# Dane osobowe pod kluczem – najczęstsze uchybienia

**Wielość i niejasność przepisów odnoszących się do przetwarzania danych osobowych przez placówki oświatowe, a także bolesna „szczupłość" środków finansowych do dyspozycji szkół powodują, że trudno znaleźć szkołę, która przetwarzałaby dane osobowe w sposób niepowodujący naruszenia przepisów o ochronie danych osobowych. Poważnym problemem są też utarte od wielu lat schematy procesów związanych z ochroną danych, niekoniecznie zgodne z wymaganiami ustawowymi.**

Powyższe stwierdzenie zostało dowiedzione w praktyce podczas kontroli przeprowadzonych przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO) w 2008 r. Mimo że zakres przedmiotowy kontroli ograniczony był wyłącznie do sposobu zabezpieczenia danych osobowych, bez badania pozostałych wymogów ustawowych, to i tak ich wyniki okazały się zatrważające. W każdej z kontrolowanych szkół stwierdzono bowiem uchybienia w procesie przetwarzania danych osobowych. Co więcej, szereg audytów przeprowadzonych w szkołach w ostatnich miesiącach przez firmę ABI Consult potwierdził wyniki kontroli GIODO z 2008 r.

**Na porządku dziennym jest wynoszenie przez nauczycieli poza teren szkoły dokumentów zawierających dane osobowe, a w szczególności klasówek, kartkówek czy też innych prac napisanych przez uczniów.**

## PRZECHOWYWANIE I PRZETWARZANIE DOKUMENTACJI

Podstawowy problem związany jest z tym, że szkoły nie stosują odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, naruszając tym samym obowiązek wynikający z art. 36 ust. 1 *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (zwanej dalej *Ustawą*). Objawia się to m.in. przechowywaniem dokumentacji zawierającej dane osobowe w warunkach umożliwiających dostęp do niej osobom nieupoważnionym. Przez dokumentację zawierającą dane osobowe trzeba w szczególności rozumieć: dokumentację przebiegu nauczania, działalności wychowawczej i opiekuńczej, sprawozdania z posiedzeń rady pedagogicznej w sprawie klasyfikacji itd. Dokumentacja ta umieszczana jest zwykle na otwartych regałach i w niezamykanych na klucz szafach. Zdarzają się również nie tak rzadkie przypadki przechowywania dokumentacji w zamkniętych szafach z kluczem pozostawionym w zamku, co nie wymaga chyba komentarza.

W tym miejscu warto poświęcić kilka słów na omówienie sposobu zarządzania kluczami. Jest to zagadnienie dość często zaniedbywane w szkołach i związane najczęściej z brakiem jednolitych procedur. Niejednokrotnie zdarza się, że nauczyciele decydują, czy zabiorą klucze ze sobą do domu, czy też przekażą je innemu pracownikowi albo zdadzą na portierni. Ponadto, nawet w przypadku zdania klucza do pomieszczenia (nie mówiąc już o ich pobieraniu), fakt ten najczęściej nie jest potwierdzany w **ewidencji pobranych i zdanych kluczy**. Na porządku dziennym jest również nieprzekazywanie na portiernię wykazów osób upoważnionych do pobierania kluczy do określonych pomieszczeń. Oznacza to w konsekwencji, że dostęp do tych kluczy może mieć bliżej nieokreślony krąg osób. Wprowadzenie jednolitych zasad postępowania – i to zarówno z kluczami do pomieszczeń, jak i z kluczami do szaf znajdujących się w salach – ma istotne znaczenie także z uwagi na to, że w pomieszczeniach tych, o czym już wspomniano, mogą przebywać osoby postronne. Chodzi tu przede wszystkim o pracowników, którzy zwykle wykonują swoje obowiązki po godzinach pracy osób upoważnionych do przetwarzania danych, takich jak np. personel sprzątający, pracownicy odpowiedzialni

za konserwację i naprawę sprzętów, instalację i aktualizację oprogramowania komputerowego, czy też uczniów i ich rodziców.

