GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH
dr Edyta Bielak-Jomaa

Warszawa, dnia maja 2015 r.

DOLiS-033-204/15/KK

Pani
Urszula Augustyn
Pełnomocnik Rządu ds. bezpieczeństwa w szkołach, Sekretarz Stanu
Ministerstwo Edukacji Narodowej
Aleja Jana Chrystiana Szucha 25
00 – 918 Warszawa

w odpowiedzi na pismo z dnia 8 maja 2015 r., (data wpływu do Biura Generalnego Inspektora Ochrony Danych Osobowych 12 maja br.) – sygnatura: DKOW-WWPB.025.4.2015 – uprzejmie informuję, że do projektu:

1) **uchwały Rady Ministrów w sprawie Rządowego programu wspomagania w latach 2015 – 2018 organów prowadzących szkoły w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w szkołach – „Bezpieczna+"** (wydawanej na podstawie delegacji zawartej w art. 90u ust. 1 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty Dz. U. z 2004 r. Nr 256, poz. 2572, z późn. zm.), oraz

2) **rozporządzenia Rady Ministrów w sprawie szczegółowych warunków, form i trybu realizacji Rządowego programu wspomagania w latach 2015 – 2018 organów prowadzących szkoły w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w szkołach – „Bezpieczna+"** (wydawanego na podstawie delegacji zawartej w art. 90u ust. 4 pkt 5 ustawy z dnia 7 września 1991 r. o systemie oświaty Dz. U. z 2004 r. Nr 256, poz. 2572, z późn. zm.)

Generalny Inspektor – z punktu widzenia przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.) – **zgłasza następujące uwagi** i wskazuje istotne kwestie, które powinny zostać przez projektodawcę rozważone.

ul. Stawki 2
00-193 Warszawa

tel. 860 70 81
fax. 860 70 90

Działania edukacyjne podejmowane przez Generalnego Inspektora Ochrony Danych Osobowych w ramach Ogólnopolskiego Programu Edukacyjnego „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa skierowana do uczniów i nauczycieli" doskonale wpisują się w cele „Rządowego programu wspomagania w latach 2015-2018 organów prowadzących szkoły w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w szkołach Bezpieczna+".

Należy również podkreślić, że wiele badań m.in. badania GIODO przeprowadzone w roku 2012 w ramach projektu „Postrzeganie zagadnień związanych z ochroną danych i prywatnością przez dzieci i młodzież" pokazują, że dzieci ze szkół podstawowych i młodzież gimnazjalna najczęściej korzystają z Internetu w swoim domu (874 dzieci, co oznacza prawie 93% badanych osób), ale ponad 55% osób badanych w szkole. Natomiast co istotne, już w roku 2012 wyniki badań potwierdziły, że co trzecie dziecko korzysta z Internetu w telefonie komórkowym.

W związku z tak szybkim rozwojem nowych technologii i powszechnym dostępem do Internetu w urządzeniach mobilnych, wydaje się, że obecnie edukacji w tym zakresie nie należy rozpatrywać tylko poprzez edukację pozaszkolną, ale poprzez wprowadzenie rozwiązań systemowych w edukacji szkolnej poprzez wprowadzenie do zajęć szkolnych treści kształtujących świadome i bezpieczne nawyki korzystania przez dzieci i młodzież z nowoczesnych technologii.

W związku z powyższym, odnosząc się również do treści celu szczegółowego nr 1 programu Bezpieczna+, **poprawa kompetencji pracowników szkoły, uczniów i ich rodziców w zakresie bezpiecznego korzystania z cyberprzestrzeni oraz reagowania na zagrożenia, zasługuje na pozytywną ocenę organu ochrony danych**. Takie podejście stanowi również priorytet realizacji Programu Edukacyjnego GIODO „Twoje dane – twoja sprawa". Podnoszenie kompetencji i popularyzacja dobrych praktyk w zakresie ochrony danych osobowych i poszanowania prawa do prywatności w cyberprzestrzeni stanowić powinno istotny element podstaw programowych kształcenia we wszystkich typach szkół. Doświadczenia GIODO z wieloletniej realizacji Programu „Twoje dane – twoja sprawa" dowodzą, że odpowiednia wiedza i kształtowanie nawyków w obszarze ochrony prywatności ma istotny wpływ na bezpieczeństwo funkcjonowania dzieci i młodzieży we współczesnym cyfrowym świecie.

