych.

Artykuł 24 ust. 1 UODO stanowi, że w przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować ją o:

- adresie swojej siedziby i jej pełnej nazwie, a gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku,
- celu zbierania danych, w szczególności o odbiorcach lub kategoriach odbiorców danych znanych mu w czasie udzielania informacji lub przewidywanych,
- prawie dostępu do treści swoich danych oraz ich poprawiania,
- dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje – o jego podstawie prawnej.

Informacje te należy w indywidualny sposób przekazać osobie, której dane dotyczą. Nie można tego zastąpić np. ogłoszeniem czy też adnotacją umieszczoną w regulaminie, jeśli dana osoba nie ma możliwości bezpośredniego zapoznania się z jego treścią. Obowiązek ten powinien być wykonany w zasadzie przed rozpoczęciem zbierania danych. Ustawa nie zawiera jednak żadnych wskazówek w tym zakresie, podobnie jak nie przesądza, w jakiej formie obowiązek informacyjny powinien być spełniony. Skoro zaś ustawodawca nie narzuca żadnej formy, należy uznać, że jest ona w zasadzie dowolna (informacje mogą być udzielone np. ustnie).

W art. 25 UODO uregulowany został natomiast obowiązek informacyjny spoczywający na administratorze danych w sytuacji, gdy gromadzi on informacje o określonych osobach i nie pochodzą one od tych osób, a z innych źródeł. W takim przypadku administrator danych jest obowiązany bezpośrednio po utrwaleniu zebranych danych poinformować tę osobę o:

- adresie swojej siedziby i pełnej nazwie, a gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku,
- celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
- źródle danych,
- prawie dostępu do treści swoich danych oraz ich poprawiania,
- uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 (chodzi o prawo do złożenia sprzeciwu wobec przetwarzania danych w celach marketingowych lub przekazywania ich innym podmiotom oraz

żądania zaprzestania przetwarzania danych ze względu na szczególną sytuację osoby, której one dotyczą).

Tomasz Soczyński jest zastępcą dyrektora Departamentu Informatyki Biura GIODO

Przypisy

[1] Słownik wyrazów obcych. Red. prof. Jan Tokarski. Warszawa 1977, s. 305.
[2] Tamże, s. 203.
[3] A.M. Gadomski, Information, Preferences and Knowledge, http://erg4146.casaccia.enea.it/wwwerg26701/gad-dict.htm.
[4] St. bryg. dr inż. Bogdan Kosowski, st. kpt. mgr inż. Robert Piec, Ochrona informacji w stanach zagrożeń, Szkoła Główna Służby Pożarniczej, Warszawa.
[5] Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
[6] Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. DzU z 2016 r., poz. 922).
[7] www.giodo.gov.pl/394/id_art/1999/j/pl
[8] ABC wybranych zagadnień z ustawy o ochronie danych osobowych, https://edugiodo.giodo.gov.pl/file.php/1/UST/UST_04.htm.

lipiec 2017