



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

DOLiS-035-756/15/BG

Warszawa, dnia 13 kwietnia 2015 r.

Pan

Prezydent Miasta

WYSTĄPIENIE

Na podstawie art. 19a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182, z późn. zm.), zwanej dalej ustawą, zgodnie z którym Generalny Inspektor Ochrony Danych Osobowych może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych, w związku z pozyskaniem przez Generalnego Inspektora informacji o tym, że nedoręczona w danym dniu korespondencja adresowana do petentów Urzędu Miejskiego jest przechowywana w domach prywatnych pracowników urzędu zajmujących się doręczaniem przesyłek – organ do spraw ochrony danych osobowych zwraca się o zmianę opisanej praktyki.

Generalny Inspektor pozyskał informację, że korespondencja kierowana do interesantów jest poza godzinami pracy Urzędu Miejskiego przechowywana w prywatnych domach pracowników urzędu zajmujących się doręczaniem przesyłek. Rozwiązanie to ma wynikać z faktu, iż korespondencja jest doręczana do godziny 21:30 (podczas gdy urząd pracuje do godziny 15:30), zatem nedoręczone listy nie mogą być danego dnia przekazane z powrotem do urzędu. Opisana praktyka wzbudza poważne wątpliwości pod względem jej zgodności z przepisami ustawy o ochronie danych osobowych.

Nadrzędnym obowiązkiem administratora danych osobowych (którym, zgodnie z definicją zamieszczoną w art. 7 pkt 4 ustawy o ochronie danych osobowych jest organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 [ustawy o ochronie danych osobowych – przyp. autora],

decydujące o celach i środkach przetwarzania danych osobowych), zgodnie z art. 26 ust. 1 pkt 1 ustawy o ochronie danych osobowych jest dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą. Ta generalna zasada znajduje swoje rozwinięcie w przepisach ustawy o ochronie danych osobowych określających m.in. wymogi, jakie powinien spełniać administrator danych w celu zapewnienia bezpieczeństwa danych w procesie ich przetwarzania. Jednym z podstawowych obowiązków spoczywających na administratorze jest, wynikający z art. 36 ust. 1 ustawy o ochronie danych osobowych, **obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną**, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Z art. 36 ust. 2 wynika natomiast obowiązek prowadzenia przez administratora **dokumentacji** opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. Dokumentacja taka powinna określać m.in. wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe. Podkreślenia wymaga również, iż zgodnie z art. 37 ustawy o ochronie danych osobowych, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające **upoważnienie** nadane przez administratora danych. Administrator danych – zgodnie z art. 38 ustawy – jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. Osoby, które zostały upoważnione do przetwarzania danych, są zaś obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia (art. 39 ust. 2 ustawy).

Wskazać należy, iż wszelkie czynności związane z przetwarzaniem danych osobowych winny być wykonywane z uwzględnieniem wszelkich środków technicznych i organizacyjnych zapewniających ich zabezpieczenie przed udostępnieniem osobom nieupoważnionym. Z powyższego wynika zatem, że ich odpowiedniego zastosowania wymaga nie tylko proces przetwarzania danych osobowych w systemach informatycznych, czy w zbiorach tradycyjnych, ale także każda inna wykonywana na nich operacja, zatem i proces przechowywania dokumentów zawierających dane osobowe. Istotnym jest bowiem, wdrożenie takiego rodzaju systemu zabezpieczania danych i kontroli tego procesu, który do minimum ograniczy możliwość wystąpienia nieprawidłowości w zakresie przetwarzania danych osobowych oraz przeszkolenie i wyczulenie na tę kwestię wykonujących te czynności pracowników.