Należy zwrócić uwagę, że szkoły często nie wykorzystują już istniejących rozwiązań w zakresie bezpieczeństwa. Jako przykład można tu wskazać zainstalowane **kamery przemysłowe**. System monitoringu przewidziany jest przede wszystkim w celu zapewnienia bezpieczeństwa uczniów, ale nic nie stoi na przeszkodzie, aby niejako „przy okazji" wykorzystać go również do monitorowania miejsc, w których przechowywane są dane osobowe. Zazwyczaj szkołom obce są także te rozwiązania, które nie wymagają żadnych inwestycji finansowych, jak np. wprowadzenie „polityki **czystego biurka"**, nakładającej na pracownika obowiązek schowania wszelkich dokumentów przed opuszczeniem stanowiska pracy.

Na problemy związane z bezpieczeństwem danych osobowych należy koniecznie uczulić samych nauczycieli. Na porządku dziennym jest bowiem wynoszenie przez nich poza obszar przetwarzania danych osobowych (przede wszystkim poza budynek szkoły) dokumentów zawierających dane osobowe, a w szczególności klasówek, kartkówek czy też innych prac napisanych przez uczniów. Przy przetwarzaniu danych osobowych (np. w celu wydrukowania świadectw) nauczyciele dosyć często korzystają także ze swoich prywatnych komputerów i wymiennych nośników danych, jak np. pendrive. Postępowanie takie jest jednoznacznie kwalifikowane jako naruszenie przepisów o ochronie danych osobowych, gdyż jego wynikiem jest znaczne poszerzenie kręgu osób, które potencjalnie mogą uzyskać nieuprawniony dostęp do danych osobowych (członkowie rodziny nauczyciela, znajomi).

Kolejne powtarzające się w szkołach naruszenie bezpieczeństwa danych osobowych związane jest z przesyłaniem tych danych z/na prywatne konta e-mailowe nauczycieli. Taki transfer odbywa się zwykle w formie niezabezpieczonej. Bardzo istotną kwestią w poruszanych powyżej zagadnieniach jest również fakt całkowitej utraty kontroli nad sposobem zabezpieczenia danych osobowych przez administratora danych (szkołę w osobie dyrektora).

Naruszeniem bezpieczeństwa danych osobowych uczniów jest także **publikowanie wyników postępowania rekrutacyjnego** na stronie internetowej szkoły lub w Biuletynie Informacji Publicznej oraz wywieszanie ich, np. w szkolnych gablotach. Skutkiem takiego postępowania jest bowiem umożliwienie dostępu do danych wszystkim osobom, a nie tylko rodzicom dziecka. Informacja o wynikach rekrutacji powinna zostać im przekazana indywidualnie.

## POLITYKA BEZPIECZEŃSTWA I INNE REGULACJE ZASAD PRZETWARZANIA DANYCH

Liczne zastrzeżenia wzbudzają również (jeżeli w ogóle zostały opracowane) **polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym** służącym do przetwarzania danych osobowych – dwa główne dokumenty wymagane przez *Ustawę* i regulujące zasady przetwarzania danych osobowych w szkole. Braki merytoryczne dotyczące polityki obejmują w szczególności: prawidłowo zdefiniowanego obszaru przetwarzania danych, wykazu zbiorów danych osobowych, opisu struktury zbiorów danych oraz sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi.

**Nadzór nad przestrzeganiem zasad ochrony danych osobowych w szkole jest iluzoryczny.**

Należy również zadbać, aby instrukcja zarządzania systemem informatycznym zawierała: procedury nadawania uprawnień do przetwarzania danych, określenie metod i środków uwierzytelnienia użytkownika, procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie oraz tworzenia kopii zapasowych środowiska informatycznego wykorzystywanego do przetwarzania danych osobowych. Instrukcja powinna określać także sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe, w tym również kopii awaryjnych. W instrukcji powinno się ponadto określić sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, co w praktyce wiąże się z ustaleniem sposobu ochrony logicznej sieci wewnętrznej szkoły przed nieuprawnioną ingerencją z internetu oraz zdefiniowaniem zasad korzystania z systemu antywirusowego. W wielu placówkach zapomina się niestety, że elementy wymagane w polityce i instrukcji stanowią katalog otwarty, co oznacza, że w dokumentacji tej prawie zawsze brak było ustaleń regulujących, a w zasadzie zabraniających, np. wynoszenia ze szkoły przez nauczycieli prac uczniów czy też korzystania przez nich z prywatnego sprzętu komputerowego.

Duże wątpliwości budzi również etap wdrożenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym. Często okazuje się bowiem, że na-

*Zdarzają się przypadki umieszczania dokumentacji w zamkniętych szafach z kluczem pozostawionym w zamku.*

uczyciele i inni pracownicy szkoły przetwarzający dane osobowe nie zapoznali się z regulacjami zawartymi we wskazanej powyżej dokumentacji lub w ogóle nie wiedzą o jej istnieniu.

**Niedopuszczalne jest przenoszenie przez ucznia na polecenie nauczyciela dziennika lekcyjnego z pokoju nauczycielskiego do klasy czy też z jednej sali lekcyjnej do drugiej.**

## ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI – *PERSONA GRATA*

Do częstych uchybień popełnianych przez szkoły należy brak administratora bezpieczeństwa informacji (tzw. ABI) lub wyznaczenie do sprawowania tej funkcji przypadkowej osoby, wyłącznie w celu spełnienia obowiązku wynikającego z art. 36 ust. 3 *Ustawy*. Zarówno w pierwszym, jak i w drugim przypadku nadzór nad przestrzeganiem zasad ochrony danych osobowych w szkole jest iluzoryczny. W konsekwencji prowadzi to do naruszenia innych obowiązków określonych w przepisach, a w szczególności wymagań związanych z nadawaniem upoważnień do przetwarzania danych osobowych czy też obowiązków dotyczących właściwego opracowania i wdrożenia dokumentacji, o której była mowa.

„Średni" stan ochrony danych osobowych w szkołach wynika w dużej mierze właśnie z braku ABI lub z wyznaczenia na tę funkcję osoby, która nie dysponuje wystarczająco szeroką wiedzą na tematy z zakresu bezpieczeństwa informacji.

## KTO MA, A KTO POWINIEN MIEĆ DOSTĘP DO DANYCH OSOBOWYCH W SZKOŁACH

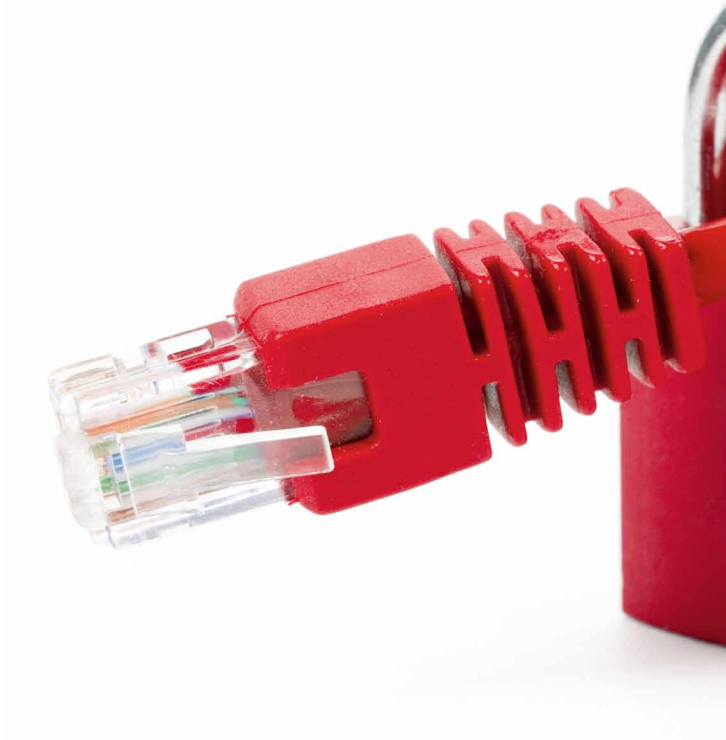
Dostęp do danych osobowych w szkołach powinny mieć wyłącznie osoby, którym wydane zostało stosowne **upoważnienie dyrektora**. Ważne, aby nie były one wydawane wszystkim pracownikom szkoły, bez względu na ich zakres obowiązków, ale wyłącznie tym osobom, którym jest to niezbędne w ramach wykonywanych czynności służbowych. Oznacza to, że z kręgu osób upoważnionych powinny zostać wyłączone np. osoby sprzątające oraz pracownicy odpowiedzialni za naprawę i konserwację sprzętu szkolnego. Nieupoważnieni do przetwarzania danych osobowych w szkole są również uczniowie tej placówki, z tego powodu niedopuszczalne jest (co niestety jest dość częstą praktyką) przenoszenie przez ucznia na polecenie nauczyciela dziennika lekcyjnego z pokoju nauczycielskiego do klasy czy też z jednej sali lekcyjnej do drugiej.

Upoważnienia do przetwarzania danych osobowych nie są nadawane także rodzicom uczniów, **ujawnianie na wywiadówkach szczegółowych informacji** na temat konkretnego ucznia jest zatem nie do przyjęcia. W obecności wszystkich rodziców dzieci uczących się w danej klasie mogą być poruszane wyłącznie te kwestie, które dotyczą całej klasy, natomiast jeśli nauczyciel chce porozmawiać o sprawach związanych z poszczególnymi uczniami, to musi to uczynić w trakcie indywidualnych rozmów.

Pewne wątpliwości może natomiast budzić kwestia, czy w ramach nadanego nauczycielowi upoważnienia do przetwarzania danych osobowych powinien mieć on dostęp do danych osobowych tych uczniów, których nie uczy. Biorąc jednak pod uwagę, że taki nauczyciel może zostać skierowany na zastępstwo do innej klasy lub uczestniczyć w innych wydarzeniach, które mogą uzasadniać konieczność posiadania danych takich uczniów, jak np. udział w wycieczce szkolnej, należy uznać, że dostęp nauczyciela do danych osobowych uczniów nie powinien być ograniczany wyłącznie do informacji o dzieciach, które uczy.

## EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Osoby, którym nadane zostały upoważnienia do przetwarzania danych osobowych, powinny zostać wpisane do **ewidencji osób upoważnionych** do ich przetwarzania. Z realizacją tego obowiązku w szkołach, w porównaniu z obowiązkiem nadawania upoważnień, jest już jednak znacznie gorzej. Zdarzają się bowiem przypadki placówek, w których taka ewidencja nie jest w ogóle prowadzona. Często prowadzona przez szkołę ewidencja osób upoważnionych do przetwarzania danych osobowych nie zawiera wszystkich wymaganych elementów, np. identyfikatora



w systemie informatycznym (tzw. loginu), daty nadania/ /ustania upoważnienia do przetwarzania danych osobowych czy zakresu tego upoważnienia. Liczne są również sytuacje wpisywania do ewidencji wyłącznie tych osób, które przetwarzają dane osobowe przy użyciu systemu informatycznego, z pominięciem pracowników korzystających nadal z tradycyjnych rozwiązań papierowych. Tymczasem w ewidencji osób upoważnionych do przetwarzania danych osobowych uwzględnione powinny zostać wszystkie osoby mające dostęp do danych osobowych, bez względu na formę, w jakiej je przetwarzają.

## UCHYBIENIA W SYSTEMACH INFORMATYCZNYCH – STAN NIEZMIENNY

Z przetwarzaniem danych osobowych w szkołach przy użyciu systemów informatycznych związana jest niestety duża liczba nieprawidłowości. Z uwagi na fakt, że przetwarzanie danych osobowych w systematach informatycznych w szkole będzie stanowić temat kolejnego artykułu we wrześniowym wydaniu „Miesięcznika Dyrektora Szkoły", w tym miejscu zaznaczymy tylko, że uchybienia pojawiające się w tym, bądź co bądź, szerokim obszarze dotyczą w szczególności: sposobu postępowania z kontami i hasłami użytkowników, niezabezpieczenia systemów informatycznych przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej, niewykonywania kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych osobowych, niestosowania mechanizmów kontroli dostępu do danych osobowych, a także nieodnotowania przez system informatyczny stosownych informacji dla każdej osoby, której dane osobowe są przetwarzane.

*Ważne jest, by transfer danych odbywał się w zabezpieczonej formie.*

Duży problem w procesie dostosowania warunków przetwarzania danych osobowych w formie elektronicznej do wymogów *Ustawy* – a *de facto Rozporządzenia 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* – stanowi fakt, że niektóre z użytkowanych programów informatycznych, takie jak np. System Informacji Oświatowej czy Hermes, zostały narzucone szkole przez struktury nadrzędne w randze ministerstwa. Powoduje to, że szkoły mają znikomy wpływ na funkcjonalności wskazanych powyżej aplikacji i bardzo ograniczone możliwości modyfikacji tego oprogramowania.

## PODSUMOWANIE

Opisane powyżej zagadnienia nie wyczerpują oczywiście tematu naruszenia przepisów *Ustawy o ochronie danych osobowych* w szkołach. Zawierają jedynie przypadki, z jakimi często styka się w swojej praktyce zawodowej zarówno inspektor GIODO, jak i audytor, spoglądający na sprawę niejako z drugiej strony „barykady". Pamiętać należy jednak, że „pomysłowość" ludzka oraz meandry bardziej lub mniej złośliwego losu działającego w obszarze ochrony danych nie znają żadnych granic, w tym również granic dobrego smaku i szacunku dla ludzkiej pracy i poczucia odpowiedzialności. Dlatego właśnie dyrektor szkoły wraz z administratorem bezpieczeństwa informacji powinni na bieżąco analizować zagrożenia pojawiające się w obszarze przetwarzania danych osobowych i stale dostosowywać do tych zagrożeń środki techniczne i organizacyjne, które zapewnią właściwą ochronę tych danych. Ważne jest również to, aby skuteczność zastosowanych środków podlegała okresowym badaniom, w toku których należy uwzględniać zmieniające się warunki przetwarzania danych osobowych, w tym także postęp techniczny, który – jak to zwykle bywa z postępem – wymusza unowocześnienie zastosowanych metod zabezpieczenia informacji.

Analiza przypadku wskazuje na to, że znakomita większość uchybień w procesie przetwarzania danych osobowych w szkołach wynika niestety w prostej linii z odwiecznych przyzwyczajeń ustalonych przez lata praktyki nauczycielskiej, niekoniecznie zgodnych z wymaganiami ustawowymi. Wszyscy uczestniczący w procesie przetwarzania danych osobowych w szkołach powinni zatem pamiętać o najważniejszym: o zmianie przyzwyczajeń.

***Adam Myziak***
*Konsultant, audytor, specjalista w dziedzinie ochrony danych osobowych. W latach 2000–2010 inspektor w Biurze GIODO. Obecnie prowadzi firmę konsultingową oferującą kompleksowe usługi w zakresie ochrony danych. Poprzez różnego rodzaju konferencje, szkolenia, warsztaty oraz publikacje aktywnie uczestniczy w procesie propagacji wiedzy na temat zgodnego z prawem i bezpiecznego przetwarzania danych osobowych w naszym kraju.*