Podejmowane działania pokazują dużą potrzebę edukacji w tym zakresie, angażując przy tym całą społeczność szkolną (uczniów, nauczycieli, rodziców) oraz środowisko lokalne (mieszkańców miast i liczne urzędy, które przetwarzają dane osobowe, media). Podejście zakładające zaangażowanie w proces edukacji środowisk lokalnych zostało również zauważone przez autorów programu Bezpieczna+, co należy odnotować z satysfakcją.

Aprobując i wyrażając poparcie dla działań wpierających bezpieczeństwo w szkołach (cel szczegółowy nr 3), wskazać należy potrzebę przeniesienia części regulacji na poziom ustawy z uwagi na szeroki zakres oddziaływania na osoby. Zgodnie z **zasadą legalizmu** wyrażoną w art. 7 Konstytucji organy władzy publicznej działają na podstawie i w granicach prawa.

W zakresie ochrony danych osobowych doprecyzowanie tej zasady zostało sformułowane w art. 51 ust. 1 Konstytucji. Zgodnie z tym przepisem nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Organy państwa mają możliwość zbierania informacji o obywatelach, jednakże jedynie w zakresie w jakim jest to niezbędne w demokratycznym państwie prawnym (art. 51 ust. 2). Monitoring wizyjny, który jest szczególną formą przetwarzania informacji o osobach, powinien zawsze mieć oparcie w przepisach rangi ustawowej. **Dlatego też istnieje konieczność uregulowania zasadniczych kwestii związanych z tym tematem, zwłaszcza, że może dochodzić do gromadzenia danych osobowych w szerokim zakresie i to danych wrażliwych w rozumieniu art. 27 ustawy o ochronie danych osobowych.** Z przetwarzaniem danych wiąże się także tworzenie zbiorów danych, które muszą być odpowiednio chronione w zależności od charakteru zebranych w nich danych osobowych zgodnie z treścią rozporządzenia MSWiA 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 2004 r. Nr 100, poz. 1024). W tej grupie znajdują się także formy przetwarzania, które mając charakter szerokiej ingerencji w prywatność powinny być uregulowane zasadami wynikającymi z ustaw. Dlatego wydaje się, iż aprobując rozwiązanie kierunkowo, regulacja na poziomie rozporządzenia jest niewystarczająca. Z uwagi na brak regulacji całościowej monitoringu wizyjnego, ważnym jest by regulacja tej kwestii w szkołach miała odzwierciedlenie w przepisach ustaw dotyczących oświaty. Ingerencja w prywatność powinna być właściwie uregulowana.

Projektodawca powinien odpowiedzieć na pytanie o **adekwatność wprowadzenia monitoringu wizyjnego do szkół** jako metody zapewniania bezpieczeństwa w szkole. Zgodnie z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych administrator danych powinien zapewnić, by przetwarzane informacje (wizerunki, dane osobowe zwykłe i wrażliwe) były adekwatne do celów, w jakich są przetwarzane. Dlatego też należy ocenić, czy inne mniej inwazyjne rozwiązania nie przyniosłyby oczekiwanych efektów w zakresie zapewniania bezpieczeństwa.

W związku z tym należy wskazać na potrzebę przeprowadzenia dla każdych, zwłaszcza nowo wprowadzanych rozwiązań, **analizy potrzeb i celowości budowy systemu**, w której podmiot podejmujący decyzję o budowie lub rozbudowie systemu monitoringu zobowiązany będzie do przeprowadzenia prognozy skuteczności funkcjonowania systemu, analizy rozwiązań alternatywnych i specyfiki zagrożeń w danym rejonie, optymalnego rozmieszczenia kamer oraz

ocenę wpływu projektowanego systemu na prywatność (tzw. ***Privacy Impact Assessment***). Zgodnie z projektem unijnego rozporządzenia o ochronie danych osobowych[1], które ma w najbliższych latach wejść w życie, takie oceny będą obowiązkowe w przypadku operacji przetwarzania stwarzających ryzyko dla ochrony praw i wolności podmiotów danych. Jako stwarzające ryzyko dla praw i wolności wskazano w tym projekcie m.in. prowadzenie monitoringu wizyjnego. Analizy te powinny także obejmować **problem przetwarzania danych innych osób**, które mogą znaleźć się na obszarze monitorowanym, gdyż z treści projektu Programu wynika, że monitoringowi mają podlegać m.in. wejścia i otoczenie szkoły (punkt IV załącznika do uchwały RM, s. 19). W tych obszarach mogą znaleźć się osoby, które nie będą świadome, iż teren placówki objęty jest monitoringiem czy też przebywający na tym terenie w innych celach niż korzystanie z usług placówki. Także wobec nich administrator danych, którym będzie kierownik jednostki, ma zobowiązania do: poinformowania o stosowaniu obserwacji, zapewnienia dostępu do danych tych osób dotyczących i ich zabezpieczenia przed niepowołanym dostępem. Oddzielną kwestią jest przetwarzanie przy pomocy kamer monitoringu danych nauczycieli i innych pracowników szkoły. Nie powinien on służyć do realizacji celu kontrolowania poczynań pracowników i uczniów, jako metoda nadmierna. Elektroniczny system nie powinien zastąpić bieżącego nadzoru, jaki przełożony może sprawować nad swoimi podwładnymi oraz nauczyciel nad uczniami.

To na ustawodawcy spoczywa obowiązek ustalenia zasad gromadzenia i udostępniania nagrań, tak by uniknąć dowolności w tym zakresie, która może wystąpić, jeżeli szkołom pozostawiona byłaby daleko idąca swoboda, jak ma to miejsce obecnie. Ogólnikowe regulacje są w tym przypadku niewystarczające i wymagają daleko posuniętego doprecyzowania. **Sygnały otrzymywane przez Biuro GIODO na temat nieuporządkowanego stosowania monitoringu wizyjnego, nie tylko w placówkach oświatowych, wskazują na możliwe negatywne konsekwencje.** Obywatele poddani monitoringowi mogą odczuwać długotrwały dyskomfort psychiczny związany z postrzeganym przez nich znaczącym naruszeniem prywatności. Jednocześnie widoczne są tendencje do poszerzania zakresu monitoringu o nowe wymiary, jak chociażby możliwość stosowania, obok rejestracji obrazu, także nagrywania dźwięku, czyli podsłuchiwania rozmów. Powstaje pytanie, czy nawet najlepiej przygotowane i kompetentni pracownicy szkół będą w stanie w sposób wystarczający zapewnić ochronę praw użytkowników tych instytucji w obliczu braku określenia przez państwo jasnych reguł dozwolonego postępowania.

W związku z tym każdorazowe wprowadzanie regulacji dotyczących monitoringu wizyjnego powinno podlegać ocenie zgodnie z **zasadą proporcjonalności ujętą w art. 31 ust. 3 Konstytucji.** Prawo do ochrony informacji dotyczących osoby, ujęte w art. 51 Konstytucji może

[1] Wniosek dotyczący Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych, COM(2012) 11, Dz. Urz. C 102 z dnia 5 kwietnia 2012 r., s. 24.

być ograniczone m.in., gdy jest to konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego. Ocena, czy monitoring wizyjny może być stosowany, jak słusznie stwierdził projektodawca, powinna opierać się na ocenie efektywności alternatywnych, możliwych do zastosowania środków mających na celu zapewnienie bezpieczeństwa. Należy tutaj przypomnieć także stanowisko Grupy Roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, zwanej dalej Grupą roboczą art. 29. Szerokie rozprzestrzenienie monitoringu w przestrzeni publicznej i prywatnej nie powinno w sposób nieuzasadniony ograniczać praw i wolności jednostki.[2]

Również brak jasnego uregulowania w zakresie **zasad pozyskiwania, gromadzenia i udostępniania nagrań** powinien zostać uzupełniony. Powinny one być adekwatne do zakładanych celów monitoringu. Tylko w takiej sytuacji możliwe będzie wprowadzanie monitoringu na prostych i klarownych zasadach. To umożliwiłoby administratorom spełnianie zobowiązań wobec osób obserwowanych do poszanowania ich prywatności i zapewniania bezpieczeństwa. Art. 32 ustawy o ochronie danych osobowych dotyczy praw do kontroli przetwarzania danych, które jej dotyczą. Zasady udostępniania nagrań z monitoringu powinny regulować także uprawnienia osób obserwowanych do dostępu, żądania usunięcia lub wniesienia sprzeciwu wobec przetwarzania ich danych. Kwestie te są ściśle związane z respektowaniem jeszcze innego obowiązku, a mianowicie obowiązku informacyjnego. Właściwie ukształtowane zasady muszą być w sposób klarowny przekazywany osobom obserwowanym poprzez **realizację obowiązku informacyjnego**. Nie powinno być możliwym zbieranie danych bez wiedzy tych osób. Realizacja obowiązku powinna się odbywać przez tablice informacyjne, piktogramy, wyraźne oznaczenie kamer oraz łatwo dostępne polityki prywatności, o czym organ ds. ochrony osobowych szeroko pisał w uwagach do projektu założeń do ustawy o monitoringu wizyjnym. Z uwagi na specyficzny charakter przetwarzania bez dodatkowej regulacji administratorzy danych mogą mieć trudności w realizacji obowiązków wynikających z ustawy o ochronie danych osobowych.

Projektodawca nie wskazał w żaden sposób, **jakie obszary na terenie szkoły mogą być obserwowane.** Koniecznym jest rozstrzygnięcie, czy ma się to odbywać także w klasach. Generalny Inspektor zaleca w tym obszarze daleko idącą ostrożność i przestrzega przed pozostawianiem takich decyzji administratorom danych – dyrektorom i kierownikom placówek – ponieważ może to rodzić nieprawidłowości i negatywne konsekwencje, a przede wszystkim nie służyć założonym celom.

Generalny Inspektor zwraca uwagę, iż konieczne jest uregulowanie **zasady ograniczenia czasowego przetwarzania danych** uzyskanych w toku pracy systemów monitoringu. Ma ona

[2] Opinia Grupy Roboczej art. 29 nr 4/2004 o przetwarzaniu danych osobowych przy pomocy wideomonitoringu z dnia 11 lutego 2004 r., 11750/02/EN WP89, s. 4.

bezpośredni związek z okresem retencji danych. Nie powinno się pozostawiać administratorom swobody w zdefiniowaniu okresu retencji z perspektywy funkcjonowania poszczególnych systemów. Celem, który przyświeca projektodawcy ma być bezpieczeństwo użytkowników szkoły. W sierpniu 2014 r. Generalny Inspektor sygnalizował, iż w niektórych państwach maksymalny okres przechowywania wynosi 72 godziny. Wydaje się zasadnym maksymalne ograniczenie okresu retencji, gdyż w szkołach mają być stosowane także inne metody zapewniania bezpieczeństwa. Ewentualne nagrania, które mogą być istotne dla wyjaśniania niepożądanych zdarzeń, mogą być zabezpieczane w okresie krótszym, gdyż sprawdzenie nagrań z systemu monitoringu będzie wykonywane w pierwszej kolejności. Nagrania nie powinny być także przechowywane dłużej dla innych, niż zapewnianie bezpieczeństwa celów. Retencja danych powinna być za każdym razem dostosowywana do celu realizowanego przez administratora. Nie powinno też dochodzić do gromadzenia nagrań na zapas.

W zakresie technologii mających być wprowadzonymi do monitorowania przestrzeni nie wskazano: jaką jakość mają mieć nagrania, czy dopuszczalne będzie rejestrowanie także dźwięku oraz czy oprogramowanie będzie umożliwiało analizę rejestrowanych obrazów (identyfikacja wizerunków, wykrywanie zachowań niepożądanych itp.). Dopuszczenie takich rozwiązań byłoby wysoce dyskusyjne z punktu widzenia ochrony podmiotu danych i z tego powodu potrzebne jest precyzyjne ustalenie kryteriów technicznych. Bez takiego uregulowania może dochodzić do daleko idących różnic w systemach używanych w szkołach. Z uwagi na specyfikę technologii i ryzyk związanych z tą formą przetwarzania danych warunki techniczne mogłyby być uregulowane na poziomie ustawy. Potrzebne jest także **uregulowanie zasad zabezpieczania wytworzonych nagrań przed dostępem osób nieupoważnionych**. W zależności od zastosowanych technologii przesyłu może to wiązać się ze stosowaniem szyfrowania transmisji bezprzewodowych albo zabezpieczenie połączeń między systemem zapisującym a kamerami.

Niezależnie od wątpliwości zgłoszonych w zakresie monitoringu wizyjnego, organ ds. ochrony danych osobowych popiera działania mające na celu zwiększenie szeroko rozumianego bezpieczeństwa użytkowników szkół oraz angażowanie w sprawy edukacji i wychowania dzieci szerokiego spektrum podmiotów działających w obszarze szkolnictwa. Sugestie zgłoszone powyżej powinny zostać potraktowane jako wkład w przygotowanie dobrych rozwiązań, które będą mogły służyć przez cały okres realizacji Programu Bezpieczna+ oraz w kolejnych perspektywach programowych. Generalny Inspektor zgłasza gotowość do aktywnego udziału w dalszych pracach nad programem i w tym zakresie zachęca projektodawcę do kontaktu.