Jednocześnie podkreślić należy, iż administrator musi mieć pełną kontrolę nad procesem przetwarzania danych, tak aby zapobiec powstawaniu zdarzeń narażających dane na udostępnienie osobom nieupoważnionym. Musi też mieć pełną wiedzę na temat całości procesu przetwarzania oraz weryfikować zachowanie pracowników pod kątem przestrzegania przez nich zasad ochrony danych osobowych, odpowiada bowiem także za ich działanie, co potwierdza nie tylko doktryna, ale i utrwalone orzecznictwo

administracyjne (por. wyrok Naczelnego Sądu Administracyjnego z dnia 4 kwietnia 2003 r., sygn. II SA 2935/02).

W tym miejscu wskazać również trzeba, że administrujący danymi, który nie wypełni obowiązków przewidzianych cytowanymi powyżej przepisami, może ponosić odpowiedzialność karną na gruncie przepisów art. 51 ust. 1 oraz art. 52 ustawy o ochronie danych osobowych. Jak bowiem stanowią wspomniane przepisy, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Odpowiedzialność ta rozszerzona została w art. 52 ustawy, zgodnie z którym penalizowane jest także nieumyślne naruszenie obowiązku zabezpieczenia danych przed ich zabraniem przez osobę nieupoważnioną, uszkodzeniem lub zniszczeniem. Jak twierdzi A. Drozd, „przestępstwo stypizowane w art. 52 może popełnić każda osoba, na której ciąży obowiązek zabezpieczenia danych osobowych przed ich zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem. Będzie to w szczególności osoba fizyczna występująca w roli administratora danych albo przetwarzającego” (A. Drozd, Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy. Warszawa 2007, Wydawnictwo Prawnicze LexisNexis, Wydanie III, s. 504).

Stosowana przez Urząd Miejski praktyka, stanowiąca przyczynek do niniejszego wystąpienia, wiąże się z ryzykiem udostępnienia danych osobom nieupoważnionym, a ponadto stwarza zagrożenie dla **tajemnicy korespondencji**, podlegającej ochronie na gruncie art. 49 Konstytucji Rzeczypospolitej Polskiej, zgodnie z którym zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony. Warto w tym miejscu zwrócić uwagę na art. 41 ustawy z dnia 23 listopada 2012 r. Prawo pocztowe (Dz. U. z 2012 r. poz. 1529), dotyczący tajemnicy pocztowej, do której zachowania są obowiązani operator pocztowy oraz osoby, które z racji wykonywanej działalności mają dostęp do tajemnicy pocztowej. Zgodnie z art. 41 ust. 3, naruszeniem obowiązku zachowania tajemnicy pocztowej jest w szczególności ujawnianie lub przetwarzanie informacji albo danych objętych tajemnicą pocztową otwieranie zamkniętych przesyłek pocztowych lub zapoznawanie się z ich treścią oraz umożliwianie osobom nieuprawnionym podejmowania działań mających na celu wykonywanie czynności, o których mowa w pkt 1 i 2.

Zgodnie zaś z art. 267 §1 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553, z późn. zm.), kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo (...) podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Mając na uwadze powyższe, zwracam się do Pana Prezydenta o wnikliwe przeanalizowanie zgłoszonych niniejszym pismem uwag oraz ustosunkowanie się do niniejszego pisma, w tym poprzez

podjęcie działań mających na celu zaprzestanie praktyki przechowywania korespondencji kierowanej do petentów Urzędu Miejskiego w prywatnych domach pracowników urzędu zajmujących się doręczaniem przesyłek oraz podjęcie działań mających na celu wyeliminowanie podobnych nieprawidłowości w przyszłości.

Zgodnie z art. 19a ust. 3 ustawy o ochronie danych osobowych, podmiot, do którego zostało skierowane wystąpienie lub wniosek, o których mowa w ust. 1 i 2, jest obowiązany ustosunkować się do tego wystąpienia lub wniosku na piśmie **w terminie 30 dni od daty jego otrzymania**.

Informuję przy tym, że treść niniejszego wystąpienia wraz z udzieloną odpowiedzią opublikowana będzie na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych.